

LOCALLY RECOVERABLE J -AFFINE VARIETY CODES

CARLOS GALINDO, FERNANDO HERNANDO AND CARLOS MUNUERA

ABSTRACT. A locally recoverable (LRC) code is a code over a finite field \mathbb{F}_q such that any erased coordinate of a codeword can be recovered from a small number of other coordinates in that codeword. We construct LRC codes correcting more than one erasure, which are subfield-subcodes of some J -affine variety codes. For these LRC codes, we compute localities (r, δ) that determine the minimum size of a set \bar{R} of positions so that any $\delta - 1$ erasures in \bar{R} can be recovered from the remaining r coordinates in this set. We also show that some of these LRC codes with lengths $n \gg q$ are $(\delta - 1)$ -optimal.

INTRODUCTION

The growth of the amount of stored information in large scale distributed and cloud storage systems makes the loss of data due to node failures a major problem. To obtain a reliable storage, when a node fails, we want to recover the data it contains by using information from other nodes. This is the *repair problem*. A naive solving method consists of the replication of information across several nodes. A more clever method is to protect the data using error-correcting codes, what has led to the introduction of locally recoverable (LRC) codes [11]. LRC codes are error-correcting codes for which one or more erased coordinates of a codeword can be recovered from a set of other coordinates in that codeword. As typical examples of this solution we can mention Google and Facebook storage systems that use Reed-Solomon (RS) codes to protect the information. The procedure is as follows: the information to be stored is a long sequence b of elements belonging to a finite field \mathbb{F}_{p^l} , where p is a prime number. This sequence is divided into blocks, $b = b_1, b_2, \dots, b_z$, of the same length h . According to the isomorphism $\mathbb{F}_{p^l}^h \cong \mathbb{F}_{p^{lh}}$, each of these blocks can be seen as an element of the finite field \mathbb{F}_q , with $q = p^s$ and $s = lh$. Fix an integer $k < q$. The vector $(b_1, b_2, \dots, b_k) \in \mathbb{F}_q^k$ is encoded by using a Reed-Solomon code of dimension k over \mathbb{F}_q , whose length n , $k < n \leq q$, is equal to the number of nodes that will be used in its storage. We choose $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{F}_q$ and send

$$f(\alpha_i) = b_1 + b_2\alpha_i + \dots + b_k\alpha_i^{k-1}$$

to the i -th node. Even if a node fails, we may recover the stored data (b_1, b_2, \dots, b_k) by using Lagrangian interpolation from any other k available nodes.

Note that this method is wasteful, since k symbols over n nodes must be used to recover just one erasure. Of course other error-correcting codes, apart from RS codes, can be used to deal more efficiently with the repair problem. Thus, in terms of coding theory the repair problem can be stated as follows: let \mathcal{C} be a linear code of length n and dimension k over \mathbb{F}_q . A coordinate $i \in \{1, 2, \dots, n\}$ is locally recoverable if there is a recovery set $R = R(i) \subset \{1, 2, \dots, n\}$ such that $i \notin R$ and for any codeword $\mathbf{x} \in \mathcal{C}$, an erasure at

Key words and phrases. LRC codes; subfield subcodes; J -affine variety codes.

Supported by the Spanish Government, Ministerio de Ciencia, Innovación y Universidades (MICINN)/FEDER (grants PGC2018-096446-B-C21 and PGC2018-096446-B-C22), Generalitat Valenciana (grant AICO-2019-223) and University Jaume I (grant PB1-1B2018-10).

position i of \mathbf{x} can be recovered by using the information given by the coordinates of \mathbf{x} with indices in R . The locality of the coordinate i is the smallest size of a recovery set for i . The code \mathcal{C} is *locally recoverable* (LRC) if each coordinate is so, and the *locality* of \mathcal{C} is the maximum locality of its coordinates. In Section 1 we shall specify these definitions. Note that strictly speaking, all codes \mathcal{C} of minimum distance $d(\mathcal{C}) > 1$ are locally recoverable; just take $\{1, 2, \dots, n\} \setminus \{i\}$ as a recovery set for coordinate i . However we are interested in codes admitting recovery sets as small as possible. Thus, in practice we restrict to consider codes with ‘moderate’ localities. In general, the locality r of an LRC code \mathcal{C} with parameters $[n, k, d]$ is upper-bounded as $r \leq k$. For example, MDS codes (RS codes in particular) of dimension k have locality k . Several lower bounds on r are known. The most commonly used is the Singleton-like bound (1).

Among the different classes of codes considered as good candidates for local recovering, cyclic codes and subfield-subcodes of cyclic codes play an important role, because the cyclic shifts of a recovery set again provide recovery sets [3, 12, 14, 22]. In this article we continue this line of research by using the very general language of affine variety codes. We consider specific J -affine variety codes, introduced in [9], whose subfield-subcodes provide LRC codes. These subfield-subcodes have large lengths over fields \mathbb{F}_q , and Theorems 2.8 and 2.9 provide bounds on their localities.

A variant of LRC codes was introduced in [19]. As multiple device failures may occur simultaneously, it is of interest to consider LRC codes correcting more than one erasure. This idea leads to the concept of localities (r, δ) of an LRC code \mathcal{C} , which measure the recovery capability of \mathcal{C} when at most $\delta - 2$ erasures occur in a recovery set (see Section 1 for a rigorous definition). LRC codes for multiple erasures have been subsequently studied in [3, 5, 1]. In [3] the authors constructed some classes of such LRC codes over \mathbb{F}_q , with lengths n such that either $n|q - 1$ or $n|q + 1$. Codes of similar type and unbounded length were given in [5]. Here $\delta = d - 1, d - 2$ or $\delta = d/2$, where d stands for the minimum distance.

The localities (r, δ) of an LRC code satisfy a Singleton-like bound ((2) in Section 1). Codes reaching equality for some (r, δ) , are called *optimal*. For example, the codes in [3, 5] are optimal. Note that, as for the original Singleton bound, the bounds (1) and (2) do not depend on the cardinality of the ground field \mathbb{F}_q . Some size dependent bounds can be found in [1].

A somewhat different definition of LRC code with localities (r, δ) is proposed in [15] for systematic codes. There, the purpose is to repair erasures on the information symbols of a codeword. Other related variants of LRC codes deal with sequential repair of erasures [20], the availability property [24], or the cooperative repair [21].

In this work we use affine variety constructions to obtain LRC codes suitable for multiple erasures, whose localities (r, δ) behave well (Theorems 2.14 and 2.15). In some cases these codes are optimal for the Singleton-like bound (2). Compared with the codes shown in [3], the ours are considerably longer, although not optimal in general. Let us recall here that most good currently known LRC codes have small lengths n , in comparison with the cardinality of the ground field q ; usually $n < q$, [13] (or $n = q + 1$ for some codes in [3]). For the opposite, our codes (as is the case with those in [5]) have lengths $n \gg q$.

The article is organized as follows: in Section 1 we recall some basic facts about LRC codes and introduce the concept of t -locality. Section 2 is devoted to develop and study LRC codes from affine varieties. In Subsection 2.1 we introduce J -affine variety codes which also gave rise to good quantum error-correcting codes in [8, 9, 6]. In subsections 2.2 and 2.3, we show that subfield-subcodes of several types of J -affine variety codes are

good LRC codes, and we determine some of their localities (r, δ) . Finally in Section 3 we give examples of LRC codes obtained by our procedure. We list some parameters and localities.

1. LRC CODES

In this section we state some definitions and facts concerning LRC codes that will be necessary for the rest of the work. We mostly follow the usual conventions and definitions of locally recoverable codes. As a notation, given a fixed coordinate i and a set R such that $i \notin R$, we write $\bar{R} = R \cup \{i\}$. Let \mathcal{C} be an $[n, k, d]$ code over \mathbb{F}_q . Let \mathbf{G} be a generator matrix of \mathcal{C} with columns $\mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_n$. A set $R \subseteq \{1, 2, \dots, n\}$ is a recovery set for a coordinate $i \notin R$ if $\mathbf{c}_i \in \langle \mathbf{c}_j : j \in R \rangle$, the linear space spanned by $\{\mathbf{c}_j : j \in R\}$. In this case, for any codeword $\mathbf{x} \in \mathcal{C}$, x_i can be obtained from the coordinates x_j , $j \in R$, just by solving the linear system whose augmented matrix is $(\mathbf{c}_j, j \in R \mid \mathbf{c}_i)$.

Let R be a set of cardinality $\#R = r$ and let $\pi_R : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^r$ be the projection on the coordinates in R . For $\mathbf{x} \in \mathbb{F}_q^n$ we write $\mathbf{x}_R = \pi_R(\mathbf{x})$. Often we shall consider the punctured and shortened codes:

$$\mathcal{C}[R] := \{\mathbf{x}_R : \mathbf{x} \in \mathcal{C}\} \text{ and } \mathcal{C}[[R]] := \{\mathbf{x}_R : \mathbf{x} \in \mathcal{C}, \text{supp}(\mathbf{x}) \subseteq R\},$$

respectively, where $\text{supp}(\mathbf{x})$ denotes the *support* of \mathbf{x} , $\text{supp}(\mathbf{x}) := \{i : x_i \neq 0\}$. Note that $\mathbf{c}_i \in \langle \mathbf{c}_j : j \in R \rangle$ if and only if $\dim(\mathcal{C}[R]) = \dim(\mathcal{C}[\bar{R}])$. So the notion of recovery set does not depend on the generator matrix chosen. If $\mathbf{c}_i \in \langle \mathbf{c}_j : j \in R \rangle$, there exist $w_1, w_2, \dots, w_n \in \mathbb{F}_q$ such that $\sum_{j=1}^n w_j \mathbf{c}_j = 0$ with $w_i \neq 0$ and $w_j = 0$ if $j \notin \bar{R}$. Then $\mathbf{w} = (w_1, w_2, \dots, w_n) \in \mathcal{C}^\perp$, the dual of \mathcal{C} , and $\mathbf{w}_R \in \mathcal{C}^\perp[[R]]$. Thus R is a recovery set for the coordinate i if and only if there exists a word $\mathbf{w}_R \in \mathcal{C}^\perp[[R]]$ with $w_i \neq 0$. In this case $\#R \geq d(\mathcal{C}^\perp) - 1$.

The smallest cardinality of a recovery set R for a coordinate i is the locality of i . The locality of \mathcal{C} , often denoted by $r = r(\mathcal{C})$, is the largest locality of any of its coordinates. Thus, we have proved the following result.

Proposition 1.1. *The locality r of an LRC code \mathcal{C} satisfies $r \geq d(\mathcal{C}^\perp) - 1$.*

A code \mathcal{C} reaching equality in the bound given by Proposition 1.1 will be called *sharp*. Note that all cyclic codes are sharp. Apart from Proposition 1.1, perhaps the most important bound on the locality r of an LCR code with parameters $[n, k, d]$ is given by the following Singleton-like inequality, see [11].

