Indian J Pure Appl Math (2023) 54:1239–1248
https://doi.org/10.1007/s13226-022-00337-3

ORIGINAL RESEARCH

An Approach to the Bases of Riemann-Roch Spaces

Chuangqiang Hu · Shudi Yang

Received: 27 June 2020 / Accepted: 28 September 2022 / Published online: 5 October 2022

Abstract For applications in algebraic geometric codes, it is extremely useful to give an explicit description of the bases of Riemann-Roch spaces associated to divisors on function fields over finite fields. We demonstrate a general approach to construct such a monomial basis for the related Riemann-Roch space. More precisely we present a criterion for finding an explicit basis for the Riemann-Roch space of a three-point divisor. Furthermore, we improve an upper bound for the genus of the related function field. Some examples are also given to illustrate our general approach.

Keywords Riemann-Roch space · Function field · AG code

Mathematics Subject Classification 11R58 · 14H55 · 94B27

1 Introduction

In the early eighties Goppa [12] constructed error-correcting linear codes using algebraic curves over finite fields. Nowadays these codes are called algebraic geometric codes, AG codes for short. We refer the reader to [26] for more information on AG codes.

With the discovery of Goppa, it becomes important to construct AG codes explicitly. A related problem emerges concerning the determination of bases for Riemann-Roch spaces. It is well known that the dimension of AG codes depends essentially on the dimension of the given Riemann-Roch space. From the Riemann-Roch space, we can determine the corresponding Weierstrass semigroups and pure gaps, which can be extremely useful in improving the parameters of AG codes. This again gives information to find an effective decoding algorithm for practical use of the code.

How to construct a basis for a given Riemann-Roch space? In general, it is indeed a hard problem. However, there are some contributions on maximal curves, such as Hermitian, Suzuki, and Ree curves, in literature. For the Hermitian function field, Stichtenoth [26] presented a basis for the Riemann-Roch space associated with the place located at infinity, and Park [23] established a basis for the Riemann-Roch space on two rational

Communicated by Sudhir R. Ghorpade.

This work is partly supported by the National Natural Science Foundation of China under Grants 12071247 and 12101616.

C. Hu
Yanqi Lake Beijing Institute of Mathematical Sciences and Applications, Peking 101408, P R China
E-mail: huchq@bimsa.cn

S. Yang (✉)
School of Mathematical Sciences, Qufu Normal University, Shandong 273165, P R China
E-mail: yangshudi@qfnu.edu.cn

places. Maharaj, Matthews and Pirsic [20] determined explicit bases for large classes of Riemann-Roch spaces of the Hermitian function field and considered their applications to AG codes and low-discrepancy sequences. The Suzuki function field, whose automorphism group is a kind of Suzuki group, was investigated in [14]. The corresponding AG codes were studied by Hansen and Stichtenoth [13] for one-point codes and Matthews [21] for two-point codes, and the bases for the Riemann-Roch spaces were also indicated. Pedersen [24] proposed a function field related to the Ree group and stated the basis for the Riemann-Roch space associated with the place at infinity. Giulietti and Korchmáros [10] constructed the so called GK maximal curve and determined a basis for the linear space on the infinite place. Fanali and Giulietti [9] considered one-point AG codes on the GK maximal curves by utilizing the basis of the Riemann-Roch space. Two-point AG codes on the GK maximal curves were investigated by Castellanos and Tizziotti [7]. A generalization of the GK curve, called GGS curve, was studied by Garcia, Güneri and Stichtenoth [11]. In [25], Skabelund constructed a new maximal curve as a cyclic cover of the Suzuki curve and stated the basis of the Riemann-Roch space with one place. Beelen et al. [5] explicitly characterized the structure of the Weierstrass semigroup at any point of the Skabelund curve. In 2016, Hu and Zhao [16] initiated a different method of finding a basis of the Riemann-Roch space from generalized Hermitian curves and they used the basis to study the corresponding multi-point AG codes. This method was then generalized to the BBGS curves [17], the Kummer extensions [18] and the GGS curves [19]. Yang and Hu [28,29] then utilized the theory in [18] to investigate Weierstrass semigroups and pure gaps from Kummer extensions. In this paper, we demonstrate a more general approach which is efficient in finding a basis for each Riemann-Roch space. Voss and Høholdt [27] gave a basis of the Riemann-Roch space on a tower of Artin-Schreier extensions. We can improve this result to a more natural one by applying our approach, see [30].

Let us introduce the main result here. Suppose that $F/\mathbb{F}_q$ is a function field with genus g, where $\mathbb{F}_q$ is a finite field with cardinality q. Let P be a rational place, Q_1, Q_2 be two distinct effective divisors. A crucial criterion is presented below to provide a way of fining an explicit monomial basis of the Riemann-Roch space with a divisor $G = rP + sQ_1 + tQ_2$, where r, s and t are integers.

