LOCALLY RECOVERABLE CODES FROM ALGEBRAIC CURVES WITH SEPARATED VARIABLES

CARLOS MUNUERA, WANDERSON TENÓRIO, AND FERNANDO TORRES

Abstract. A Locally Recoverable code is an error-correcting code such that any erasure in a single coordinate of a codeword can be recovered from a small subset of other coordinates. We study Locally Recoverable Algebraic Geometry codes arising from certain curves defined by equations with separated variables. The recovery of erasures is obtained by means of Lagrangian interpolation in general, and simply by one addition in some particular cases.

1. Introduction

Locally Recoverable (LRC) codes were introduced in [4] motivated by the use of coding techniques applied to distributed and cloud storage systems. Roughly speaking, local recovery techniques enable us to repair lost encoded data by a local procedure, that is by making use of small amount of data instead of all information contained in a codeword.

Let $\mathcal{C}$ be a linear code of length n, dimension k and minimum distance d over the field $\mathbb{F}_q$. A coordinate $i \in \{1, \ldots, n\}$ is *locally recoverable with locality* r if there is a *recovery set* $R_i \subseteq \{1, \ldots, n\}$ with $i \notin R_i$ and $\#R_i = r$, such that for any two codewords $\mathbf{u}, \mathbf{v} \in \mathcal{C}$, whenever $\pi_i(\mathbf{u}) = \pi_i(\mathbf{v})$ we have $u_i = v_i$, where π_i is the projection on the coordinates of R_i. Under this condition, an erasure at position i of $\mathbf{v}$ can be recovered by using the information given by the coordinates of $\mathbf{v}$ with indices in R_i. We can also be interested on existence of distinct recovering sets R_i for the same coordinate, which is known as the *availability problem*. The code $\mathcal{C}$ is *locally recoverable with locality* r if any coordinate is locally recoverable with locality at most r.

Every code with minimum distance $d > 1$ is a LRC code of locality $r \leq k$. In practice we are interested in LRC codes $\mathcal{C}$ allowing small recovering sets, in relation to the other parameters $[n, k, d]$ of $\mathcal{C}$. We have the following Singleton-like bound: the locality r of

2010 *Mathematics Subject Classification.* 94B27, 11G20, 11T71, 14G50, 94B05.

Key words and phrases. error-correcting code, locally recoverable code, algebraic geometry code.

The first author was supported by Spanish Ministerio de Economía y Competitividad under grant MTM2015-65764-C3-1-P MINECO/FEDER. The second author was supported by CNPq-Brazil, under grants 201584/2015-8 and 159852/2014-5. The third author was supported by CNPq-Brazil under grant 310623/2017-0.

such a code verifies the relation, [4],

$$k + d + \left\lceil \frac{k}{r} \right\rceil \leq n + 2 \tag{1}$$

which gives a lower bound on r. Codes reaching equality are called *Singleton-optimal* (or simply optimal). The difference $\Delta = (n+2) - (k + d + \lceil \frac{k}{r} \rceil)$ is the *Singleton-optimal defect* of $\mathcal{C}$.

MDS codes (Reed-Solomon, RS, codes in particular) are optimal, but they have the largest possible locality $r = k$. In [17] a variation of RS codes for local recoverability purposes was introduced by Tamo and Barg. These so-called LRC RS codes are optimal and can have much smaller locality than RS codes. Its length is smaller than the size of $\mathbb{F}_q$. This is a usual fact: for most known optimal codes, the cardinality of the ground field $\mathbb{F}_q$ is larger than the code length n, [9]. Then the use of such codes for parctical applications rely on alphabets of large size, what limits its usefulness. Thus the search for long optimal codes has become a challenging problem. A method to obtain long codes is to consider codes from algebraic curves with many rational points. In this way the above construction of LRC RS codes was extended by Barg, Tamo and Vladut [2], to the *LRC Algebraic Geometry (LRC AG) codes*, obtaining larger LRC codes. The availability problem for LRC AG codes has been treated in [2] and [5].

In this article we study LRC AG codes coming from curves defined by equations with separated variables $A(Y) = B(X)$, paying special attention to the case in which the degrees of $A(Y)$ and $B(X)$ are coprime. We study also the generalized Hamming weights of these codes, and show how in some special cases the recovery can be done simply by one addition. The paper is organized as follows: Section 2 contains some introductory material. The core of this article is in Section 3, where the definition and main properties of our codes are treated. The fact that some of these codes admit a simple recovering method by just one addition is stated in Section 4. The generalized Hamming weights of general LRC codes, and codes coming from curves defined by equations with separated variables in particular, are studied in Section 5. Finally in Section 6 we show some worked examples of our constructions.

2. Construction of LRC codes from curves

The construction of LRC codes we study is based on ideas of [2, 13]. For the convenience of the reader, we briefly recall these constructions. Since the codes we study in this article are subcodes of Algebraic Geometry (AG) codes, we begin with a short reminder of this theory. For a complete reference on AG codes we address the reader to [11, 16].

2.1. *Algebraic Geometry codes.* Let $\mathcal{X}$ be a (projective, non-singular, absolutely irreducible, algebraic) curve of genus g defined over the field $\mathbb{F}_q$. Let $\mathcal{P} = \{P_1, \ldots, P_n\} \subseteq$

$\mathcal{X}(\mathbb{F}_q)$ be a set of n rational distinct points, $D = P_1 + \cdots + P_n$, and let G be a rational divisor with support disjoint from $\mathcal{P}$. The AG code $\mathcal{C}(\mathcal{P}, \mathcal{L}(G))$ is defined as $\mathcal{C}(\mathcal{P}, \mathcal{L}(G)) = \mathrm{ev}_{\mathcal{P}}(\mathcal{L}(G))$, where $\mathcal{L}(G) = \{\text{rational functions } f : \mathrm{div}(f) + G \geq 0\} \cup \{0\}$ is the Riemann space associated to G and $\mathrm{ev}_{\mathcal{P}}$ is the evaluation at $\mathcal{P}$ map, $\mathrm{ev}_{\mathcal{P}}(f) = (f(P_1), \ldots, f(P_n))$.

Given a divisor E we write $\ell(E) = \dim(\mathcal{L}(E))$. For a positive integer t the t-th *gonality* of $\mathcal{X}$ is defined as $\gamma_t = \min\{\deg(E) : E \text{ is a divisor on } \mathcal{X} \text{ with } \ell(E) \geq t\}$. Thus, from Riemann-Roch theorem we have $\gamma_t \leq t + g - 1$ with equality if $t \geq 2g - 1$.

The code $\mathcal{C}(\mathcal{P}, \mathcal{L}(G))$ is called *nonbundant* when $\mathrm{ev}_{\mathcal{P}}$ is injective; otherwise $\mathcal{C}(\mathcal{P}, \mathcal{L}(G))$ is *abundant* and $w = \ell(G - D) = \dim(\ker(\mathrm{ev}_{\mathcal{P}}))$ is its *abundance*. The dimension of this code is $k = \ell(G) - w$ and its minimum distance verifies $d \geq n - \deg(G) + \gamma_{w+1}$ (the generalized Goppa bound).

When the divisor G is a multiple of a single point $G = mQ$, $Q \notin \mathcal{P}$, then the code $\mathcal{C}(\mathcal{P}, \mathcal{L}(mQ))$ is called *one-point*. The properties and parameters of these codes are closely related to the *Weierstrass semigroup* of $\mathcal{X}$ at Q, $H = H(Q) = \{v(f) : f \text{ is a rational function on } \mathcal{X} \text{ with poles only at } Q\}$, where v is the pole order at Q. Usually we write H as an enumeration of its elements in increasing order, $H = \{h_1 = 0 < h_2 < \ldots\}$. It is clear that $\gamma_t \leq h_t$ for all t, with equality if $t \geq 2g - 1$.