Theorem 1.2. *The locality r of an LRC code \mathcal{C} satisfies*

$$(1) \quad d + k + \left\lceil \frac{k}{r} \right\rceil \leq n + 2.$$

The difference between the two terms in Theorem 1.2, $D_1 := n + 2 - d - k - \lceil k/r \rceil$, is the *LRC-Singleton defect* of \mathcal{C} . Codes with $D_1 = 0$ are called *Singleton-optimal* (or simply *optimal*). While optimal LRC codes are known for all lengths $n \leq q$, [16], the problem of finding codes of this type when $n > q$ is currently a challenge [13]. To avoid confusion in what follows, we shall sometimes refer to r as the *classical* locality of \mathcal{C} .

The LRC codes that we have described above allow local recovery of the information stored in a failed node. However, concurrent failures of several nodes in a network are also possible and uncommon. This problem was first treated in [19]. According to the definition given in that article, an LRC code \mathcal{C} has locality (r, δ) if for any coordinate i there exists a set of positions $\bar{R} = \bar{R}(i) \subset \{1, 2, \dots, n\}$ such that

(RD1) $i \in \overline{R}$ and $\#\overline{R} \leq r + \delta - 1$; and

(RD2) $d(\mathcal{C}[\overline{R}]) \geq \delta$.

The sets \overline{R} satisfying the above conditions (RD1) and (RD2) are called (r, δ) recovery sets. Given such a set \overline{R} and $i \in \overline{R}$, the correction capability of $\mathcal{C}[\overline{R}]$ can be used to correct an erasure at position i plus any other $\delta - 2$ erasures in $\overline{R} \setminus \{i\}$. Notice that the original definition of locality of LRC codes corresponds to the case $\delta = 2$. Provided that $\delta \geq 2$, any subset $R \subset \overline{R}$ of cardinality r with $i \notin R$, satisfies $d(\mathcal{C}([R] \cup \{i\})) \geq 2$ and consequently R is a recovery set for i . Thus if \mathcal{C} has a locality (r, δ) , then the classical locality of \mathcal{C} is $\leq r$ and the number of recovery sets of cardinality r for any coordinate i is at least

$$\binom{\#\overline{R} - 1}{r},$$

which can be relevant to improve the availability of \mathcal{C} for recovering erasures. We remark that associated to \mathcal{C} we have several localities (r, δ) , corresponding to the $d(\mathcal{C}) - 1$ values of $\delta = 2, 3, \dots, d(\mathcal{C})$. These localities satisfy the following generalization of the Singleton-like bound of Theorem 1.2, which was proved in [19].

Proposition 1.3. *Let \mathcal{C} be an LRC code with parameters $[n, k, d]$ and locality (r, δ) . Then, the following inequality holds*

$$(2) \quad d + k + \left(\left\lceil \frac{k}{r} \right\rceil - 1 \right) (\delta - 1) \leq n + 1.$$

Analogously to what was done for the classical locality r , for $t = 1, 2, \dots, d(\mathcal{C}) - 1$, in this article we define

$$r_t = r_t(\mathcal{C}) := \min \left\{ \rho : \text{for all } i = 1, 2, \dots, n, \text{ there is a set } \overline{R}_i \subseteq \{1, 2, \dots, n\} \right. \\ \left. \text{with } i \in \overline{R}_i, \#\overline{R}_i \leq \rho \text{ and } d(\mathcal{C}[\overline{R}_i]) \geq t + 1 \right\} - 1.$$

The value r_t is the minimum number of positions, $\#\overline{R} - 1$, needed to recover a given coordinate $i \in \overline{R}$ of any codeword \mathbf{x} , when at most t erasures occur in $\mathbf{x}_{\overline{R}}$. Clearly r_1 is the classical locality of \mathcal{C} . We refer to r_t as the t -locality of \mathcal{C} . For example, since puncturing $< d$ times an MDS code gives a new MDS code of the same dimension, for $t < d$ the t -locality of an $[n, k, d]$ MDS code is $r_t = k + t - 1$.

Note that from the above definitions, the code \mathcal{C} has locality (ρ, δ) if and only if $r_{\delta-1} \leq \rho + \delta - 2$. Thus we can translate the bound given by Proposition 1.3 in terms of r_t 's, as

$$(3) \quad d + k + \left\lceil \frac{k}{r_t - t + 1} \right\rceil t \leq n + t + 1.$$

The difference between the two terms of Inequation (3)

$$(4) \quad D_t := n + t + 1 - d - k - \left\lceil \frac{k}{r_t - t + 1} \right\rceil t,$$

is the t -th LRC-Singleton defect of \mathcal{C} . Codes with $D_t = 0$ will be called t -optimal. For example, MDS codes are t -optimal for all $t = 1, 2, \dots, d - 1$.

The sequence $(r_1, r_2, \dots, r_{d-1})$ we have associated to an LRC code \mathcal{C} , resembles, up to some extent, the weight hierarchy of \mathcal{C} . Let us recall that for $t = 1, 2, \dots, k = \dim(\mathcal{C})$, the t -th *generalized Hamming weight* of \mathcal{C} is defined as

$$d_t = d_t(\mathcal{C}) := \min \{ \#\text{supp}(E) : E \text{ is a } t\text{-dimensional subcode of } \mathcal{C} \},$$

where $\text{supp}(E) := \{i : \text{there exists } \mathbf{x} \in E \text{ with } x_i \neq 0\}$, see [18, Section 3.3]. We extend the bound given by Proposition 1.1 to all localities r_t 's in the following new result.

Proposition 1.4. *For $t = 1, 2, \dots, d-1$, the t -locality of an $[n, k, d]$ LRC code \mathcal{C} satisfies $r_t \geq d_t(\mathcal{C}^\perp) - 1$, where $d_t(\mathcal{C}^\perp)$ is the t -th generalized Hamming weight of the dual code \mathcal{C}^\perp .*

Proof. First note that $d-1 \leq \dim(\mathcal{C}^\perp)$. Let \bar{R} be a set of coordinates such that $\#\bar{R} \leq r_t + 1$ and $d(\mathcal{C}[\bar{R}]) \geq t + 1$. According to the Singleton bound, we have $\dim(\mathcal{C}[\bar{R}]) \leq \#\bar{R} - t$. Since $\mathcal{C}[\bar{R}]^\perp = \mathcal{C}^\perp[[\bar{R}]]$ (see [18], Proposition 3.1.17), it holds that $\dim(\mathcal{C}^\perp[[\bar{R}]]) \geq t$. Thus $d_t(\mathcal{C}^\perp) \leq \#\bar{R}$ and the result follows. \square

The above result can be stated in terms of localities (r, δ) as follows.

Corollary 1.5. *Let \mathcal{C} be an LRC code with locality (r, δ) . Then the following inequality holds*

$$r + \delta \geq d_{\delta-1}(\mathcal{C}^\perp) + 1.$$

Proof. From the definition of locality (r, δ) we have $r_{\delta-1} \leq r + \delta - 2$. Since $r_t < r_{t+1}$ for all $1 \leq t \leq d-2$, we deduce $r_{\delta-1} = r + \delta - 2$. Then, Proposition 1.4 gives $r + \delta \geq d_{\delta-1}(\mathcal{C}^\perp) + 1$. \square

2. J -AFFINE VARIETY CODES GIVING LRC CODES

In this section we show that subfield-subcodes of some codes arising from J -affine varieties are LRC codes with good recovery properties. We keep the notations as in the previous sections. In particular our LRC codes will be defined over the finite field \mathbb{F}_q , where $q = p^s$ and p is a prime number. We shall consider an extension field \mathbb{F}_Q of \mathbb{F}_q , where $Q = p^\ell$ and s divides ℓ . The affine varieties we manage, and so the codes arising from them, will be defined over \mathbb{F}_Q . Subfield-subcodes of these codes will be defined over \mathbb{F}_q .

The concept of J -affine variety code was introduced in [9] and used in [6, 7] for constructing quantum and LCD codes with good parameters. In the first subsection we recall the construction of J -affine variety codes over \mathbb{F}_Q and their subfield-subcodes over \mathbb{F}_q .

2.1. J -affine variety codes and their subfield-subcodes. Let \mathbb{F}_q , $q = p^s$, be a finite field and let \mathbb{F}_Q , $Q = p^\ell$, be an extension field of \mathbb{F}_q . Let $\mathfrak{R} := \mathbb{F}_Q[X_1, X_2, \dots, X_m]$ be the polynomial ring in $m \geq 1$ variables over \mathbb{F}_Q . For simplicity we will often write the monomial $X_1^{a_1} X_2^{a_2} \dots X_m^{a_m} \in \mathfrak{R}$ as $X^{\mathbf{a}}$, with $\mathbf{a} = (a_1, a_2, \dots, a_m)$. Fix positive integers $N_j > 1$, $j = 1, 2, \dots, m$, such that $N_j - 1$ divides $Q - 1$. Let J be a subset of indices of variables, $J \subseteq \{1, 2, \dots, m\}$, and let I_J be the ideal of \mathfrak{R} generated by the binomials $X_j^{N_j-1} - 1$ if $j \in J$, and $X_j^{N_j} - X_j$ if $j \notin J$. Denote by \mathfrak{R}_J the quotient ring $\mathfrak{R}_J = \mathfrak{R}/I_J$. Set $T_j = N_j - 2$ if $j \in J$ and $T_j = N_j - 1$ otherwise, and let

$$\mathcal{H}_J := \{0, 1, \dots, T_1\} \times \{0, 1, \dots, T_2\} \times \dots \times \{0, 1, \dots, T_m\}.$$

Let $Z_J = \{P_1, P_2, \dots, P_{n_J}\}$ be the set of zeros of I_J over \mathbb{F}_Q . This set has cardinality

$$n_J = \prod_{j \notin J} N_j \prod_{j \in J} (N_j - 1).$$

Consider the well-defined evaluation map

$$\text{ev}_J : \mathfrak{R}_J \rightarrow \mathbb{F}_Q^{n_J}, \quad \text{ev}_J(f) = (f(P_1), f(P_2), \dots, f(P_{n_J})),$$

where f denotes both the polynomial in \mathfrak{R} and its corresponding equivalence class in \mathfrak{R}_J .

Definition 2.1. Given a non-empty subset $\Delta \subseteq \mathcal{H}_J$, the J -affine variety code E_Δ^J , is the linear subspace $E_\Delta^J := \langle \text{ev}_J(X^{\mathbf{a}}) : \mathbf{a} \in \Delta \rangle \subseteq \mathbb{F}_Q^{n_J}$.

