Noname manuscript No.
(will be inserted by the editor)

Multi-point Codes from the GGS Curves

Chuangqiang Hu · Shudi Yang

Received: date / Accepted: date

Abstract This paper is concerned with the construction of algebraic geometric codes defined from GGS curves. It is of significant use to describe bases for the Riemann-Roch spaces associated with totally ramified places, which enables us to study multi-point AG codes. Along this line, we characterize explicitly the Weierstrass semigroups and pure gaps. Additionally, we determine the floor of a certain type of divisor and investigate the properties of AG codes from GGS curves. Finally, we apply these results to find multi-point codes with excellent parameters. As one of the examples, a presented code with parameters $[216, 190, \geqslant 18]$ over $\mathbb{F}_{64}$ yields a new record.

Keywords Algebraic geometric codes · GGS curve · Weierstrass semigroup · Weierstrass pure gap

Mathematics Subject Classification (2010) 14H55 · 11R58

1 Introduction

In the early 1980s, Goppa [12] constructed algebraic geometric codes (AG codes for short) from algebraic curves. Since then, the study of AG codes becomes an important instrument in the theory of error-correcting codes. Roughly speaking, the parameters of an AG code are good when the underlying curve has many rational points with respect to its genus. For this reason maximal curves, that is curves attaining the Hasse-Weil upper bound, have

C. Hu
School of Mathematics, Sun Yat-sen University, Guangzhou 510275, P.R. China
E-mail: huchq@mail2.sysu.edu.cn

S. Yang
School of Mathematical Sciences, Qufu Normal University, Shandong 273165, P.R.China
E-mail: yangshudi7902@126.com

been widely investigated in the literature: for example the Hermitian curve and its quotients, the Suzuki curve, the Klein quartic and the GK curve. In this work we will study multi-point AG codes on the GGS curves.

In order to construct good AG codes we need to study Weierstrass semigroups and pure gaps. Their use comes from the theory of one-point codes. For example, the authors in [26, 14, 28, 29] examined one-point codes from Hermitian curves and develop efficient methods to decode them. Korchmáros and Nagy [19] computed the Weierstrass semigroup of a degree three closed point of the Hermitian curve. Matthews [24] determined the Weierstrass semigroup of any r-tuple rational points on the quotient of the Hermitian curve. As is known, Weierstrass pure gap is also an useful tool in coding theory. Garcia, Kim and Lax improved the Goppa bound using arithmetical structure of the Weierstrass gaps at one place in [9, 10]. The concept of pure gaps of a pair of points on a curve was initiated by Homma and Kim [15], and it has been pushed forward by Carvalho and Torres [4] to several points. Maharaj, Matthews and Pirsic [22, 21] extended this construction by introducing the notion of the floor of a divisor and obtained improved bounds on the parameters of AG codes.

In this work, we focus our attention on the GGS curves, which are maximal curves constructed by Garcia, Güneri and Stichtenoth [8] over $\mathbb{F}_{q^{2n}}$ defined by the equations

$$\begin{cases} x^q + x = y^{q+1}, \\ y^{q^2} - y = z^m, \end{cases}$$

where q is a prime power and $m = (q^n + 1)/(q + 1)$ with $n > 1$ to be an odd integer. Obviously the GGS curve is a generalization of the GK curve initiated by Giulietti and Korchmáros [11] where we take $n = 3$. Recall that Fanali and Giulietti [7] have investigated one-point AG codes over the GK curves and obtained linear codes with better parameters with respect those known previously. Two-point and multi-point AG codes on the GK maximal curves have been studied in [6] and [3], respectively. Bartoli, Montanucci and Zini [2] examined one-point AG codes from the GGS curves. Inspired by the above work and [16, 5], here we will examine multi-point AG codes arising from GGS curves. To be precise, an explicit basis for the Riemann-Roch space $\mathcal{L}(G)$ is determined by constructing a related set of lattice points. Then we use this result to characterize the Weierstrass semigroups and the pure gaps with respect to several totally ramified places. In addition, we give an effective algorithm to compute the floor of divisors. The properties of AG codes from GGS curves are also considered. Finally, our results will lead us to find new codes with better parameters in comparison with the existing codes in MinT's Tables [25]. A new record-giving $[216, 190, \geqslant 18]$-code over $\mathbb{F}_{64}$ is presented as one of the examples.

The remainder of the paper is organized as follows. In Section 2 we briefly recall some preliminary results over arbitrary function fields. Section 3 focuses on the construction of bases for the Riemann-Roch space from GGS curves. In Section 4 we determine the Weierstrass semigroups and the pure gaps.

Section 5 devotes to the floor of divisors of function fields. Section 6 studies the properties of AG codes associated with GGS curves. Finally, in Section7 we use the results of the previous sections to construct multi-point codes with excellent parameters.

2 Background and preliminary results

Let q be a power of a prime p and $\mathbb{F}_q$ be a finite field of cardinality q, with characteristic p. We denote by F a function field over $\mathbb{F}_q$ and by $\mathbb{P}_F$ the set of places of F. The free abelian group generated by the places of F is denoted by $\mathcal{D}_F$, whose element is called a divisor. If a divisor D is of the form $D = \sum_{P\in\mathbb{P}_F} n_P P$ with $n_P \in \mathbb{Z}$, almost all $n_P = 0$, then the degree of D is $\deg(D) = \sum_{P\in\mathbb{P}_F} n_P$. For a function $f \in F$, the symbol $v_P(f)$ represents the valuation of f at a rational place P. The divisor of f will be denoted by (f) and the divisor of poles of f will be denoted by $(f)_\infty$. The Riemann-Roch vector space with respect to D is defined by

$$\mathcal{L}(D) = \Big\{ f \in F \Big| (f) + D \geqslant 0 \Big\} \cup \{0\}.$$

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 the canonical divisor and g is the genus of the associated curve.

Let G be a divisor of F and let $D := Q_1 + \cdots + Q_N$ be another divisor of F such that $Q_1, \cdots, Q_N$ are distinct rational places, each not belonging to the support of G. There are two classical ways of constructing AG codes associated with D and G. One is based on the Riemann-Roch space $\mathcal{L}(G)$,

$$C_{\mathcal{L}}(D, G) := \Big\{ (f(Q_1), \cdots, f(Q_N)) \Big| f \in \mathcal{L}(G) \Big\} \subseteq \mathbb{F}_q^N.$$

The other one is depends on the space of differentials $\Omega(G - D)$,

$$C_\Omega(D, G) := \Big\{ (\mathrm{res}_{Q_1}(\eta), \cdots, \mathrm{res}_{Q_N}(\eta)) \Big| \eta \in \Omega(G - D) \Big\}.$$

It is well-known the codes $C_{\mathcal{L}}(D, G)$ and $C_\Omega(D, G)$ are dual to each other. In this work we will take $C_\Omega(D, G)$ for consideration, whose parameters are $[N, k_\Omega, d_\Omega]$ with $k_\Omega = N - k$ and $d_\Omega \geqslant \deg(G) - (2g - 2)$, where $k = \ell(G) - \ell(G - D)$ is the dimension of $C_{\mathcal{L}}(D, G)$. If moreover $2g - 2 < \deg(G) < N$ then

$$k_\Omega = N + g - 1 - \deg(G).$$

We refer the reader to [26] for more information.

We briefly introduce some definitions and notations [23]. Let $Q_1, \cdots, Q_l$ be distinct rational places of F, then the Weierstrass semigroup $H(Q_1, \cdots, Q_l)$ is defined by

$$\Big\{(s_1, \cdots, s_l) \in \mathbb{N}_0^l \Big| \exists f \in F \text{ with } (f)_\infty = \sum_{i=1}^{l} s_i Q_i \Big\},$$

and the Weierstrass gap set $G(Q_1, \cdots, Q_l)$ is defined by $\mathbb{N}_0^l \backslash H(Q_1, \cdots, Q_l)$, where $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$ denotes the set of nonnegative integers.

