Some contributions to the construction of Locally Recoverable codes from algebraic curves

Carlos Munuera and Wanderson Tenório

Abstract

We point some contributions to the construction of Locally Recoverable codes from algebraic curves recently presented by A. Barg, I. Tamo and S. Vladut, that can lead to improvements concerning the definition, the parameters and the local recovering of these codes.

I. INTRODUCTION

Locally Recoverable (or LRC) codes were introduced in [5] motivated by the recent and significant use of coding techniques applied to distributed and cloud storage systems [2], [3], [8]. Roughly speaking, local recovery techniques enable us to repair lost encoded data by a “local procedure”, which means by making use of small amount of data instead of all information, ensuring a high performance of the system.

Let $C$ be a code of length $n$ and cardinality $q^k$ over the field $\mathbb{F}_q$. As a notation, given a vector $x \in \mathbb{F}_q^n$ and a subset $R \subseteq \{1, \ldots, n\}$, we write $x_R = pr_R(x)$ and $C_R = pr_R(C)$, where $pr_R$ is the projection on the coordinates of $R$. We recall that 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 $i \not\in R(i)$ and $\#R(i) \leq r$, such that for any codeword $x \in C$, an erasure at position $i$ can be recovered by using the information of $x_{R(i)}$. That is to say, if for all $x, y \in C$, $x_{R(i)} = y_{R(i)}$ implies $x_i = y_i$. This is equivalent to say that the code $C_R$ has minimum distance $d(C_R) \geq 2$, where $R = R \cup \{i\}$, as a code of minimum distance $d$ corrects up to $d - 1$ erasures. Under this condition there is a well-defined recovering map $\text{rec}_i : C_{R(i)} \rightarrow \mathbb{F}_q$, $\text{rec}_i(x_{R(i)}) = x_i$, that allows us the recovering of $x_i$ by evaluating $\text{rec}_i(x_{R(i)})$. The code $C$ has all-symbol locality $r$ if any coordinate is locally recoverable with locality at most $r$. We use the notation $(n, k, r)$ to refer to the parameters of $C$. The minimum distance of an $(n, k, r)$ code is bounded by the Singleton-like relation

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

see [5]. Codes reaching equality are called optimal LCR codes.

The notion of local recoverability can be extended to multiple erasures as follows: $C$ is said to have the $(\rho, r)$ locality property if for each coordinate $i$ there is a subset $R(i)$ containing $i$ such that $\#R(i) \leq r + \rho - 1$ and $d(C_{R(i)}) \geq \rho$, that is if $\rho - 1$ erasures in $x_{R(i)}$ can be recovered from the remaining $\leq r$ coordinates of $x_{R(i)}$. We use the notation $(n, k, r, \rho)$ to refer to the parameters of such a code.

MDS codes (and Reed-Solomon codes in particular) are systematic at every $k$ positions, hence they have the largest locality $r = k$. Thus they are optimal but not good candidates as LRC codes. In [8] a variation of RS codes for local recoverability purposes was introduced by Tamo and Barg. These so-called LRC-RS codes are also optimal and can have much smaller locality. However, it is well known that one of the main drawbacks of RS codes for practical applications relies on its small length. The same happens for LRC-RS codes. A classical way to overcome this problem 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,

C. Munuera is with the Department of Applied Mathematics, University of Valladolid, Avda Salamanca SN, 47014 Valladolid, Castilla, Spain (email: cmunuera@arq.uva.es). Research supported by Spanish Ministerio de Economía y Competitividad under grant MTM2015-65764-C3-1-P MINECO/FEDER.

W. Tenório is with the Institute of Mathematics, Statistics and Computer Science (IMECC), University of Campinas (UNICAMP), R. Sérgio Buarque de Holanda, 651, Cidade Universitária “Zeferino Vaz”, 13083-059, Campinas, SP, Brazil (email: dersonwt@yahoo.com.br). Research supported by CNPq-Brazil under grant 201584/2015-8.
Tamo and Vladut [2], [3], to the so-called **LRC-Algebraic Geometry (LRC-AG) codes**, obtaining larger and powerful LRC codes.

In this paper we present some observations on the construction and properties of LRC-AG codes. In Section III we slightly generalize the original definition given by Barg, Tamo and Vladut. This generalization expands the family of LRC-AG codes so that we can get some codes with better parameters. In particular, some of these new LRC codes are of algebraic geometry type as shown in Section IV. Finally in Section V we deal with local recovery. We prove that some LRC-AG codes admit a simplified recovering method by simple checksum and propose a family of curves that provide codes with this property. For the convenience of the reader, we start by briefly recalling the construction of LRC-AG codes.