2.2. *LRC codes from Algebraic Geometry.* We can construct LRC AG codes from algebraic curves as follows [2]: let $\mathcal{X}, \mathcal{Y}$ be two algebraic curves over $\mathbb{F}_q$ and let $\phi : \mathcal{X} \to \mathcal{Y}$ be a rational separable morphism of degree $r + 1$. Take a set $\mathcal{U} \subseteq \mathcal{Y}(\mathbb{F}_q)$ of rational points with totally split fibres and let $\mathcal{P} = \phi^{-1}(\mathcal{U})$. Let E be a rational divisor on $\mathcal{Y}$ with support disjoint from $\mathcal{U}$ and $\mathcal{L}(E)$ its associated Riemann-Roch space of dimension $m = \ell(E)$. By the separability of ϕ there exists $x \in \mathbb{F}_q(\mathcal{X})$ satisfying $\mathbb{F}_q(\mathcal{X}) = \mathbb{F}_q(\mathcal{Y})(x)$. Let

$$V = \left\{ \sum_{i=0}^{r-1} \sum_{j=1}^{m} a_{ij} f_j x^i \ : \ a_{ij} \in \mathbb{F}_q \right\}$$

where $\{f_1, \ldots, f_m\}$ is a basis of $\mathcal{L}(E)$. The LRC AG code $\mathcal{C}$ is defined as $\mathcal{C} = \mathrm{ev}_{\mathcal{P}}(V) \subseteq \mathbb{F}_q^n$, with $n = \#\mathcal{P}$. Note that $\mathcal{C}$ is a subcode of $C(\mathcal{P}, \mathcal{L}(G)) = \mathrm{ev}_{\mathcal{P}}(\mathcal{L}(G))$, where G is any divisor on $\mathcal{X}$ satisfying $V \subseteq \mathcal{L}(G)$. In particular $d(\mathcal{C}) \geq d(C(\mathcal{P}, \mathcal{L}(G))) \geq n - \deg(G)$. Let $\mathrm{ev}_{\mathcal{P}}(f)$, $f \in V$, be a codeword in $\mathcal{C}$. Since the functions of $\mathcal{L}(E)$ are constant on each fibre $\phi^{-1}(U)$, $U \in \mathcal{U}$, the local recovery of an erased coordinate $f(P)$ of $\mathrm{ev}_{\mathcal{P}}(f)$ can be performed by Lagrangian interpolation at the remaining r coordinates of $\mathrm{ev}_{\mathcal{P}}(f)$ corresponding to points in the fibre $\phi^{-1}(\phi(P))$ of P.

Theorem 1. [2] *If $ev_{\mathcal{P}}$ is injective on V then $\mathcal{C} \subseteq \mathbb{F}_q^n$ is a linear $[n, k, d]$ LRC code with parameters $n = s(r+1)$, $k = r\ell(E)$, $d \geq n - \deg(E)(r+1) - (r-1)\deg(x)$ and locality r.*

3. LRC codes from curves with separated variables

The above method for constructing LRC codes gives good codes, but it is rather complex technically. In this article we study that construction for curves defined by equations with separated variables. Furthermore we extend it somewhat in several directions, obtaining more and sometimes better codes. For a reference on the arithmetic and geometry of a class of curves defined by equations with separated variables we address the reader to [10, Lemma 6.54] and [6, Sect. 12.1].

3.1. *General construction of LRC codes from curves with separated variables.* Let $A(Y)$, $B(X)$ be two univariate polynomials over $\mathbb{F}_q$ of degrees a, b, respectively, and such that $A(Y)-B(X)$ is absolutely irreducible. Let us consider the curve $\mathcal{X}$ of plane affine equation $A(Y) = B(X)$. As usual, we denote by x and y, respectively, the cosets of X and Y in $\mathbb{F}_q[X,Y]/(A(Y)-B(X))$. Throughout this article, we shall assume the following condition

$(*)$: the functions x, y, have just one pole, $Q \in \mathcal{X}(\mathbb{F}_q)$, which is common to both.

Note that the above condition implies that $\mathcal{X}$ is unibranched at Q. This always happens if Q is a regular point. In case Q is singular, then it it must be a cusp. In any case, the condition $(*)$ implies the existence of a well defined pole-order at Q map on $\mathbb{F}_q(\mathcal{X})$, which we will denote by v. Note that $av(y) = bv(x)$, so when $\gcd(a,b) = 1$ then we have $v(x) = a$, $v(y) = b$ and (*) is satisfied.

Remark 1. Two simple cases where the above conditions on $\mathcal{X}$ are verified, are the following:
(a) if the above plane model is non-singular and $a \neq b$, then $A(Y) - B(X)$ is absolutely irreducible by Bézout's theorem, and Q is the only point at infinity of $\mathcal{X}$;
(b) ([6, Lemma 12.1]) Recall that a polynomial is called *linearized* if the exponents of monomials associated to all its nonzero coefficients are powers of $p = \mathrm{char}(\mathbb{F}_q)$. If $B(X)$ is linearized, $B(X) = \lambda_0 X + \lambda_1 X^p + \lambda_2 X^{p^2} + \ldots$, with $\lambda_0 \neq 0$, and $A(Y)$ has degree $a \geq 2$ with $a \not\equiv 0 \pmod{p}$, then $A(Y) - B(X)$ is absolutely irreducible and $\gcd(a,b) = 1$, so $(*)$ above is satisfied. Moreover, the Weierstrass semigroup at Q is $H = \langle a, b\rangle$ and thus the genus of $\mathcal{X}$ is $g = (a-1)(b-1)/2$. In addition, as $B'(X) \neq 0$, we have $\#y^{-1}(\beta) = b$ for any β in the algebraic closure of $\mathbb{F}_q$.

Define the set $\mathcal{L}(\infty Q) = \cup_{m\geq 0}\mathcal{L}(mQ)$. Let us recall that this is a finitely generated $\mathbb{F}_q$-algebra. Take two rational functions $\phi_1, \phi_2 \in \mathcal{L}(\infty Q)$. Let $\mathcal{X}(\mathbb{F}_q)^+ = \mathcal{X}(\mathbb{F}_q) \setminus \{Q\}$. Since neither ϕ_1 nor ϕ_2 have poles in $\mathcal{X}(\mathbb{F}_q)^+$, we have two well defined maps $\phi_1, \phi_2 : \mathcal{X}(\mathbb{F}_q)^+ \to \mathbb{A}^1(\mathbb{F}_q)$. Let $\mathcal{P}_1, \ldots, \mathcal{P}_s$ be disjoint subsets of $\mathcal{X}(\mathbb{F}_q)^+$ in which ϕ_1 is constant. Then each of these sets, $\mathcal{P}_i$, is contained in a fibre of ϕ_1, and so $\#\mathcal{P}_i \leq v(\phi_1)$. Let $r_i + 1$ be the number of different values took by ϕ_2 when acting over $\mathcal{P}_i$,

$$r_i = \#\{\phi_2(P) : P \in \mathcal{P}_i\} - 1,\ i = 1, \ldots, s.$$

Now fix an integer $r \geq 1$ and select those $\mathcal{P}_i$ verifying $r_i \geq r$ (if any), say $\mathcal{P}_1, \ldots, \mathcal{P}_u$. Set $\mathcal{P} = \mathcal{P}_1 \cup \cdots \cup \mathcal{P}_u$ and $n = \#\mathcal{P}$. Fix also numbers $\ell_0, \ldots \ell_{r-1}$ and consider the linear space of functions

$$V = \sum_{i=0}^{r-1} \epsilon_i \langle 1, \phi_1, \ldots, \phi_1^{\ell_i} \rangle \phi_2^i \subset \mathcal{L}(\infty Q) \tag{2}$$

where $\epsilon_i = 0$ or 1 and $\langle 1, \phi_1, \ldots, \phi_1^{\ell_i} \rangle$ stands for the linear space generated by $1, \phi_1, \ldots, \phi_1^{\ell_i}$ over $\mathbb{F}_q$. Then we get a code $\mathcal{C} = \mathcal{C}(\mathcal{P}, V) = \mathrm{ev}_{\mathcal{P}}(V)$. As in the case of AG codes we say that $\mathcal{C}(\mathcal{P}, V)$ is abundant if the evaluation map related to V is not injective. In order to give an estimate of its parameters we shall consider the number

$$m = m(V) = \max\{\epsilon_i(\ell_i v(\phi_1) + i v(\phi_2)) : i = 0, \ldots, r-1\}. \tag{3}$$

Lemma 1. *$V \subseteq \mathcal{L}(mQ)$ and so $\mathcal{C}(\mathcal{P}, V)$ is a subcode of the algebraic geometry code $\mathcal{C}(\mathcal{P}, \mathcal{L}(mQ))$.*

Proof. By the properties of valuations, if $f \in V$ then $v(f) \leq m$ and so $f \in \mathcal{L}(mQ)$. □

To be consistent with the usual notation used in algebraic geometry, we shall write $\ell(V) = \dim(V)$. Furthermore, for a divisor G on $\mathcal{X}$ we define $\mathcal{L}_V(G) = V \cap \mathcal{L}(G)$.