Homma and Kim [15] introduced the concept of pure gap set with a pair of rational places. This was generalized by Carvalho and Torres [4] to several rational places, denoted by $G_0(Q_1, \cdots, Q_l)$, which is given by

$$\Big\{(s_1, \cdots, s_l) \in \mathbb{N}^l \Big| \ell(G) = \ell(G - Q_j) \text{ for } 1 \leqslant j \leqslant l, \text{ where } G = \sum_{i=1}^{l} s_i Q_i \Big\}.$$

In addition, they showed that $(s_1, \cdots, s_l)$ is a pure gap at $(Q_1, \cdots, Q_l)$ if and only if

$$\ell(s_1 Q_1 + \cdots + s_l Q_l) = \ell((s_1 - 1)Q_1 + \cdots + (s_l - 1)Q_l).$$

The following lemma, regarded as an easy generalization of a result due to Kim [17], provides us with a way to calculate the Weierstrass semigroups.

Lemma 1 *For rational places $Q_1, \cdots, Q_l$ with $1 \leqslant l \leqslant r$, the set $H(Q_1, \cdots, Q_l)$ is given by*

$$\Big\{(s_1, \cdots, s_l) \in \mathbb{N}_0^l \Big| \ell(G) \neq \ell(G - Q_j) \textit{ for } 1 \leqslant j \leqslant l, \textit{ where } G = \sum_{i=1}^{l} s_i Q_i \Big\}.$$

3 Bases for Riemann-Roch spaces from GGS curves

Let q be a prime power and consider an odd integer $n > 1$. The GGS curve $\mathrm{GGS}(q, n)$ over $\mathbb{F}_{q^{2n}}$ is defined by the equations

$$\begin{cases} x^q + x = y^{q+1}, \\ y^{q^2} - y = z^m, \end{cases} \tag{1}$$

where $m = (q^n + 1)/(q + 1)$. The genus of $\mathrm{GGS}(q, n)$ is $\frac{1}{2}(q-1)(q^{n+1} + q^n - q^2)$ and there are $q^{2n+2} - q^{n+3} + q^{n+2} + 1$ rational places, see [8] for more details. Especially when $n = 3$, the equation (1) gives the well-known maximal curve, the so-called GK curve, proposed by Giulietti and Korchmáros in [11].

Denote by $\mathcal{P}_{\alpha,\beta,\gamma}$ the rational place of this curve except for the one centered at infinity P_∞. Take $Q_\beta := \sum_{\alpha^q + \alpha = \beta^{q+1}} \mathcal{P}_{\alpha,\beta,0}$ where $\beta \in \mathbb{F}_{q^2}$. Then $\deg Q_\beta = q$. For later use, we write $P_0 := \mathcal{P}_{0,0,0}$ and $Q_0 = P_0 + P_1 + \cdots + P_{q-1}$.

The following proposition describes some principle divisors from GGS curves.

Proposition 1 *Let the curve* $\mathrm{GGS}(q,n)$ *be given in* (1) *and assume that* α_μ *with* $0 \leqslant \mu < q$ *are the solutions of* $x^q + x = 0$. *Then we obtain*

1. $(x-\alpha_\mu) = m(q+1)P_\mu - m(q+1)P_\infty$,
2. $(y-\beta) = mQ_\beta - mqP_\infty$ *for* $\beta \in \mathbb{F}_{q^2}$,
3. $(z) = \sum_{\beta\in\mathbb{F}_{q^2}} Q_\beta - q^3 P_\infty$.

For convenience, we use Q_ν $(0 \leqslant \nu \leqslant q^2-1)$ to represent the divisors Q_β $(\beta \in \mathbb{F}_{q^2})$. In particular, $Q_\nu|_{\nu=0} = Q_\beta|_{\beta=0}$.

Let $G := \sum_{\mu=0}^{q-1} r_\mu P_\mu + \sum_{\nu=1}^{q^2-1} s_\nu Q_\nu + tP_\infty$. Maharaj [20] showed that the Riemann-Roch space $\mathcal{L}(G)$ can be decomposed as a direct sum of Riemann-Roch spaces of divisors of the projective line. For applications to computing pure gaps, we would like to give an explicit basis of $\mathcal{L}(G)$, which consists of monomials of r elements. Actually, we generalize the result of [22] concerning about the basis of Hermitian curves.

Let $\boldsymbol{j} = (j_1, j_2, \cdots, j_{q-1})$ and $\boldsymbol{k} = (k_1, k_2, \cdots, k_{q^2-1})$. For $(i,\boldsymbol{j},\boldsymbol{k}) \in \mathbb{Z}^{q^2+q-1}$, we define

$$E_{i,\boldsymbol{j},\boldsymbol{k}} := z^i \prod_{\mu=1}^{q-1}(x-\alpha_\mu)^{j_\mu} \prod_{\nu=1}^{q^2-1}(y-\beta_\nu)^{k_\nu}. \tag{2}$$

Set $|\boldsymbol{j}| = \sum_{\mu=1}^{q-1} j_\mu$ and $|\boldsymbol{k}| = \sum_{\nu=1}^{q^2-1} k_\nu$. By Proposition1, one can compute the divisor of $E_{i,\boldsymbol{j},\boldsymbol{k}}$:

$$\begin{aligned}\mathrm{div}(E_{i,\boldsymbol{j},\boldsymbol{k}}) =& iP_0 + \sum_{\mu=1}^{q-1}(i+m(q+1)j_\mu)P_\mu + \sum_{\nu=1}^{q^2-1}(i+mk_\nu)Q_\nu \\ &- \left(q^3 i + m(q+1)|\boldsymbol{j}| + mq|\boldsymbol{k}|\right)P_\infty. \end{aligned} \tag{3}$$

For later use, we denote by $\lfloor x \rfloor$ the largest integer not greater than x and by $\lceil x \rceil$ the smallest integer not less than x. It is easy to show that $j = \left\lceil \frac{\alpha}{\beta} \right\rceil$ if and only if $0 \leqslant \beta j - \alpha < \beta$, where $\beta \in \mathbb{N}$ and $\alpha \in \mathbb{Z}$.

Put $\boldsymbol{r} = (r_0, r_1, \cdots, r_{q-1})$ and $\boldsymbol{s} = (s_1, s_2, \cdots, s_{q^2-1})$. Let us define a set of lattice points for $(\boldsymbol{r},\boldsymbol{s},t) \in \mathbb{Z}^{q^2+q}$,

$$\begin{aligned}\Omega_{\boldsymbol{r},\boldsymbol{s},t} := \Big\{(i,\boldsymbol{j},\boldsymbol{k})\Big|\, & i+r_0 \geqslant 0, \\ & 0 \leqslant i + m(q+1)j_\mu + r_\mu < m(q+1) \text{ for } \mu = 1,\cdots,q-1, \\ & 0 \leqslant i + mk_\nu + s_\nu < m \text{ for } \nu = 1,\cdots,q^2-1, \\ & q^3 i + m(q+1)|\boldsymbol{j}| + mq|\boldsymbol{k}| \leqslant t\Big\},\end{aligned}$$

or equivalently,

$$\Omega_{\boldsymbol{r},\boldsymbol{s},t} := \Big\{(i,\boldsymbol{j},\boldsymbol{k})\Big|\, i + r_0 \geqslant 0,$$

$$j_\mu = \left\lceil \frac{-i - r_\mu}{m(q+1)} \right\rceil \text{ for } \mu = 1, \cdots, q-1,$$
$$k_\nu = \left\lceil \frac{-i - s_\nu}{m} \right\rceil \text{ for } \nu = 1, \cdots, q^2-1,$$
$$q^3 i + m(q+1)|\boldsymbol{j}| + mq|\boldsymbol{k}| \leqslant t \Big\}. \tag{4}$$

The following lemma is crucial for the proof of our key result. However, the proof of this lemma is technical, and will be completed later.