II. LRC codes from Algebraic Geometry

The construction of LRC-RS codes is as follows [8]: let $A(\mathbb{F}_q)$ be the affine line over $\mathbb{F}_q$ and let $\mathcal{P}_1, \ldots, \mathcal{P}_t \subset A(\mathbb{F}_q)$ be $t > 1$ pairwise disjoint subsets of cardinality $r + 1$ such that there exists a polynomial $\phi(x) \in \mathbb{F}_q[x]$ which is constant over each $\mathcal{P}_i = \{ P_{i,1}, \ldots, P_{i,r+1} \}$, $i = 1, \ldots, t$. Let $\mathcal{P} = \mathcal{P}_1 \cup \cdots \cup \mathcal{P}_t$ and $n = t(r + 1)$. Fix an integer $k$ such that $r | k$ and $k + \frac{k}{r} \leq n$, and consider the linear space

$$V = \bigoplus_{i=0}^{r-1} \langle 1, \phi, \ldots, \phi^{\frac{k}{r} - 1} \rangle x^i.$$ 

The code $C$ is obtained by evaluation of $V$ at the points of $\mathcal{P}$, $ev : V \to \mathbb{F}_q^n$, $ev(f) = (f(P_{ij}), i = 1, \ldots, t, j = 1, \ldots, r + 1)$. Since $\deg(f) \leq k + \frac{k}{r} - 2 < n$ for all $f \in V$, then $ev$ is injective hence $\dim(C) = \dim(V) = k$. Furthermore given $f \in V$, for all $i = 1, \ldots, t$, there exists a polynomial $\delta_i(x)$ of degree $\leq r - 1$ such that $\delta_i(P_{ij}) = f(P_{ij})$, $j = 1, \ldots, r + 1$. Such $\delta_i$'s can be computed through interpolation at any $r$ points of $\mathcal{P}_i$, so a recovering set for the coordinate corresponding to a point $P_{ij}$ is $R(i) = \mathcal{P}_i \setminus \{ P_{ij} \}$. Then $C$ is an $(n, k, r)$ optimal code. Slight modifications allow to construct codes for multiple erasures.

The above method is extended to construct LRC-AG codes as follows [2], [3]: let $\mathcal{X}, \mathcal{Y}$ be two algebraic (projective, non-singular, absolutely irreducible) 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 $S \subseteq \mathcal{Y}(\mathbb{F}_q)$ of rational points with totally split fibres of rational points of $\mathcal{X}$ and let $\mathcal{P} = \phi^{-1}(S) \subseteq \mathcal{X}(\mathbb{F}_q)$. Take also a rational divisor $D$ on $\mathcal{Y}$ with support disjoint from $S$. Denote by $\mathcal{L}(D)$ its associated Riemann-Roch space of dimension $\ell(D)$. By the separability of $\phi$ there exists an element $y \in \mathbb{F}_q(\mathcal{X})$ verifying $\mathbb{F}_q(\mathcal{X}) = \mathbb{F}_q(\mathcal{Y})(y)$. Since $\phi$ has degree $r + 1$ we can consider the $\mathbb{F}_q$-linear space

$$V = \bigoplus_{i=0}^{r-1} \mathcal{L}(D)y^i \subseteq \mathbb{F}_q(\mathcal{X}).$$

The LRC-AG code $C$ is defined as the image of $V$ by the evaluation at $\mathcal{P}$ map, $C = ev_{\mathcal{P}}(V) \subseteq \mathbb{F}_q^n$, with $n = \# \mathcal{P}$. Note that $C$ is a subcode of the algebraic geometry code $C(\mathcal{P}, G) = ev_{\mathcal{P}}(\mathcal{L}(G))$, where $G$ is the smallest divisor on $\mathcal{X}$ verifying $V \subseteq \mathcal{L}(G)$. In particular $d(C) \geq d(C(\mathcal{P}, G)) \geq n - \deg(G)$. Let $ev_{\mathcal{P}}(f), f \in V$, be a codeword in $C$. Since the functions of $\mathcal{L}(D)$ are constant on each fibre $\phi^{-1}(S)$, $S \in S$, the local recovery of an erased coordinate $f(P)$ of $ev_{\mathcal{P}}(f)$ can be performed by Lagrangian interpolation at the remaining $r$ coordinates of $ev_{\mathcal{P}}(f)$ corresponding to points in the fibre $\phi^{-1}(\phi(P))$ of $P$.

