Cryptography and Communications (2024) 16:949–959
https://doi.org/10.1007/s12095-024-00713-2

RESEARCH

Mumford representation and Riemann-Roch space of a divisor on a hyperelliptic curve

Giovanni Falcone[1] · **Giuseppe Filippone**[1]

Received: 23 October 2023 / Accepted: 27 March 2024 / Published online: 10 April 2024

Abstract
For an (imaginary) hyperelliptic curve $\mathcal{H}$ of genus g, with a Weierstrass point Ω, taken as the point at infinity, we determine a basis of the Riemann-Roch space $\mathcal{L}(\Delta + m\Omega)$, where Δ is of degree zero, directly from the Mumford representation of Δ. This provides in turn a generating matrix of a Goppa code.

Keywords Goppa codes · Riemann-Roch space · Hyperelliptic curves

Mathematics Subject Classification 94B27 · 14H51 · 14G50

The first algorithm for the computation of a basis of the Riemann-Roch space $\mathcal{L}(D)$ associated to a divisor D on a curve is ascribed to von Brill and Noether [2]. Because such a basis allows both to construct algebraic geometric codes and to give addition formulas in the divisor class group of the curve, it is an essential tool in Coding Theory and Cryptography, and many authors have worked on the problem to make its computation more effective (e.g., [5, 8]), often in the equivalent scenario of function fields (cf. [19, Remark 2.3.15]). In particular, an algorithm, which is polynomial in the input size, is given in [7] with an arithmetic approach to the Riemann-Roch problem, and other algorithms were developed in order to simplify the computation, each under particular assumptions.

In this paper the class of hyperelliptic curves is considered. Many papers have been devoted to the study of arithmetic in these curves, among the others we mention in particular [3, 11, 12]. The interest on the subject does not seem to decline, as witnessed by more recent publications (cf. [14, 20]). A significant literature has also been produced in order to consider

Supported by **Budget strategico Dip (BsD)**, Supported by **Sustainability Decision Framework (SDF)** Research Project – CUP **B79J23000540005** – Grant Assignment Decree No. **5486** adopted on **2023-08-04**.

✉ Giuseppe Filippone
giuseppe.filippone01@unipa.it

Giovanni Falcone
giovanni.falcone@unipa.it

[1] Dipartimento di Matematica e Informatica, Università degli Studi di Palermo, Via Archirafi 34, Palermo 90123, Italy

codes over hyperelliptic curves [1, 13, 17], and hyperelliptic curves in Cryptography have been investigated, e.g., in [10, 11, 18].

Both the Mumford representation of a divisor Δ of degree zero on a hyperelliptic curve and the Riemann-Roch space $\mathcal{L}(D)$, where $D = \Delta + m\Omega$, are the subject of a large number of papers, also due to their applications in Coding theory. The dimension of $\mathcal{L}(D)$ has been computed in [1, Lemma 2.1, p. 155] and an explicit basis of $\mathcal{L}(D)$ has been indicated in [4, Theorem 1, p. 275].

But it has not been indicated in the literature that a basis of the latter can be directly found from the former, and it is the aim of the present note to give an explicit basis of $\mathcal{L}(D)$, stressing the meaning of the Mumford representation of Δ in this context. Note that, for a nodal curve, a data structure inspired by the Mumford representation has been used for the same purpose in a recent paper by Le Gluher and Spaenlehauer [14], and that in a paper by Garzón and Navarro [5] a basis of $\mathcal{L}(D)$ in the more general case of superelliptic curves is provided, but for a given divisor D.

Algebraic geometric codes were introduced by Goppa in [6] several decades ago. These codes turned out not only to be interesting in Coding Theory, but also to be applicable in Cryptography, e.g. in public-key cryptographic systems [9, 16].

Using this basis, one constructs directly a generating matrix of an algebraic geometric code over a hyperelliptic curve defined over a Galois field of characteristic $p \geq 2$. Also, it is possible to construct MDS codes. We make this for a toy model of MDS codes in Section 3. Although the reduction of a divisor D to its reduced Mumford form might be an inconvenient task, involving the application of the Cantor algorithm (see Remark 1), this difficulty does not occur in the construction of algebraic geometric codes, because in that case one can directly take D in the reduced form $D = \Delta + m\Omega$.

1 Notations and reduction to the Mumford representation

Let K be the algebraic closure of the field k and let $\mathcal{H}$ be a hyperelliptic curve of genus g over k with a rational Weierstrass point Ω. The non-singular curve $\mathcal{H}$ is described by an affine equation of the form

$$y^2 + yh(x) = f(x) \tag{1.1}$$

where $f(x)$ is a polynomial of degree $d = 2g + 1$, $h(x)$ is a polynomial of degree at most g, and $\Omega = [0 : 1 : 0]$ is the point at infinity of $\mathcal{H}$ [15, Prop. 1.2]. If $\mathrm{char}\,\mathsf{k} \neq 2$, changing y into $y - h(x)/2$, and $f(x)$ into $f(x) - h^2(x)/4$, transforms the above equation into

$$y^2 = f(x),$$

whereas, if $\mathrm{char}\,\mathsf{k} = 2$, then it is not possible to reduce $h(x)$ to zero.