Lemma 2 *The number of lattice points in $\Omega_{\boldsymbol{r},\boldsymbol{s},t}$ can be expressed as:*

$$\#\Omega_{\boldsymbol{r},\boldsymbol{s},t} = 1 - g + t + |\boldsymbol{r}| + q|\boldsymbol{s}|,$$

for $t \geqslant 2g - 1 - q^3 w$, where $w = \min_{\substack{0 \leqslant \mu \leqslant q-1 \\ 1 \leqslant \nu \leqslant q^2-1}} \Big\{ r_\mu, s_\nu \Big\}$.

Let $G := \sum_{\mu=0}^{q-1} r_\mu P_\mu + \sum_{\nu=1}^{q^2-1} s_\nu Q_\nu + tP_\infty$. It is trivial that $\deg G = |\boldsymbol{r}| + q|\boldsymbol{s}| + t$. Now we can easily prove the main result of this section.

Theorem 1 *Let $G := \sum_{\mu=0}^{q-1} r_\mu P_\mu + \sum_{\nu=1}^{q^2-1} s_\nu Q_\nu + tP_\infty$. The elements $E_{i,\boldsymbol{j},\boldsymbol{k}}$ with $(i, \boldsymbol{j}, \boldsymbol{k}) \in \Omega_{\boldsymbol{r},\boldsymbol{s},t}$ constitute a basis for the Riemann-Roch space $\mathcal{L}(G)$. Moreover, we have $\ell(G) = \#\Omega_{\boldsymbol{r},\boldsymbol{s},t}$.*

Proof Let $(i, \boldsymbol{j}, \boldsymbol{k}) \in \Omega_{\boldsymbol{r},\boldsymbol{s},t}$. It follows from the definition that $E_{i,\boldsymbol{j},\boldsymbol{k}} \in \mathcal{L}(G)$, where $G = \sum_{\mu=0}^{q-1} r_\mu P_\mu + \sum_{\nu=1}^{q^2-1} s_\nu Q_\nu + tP_\infty$. From Equation (3), we have $v_{P_0}(E_{i,\boldsymbol{j},\boldsymbol{k}}) = i$, which indicates that the valuation of $E_{i,\boldsymbol{j},\boldsymbol{k}}$ at the rational place P_0 uniquely depends on i. Since lattice points in $\Omega_{\boldsymbol{r},\boldsymbol{s},t}$ provide distinct values of i, the elements $E_{i,\boldsymbol{j},\boldsymbol{k}}$ are linearly independent of each other, with $(i, \boldsymbol{j}, \boldsymbol{k}) \in \Omega_{\boldsymbol{r},\boldsymbol{s},t}$. To show that they constitute a basis for $\mathcal{L}(G)$, the only thing is to prove that

$$\ell(G) = \#\Omega_{\boldsymbol{r},\boldsymbol{s},t}.$$

For the case of r_0 sufficiently large, it follows from the Riemann-Roch Theorem and Lemma 2 that

$$\begin{aligned} \ell(G) &= 1 - g + \deg(G) \\ &= 1 - g + |\boldsymbol{r}| + q|\boldsymbol{s}| + t = \#\Omega_{\boldsymbol{r},\boldsymbol{s},t}. \end{aligned}$$

This implies that $\mathcal{L}(G)$ is spanned by elements $E_{i,\boldsymbol{j},\boldsymbol{k}}$ with $(i, \boldsymbol{j}, \boldsymbol{k})$ in the set $\Omega_{\boldsymbol{r},\boldsymbol{s},t}$.

For the general case, we choose $r_0' > r_0$ large enough and set $G' := r_0' P_0 + \sum_{\mu=1}^{q-1} r_\mu P_\mu + \sum_{\nu=1}^{q^2-1} s_\nu Q_\nu + tP_\infty$, $\boldsymbol{r'} = (r_0', r_1, \cdots, r_{q-1})$. From above argument, we know that the elements $E_{i,\boldsymbol{j},\boldsymbol{k}}$ with $(i, \boldsymbol{j}, \boldsymbol{k}) \in \Omega_{\boldsymbol{r'},\boldsymbol{s},t}$ span the whole space of $\mathcal{L}(G')$. Remember that $\mathcal{L}(G)$ is a linear subspace of $\mathcal{L}(G')$, which can be written as

$$\mathcal{L}(G) = \Big\{ f \in \mathcal{L}(G') \Big| v_{P_0}(f) \geqslant -r_0 \Big\}.$$

Thus, we choose $f \in \mathcal{L}(G)$ and suppose that

$$f = \sum_{(i,\boldsymbol{j},\boldsymbol{k}) \in \Omega_{\boldsymbol{r'},\boldsymbol{s},t}} a_i E_{i,\boldsymbol{j},\boldsymbol{k}},$$

since $f \in \mathcal{L}(G')$. The valuation of f at P_0 is $v_{P_0}(f) = \min_{a_i \neq 0}\{i\}$. Then the inequality $v_{P_0}(f) \geqslant -r_0$ gives that, if $a_i \neq 0$, then $i \geqslant -r_0$. Equivalently, if $i < -r_0$, then $a_i = 0$. From the definition of $\Omega_{\boldsymbol{r},\boldsymbol{s},t}$ and $\Omega_{\boldsymbol{r'},\boldsymbol{s},t}$, we get that

$$f = \sum_{i,\boldsymbol{j},\boldsymbol{k} \in \Omega_{\boldsymbol{r},\boldsymbol{s},t}} a_i E_{i,\boldsymbol{j},\boldsymbol{k}}.$$

Then the theorem follows. □

We now turn to prove Lemma 2 which requires a series of results listed as follows.

Definition 1 Let $(a_1, \cdots, a_k)$ be a sequence of positive integers such that the greatest common divisor is 1. Define $d_i = \gcd(a_1, \cdots, a_i)$ and $A_i = \{a_1/d_i, \cdots, a_i/d_i\}$ for $i = 1, \cdots, k$. Let $d_0 = 0$. Let S_i be the semigroup generated by A_i. If $a_i/d_i \in S_i$ for $i = 2, \cdots, k$, we call the sequence $(a_1, \cdots, a_k)$ telescopic. A semigroup is called telescopic if it is generated by a telescopic sequence.

Lemma 3 ([18]) *If $(a_1, \cdots, a_k)$ is telescopic and $M \in S_k$, then there exist uniquely determined non-negative integers $0 \leqslant x_i < d_{i-1}/d_i$ for $i = 2, \cdots, k$, such that*

$$M = \sum_{i=1}^{k} x_i a_i.$$

We call this representation the normal representation of M by $(a_1, \cdots, a_k)$.

Lemma 4 ([18]) *For the semigroup generated by the telescopic sequence $(a_1, \cdots, a_k)$ we have*

$$l_g(S_k) = \sum_{i=1}^{k} (d_{i-1}/d_i - 1)a_i,$$
$$g(S_k) = (l_g(S_k) + 1)/2,$$

where $l_g(S_k)$ and $g(S_k)$ denote the largest gap and the number of gaps of S_k, respectively.