**Theorem II.1.** [8 Th. 3.1] If $ev_{\mathcal{P}}|_Y$ is injective then $C \subseteq \mathbb{F}_q^n$ is a linear $(n, k, r)$ LRC code with parameters $n = s(r + 1)$, $k = r\ell(D)$ and $d \geq n - \deg(G)(r + 1) - (r - 1)\deg(y)$.

In all examples we present in this paper we shall take $\mathcal{Y} = \mathbb{P}^1$. So often we only specify the curve $\mathcal{X}$.

**Example II.2.** In [8] two families of LRC codes from the Hermitian curve $\mathcal{H}$ defined by $x^{q+1} = y + y^q$ over $\mathbb{F}_{q^2}$ are studied. (a) For the first one we consider the morphism $\phi = x : \mathcal{H} \to \mathbb{P}^1$ of degree $q$ which leads to a code with locality $r = q - 1$. We take $S = A(\mathbb{F}_{q^2}) \subseteq \mathbb{P}^1$ and thus $x^{-1}(S) = \mathcal{H}(\mathbb{F}_{q^2}) \setminus \{ Q \}$, where $Q$ is
the point at infinity of $\mathcal{H}$. If $D = l\infty$ then $V = \bigoplus_{i=0}^{r-1}(1, x, x^2, \ldots, x^i)y^i \subseteq \mathbb{F}_q(\mathcal{H})$. We get LRC codes with parameters $n = q^3$, $k = r(l+1)$ and $d \geq n - \deg(G)$, where $G = (-v_Q(x^iy^r))Q = (lq+(r-1)(q+1))Q$.

(b) The second family is obtained by using the morphism $\phi = y$ of degree $q + 1$. The ramified points are exactly the points in the set $M = \{ b \in \mathbb{A}(\mathbb{F}_q) : b^q + b = 0 \} \cup \{ \infty \}$, so we take $S = \mathbb{P}^1 \setminus M$. If $D = l\infty$ we get LRC codes with locality $r = q$ and parameters $n = q^3 - q$, $k = r(l+1)$ and $d \geq n - \deg(G)$, where $G = (-v_Q(y^ix^r))Q = (l(q+1)+(r-1)q)Q$ and $v_Q$ is the valuation of $X$ at $Q$.

Example II.3. LRC-AG codes from the Norm-Trace curve $x^1 + q^2 + \cdots + q^{n-1} = y + y^q + \cdots + y^{q^n-1}$ over $\mathbb{F}_q$ are studied by Ballico and Marcolla in \cite{1}. Following similar ideas as in the previous example, they find (a) a family of LRC codes of locality $r = q^{u-1} - 1$ and parameters $n = q^{2u-1} - 1$, $k = (t+1)(q^{u-1} - 1)$, $d \geq n - tq^{u-1} - (q^{u-1} - 1)(1 + q + \cdots + q^{u-1})$; and (b) a family of LRC codes of locality $r = q + \cdots + q^{u-1}$ and parameters $n = q^{2u-1} - q^{u-1}$, $k = (t+1)(q + \cdots + q^{u-1})$, $d \geq n - tq^{u-1} - (q + \cdots + q^{u-1}) - q^{u-1}(1 + q + \cdots + q^{u-1})$. Furthermore, in that paper a detailed analysis on the distance of Hermitian LRC codes is done.

Example II.4. Constructions (a) in the previous examples can be generalized in the following way. A pointed curve $(\mathcal{X}, \mathcal{Y})$ over $\mathbb{F}_q$ is called Castle if the Weierstrass semigroup $S(Q)$ at $Q$ is symmetric and we have equality in the Lewittes bound, $\#\mathcal{X}(\mathbb{F}_q) = qm + 1$, where $m$ is the first nonzero element of $S(Q)$, \cite{2}. Thus Hermitian and Norm-Trace curves (among many others) are Castle. Take $\phi \in \mathcal{L}(\infty Q)$ such that $-v_Q(\phi) = m$. Under the Castle conditions it holds that for every $a \in \mathbb{F}_q$ the fibre $\phi^{-1}(a)$ consists of $m$ points. Then, by taking $S = \mathbb{F}_q$ and $D = l\infty$ we can construct LRC codes of length $n = qm = \#\mathcal{X}(\mathbb{F}_q) - 1$ and locality $r = m - 1$. Another possible generalization of these constructions will be given in Section V.

III. IMPROVING THE PARAMETERS

In this section we propose a slight variation on the definition of LRC-AG codes that may lead to improvements on the parameters $k$ and $d$ of the obtained codes without affecting neither the locality nor the recovering method. As LRC codes are designed to be used in large storage systems, improvements on the dimension could be of practical interest.