Theorem 1.1 *Suppose that the divisors of $y_1, y_2 \in F/\mathbb{F}_q$ are given by*

$$\begin{aligned}\operatorname{div}(y_1) &= P + b_{11}Q_1 + b_{12}Q_2,\\ \operatorname{div}(y_2) &= b_{21}Q_1 + b_{22}Q_2,\end{aligned}$$

where the coefficients b_{ij} are all integers and $\gcd(b_{11}, b_{21}) = 1$, $\gcd(b_{12}, b_{22}) = 1$. *Denote*

$$g_0 := \frac{1}{2}\big(|b_{11}b_{22} - b_{12}b_{21}| \deg(Q_1)\deg(Q_2) - \deg(Q_1) - \deg(Q_2) + 1\big). \tag{1.1}$$

Then

$$g \leqslant g_0.$$

Moreover, if $g = g_0$, then the elements $y_1^i y_2^j$ with $(i, j) \in \Omega_{r,s,t}$ form a basis of the Riemann-Roch space $\mathcal{L}(rP + sQ_1 + tQ_2)$, where $\Omega_{r,s,t}$ denotes the lattice point set

$$\Omega_{r,s,t} = \left\{ (i, j) \in \mathbb{Z}^2 \;\middle|\; \begin{aligned} &-r \leqslant i,\\ &-s \leqslant b_{11}i + b_{21}j < -s + b_{21},\\ &-t \leqslant b_{12}i + b_{22}j \end{aligned} \right\}. \tag{1.2}$$

The paper is organized as follows. In Section 2, we briefly introduce some arithmetic properties of the function fields and the Riemann-Roch space $\mathcal{L}(G)$ with respect to a divisor G. It is shown that the dimension of a Riemann-Roch space is closely related to the dimension of the corresponding AG code. Section 3 is devoted to giving a general approach of how to construct a basis of the Riemann-Roch space $\mathcal{L}(G)$. A crucial criterion is developed for the monomial basis of the Riemann-Roch space with a three-point divisor. Finally, in Section 4 we provide some examples.

2 Notations

Let q be a power of a prime p and let $\mathbb{F}_q$ be a finite field of cardinality q. We denote by $F/\mathbb{F}_q$ a function field over $\mathbb{F}_q$. A place P of the function field $F/\mathbb{F}_q$ is the maximal ideal of some valuation ring of $F/\mathbb{F}_q$. The set of places of $F/\mathbb{F}_q$ is denoted by $\mathbb{P}_F$. A place P in $\mathbb{P}_F$ of degree one is also called a rational place of $F/\mathbb{F}_q$. The free abelian group generated by the places of $F/\mathbb{F}_q$ is denoted by $\mathcal{D}_F$, whose element is called a divisor. Hence a divisor D is expressed as $D = \sum_{P\in\mathbb{P}_F} n_P P$ with $n_P \in \mathbb{Z}$, almost all $n_P = 0$. The degree of D is defined as $\deg(D) = \sum_{P\in\mathbb{P}_F} n_P$. A divisor $D \geqslant 0$ is called effective (or positive). For a function $f \in F/\mathbb{F}_q$, the symbol $v_P(f)$ represents the valuation of f at a rational place P. The principal divisor of f will be denoted by $\mathrm{div}(f)$. The Riemann-Roch vector space with respect to D is defined by

$$\mathcal{L}(D) = \left\{ f \in F/\mathbb{F}_q \,\middle|\, \mathrm{div}(f) + D \geqslant 0 \right\} \cup \{0\}.$$

Let $\ell(D)$ be the dimension of $\mathcal{L}(D)$. From the famous Riemann-Roch Theorem, we know that

$$\ell(D) - \ell(W - D) = 1 - g + \deg(D),$$

where W is a canonical divisor and g is the genus of the associated curve.

We present necessary definitions and auxiliary results concerning AG codes and their parameters. Let G be a divisor of $F/\mathbb{F}_q$ and let $D = Q_1 + \cdots + Q_n$ be another divisor of $F/\mathbb{F}_q$ such that $Q_i \neq Q_j$ for $i \neq j$ and $\mathrm{supp}(G) \cap \mathrm{supp}(D) = \varnothing$. The AG code $C_{\mathcal{L}}(D, G)$ is constructed from the Riemann-Roch space $\mathcal{L}(G)$, namely,

$$C_{\mathcal{L}}(D, G) := \left\{ (f(Q_1), \cdots, f(Q_n)) \,\middle|\, f \in \mathcal{L}(G) \right\} \subseteq \mathbb{F}_q^n.$$

Let n, k and d be the length, dimension and minimum distance of $C_{\mathcal{L}}(D, G)$, respectively. Then $k = \ell(G) - \ell(G - D)$ and $d \geqslant n - \deg(G)$. They are restricted by the Singleton bound: $k + d \leqslant n + 1$. By the Riemann-Roch Theorem we can further estimate the parameters. In particular, if $2g - 2 < \deg(G) < n$ then $k = \deg(G) - g + 1$. Thus the connection between the dimensions of a Riemann-Roch space and its corresponding AG code is clear. With the declaration of the basis, it will be possible to find an formula for the order bound on the minimum distance of an AG code, see [4,22] for example.

More details on AG codes and their parameters can be found in [1–3,6,15,26] and the references therein.