Lemma 5 *Let $m = (q^n + 1)/(q + 1)$, $g = \frac{1}{2}(q - 1)(q^{n+1} + q^n - q^2)$ for an odd integer n. Let $t \in \mathbb{Z}$. Consider the lattice point set $\Psi(t)$ defined by*

$$\left\{(\alpha, \beta, \gamma) \middle| 0 \leqslant \alpha < m, 0 \leqslant \beta \leqslant q, \gamma \geqslant 0, q^3\alpha + mq\beta + m(q + 1)\gamma \leqslant t\right\},$$

If $t \geqslant 2g - 1$, then $\Psi(t)$ has cardinality

$$\#\Psi(t) = 1 - g + t.$$

Proof Let $a_1 = q^3, a_2 = mq, a_3 = m(q+1)$. It is easily verified that the sequence (a_1, a_2, a_3) is telescopic. By Lemma 3 every element M in S_3 has a unique representation $M = a_1\alpha + a_2\beta + a_3\gamma$, where S_3 is the semigroup generated by (a_1, a_2, a_3). One obtains from Lemma 4 that

$$\begin{aligned} l_g(S_3) &= (q-1)(q^n+1)(q+1) - q^3, \\ g(S_3) &= \frac{1}{2}(l_g(S_3)+1) = \frac{1}{2}(q-1)(q^{n+1}+q^n-q^2) = g. \end{aligned}$$

It follows that the set $\Psi(t)$ has cardinality $1-g+t$ provided that $t \geqslant 2g-1 = l_g(S_3)$, which finishes the proof. □

From Lemma 5, we get the number of lattice points in $\Omega_{\mathbf{0},\mathbf{0},t}$.

Lemma 6 *If $t \geqslant 2g-1$, then the number of lattice points in $\Omega_{\mathbf{0},\mathbf{0},t}$ is*

$$\#\Omega_{\mathbf{0},\mathbf{0},t} = 1-g+t.$$

Proof Note that

$$\begin{aligned} \Omega_{\mathbf{0},\mathbf{0},t} := \Big\{(i,\boldsymbol{j},\boldsymbol{k}) \Big| \, & i \geqslant 0, \\ & j_\mu = \left\lceil \frac{-i}{m(q+1)} \right\rceil \text{ for } \mu = 1, \cdots, q-1, \\ & k_\nu = \left\lceil \frac{-i}{m} \right\rceil \text{ for } \nu = 1, \cdots, q^2-1, \\ & q^3 i + m(q+1)|\boldsymbol{j}| + mq|\boldsymbol{k}| \leqslant t \Big\}. \end{aligned} \tag{5}$$

Set $i := \alpha + m(\beta + (q+1)\gamma)$ with $0 \leqslant \alpha < m$, $0 \leqslant \beta \leqslant q$ and $\gamma \geqslant 0$. Then Equation (5) gives that

$$\Omega_{\mathbf{0},\mathbf{0},t} \cong \Big\{(\alpha,\beta,\gamma)\Big| 0 \leqslant \alpha < m, 0 \leqslant \beta \leqslant q, \gamma \geqslant 0, q^3\alpha + mq\beta + (q^n+1)\gamma \leqslant t\Big\}.$$

Here and thereafter, the notation $A \cong B$ means that two lattice point sets A, B are bijective. Thus the assertion $\#\Omega_{\mathbf{0},\mathbf{0},t} = 1-g+t$ follows from Lemma 5. □

Lemma 7 *The lattice point set $\Omega_{\boldsymbol{r},\boldsymbol{s},t}$ as defined in Section 3 is symmetric with respect to $r_0, r_1, \cdots, r_{q-1}$ and $s_1, \cdots, s_{q^2-1}$, respectively. In other words, we have $\#\Omega_{\boldsymbol{r},\boldsymbol{s},t} = \#\Omega_{\boldsymbol{r'},\boldsymbol{s'},t}$, where the sequences $\big(r_i\big)_{i=0}^{q-1}$ and $\big(s_i\big)_{i=1}^{q^2-1}$ are equal to $\big(r'_i\big)_{i=0}^{q-1}$ and $\big(s'_i\big)_{i=1}^{q^2-1}$ up to permutation, respectively.*

Proof Recall that $\Omega_{\boldsymbol{r},\boldsymbol{s},t}$ is defined by

$$\begin{aligned} \Omega_{\boldsymbol{r},\boldsymbol{s},t} := \Big\{(i',\boldsymbol{j'},\boldsymbol{k'}) \Big| \, & i' + r_0 \geqslant 0, \\ & j'_\mu = \left\lceil \frac{-i' - r_\mu}{m(q+1)} \right\rceil \text{ for } \mu = 1, \cdots, q-1, \end{aligned}$$

$$k'_\nu = \left\lceil \frac{-i' - s_\nu}{m} \right\rceil \text{ for } \nu = 1, \cdots, q^2 - 1,$$
$$q^3 i' + m(q+1)|\boldsymbol{j'}| + mq|\boldsymbol{k'}| \leqslant t \Big\},$$

where $\boldsymbol{j'} = (j'_1, \cdots, j'_{q-1})$ and $\boldsymbol{k'} = (k'_1, \cdots, k'_{q^2-1})$. It is important to write $i' = i + m(q+1)l$ with $0 \leqslant i < m(q+1)$. Let $j'_\mu = j_\mu - l$ for $\mu \geqslant 1$, $k'_\nu = k_\nu - (q+1)l$ for $\nu \geqslant 1$. Then

$$\begin{aligned} \Omega_{\boldsymbol{r},\boldsymbol{s},t} \cong \Big\{(i, l, \boldsymbol{j}, \boldsymbol{k}) \Big| & \, i + m(q+1)l \geqslant -r_0, 0 \leqslant i < m(q+1), \\ & j_\mu = \left\lceil \frac{-i - r_\mu}{m(q+1)} \right\rceil \text{ for } \mu = 1, \cdots, q-1, \\ & k_\nu = \left\lceil \frac{-i - s_\nu}{m} \right\rceil \text{ for } \nu = 1, \cdots, q^2 - 1, \\ & q^3 i + m(q+1)\big(l + |\boldsymbol{j}|\big) + mq|\boldsymbol{k}| \leqslant t \Big\}, \end{aligned}$$

where $\boldsymbol{j} = (j_1, \cdots, j_{q-1})$ and $\boldsymbol{k} = (k_1, \cdots, k_{q^2-1})$. The first inequality in $\Omega_{\boldsymbol{r},\boldsymbol{s},t}$ gives that $l \geqslant j_0 := \left\lceil \dfrac{-i - r_0}{m(q+1)} \right\rceil$. So we write $l = j_0 + \iota$ with $\iota \geqslant 0$. Then

$$\begin{aligned} \Omega_{\boldsymbol{r},\boldsymbol{s},t} \cong \Big\{(i, \iota, j_0, \boldsymbol{j}, \boldsymbol{k}) \Big| & \, 0 \leqslant i < m(q+1), \iota \geqslant 0, \\ & j_\mu = \left\lceil \frac{-i - r_\mu}{m(q+1)} \right\rceil \text{ for } \mu = 0, 1, \cdots, q-1, \\ & k_\nu = \left\lceil \frac{-i - s_\nu}{m} \right\rceil \text{ for } \nu = 1, \cdots, q^2 - 1, \\ & q^3 i + m(q+1)\big(j_0 + \iota + |\boldsymbol{j}|\big) + mq|\boldsymbol{k}| \leqslant t \Big\}. \end{aligned}$$

The right hand side means that the number of the lattice points does not depend on the order of r_μ, $0 \leqslant \mu \leqslant q-1$, and the order of s_ν, $1 \leqslant \nu \leqslant q^2 - 1$, which concludes the desired assertion. □

Lemma 8 *Let* $\boldsymbol{r} = (r_0, r_1, \cdots, r_{q-1})$ *and* $\boldsymbol{s} = (s_1, s_2, \cdots, s_{q^2-1})$. *The following equality holds:*

$$\#\Omega_{\boldsymbol{r},\boldsymbol{s},t} = \#\Omega_{\boldsymbol{0},\boldsymbol{s},t} + |\boldsymbol{r}|,$$

where $r_\mu \geqslant 0$ *for* $\mu \geqslant 0$, $s_\nu \geqslant 0$ *for* $\nu \geqslant 1$, *and* $t \geqslant 2g - 1$.