Keeping the notation used in the previous section, we have two curves $\mathcal{X}, \mathcal{Y}$, over $\mathbb{F}_q$ and a separable morphism $\phi : \mathcal{X} \rightarrow \mathcal{Y}$ of degree $r + 1$. Instead of considering a unique divisor $D$ on $\mathcal{Y}$, we may consider $r$ rational divisors, $D_0, \ldots, D_{r-1}$, on $\mathcal{Y}$ with support disjoint from $\mathcal{S}$. Then we have the space of functions

$$V' := \bigoplus_{i=0}^{r-1} \mathcal{L}(D_i)y^i \subseteq \mathbb{F}_q(\mathcal{X})$$

and define $C = ev_{V'}(V') \subseteq \mathbb{F}_q^n$.

Theorem III.1. $C = ev_{V'}(V') \subseteq \mathbb{F}_q^n$ is a linear $(n, k, r)$ LRC code with parameters

$$n = s(r + 1), \quad k = \sum_{i=0}^{r-1} \ell(D_i) \quad \text{and} \quad n - \deg(G) \leq d \leq \min_{0 \leq i \leq r - 1} \{d_i\}$$

provided $ev_{V'}|_{V'}$ is injective, where $G$ is the smallest rational divisor with respect to $\leq$ whose space $\mathcal{L}(G)$ contains $V'$, and $d_i$ is the minimum distance of $C_i = ev_{V'}(\mathcal{L}(D_i)y^i)$, $i = 0, \ldots, r - 1$. The local recovery of an erased coordinate $f(P)$ of $ev_{V'}(f)$ can be performed by Lagrangian interpolation at the remaining $r$ coordinates of $ev_{V'}(f)$ corresponding to points in the fibre $\phi^{-1}(\phi(P))$ of $P$.

Proof: The statement on the parameters follows immediately from the construction. Since the functions in $\mathcal{L}(D_i)$, $i = 0, \ldots, r - 1$, are constant over each fibre of $\phi$, for any codeword in $C$ the coordinates corresponding to points in such a fibre can be seen as evaluations of polynomials of degree $r - 1$, which can be retrieved from any $r$ coordinates in the fibre through interpolation.


Note that $n > \deg(G)$ implies that $ev_P|_{V'}$ is injective. Codes of this type were considered by Maharaj in [9] using the language of function fields. In that paper, it is shown that the divisor $G$ may be described as $G = \max\{\langle \phi^*(D_i) - div(y^i) : 0 \leq i \leq r - 1 \} \}$, where $\max\{G, G'\} = \sum_{P \in X} \max\{v_P(G), v_P(G')\}P$ and $\phi^* : \text{Div}(Y) \rightarrow \text{Div}(X)$ is the pull-back map induced by $\phi$.

Using a sequence of divisors $D_0, \ldots, D_{r-1}$, instead of a single divisor $D$ provides greater flexibility to the construction. Typically one can take $D_0 \geq \cdots \geq D_{r-1}$. Since codewords of smaller weight come from evaluation of functions $f \in L(D_i)y^i$ with larger $i$, this strategy allows to increase the dimension of $C$ without decreasing its minimum distance. For example, if $Y = \mathbb{P}^1$ and $Q = \phi^{-1}(\infty)$, instead of $V = \bigoplus_{i=0}^{r-1} L(l_i)\mathbb{P}^1$ we can consider the space $V' = \bigoplus_{i=0}^{r-1} L(l_i)\mathbb{P}^1$. Whenever $-v_Q(x^iy^i) \leq -v_Q(x^iy'^i)$, it holds that $V \subseteq L(G)$ for every divisor $G$ such that $V \subseteq L(G)$, so that we increase the dimension without affecting the estimate on the minimum distance.

**Example III.2.** Consider the Hermitian code $C$ of Example II.2(a), $C = ev_P(V)$ with $V = \bigoplus_{i=0}^{r-1} L(l_i)\mathbb{P}^1$. The condition $-v_Q(x^iy^i) \leq -v_Q(x^iy'^i)$ is now equivalent to $(l_i - l)q + i(q + 1) \leq lq + (r - 1)(q + 1)$. By taking $l_i = l + i - 1$, $i = 0, \ldots, r$, and $V' = \bigoplus_{i=0}^{r-1} L(l_i)\mathbb{P}^1$, we can increase the dimension by $(r - 1) + \cdots + 1 = r(r - 1)/2$ units without affecting the estimate on the minimum distance. For example, if $q = 5$ then $r = 4$. For any value of $l$ whenever $ev_P$ is injective, the dimension increases by 6 units while the Singleton-optimal defect $n - k - \lceil \frac{k}{d} \rceil + 2 - d$ decreases by 8 units. For example, for $l = 2$ this defect is reduced from 15 to 7. For codes on other curves for which the order of $y$ is much larger than the order of $x$ the increase on dimension may be higher.