3 A general approach

In this section we introduce a general approach for computing bases for a family of Riemann-Roch spaces. Let $F/\mathbb{F}_q$ be a function field. Let P be a rational place, and let $Q_1, \cdots, Q_n$ be some effective divisors. We choose n distinct elements $x_1, x_2, \cdots, x_n$ of $F/\mathbb{F}_q$ with divisors

$$\begin{aligned}
\mathrm{div}(x_1) &= a_{10}P + a_{11}Q_1 + a_{12}Q_2 + \cdots + a_{1n}Q_n,\\
\mathrm{div}(x_2) &= a_{20}P + a_{21}Q_1 + a_{22}Q_2 + \cdots + a_{2n}Q_n,\\
&\cdots,\\
\mathrm{div}(x_n) &= a_{n0}P + a_{n1}Q_1 + a_{n2}Q_2 + \cdots + a_{nn}Q_n,
\end{aligned}$$

where the coefficients a_{ik} are all integers for $1 \leqslant i \leqslant n$ and $0 \leqslant k \leqslant n$. If we assume that $\gcd(a_{10}, a_{20}, \cdots, a_{n0}) = 1$, then we can choose $y_i = \prod_{j=1}^{n} x_j^{d_{ij}}$ for some integers d_{ij}, $1 \leqslant i, j \leqslant n$, such that their divisors are given by linear transformation that

$$\begin{aligned}
\mathrm{div}(y_1) &= P + b_{11}Q_1 + b_{12}Q_2 + \cdots + b_{1n}Q_n,\\
\mathrm{div}(y_2) &= b_{21}Q_1 + b_{22}Q_2 + \cdots + b_{2n}Q_n,\\
&\cdots,\\
\mathrm{div}(y_n) &= b_{n1}Q_1 + b_{n2}Q_2 + \cdots + b_{nn}Q_n,
\end{aligned}$$

where the coefficients b_{ij} are all integers. Let $\Gamma = (\gamma_0, \gamma_1, \cdots, \gamma_n) \in \mathbb{Z}^{n+1}$, we define a divisor G_Γ on $F/\mathbb{F}_q$ given by

$$G_\Gamma = \gamma_0 P + \gamma_1 Q_1 + \gamma_2 Q_2 + \cdots + \gamma_n Q_n.$$

Our aim is to construct a basis for the Riemann-Roch space $\mathcal{L}(G_\Gamma)$ associated to G_Γ. Recall that the Riemann-Roch space $\mathcal{L}(G_\Gamma)$ is defined as

$$\mathcal{L}(G_\Gamma) = \left\{ f \in F/\mathbb{F}_q \,\middle|\, \operatorname{div}(f) \geqslant -G_\Gamma \right\} \cup \{0\}.$$

Set $u_i \in \mathbb{Z}$ for $i = 1, \cdots, n$. From the definition, it follows that

$$y_1^{u_1} y_2^{u_2} \cdots y_n^{u_n} \in \mathcal{L}(G_\Gamma)$$

if and only if

$$u_1 \geqslant -\gamma_0 \quad \text{and} \quad \sum_{i=1}^{n} u_i b_{ij} \geqslant -\gamma_j \text{ for } 1 \leqslant j \leqslant n. \tag{3.1}$$

Note that the valuation of $y_1^{u_1} y_2^{u_2} \cdots y_n^{u_n}$ at P is

$$v_P(y_1^{u_1} y_2^{u_2} \cdots y_n^{u_n}) = u_1.$$

So the elements $y_1^{u_1} y_2^{u_2} \cdots y_n^{u_n}$ will be linearly independent provided that their indexes u_1 are different from each other. Denote by C_Γ the set of n-tuples $(u_1, u_2, \cdots, u_n)$ verifying (3.1). Define a projection from the set C_Γ to $\mathbb{Z}$ by

$$\mathrm{Pr}_1 C_\Gamma = \left\{ u_1 \in \mathbb{Z} \,\middle|\, (u_1, u_2, \cdots, u_n) \in C_\Gamma \right\}.$$

Since we only care about the value of u_1, we would like to give a canonical choice of $u_2, \cdots, u_n$ depending on u_1. Precisely, we need to choose a subset in C_Γ, denoted by Ω_Γ, to insure that

(1) all the elements in Ω_Γ have distinct component u_1, and
(2) $\mathrm{Pr}_1\, \Omega_\Gamma = \mathrm{Pr}_1\, C_\Gamma$.

The following is one of the available approaches to determine the subset Ω_Γ. Define the following integer linear program (ILP for short) for a fixed integer u_1:

$$\text{(ILP)} \begin{cases} \max & \sum_{i=2}^{n} u_i b_{in}, \\ \text{s.t.} & \sum_{i=1}^{n} u_i b_{ij} \geqslant -\gamma_j \text{ where } u_i \in \mathbb{Z},\, 1 \leqslant i \leqslant n \text{ and } 1 \leqslant j \leqslant n-1. \end{cases}$$

Denote one of the optimal solutions by $(\tilde{u}_2, \tilde{u}_3, \cdots, \tilde{u}_n) := (u_2(u_1), u_3(u_1), \cdots, u_n(u_1))$. Put $\tilde{u}_1 = u_1$. Then the lattice point set Ω_Γ is expressed as

$$\Omega_\Gamma := \left\{ (\tilde{u}_1, \tilde{u}_2, \cdots, \tilde{u}_n) \in \mathbb{Z}^n \,\middle|\, \tilde{u}_1 \geqslant -\gamma_0,\ \sum_{i=1}^{n} \tilde{u}_i b_{in} \geqslant -\gamma_n \right\}.$$

Taking into account (3.1) and noting the fact that u_1 determines the integers $\tilde{u}_2, \cdots, \tilde{u}_n$, one can easily verify that Ω_Γ meets the requirements (1) and (2) listed above.