Let D be a divisor of $\mathcal{H}$. Since its Riemann-Roch space

$$\mathcal{L}(D) = \{F \in \mathsf{K}(\mathcal{H}) : \mathrm{div}(F) + D \text{ is effective}\} \cup \{0\}$$

is null both in the case where D has negative degree, and in the case where D has degree zero and $D \notin \mathrm{Princ}(\mathcal{H})$, whereas $\mathcal{L}(D) = \left\langle F_0^{-1} \right\rangle$ in the case where $D = \mathrm{div}(F_0)$, from now on we will assume D has positive degree m.

Remark 1 In order to extend the use of Mumford representation to divisors of arbitrary degree, first we recap the results in [3, 10].

It follows from the Riemann-Roch theorem that each divisor of $\mathcal{H}$ can be written uniquely in the following form

$$D = P_1 + P_2 + \cdots + P_t + (m-t)\Omega + \mathrm{div}(\psi(x,y))$$

for t points $P_1, \ldots, P_t$ in $\mathcal{H}$ distinct from Ω, with $t \leq g$, $P_i + P_j - 2\Omega \notin \mathrm{Princ}(\mathcal{H})$, and a suitable $\psi(x,y) \in \mathsf{K}(\mathcal{H})$, that is, any divisor class $D + \mathrm{Princ}(\mathcal{H}) \in \mathrm{Div}(\mathcal{H})/\mathrm{Princ}(\mathcal{H})$ can be reduced to the form $P_1 + \cdots + P_t + (m-t)\Omega$.

Let $P_i = (x_i, y_i)$ and note that any divisor

$$\Delta = l_1 P_1 + \cdots + l_s P_s - (l_1 + \cdots + l_s)\Omega$$

on the curve $\mathcal{H}$, of degree zero and such that $l_i > 0$ for any index i, determines uniquely the polynomial $a(x) = (x - x_1)^{l_1} \cdots (x - x_s)^{l_s}$ and the polynomial $b(x)$ which is the polynomial such that $b(x_t) = y_t$ (with a corresponding degree of contact with $\mathcal{H}$, in the case where $l_i > 1$, that is, such that $\left(\frac{d}{dx}\right)^j (b^2(x) + b(x)h(x) - f(x))|_{x=x_i} = 0$, for $0 \leq j \leq l_i - 1$). Hence $b^2(x) + h(x)b(x) - f(x)$ is a multiple of $a(x)$ and the degree of $b(x)$ is smaller than the degree of $a(x)$, and conversely, a pair of polynomials $a(x)$ and $b(x)$ such that $b^2(x) + h(x)b(x) - f(x)$ is a multiple of $a(x)$ and the degree of $b(x)$ is smaller than the degree of $a(x)$ defines such a divisor of degree zero, which is written as $\Delta = \mathrm{div}(a(x), b(x))$. Note that an intersection point of the curve with the x-axis is contained in the support of Δ if and only if $\mathrm{GCD}(a(x), a'(x), b(x)) \neq 1$. If $\mathrm{GCD}(a(x), a'(x), b(x)) = 1$ and the degree of $a(x)$ is not greater than the genus g of the curve (or equivalently, if the support of Δ contains at most g points which are mutually non-opposite), one says that $\mathrm{div}(a(x), b(x))$ is in Mumford form (or reduced form).

Now, we can directly extend the Mumford representation to any divisor $D = D_1 - D_2$ (with D_i effective of degree $m_i \in \mathbb{Z}$) by writing it as

$$D = \Delta + m\Omega + \mathrm{div}(\psi(x,y)),$$

with $m = m_1 - m_2$, for a suitable divisor $\Delta = \mathrm{div}\left(u(x), v(x)\right)$ in Mumford form, and a suitable function $\psi(x,y)$, obtained with the following argument.

First, taking the vertical lines $x - x_i$ passing through the points in the support of D_2 we can write

$$-D_2 = D_2' - 2m_2\Omega - \mathrm{div}(\phi),$$

with $\phi = \prod(x - x_i)$ and D_2' effective, hence

$$D = D_1 - D_2 = D_3 - 2m_2\Omega - \mathrm{div}(\phi),$$

with $D_3 = D_1 + D_2'$ an effective divisor of degree $m_1 + m_2$, hence of the form

$$D_3 = \mathrm{div}(a(x), b(x)) + (m_1 + m_2)\Omega.$$

Secondly, applying the reduction step in Cantor's algorithm (cf. [3], and [10] in the case where $\mathrm{char}\,\mathsf{k} = 2$), we change D_3 with

$$D_3' = D_3 - \mathrm{div}(y - b(x)) = \mathrm{div}(a'(x), b'(x)) + (m_1 + m_2)\Omega,$$

which belong to the same divisor class, where

$$a'(x) = \frac{f(x) - b(x)h(x) - b^2(x)}{a(x)}$$

and

$$b'(x) = -h(x) - b(x) \mod a'(x).$$

This way $\deg a'(x) < \deg a(x)$, hence after finitely many iterations one gets $\deg a'(x) \leq g$, and one can write

$$D = \Delta + m\Omega + \mathrm{div}(\psi(x, y)),$$

where $\psi(x, y)$ is the resulting function of the above reduction.

Finally, the function

$$\Phi : \mathcal{L}(D) \mapsto \mathcal{L}(\Delta + m\Omega),$$

mapping F onto the product $\psi(x, y)F$, is an isomorphism.

Up to the latter isomorphism, we will directly assume that $D = \Delta + m\Omega$, $m > 0$.