**Example III.3.** In this example we take the opposite way and construct Hermitian LRC codes with improved minimum distance and the same dimension. Let $q = 3$. Instead of consider $V = L(l_\infty) \oplus L(l_\infty)\mathbb{P}^1$ we shall consider $V' = L((l+1)\infty) \oplus L((l-1)\infty)y$. It is clear that $C = ev_P(V)$ and $C' = ev_P(V')$ have the same dimension. We have $V \subseteq L((3l+4)Q)$ and $V' \subseteq L((3l+3)Q)$ what leads to an increment of one unit in the minimum distance. For larger values of $q$ the improvements became more significant. For $q = 4$, evaluating the spaces $V = L(l_\infty) \oplus L(l_\infty)y \oplus L(l_\infty)y^2$ and $V' = L((l+1)\infty) \oplus L(l_\infty)y \oplus L((l-1)\infty)y^2$, we get LRC codes over $\mathbb{F}_{16}$ with length $n = 64$ and locality $r = 3$. Here $V \subseteq L((4l+10)Q)$ and $V' \subseteq L((4l+6)Q)$, so the improvement on the minimum distance should be about 4 units. The dimension $k$ and true minimum distances $d, d'$ of these codes have been computed with Magma [6] and are listed in Table 1.

The modified construction also allows us to recover more than one erasure. Following the standard notation stated in the Introduction, suppose we want to correct $r - 1$ erasures in the $r + p - 1$ coordinates corresponding to a fibre of $\phi$. For this, write the degree of the separable morphism $\phi : X \rightarrow Y$ as $r + p - 1$. Then we consider the space of functions
\[
V' = \bigoplus_{i=0}^{r-1} L(D_i)y^i \subseteq \mathbb{F}_q(X)
\]
and define $C = ev_P(V') \subseteq \mathbb{F}_q^n$. Given a function $f \in V'$, the restriction of $f$ at the points in a fibre of $\phi$ is a polynomial of degree $r - 1$ that can be computed from the information of any $r$ available coordinates among the $r + p - 1$ corresponding to points in this fibre. As in the case of one erasure, $C$ is an LRC code of parameters $k = \sum_{i=0}^{r-1} \ell(D_i)$ and $n - \deg(G) \leq d \leq \min\{d_i : 0 \leq i \leq r - 1\}$, provided that $ev_P|_{V'}$ is injective, where $G$ and the $d_i$’s are as in the case of one erasure.

| $l$  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
|-----|---|---|---|---|---|---|---|---|---|----|----|----|----|
| $k$ | 6 | 9 | 12| 15| 18| 21| 24| 27| 30| 33 | 36 | 39 | 42 |
| $d$ | 50| 46| 42| 38| 34| 30| 26| 22| 18| 14 | 10 | 8  | 6  |
| $d'$| 54| 50| 46| 42| 38| 34| 30| 26| 22| 18 | 14 | 10 | 8  |

Table I. Parameters of $C$ and $C'$ in Example III for $q = 4$. 


IV. AG codes as LRC codes

As in the previous section, let $\mathcal{X}, \mathcal{Y}$ be two curves over $\mathbb{F}_q$, $V = \bigoplus_{i=0}^{r-1} L(D_i) y^i \subseteq \mathbb{F}_q(\mathcal{X})$ and $C = ev_P(V)$. Our estimate on the minimum distance of $C$ comes from the Goppa bound on the minimum distance of the AG code $C(\mathcal{P}, G) = ev_P(L(G))$, where $G$ is the smallest divisor on $\mathcal{X}$ such that $V \subseteq L(G)$. It follows that $C(\mathcal{P}, G)$ is the smallest AG code containing $C$. The error correction capabilities of $C$ are estimated through the corresponding capabilities of $C(\mathcal{P}, G)$. Furthermore, no efficient algorithms for decoding $C$ are currently available, so that we are compelled to decode $C$ as a subcode of $C(\mathcal{P}, G)$. Consequently the best results are obtained when $C$ is an AG code itself, that is when $V = L(G)$. In general we can not expect this to happen when $D_0 = \cdots = D_{l-1}$ but it is possible when these divisors are suitably chosen. To show an example, in this section we discuss the case of Hermitian codes and the morphism $\phi = x$. Note that in this case a function $f \in L(\infty Q) \subset \mathbb{F}_q^*(\mathcal{H})$ can be uniquely written as a polynomial $f \in \mathbb{F}_q[x][y]$ with $\deg_y(f) < q$. Such $f$ may appear in the set $V$ of an LRC code if $\deg_y(f) < q - 1$.