Proof Let us take the sets $\Omega_{\boldsymbol{r},\boldsymbol{s},t}$ and $\Omega_{\boldsymbol{r'},\boldsymbol{s},t}$ into consideration, where $\boldsymbol{r'} = (0, r_1, \cdots, r_{q-1})$. It follows from the definition that the complementary set $\Delta := \Omega_{\boldsymbol{r},\boldsymbol{s},t} \backslash \Omega_{\boldsymbol{r'},\boldsymbol{s},t}$ is given by

$$\begin{aligned} \Big\{(i, \boldsymbol{j}, \boldsymbol{k}) \Big| & -r_0 \leqslant i < 0, \\ & j_\mu = \left\lceil \frac{-i - r_\mu}{m(q+1)} \right\rceil \text{ for } \mu = 1, \cdots, q-1, \end{aligned}$$

$$k_\nu = \left\lceil \frac{-i - s_\nu}{m} \right\rceil \text{ for } \nu = 1, \cdots, q^2 - 1,$$
$$q^3 i + m(q+1)|\boldsymbol{j}| + mq|\boldsymbol{k}| \leqslant t \Big\}.$$

It is trivial that $\Delta = \varnothing$ if $r_0 = 0$. To determine the cardinality of Δ with $r_0 > 0$, we denote $i := \alpha + m(\beta + (q+1)\gamma)$ with α, β, γ satisfying $0 \leqslant \alpha < m$, $0 \leqslant \beta \leqslant q$ and $\gamma \leqslant -1$. Then $j_\mu \leqslant -\gamma$ for $\mu \geqslant 1$, $k_\nu \leqslant -\beta - (q+1)\gamma$ for $\nu \geqslant 1$. A straightforward computation shows

$$\begin{aligned} q^3 i + m(q+1)|\boldsymbol{j}| + mq|\boldsymbol{k}| &\leqslant q^3\alpha + mq\beta + m(q+1)\gamma \\ &\leqslant q^3(m-1) + mq^2 - m(q+1) = 2g - 1. \end{aligned}$$

So the last inequality in Δ always holds for all $t \geqslant 2g - 1$, which means that the cardinality of Δ is determined by the first inequality, that is $\#\Delta = r_0$. Then we must have

$$\#\Omega_{\boldsymbol{r},\boldsymbol{s},t} = \#\Omega_{\boldsymbol{r}',\boldsymbol{s},t} + r_0,$$

whenever $r_0 \geqslant 0$. Repeating the above routine and using Lemma 7, we get

$$\#\Omega_{\boldsymbol{r},\boldsymbol{s},t} = \#\Omega_{\boldsymbol{0},\boldsymbol{s},t} + |\boldsymbol{r}|,$$

where $\boldsymbol{r} = (r_0, r_1, \cdots, r_{q-1})$. □

Lemma 9 *Let $\boldsymbol{s} = (s_1, s_2, \cdots, s_{q^2-1})$. The following equality holds:*

$$\#\Omega_{\boldsymbol{0},\boldsymbol{s},t} = \#\Omega_{\boldsymbol{0},\boldsymbol{0},t} + q|\boldsymbol{s}|,$$

where $s_i \geqslant 0$ for $i = 1, 2, \cdots, q^2 - 1$ and $t \geqslant 2g - 1$.

Proof For convenience, let us denote $\boldsymbol{r} := (s_0, s_0, \cdots, s_0)$ to be the q-tuple with all elements equal s_0, where $s_0 \geqslant 0$, and write $\Omega_{\boldsymbol{r},\boldsymbol{s},t}$ as $\Gamma_{s_0,(s_1,\cdots,s_{q^2-1}),t}$. To get the desired conclusion, we first claim that

$$\#\Gamma_{s_0,(s_1,\cdots,s_{q^2-1}),t} = \#\Gamma_{s'_0,(s'_1,\cdots,s'_{q^2-1}),t}, \tag{6}$$

where the sequence $\left(s_i\right)_{i=0}^{q^2-1}$ is equal to $\left(s'_i\right)_{i=0}^{q^2-1}$ up to permutation.

Note that $\Gamma_{s_0,(s_1,\cdots,s_{q^2-1}),t}$ is equivalent to

$$\Big\{(i', j', k'_1, \cdots, k'_{q^2-1}) \Big| i' + s_0 \geqslant 0,$$
$$0 \leqslant i' + m(q+1)j' + s_0 < m(q+1),$$
$$0 \leqslant i' + mk'_\nu + s_\nu < m \text{ for } \nu = 1, \cdots, q^2 - 1,$$
$$q^3 i' + m(q+1)(q-1)j' + mq|\boldsymbol{k}'| \leqslant t \Big\},$$

where $|\boldsymbol{k}'| = \sum_{\nu=1}^{q^2-1} k'_\nu$. By setting $i' := i + m\kappa$ where $0 \leqslant i < m$ and $k'_\nu := k_\nu - \kappa$ for $\nu \geqslant 1$, we obtain

$$\Gamma_{s_0,(s_1,\cdots,s_{q^2-1}),t} \cong \Big\{(i, \kappa, j', k_1, \cdots, k_{q^2-1}) \Big| 0 \leqslant i < m, i + m\kappa + s_0 \geqslant 0,$$

$$0 \leqslant i + m\kappa + m(q+1)j' + s_0 < m(q+1),$$
$$0 \leqslant i + mk_\nu + s_\nu < m \text{ for } \nu = 1, \cdots, q^2-1,$$
$$\left. q^3 i + m(q+1)(q-1)j' + mq(\kappa + |\boldsymbol{k}|) \leqslant t \right\}.$$

By setting $\kappa := k_0 + \varepsilon$, where $\varepsilon := -(q+1)j_0 + \eta$, $0 \leqslant \eta < q+1$ and $k_0 := \left\lceil \dfrac{-i - s_0}{m} \right\rceil$, one gets that $0 \leqslant i + mk_0 + s_0 < m$, which leads to $0 \leqslant i + m\kappa + m(q+1)j_0 - m\eta + s_0 < m$. So the inequality $0 \leqslant i + m\kappa + m(q+1)j_0 + s_0 < m + m\eta \leqslant m(q+1)$ holds since $\varepsilon = -(q+1)j_0 + \eta$. Thus we must have $j_0 = j' \leqslant 0$. Therefore

$$\begin{aligned} \Gamma_{s_0,(s_1,\cdots,s_{q^2-1}),t} \cong \Big\{ &(i, j_0, \eta, k_0, k_1, \cdots, k_{q^2-1}) \Big| 0 \leqslant i < m, j_0 \leqslant 0, \\ &0 \leqslant \eta < q+1, \\ &k_\nu = \left\lceil \frac{-i - s_\nu}{m} \right\rceil \text{ for } \nu = 0, 1, \cdots, q^2-1, \\ &q^3 i - m(q+1)j_0 + mq(k_0 + \eta + |\boldsymbol{k}|) \leqslant t \Big\}. \end{aligned}$$

The right hand side means that the lattice points does not depend on the order of s_ν with $0 \leqslant \nu \leqslant q^2-1$, concluding the claim we presented by (6). In other words, we have shown that the number of lattice points in $\Gamma_{s_0,(s_1,\cdots,s_{q^2-1}),t}$ does not depend on the order of s_ν with $0 \leqslant \nu \leqslant q^2-1$. It follows from (6) and Lemma 8 that

$$\begin{aligned} \#\Gamma_{0,(s_1,s_2,\cdots,s_{q^2-1}),t} &= \#\Gamma_{s_1,(0,s_2,\cdots,s_{q^2-1}),t} \\ &= \#\Gamma_{0,(0,s_2,\cdots,s_{q^2-1}),t} + qs_1. \end{aligned}$$

By repeated using Lemma 8, we get

$$\#\Gamma_{0,(s_1,s_2,\cdots,s_{q^2-1}),t} = \#\Gamma_{0,(0,0,\cdots,0),t} + q(s_1 + \cdots + s_{q^2-1}),$$

giving the desired formula $\#\Omega_{\mathbf{0},\boldsymbol{s},t} = \#\Omega_{\mathbf{0},\mathbf{0},t} + q|\boldsymbol{s}|$. □

With the above preparations, we are now in a position to give the proof of Lemma 2.