Theorem 2. *$\mathcal{C}(\mathcal{P}, V)$ is a $[n, k, d]$ LRC code of locality r with $k = \ell(V) - \dim(\mathcal{L}_V(mQ - D)) \geq \ell(V) - w$ and $d \geq d(\mathcal{C}(\mathcal{P}, \mathcal{L}(mQ))) \geq n - m + \gamma_{w+1}$ where $w = \ell(mQ - D)$ and γ_{w+1} is the $(w+1)$-th gonality of $\mathcal{X}$. In particular, if $m < n$ then $w = 0$ hence $k = \ell(V)$ and $d \geq n - m$.*

Proof. The kernel of the evaluation map $\mathrm{ev}_{\mathcal{P}} : V \to \mathbb{F}_q^n$ is $\mathcal{L}_V(mQ - D)$. In particular when $m < n$ this map is injective. This facts, together with Lemma 1 and the generalized Goppa bound on the minimum distance, imply the statements about k and d. Let us see that $\mathcal{C}(\mathcal{P}, V)$ is a LRC code of locality r whose recovery sets are subsets of $\mathcal{P}_1, \ldots, \mathcal{P}_u$. Let $f \in V$ and suppose we want to recover an erasure at position P, $P \in \mathcal{P}_i$. Let $\{P_{i,1}, \ldots, P_{i,r+1} = P\} \subseteq \mathcal{P}_i$ be a set in which ϕ_2 takes $r+1$ different values. Since all functions in $\mathbb{F}_q[\phi_1]$ are constant on $\mathcal{P}_i$, the restriction of f to this set acts as a polynomial $L_i = \sum_{j=0}^{r-1} a_j T^j$ of degree $\leq r-1$, that is $f(P_{i,j}) = L_i(\phi_2(P_{i,j}))$ for all $j = 1, \ldots, r+1$. Since ϕ_2 takes r different values in $\{P_{i,1}, \ldots, P_{i,r}\}$, the polynomial L_i may be computed by Lagrangian interpolation from $\phi_2(P_{i,1}), \ldots, \phi_2(P_{i,r})$ and $f(P_{i,1}), \ldots, f(P_{i,r})$. Finally $f(P) = L_i(\phi_2(P))$. □

Example 1. (a) (Example 1 of [17]). Consider the curve $Y = X^3$ over $\mathbb{F}_{13}$. This is a rational curve with 13 affine points plus one point Q at infinity. Let $\phi_1 = y, \phi_2 = x$. The fibres of ϕ_1 are the sets $\mathcal{P}_1 = \{1, 3, 9\}$, $\mathcal{P}_2 = \{2, 6, 5\}$ and $\mathcal{P}_3 = \{4, 10, 12\}$ (note that $13 \equiv 1 \pmod 3$ hence $\mathbb{F}_{13}$ contains a cubic root of unity). We obtain optimal LRC codes of length 9, locality 2 and dimensions $k = 2, 4, 6$.
(b) Let us slightly modify the curve of (a) to get larger codes. The curve $Y^2 = X^3$ over

$\mathbb{F}_{13}$ is again rational and hence it has 13 affine points. Take $\xi = 2$ as a primitive element of $\mathbb{F}_{13}$. The curve $\mathcal{X} : Y^2 = X^3 + 2$ is nonsingular of genus 1. It has 18 affine points. Since $13 \equiv 1 (\mathrm{mod}\ 3)$, $\omega = \xi^4 = 3$ is a cubic root of unity. Then the map $\sigma(x, y) = (\omega x, y)$ is an automorphism of $\mathcal{X}$, whose orbits have length 3. Thus the 18 points of $\mathcal{X}(\mathbb{F}_{13})^+$ are grouped in 6 orbits $\mathcal{P}_\beta = \{(\alpha, \beta), (\omega\alpha, \beta), (\omega^2\alpha, \beta)\}$. By taking $\phi_1 = y, \phi_2 = x$, we get LRC optimal codes of length $n = 18$, locality $r = 2$ and dimensions $k = 3, 5, 7, 9, 11$.
(c) LRC codes arising from the Hermitian curve $\mathcal{H} : Y^{q+1} = X^q + X$ over $\mathbb{F}_{q^2}$ were treated in [2], although in that work the authors only consider the case in which $m < n$ and $\ell_0 = \cdots = \ell_{r-1}$. To give a concrete example, take $q = 4, \phi_1 = y, \phi_2 = x$. Let Q be the only point at infinity of $\mathcal{H}$. We obtain codes of length $n = 64 = \#\mathcal{H}(\mathbb{F}_{16})^+$. Since $v(x) = 5, v(y) = 4$ we have $r = 3$. The biggest code we get comes from the space

$$V = \sum_{i=0}^{2} \langle 1, y, \ldots, y^{13} \rangle x^i \subseteq \mathcal{L}(62Q)$$

which leads to a code of dimension $k = 42$ and minimum distance $d \geq n - 62 = 2$. A simple computation shows that such code has optimal defect $\Delta \leq 8$.
(d) Following the procedure stated above, we can obtain bigger and better codes than in [2]. By continuing with the example of the Hermitian curve $\mathcal{H}$ over $\mathbb{F}_{16}$, we can consider the space

$$V = \sum_{i=0}^{2} \langle 1, y, \ldots, y^{16-i} \rangle x^i.$$

Then $\ell(V) = 48$ and $m(V) = 66$. The evaluation map is not injective as $f = \prod_{\beta \in \mathbb{F}_{16}} (y - \beta) \in V$ and $f(P) = 0$ for every point $P \in \mathcal{H}(\mathbb{F}_{16})^+$, hence $\mathcal{C}(\mathcal{P}, V)$ is an abundant code. Since the second gonality of $\mathcal{H}$ is known to be $\gamma_2 = q = 4$ (eg. [12]) we have $w = \ell(\mathcal{L}(66Q - D)) = 1$ and hence the kernel of the evaluation map related to V is generated by f. Then we obtain a code of dimension 47 and distance $d \geq n - 66 + \gamma_2 = 2$. Its optimal defect is $\Delta \leq 1$ (compare to (c)).
(e) LRC codes from the Norm-Trace curve have been studied in [1] where the approach is similar to that of (c).

3.2. *The case of prime degrees.* The bound for the minimum distance of $\mathcal{C}(\mathcal{P}, V)$ given in Theorem 2 strongly depends on the values $v(\phi_1)$ and $v(\phi_2)$. This, and the previous examples, invites us to consider functions ϕ_1, ϕ_2 for which these values are as small as possible. Of particular interest is the case in which the degrees a and b are coprime $\gcd(a, b) = 1$. In this setting $v(x) = a, v(y) = b$ and the Weiestrass semigroup at Q contains $\langle a, b \rangle$, $H \supseteq \langle a, b \rangle$, where Q is the common pole of x and y. This suggests taking $\phi_1 = y$ and $\phi_2 = x$ (or vice versa). This is the case treated in this subsection, and from now on in this article.