2 Main theorem

In the following theorem we determine a basis of $\mathcal{L}(D)$, with $D = \Delta + m\Omega$, and $\Delta = \mathrm{div}(u(x), v(x))$ is in Mumford representation, with $\deg u(x) \leq g$. We recall that, up to the isomorphism defined in Remark 1, any divisor can be reduced in such a form. Also, the kind of unexpected varying, according to m, of its dimension becomes manifest: in order to determine $\dim \mathcal{L}(D)$, in [1, Lemma 2.1] it is distinguished the case $m \geq 2g - t - 1$ (with $t := \deg u(x)$, where it is proved that, in spite of the general behavior, $\dim \mathcal{L}(D) = m - g + 1$, and the case $t \leq m < 2g - t - 1$, where $\dim \mathcal{L}(D) = \left\lfloor \frac{m-t}{2} \right\rfloor + 1$ (cf. Remark 2 for details).

Theorem 1 Given the hyperelliptic curve $\mathcal{H}$ of genus g and degree $d = 2g + 1$ defined by (1.1), given the divisor $D = \Delta + m\Omega$ of positive degree m on $\mathcal{H}$, with $\Delta = \mathrm{div}(u(x), v(x))$ in Mumford representation, let $t := \deg u(x) \leq g$ and let

$$\Psi(x, y) = \frac{y + v(x)}{u(x)},$$

for $\mathrm{char}\, \mathsf{k} = p > 2$, and $\Psi(x, y) = \frac{y+v(x)+h(x)}{u(x)}$, for $p = 2$.

If $m < d - t$, then a basis of $\mathcal{L}(D)$ is provided by the set of functions x^i, with $0 \leq i \leq \frac{m-t}{2}$.

If $m \geq d - t$, then a basis of $\mathcal{L}(D)$ is provided by the set of functions x^i and $\Psi(x, y) \cdot x^j$, with $0 \leq i \leq \frac{m-t}{2}$ and $0 \leq j \leq \frac{m-(d-t)}{2}$.

Proof In order to compute $\mathrm{div}(\Psi(x, y))$, recall that $\deg v(x) < \deg u(x) \leq g$ and that, in the case where $p = 2$, $\deg h(x) \leq g$, as well.

Since $l = \max(\deg v(x), \deg h(x)) \leq g$, the degree of $\big(-v(x) - h(x)\big)^2$ is smaller than the degree of $f(x)$, hence there are $d = 2g + 1$ (not necessarily distinct) intersection points of the curve $y + v(x) + h(x) = 0$ and $\mathcal{H}$ in the affine plane, the remaining $d(l - 1)$ intersection points coinciding with Ω. More precisely, t intersection points in the affine plane belong to the support of the divisor $\widehat{\Delta} = \mathrm{div}\,\big(u(x), w(x)\big)$ in Mumford representation, where $w(x) = -v(x) - h(x) \mod u(x)$, therefore

$$\mathrm{div}\,\big(y + v(x) + h(x)\big) = \widehat{\Delta} + W + \big(t + d(l - 1)\big)\Omega,$$

where W is the effective divisor of degree $d - t$, whose support consists of the remaining intersection points in the affine plane. Note that, in the case $t = 0$, the divisor Δ has the

Mumford representation $(1, 0)$ and the degree of W is $d = 2g + 1$ and the support of W coincides with the intersections of $\mathcal{H}$ with the curve $y + h(x) = 0$.

On the other hand, the intersection of $u(x) = 0$ and $\mathcal{H}$ is simply

$$\operatorname{div}\big(u(x)\big) = \Delta + \widehat{\Delta} + (td)\Omega.$$

Summarizing, if $t > 0$, then

$$\begin{aligned}\operatorname{div}(\Psi(x, y)) &= \operatorname{div}\big(y + v(x) + h(x)\big) - \operatorname{div}\big(u(x)\big)\\ &= W - \Delta - (d - t)\Omega\end{aligned} \tag{2.1}$$

and, if $t = 0$, then $\Delta = (1, 0)$ and $\Psi(x, y) = y + h(x)$, whence

$$\operatorname{div}(\Psi(x, y)) = \operatorname{div}(y + h(x)) - \operatorname{div}(1) = W - d\Omega,$$

thus in both cases the equality (2.1) holds. Hence

$$\Psi(x, y) \in \mathcal{L}(D) \text{ if and only if } m \geq d - t. \tag{2.2}$$

Let $m \geq d - t$, that is, the case where $\Psi(x, y) \in \mathcal{L}(D)$. First we consider the cases where either $t = 0$ (hence $m \geq d = 2g + 1$), or $t = 1$ (hence $m \geq d - 1$), or $t \geq 2$ and $m \geq d - 2$, as in these cases we know, by the theorem of Riemann-Roch, that the dimension of $\mathcal{L}(D)$ is $m - g + 1$. Thus, in order to prove that

$$\mathcal{L}(D) = \left\langle x^i, \Psi(x, y) \cdot x^j \right\rangle, \text{ with } 0 \leq i \leq \frac{m - t}{2} \text{ and } 0 \leq j \leq \frac{m - (d - t)}{2}, \tag{2.3}$$

it is sufficient to note that, for each of those values of the parameters i and j, these functions belong to $\mathcal{L}(D)$, because

$$1 + \left\lfloor \frac{m - t}{2} \right\rfloor + 1 + \left\lfloor \frac{m - (d - t)}{2} \right\rfloor = m - g + 1,$$

and the claim will follow from dimensional reasons. Now,

$$D + \operatorname{div}(x^i) = (\Delta + m\Omega) + i \cdot \operatorname{div}(x), \tag{2.4}$$

as well as

$$\begin{aligned}D + \operatorname{div}\left(\Psi(x, y) \cdot x^j\right) &= (\Delta + m\Omega) + j \cdot \operatorname{div}(x) + \big(W - \Delta - (d - t)\Omega\big)\\ &= W + j \cdot \operatorname{div}(x) - (d - t - m)\Omega,\end{aligned} \tag{2.5}$$

are effective divisors, hence the functions belong to $\mathcal{L}(D)$.