Proof (Proof of Lemma 2) By taking $w := \min_{\substack{0 \leqslant \mu \leqslant q-1 \\ 1 \leqslant \nu \leqslant q^2-1}} \left\{ r_\mu, s_\nu \right\}$, we obtain from the definition that $\Omega_{\boldsymbol{r},\boldsymbol{s},t}$ is equivalent to $\Omega_{\boldsymbol{r'},\boldsymbol{s'},t'}$, where $\boldsymbol{r'} = (r_0 - w, \cdots, r_{q-1} - w)$, $\boldsymbol{s'} = (s_1 - w, \cdots, s_{q^2-1} - w)$ and $t' = t + q^3 w$. By observing that $r_\mu - w \geqslant 0$, $s_\nu - w \geqslant 0$ and $t' \geqslant 2g-1$, we establish from Lemmas 6, 8 and 9 that

$$\begin{aligned} \#\Omega_{\boldsymbol{r'},\boldsymbol{s'},t'} &= \#\Omega_{\mathbf{0},\boldsymbol{s'},t'} + |\boldsymbol{r'}| \\ &= \#\Omega_{\mathbf{0},\mathbf{0},t'} + q|\boldsymbol{s'}| + |\boldsymbol{r'}| \\ &= 1 - g + t' + q|\boldsymbol{s'}| + |\boldsymbol{r'}| \end{aligned}$$

$$= 1 - g + t + q|\boldsymbol{s}| + |\boldsymbol{r}|.$$

On the other hand, $\#\Omega_{\boldsymbol{r},\boldsymbol{s},t} = \#\Omega_{\boldsymbol{r}',\boldsymbol{s}',t'}$. It follows that

$$\#\Omega_{\boldsymbol{r},\boldsymbol{s},t} = 1 - g + t + q|\boldsymbol{s}| + |\boldsymbol{r}|,$$

completing the proof Lemma 2. □

We finish this section with a result that allows us to give a new form of the basis for our Riemann-Roch space $\mathcal{L}(G)$ with $G = \sum_{\mu=0}^{q-1} r_\mu P_\mu + \sum_{\nu=1}^{q^2-1} s_\nu Q_\nu + tP_\infty$. Denote $\boldsymbol{\lambda} := (\lambda_1, \cdots, \lambda_{q-1})$ and $\boldsymbol{\gamma} := (\gamma_1, \cdots, \gamma_{q^2-1})$. For $(u, \boldsymbol{\lambda}, \boldsymbol{\gamma}) \in \mathbb{Z}^{q^2+q-1}$, we define

$$\Lambda_{u,\boldsymbol{\lambda},\boldsymbol{\gamma}} := \tau^u \prod_{\mu=1}^{q-1} f_\mu^{\lambda_\mu} \prod_{\mu=1}^{q^2-1} h_\nu^{\gamma_\nu},$$

where $\tau := \dfrac{z^{q^{n-3}}}{x - \alpha_0}$, $f_\mu := \dfrac{x - \alpha_\mu}{x - \alpha_0}$ for $\mu \geqslant 1$, and $h_\nu := \dfrac{y - \beta_\nu}{y - \beta_0}$ for $\nu \geqslant 1$. The divisor of $\Lambda_{u,\boldsymbol{\lambda},\boldsymbol{\gamma}}$ is computed from Proposition 1 that

$$\begin{aligned}
\mathrm{div}(\Lambda_{u,\boldsymbol{\lambda},\boldsymbol{\gamma}}) =& \sum_{\mu=1}^{q-1} \Big(q^{n-3}u + m(q+1)\lambda_\mu - m|\boldsymbol{\gamma}|\Big) P_\mu + \sum_{\nu=1}^{q^2-1} (q^{n-3}u + m\gamma_\nu) Q_\nu \\
& - \Big((m(q+1) - q^{n-3})u + m(q+1)|\boldsymbol{\lambda}| + m|\boldsymbol{\gamma}|\Big) P_0 + uP_\infty.
\end{aligned}$$

There is a close relationship between the elements $\Lambda_{u,\boldsymbol{\lambda},\boldsymbol{\gamma}}$ and $E_{i,\boldsymbol{j},\boldsymbol{k}}$ explored as follows.

Corollary 1 *Let $G := \sum_{\mu=0}^{q-1} r_\mu P_\mu + \sum_{\nu=1}^{q^2-1} s_\nu Q_\nu + tP_\infty$. Then the elements $\Lambda_{u,\boldsymbol{\lambda},\boldsymbol{\gamma}}$ with $(u, \boldsymbol{\lambda}, \boldsymbol{\gamma}) \in \Theta_{\boldsymbol{r},\boldsymbol{s},t}$ form a basis for the Riemann-Roch space $\mathcal{L}(G)$, where the set $\Theta_{\boldsymbol{r},\boldsymbol{s},t}$ is given by*

$$\begin{aligned}
&\Big\{(u, \boldsymbol{\lambda}, \boldsymbol{\gamma}) \Big| u \geqslant -t, \\
&\quad 0 \leqslant q^{n-3}u + m\gamma_\nu + s_\nu < m \text{ for } \nu = 1, \cdots, q^2 - 1 \\
&\quad 0 \leqslant q^{n-3}u + m(q+1)\lambda_\mu - m|\boldsymbol{\gamma}| + r_\mu < m(q+1) \text{ for } \mu = 1, \cdots, q-1, \\
&\quad (m(q+1) - q^{n-3})u + m(q+1)|\boldsymbol{\lambda}| + m|\boldsymbol{\gamma}| \leqslant r_0 \Big\}.
\end{aligned} \tag{7}$$

In addition we have $\#\Theta_{\boldsymbol{r},\boldsymbol{s},t} = \#\Omega_{\boldsymbol{r},\boldsymbol{s},t}$.