Then E_{Δ}^J is a linear code over \mathbb{F}_Q . Its length is n_J and its dimension equals the cardinality of Δ , since ev_J is injective, [9]. Recall that $q = p^s$ where s divides ℓ and thus \mathbb{F}_q is a subfield of \mathbb{F}_Q .

Definition 2.2. The *subfield-subcode* of E_{Δ}^J over the field \mathbb{F}_q , denoted \mathcal{C}_{Δ}^J , is the linear code $\mathcal{C}_{\Delta}^J := E_{\Delta}^J \cap \mathbb{F}_q^{n_J}$.

In order to study the codes \mathcal{C}_{Δ}^J , we shall manage the elements of \mathcal{H}_J in a particular manner. Let j , $1 \leq j \leq m$. If $j \in J$ then we identify the set $\{0, 1, \dots, T_j\}$ with the ring $\mathbb{Z}/(T_j+1)\mathbb{Z}$. When $j \notin J$, we identify the set $\{1, 2, \dots, T_j\}$ with $\mathbb{Z}/T_j\mathbb{Z}$, and we extend the addition and multiplication of this ring to $\{0, 1, \dots, T_j\}$, by setting $0 + \alpha = \alpha$, $0 \cdot \alpha = 0$ for all $\alpha = 0, 1, \dots, T_j$. The reason that explains these different ways of treating $\{0, 1, \dots, T_j\}$ is the fact that the evaluation of monomials containing X_j^0 or containing $X_j^{N_j-1}$ may be different when $j \notin J$, see [6] for details.

Under the above conventions, a set $\mathfrak{S} \subseteq \mathcal{H}_J$ is a *cyclotomic set with respect to q* if $q\mathbf{y} \in \mathfrak{S}$ for all $\mathbf{y} = (y_1, y_2, \dots, y_m) \in \mathfrak{S}$. Minimal cyclotomic sets are those of the form $\mathfrak{I} = \{q^i \mathbf{y} : i \geq 0\}$, for some element $\mathbf{y} \in \mathcal{H}_J$. For each minimal cyclotomic set \mathfrak{I} , we consider a unique representative $\mathbf{a} = (a_1, a_2, \dots, a_m) \in \mathfrak{I}$, constructed iteratively as follows: $a_1 = \min\{y_1 : (y_1, y_2, \dots, y_m) \in \mathfrak{I}\}$, and $a_j = \min\{y_j : (a_1, a_2, \dots, a_{j-1}, y_j, \dots, y_m) \in \mathfrak{I}\}$ for $j = 2, 3, \dots, m$. We shall denote by $\mathfrak{I}_{\mathbf{a}}$ the minimal cyclotomic set with representative \mathbf{a} and by $i_{\mathbf{a}}$ the cardinality of $\mathfrak{I}_{\mathbf{a}}$. Thus $\mathfrak{I}_{\mathbf{a}} = \{\mathbf{a}, q\mathbf{a}, \dots, q^{(i_{\mathbf{a}}-1)}\mathbf{a}\}$.

Let \mathcal{A} be the set of representatives of all minimal cyclotomic sets in \mathcal{H}_J . Given a non-empty subset $\Delta \subseteq \mathcal{H}_J$, we define $\mathcal{A}(\Delta) = \{\mathbf{a} \in \mathcal{A} : \mathfrak{I}_{\mathbf{a}} \subseteq \Delta\}$. The set Δ is called *closed* if it is a union of minimal cyclotomic sets, that is, if

$$\Delta = \bigcup_{\mathbf{a} \in \mathcal{A}(\Delta)} \mathfrak{I}_{\mathbf{a}}.$$

An important tool to study subfield-subcodes is the trace map. Since we are interested in subfield-subcodes over \mathbb{F}_q of evaluation codes over \mathbb{F}_Q , for $\mathbf{a} \in \mathcal{A}$ we consider the map

$$\mathcal{T}_{\mathbf{a}} : \mathfrak{R}_J \rightarrow \mathfrak{R}_J, \quad \mathcal{T}_{\mathbf{a}}(f) = f + f^q + \dots + f^{q^{(i_{\mathbf{a}}-1)}}.$$

Let $\xi_{\mathbf{a}}$ be a fixed primitive element of the field $\mathbb{F}_{q^{i_{\mathbf{a}}}}$. The next result gives an explicit description of the code \mathcal{C}_{Δ}^J . It extends Theorem 4 in [8]. Here we state the result for any set $J \subseteq \{1, 2, \dots, m\}$, while in [8] only the case $J = \{1, 2, \dots, m\}$ was considered.

Theorem 2.3. *With the above notation, if $\Delta \subseteq \mathcal{H}_J$ then the set of vectors*

$$\bigcup_{\mathbf{a} \in \mathcal{A}(\Delta)} \left\{ \text{ev}_J(\mathcal{T}_{\mathbf{a}}(\xi_{\mathbf{a}}^k X^{\mathbf{a}})) : 0 \leq k \leq i_{\mathbf{a}} - 1 \right\}$$

is a basis of \mathcal{C}_{Δ}^J over \mathbb{F}_q . In particular, if Δ is a closed set, then $\dim(\mathcal{C}_{\Delta}^J) = \dim(E_{\Delta}^J) = \#\Delta$.

The proof of Theorem 2.3 is similar to that of Theorem 4 in [8] and we omit it. Instead we show an example illustrating this theorem.

Example 2.4. Take $p = 2$, $s = 3$, $\ell = 6$ and $m = 2$, so $q = 2^3 = 8$ and $Q = 2^6 = 64$. Take $J = \{1\}$, $N_1 = 8$ and $N_2 = 10$, so that $T_1 = 6$ and $T_2 = 9$. Let $\mathbf{a}_1 = (1, 2)$, $\mathbf{a}_2 = (2, 3)$ and $\mathbf{a}_3 = (1, 3)$. Then $\mathfrak{I}_{\mathbf{a}_1} = \{(1, 2), (1, 7)\}$, $\mathfrak{I}_{\mathbf{a}_2} = \{(2, 3), (2, 6)\}$ and $\mathfrak{I}_{\mathbf{a}_3} = \{(1, 3), (1, 6)\}$, hence $i_{\mathbf{a}_1} = i_{\mathbf{a}_2} = i_{\mathbf{a}_3} = 2$. Let $\Delta_1 = \mathfrak{I}_{\mathbf{a}_1} \cup \mathfrak{I}_{\mathbf{a}_2}$ and $\Delta_2 = \mathfrak{I}_{\mathbf{a}_1} \cup \mathfrak{I}_{\mathbf{a}_2} \cup \{(1, 3)\}$. Thus Δ_1 is closed but Δ_2 is not. Consider the affine variety codes $E_{\Delta_1}^J, E_{\Delta_2}^J$ defined over \mathbb{F}_{64} and

the subfield-subcodes $\mathcal{C}_{\Delta_1}^J, \mathcal{C}_{\Delta_2}^J$ over \mathbb{F}_8 . All of them have length $n_J = 70$. Furthermore $\dim(E_{\Delta_1}^J) = 4, \dim(E_{\Delta_2}^J) = 5$. In fact we have

$$\begin{aligned} E_{\Delta_1}^J &= \langle \text{ev}_J(X_1 X_2^2), \text{ev}_J(X_1 X_2^7), \text{ev}_J(X_1^2 X_2^3), \text{ev}_J(X_1^2 X_2^6) \rangle, \\ E_{\Delta_2}^J &= \langle \text{ev}_J(X_1 X_2^2), \text{ev}_J(X_1 X_2^7), \text{ev}_J(X_1^2 X_2^3), \text{ev}_J(X_1^2 X_2^6), \text{ev}_J(X_1 X_2^3) \rangle \end{aligned}$$

over \mathbb{F}_{64} . And from Theorem 2.3

$$\begin{aligned} \mathcal{C}_{\Delta_1}^J = \mathcal{C}_{\Delta_2}^J &= \langle \text{ev}_J(X_1 X_2^2 + X_1 X_2^7), \text{ev}_J(\xi X_1 X_2^2 + \xi^8 X_1 X_2^7), \\ &\quad \text{ev}_J(X_1^2 X_2^3 + X_1^2 X_2^6), \text{ev}_J(\xi X_1^2 X_2^3 + \xi^8 X_1^2 X_2^6) \rangle \end{aligned}$$

over the field \mathbb{F}_8 , where ξ a primitive element of \mathbb{F}_{64} . This example shows that when we study the properties of a code \mathcal{C}_{Δ}^J , we can always assume that the set Δ , from which it arises, is closed.

2.2. LRC codes from J -affine variety codes. In this subsection we present some specific families of J -affine variety codes whose subfield-subcodes are LRC codes. We determine recovery sets for these LRC codes and show that their localities (r, δ) behave well.

Let us remember that the construction of J -affine variety codes begins by taking a set of indices $J \subseteq \{1, 2, \dots, m\}$ and integers N_1, N_2, \dots, N_m , such that $N_j - 1$ divides $Q - 1$ for all j . In order to obtain good LRC codes, from now on we shall assume the additional property that N_1, N_2, \dots, N_m have been chosen in a way that there exists a non-empty subset $L \subseteq J$ such that $q - 1$ divides $N_j - 1$ for all $j \in L$. Throughout the rest of this section we shall assume that the integers N_1, N_2, \dots, N_m , and the sets J and L , have been fixed satisfying the above conditions.

Let α and η be primitive elements of \mathbb{F}_Q and \mathbb{F}_q , respectively. For $1 \leq j \leq m$, let $\gamma_j = \alpha^{(Q-1)/(N_j-1)} \in \mathbb{F}_Q$. The following property will be used later.

Lemma 2.5. *Let l and n be two nonnegative integers. If $j \in L$, then the following equality holds in \mathbb{F}_Q ,*

$$\left(\gamma_j^l \eta^n \right)^{N_j-1} = 1.$$

Proof. The statement follows from the chain of equalities

$$\left(\gamma_j^l \eta^n \right)^{N_j-1} = \left(\alpha^{\frac{Q-1}{N_j-1}} \right)^{l(N_j-1)} (\eta^{N_j-1})^n = (\alpha^{Q-1})^l (\eta^{q-1})^{n \frac{N_j-1}{q-1}} = 1.$$

□

As defined in Subsection 2.1, let I_J be the ideal in \mathfrak{A} generated by the binomials $X_j^{N_j-1} - 1$ if $j \in J$ and $X_j^{N_j} - X_j$ if $j \notin J$, and let $Z_J = \{P_1, P_2, \dots, P_{n_J}\}$ be the set of zeros of I_J over \mathbb{F}_Q . In this subsection we determine recovery sets for codes \mathcal{C}_{Δ}^J . These recovery sets will be obtained from subsets $R \subset Z_J$ satisfying some geometrical properties. Given a point $P \in Z_J$ we set $\text{coord}(P) := j$ if $P = P_j$; consequently, given a set $R \subseteq Z_J$, we set $\text{coord}(R) := \{\text{coord}(P) : P \in R\}$.