Secondly, we consider the case where $d - t \leq m < d - 2$. In this case, the dimension of $\mathcal{L}(D)$ is not necessarily $m - g + 1$, but still $\Psi(x, y) \in \mathcal{L}(D)$.

If $0 \leq \epsilon \leq t - 2$, and if, for short, we put $m = m_\epsilon = d - 2 - \epsilon$, then

$$\mathcal{L}_\epsilon := \mathcal{L}(\Delta + m_\epsilon\Omega),$$

hence the space $\mathcal{L}_0 = \mathcal{L}(\Delta + (d - 2)\Omega)$ is generated, by the above case, by the functions x^i and $\Psi(x, y) \cdot x^j$ with $0 \leq i \leq \frac{m_0 - t}{2}$ and $0 \leq j \leq \frac{m_0 - (d-t)}{2}$. Of course, $\mathcal{L}_{\epsilon+1} \subseteq \mathcal{L}_\epsilon$, and we will see that $\dim(\mathcal{L}_{\epsilon+1}) = \dim(\mathcal{L}_\epsilon) - 1$. Indeed, by (2.4) and (2.5), the functions x^i, $\Psi(x, y)x^j$ of $\mathcal{L}_\epsilon$ belong to $\mathcal{L}_{\epsilon+1}$ as long as $i \leq \frac{m_{\epsilon+1} - t}{2}$, and $j \leq \frac{m_{\epsilon+1} - (d-t)}{2}$, that is,

$$\dim(\mathcal{L}_{\epsilon+1}) = 1 + \left\lfloor \frac{m_{\epsilon+1} - t}{2} \right\rfloor + 1 + \left\lfloor \frac{m_{\epsilon+1} - (d - t)}{2} \right\rfloor,$$

and our assertion is proved. In particular, we found that $\dim(\mathcal{L}_{\epsilon+1}) = \dim(\mathcal{L}_\epsilon) - 1$, because $m_{\epsilon+1} = m_\epsilon - 1$ and

$$\dim(\mathcal{L}_\epsilon) = 1 + \left\lfloor \frac{m_\epsilon - t}{2} \right\rfloor + 1 + \left\lfloor \frac{m_\epsilon - (d-t)}{2} \right\rfloor,$$

where the missing function is, once for one, x^i or $\Psi(x, y)x^j$, because d is odd and changes the parity of $m_{\epsilon+1} - t$ in that of $m_{\epsilon+1} - (d - t)$.

Now we consider the cases where $m < d - t$, that is, the cases where, by (1.1), $\Psi(x, y) \notin \mathcal{L}(D)$. If $t = 0$ and $m \in \{d - 2, d - 1\}$, or if $t = 1$ and $m = d - 2$, then on the one hand $\lfloor \frac{m-t}{2} \rfloor = m - g$ and, on the other hand, by the theorem of Riemann-Roch, the dimension of $\mathcal{L}(D)$ is $m - g + 1$. Thus, by dimensional reasons, $\mathcal{L}(D) = \langle x^i \rangle$, where $0 \le i \le \lfloor \frac{m-t}{2} \rfloor$.

In order to prove that $\mathcal{L}(D) = \langle x^i \rangle$, where $0 \le i \le \frac{(m-t)}{2}$ also in the remaining cases where either $t = 0, 1$ and $m < d - 2$, or $2 \le t \le m < d - t$, write $m = m_\epsilon = d - t - \epsilon$ with $1 \le \epsilon \le d - 2t$, and again put, for short,

$$\mathcal{L}_\epsilon := \mathcal{L}(\Delta + m_\epsilon \Omega).$$

Note that appending the value $\epsilon = 0$, that is, considering also the case where $m = m_0 = d - t$, by (2.3) we have $\mathcal{L}_0 = \langle x^i, \Psi(x, y) \rangle$, with $0 \le i \le \frac{m_0 - t}{2}$.

Of course, $\mathcal{L}_{\epsilon+1} \subseteq \mathcal{L}_\epsilon$ for any $0 \le \epsilon \le d - 2t$, but in this case we will see that

$$\dim(\mathcal{L}_{\epsilon+1}) = \begin{cases} \dim(\mathcal{L}_\epsilon) & \text{if } m_\epsilon - t \text{ is odd,} \\ \dim(\mathcal{L}_\epsilon) - 1 & \text{if } m_\epsilon - t \text{ is even.} \end{cases} \tag{2.6}$$

Indeed, by (2.2) $\Psi(x, y) \notin \mathcal{L}_\epsilon$ as soon as $\epsilon > 0$, and since, by (2.4), the functions x^i of $\mathcal{L}_\epsilon$ belong to $\mathcal{L}_{\epsilon+1}$ as long as $i \le \frac{m_{\epsilon+1} - t}{2}$, we see that

$$\dim(\mathcal{L}_{\epsilon+1}) = 1 + \left\lfloor \frac{m_{\epsilon+1} - t}{2} \right\rfloor,$$

and we get the equalities in (2.6), because $m_{\epsilon+1} = m_\epsilon - 1$. But this equality shows, as well, that the theorem is true for any value of m. □

Remark 2 It is remarkable that the dimensions in [1, Lemma 2.1] look different from the ones above: for $m = 2g - t, 2g - t - 1$, in our theorem we find $\dim \mathcal{L}(D) = 1 + \lfloor \frac{m-t}{2} \rfloor$, whereas in [1, Lemma 2.1] we read $\dim \mathcal{L}(D) = m - g + 1$. Of course, the two values coincide exactly for $m = 2g - t, 2g - t - 1$.