**Proposition IV.1.** Let $\mathcal{H}$ be the Hermitian curve $x^q + 1 = y + y^q$ over $\mathbb{F}_q$. The space of functions $V = \bigoplus_{i=0}^{t} \langle 1, x, x^2, \ldots, x^i \rangle y^i \subseteq \mathbb{F}_q(\mathcal{H})$, with $t \leq q - 2$ is a Riemann-Roch space $L(G)$ if and only if there exists $j$, $0 \leq j \leq t + 1$, such that $l_{j-i} = i$ if $i < j$ and $l_{j-i} = i + 1$ if $i \geq j$. In this case $G = mQ$, where $Q$ is the point at infinity of $\mathcal{H}$ and $m = (t + 1)q + t - j$ if $j \leq t$ or $m = t(q + 1)$ if $j = t + 1$.

**Proof:** The smallest Riemann-Roch space containing $V$ is $L(mQ)$ with $m = \max \{-v_Q(x^i y^j) : i = 0, \ldots, t\} = \max \{l_i + q(i+1) : i = 0, \ldots, t\}$. Let us first assume $V = L(mQ)$. Then for $i = 0, \ldots, t$, we have $l_i \leq i + 1$, since otherwise $-v_Q(x^i y^j) > -v_Q(y^i y^{j-i}) > -v_Q(y^{i+1})$ so $y^{i+1} \in V$. In particular $l_0 = 0$ and $l_t = 1$. A similar argument proves that for all $i = 1, \ldots, t$, we have $l_{i-1} \geq l_i + 1$. From these two conditions we deduce that there exists $j$, $0 \leq j \leq t + 1$, such that $l_{j-i} = i$ if $i < j$ and $l_{j-i} = i + 1$ if $i \geq j$. Conversely, it is simple to check that under these conditions we have $m = -v_Q(x^{l_i} y^{l_{j-i}}) = (j + 1)q + (t - j)(q + 1) = (t + 1)q + t - j$ if $j \leq t$ and $m = -v_Q(y^{l_j}) = t(q + 1)$ if $j = t + 1$. In either case it holds that $\dim(V) = \ell(mQ)$, hence we get equality $V = L(mQ)$.

**Example IV.2.** Consider the LRC codes obtained from the Hermitian curve with $q = 4$ and the morphism $\phi = x$. For short let us restrict to those codes correcting one erasure per fibre (that is $t = 2$). There are exactly four among them which are AG codes, namely the evaluation of the following spaces

$V = \langle 1, x, x^2 \rangle \oplus \langle 1, x \rangle y \oplus \langle 1 \rangle y^2 = L(-v_Q(y^2)Q) = L(10Q)$

$V = \langle 1, x, x^2, x^3 \rangle \oplus \langle 1, x \rangle y \oplus \langle 1 \rangle y^2 = L(-v_Q(x^3)Q) = L(12Q)$

$V = \langle 1, x, x^2, x^3 \rangle \oplus \langle 1, x \rangle x^2 y \oplus \langle 1 \rangle y^2 = L(-v_Q(x^2 y)Q) = L(13Q)$

$V = \langle 1, x, x^2, x^3 \rangle \oplus \langle 1, x \rangle x^2 y \oplus \langle 1, x \rangle y^2 = L(-v_Q(x y^2)Q) = L(14Q)$.

V. A simplified recovering method for some LRC-AG codes

The second remark on the properties of LRC-AG codes we present concerns the recovering method. In order to motivate this section, we begin with a simple example.

**Example V.1.** Let us consider the Hermitian LRC-AG codes of Example II.2(a) over the field $\mathbb{F}_9$. Here $r = 2$. Each fibre $\phi^{-1}(a)$ is of type $\{P_{ab_1}, P_{ab_2}, P_{ab_3}\}$ with $a^4 = b_1^3 + b_2$ for $i = 1, 2, 3$. Since a function $f \in V$ can be written as $f = g_0(x) + g_1(x) y$, with $g_0, g_1 \in L(D)$, we have $f(P_{ab_i}) = g_0(a) + g_1(a) b_i$ and thus

$f(P_{ab_1}) + f(P_{ab_2}) + f(P_{ab_3}) = 3g_0(a) + g_1(a)(b_1 + b_2 + b_3) = g_1(a)(b_1 + b_2 + b_3) = 0$

because $b_1 + b_2 + b_3 = 0$ as it is the sum of the roots of the polynomial $t(T) = T^3 + T - a^4$ (that is the coefficient of $T^2$). Then the coordinate $f(P_{ab_1})$ of the codeword $ev_P(f)$ can be recovered as $f(P_{ab_1}) = -f(P_{ab_2}) - f(P_{ab_3})$. 