Given a nonzero element $\lambda \in \mathbb{F}_Q^*$ and a point $P \in \mathbb{F}_Q^m$, we define the product $\lambda \cdot_L P$ as the point of \mathbb{F}_Q^m obtained by multiplying by λ the coordinates of P corresponding to positions in L and leaving unchanged its remaining coordinates.

Lemma 2.6. *If $P \in Z_J$, then $\eta^n \cdot_L P \in Z_j$ for every nonnegative integer n .*

The proof of this lemma follows directly from the definition of L and Lemma 2.5. We define the *orbit* of a point $P_{t_0} \in Z_J$ as the set

$$(5) \quad R_{t_0} := \{\eta^n \cdot_L P_{t_0} : 0 \leq n \leq q-2\}.$$

Notice that $R_{t_0} \subset Z_J$ by Lemma 2.6. As we shall see later, these orbits are closely related to recovery sets of our codes. For short, the point $\eta^n \cdot_L P_{t_0}$ will be denoted P_{n,t_0}^L .

Let \mathcal{A} be the set of representatives of all minimal cyclotomic sets in \mathcal{H}_J , as defined in Subsection 2.1. For $\mathbf{a} \in \mathcal{A}$ we write $\sigma_L(\mathbf{a}) = \sum_{j \in L} a_j$, where the a_j 's and the sum $\sigma_L(\mathbf{a})$ are seen as integers.

Lemma 2.7. *Let $\mathbf{a} \in \mathcal{A}$ and let k and n be two integers such that $0 \leq k \leq i_{\mathbf{a}} - 1$ and $0 \leq n \leq q-1$. Then we have*

$$(6) \quad \mathcal{T}_{\mathbf{a}}(\xi_{\mathbf{a}}^k X^{\mathbf{a}})(P_{n,t_0}^L) = \eta^{n\sigma_L(\mathbf{a})} \mathcal{T}_{\mathbf{a}}(\xi_{\mathbf{a}}^k X^{\mathbf{a}})(P_{t_0}).$$

Proof. Since no coordinate of P_{t_0} in the positions of L vanishes, we can write $P_{t_0} = (\gamma_1^{k_1}, \gamma_2^{k_2}, \dots, \gamma_m^{k_m})$ without loss of generality. Then

$$(7) \quad \begin{aligned} \mathcal{T}_{\mathbf{a}}(\xi_{\mathbf{a}}^k X^{\mathbf{a}})(P_{n,t_0}^L) &= \sum_{t=0}^{i_{\mathbf{a}}-1} \left(\xi_{\mathbf{a}}^k \prod_{l \in L} (\eta^n \gamma_l^{k_l})^{a_l} \prod_{l \notin L} (\gamma_l^{k_l})^{a_l} \right)^{tq} \\ &= \eta^{n\sigma_L(\mathbf{a})} \sum_{t=0}^{i_{\mathbf{a}}-1} \left(\xi_{\mathbf{a}}^k \prod_{l=1}^m (\gamma_l^{k_l})^{a_l} \right)^{tq} = \eta^{n\sigma_L(\mathbf{a})} \mathcal{T}_{\mathbf{a}}(\xi_{\mathbf{a}}^k X^{\mathbf{a}})(P_{t_0}) \end{aligned}$$

as stated. \square

The J -affine variety code E_{Δ}^J was defined as the linear subspace spanned by the vectors $\text{ev}_J(X^{\mathbf{a}})$, $\mathbf{a} \in \Delta$, where Δ is any non-empty subset of \mathcal{H}_J . Taking advantage of Theorem 2.3, from now on all the sets Δ we consider will be closed, that is a union of minimal cyclotomic sets, $\Delta = \cup_{l=1}^r \mathcal{J}_{\mathbf{a}_l}$, with $\mathbf{a}_l \in \mathcal{A}$, $1 \leq l \leq r$. Later in this article we shall impose even more restrictive conditions.

Theorem 2.8. *Let $\Delta = \cup_{l=1}^r \mathcal{J}_{\mathbf{a}_l}$, where $\{\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_r\}$ is a subset of \mathcal{A} with cardinality $r \leq q-2$. If the integers $\sigma_L(\mathbf{a}_1), \sigma_L(\mathbf{a}_2), \dots, \sigma_L(\mathbf{a}_r)$ are pairwise different modulo $q-1$, then the subfield-subcode \mathcal{C}_{Δ}^J is an LRC code with locality $\leq r$.*

Proof. Let $\mathbf{c} = \text{ev}_J(h)$ be a codeword of \mathcal{C}_{Δ}^J . By Theorem 2.3, h can be written as

$$h = h_{\mathbf{a}_1} + h_{\mathbf{a}_2} + \dots + h_{\mathbf{a}_r},$$

where each $h_{\mathbf{a}_l}$ is a linear combination of polynomials of the form $\mathcal{T}_{\mathbf{a}_l}(\xi_{\mathbf{a}_l}^k X^{\mathbf{a}_l})$, $0 \leq k \leq i_{\mathbf{a}_l} - 1$, and coefficients in \mathbb{F}_q . Fix a position $t_0 \in \{1, 2, \dots, n\}$. We shall show that the set $R = \{P_{n_i, t_0}^L : i = 1, 2, \dots, r\}$ of points corresponding to r consecutive nonzero n_i 's, gives a recovery set $\text{coord}(R)$ for t_0 . According to Lemma 2.6, the points in R belong to Z_J . Assume we know the r coordinates $h(P_{n_i, t_0}^L)$, $i = 1, 2, \dots, r$, of \mathbf{c} . By linearity

$$(8) \quad h(P_{t_0}) = h_{\mathbf{a}_1}(P_{t_0}) + h_{\mathbf{a}_2}(P_{t_0}) + \dots + h_{\mathbf{a}_r}(P_{t_0}).$$

Then, from Lemma 2.7 we get the equalities

$$\begin{aligned} h(\eta^{n_1} \cdot_L P_{t_0}) &= \eta^{n_1 \sigma_L(\mathbf{a}_1)} h_{\mathbf{a}_1}(P_{t_0}) + \eta^{n_1 \sigma_L(\mathbf{a}_2)} h_{\mathbf{a}_2}(P_{t_0}) + \cdots + \eta^{n_1 \sigma_L(\mathbf{a}_r)} h_{\mathbf{a}_r}(P_{t_0}), \\ h(\eta^{n_2} \cdot_L P_{t_0}) &= \eta^{n_2 \sigma_L(\mathbf{a}_1)} h_{\mathbf{a}_1}(P_{t_0}) + \eta^{n_2 \sigma_L(\mathbf{a}_2)} h_{\mathbf{a}_2}(P_{t_0}) + \cdots + \eta^{n_2 \sigma_L(\mathbf{a}_r)} h_{\mathbf{a}_r}(P_{t_0}), \\ &\vdots \\ h(\eta^{n_r} \cdot_L P_{t_0}) &= \eta^{n_r \sigma_L(\mathbf{a}_1)} h_{\mathbf{a}_1}(P_{t_0}) + \eta^{n_r \sigma_L(\mathbf{a}_2)} h_{\mathbf{a}_2}(P_{t_0}) + \cdots + \eta^{n_r \sigma_L(\mathbf{a}_r)} h_{\mathbf{a}_r}(P_{t_0}). \end{aligned}$$

Write $\eta_i := \eta^{\sigma_L(\mathbf{a}_i)}$, $1 \leq i \leq r$. We have obtained the square system of linear equations

$$\begin{pmatrix} \eta_1^{n_1} & \cdots & \eta_r^{n_1} \\ \eta_1^{n_2} & \cdots & \eta_r^{n_2} \\ \vdots & \ddots & \vdots \\ \eta_1^{n_r} & \cdots & \eta_r^{n_r} \end{pmatrix} \begin{pmatrix} h_{\mathbf{a}_1}(P_{t_0}) \\ h_{\mathbf{a}_2}(P_{t_0}) \\ \vdots \\ h_{\mathbf{a}_r}(P_{t_0}) \end{pmatrix} = \begin{pmatrix} h(\eta^{n_1} \cdot_L P_{t_0}) \\ h(\eta^{n_2} \cdot_L P_{t_0}) \\ \vdots \\ h(\eta^{n_r} \cdot_L P_{t_0}) \end{pmatrix}.$$

The matrix of this system is of Vandermonde type, and thus nonsingular. Then the solution is unique and gives the values $h_{\mathbf{a}_i}(P_{t_0})$, $1 \leq i \leq r$. Once these values are known, from (8) we can deduce $h(P_{t_0})$. \square

Under some supplementary conditions we can obtain LRC codes with larger dimension. In the next theorem we restrict to the case $L = \{1\}$, so that $\sigma_L(\mathbf{a}_l)$ is the first coordinate of \mathbf{a}_l . We denote by a_l such first coordinate.

Theorem 2.9. *Let $L = \{1\}$. Let $\Delta = \cup_{l=1}^{q-1} \mathcal{J}_{\mathbf{a}_l}$, where $\{\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_{q-1}\}$ is a subset of \mathcal{A} such that the first coordinates a_1, a_2, \dots, a_{q-1} of $\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_{q-1}$, are pairwise different modulo $q-1$. If there is an index v , $1 \leq v \leq q-1$, for which the following conditions*

- (1) a_v divides $N_1 - 1$,
- (2) $\gcd(a_v, a_l) = 1$ for all $1 \leq l \leq q-1$, $l \neq v$, and
- (3) $\gcd(a_v, q-1) = 1$;

hold, then \mathcal{C}_Δ^J is an LRC code with locality $\leq q-1 + (a_v - 1)$.