Proof It suffices to prove that the set

$$\Big\{\Lambda_{u,\boldsymbol{\lambda},\boldsymbol{\gamma}} \Big| (u, \boldsymbol{\lambda}, \boldsymbol{\gamma}) \in \Theta_{\boldsymbol{r},\boldsymbol{s},t}\Big\}$$

equals the set

$$\Big\{E_{i,\boldsymbol{j},\boldsymbol{k}} \Big| (i, \boldsymbol{j}, \boldsymbol{k}) \in \Omega_{\boldsymbol{r},\boldsymbol{s},t}\Big\}.$$

In fact, for fixed $(u, \boldsymbol{\lambda}, \boldsymbol{\gamma}) \in \mathbb{Z}^{q^2+q-1}$, we obtain $\Lambda_{u,\boldsymbol{\lambda},\boldsymbol{\gamma}}$ equals $E_{i,\boldsymbol{j},\boldsymbol{k}}$ with

$$\begin{aligned} i &= -(m(q+1) - q^{n-3})u - m(q+1)|\boldsymbol{\lambda}| - m|\boldsymbol{\gamma}|, \\ j_\mu &= u + |\boldsymbol{\lambda}| + \lambda_\mu \text{ for } \mu = 1, \cdots, q-1, \\ k_\nu &= (q+1)(u + |\boldsymbol{\lambda}|) + |\boldsymbol{\gamma}| + \gamma_\nu \text{ for } \nu = 1, \cdots, q^2 - 1. \end{aligned}$$

On the contrary, if we set

$$\begin{aligned} u &= -q^3 i - m(q+1)|\boldsymbol{j}| - mq|\boldsymbol{k}|, \\ \lambda_\mu &= q^2 i + q^{n-1}|\boldsymbol{j}| + m|\boldsymbol{k}| + j_\mu \text{ for } \mu = 1, \cdots, q-1, \\ \gamma_\nu &= (q+1)(i + q^{n-3}|\boldsymbol{j}|) + q^{n-2}|\boldsymbol{k}| + k_\nu \text{ for } \nu = 1, \cdots, q^2 - 1, \end{aligned}$$

then $E_{i,\boldsymbol{j},\boldsymbol{k}}$ is exactly the element $\Lambda_{u,\boldsymbol{\lambda},\boldsymbol{\gamma}}$. Therefore, if we restrict $(i, \boldsymbol{j}, \boldsymbol{k})$ in $\Omega_{\boldsymbol{r},\boldsymbol{s},t}$, then we must have $(u, \boldsymbol{\lambda}, \boldsymbol{\gamma})$ is in $\Theta_{\boldsymbol{r},\boldsymbol{s},t}$ and vice versa. This completes the proof of the claim and hence of this corollary. □

In the following, we will demonstrate an interesting property of $\#\Omega_{\boldsymbol{r},\boldsymbol{s},t}$ for GK curves.

Corollary 2 *Let $n = 3$ and $|\gamma|$ be given as in Corollary 1. Suppose that $|\boldsymbol{\gamma}|$ is divisible by $q+1$. Then lattice point set $\Omega_{\boldsymbol{r},\boldsymbol{s},t}$ is symmetric with respect to $r_0, r_1, \cdots, r_{q-1}, t$. In other words, we have $\#\Omega_{\boldsymbol{r},\boldsymbol{s},t} = \#\Omega_{\boldsymbol{r}',\boldsymbol{s},t'}$, where the sequences $(r_i)_{i=0}^q$ is equal to $(r_i')_{i=0}^q$ up to permutation by putting $r_q := t$ and $r_q' := t'$.*

Proof Denote $\boldsymbol{r} := (r_0, \tilde{\boldsymbol{r}}) = (r_0, r_1, \cdots, r_{q-1})$ and $\Omega_{(r_0,\tilde{\boldsymbol{r}}),\boldsymbol{s},t} := \Omega_{\boldsymbol{r},\boldsymbol{s},t}$. It follows from Lemma 7 that the only thing we need to prove is that

$$\#\Omega_{(r_0,\tilde{\boldsymbol{r}}),\boldsymbol{s},t} = \#\Theta_{(r_0,\tilde{\boldsymbol{r}}),\boldsymbol{s},t} = \#\Omega_{(t,\tilde{\boldsymbol{r}}),\boldsymbol{s},r_0}.$$

The first identity follows directly from Corollary 1. Applying Corollary 1 again gives the set $\Theta_{(r_0,\tilde{\boldsymbol{r}}),\boldsymbol{s},t}$ as

$$\begin{aligned} &\Big\{(u, \boldsymbol{\lambda}, \boldsymbol{\gamma})\Big| u + t \geqslant 0, \\ &0 \leqslant u + m\gamma_\nu + s_\nu < m \text{ for } \nu = 1, \cdots, q^2 - 1, \\ &0 \leqslant u + m(q+1)\lambda_\mu - m|\boldsymbol{\gamma}| + r_\mu < m(q+1) \text{ for } \mu = 1, \cdots, q-1, \\ &q^3 u + m(q+1)|\boldsymbol{\lambda}| + m|\boldsymbol{\gamma}| \leqslant r_0\Big\}. \end{aligned}$$

Take $i := u$, $j_\mu := \lambda_\mu - \dfrac{|\gamma|}{q+1}$ for $\mu \geqslant 1$ and $k_\nu := \gamma_\nu$ for $\nu \geqslant 1$. Then $\Theta_{(r_0,\tilde{\boldsymbol{r}}),\boldsymbol{s},t}$ is equivalent to

$$\begin{aligned} &\Big\{(i, \boldsymbol{j}, \boldsymbol{k})\Big| i + t \geqslant 0, \\ &0 \leqslant i + mk_\nu + s_\nu < m \text{ for } \nu = 1, \cdots, q^2 - 1, \\ &0 \leqslant i + m(q+1)j_\mu + r_\mu < m(q+1) \text{ for } \mu = 1, \cdots, q-1, \\ &q^3 i + m(q+1)|\boldsymbol{j}| + m|\boldsymbol{k}| \leqslant r_0\Big\}. \end{aligned}$$

The right-hand side is exactly $\Omega_{(t,\tilde{\boldsymbol{r}}),\boldsymbol{s},r_0}$ by definition. Hence the second identity is just shown, completing the proof. □

4 Weierstrass semigroups and pure gap sets

In this section, we always make the assumption that $G := \sum_{\mu=0}^{q-1} r_\mu P_\mu + tP_\infty$ and denote $\boldsymbol{r} = (r_0, r_1, \cdots, r_{q-1})$. The main purpose of this section is to calculate the Weierstrass semigroups and the pure gap sets at totally ramified places $P_0, P_1, \cdots, P_{q-1}, P_\infty$, which will require auxiliary results described below.

In the following, we denote $\Omega_{\boldsymbol{r},\boldsymbol{0},t}$ by $\Omega_{(r_0,r_1,\cdots,r_{q-1}),t}$ for the clarity of description.

Lemma 10 *For the lattice point set $\Omega_{(r_0,r_1,\cdots,r_{q-1}),t}$, we have the following assertions.*

1. $\#\Omega_{(r_0,r_1,\cdots,r_{q-1}),t} = \#\Omega_{(r_0-1,r_1,\cdots,r_{q-1}),t} + 1$ *if and only if*
$$\sum_{\mu=1}^{q-1} \left\lceil \frac{r_0 - r_\mu}{m(q+1)} \right\rceil + q(q-1)\left\lceil \frac{r_0}{m} \right\rceil \leqslant \frac{t + q^3 r_0}{m(q+1)}.$$
2. $\#\Omega_{(r_0,r_1,\cdots,r_{q-1}),t} = \#\Omega_{(r_0,r_1,\cdots,r_{q-1}),t-1} + 1$ *if and only if*
$$\sum_{\mu=1}^{q-1} \left\lceil \frac{q^{n-3}t - r_\mu}{m(q+1)} \right\rceil + q(q-1)\left\lceil \frac{q^{n-3}t}{m} \right\rceil \leqslant t + \frac{r_0 - q^{n-3}t}{m(q+1)}.$$

Proof Consider two lattice point sets $\Omega_{(r_0,r_1,\cdots,r_{q-1}),t}$ and $\Omega_{(r_0-1,r_1,\cdots,r_{q-1}),t}$, which are given in Equation (4). Clearly, the latter one is a subset of the former one, and the complementary set Φ of $\Omega_{(r_0-1,r_1,\cdots,r_{q-1}),t}$ in $\Omega_{(r_0,r_1,\cdots,r_{q-1}),t}$ is given by

$$\begin{aligned}\Phi :=\Big\{(i,\boldsymbol{j},\boldsymbol{k})\Big|\, & i + r_0 = 0,\\ & j_\mu = \left\lceil \frac{-i - r_\mu}{m(q+1)} \right\rceil \text{ for } \mu = 1,\cdots,q-1,\\ & k_\nu = \left\lceil \frac{-i}{m} \right\rceil \text{ for } \nu = 1,\cdots,q^2-1,\\ & q^3 i + m(q+1)|\boldsymbol{j}| + mq|\boldsymbol{k}| \leqslant t\Big\}.\end{aligned}$$

It follows immediately that the set Φ is not empty if and only if

$$-q^3 r_0 + m(q+1)\sum_{\mu=1}^{q-1}\left\lceil \frac{r_0 - r_\mu}{m(q+1)} \right\rceil + mq(q^2-1)\left\lceil \frac{r_0}{m} \right\rceil \leqslant t,$$

which concludes the desired assertion.