The following theorem plays an essential role in constructing bases.

Theorem 3.1 *With notation as above, we define a subset of $F/\mathbb{F}_q$*

$$B_\Gamma := \left\{ y_1^{\tilde{u}_1} y_2^{\tilde{u}_2} \cdots y_n^{\tilde{u}_n} \,\middle|\, (\tilde{u}_1, \tilde{u}_2, \cdots, \tilde{u}_n) \in \Omega_\Gamma \right\}.$$

Then we have the following assertions.

(1) *The elements of B_Γ are all contained in the Riemann-Roch space $\mathcal{L}(G_\Gamma)$, and they are linearly independent over $\mathbb{F}_q$.*
(2) *If there exists a number δ depending on $\gamma_1, \gamma_2, \cdots, \gamma_n$, such that the equality*

$$\#\Omega_\Gamma = 1 - g + \deg(G_\Gamma)$$

holds for each $\gamma_0 \geqslant \delta$, then the elements in B_Γ form a basis of $\mathcal{L}(G_\Gamma)$.

Proof (1) It is trivial from the definition that $\Omega_\Gamma \subseteq C_\Gamma$. This implies that $B_\Gamma \subseteq \mathcal{L}(G_\Gamma)$. Note that the valuation of $y_1^{\tilde{u}_1} y_2^{\tilde{u}_2} \cdots y_n^{\tilde{u}_n}$ with respect to P is equal to $\tilde{u}_1$. So all elements in B_Γ have distinct valuations at P. Therefore, these elements are linearly independent of each other.

(2) By the Riemann-Roch Theorem, we find that there exists a number η such that for each $\gamma_0 \geqslant \eta$,

$$\ell(G_\Gamma) = 1 - g + \deg(G_\Gamma).$$

Put $\overline{\gamma}_0 := \max\left\{\gamma_0, \delta\right\}$, $\overline{\Gamma} := (\overline{\gamma}_0, \gamma_1, \cdots, \gamma_n)$ and $G_{\overline{\Gamma}} = \overline{\gamma}_0 P + \gamma_1 Q_1 + \cdots + \gamma_n Q_n$. By assumption, we obtain

$$\# B_{\overline{\Gamma}} = \# \Omega_{\overline{\Gamma}} = \ell(G_{\overline{\Gamma}}).$$

This shows that $\mathcal{L}(G_{\overline{\Gamma}})$ is linearly generated by $B_{\overline{\Gamma}}$. Moreover, since $\mathcal{L}(G_\Gamma)$ is a subspace of $\mathcal{L}(G_{\overline{\Gamma}})$, we get

$$\begin{aligned}\mathcal{L}(G_\Gamma) &= \left\{ f \in \mathcal{L}(G_{\overline{\Gamma}}) \,\middle|\, v_P(f) \geqslant -\gamma_0 \right\} \\ &= \operatorname{span}\left\{ y_1^{\tilde{u}_1} y_2^{\tilde{u}_2} \cdots y_n^{\tilde{u}_n} \,\middle|\, (\tilde{u}_1, \tilde{u}_2, \cdots, \tilde{u}_n) \in \Omega_{\overline{\Gamma}} \text{ and } \tilde{u}_1 \geqslant -\gamma_0 \right\} \\ &= \operatorname{span}\left\{ B_\Gamma \right\},\end{aligned}$$

which completes the proof. □

Here we propose a concrete procedure for the case $n = 2$. In this case, it is easy to solve the ILP, and to calculate the exact number of lattice points in the set Ω_Γ. Using the previous notation we have

$$G := G_\Gamma = rP + sQ_1 + tQ_2,$$

$$\operatorname{div}(y_1) = P + b_{11} Q_1 + b_{12} Q_2, \tag{3.2}$$

$$\operatorname{div}(y_2) = b_{21} Q_1 + b_{22} Q_2. \tag{3.3}$$

For convenience, we assume that $b_{22} < 0$. Since $\deg(\operatorname{div}(y_2)) = 0$, we get $b_{21} > 0$. The related ILP is now written as

$$\begin{cases} \max & u_2 b_{22}, \\ \text{s.t.} & u_1 b_{11} + u_2 b_{21} \geqslant -s, \ \text{where } u_1, u_2 \in \mathbb{Z}. \end{cases}$$

One can prove that the optimal value of u_2 is $\left\lceil \frac{-s - u_1 b_{11}}{b_{21}} \right\rceil$, or equivalently, the unique integer u_2 such that $-s \leqslant u_1 b_{11} + u_2 b_{21} < -s + b_{21}$.

Now let us prove our main result in the following.