Proof. As in the proof of Theorem 2.8, let $\mathbf{c} = \text{ev}_J(h)$ be a codeword of \mathcal{C}_Δ^J . Fix a coordinate t_0 and consider the set of points

$$\bar{R} := \{\eta^n \cdot_L P_{t_0} : 0 \leq n \leq q-1\} \cup \{\omega^k \eta \cdot_L P_{t_0} : 1 \leq k \leq a_v - 1\},$$

where ω is a primitive a_v -root of unity. Since a_v divides $N_1 - 1$, then it holds that $\omega^k \eta \cdot_L P_{t_0} \in Z_J$ for all $1 \leq k \leq a_v - 1$. We shall show that $\text{coord}(\bar{R}) \setminus \{t_0\}$ is a recovery set for the coordinate t_0 . For simplicity we can assume $v = 1$. As in Theorem 2.8, we can write h as

$$h = h_{\mathbf{a}_1} + h_{\mathbf{a}_2} + \cdots + h_{\mathbf{a}_{q-1}},$$

$h_{\mathbf{a}_l}$ being a linear combination with coefficients in \mathbb{F}_q of polynomials of the form $\mathcal{T}_{\mathbf{a}_l}(\xi_{\mathbf{a}_l}^k X^{\mathbf{a}_l})$, $0 \leq k \leq i_{\mathbf{a}_l} - 1$. So we have

$$\begin{aligned} (9) \quad h(\eta \cdot_L P_{t_0}) &= \eta^{a_1} h_{\mathbf{a}_1}(P_{t_0}) + \eta^{a_2} h_{\mathbf{a}_2}(P_{t_0}) + \cdots + \eta^{a_{q-1}} h_{\mathbf{a}_{q-1}}(P_{t_0}), \\ h(\omega \eta \cdot_L P_{t_0}) &= \eta^{a_1} h_{\mathbf{a}_1}(P_{t_0}) + \eta^{a_2} h_{\mathbf{a}_2}(\omega \cdot_L P_{t_0}) + \cdots + \eta^{a_{q-1}} h_{\mathbf{a}_{q-1}}(\omega \cdot_L P_{t_0}), \\ &\vdots \\ h(\omega^{a_1-1} \eta \cdot_L P_{t_0}) &= \eta^{a_1} h_{\mathbf{a}_1}(P_{t_0}) + \eta^{a_2} h_{\mathbf{a}_2}(\omega^{a_1-1} \cdot_L P_{t_0}) + \cdots + \eta^{a_{q-1}} h_{\mathbf{a}_{q-1}}(\omega^{a_1-1} \cdot_L P_{t_0}). \end{aligned}$$

The facts that a_1 divides $N_1 - 1$ and $\gcd(a_1, q - 1) = 1$ imply that none of the points $\omega^k \eta^{-L} P_{t_0}$, $0 \leq k \leq a_1 - 1$, coincide neither with P_{t_0} nor among them. Adding the equalities in (9) we get a known value on the left hand. On the right hand we get

$$(10) \quad (a_1 - 1)(\eta^{a_1} h_{\mathbf{a}_1}(P_{t_0})) + \eta^{a_2} h_{\mathbf{a}_2}(P_{t_0}) (1 + \omega^{a_2} + (\omega^{a_2})^2 + \dots + (\omega^{a_2})^{a_1 - 1}) + \dots \\ + \eta^{a_{q-1}} h_{\mathbf{a}_{q-1}}(P_{t_0}) (1 + \omega^{a_{q-1}} + (\omega^{a_{q-1}})^2 + \dots + (\omega^{a_{q-1}})^{a_1 - 1}).$$

Since $\gcd(a_1, a_l) = 1$ for $2 \leq l \leq q - 1$, it holds that

$$1 + \omega^{a_l} + (\omega^{a_l})^2 + \dots + (\omega^{a_l})^{a_1 - 1} = 0$$

as this expression is the sum of all a_1 -roots of unity. Then (10) becomes $(a_1 - 1)(\eta^{a_1} h_{\mathbf{a}_1}(P_{t_0}))$, from which we deduce $h_{\mathbf{a}_1}(P_{t_0})$. The polynomial $h - h_{\mathbf{a}_1} = h_{\mathbf{a}_2} + \dots + h_{\mathbf{a}_{q-1}}$ is related to $q - 2$ minimal cyclotomic sets, hence we can apply now the procedure developed in the proof of Theorem 2.8 to compute $(h - h_{\mathbf{a}_1})(P_{t_0})$. Finally $h(P_{t_0}) = (h - h_{\mathbf{a}_1})(P_{t_0}) + h_{\mathbf{a}_1}(P_{t_0})$. \square

2.3. The case of $\{1, 2, \dots, m\}$ -affine variety codes. In this subsection we study the codes \mathcal{C}_Δ^J when J equals the whole set of indices, $J = \{1, 2, \dots, m\}$. Let L be a non-empty subset of J . As in the previous subsection, we take the closed set Δ as a union of minimal cyclotomic sets, $\Delta = \cup_{i=1}^z \mathcal{J}_{\mathbf{a}_i}$, but now we shall add the condition that the set $\{\sigma_L(\mathbf{a}_1), \sigma_L(\mathbf{a}_2), \dots, \sigma_L(\mathbf{a}_z)\}$ contains exactly r consecutive integers. With these ingredients we construct the J -affine variety code E_Δ^J over \mathbb{F}_Q and its subfield-subcode \mathcal{C}_Δ^J over \mathbb{F}_q .

Let us first deal with the case $m = 1$ and $r = z$. So let $J = L = \{1\}$. The set \mathcal{A} of representatives of all minimal cyclotomic sets in \mathcal{H}_J can be seen now as a subset of \mathbb{Z} . Let $\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_r, \mathbf{a}_{r+1}$ be the $r + 1$ smallest (with respect to the natural order in \mathbb{Z}) representatives in \mathcal{A} and let $\Delta = \cup_{i=1}^r \mathcal{J}_{\mathbf{a}_i}$. The codes E_Δ^J we obtain in this case were studied in [6], where the following result was proved by using the BCH bound.

Proposition 2.10. ([6, Theorem 3.7]) *Let $m = 1$ and let $\Delta = \cup_{i=1}^r \mathcal{J}_{\mathbf{a}_i}$, where $\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_r, \mathbf{a}_{r+1}$ are the $r + 1$ smallest elements of \mathcal{A} . Then the minimum distance of the dual code $(E_\Delta^J)^\perp$ satisfies $d((E_\Delta^J)^\perp) \geq \mathbf{a}_{r+1} + 1$.*

Let us recall that there exists a close relation between the dual of any linear code \mathcal{D} of length n , defined over \mathbb{F}_Q and the subfield-subcode $\mathcal{D} \cap \mathbb{F}_q^n$. This relation is given by the Delsarte Theorem, as follows

$$(\mathcal{D} \cap \mathbb{F}_q^n)^\perp = \text{Tr}(\mathcal{D}^\perp)$$

where Tr is the trace map of the extension $\mathbb{F}_Q/\mathbb{F}_q$, see [4]. In our case $m = 1$, this theorem implies

$$(11) \quad (\mathcal{C}_\Delta^J)^\perp = (E_\Delta^J)^\perp \cap \mathbb{F}_q^{n_J}$$

see [10, Proposition 11] for a complete proof of this equality. If $r \leq q - 2$, then the r smallest elements of \mathcal{A} are $\mathbf{a}_l = l - 1$, $l = 1, 2, \dots, r$, and hence from Proposition 2.10 and Equality (11) we have $d((\mathcal{C}_\Delta^J)^\perp) \geq r + 1$.

Proposition 2.11. *Let $m = 1$ and $\Delta = \cup_{i=1}^r \mathcal{J}_{\mathbf{a}_i}$, where $r \leq q - 2$ and $\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_r$ are the r smallest elements of \mathcal{A} . Then \mathcal{C}_Δ^J is a sharp LRC code of locality $r_1 = r$.*

Proof. According to Theorem 2.8, \mathcal{C}_Δ^J is an LRC code of locality $\leq r$. Since $d((\mathcal{C}_\Delta^J)^\perp) \geq r + 1$, Proposition 1.1 implies the result. \square

Let us study now the general case $m \geq 1$. So let $J = \{1, 2, \dots, m\}$, let L be a non-empty subset of J , and $\Delta = \cup_{l=1}^z \mathcal{J}_{\mathbf{a}_l}$. We are going to construct codes \mathcal{C}_Δ^J with locality $(r, q-r)$ for some $r \leq z$, whose $(r, q-r)$ recovery sets satisfy the conditions (RD1) and (RD2) stated in Section 1 with equality. Fix a coordinate t_0 , $1 \leq t_0 \leq n_J$, and let us consider the orbit of P_{t_0} , defined in Equation (5),

$$R_{t_0} = \{\eta^n \cdot_L P_{t_0} : 0 \leq n \leq q-2\} = \{P_{t_0}, P_{1,t_0}^L, \dots, P_{q-2,t_0}^L\} \subseteq Z_J.$$

Lemma 2.12. *Let $J = \{1, 2, \dots, m\}$ and let $\Delta = \cup_{l=1}^z \mathcal{J}_{\mathbf{a}_l}$ be a closed set. Let t_0 be a coordinate, $1 \leq t_0 \leq n_J$, and let R_{t_0} be the orbit of $P_{t_0} \in Z_J$. If the set $\{\sigma_L(\mathbf{a}_1), \sigma_L(\mathbf{a}_2), \dots, \sigma_L(\mathbf{a}_z)\}$ contains exactly $r \leq q-2$ distinct elements modulo $q-1$, then the punctured code $\mathcal{C}_\Delta^J[\text{coord}(R_{t_0})]$ has length $q-1$ and dimension r .*

Proof. The statement about the length is clear, since $R_{t_0} \subseteq Z_J$. Let us compute the dimension of $\mathcal{C}_\Delta^J[\text{coord}(R_{t_0})]$. According to Theorem 2.3, this code is generated by the set of vectors

$$(12) \quad \mathbf{v}_{lk} = \left(\mathcal{T}_{\mathbf{a}_l}(\xi_{\mathbf{a}_l}^k X^{\mathbf{a}_l})(P_{t_0}), \mathcal{T}_{\mathbf{a}_l}(\xi_{\mathbf{a}_l}^k X^{\mathbf{a}_l})(P_{1,t_0}^L), \dots, \mathcal{T}_{\mathbf{a}_l}(\xi_{\mathbf{a}_l}^k X^{\mathbf{a}_l})(P_{q-2,t_0}^L) \right)$$