Thus, although the general construction of LRC-AG codes ensures the local recovery by polynomial interpolation, the above example shows that in some cases recovering may be performed also through a simple checksum, which is much faster and easier. Furthermore this property can be viewed as an additional feature of such codes, allowing a simple and fast checking of each block in a codeword for possible errors. In this section we shall show a wide family of LRC-AG codes with this property. To that end we first recall some identities regarding roots of univariate polynomials. Consider the elementary symmetric polynomials over a domain $A$

\[
\sigma_1 = \sigma_1(x_1, \ldots, x_d) = x_1 + \ldots + x_d
\]
\[
\sigma_2 = \sigma_2(x_1, \ldots, x_d) = x_1x_2 + x_1x_3 + \ldots + x_{d-1}x_d
\]
\[\vdots
\]
\[
\sigma_d = \sigma_d(x_1, \ldots, x_d) = x_1 \cdots x_d.
\]

The monic polynomial $T^d - \sigma_1 T^{d-1} + \sigma_2 T^{d-2} + \cdots + (-1)^d \sigma_d$ has roots $x_1, \ldots, x_d$. Consequently, for a polynomial $t(x) = t_d T^d + \ldots + t_1 T + t_0 \in A[x]$, the elementary symmetric polynomials on the roots $x_1, \ldots, x_d$ of $t$ are related to its coefficients by the identities

\[
\sigma_i = (-1)^i \frac{t_{d-i}}{t_d}, \quad i = 1, \ldots, d
\]

known as the Vieta’s formulae [4]. Consider now for $s \geq 1$ the multivariate polynomials

\[
\pi_s = \pi_s(x_1, \ldots, x_d) = x_1^s + \cdots + x_d^s \in A[x_1, \ldots, x_d],
\]

which are related to the elementary symmetric polynomials by the Newton-Girard relations [4]: for each integer $s \geq 1$ we have

\[
\pi_1 = \sigma_1
\]
\[
\pi_2 = \sigma_1 \pi_1 - 2\sigma_2
\]
\[\vdots
\]
\[
\pi_s = -\left(\sum_{j=1}^{s-1}(-1)^j \pi_{s-j} \sigma_j\right) - (-1)^s s \sigma_s.
\]

Let $p$ be the characteristic of $\mathbb{F}_q$. Remember that a polynomial $L(x) \in \mathbb{F}_q[x]$ is linearized if the exponents of all its nonzero monomials are powers of $p$. In this case, a polynomial $L(x) - \alpha$, $\alpha \in \mathbb{F}_q$, is called affine $p$-polynomial.

**Lemma V.2.** If $x_1, \ldots, x_d$ are roots of an affine $p$-polynomial of degree $d$ over $\mathbb{F}_q$, then $\pi_i(x_1, \ldots, x_d) = 0$ for $i = 1, \ldots, d - 2$.

**Proof:** By induction. Clearly $\pi_1 = \sigma_1 = 0$. Assume $\pi_1 = \cdots = \pi_{i-1} = 0$ for $i \leq d - 3$. Then $\pi_i = \pm i \sigma_i$. If $\sigma_i = 0$ we have $\pi_i = 0$. If $\sigma_i \neq 0$ then $d - i = p^h - i$ is a power of $p$. Thus $i \equiv 0 \pmod{p}$ and again $\pi_i = 0$. Therefore $\pi_1 = \cdots = \pi_{d-2} = 0$.

Next we extend the idea of Example V.1 to a wide class of curves providing families of LRC codes allowing local recovery by a checksum function. The codes we propose come from the family of Artin-Schreier curves. More precisely let $\mathcal{X}$ be an algebraic smooth curve defined over $\mathbb{F}_q$ by an equation of separated variables $u(x) = v(y)$, where $u$ and $v$ are univariate polynomials over $\mathbb{F}_q$ of coprime degrees and $v$ is a separable linearized polynomial of degree $m = p^h$, with $p = \text{char}(\mathbb{F}_q)$. Let $\phi : \mathcal{X} \to \mathbb{P}^1$ be the morphism of degree $m$ given by the rational function $x$ and consider the set

\[
M = \{a \in \mathbb{F}_q : \text{there exists } b \in \mathbb{F}_q \text{ with } u(a) = v(b)\}.
\]