In particular, the necessary condition in [1, Lemma 2.1] to have $\dim \mathcal{L}(D) \ne m - g + 1$, that is, $m < d - t - 2$, is also sufficient.

An interesting phenomenon occurs when $g < m < 2g - 1$ and $t \in \{g, g - 1, g - 2\}$, because in these cases $m \ge d - t - 2$, hence $\dim \mathcal{L}(D) = m - g + 1$, regardless of the theorem of Riemann-Roch.

3 Applications to coding theory

A $[n, k, \delta]$ *linear code of minimal distance* δ is a k-dimensional subspace of the n-dimensional vector space over the Galois field $\mathrm{GF}(q)$, such that any two vectors of the code differ in at least δ entries (we address the reader to, e.g., [19] for a general reference). The number of entries for which any two vectors are different defines the *Hamming distance*, and it is easy

to prove, by using the triangular inequality, that corrupting a vector of a $[n, k, \delta]$ linear code in at most $\frac{\delta-1}{2}$ entries does not give a vector belonging to the code, thus avoiding possible misunderstandings in communication. The distance between a vector $\mathbf{w}$ and the zero vector is the *weight* of $\mathbf{w}$, and it is manifest that the minimal distance of a code coincides with the minimal weight of a non-zero vector. The *Singleton bound* states that $\delta \leq n - k + 1$, and a linear code is *optimal* or MDS (maximum distance separable) if the equality holds.

Algebraic geometric linear codes are defined by taking a divisor D on a curve $\mathcal{C}$ over a finite field $\mathrm{GF}(q)$ and a divisor $R = \sum_{i=1}^{n} P_i$, with $P_1, \ldots, P_n$ fixed rational points of the curve, not in the support $\mathrm{supp}(D)$ of D, then

$$C_{\mathcal{L}}(R, D) = \{(f(P_1), \ldots, f(P_n)) \colon f \in \mathcal{L}(D)\}$$

is an $[n, k, \delta]$ code with parameters $k = \ell(D) - \ell(D - R)$, where $\ell(*) = \dim(\mathcal{L}(*))$, and δ satisfying the *Goppa lower bound* $\delta \geq n - \deg(D)$ (cf. [6]).

Under the additional hypothesis $n - \deg(D) > 0$, we have that the divisor $D - R$ has negative degree, thus $\ell(D - R) = 0$ and $k = \ell(D)$. In this case, evaluating the k functions $f_1, \ldots, f_k$ of a basis of $\mathcal{L}(D)$ on the points $P_i \in \mathrm{supp}(R)$, the vectors $\big(f_j(P_1), \ldots, f_j(P_n)\big)$ give the rows of a generator matrix of $C_{\mathcal{L}}(R, D)$.

In this section we assume $\mathsf{k} = \mathrm{GF}(p^c)$, where $p \geq 2$ is a prime number and c a positive integer.

Note that, for any polynomials $u(x)$ and $v(x)$, with $u(x)$ of degree t, and $v(x)$ of degree smaller than t (and, if $p = 2$, for any arbitrary non-zero polynomial $h(x)$), there is a hyperelliptic curve of arbitrary genus $g \geq \max\{t, \deg(h)\}$, of equation $y^2 + yh(x) = v^2(x) + v(x)h(x) - c(x)u(x)$, for each polynomial $c(x)$ of degree $2g + 1 - t$, passing through the support of $D = \Delta + m\Omega$, with $\Delta = \mathrm{div}\big(u(x), v(x)\big)$ in Mumford representation, and all of these curves determine the same Riemann Roch space $\mathcal{L}(D)$ for D. That is, in order to give a basis of the space $\mathcal{L}(D)$ one does not have to know the curve containing the support of D. Note also that one does not need to give explicitly the points in the support of D, a sensible advantage in the construction of algebraic geometric codes, as we will see in Example 1. In that Example, we compute the generating matrix of a toy model of an algebraic geometric code of length $n = 10$ and dimension $k = 5$, arising from a hyperelliptic curves of genus $g = 11$, and which is a MDS code, although here the Goppa lower bound is equal to -5, and $D - R$ has positive degree.

Remark 3 Note that, for $p \leq \frac{m-t}{2}$, the polynomials x and x^{p^c} in the basis of $\mathcal{L}(D)$ take the same values in the field $\mathsf{k} = \mathrm{GF}(p^c)$, and the same occurs, for $p \leq \frac{m-(d-t)}{2}$, to the functions $\Psi(x, y)x$ and $\Psi(x, y)x^{p^c}$. This fact must be taken into account, for instance, when constructing a Goppa code.

Theorem 2 Let k be a field of characteristic $p \geq 2$, let $u(x)$ be a monic polynomial of degree t and $v(x)$ be a polynomial with $\deg(v) < t$, such that $\mathrm{GCD}(u(x), u'(x), v(x)) = 1$, and let $P_s = (x_s, y_s)$ be n pairs such that $u(x_s) \neq 0$, for any $s = 1, \ldots, n$.