Any element $m \in \langle a, b\rangle$ can be written uniquely as $m = \lambda a + \mu b$ with $\lambda < b$. Thus we have

$$\mathcal{L}(\infty Q) \supseteq \mathbb{F}_q[x, y] = \bigoplus_{i=0}^{b-1} \mathbb{F}_q[y]x^i. \tag{4}$$

Let $\phi_1 = y$ and $\phi_2 = x$. Let $\mathcal{U}$ be the set of unramified points of ϕ_1, that is the set of $\beta \in \mathbb{F}_q$ such that the fibre $\phi_1^{-1}(\beta)$ totally split and so it consists of $b = v(\phi_1)$ distinct rational points in $\mathcal{X}(\mathbb{F}_q)^+$. Let $u = \#\mathcal{U}$ and $n = ub$. For $\beta \in \mathcal{U}$ set $\mathcal{P}_\beta = \phi_1^{-1}(\beta) = \{P_{\beta,1}, \ldots, P_{\beta,b}\}$. Write $D_\beta = P_{\beta,1} + \cdots + P_{\beta,b}$, $\mathcal{P} = \cup_{\beta\in\mathcal{U}}\mathcal{P}_\beta$ and $D = \sum_{\beta\in\mathcal{U}} D_\beta$.

In the best case, $\mathcal{U} = \mathbb{F}_q$ and hence $\mathcal{P} = \mathcal{X}(\mathbb{F}_q)^+$. This is the case of the so-called *Castle curves*, see [12]. Note that if this holds then the number rational of points of $\mathcal{X}$ attains the Lewittes bound $\#\mathcal{X}(\mathbb{F}_q) \le qh_2 + 1$.

Proposition 1. *(a)* $\operatorname{div}(\phi_1 - \beta) = D_\beta - bQ$ *hence we have the equivalence of divisors* $D_\beta \sim bQ$.
(b) $\operatorname{div}(\prod_{\beta\in\mathcal{U}}(\phi_1 - \beta)) = D - nQ$ *hence* $D \sim nQ$.

Being $\mathcal{X}$ a plane curve, the function $\phi_2 = x$ takes b different values on each $\mathcal{P}_\beta$, $\beta \in \mathcal{U}$. Set $r = b - 1$. As in the former Section 3.1 we consider the linear space of functions $V \subset \mathbb{F}_q[x, y] \subseteq \mathcal{L}(\infty Q)$ stated by equation (2).

Proposition 2. *If* $\phi_1 = y, \phi_2 = x$ *and* $\gcd(a, b) = 1$, *then the sum defining* V *in equation (2) is direct,* $V = \bigoplus_{i=0}^{b-2} \epsilon_i\langle 1, \phi_1, \ldots, \phi_1^{\ell_i}\rangle\phi_2^i$, *hence* $\ell(V) = \epsilon_0(1 + \ell_0) + \cdots + \epsilon_{b-2}(1 + \ell_{b-2})$.

Proof. If $\langle 1, \phi_1, \ldots, \phi_1^{\ell_i}\rangle\phi_2^i \cap \langle 1, \phi_1, \ldots, \phi_1^{\ell_j}\rangle\phi_2^j \neq (0)$ for some $i \le j$, then by taking pole orders we get $(\ell_i - \ell_j)v(\phi_1) = (j - i)v(\phi_2)$. Thus $v(\phi_1) = b|(j - i) < b$ so $i = j$. □

In our case $m = m(V) = \max\{\epsilon_i(\ell_i b + ia) : i = 0, \ldots, b-2\}$. The semigroup $H = H(Q) = \{h_1 = 0 < h_2 < \ldots\}$ can help us to simplify our estimates on the parameters of $\mathcal{C}(\mathcal{P}, V)$. For a non negative integer m define

$$\iota(m) = \max\{t : h_t \le m\}.$$

Then $\iota(m) = \ell(mQ)$, hence from Riemann-Roch theorem we have $\iota(m) \ge m + 1 - g$ with equality if $m \ge 2g$, where g is the genus of $\mathcal{X}$ (or equivalently the genus of H). Since $\gamma_t \le h_t$ for all t and $D \sim nQ$, we have $w = \ell((m - n)Q) = \iota(m - n)$. According to Theorem 2, $\mathcal{C}(\mathcal{P}, V)$ is an LRC code of locality $r = b - 1$, length n, dimension $k = \ell(V) - \dim(\mathcal{L}_V(mQ - D)) \ge \ell(V) - \iota(m - n)$ and minimum distance $d \ge n - m + \gamma_{\iota(m-n)+1}$. A upper bound on d is given by the following result.

Proposition 3. *Assume* $\epsilon_0 = 1$. *If* $\ell_0 b \ge n$ *then* $\mathcal{C}(\mathcal{P}, V)$ *is an abundant code. If* $\ell_0 b < n$ *then the minimum distance of* $\mathcal{C}(\mathcal{P}, V)$ *verifies* $n - m \le d \le n - \ell_0 b$.

Proof. Let $\tau = \prod_{\beta \in \mathcal{U}^*}(\phi_1 - \beta) \in \langle 1, \phi_1, \ldots, \phi_1^{\ell_0} \rangle \subseteq V$, where $\mathcal{U}^* = \mathcal{U}$ if $\ell_0 b \geq n$ and $\mathcal{U}^*$ is a subset of ℓ_0 distinct elements of $\mathcal{U}$ if $\ell_0 b < n$. Then $\mathrm{ev}_{\mathcal{P}}(\tau)$ vanishes at all points of $\mathcal{P}_\beta$, $\beta \in \mathcal{U}^*$. This means that $\tau \in \ker(\mathrm{ev}_{\mathcal{P}})$ if $\ell_0 b \geq n$ and $d \leq \mathrm{wt}(\mathrm{ev}_{\mathcal{P}}(\tau)) = n - \ell_0 b$ if $\ell_0 b < n$. □

3.3. *Complete spaces.* To conclude this section, we will study which linear spaces V produce LRC codes with the best possible parameters in the case $\gcd(a, b) = 1, \phi_1 = y, \phi_2 = x$. Given a positive integer m we can consider the space

$$V_m = \mathcal{L}(mQ) \cap \bigoplus_{i=0}^{b-2} \mathbb{F}_q[y]x^i.$$

Thus $m(V_m) \leq m$ and equality holds when $m \in \langle a, b \rangle$. If V is a linear space of functions defined by an equation (2) then $V \subseteq V_{m(V)}$, $m(V) = m(V_{m(V)})$, and the Goppa bounds on minimum distances of $\mathcal{C}(\mathcal{P}, V)$ and $\mathcal{C}(\mathcal{P}, V_{m(V)})$ given by Theorem 2 coincide. We say that $V_{m(V)}$ is the *completion* of V, and V is *complete* if $V = V_{m(V)}$. Let us detail a little more the structure of these V. From (4),

$$\mathcal{L}(mQ) \cap \mathbb{F}_q[x, y] = \bigoplus_{i=0}^{b-1} \epsilon_i \langle 1, y, \ldots, y^{\ell_i} \rangle x^i \tag{5}$$

with $\epsilon_i = 0$ if $ia > m$ and $\epsilon_i = 1$, $\ell_i b + ia \leq m$ if $ia \leq m$. Then $\ell_i = \lfloor (m - ia)/b \rfloor$ for $ia \leq m$. Thus we have the following.

Proposition 4. *V is complete iff $\epsilon_i = 1$ for $i = 0, \ldots, s$, where $s = \min\{b-2, \lfloor m(V)/a \rfloor\}$, $\epsilon_i = 0$ otherwise, and $\ell_i = \lfloor (m(V) - ia)/b \rfloor$, $i = 0, \ldots, s$.*

Corollary 1. *If V is complete then the minimum distance of $\mathcal{C}(\mathcal{P}, V)$ verifies $n - m(V) \leq d \leq n - \lfloor m(V)/b \rfloor b$.*

Proof. If V is complete then $\ell_0 = \lfloor m(V)/b \rfloor$ and the result follows from Proposition 3 and the Goppa bound. □

In some cases the set V is precisely a Riemann space $\mathcal{L}(mQ)$. If this happens then $\mathcal{C}(\mathcal{P}, V)$ is an AG code and so its dimension is maximized with respect to the Goppa bound we have used to estimate its minimum distance. An obvious necessary (but not sufficient) condition for this to hold is that V be complete.