Proof of Theorem 1.1 Recall that the set $\Omega_{r,s,t}$ is defined in (1.2). According to Theorem 3.1, we only need to show that there exists a number δ depending on s and t, such that for each $r \geqslant \delta$,

$$\# \Omega_{r,s,t} = 1 - g_0 + \deg(G),$$

where $G = rP + sQ_1 + tQ_2$. By Equations (3.2) and (3.3), we have

$$\begin{aligned} b_{11} \deg(Q_1) + b_{12} \deg(Q_2) &= -1, \\ b_{21} \deg(Q_1) + b_{22} \deg(Q_2) &= 0, \end{aligned}$$

which implies that

$$\begin{aligned} \deg(Q_1) = e &:= \frac{-b_{22}}{b_{11} b_{22} - b_{12} b_{21}}, \\ \deg(Q_2) = h &:= \frac{b_{21}}{b_{11} b_{22} - b_{12} b_{21}}. \end{aligned}$$

Without loss of generality, we suppose that $b_{22} < 0$, $b_{21} > 0$ and $b_{11} b_{22} - b_{12} b_{21} > 0$. Let $\delta := -b_{22} h$. The proof is completed step by step.

Step 1: If $r = \delta$, $s = 0$ and $t \geqslant 0$, then we proceed as follows to determine the number of lattice points in the set $\Omega_{\delta,0,t}$. Put $O = (0, 0)$, $A = (b_{22}h, b_{11}e)$ and $B = (b_{22}h, -b_{12}h)$. Denote by S the area of the triangle $\triangle OAB$, and by M the number of lattice points on the boundary of $\triangle OAB$. It is easy to see that $S = -b_{22}h/2$ and $M = 1 + e + h$. Note that the edge AB has no lattice point except the vertexes A and B. Applying Pick's theorem, the number I of lattice points within $\triangle OAB$ verifies

$$I = S - M/2 + 1.$$

Since $\Omega_{\delta,0,t}$ contains exactly the lattice points in the triangle $\triangle OAB$ except the vertex B, we see that

$$\#\Omega_{\delta,0,t} = I + M - 1 = S + M/2 = (-b_{22}h + e + h + 1)/2. \tag{3.4}$$

Step 2: If $r \geqslant \delta$, $s = 0$ and $t = 0$, then we consider the lattice points in the difference set $\Omega_{r,0,0} \setminus \Omega_{\delta,0,0}$, where

$$\begin{aligned} \Omega_{r,0,0} \setminus \Omega_{\delta,0,0} = \Big\{ (i, j) \in \mathbb{Z}^2 \Big| & -r \leqslant i < -\delta, \\ & 0 \leqslant b_{11}i + b_{21}j < b_{21}, \\ & 0 \leqslant b_{12}i + b_{22}j \Big\}. \end{aligned}$$

The second condition implies that j is uniquely determined by i, namely,

$$j = \left\lceil -\frac{b_{11}}{b_{21}} i \right\rceil \leqslant 1 - \frac{b_{11}}{b_{21}} i.$$

We observe from the first condition that $i < -\delta$, and consequently

$$\begin{aligned} b_{12}i + b_{22}j &\geqslant b_{12}i + b_{22} - \frac{b_{11}b_{22}}{b_{21}} i \\ &> \frac{b_{12}b_{21} - b_{11}b_{22}}{b_{21}} (-\delta) + b_{22} = 0. \end{aligned}$$

This yields that the third inequality always holds. So the number of lattice points in $\Omega_{r,0,0} \setminus \Omega_{\delta,0,0}$ only depends on the first condition, that is,

$$\#(\Omega_{r,0,0} \setminus \Omega_{\delta,0,0}) = r - \delta. \tag{3.5}$$

Hence, it follows from (3.4) and (3.5) that

$$\#\Omega_{r,0,0} = \#\Omega_{\delta,0,0} + \#(\Omega_{r,0,0} \setminus \Omega_{\delta,0,0}) = (b_{22}h + e + h + 1)/2 + r. \tag{3.6}$$

Step 3: If $r \geqslant \delta$, $s = 0$ and $t \geqslant 0$, then we consider the lattice points in the difference set $\Omega_{r,0,t} \setminus \Omega_{r,0,0}$, where

$$\begin{aligned} \Omega_{r,0,t} \setminus \Omega_{r,0,0} = \Big\{ (i, j) \in \mathbb{Z}^2 \Big| & -r \leqslant i, \\ & 0 \leqslant b_{11}i + b_{21}j < b_{21}, \\ & -t \leqslant b_{12}i + b_{22}j < 0 \Big\}. \end{aligned}$$

For an integer τ, we denote

$$L_\tau := \Big\{ (i, j) \in \mathbb{Z}^2 \Big| 0 \leqslant b_{11}i + b_{21}j < b_{21},\ b_{12}i + b_{22}j = -\tau \Big\}.$$

Then the difference set $\Omega_{r,0,t} \setminus \Omega_{r,0,0}$ is a union of some L_τ, that is

$$\Omega_{r,0,t} \setminus \Omega_{r,0,0} = \bigcup_{\tau=1}^{t} L_\tau. \tag{3.7}$$

It is clear that the number of lattice points in the set L_τ is

$$\#L_\tau = h. \tag{3.8}$$

So we have from (3.6), (3.7) and (3.8) that

$$\#\Omega_{r,0,t} = \#\Omega_{r,0,0} + \#(\Omega_{r,0,t} \setminus \Omega_{r,0,0}) = (b_{22}h + e + h + 1)/2 + r + ht.$$