$1 \leq l \leq z$; $0 \leq k \leq i_{\mathbf{a}_l} - 1$. From Lemma 2.7 we have

$$\mathbf{v}_{lk} = \left(\mathcal{T}_{\mathbf{a}_l}(\xi_{\mathbf{a}_l}^k X^{\mathbf{a}_l})(P_{t_0}) \right) (1, \eta^{\sigma_L(\mathbf{a}_l)}, \dots, \eta^{(q-2)\sigma_L(\mathbf{a}_l)}) = \left(\mathcal{T}_{\mathbf{a}_l}(\xi_{\mathbf{a}_l}^k X^{\mathbf{a}_l})(P_{t_0}) \right) \mathbf{w}_l$$

for $1 \leq l \leq z$ and $0 \leq k \leq i_{\mathbf{a}_l} - 1$, where $\mathbf{w}_l = (1, \eta^{\sigma_L(\mathbf{a}_l)}, \dots, \eta^{(q-2)\sigma_L(\mathbf{a}_l)})$. Since η is a primitive element of \mathbb{F}_q , then the set of vectors $\{\mathbf{w}_1, \mathbf{w}_2, \dots, \mathbf{w}_z\}$ has rank exactly r . Thus, to prove our claim on the dimension of $\mathcal{C}_\Delta^J[\text{coord}(R_{t_0})]$ it suffices to prove that for any $\mathbf{a} \in \{\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_z\}$, there exists k such that $\mathcal{T}_{\mathbf{a}}(\xi_{\mathbf{a}}^k X^{\mathbf{a}})(P_{t_0}) \neq 0$. Suppose, on the contrary, that there is \mathbf{a} such that $\mathcal{T}_{\mathbf{a}}(\xi_{\mathbf{a}}^k X^{\mathbf{a}})(P_{t_0}) = 0$ for all k , $0 \leq k \leq i_{\mathbf{a}} - 1$. Let $i = i_{\mathbf{a}}$. A simple computation shows that we can write

$$\begin{aligned} 0 &= \mathcal{T}_{\mathbf{a}}(X^{\mathbf{a}})(P_{t_0}) = X^{\mathbf{a}}(P_{t_0})(1 + b_1 + \dots + b_{i-1}), \\ 0 &= \mathcal{T}_{\mathbf{a}}(\xi_{\mathbf{a}} X^{\mathbf{a}})(P_{t_0}) = X^{\mathbf{a}}(P_{t_0})(\xi_{\mathbf{a}} + \xi_{\mathbf{a}}^q b_1 + \dots + \xi_{\mathbf{a}}^{(i-1)q} b_{i-1}), \\ &\vdots \\ 0 &= \mathcal{T}_{\mathbf{a}}(\xi_{\mathbf{a}}^{i-1} X^{\mathbf{a}})(P_{t_0}) = X^{\mathbf{a}}(P_{t_0})(\xi_{\mathbf{a}}^{i-1} + (\xi_{\mathbf{a}}^{i-1})^q b_1 + \dots + (\xi_{\mathbf{a}}^{i-1})^{(i-1)q} b_{i-1}) \end{aligned}$$

for some elements $b_1, b_2, \dots, b_{i-1} \in \mathbb{F}_q$. Note that $X^{\mathbf{a}}(P_{t_0}) \neq 0$ since $J = \{1, 2, \dots, m\}$. Thus the vector $(1, b_1, b_2, \dots, b_{i-1}) \neq \mathbf{0}$ is a solution of a homogeneous square linear system whose matrix is of Vandermonde type, what is not possible. \square

Let us recall here the well-known fact that the dual code of a linear MDS code is again an MDS code.

Proposition 2.13. *Let $J = \{1, 2, \dots, m\}$ and $\Delta = \cup_{l=1}^z \mathcal{J}_{\mathbf{a}_l}$ be a closed set. If the set $\{\sigma_L(\mathbf{a}_1), \sigma_L(\mathbf{a}_2), \dots, \sigma_L(\mathbf{a}_z)\}$ contains exactly $r \leq q-2$ distinct values and these values are consecutive integers, then for any coordinate t_0 , the punctured code $\mathcal{C}_\Delta^J[\text{coord}(R_{t_0})]$ is an MDS code with parameters $[q-1, r, q-r]$, where R_{t_0} is the orbit of $P_{t_0} \in Z_J$.*

Proof. For simplicity suppose that $\sigma_L(\mathbf{a}_1), \sigma_L(\mathbf{a}_2), \dots, \sigma_L(\mathbf{a}_r)$ are the consecutive integers mentioned in the statement. Since $r \leq q-2$ all these integers are distinct modulo $q-1$, and hence the statements about length and dimension follow from Lemma 2.12. Let us

compute the minimum distance of $\mathcal{C}_\Delta^J[\text{coord}(R_{t_0})]$. A generator matrix of this code is

$$\begin{pmatrix} \mathcal{T}_{\mathbf{a}_1}(X^{\mathbf{a}_1})(P_{t_0}) & \eta^{\sigma_L(\mathbf{a}_1)}\mathcal{T}_{\mathbf{a}_1}(X^{\mathbf{a}_1})(P_{t_0}) & \dots & \eta^{(q-2)\sigma_L(\mathbf{a}_1)}\mathcal{T}_{\mathbf{a}_1}(X^{\mathbf{a}_1})(P_{t_0}) \\ \vdots & \vdots & & \vdots \\ \mathcal{T}_{\mathbf{a}_r}(X^{\mathbf{a}_r})(P_{t_0}) & \eta^{\sigma_L(\mathbf{a}_r)}\mathcal{T}_{\mathbf{a}_r}(X^{\mathbf{a}_r})(P_{t_0}) & \dots & \eta^{(q-2)\sigma_L(\mathbf{a}_r)}\mathcal{T}_{\mathbf{a}_r}(X^{\mathbf{a}_r})(P_{t_0}) \end{pmatrix}.$$

If $\mathcal{T}_{\mathbf{a}_i}(X^{\mathbf{a}_i})(P_{t_0}) = 0$ we can remove the corresponding row in this matrix, hence we can assume $\mathcal{T}_{\mathbf{a}_i}(X^{\mathbf{a}_i})(P_{t_0}) \neq 0$ for all \mathbf{a}_i . To study the independence of columns, it suffices to consider the matrix

$$\mathbf{A} = \begin{pmatrix} 1 & \eta^{\sigma_L(\mathbf{a}_1)} & \dots & \eta^{(q-2)\sigma_L(\mathbf{a}_1)} \\ \vdots & \vdots & & \vdots \\ 1 & \eta^{\sigma_L(\mathbf{a}_r)} & \dots & \eta^{\sigma_L((q-2)\mathbf{a}_r)} \end{pmatrix}.$$

Since $\sigma_L(\mathbf{a}_1), \sigma_L(\mathbf{a}_2), \dots, \sigma_L(\mathbf{a}_r)$ are consecutive integers, any submatrix of \mathbf{A} obtained by taking r columns of \mathbf{A} has rank r , see [23, Lemma 6.6.5]. Thus the minimum distance of $\mathcal{C}_\Delta^J[\text{coord}(R_{t_0})]^\perp$ is $\geq r + 1$. So it has parameters $[q - 1, q - 1 - r, r + 1]$ and then it is an MDS code. Therefore $\mathcal{C}_\Delta^J[\text{coord}(R_{t_0})]$ is also MDS with parameters $[q - 1, r, q - r]$. \square

As a direct consequence of this proposition, we have the following theorem.

Theorem 2.14. *Let $J = \{1, 2, \dots, m\}$ and $\Delta = \cup_{i=1}^z \mathfrak{J}_{\mathbf{a}_i}$ be a closed set. If the set $\{\sigma_L(\mathbf{a}_1), \sigma_L(\mathbf{a}_2), \dots, \sigma_L(\mathbf{a}_z)\}$ contains exactly $r \leq q - 2$ distinct values and these values are consecutive integers, then for any coordinate t_0 , the set $\text{coord}(R_{t_0})$ is a $(r, q - r)$ recovery set for t_0 , where R_{t_0} is the orbit of $P_{t_0} \in Z_J$. Consequently \mathcal{C}_Δ^J is an LRC code with locality $(r, q - r)$ and $r_{q-r-t} \leq q - 1 - t$ for $t = 1, 2, \dots, q - r - 1$.*

Proof. The first statement follows from Proposition 2.13. The second one follows from the definition of r_t 's and the fact that puncturing $t < d$ times an $[n, k, d]$ MDS code gives an $[n - t, k, d - t]$ MDS code. \square

Let us note that formulas for the length and dimension of the codes \mathcal{C}_Δ^J are given given by Theorem 2.3. For the opposite, we do not have any explicit bound for its minimum distance (apart from the trivial bound $d(\mathcal{C}_\Delta^J) \geq d(E_\Delta^J)$). The same happens to most codes obtained as subfield-subcodes. Therefore, we cannot explicitly calculate formulas for the Singleton defect. In some of the examples we shall show in Section 3, these distances are calculated by computer search. Next we shall show that we can give such explicit formulas in the univariate case, $m = 1$, when $\text{char}(\mathbb{F}_q) \neq 2$ and $Q = q^2$.

So let $m = 1$. Given a closed set $\Delta = \cup_{i=1}^r \mathfrak{J}_{\mathbf{a}_i} \subset \mathcal{H}_J$, we define its *dual set* as $\Delta^\perp := \mathcal{H}_J \setminus \cup_{i=1}^r \mathfrak{J}_{n_J - \mathbf{a}_i}$. The dual code $(\mathcal{C}_\Delta^J)^\perp$ is related to the dual set Δ^\perp as follows

$$(13) \quad (\mathcal{C}_\Delta^J)^\perp = (E_\Delta^J \cap \mathbb{F}_q^{n_J})^\perp = E_{\Delta^\perp}^J \cap \mathbb{F}_q^{n_J},$$

see [6, Proposition 2.4].

Theorem 2.15. *Assume $Q = q^2$ with q odd. Let $m = 1$, $J = L = \{1\}$ and $N_1 = 2(q - 1) + 1$. Take $r \leq q - 2$ consecutive integers $\mathbf{a}_1 = 0, \mathbf{a}_2 = 1, \dots, \mathbf{a}_r = r - 1$, and let $\Delta = \cup_{i=1}^r \mathfrak{J}_{\mathbf{a}_i}$. Then the subfield-subcode \mathcal{C}_Δ^J has length $n_J = 2(q - 1)$, dimension $k = 2r - \lceil \frac{r}{2} \rceil$ and minimum distance $d \geq (q - 1) - 2 \lfloor \frac{r-2}{2} \rfloor$. It is a sharp LRC code with locality $(r, q - r)$ and $(q - r - 1)$ -th Singleton defect*

$$D_{q-r-1} \leq \left\lceil \frac{r}{2} \right\rceil + 2 \left\lfloor \frac{r-2}{2} \right\rfloor + 1 - r.$$

Proof. The length of \mathcal{C}_Δ^J is $n_J = N_1 - 1 = 2(q-1)$. The minimal cyclotomic sets in \mathcal{H}_J are $\mathfrak{J}_\mathbf{a} = \{\mathbf{a}\}$ when \mathbf{a} is even and $\mathfrak{J}_\mathbf{a} = \{\mathbf{a}, q + \mathbf{a} - 1\}$ when \mathbf{a} is odd. Thus $\#\Delta = 2r - \lceil \frac{r}{2} \rceil$ and since Δ is a closed set, \mathcal{C}_Δ^J has dimension $k = \#\Delta = 2r - \lceil \frac{r}{2} \rceil$ according to Theorem 2.3. Furthermore, a simple computation shows that the dual set $\Delta^\perp = \mathcal{H}_J \setminus \cup_{l=1}^r \mathfrak{J}_{n_J - \mathbf{a}_l}$ is the union of $(q-2) - 2\lfloor (r-2)/2 \rfloor$ minimal cyclotomic sets with consecutive representatives. Then from equation (13) and Proposition 2.11 we get a bound on the minimum distance of \mathcal{C}_Δ^J as follows

$$d(\mathcal{C}_\Delta^J) = d\left(\left((\mathcal{C}_\Delta^J)^\perp\right)^\perp\right) \geq d\left(\left(E_{\Delta^\perp}^J\right)^\perp\right) \geq (q-1) - 2\left\lfloor \frac{r-2}{2} \right\rfloor.$$