Proposition 5. *Let V be a linear space of functions defined as in equation (2) and let $m = m(V)$. Then $V = \mathcal{L}(mQ)$ if and only if $H = \langle a, b \rangle$, V is complete and $m < a(b-1)$.*

Proof. If V is not complete, then $V \neq \mathcal{L}(mQ)$ by definition. Assume V is complete and $H = \langle a, b \rangle$. According to Proposition 4 we have equality $V = \mathcal{L}(mQ)$ if and only if $\epsilon_{b-1} = 0$ in equation (5). This happens when $m < a(b-1)$. □

Corollary 2. *Let V be a complete linear space of functions and let $m = m(V)$. If $H = \langle a, b\rangle$ and $m \geq a(b-1)$ then $\ell(mQ) - \ell(V) = 1 + \lfloor (m - a(b-1))/b \rfloor$.*

Proof. If $m \geq a(b-1)$ then $\ell(mQ) - \ell(V) = \dim(\langle 1, y, \ldots, y^{\ell_{b-1}}\rangle x^{b-1}) = 1 + \ell_{b-1}$. □

This result allows us to give a bound on the optimal defect of codes coming from complete spaces. For simplicity we restrict to the non-abundant case $m < n$.

Corollary 3. *Let V be a complete linear space of functions. If $H = \langle a, b\rangle$ and $m = m(V) < n$, then the Singleton-optimal defect Δ of $\mathcal{C}(\mathcal{P}, V)$ verifies*
(a) If $m < a(b-1)$ then $\Delta \leq g + 1 - \lceil (m + 1 - g)/(b-1) \rceil \leq g$;
(b) If $m \geq a(b-1)$ then $\Delta \leq g + 2 + \ell_{b-1} - \lceil (m - g - \ell_{b-1})/(b-1) \rceil \leq g + \ell_{b-1} + 1$;
where g is the genus of $\mathcal{X}$ and $\ell_{b-1} = \lfloor (m - a(b-1))/b \rfloor$.

Proof. Let $[n, k, d]$ be the parameters of $\mathcal{C}(\mathcal{P}, V)$ and let $[n, k^*, d^*]$ be the parameters of $\mathcal{C}(\mathcal{P}, \mathcal{L}(mQ))$. Then $d \geq d^*$, $k^* \geq m + 1 - g$ and $k = k^*$ if $m < a(b-1)$, $k = k^* - 1 - \ell_{b-1}$ if $m \geq a(b-1)$. The result follows from a straightforward computation using the well known fact that $k^* + d^* \geq n + 1 - g$ (see [11, Sect. 4.2]). □

Example 2. Let us consider the elliptic curve $\mathcal{X} : Y^2 = X^3 + 2$ over $\mathbb{F}_{13}$ of Example 1(b). Here $g = 1, a = 2, b = 3, H = \langle 2, 3\rangle$. Take the space of functions $V = \langle 1, y, y^2\rangle \oplus \langle 1, y, y^2\rangle x$. This is a complete space of dimension $l(V) = 6$ and $m(V) = 8$. Note that

$$\mathcal{L}(8Q) = \langle 1, y, y^2\rangle \oplus \langle 1, y, y^2\rangle x \oplus \langle 1, y\rangle x^2$$

so $\ell_{b-1} = \ell_2 = 1$. As explained in Example 1(b), we a get a code $\mathcal{C}(\mathcal{P}, V)$ of length $n = 18$, dimension $k = 6$ and locality $r = 2$. According to Corollary 3(b), its optimal defect verifies $\Delta \leq 1$. A direct computation shows that this estimate gives the true value of Δ.

4. A simplified recovering method

In this section we shall show how in some cases the recovering process can be performed simply by one addition, which is much faster and simpler than the interpolation method. Working with curves with separated variables is fundamental to the approach we present, which is based on ideas of [13]. We keep the same notations and assumptions of the previous section. In particular we assume $\phi_1 = y$ and $\phi_2 = x, \gcd(a, b) = 1$.

Let $L(T) = T^s + \lambda_{s-1}T^{s-1} + \cdots + \lambda_0 \in \mathbb{F}_q[T]$ be a polynomial. The roots $a_1, \ldots, a_s$ of L are related to its coefficients by the *Vieta's formulae* [3], $\sigma_i = (-1)^i \lambda_{s-i}$, $1 \leq i \leq s$, where $\sigma_i = \sigma_i(a_1, \ldots, a_s)$ is the i-th elementary symmetric polynomial on $a_1, \ldots, a_s$, that is $\sigma_1 = a_1 + \cdots + a_s; \ldots; \sigma_s = a_1 \cdots a_s$. For $i \geq 1$, the sums of successive i-powers of

$a_1, \ldots, a_s$, $\pi_i = \pi_i(a_1, \ldots, a_s) = a_1^i + \cdots + a_s^i$, are related to the elementary symmetric polynomials by the *Newton-Girard indentities* [3]: $\pi_1 = \sigma_1$ and for each integer $i > 1$,

$$\pi_i = (-1)^{i-1} i\sigma_i - \sum_{j=1}^{i-1} (-1)^j \pi_{i-j}\sigma_j. \tag{6}$$

Therefore the sums of powers of roots of $L(T)$ are related to its coefficients through (6). Such relations can be applied to simplify the recovering method in our codes from the curve $A(Y) = B(X)$. Let $V = \bigoplus_{i=0}^{r-1} \epsilon_i \langle 1, \phi_1, \ldots, \phi_1^{\ell_i} \rangle \phi_2^i$.

Theorem 3. *If $B(X)$ is a polynomial of degree $b \geq 3$ with $\pi_i = 0$ for $1 \leq i \leq b-2$, and any of the following conditions:*

(i) $\mathrm{char}(\mathbb{F}_q) | b$; *or*
(ii) $\epsilon_0 = 0$;

is verified, then for each fibre $\mathcal{P}_\beta = \{P_{\beta,1}, \ldots, P_{\beta,b}\}$ of $\phi_1 = y$, $\beta \in \mathcal{U}$, and each function $f \in V$, it holds that $\sum_{i=1}^{b} f(P_{\beta,i}) = 0$. Thus the recovering of one erasure can be obtained by one addition.

Proof. Let $\beta \in \mathcal{U}$ and let $f = \sum_{j=0}^{b-2} g_i(y)x^i \in V$. The points of $\mathcal{P}_\beta$ have coordinates $(\alpha_1, \beta), \ldots, (\alpha_b, \beta)$, being $\alpha_1, \ldots, \alpha_b$, the roots of the polynomial $B(X) - A(\beta)$. From (6) the sums of i-powers of roots of $B(T) - A(\beta)$ coincide with the sums of i-powers of roots of $B(T)$ for $i = 1, \ldots, b-2$, since the coefficients of $B(T)$ and $B(T) - A(\beta)$ are equal except by the constant part $A(\beta)$. Then

$$\sum_{i=1}^{b} f(P_{\beta,i}) = \sum_{i=1}^{b} \sum_{j=0}^{b-2} g_j(\beta)\alpha_i^j = \sum_{j=0}^{b-2} g_j(\beta)\pi_j(\alpha_1, \ldots, \alpha_b) = b g_0(\beta) = 0$$

by the conditions (i) and (ii). □

Example 3. The class of polynomials $B(X) = X^b + \lambda_1 X + \lambda_0$ over $\mathbb{F}_q$ fits in the framework of the previous Theorem. Indeed, $\pi_1 = \sigma_1 = -\lambda_{b-1} = 0$. By induction, if $\pi_1 = \cdots = \pi_{i-1} = 0$ for $1 < i \leq b-2$, then from equation (6) we have $\pi_i = (-1)^{i-1} i\sigma_i = -i\lambda_{b-i} = 0$. Therefore $\pi_1 = \cdots = \pi_{b-2} = 0$. For instance, in the Hermitian curve $\mathcal{H}$ of Example 1(c)(d) we have $B(X) = X^q + X$. Hence the conditions of the above theorem are fulfilled and the LRC codes in that example have recovering obtained by one addition.