Step 4: If $s = 0$ and $t < 0$, then we denote $t' := t + (b_{11}b_{22} - b_{12}b_{21})k$, where the integer k is chosen such that $t' \geqslant 0$. Let $i' := i + b_{21}k$, $j' := j - b_{11}k$ and $r' := r - b_{21}k$. Then we obtain a new lattice point set $\Omega_{r',0,t'}$ from $\Omega_{r,0,t}$, where

$$\begin{aligned}\Omega_{r',0,t'} = \Big\{ (i', j') \in \mathbb{Z}^2 \,\Big|\, & -r' \leqslant i', \\ & 0 \leqslant b_{11}i' + b_{21}j' < b_{21}, \\ & -t' \leqslant b_{12}i' + b_{22}j' \Big\}.\end{aligned}$$

Since the two sets $\Omega_{r',0,t'}$ and $\Omega_{r,0,t}$ are equivalent to each other, we have

$$\begin{aligned}\#\Omega_{r,0,t} &= \#\Omega_{r',0,t'} \\ &= (b_{22}h + e + h + 1)/2 + r' + ht' \\ &= (b_{22}h + e + h + 1)/2 + r + ht.\end{aligned}$$

Step 5: If $s \neq 0$, then we proceed as follows.

Since b_{11} and b_{21} are coprime integers, there exist two integers i_0, j_0, such that $b_{11}i_0 + b_{21}j_0 = 1$. Let $\bar{i} := i + i_0 s$, $\bar{j} := j + j_0 s$, $\bar{r} := r - i_0 s$, $\bar{t} := t - (b_{12}i_0 + b_{22}j_0)s$. Then the lattice point set $\Omega_{r,s,t}$ becomes

$$\begin{aligned}\overline{\Omega}_{\bar{r},0,\bar{t}} = \Big\{ (\bar{i}, \bar{j}) \in \mathbb{Z}^2 \,\Big|\, & -\bar{r} \leqslant \bar{i}, \\ & 0 \leqslant b_{11}\bar{i} + b_{21}\bar{j} < b_{21}, \\ & -\bar{t} \leqslant b_{12}\bar{i} + b_{22}\bar{j} \Big\}.\end{aligned}$$

Hence, we get

$$\begin{aligned}\#\Omega_{r,s,t} &= \#\overline{\Omega}_{\bar{r},0,\bar{t}} \\ &= (b_{22}h + e + h + 1)/2 + \bar{r} + h\bar{t} \\ &= (b_{22}h + e + h + 1)/2 + r + es + ht.\end{aligned}$$

Note that $\deg(G) = r + es + ht$. By taking $g_0 := (-b_{22}h - e - h + 1)/2$, we have

$$\#\Omega_{r,s,t} = 1 - g_0 + \deg(G).$$

It follows from the famous Riemann-Roch Theorem that

$$\ell(G) \leqslant 1 - g + \deg(G).$$

Since $\#\Omega_{r,s,t} \leqslant \ell(G)$, we have $g \leqslant g_0$. If moreover $g = g_0$, then the desired conclusion follows from Theorem 3.1. □

From Theorem 1.1, we can derive a new form of the basis for our Riemann-Roch space $\mathcal{L}(rP + sQ_1 + tQ_2)$.

Corollary 3.2 *With the above notation, we suppose that the divisors of $x_1, x_2 \in F/\mathbb{F}_q$ satisfy*

$$\begin{aligned}\operatorname{div}(x_1) &= a_{10}P + a_{11}Q_1 + a_{12}Q_2, \\ \operatorname{div}(x_2) &= a_{20}P + a_{21}Q_1 + a_{22}Q_2,\end{aligned}$$

where $\gcd(a_{1j}, a_{2j}) = 1$ *for* $j = 0, 1, 2$. *Then*

$$g \leqslant g_0 := \frac{1}{2}\left(|a_{11}a_{22} - a_{12}a_{21}| \deg(Q_1)\deg(Q_2) - \deg(Q_1) - \deg(Q_2) + 1\right).$$

Moreover, if $g = g_0$*, then the elements* $x_1^i x_2^j$ *with* $(i, j) \in \widetilde{\Omega}_{r,s,t}$ *form a basis of the Riemann-Roch space* $\mathcal{L}(rP + sQ_1 + tQ_2)$*, where* $\widetilde{\Omega}_{r,s,t}$ *denotes the lattice point set*

$$\widetilde{\Omega}_{r,s,t} = \Big\{ (i, j) \in \mathbb{Z}^2 \,\Big|\, -r \leqslant a_{10}i + a_{20}j, \\ -s \leqslant a_{11}i + a_{21}j < -s + (a_{10}a_{21} - a_{11}a_{20}), \\ -t \leqslant a_{12}i + a_{22}j \Big\}.$$

4 Examples

We now illustrate how the general approach can be used to compute the bases of Riemann-Roch spaces on certain function fields. In the following we take the Hermitian function field and the special Kummer extension as examples. Also note that the GGS curve is discussed in [19].