From Proposition 2.11 the code \mathcal{C}_Δ^J is sharp. Finally, according to Theorem 2.14, \mathcal{C}_Δ^J is an LRC code with locality $(r, \delta) = (r, q-r)$. Based on this locality, the $(q-r-1)$ -th Singleton defect of \mathcal{C}_Δ^J satisfies

$$D_{q-r-1} \leq 2(q-1) + 1 - \left((q-1) - 2\left\lfloor \frac{r-2}{2} \right\rfloor + 2r - \lceil \frac{r}{2} \rceil + \left\lfloor \frac{2r - \lceil \frac{r}{2} \rceil}{r} - 1 \right\rfloor (q-r-1) \right).$$

Since

$$\left\lfloor \frac{2r - \lceil \frac{r}{2} \rceil}{r} - 1 \right\rfloor = 1,$$

we get the bound on the defect D_{q-r-1} . \square

3. EXAMPLES

In this section we give examples of parameters of LRC codes \mathcal{C}_Δ^J over \mathbb{F}_q correcting several erasures, which are obtained as subfield-subcodes of J -affine variety codes E_Δ^J . The theoretical support for these examples is in theorems 2.3, 2.14 and 2.15. So the parameters we show arise from these theorems when they provide these data, and are calculated by computer search otherwise (see below for details). In particular, all codes we present have locality $(r, q-r)$, where $r \leq q-2$ depends on the cyclotomic sets in Δ . In order to evaluate the quality of these codes for local recovery purposes, we use the Singleton bounds (2) and (3), and compute the corresponding Singleton defects as stated in Section 1. Let us recall that when a code of parameters $[n, k, d]$ has locality (r, δ) , then $r_1 \leq r$ and its defect $D_{\delta-1}$ satisfies

$$(14) \quad D_{\delta-1} \leq n + 1 - \left(d + k + \left(\left\lfloor \frac{k}{r} \right\rfloor - 1 \right) (\delta - 1) \right).$$

In most cases, the codes we present are optimal ($D_{\delta-1} = 0$); otherwise they have small defect $D_{\delta-1}$. Let us remark that, besides the Singleton-like bound, there exist other available bounds on the (r, δ) 's (eg. Corollary 3 of [1]). To gain clarity, these bounds are not included here.

This section is organized in two subsections. In the first one we show examples with $m = 1$; the second one contains examples of bivariate codes, $m = 2$, improving some results obtained in the univariate case. We also include an example showing that this improvement does not always happen.

3.1. Examples of LRC codes coming from the univariate case. We take $m = 1$, $J = L = \{1\}$, and apply Theorems 2.14 and 2.15. The following tables contain the relevant data of the obtained codes: the cardinality q of the ground field over which the code is defined; their parameters $[n, k, d]$; the dual distance d^\perp ; the locality (r, δ) given by Theorems 2.14 or 2.15; and the estimate on the $(\delta - 1)$ -th Singleton defect $D_{\delta-1}$ given by the bound of Equation (14). All these data have been computed from the above theorems, except the minimum distance in Table 1, which has been obtained by computer search using Magma [2].

Let us note that in all cases, the localities (r, δ) shown satisfy that $\delta = q - r$ and r is equal to $d^\perp - 1$. So from Proposition 1.1 it follows that all our codes are sharp and $r = r_1$, the classical locality.

Example 3.1. Let $q = 8$, $Q = 64$, $N_1 = 22$, $\mathbf{a}_l = l - 1$, $1 \leq l \leq 6$, and let $\Delta = \cup_{l=1}^r \mathcal{J}_{\mathbf{a}_l}$ for $r = 2, 3, 4, 6$. We get codes with the parameters given in Table 1.

q	$[n, k, d]$	d^\perp	(r, δ)	$D_{\delta-1}$
8	[21, 3 14]	3	(2,6)	0
8	[21, 5 12]	4	(3,5)	1
8	[21, 6 12]	5	(4,4)	1
8	[21, 10 8]	7	(6,2)	3

TABLE 1. Univariate LRC codes over \mathbb{F}_8 .

Look, for example, at the $[21, 6, 12]$ code of the third row of Table 1. Its has locality $(4, 4)$, so $r_3 \leq 6$ and thus $r_2 \leq 5, r_1 \leq 4$. Since $d^\perp = 5$, from Proposition 1.4 we get equality in all cases. Then this code has defects $D_1 = 3, D_2 = 2$ and $D_3 = 1$. Note furthermore that the best known $[21, 6]$ code over \mathbb{F}_8 has minimum distance $d = 13$, [17]. So no currently known $[21, 6]$ code can be 1-optimal.

Example 3.2. Let $q = 9$, $Q = 81$, $N_1 = 2(q - 1) + 1 = 17$, $\mathbf{a}_l = l - 1$, $1 \leq l \leq 7$, and let $\Delta = \cup_{l=1}^r \mathcal{J}_{\mathbf{a}_l}$ for $r = 2, 3, 4, 5, 6, 7$. We get codes with the parameters given in Table 2.

q	$[n, k, d]$	d^\perp	(r, δ)	$D_{\delta-1}$
9	[16,3,8]	3	(2,7)	0
9	[16,4,8]	4	(3,6)	0
9	[16,6,6]	5	(4,5)	1
9	[16,7,6]	6	(5,4)	1
9	[16,9,4]	7	(6,3)	2
9	[16,10,4]	8	(7,2)	2

TABLE 2. Univariate LRC codes over \mathbb{F}_9 .

Example 3.3. Let $q = 11$, $Q = 121$, $N_1 = 2(q - 1) + 1 = 21$, $\mathbf{a}_l = l - 1$, $1 \leq l \leq 7$, and let $\Delta = \cup_{l=1}^r \mathcal{J}_{\mathbf{a}_l}$ for $r = 2, 3, \dots, 7$. We get codes with the parameters given in Table 3.

Example 3.4. Let $q = 25$, $Q = 625$, $N_1 = 49$, $\mathbf{a}_l = l - 1$, $1 \leq l \leq 7$, and let $\Delta = \cup_{l=1}^r \mathcal{J}_{\mathbf{a}_l}$ for $r = 2, 3, \dots, 7$. We get codes with the parameters given in Table 4.

Example 3.5. Let $q = 27$, $Q = 729$, $N_1 = 53$, $\mathbf{a}_l = l - 1$, $1 \leq l \leq 7$, and let $\Delta = \cup_{l=1}^r \mathcal{J}_{\mathbf{a}_l}$ for $r = 2, 3, \dots, 7$. We get codes with the parameters given in Table 5.

q	$[n, k, d]$	d^\perp	(r, δ)	$D_{\delta-1}$
11	[20, 3, 10]	3	(2,9)	0
11	[20, 5, 10]	4	(3,8)	0
11	[20, 6, 8]	5	(4,7)	1
11	[20, 7, 8]	6	(5,6)	1
11	[20, 9, 6]	7	(6,5)	2
11	[20, 10, 6]	8	(7,4)	2

 TABLE 3. Univariate LRC codes over \mathbb{F}_{11} .

q	$[n, k, d]$	d^\perp	(r, δ)	$D_{\delta-1}$
25	[48,3,24]	3	(2,23)	0
25	[48,4,24]	4	(3,22)	0
25	[48,6,22]	5	(4,21)	1
25	[48,7,22]	6	(5,20)	1
25	[48,9,20]	7	(6,19)	2
25	[48,10,20]	8	(7,18)	2

 TABLE 4. Univariate LRC codes over \mathbb{F}_{25} .

q	$[n, k, d]$	d^\perp	(r, δ)	$D_{\delta-1}$
27	[52,3,26]	3	(2,25)	0
27	[52,4,26]	4	(3,24)	0
27	[52,6,24]	5	(4,23)	1
27	[52,7,24]	6	(5,22)	1
27	[52,9,22]	7	(6,21)	2
27	[52,10,22]	8	(7,20)	2

 TABLE 5. Univariate LRC codes over \mathbb{F}_{27} .

3.2. Examples of LRC codes coming from the bivariate case. Let us consider now the bivariate case $m = 2$, with $J = \{1, 2\}$ and $L = \{1\}$. As above we show tables of parameters of codes \mathcal{C}_Δ^J over \mathbb{F}_q for different values of q . The minimum distances in these tables have been computed with Magma [2]. The dual distances d^\perp have been also computed with Magma; they are included in the tables only when they provide relevant information about sharpness, what corresponds to the cases $q = 8, 11, 16$. For $q = 25, 27$, the codes are far from being sharp, and the value of d^\perp is omitted. The examples we are going to present seem to suggest that bivariate codes give better results than the univariate ones. However, this is not always true, as shown in Example 3.11.

Example 3.6. Let $q = 8, Q = q^4 = 4096, N_1 = 8$ and $N_2 = 6$. Table 6 contains the parameters of codes \mathcal{C}_Δ^J obtained by using successively the following defining sets Δ : $\mathfrak{I}_{(0,1)}$; $\mathfrak{I}_{(0,1)} \cup \mathfrak{I}_{(1,1)}$; and $\mathfrak{I}_{(0,1)} \cup \mathfrak{I}_{(1,1)} \cup \mathfrak{I}_{(2,1)}$.

Example 3.7. Let $q = Q = N_1 = 11$ and $N_2 = 3$. Table 7 contains the parameters of codes \mathcal{C}_Δ^J obtained by using the following defining sets Δ : the first code (first row of Table 7) comes from the set $\mathfrak{I}_{(0,0)} \cup \mathfrak{I}_{(0,1)} \cup \mathfrak{I}_{(1,0)} \cup \mathfrak{I}_{(2,0)}$; the defining sets for the remaining codes are obtained by successively adding the cyclotomic sets $\mathfrak{I}_{(3,0)}$; $\mathfrak{I}_{(4,0)}$; $\mathfrak{I}_{(5,0)}$; $\mathfrak{I}_{(1,1)} \cup \mathfrak{I}_{(6,0)}$; and $\mathfrak{I}_{(7,1)}$.

q	$[n, k, d]$	d^\perp	(r, δ)	$D_{\delta-1}$
8	[35,4,14]	2	(1,7)	0
8	[35,8,12]	3	(2,6)	1
8	[35,12,10]	4	(3,5)	2

TABLE 6. Bivariate LRC codes over \mathbb{F}_8 .

q	$[n, k, d]$	d^\perp	(r, δ)	$D_{\delta-1}$
11	[20,4,10]	4	(3,8)	0
11	[20,5,10]	4	(4,7)	0
11	[20,6,10]	4	(5,6)	0
11	[20,7,10]	4	(6,5)	0
11	[20,9,8]	6	(7,4)	1
11	[20,10,8]	8	(8,3)	1

TABLE 7. Bivariate LRC codes over \mathbb{F}_{11} .