Example 4. Linearized polynomials over $\mathbb{F}_q$ constitute also a class of polynomials in the conditions of Theorem 3. Indeed, assuming that $B(X)$ is a linearized polynomial of degree b, a power of $\mathrm{char}(\mathbb{F}_q)$, it can be proved by induction that $\pi_1 = \cdots = \pi_{b-2} = 0$, [13]. For instance, the Norm-Trace curves of Example 1(e) have $B(X)$ given by a linearized polynomial and their associated LRC codes have recovering obtained by one addition. More in general, LRC codes arising from Artin-Schreier curves under our construction, admit a recovering performed by one addition.

5. Generalized Hamming weights and optimal rank of LRC codes

An important invariant associated to a $[n,k]$ code $\mathcal{C}$ is its *weight hierarchy*, that is the sequence of its generalized Hamming weights $d_1,\dots,d_k$, where

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

$\mathrm{supp}(\mathcal{E}) = \cup_{\mathbf{v}\in\mathcal{E}}\mathrm{supp}(\mathbf{v})$ and the *support* of a vector $\mathbf{v}$ is the set of positions i where $v_i \neq 0$. In particular d_1 is the usual minimum distance, see [14, Sect. 4.5.1].

In this section we shall show an extension of the bound given by equation (1) to all generalized weights. This extension is valid for any LRC code and the proof is similar to that of (1) given in [4]. Next we will focus on our codes from curves with separate variables. We recall that Hamming weights of LRC codes from algebraic geometry have already been studied in [1].

5.1. *A bound on the Generalized Hamming weights of LRC codes.* Let $\mathcal{C}$ be a $[n,k,d]$ nondegenerate LRC code. It is well known that the t-th generalized Hamming weight of $\mathcal{C}$ verifies (see [14, Prop. 4.3.12])

$$n - d_t = \max\{\#R \subseteq \{1,\dots,n\} : \dim(\mathcal{C}(R)) \leq k-t\}. \tag{7}$$

For $i = 1,\dots,n$, let R_i be a minimal recovery set for coordinate i, and write $\bar{R}_i = R_i \cup \{i\}$.

Theorem 4. *Let $\mathcal{C}$ be a $[n,k]$ nondegenerate LRC code of locality r. For $t = 1,\dots,k$, it holds that*

$$k + d_t + \left\lceil \frac{k-t+1}{r} \right\rceil \leq n + t + 1. \tag{8}$$

Proof. Starting from $S_0 = \emptyset$, iteratively construct sets $S_1,\dots,S_l \subseteq \{1,\dots,n\}$, in the following way: while $\dim(\mathcal{C}(S_{i-1})) < k-t$, choose an index j_i such that $\dim(\mathcal{C}(S_{i-1}\cup R_{j_i})) > \dim(\mathcal{C}(S_{i-1}))$ and define $S_i = S_{i-1}\cup \bar{R}_{j_i}$. Then l is the smallest index such that $\dim(\mathcal{C}(S_l)) \geq k-t$. By a similar argumet as in [4, Theorem 5], we have $\dim(\mathcal{C}(\bar{R}_i)) < \#\bar{R}_i \leq r+1$, so $\#S_l \geq \dim(\mathcal{C}(S_l)) + l$ and $l \geq \dim(\mathcal{C}(S_l))/r$. Thus

$$\#S_l \geq \dim(\mathcal{C}(S_l)) + \frac{\dim(\mathcal{C}(S_l))}{r}.$$

Let $\dim(\mathcal{C}(S_l)) = k - t + \delta$ for some $0 \leq \delta < r$. If $\delta = 0$ set $S = S_l$. We get $\#S \geq k - t + (k-t)/r \geq k - t - 1 + (k-t+1)/r$. If $\delta > 0$, since R_{j_l} is minimal we can remove $\leq \delta + 1$ coordinates in $\bar{R}_{j_l}$ to obtain a set R'_l such that $S = \bar{R}_{j_1}\cup\cdots\cup\bar{R}_{j_{l-1}}\cup R'_l$ verifies $\dim(\mathcal{C}(S)) = \dim(\mathcal{C}(S_l)) - \delta = k-t$. As $\#S \geq \#S_l - \delta - 1$, substituting in the above equation we obtain $\#S \geq k - t - 1 + (k-t+\delta)/r \geq k - t - 1 + (k-t+1)/r$. Then the result follows by applying (7) to the set S. □

The bound of Theorem 4 extends both the Singleton optimal bound given in equation (1) and the Singleton bound for generalized Hamming weights, $k + d_t \leq n + t$. Let $\mathcal{C}$ be a LRC code of length n. The smallest t for which we have equality in this bound, $k + d_t = n + t$ is called the *MDS rank* of $\mathcal{C}$, $t = \text{mdsrank}(\mathcal{C})$. Similarly we can define the *Singleton optimal rank* of $\mathcal{C}$, $\text{optrank}(\mathcal{C})$, as the smallest t for which we have equality in the bound (8). Thus the optimal rank of $\mathcal{C}$ measures how far from optimal is the code $\mathcal{C}$. Contrary to that happens for the MDS rank, having equality in this bound for a certain t does not imply equality for all $t' > t$ (see Example 5 below).

Proposition 6. *Let $\mathcal{C}$ be a code of length n, locality r and dimension k. Then we have*
(a) $\text{optrank}(\mathcal{C}) \leq \text{mdsrank}(\mathcal{C})$.
(b) $\text{mdsrank}(\mathcal{C}) \geq k - r + 1$.
(c) $d_{k-r} \leq n - r - 1$. *If equality holds then* $\text{optrank}(\mathcal{C}) \leq k - r$.

Proof. (a) If $d_t = n - k + t$ then we have equality in the bound (8). (b) Note that $\mathcal{C}$ has MDS rank t iff for any set R of $k-t+1$ coordinates, $\mathcal{C}(R)$ has full rank. Then $k+t+1 \leq r$. (c) Take a minimal recovering set R. From equation (7) we have $n - d_{k-r} \geq r + 1$. If $n - d_{k-r} = r + 1$ then we have equality in (8) for $t = k - r$. □

5.2. *Generalized Hamming weights of LRC codes from curves with separated variables.* Let us return to our case of LRC codes from the curve $\mathcal{X} : A(Y) = B(X)$ with $\gcd(a, b) = 1$. Keeping the notation of the previous sections, let $V = \bigoplus_{i=0}^{r-1} \epsilon_i \langle 1, \phi_1, \ldots, \phi_1^{\ell_i} \rangle \phi_2^i$ and $m = m(V)$. As in the case of the minimum distance, we have (see [11])

$$n - d_t = \max\{\deg(E) : E \leq D, \dim(\mathcal{L}_V(mQ - E)) \geq t + w\} \tag{9}$$

so $d_t \geq n - m + \gamma_{w+t}$. In some cases this bound provides us the true value of d_t.

Proposition 7. *Let $\mu \leq u$ be a positive integer such that $\mu b < m$ and let $t = \iota(m - \mu b) - w$. Then $d_t \leq n - \mu b$.*

Proof. Take $\beta_1, \ldots, \beta_u \in \mathcal{U}$ and let $E = D_{\beta_1} + \cdots + D_{\beta_\mu}$. Then $E \sim \mu b Q$ hence $\ell(mQ - E) = \ell((m - \mu b)Q) = \iota(m - \mu b) \geq t + w$. According to (9) we have $n - d_t \geq \deg(E) = \mu b$. □

Example 5. Let us consider the curve $\mathcal{X} : Y^2 = X^3 + 2$ over $\mathbb{F}_{13}$ of examples 1(b) and 2. Take the space of functions $V = \langle 1, y, y^2 \rangle \oplus \langle 1, y, y^2 \rangle x$. We a get a code of length $n = 18$, dimension $k = 6$ and locality $r = 2$. The gonality sequence of $\mathcal{X}$ is $0, 2, 3, \ldots$, and $m(V) = 8$. The bounds on its generalized Hamming weights given by equations (8) and (9) are listed in the following Table 1, where the true values are indicated in boldface. These are obtained as follows: by taking a function $f = (y - \beta_1)(y - \beta_2)(x - \alpha) \in V$ (for example $f = (y - 1)(y + 1)(x - 1)$) we get a codeword of weight 10. By Proposition 7 we have $d_2 = 12$ and $d_5 = 15$, so $d_3 = 13, d_4 = 14$. Finally, since $1 \in V$ we have $d_6 = 18$.