Note that, by our assumptions on $v$, for each $a \in M$ the function $x - a$ has $m$ distinct zeroes. Note also that $\mathcal{X}$ has exactly one point at infinity $Q$ which is the common pole of $x$ and $y$. $Q$ is the only point of
Therefore of the remaining symbols in the fibre $v$ we have $\pi f = g$. Clearly it holds that $V \subseteq L(\infty Q)$ and the Weierstrass semigroup $S(Q)$ of $X$ at $Q$ is generated by $-v_Q(x) = \deg(v)$ and $-v_Q(y) = \deg(u)$. Consider also the set of points $P = \phi^{-1}(S) \setminus \{Q\}$. Then we have a code $C = ev_P(V) \subseteq \mathbb{F}_q^n$ of length $n = \#P = ms$. According to the results stated in Section III, $C$ is an LRC code based on polynomial interpolation with locality $r = m - 1$.

**Proposition V.3.** The linear code $C \subseteq \mathbb{F}_q^n$ described above is an LRC code with locality $m - 1$ allowing a local recovery based on addition.

**Proof:** Let $\phi^{-1}(a) = \{P_1, \ldots, P_m\}$ be the fibre of $x$ at $a \in \mathbb{F}_q$ and write $f_{aj} = f(P_j)$ the evaluation at the point $P_j \in \phi^{-1}(a)$ of a function

$$f = \sum_{i=0}^{m-2} g_i y^i \in V.$$

The functions $g_i \in L(D_i)$ are constant over each fibre so we can write $g_i = g_i(P_j) \in \mathbb{F}_q$ for any $P_j$. Then $f_{aj} = g_0 b_j^0 + \cdots + g_{m-2} b_j^{m-2}$ with $b_j = y(P_j)$ and so

$$\sum_{j=1}^{m} f_{aj} = mg_0 + g_1 \pi_1 + \cdots + g_{m-2} \pi_{m-2} = g_1 \pi_1 + \cdots + g_{m-2} \pi_{m-2}$$

where $\pi_i = \pi_i(b_1, \ldots, b_m)$ is the $i$-th Newton-Girard polynomial on the roots $b_1, \ldots, b_m$ of $t(T) = v(T) - u(a)$. Since $t(T)$ is an affine $p$-polynomial, it follows from Lemma V.2 that $\pi_1 = \cdots = \pi_{m-2} = 0$. Therefore $f_{a1} + \cdots + f_{am} = 0$ and the local recovery of an erased symbol $f_{aj}$ is obtained from the sum of the remaining symbols in the fibre $x^{-1}(a)$. 

**Example V.4.** LRC codes arising from Hermitian and Norm-Trace curves by means of construction (a) of Examples II.2 and II.3 verify the above conditions. Thus recovering single erasures on these codes can be performed through addition.

**References**

[1] E. Ballico, C. Marcolla, *Higher Hamming weights for locally recoverable codes on algebraic curves*, Finite Fields and Their Applications 40 (2016), pp. 61–72.
[2] A. Barg, I. Tamo, S. Vladut, *Locally recoverable codes on algebraic curves*. Proceedings of the 2015 IEEE International Symposium on Information Theory, Hong Kong, 2015, pp. 1252–1256.
[3] A. Barg, I. Tamo, S. Vladut, *Locally recoverable codes on algebraic curves*. [arXiv:1603.08876](http://arxiv.org/abs/1603.08876)
[4] D. Cox, J. Little, D. O’Shea, *Ideals, Varieties, and Algorithms*. New York: Springer-Verlag, 1992.
[5] P. Gopalan, C. Huang, H. Simitci, S. Yekhanin, *On the locality of codeword symbols*, IEEE Transactions on Information Theory vol. 58, no. 11 (2012), pp. 6925–6934.
[6] Magma Computational Algebra System. Online available at [http://magma.maths.usyd.edu.au/magma/](http://magma.maths.usyd.edu.au/magma/).
[7] C. Munuera, A. Sepúlveda, F. Torres, *Castle curves and codes*, Advances in Mathematics of Communications 3 (2009), pp. 399-408.
[8] I. Tamo, A. Barg, *A family of optimal locally recoverable codes*, IEEE Transactions on Information Theory vol. 60, no. 8 (2014), pp. 4661–4676.
[9] H. Maharaj, *Explicit constructions of algebraic-geometric codes*, IEEE Transactions on Information Theory vol. 51, no. 2 (2005), pp. 714–722.