Example 3.8. Let $q = Q = N_1 = 16$ and $N_2 = 4$. Table 8 contains the parameters of codes \mathcal{C}_Δ^J obtained by using the following defining sets Δ : the first code comes from the set $\mathfrak{I}_{(0,0)} \cup \mathfrak{I}_{(0,1)} \cup \mathfrak{I}_{(1,1)} \cup \mathfrak{I}_{(2,0)} \cup \mathfrak{I}_{(3,0)}$. The defining sets for the remaining ones are obtained by successively adding the cyclotomic sets $\mathfrak{I}_{(4,0)}$; $\mathfrak{I}_{(5,0)}$; and $\mathfrak{I}_{(4,1)} \cup \mathfrak{I}_{(6,1)}$.

q	$[n, k, d]$	d^\perp	(r, δ)	$D_{\delta-1}$
16	[45,5,30]	3	(4,12)	0
16	[45,6,30]	3	(5,11)	0
16	[45,7,30]	3	(6,10)	0
16	[45,9,28]	3	(7,9)	1

TABLE 8. Bivariate LRC codes over \mathbb{F}_{16} .

Example 3.9. Let $q = Q = N_1 = 25$ and $N_2 = 3$. Table 9 contains the parameters of codes \mathcal{C}_Δ^J obtained by using the following defining sets Δ : the first code comes from the set $\mathfrak{I}_{(0,0)} \cup \mathfrak{I}_{(0,1)} \cup \mathfrak{I}_{(1,0)} \cup \mathfrak{I}_{(1,1)} \cup \mathfrak{I}_{(2,0)}$. The defining sets for the remaining ones are obtained by successively adding the following cyclotomic sets: $\mathfrak{I}_{(3,0)}$; $\mathfrak{I}_{(4,0)}$; $\mathfrak{I}_{(5,0)}$; $\mathfrak{I}_{(6,0)}$; $\mathfrak{I}_{(7,0)}$; $\mathfrak{I}_{(8,0)}$; and $\mathfrak{I}_{(9,0)}$.

q	$[n, k, d]$	(r, δ)	$D_{\delta-1}$
25	[48,5,23]	(3,22)	0
25	[48,6,23]	(4,21)	0
25	[48,7,23]	(5,20)	0
25	[48,8,23]	(6,19)	0
25	[48,9,23]	(7,18)	0
25	[48,10,23]	(8,17)	0
25	[48,11,23]	(9,16)	0
25	[48,12,23]	(10,15)	0

TABLE 9. Bivariate LRC codes over \mathbb{F}_{25} .

Example 3.10. Let $q = Q = N_1 = 27$ and $N_2 = 3$. Table 10 contains the parameters of codes \mathcal{C}_Δ^J obtained by using the following defining sets Δ : the first code comes from the set $\mathfrak{I}_{(0,0)} \cup \mathfrak{I}_{(0,1)} \cup \mathfrak{I}_{(1,0)} \cup \mathfrak{I}_{(1,1)} \cup \mathfrak{I}_{(2,0)} \cup \mathfrak{I}_{(3,0)}$. The defining sets for the remaining ones are obtained by successively adding the cyclotomic sets $\mathfrak{I}_{(4,0)}$; $\mathfrak{I}_{(5,0)}$; $\mathfrak{I}_{(6,0)}$; $\mathfrak{I}_{(7,0)}$; $\mathfrak{I}_{(8,0)}$; $\mathfrak{I}_{(9,0)}$; and $\mathfrak{I}_{(10,0)} \cup \mathfrak{I}_{(11,0)}$.

q	$[n, k, d]$	(r, δ)	$D_{\delta-1}$
27	[52,6,25]	(4,23)	0
27	[52,7,25]	(5,22)	0
27	[52,8,25]	(6,21)	0
27	[52,9,25]	(7,20)	0
27	[52,10,25]	(8,19)	0
27	[52,11,25]	(9,18)	0
27	[52,12,25]	(10,17)	0
27	[52,13,25]	(11,16)	0
27	[52,14,25]	(12,15)	0

TABLE 10. Bivariate LRC codes over \mathbb{F}_{27} .

Example 3.11. To conclude this work we show the parameters of some univariate LRC codes over \mathbb{F}_{32} which seem not to be improved by the bivariate ones. Let $m = 1$. Take $q = 32$, $Q = 1024$, $N_1 = 94$, $\mathbf{a}_l = l - 1$ for $1 \leq l \leq 4$, and let $\Delta = \cup_{l=1}^r \mathfrak{I}_{\mathbf{a}_l}$ for $r = 2, 3, 4$. We get univariate codes with the parameters given in Table 11. Bivariate codes improving

q	$[n, k, d]$	d^\perp	(r, δ)	$D_{\delta-1}$
32	[93,3,62]	3	(2,30)	0
32	[93,5,60]	4	(3,29)	1
32	[93,6,60]	5	(4,28)	1

TABLE 11. Univariate LRC codes over \mathbb{F}_{32} that cannot be improved by the bivariate ones.

these should come from the choice $N_1 = 32$, $N_2 = 4$, and we are forced to use the same field extension. An exhaustive computer search shows that such bivariate codes do not improve the univariate ones.

Acknowledgement. We would like to thank the reviewers of this article for their comments and suggestions, which have contributed to significantly improve it. This work was written during a visit by the third author to the Department of Mathematics at University Jaume I. This author wishes to express his gratitude to the staff of this university for their hospitality.

REFERENCES

[1] A. Agarwal, A. Barg, S. Hu and A. Mazumdar, Combinatorial alphabet-dependent bounds for locally recoverable codes, *IEEE Trans. Inform. Theory* **64** (2018) 3481-3492.
 [2] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.* **24** (1997) 235-265.
 [3] B. Chen, S-T. Xia, J. Hao and F-W. Fu, Constructions of optimal cyclic (r, δ) locally repairable codes, *IEEE Trans. Inform. Theory* **64** (2018), 2499-2511.

- [4] P. Delsarte, On subfield-subcodes of modified Reed-Solomon codes, *IEEE Trans. Inform. Theory* **21** (1975), 575-576.
- [5] W. Fang and F.W. Fu, Optimal cyclic (r, δ) locally repairable codes with unbounded length, IEEE Inform. Theory Workshop (ITW), Guangzhou, November 25-29, 2018.
- [6] C. Galindo, O. Geil, F. Hernando and D. Ruano, On the distance of stabilizer quantum codes from J -affine variety codes, *Quantum Inform. Process.* **16** (2017) 111.
- [7] C. Galindo, O. Geil, F. Hernando and D. Ruano, New binary and ternary LCD codes, *IEEE Trans. Inform. Theory* **65** (2019) 1008-1016.
- [8] C. Galindo and F. Hernando, Quantum codes from affine variety codes and their subfield subcodes, *Des. Codes Cryptogr.* **76** (2015) 89-100.
- [9] C. Galindo, F. Hernando and D. Ruano, Stabilizer quantum codes from J -affine variety codes and a new Steane-like enlargement, *Quantum Inform. Process.* **14** (2015) 3211-3231.
- [10] C. Galindo, F. Hernando and D. Ruano, Classical and quantum evaluation codes at the trace roots, *IEEE Trans. Inform. Theory* **65** (2019) 2593-2602.
- [11] P. Gopalan, C. Huang, H. Simitci and S. Yekhanin, On the locality of codeword symbols, *IEEE Trans. Inform. Theory* **58** (2012), 6925-6934.
- [12] S. Goparaju and R. Calderbank, Binary cyclic codes that are locally repairable, IEEE Int. Symp. Inform. Theory (ISIT-2014), Honolulu, 2014.
- [13] V. Guruswami, C. Xing and C. Yuan, How long can optimal locally repairable codes be? *IEEE Trans. Inform. Theory* **65** (2019), 3662-3670.
- [14] P. Huang, E. Yaakobi, H. Uchikawa and P.H. Siegel, Cyclic linear binary locally repairable codes, IEEE Inform. Theory Workshop (ITW), 2015.
- [15] G.M. Kamath, N. Prakash, V. Lalitha and P.V. Kumar, Codes with local regeneration, Proceedings of IEEE Int. Symp. Inform. Theory (ISIT-2013), 1606-1610, Istanbul 2013.
- [16] O. Kolosov, A. Barg, I. Tamo and G. Yadgar, Optimal LRC codes for all lengths $n \leq q$ (2018). Online available at <https://arxiv.org/abs/1802.00157>.
- [17] MinT, The online database for optimal parameters of (t, m, s) -nets, (t, s) -sequences, orthogonal arrays, linear codes, and OOA's. Online available at <http://mint.sbg.ac.at/>
- [18] R. Pellikaan, X.W. Wu, S. Bulygin and R. Jurrius, Codes, cryptology and curves with Computer Algebra, Cambridge University Press, Cambridge, 2017.
- [19] N. Prakash, G.M. Kamath, V. Lalitha and P.V. Kumar, Optimal linear codes with a local-error-correction property, Proceedings of IEEE Int. Symp. Inform. Theory (ISIT-2012), 2776-2780, Boston 2012.
- [20] N. Prakash, V. Lalitha and P.V. Kumar, Codes with locality for two erasures, Proceedings of IEEE Int. Symp. Inform. Theory (ISIT-2014), 1962-1966, Honolulu 2014.
- [21] A.S. Rawat, A. Mazumdar and S. Vishwanath, Cooperative local repair in distributed storage, *J. Adv. Signal Process.* **2015** (2015), 107.
- [22] I. Tamo, A. Barg, S. Goparaju and R. Calderbank, Cyclic LRC codes and their subfield subcodes, Proceedings of IEEE Int. Symp. Inform. Theory (ISIT-2015), 1262-1266, Hong-Kong 2015.
- [23] J.H. van Lint, Introduction to coding theory, Second edition, Springer-Verlag, 1992.
- [24] A. Wang and Z. Zhang, Repair locality with multiple erasure tolerance, *IEEE Trans. Inform. Theory* **60** (2014), 6979-6987.

Current address: Carlos Galindo and Fernando Hernando: Instituto Universitario de Matemáticas y Aplicaciones de Castellón and Departamento de Matemáticas, Universitat Jaume I, Campus de Riu Sec. 12071 Castelló (Spain), Carlos Munuera: Instituto de Matemáticas (Imuva) and Departamento de Matemática Aplicada, Universidad de Valladolid, Avda Salamanca SN, 47014 Valladolid (Spain).

E-mail address: Galindo: galindo@uji.es; Hernando: carrillf@uji.es; Munuera: cmunuera@arq.uva.es