Note that the optimal rank of $\mathcal{C}(\mathcal{P}, V)$ is 2, but we have not equality in the bound (8)

t	1	2	3	4	5	6
lower bound (9)	**10**	**12**	**13**	**14**	**15**	16
upper bound (8)	11	**12**	14	15	17	**18**

TABLE 1. Hamming weights of Example 5.

for $t = 3, 4, 5$. Furthermore, its MDS rank is the one estimated by Proposition 6(b).

Proposition 8. *Let $V = V_m$ be complete space with $m < n$. If $H(Q) = \langle a, b\rangle$, then for $t = 1, \dots, k = \dim(\mathcal{C}(\mathcal{P}, V))$ we have*
(a) If $m < a(b-1)$ then $d_t(\mathcal{C}(\mathcal{P}, V)) = d_t(\mathcal{C}(\mathcal{P}, \mathcal{L}(mQ)))$.
(b) If $m \geq a(b-1)$ then $d_t(\mathcal{C}(\mathcal{P}, \mathcal{L}(mQ))) \leq d_t(\mathcal{C}(\mathcal{P}, V)) \leq d_{t+\ell_{b-1}+1}(\mathcal{C}(\mathcal{P}, \mathcal{L}(mQ)))$, where ℓ_{b-1} is defined as in Section 3.3, $\ell_{b-1} = \lfloor (m - a(b-1))/b \rfloor$.

Proof. According to Proposition 5 and Corollary 2, if $m < a(b-1)$ then $\mathcal{C}(\mathcal{P}, V)) = \mathcal{C}(\mathcal{P}, \mathcal{L}(mQ)$; if $m \geq a(b-1)$ then $\mathcal{C}(\mathcal{P}, V))$ is a linear subspace of $\mathcal{C}(\mathcal{P}, \mathcal{L}(mQ))$ of co-dimension $\ell_{b-1} + 1$, hence for any subspace $W \subseteq \mathcal{C}(\mathcal{P}, \mathcal{L}(mQ))$ of dimension $t + \ell_{b-1} + 1$ we have $\dim(\mathcal{C}(\mathcal{P}, V)) \cap W) \geq t$. □

6. Two worked examples

To end this article we present examples of two families of curves and the corresponding LRC codes arising from them. To obtain concrete numerical results, we will detail each of the examples over the field $\mathbb{F}_{64}$.

6.1. *The Kondo-Katagiri-Ogihara curve.* Let us consider the curve $\mathcal{X} : Y^q + Y = X^{q^s+1}$ over the field $\mathbb{F}_{q^{2s}}$, where q is a prime power and s and odd integer. Codes arising from this curve have been studied in [7, 15]. $\mathcal{X}$ has one singular point at infinity, Q, plus q^{2s+1} affine points. Its genus is $g = q^s(q-1)/2$, hence it is a maximal curve and the Weierstrass semigroup of Q is $H = \langle q, q^s + 1\rangle$.

Let ξ be a primitive element of $\mathbb{F}_{q^{2s}}$. Then ξ^{q^s-1} is a primitive (q^s+1)-th root of unity in $\mathbb{F}_{q^{2s}}$ and so the map $\sigma(x, y) = (\xi^{q^s-1}x, y)$ is an automorphism of $\mathcal{X}$. The orbits of $\mathcal{X}(\mathbb{F}_{q^{2s}})^+$ under the action of σ are as follows: there are $q(q^s-1)$ orbits with q^s+1 points; and q orbits with one point, $(0, \beta)$. Then, by taking the sets $\mathcal{P}_\beta$ as these multi-point orbits, $\mathcal{P}_\beta = \{(\alpha, \beta), (\xi^{q^s-1}\alpha, \beta), \dots\}$, we get LRC codes from $\mathcal{X}$ of length $n = q^{2s+1} - q$ and locality $r = q^s$.

Example 6. Take $q = 2, s = 3$ and consider the curve $\mathcal{X} : Y^2 + Y = X^9$ over $\mathbb{F}_{64}$. This is a maximal hyperelliptic curve of genus $g = 4$. It has 128 rational affine points plus one point at infinity, Q, which is the only rational hyperelliptic point of $\mathcal{X}$. The Weierstrass semigroup of Q is $H = \langle 2, 9\rangle$. Observe that, according to Clifford's theorem, for all non-negative integer t the t-th gonality of $\mathcal{X}$ is precisely the t-th element of H, $\gamma_t = h_t$. Let ξ

be a primitive element of $\mathbb{F}_{64}$. Then ξ^7 is a primitive ninth root of unity. Under the action of the automorphism $\sigma(x,y) = (\xi^7 x, y)$, the 128 rational points of $\mathcal{X}(\mathbb{F}_{64})^+$ are grouped in 14 orbits of length 9, namely

$$\begin{array}{rlrl}
\mathcal{P}_1 = & \{(\xi,\xi^{18}),\dots,(\xi^{57},\xi^{18})\}, & \mathcal{P}_2 = & \{(\xi,\xi^{54}),\dots,(\xi^{57},\xi^{54})\},\\
\mathcal{P}_3 = & \{(\xi^2,\xi^{36}),\dots,(\xi^{58},\xi^{36})\}, & \mathcal{P}_4 = & \{(\xi^2,\xi^{45}),\dots,(\xi^{58},\xi^{45})\},\\
\mathcal{P}_5 = & \{(\xi^3,\xi^{31}),\dots,(\xi^{59},\xi^{31})\}, & \mathcal{P}_6 = & \{(\xi^3,\xi^{59}),\dots,(\xi^{59},\xi^{59})\},\\
\mathcal{P}_7 = & \{(\xi^4,\xi^{9}),\dots,(\xi^{60},\xi^{9})\}, & \mathcal{P}_8 = & \{(\xi^4,\xi^{27}),\dots,(\xi^{60},\xi^{27})\},\\
\mathcal{P}_9 = & \{(\xi^5,\xi^{47}),\dots,(\xi^{61},\xi^{47})\}, & \mathcal{P}_{10} = & \{(\xi^5,\xi^{61}),\dots,(\xi^{61},\xi^{61})\},\\
\mathcal{P}_{11} = & \{(\xi^6,\xi^{55}),\dots,(\xi^{62},\xi^{55})\}, & \mathcal{P}_{12} = & \{(\xi^6,\xi^{62}),\dots,(\xi^{62},\xi^{62})\},\\
\mathcal{P}_{13} = & \{(\xi^7,\xi^{21}),\dots,(1,\xi^{21})\}, & \mathcal{P}_{14} = & \{(\xi^7,\xi^{42}),\dots,(1,\xi^{42})\},
\end{array}$$

plus 2 orbits of length one, $\{(0,0)\},\{(0,1)\}$. Let $\mathcal{P} = \mathcal{P}_1 \cup \cdots \cup \mathcal{P}_{14}$, $\phi_1 = y, \phi_2 = x$, and hence $a = 2, b = 9$. We construct LRC codes of length $n = 126$ and locality $r = 8$ by evaluating at $\mathcal{P}$ the functions in the linear spaces $V = \bigoplus_{i=0}^{7} \epsilon_i \langle 1, y, \dots, y^{\ell_i}\rangle x^i$. To give a concrete example, take $m = 50$ and let V the complete space $V = V_{50}$. As computed in Proposition 4, we have $\ell_0 = \ell_1 = \ell_2 = 5; \ell_3 = \ell_4 = \ell_5 = \ell_6 = \ell_7 = 4$, so $k = \dim(\mathcal{C}(\mathcal{P}, V)) = \ell(V) = 43$. The minimum distance of this code is at least $d \geq 126 - 50 = 76$, and thus its optimal defect is $\Delta \leq 3$. Its generalized Hamming weights can be bounded by using the relations given by equations (8) and (9). For example, the first five of them verify $76 \leq d_1 \leq 79, 78 \leq d_2 \leq 80 \leq d_3 \leq 81, 82 \leq d_4 < d_5 = 84$.