If $g \geq t$, then, for any $g - t + 2 \leq k < n$, the rows of the matrix $G = (\gamma_{rs})$

$$\begin{cases} \gamma_{rs} = x_s^{r-1} & \text{for } 1 \leq r \leq \eta + 1 \\ \gamma_{rs} = \Psi(x_s, y_s) \cdot x_s^{r-\eta} & \text{for } \eta + 2 \leq r \leq k \end{cases} \quad \left(\text{where } \eta = \left\lfloor \frac{k + g - 1 - t}{2} \right\rfloor\right) \tag{3.1}$$

generate an algebraic geometric code, of dimension $\mathrm{rank}(G) \leq k$, and $n - k + 1 - g \leq \delta \leq n - \mathrm{rank}(G) + 1$, and with $\Psi(x_s, y_s) = \frac{y_s + v(x_s) + h(x_s)}{u(x_s)}$, where $h(x) = 0$, if $p > 2$, or

$h(x)$ is an arbitrary non-zero polynomial with $\deg(h) \leq g$, if $p = 2$. If $n > k + g - 1$, then $\text{rank}(G) = k$; hence G is the generator matrix of a $[n, k, \delta]$ code.

Proof Let $c(x)$ be a polynomial of degree $2g + 1 - t$ such that

$$c(x_s) = \frac{v(x_s)^2 + h(x_s)v(x_s) - y_s^2 - y_s h(x_s)}{u(x_s)},$$

for any (x_s, y_s) with $s = 1, \ldots, n$.

Hence, there is an hyperelliptic curve of genus g of equation

$$y^2 + yh(x) = f(x) = v(x)^2 + h(x)v(x) - c(x)u(x),$$

passing through the n points (x_s, y_s) and the points belonging to the support of the divisor $\text{div}(u(x), v(x))$.

The claim follows from the fact that the functions taken into account in the theorem give in turn a set of generators of the Riemann-Roch space $\mathcal{L}(D)$, where $D = \text{div}(u(x), v(x)) + (k + g - 1)\Omega$, whose dimension is k, under the additional assumption that $n > k + g - 1$.□

Remark 4 Note that, as long as $k < g - t + 2$ and the n points $P_s = (x_s, y_s)$ where we evaluate the functions of the basis of $\mathcal{L}(D)$ have different abscissæ x_s, the algebraic geometric code coincides with the $[n, k, n - k + 1]$ Reed-Solomon code on the n values $\{x_1, \ldots, x_n\} \subset \mathsf{k}$.

In the next Example 1, the additional assumption $n - \deg(D) \geq 0$ does not hold. Instead, we choose the points in the support of the divisor R as in the following Corollary, yet obtaining a k-dimensional MDS code.

Corollary 3 *Under the assumption of Theorem 2, for any $s = 1, \ldots, l$,*

- *let $(x_s, \pm y_s)$ be $n = 2l$ distinct pairs with $y_s \neq 0$, if $p > 2$, or*
- *let (x_s, y_s), $(x_s, -y_s - h(x_s))$ be $n = 2l$ distinct pairs with $h(x_s) \neq 0$, if $p = 2$, where $h(x)$ is an arbitrary non-zero polynomial with $\deg(h) \leq g$,*

such that $x_i \neq x_j$, for any $i \neq j$, $u(x_s) \neq 0$. Then the matrix G has full rank k. Furthermore, if $n = 2k$, then the code having G as generator matrix has minimal distance $\delta \geq n - k$.

Proof Let $a_s = \Psi(x_s, y_s)$ and let $b_s = \Psi(x_s, -y_s)$ if $p > 2$, or $b_s = \Psi(x_s, -y_s - h(x_s))$ if $p = 2$, for all indices s. Since

$$G := \begin{pmatrix} 1 & 1 & \cdots & 1 & 1 \\ x_1 & x_1 & \cdots & x_n & x_n \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_1^{\eta} & x_1^{\eta} & \cdots & x_l^{\eta} & x_l^{\eta} \\ a_1 & b_1 & \cdots & a_l & b_l \\ x_1 a_1 & x_1 b_1 & \cdots & x_l a_l & x_l b_l \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_1^{k-\eta-2} a_1 & x_1^{k-\eta-2} b_1 & \cdots & x_l^{k-\eta-2} a_l & x_l^{k-\eta-2} b_l \end{pmatrix},$$

subtracting to the even columns their preceding columns, one gets the following matrix:

$$\begin{pmatrix} 1 & 0 & \cdots & 1 & 0 \\ x_1 & 0 & \cdots & x_l & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_1^{\eta} & 0 & \cdots & x_l^{\eta} & 0 \\ a_1 & c_1 & \cdots & a_l & c_l \\ x_1 a_1 & x_1 c_1 & \cdots & x_l a_l & x_n c_l \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_1^{k-\eta-2} a_1 & x_1^{k-\eta-2} c_1 & \cdots & x_l^{k-\eta-2} a_l & x_l^{k-\eta-2} c_l \end{pmatrix},$$

where $c_s = b_s - a_s$ is equal to $-2\frac{y_s}{u(x_s)}$ if $p > 2$, while c_s is equal to $\frac{h(x_s)}{u(x_s)}$ if $p = 2$. In both cases they are non-zero, and, collecting the odd columns on the left and the even columns on the right, we reduce the matrix to the following block matrix form

$$\left(\begin{array}{c|c} \mathbf{V} & \mathbf{0} \\ \hline * & \mathbf{V}' \end{array}\right)$$

where $\mathbf{V}$ is a (rectangular) Vandermonde matrix, and $\mathbf{V}'$ is obtained by multiplying the columns of a (rectangular) Vandermonde matrix times c_s, thus the rank of G is k.