Example 4.1 The first example we give is the Hermitian function field H over $\mathbb{F}_{q^2}$. This function field can be defined by

$$H = \mathbb{F}_{q^2}(x, y) \text{ with } x^q + x = y^{q+1}.$$

The genus of H is $g = q(q-1)/2$. For each $\beta \in \mathbb{F}_{q^2}$ there are q elements $\alpha_{1\beta}, \cdots, \alpha_{q\beta} \in \mathbb{F}_{q^2}$ such that $\alpha_{i\beta}^q + \alpha_{i\beta} = \beta^{q+1}$. Let $\beta = 0$ and simplify α_{i0} as α_i. Denote by P_i the place of degree one located at $(\alpha_i, 0)$. The place located at infinity is denoted by P_∞. Consider $G := rP_\infty + sP_1 + tQ$, where Q is a divisor defined by $Q = P_2 + \cdots + P_q$. Elementary computation shows that

$$\operatorname{div}(x - \alpha_i) = (q+1)P_i - (q+1)P_\infty, \text{ for } 1 \leqslant i \leqslant q, \\ \operatorname{div}(y) = P_1 - qP_\infty + Q.$$

Let $y_1 = y/(x - \alpha_1)$ and $y_2 = (x - \alpha_1)^{q+1} \prod_{i=2}^{q}(x - \alpha_i)/y^{2(q+1)}$. It is checked that

$$\operatorname{div}(y_1) = P_\infty - qP_1 + Q, \\ \operatorname{div}(y_2) = (q^2 - 1)P_1 - (q+1)Q.$$

Substitution of $b_{11} = -q$, $b_{12} = 1$, $b_{21} = q^2 - 1$, $b_{22} = -q - 1$ in (1.1) yields that

$$g_0 = \frac{1}{2}\big(|q(q+1) - (q^2 - 1)|(q-1) - 1 - (q-1) + 1\big) = \frac{q(q-1)}{2}.$$

Since $g = g_0$, we conclude from Theorem 1.1 that the elements $y_1^i y_2^j$ with $(i, j) \in \Omega_{r,s,t}$ form a basis of the Riemann-Roch space $\mathcal{L}(rP_\infty + sP_1 + tQ)$, where $\Omega_{r,s,t}$ denotes the lattice point set

$$\Omega_{r,s,t} = \Big\{ (i, j) \in \mathbb{Z}^2 \,\Big|\, -r \leqslant i, \\ -s \leqslant -qi + (q^2 - 1)j < -s + (q^2 - 1), \\ -t \leqslant i - (q+1)j \Big\}.$$

We remark that the bases of the related Riemann-Roch space on Hermitian function field had been investigated in the literature. For instance,

(i) when $r \geqslant 0$ and $s = t = 0$, Stichtenoth established a basis of $\mathcal{L}(rP_\infty)$ in Lemma 6.4.4 of [26];
(ii) when $t = 0$, the authors in [8,23] indicated a basis of $\mathcal{L}(rP_\infty + sP_1)$, see Lemma 6.2 in [8].

Example 4.2 The second example we give is related to Kummer extensions, see [18] for more details. Consider a Kummer extension $F/\mathbb{F}_q(x)$ defined by $y^m = f(x)^\lambda = \prod_{i=1}^r (x-\alpha_i)^\lambda$, where $m > 1$, $\gcd(m, r\lambda) = 1$ and the α_i's are pairwise distinct elements in $\mathbb{F}_q$. This function field has genus $g = (r-1)(m-1)/2$. Let $P_1, \cdots, P_r$ be the places of this rational function field associated to the zeros of $x - \alpha_1, \cdots, x - \alpha_r$, respectively, and P_∞ be the unique place at infinity. Suppose that $(i, j_2, j_3, \cdots, j_r) \in \mathbb{Z}^r$, we write

$$E_{i,j_2,j_3,\cdots,j_r} := z^i (x-\alpha_2)^{j_2} (x-\alpha_3)^{j_3} \cdots (x-\alpha_r)^{j_r},$$

where $z = y^A f(x)^B$ with integers A and B satisfying $A\lambda + Bm = 1$. Let

$$G := \sum_{\mu=1}^r s_\mu P_\mu + t P_\infty$$

for integers s_μ and t. Denote a lattice point set

$$\begin{aligned}\Omega_{s_1,\cdots,s_r,t} := \Big\{ (i, j_2, j_3, \cdots, j_r) \in \mathbb{Z}^r \;\Big|\; & i + s_1 \geqslant 0, \\ & 0 \leqslant i + m j_\mu + s_\mu < m \text{ for } \mu = 2, \cdots, r, \\ & ri + m(j_2 + \cdots + j_r) \leqslant t \Big\}.\end{aligned}$$

From Lemma 2 of [18], we see that

$$\#\Omega_{s_1,\cdots,s_r,t} = 1 - g + s_1 + \cdots + s_r + t,$$

for $s_1 + \cdots + s_r + t \geqslant (2r-1)m$. According to Theorem 3.1, we conclude that the elements $E_{i,j_2,j_3,\cdots,j_r}$ with $(i, j_2, j_3, \cdots, j_r) \in \Omega_{s_1,\cdots,s_r,t}$ constitute a basis for the Riemann-Roch space $\mathcal{L}(G)$.