6.2. *A quotient of the Hermitian curve.* Let $\mathcal{X}$ by the curve over $\mathbb{F}_{q^2}$ defined by the equation : $Y^s = X^q + X$, where q is a prime power and $s|q+1$. These curves have been studied in [16, Sect. VI.4] for example. $\mathcal{X}$ has genus $(s-1)(q-1)/2$ and $q(1+(q-1)s)$ rational affine points, plus one point at infinity. Then it is a maximal curve. Note that the mapping $\alpha \mapsto \alpha^q + \alpha$ is the trace map onto $\mathbb{F}_q$. Let ξ be a primitive element of $\mathbb{F}_{q^2}$. Then $\omega = \xi^{(q+1)/s}$ is a primitive $(q-1)s$-th root of unity. Let $\mathcal{U}^*$ be the subgroup of $\mathbb{F}_{q^2}^*$ generated by ω and $\mathcal{U} = \mathcal{U}^* \cup \{0\}$. If $\beta \in \mathcal{U}$ then $\beta^s \in \mathbb{F}_q$ and so the polynomial $T^q + T = \beta^s$ has q roots in $\mathbb{F}_{q^2}$.

Let $\phi_1 = y, \phi_2 = x$, $\mathcal{P}_\beta = \phi_1^{-1}(\beta)$ for $\beta \in \mathcal{U}$ and $\mathcal{P} = \cup_{\beta \in \mathcal{U}} \mathcal{P}_\beta$. We obtain LRC codes of length $n = q(1+(q-1)s)$ and locality $r = q-1$. Furthermore, according to Theorem 3, when $q \geq 3$ then the recovery of one erasure can be obtained by one addition.

Example 7. Take $q = 8, s = 3$ and consider the curve $\mathcal{X} : Y^3 = X^8 + X$ over $\mathbb{F}_{64}$. It has genus 7 and 176 affine points grouped in 22 sets $\mathcal{P}_\beta$ of 8 points. By considering the spaces of functions $V = \bigoplus_{i=0}^{6} \epsilon_i \langle 1, y, \dots, y^{\ell_i}\rangle x^i$, we obtain LRC codes of locality $r = 7$. For example, if $V = V_{50}$ then $\ell_0 = 6, \ell_1 = \ell_2 = \ell_3 = 5, \ell_4 = \ell_5 = \ell_6 = 4$. The corresponding code has dimension 40, minimum distance ≥ 126 and optimal defect ≤ 6. This defect is worse than that of Example 6, which can be compensated by the fact that the recovery or an erasure is carried out by a simple addition.

Conversely, since ω^{q-1} is a primitive s-th root of unity, for any $\alpha \in \mathbb{F}_{q^2}$, the polynomial $T^s = \alpha^q + \alpha$ has one root if $\alpha^q + \alpha = 0$ and s roots otherwise, all of them belonging to the set $\mathcal{U}$. Therefore we can group the $sq(q-1)$ points $(\alpha, \beta) \in \mathcal{X}(\mathbb{F}_{q^2})$ with $\alpha^q + \alpha = 0$ in $q(q-1)$ fibres $\phi_2^{-1}(\alpha)$, each of them with s points. In this way we get LRC codes of length $n = sq(q-1)$ and locality $r = s - 1$.

Example 8. Let us consider again the curve $\mathcal{X} : Y^3 = X^8 + X$ over $\mathbb{F}_{64}$ of Example 7. It has 168 rational affine points (α, β) with $\alpha^8 + \alpha \neq 0$. They are grouped in 56 fibers $\phi_2^{-1}(\alpha)$, with 3 points each. By taking spaces $V = \epsilon_0\langle 1, x, \ldots, x^{\ell_0}\rangle \oplus \epsilon_1\langle 1, x, \ldots, x^{\ell_1}\rangle y$, we obtain LRC codes of length $n = 168$ and locality $r = 2$. For example, if $V = V_{50} = V_{48}$ then $\ell_0 = 16, \ell_1 = 14$. The corresponding code has dimension 32, minimum distance ≥ 120 and optimal defect ≤ 2.

Acknowledgments

The third author wishes to thank the research group SINGACOM from Valladolid University for the finantial support received during his academic visit in January-February 2018.

References

[1] E. Ballico and C. Marcolla, Higher Hamming weights for locally recoverable codes on algebraic curves, *Finite Fields and their Applications*, **40** (2016), 61–72.

[2] A. Barg, I. Tamo and S. Vladut, Locally recoverable codes on algebraic curves, in *Proceedings of ISIT-2015*, Hong Kong, (2015), 1252–1256.

[3] D. Cox, J. Little and D. O'Shea, *Ideals, varieties, and algorithms*, Springer, New York, 1992.

[4] P. Gopalan, C. Huang, H. Simitci and S. Yekhanin, On the locality of codeword symbols, *IEEE Transactions on Information Theory*, **58** (2012), 6925–6934.

[5] K. Haymaker, B. Malmskog and G.L. Matthews, Locally recoverable codes with availability $t \geq 2$ from fiber products of curves, *Advances in Mathematics of Communications*, **12** 2018, 317–336.

[6] J.W.P. Hirschfeld, G. Korchmaros and F. Torres, *Algebraic Curves over a finite field*, Princeton University Press, Princeton, 2013.

[7] S. Kondo, T. Katagiri and T. Ogihara, Automorphism groups of one-point codes from the curves $y^q + y = x^{q^r+1}$, *IEEE Transactions on Information Theory*, **47** (2001), 2573–2579.

[8] A. Teplinsky, Herman's theory revisited, preprint,

[9] O. Kolosov, A. Barg, I. Tamo and G. Yadgar, Optimal LRC codes for all lengths $n \leq q$, preprint, arXiv:1802.00157 (2018).

[10] R. Lidl and H. Niederreiter, *Finite Fields*, Addison-Wesley, Reading, 1983.

[11] C. Munuera and W. Olaya, An introduction to algebraic geometry codes, in *Algebra for Secure and Reliable Communication Modelling*, (eds. M Lahyane and E, Martinez), AMS-Contemporary Mathematics (2015), 87-118.

[12] C. Munuera, A. Sepulveda and F. Torres, Castle curves and codes, *Advances in Mathematics of Communications*, **3** (2009), 399–408.

[13] C. Munuera and W. Tenório, Locally Recoverable codes from rational maps, preprint, arXiv:1606.09073 (2017).

[14] R. Pellikaan, X.W. Wu,??? S. Bulygin and R. Jurrius, *Codes, Cryptology and curves with computer algebra*, Cambridge University Press, Cambridge, 2017.
[15] A. Sepulveda and G. Tizziotti, Weierstrass semigroups and codes over the curve $y^q + y = x^{q^r+1}$, *Advances in Mathematics of Communications* **8** (2014), 67–72.
[16] H. Stichtenoth, *Algebraic function fields and codes*, Springer, Berlin 1991,
[17] I. Tamo and A. Barg, A family of optimal locally recoverable codes, *IEEE Transactions on Information Theory*, **60** (2014), 4661–4676.
[18] V.K. Wei, Generalized Hamming weights for linear codes, *IEEE Transactions on Information Theory*, **37** (1991), 1412–1418.

Department of Applied Mathematics, University of Valladolid, Avda Salamanca SN, 47014 Valladolid, Castilla, Spain

Email address: cmunuera@arq.uva.es

Departamento de Matemática, Universidade Federal de Mato Grosso, Av. F. C. Costa 2367, 78060-900, Cuiabá, Brazil

Email address: dersonwt@yahoo.com.br

Institute of Mathematics, Statistics and Computer Science, University of Campinas Cidade Universitaria "Zeferino Vaz", Barão Geraldo 13083-859, Campinas, Brazil

Email address: ftorres@ime.unicamp.br