In order to prove that for $n = 2k$ the code having G as generator matrix has minimal distance $\delta \geq n - k$, we look for a vector $\mathbf{w}$ of the code of minimal weight δ

$$\begin{aligned} \mathbf{w} &= (u_1, \ldots, u_k) \cdot G \\ &= \big(\mathbf{f}_1(x_1) + a_1\mathbf{f}_2(x_1),\ \mathbf{f}_1(x_1) + b_1\mathbf{f}_2(x_1),\ \ldots,\ \mathbf{f}_1(x_l) + a_l\mathbf{f}_2(x_l),\ \mathbf{f}_1(x_l) + b_l\mathbf{f}_2(x_l)\big), \end{aligned}$$

where $\mathbf{f}_1(x_s) = \sum_{i=1}^{\eta+1} u_i \cdot x_s^{(i-1)}$, and $\mathbf{f}_2(x_s) = \sum_{i=\eta+2}^{k} u_i \cdot x_s^{(i-\eta-2)}$, for all $s = 1, \ldots, l$. It is harmless to assume that $\eta \geq k - \eta - 2$.

In order to count the maximal possible number of zeros in the entries $\mathbf{f}_1(x_s) + a_s\mathbf{f}_2(x_s)$ or $\mathbf{f}_1(x_s) + b_s\mathbf{f}_2(x_s)$ of $\mathbf{w}$, first we observe that we can annihilate $\mathbf{f}_2(x_s)$ on $k - \eta - 2$ values x_s, and since $\eta \geq k - \eta - 2$, we can annihilate $\mathbf{f}_1(x_s)$ there, as well, taking $\mathbf{f}_1(x) = \mathbf{f}_2(x)\mathbf{f}_3(x)$ for a suitable polynomial $\mathbf{f}_3(x)$. This argument gives $2(k-\eta-2)$ zero, pairwise consecutive, entries of $\mathbf{w}$.

On the remaining entries, where $\mathbf{f}_2(x_s)$ must be non-zero, we can still annihilate $\mathbf{f}_1(x_s) + a_s\mathbf{f}_2(x_s)$ on $\eta-(k-\eta-2)+1$ values x_s, because the polynomial $\mathbf{f}_3(x)$ has degree $\eta-(k-\eta-2)$. This argument gives exactly $2\eta-k+3$ further zero entries of $\mathbf{w}$, because now $\mathbf{f}_1(x_s)+b_s\mathbf{f}_2(x_s)$ must be non zero.

Therefore the maximal possible number of zeros of $\mathbf{w}$ is $2(k-\eta-2)+(2\eta-k+3) = k-1$, so $\delta \geq n - (k-1)$, thus reaching the Singleton bound.

On the other hand, in the case $\gcd(\mathbf{f}_1(x), \mathbf{f}_2(x)) \neq \mathbf{f}_2(x)$, we note that the maximal number of zeros of $\mathbf{w}$ is at most $\frac{n}{2} = k$ since $\mathbf{f}_1(x_s)+a_s\mathbf{f}_2(x_s) = 0$ implies that $\mathbf{f}_1(x_s)+b_s\mathbf{f}_2(x_s) \neq 0$, and vice versa. Thus, $\delta \geq n - k = k$ in this case. □

Example 1 Let $\mathsf{k} = \mathrm{GF}(101)$, choose a pair of polynomials $(u(x), v(x))$ with $\mathrm{GCD}(u(x), u'(x), v(x)) = 1$, for instance $(u(x), v(x)) = (x^{11} + 1, x^6 + 1)$, and consider the function

$$\Psi(x, y) = \frac{y + v(x)}{u(x)} = \frac{y + x^6 + 1}{x^{11} + 1}.$$

Choose five pairs (x_s, y_s) such that $x_r \neq x_l$ whenever $r \neq l$, such that $u(x_s) \neq 0$ for any index s, for instance (15, 45), (53, 48), (58, 10), (64, 13), (80, 2). Evaluating the functions

$\{1, x, x^2, \Psi(x, y), x\Psi(x, y)\}$ on the ten points $(15, \pm 45)$, $(53, \pm 48)$, $(80, \pm 2)$, $(58, \pm 10)$, $(64, \pm 13)$, one obtains a matrix

$$G := \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 15 & 15 & 53 & 53 & 80 & 80 & 58 & 58 & 64 & 64 \\ 23 & 23 & 82 & 82 & 37 & 37 & 31 & 31 & 56 & 56 \\ 73 & 41 & 35 & 92 & 1 & 45 & 99 & 71 & 48 & 21 \\ 85 & 9 & 37 & 28 & 80 & 65 & 86 & 78 & 42 & 31 \end{pmatrix}$$

which, by the above Corollary 3, is a generating matrix of a linear code $\mathcal{C}$ over GF(101), having minimal distance $\delta \geq 5$. Furthermore, since all the 5×5 minors of G can be checked to have full rank, the code $\mathcal{C}$ is [10, 5, 6] MDS code.