References

1. É. Barelli, P. Beelen, M. Datta, V. Neiger, J. Rosenkilde, Two-point codes for the generalized GK curve, *IEEE Transactions on Information Theory*, **64** (9) (2018), 6268–6276.
2. D. Bartoli, M. Montanucci, G. Zini, AG codes and AG quantum codes from the GGS curve, *Designs, Codes and Cryptography*, **86** (2018), 2315–2344.
3. D. Bartoli, L. Quoos, G. Zini, Algebraic geometric codes on many points from Kummer extensions, *Finite Fields and Their Applications*, **52** (2018), 319–335.
4. P. Beelen, The order bound for general algebraic geometric codes, *Finite Fields and Their Applications*, **13** (2007), 665–680.
5. P. Beelen, L. Landi, M. Montanucci, Weierstrass semigroups on the Skabelund maximal curve, *Finite Fields and Their Applications*, **72** (2021), 101811.
6. C. Carvalho, F. Torres, On Goppa codes and Weierstrass gaps at several points, *Designs Codes and Cryptography*, **35** (2005), 211–225.
7. A. S. Castellanos, G. C. Tizziotti, Two-point AG codes on the GK maximal curves, *IEEE Transactions on Information Theory*, **62** (2) (2016), 681–686.
8. I. M. Duursma, R. Kirov, Improved two-point codes on Hermitian curves, *IEEE Transactions on Information Theory*, **57** (7) (2011), 4469–4476.
9. S. Fanali, M. Giulietti, One-point AG codes on the GK maximal curves, *IEEE Transactions on Information Theory*, **56** (1) (2010), 202–210.
10. M. Giulietti, G.Korchmáros, A new family of maximal curves over a finite field, *Mathematische Annalen*, **343** (2009), 229–245.
11. A. Garcia, C. Güneri, H. Stichtenoth, A generalization of the Giulietti-Korchmaros maximal curve, *Advances in Geometry*, **10** (2010), 427–434.
12. V. D. Goppa, Algebraic-geometric codes (in Russian). *Izv. Akad. Nauk SSSR, Ser. Mat.*, **46** (4) (1982), 762–781.
13. J. P. Hansen, H. Stichtenoth, Group codes on certain algebraic curves with many rational points, *Appl. Alg. Engrg. Comm. Comput.*, **1** (1) (1990), 67–77.
14. H. W. Henn, Funktionenkörper mit grosser automorphismengruppe (in German), *J. Reine Angew. Math.*, **302** (1978), 96–115.
15. M. Homma, S. J. Kim, The two-point codes on a Hermitian curve with the designed minimum distance, *Designs, Codes and Cryptography*, **38** (2006), 55–81.
16. C. Hu, C. Zhao, Multi-point codes from generalized Hermitian curves, *IEEE Transactions on Information Theory*, **62** (5) (2016), 2726–2736.
17. C. Hu, Explicit construction of AG codes from a curve in the tower of Bassa-Beelen-Garcia-Stichtenoth, *IEEE Transactions on Information Theory*, **63** (11) (2017), 7237–7246.
18. C. Hu, S. Yang, Multi-point codes over Kummer extensions, *Designs, Codes and Cryptography*, **86** (2018), 211–230.

19. C. Hu, S. Yang, Multi-point codes from the GGS curves, *Advances in Mathematics of Communications*, **14** (2) (2020), 279–299.
20. H. Maharaj, G. L. Matthews, G. Pirsic, Riemann-Roch spaces of the Hermitian function field with applications to algebraic geometry codes and low-discrepancy sequences, *Journal of Pure and Applied Algebra*, **195** (2005), 261–280.
21. G. L. Matthews, Codes from the Suzuki function field, *IEEE Transactions on Information Theory*, **50** (12) (2004), 3298–3302.
22. A. Oneto, G. Tamone, On the order bound of one-point algebraic geometry codes, *Journal of Pure and Applied Algebra*, **213** (2009), 1179–1191.
23. S. Park, Minimum distance of Hermitian two-point codes, *Designs, Codes, and Cryptography*, **57** (2) (2010), 195–213.
24. J. P. Pedersen, A function field related to the Ree group, Coding Theory and Algebraic Geometry, Lectures Notes in Mathematics, vol. 1518, pp. 122–132. Springer, Berlin, 1992.
25. D. Skabelund, New maximal curves as ray class fields over Deligne-Lusztig curves, *Proceedings of the American Mathematical Society*, **146** (2) (2018), 525–540.
26. H. Stichtenoth, Algebraic Function Fields and Codes, Springer, Berlin (2009).
27. C. Voss, T. Høholdt, An explicit construction of a sequence of codes attaining the Tsfasman-Vlăduţ-Zink bound–the first steps, *IEEE Transactions on Information Theory*, **43** (1) (1997), 128–135.
28. S. Yang, C. Hu, Weierstrass semigroups from Kummer extensions, *Finite Fields and Their Applications*, **45** (2017), 264–284.
29. S. Yang, C. Hu, Pure Weierstrass gaps from a quotient of the Hermitian curve, *Finite Fields and Their Applications*, **50** (2018), 251–271.
30. S. Yang, C. Hu, Weierstrass semigroups on the third function field in a tower attaining the Drinfeld-Vlăduţ bound, *Advances in Mathematics of Communications*, online, https://doi.org/10.3934/amc.2022066.