In order to give the equation of a hyperelliptic curve $\mathcal{H}$ realizing the above code as an algebraic geometric code, defined by $D = \mathrm{div}(u(x), v(x)) + 15\Omega$ (following the proof of Theorem 2) by evaluating the functions in $\mathcal{L}(D)$ on the above five points (x_s, y_s), we note that the genus g of $\mathcal{H}$ must be equal at least to the degree of $u(x)$. With g equal to the degree of $u(x)$, hence with the degree of $\mathcal{H}$ equal to 23, we need eight further points, because $\mathcal{H}$ passes through the five points (x_s, y_s) and through the eleven points (in the affine plane) of the support of $\mathrm{div}(u(x), v(x))$. Choose arbitrarily eight pairs (x_s, y_s) (now with $s = 6, \ldots, 13$) such that $u(x_s) \neq 0$ and $x_i \neq x_j$ for all $1 \leq i < j \leq 13$, for instance $(48, 80)$, $(58, 91)$, $(64, 88)$, $(89, 16)$, $(95, 33)$, $(53, 4)$, $(51, 85)$, $(71, 35)$.

With this choice, the curve $\mathcal{H}$ defined by the equation

$$y^2 = v^2(x) - c(x)u(x),$$

where $c(x)$ is the polynomial such that

$$c(x_s) = \frac{v(x_s)^2 - y_s^2}{u(x_s)},$$

for $s = 1, \ldots, 13$, has degree 23, passes through the 13 points (x_s, y_s) and the eleven points (in the affine plane) of the support of $\mathrm{div}(u(x), v(x))$, thus realizing the [10, 5, 6] code as the algebraic geometric code defined by $\mathcal{L}(D)$ and the ten points $(x_s, \pm y_s)$, for $s = 1, \ldots, 5$.

Funding Open access funding provided by Università degli Studi di Palermo within the CRUI-CARE Agreement.

References

1. de Boer, M.A.: The generalized Hamming weights of some hyperelliptic codes. J. Pure Appl. Algebra **123**, 153–163 (1998)
2. von Brill, A., Noether, M.: Über die algebraischen Functionen und ihre Anwendung in der Geometrie. Math. Annalen **7**, 269–316 (1874)
3. Cantor, D.G.: Computing in the Jacobian of a Hyperelliptic Curve. Math. Comp. **48**, 95–101 (1987)

4. Falcone, G., Figula, Á., Hannusch, C.: On the generating matrices of Goppa codes over hyperelliptic curves. J. Ramanujan Math. Soc. **37**(3), 273–279 (2022)
5. Garzón, A.(CL-VAL), Navarro, H.(CL-VAL): Bases of Riemann-Roch spaces from Kummer extensions and algebraic geometry codes. (English summary) Finite Fields Appl. 80, Paper No. 102025, 19 pp. (2022)
6. Goppa, V.D.: Algebraic-geometric codes. Izv. Akad. Nauk SSSR Ser. Mat. **46**, 762–781 (1982). (**(in Russian)**)
7. Hess, F.: Computing Riemann-Roch Spaces in Algebraic Function Fields and Related Topics. J. Symbolic Comp. **33**, 425–445 (2002)
8. Huang, M., Ierardi, D.: Efficient algorithms for the Riemann-Roch problem and for addition in the Jacobian of a curve. J. Symbolic Comp. **18**, 519–539 (1994)
9. Janwa, H., Moreno, O.: McEliece public key cryptosystems using algebraic-geometric codes. Designs, Codes and Cryptography **8**, 293–307 (1996)
10. Koblitz, N.: Hyperelliptic Cryptosystems. J. Cryptology **1**, 139–150 (1989)
11. Kuroki, J., Gonda, M., Matsuo, K., Chao, J., Tsujii, S.: Fast Genus Three Hyperelliptic Curve Cryptosystems, In The 2002 Symposium on Cryptography and Information Security, Japan - SCIS 2002, (2002)
12. Lange, T.: Formulae for Arithmetic on Genus 2 Hyperelliptic Curves. AAECC **15**, 295–328 (2005)
13. Le Brigand, D.: Decoding of codes on hyperelliptic curves. In: Cohen, G., Charpin, P. (eds.) EUROCODE '90, EUROCODE 1990, LNCS, vol. 514, pp. 126–134. Springer, Berlin, Heidelberg (1990)
14. Le Gluher, A., Spaenlehauer, P.-J.: A fast randomized geometric algorithm for computing Riemann-Roch spaces. Math. Comp. **89**, 2399–2433 (2020)
15. Lockhart, P.: On the discriminant of a hyperelliptic curve. Trans. Amer. Math. Soc. **342**, 729–752 (1994)
16. McEliece, R.J.: A public-key cryptosystem based on algebraic coding theory. *DSN Progress Report* 42–44, *Jet Propulsion Laboratory*, Pasadena (1978)
17. Niehage, A.: Nonbinary Quantum Goppa Codes Exceeding the Quantum Gilbert-Varshamov Bound. Quantum Inf. Process **6**, 143–158 (2007)
18. Pelzl, J., Wollinger, T., Guajardo, J., Paar, C.: Hyperelliptic curves cryptosystems: closing the performance gap to elliptic curves, In: C.D. Walter, Ç.K. Koç, C. Paar (Eds.) Cryptographic Hardware and Embedded Systems - CHES 2003, CHES 2003, LNCS, vol. 2779., Springer, Berlin, Heidelberg, pp. 351–365 (2003)
19. Stichtenoth, H.: Algebraic function fields and codes. Springer, Berlin, Heidelberg (2009)
20. Sutherland, A.V.: Fast Jacobian arithmetic for hyperelliptic curves of genus 3, Thirteenth Algorithmic Number Theory Symposium (ANTS XIII). Open Book Series **2**, 425–442 (2019)