For the second assertion, we obtain from Corollary 1 that the difference between $\#\Omega_{(r_0,r_1,\cdots,r_{q-1}),t}$ and $\#\Omega_{(r_0,r_1,\cdots,r_{q-1}),t-1}$ is exactly the same as the one between $\#\Theta_{\boldsymbol{r},\boldsymbol{0},t}$ and $\#\Theta_{\boldsymbol{r},\boldsymbol{0},t-1}$. Similar to the argument of the first assertion, we define Ψ as the complementary set of $\Theta_{\boldsymbol{r},\boldsymbol{0},t-1}$ in $\Theta_{\boldsymbol{r},\boldsymbol{0},t}$, namely

$$\Psi := \Big\{(u,\boldsymbol{\lambda},\boldsymbol{\gamma})\Big| u = -t,$$

$$0 \leqslant q^{n-3}u + m\gamma_\nu < m \text{ for } \nu = 1, \cdots, q^2 - 1,$$
$$0 \leqslant q^{n-3}u + m(q+1)\lambda_\mu - m|\boldsymbol{\gamma}| + r_\mu < m(q+1) \text{ for } \mu = 1, \cdots, q-1,$$
$$-\Big((m(q+1) - q^{n-3})u + m(q+1)|\boldsymbol{\lambda}| + m|\boldsymbol{\gamma}|\Big) + r_0 \geqslant 0\Big\}.$$

The set Ψ is not empty if and only if

$$m(q+1)\sum_{\mu=1}^{q-1}\left\lceil \frac{q^{n-3}t - r_\mu}{m(q+1)} \right\rceil + mq(q^2-1)\left\lceil \frac{q^{n-3}t}{m} \right\rceil \leqslant r_0 + (q^n + 1 - q^{n-3})t,$$

completing the proof of the second assertion. □

We are now ready for the main results of the section dealing with the Weierstrass semigroups and the pure gap sets, which play an interesting role in finding codes with good parameters. For convenience, we define

$$W_j(\boldsymbol{r}_l, t, l) := \sum_{\substack{i=0\\ i\neq j}}^{l}\left\lceil \frac{r_j - r_i}{m(q+1)} \right\rceil + (q-1-l)\left\lceil \frac{r_j}{m(q+1)} \right\rceil + q(q-1)\left\lceil \frac{r_j}{m} \right\rceil - \frac{t + q^3 r_j}{m(q+1)},$$

for $j \neq \infty$, and

$$W_\infty(\boldsymbol{r}_l, t, l) := \sum_{i=1}^{l}\left\lceil \frac{q^{n-3}t - r_i}{m(q+1)} \right\rceil + (q-1-l)\left\lceil \frac{q^{n-3}t}{m(q+1)} \right\rceil + q(q-1)\left\lceil \frac{q^{n-3}t}{m} \right\rceil - t - \frac{r_0 - q^{n-3}t}{m(q+1)},$$

where $\boldsymbol{r}_l = (r_0, r_1, \cdots, r_l)$.

Theorem 2 *Let $P_0, P_1, \cdots, P_l$ be the rational places defined previously. For $0 \leqslant l < q$, the following assertions hold.*

(1) *The Weierstrass semigroup $H(P_0, P_1, \cdots, P_l)$ is given by*

$$\Big\{(r_0, r_1, \cdots, r_l) \in \mathbb{N}_0^{l+1} \Big| W_j(\boldsymbol{r}_l, 0, l) \leqslant 0 \textit{ for } 0 \leqslant j \leqslant l\Big\}.$$

(2) *The Weierstrass semigroup $H(P_0, P_1, \cdots, P_l, P_\infty)$ is given by*

$$\Big\{(r_0, r_1, \cdots, r_l, t) \in \mathbb{N}_0^{l+2} \Big| W_j(\boldsymbol{r}_l, t, l) \leqslant 0 \textit{ for } 0 \leqslant j \leqslant l \textit{ and } j = \infty\Big\}.$$

(3) *The pure gap set $G_0(P_0, P_1, \cdots, P_l)$ is given by*

$$\Big\{(r_0, r_1, \cdots, r_l) \in \mathbb{N}^{l+1} \Big| W_j(\boldsymbol{r}_l, 0, l) > 0 \textit{ for } 0 \leqslant j \leqslant l\Big\}.$$

(4) *The pure gap set $G_0(P_0, P_1, \cdots, P_l, P_\infty)$ is given by*

$$\Big\{(r_0, r_1, \cdots, r_l, t) \in \mathbb{N}_0^{l+2} \Big| W_j(\boldsymbol{r}_l, t, l) > 0 \textit{ for } 0 \leqslant j \leqslant l \textit{ and } j = \infty\Big\}.$$

Proof The desired conclusions follow from Theorem 1, Lemmas 1, 7 and 10. □

The following corollary gives the descriptions of the Weierstrass semigroup and gaps at only one point.

Corollary 3 *With notation as before, we have the following statements.*

(1) $H(P_0) = \left\{ k \in \mathbb{N}_0 \middle| (q-1)\left\lceil \frac{k}{m(q+1)} \right\rceil + q(q-1)\left\lceil \frac{k}{m} \right\rceil \leqslant \frac{q^3 k}{m(q+1)} \right\}.$

(2) *Let $\alpha, \beta, \gamma \in \mathbb{Z}$. Then $\alpha + m(\beta + (q+1)\gamma) \in \mathbb{N}$ is a gap at P_0 if and only if exactly one of the following two conditions is satisfied:*
(i) $\alpha = 0, 0 < \beta \leqslant q-1, 0 \leqslant \gamma \leqslant q-1-\beta$.
(ii) $0 < \alpha < m, 0 \leqslant \beta \leqslant q, 0 \leqslant \gamma \leqslant q^2 - 1 - \beta + \left\lfloor \frac{\beta}{q+1} - \frac{q^3\alpha}{m(q+1)} \right\rfloor$ and $\beta - \left\lfloor \frac{\beta}{q+1} - \frac{q^3\alpha}{m(q+1)} \right\rfloor \leqslant q^2 - 1$.

Proof The first statement is an immediate consequence of Theorem 2 (1).

We now focus on the second statement. It follows from Theorem 2 (3) that the Weierstrass gap set at P_0 is

$$G(P_0) = \left\{ k \in \mathbb{N} \middle| (q-1)\left\lceil \frac{k}{m(q+1)} \right\rceil + q(q-1)\left\lceil \frac{k}{m} \right\rceil > \frac{q^3 k}{m(q+1)} \right\}.$$

Let $k \in G(P_0)$ and write $k = \alpha + m(\beta + (q+1)\gamma)$, where $0 \leqslant \alpha < m$, $0 \leqslant \beta \leqslant q$ and $\gamma \geqslant 0$. We find that the case $\alpha + m\beta = 0$ does not occur, since otherwise we have $k = m(q+1)\gamma$ and

$$\begin{aligned}
&(q-1)\left\lceil \frac{k}{m(q+1)} \right\rceil + q(q-1)\left\lceil \frac{k}{m} \right\rceil - \frac{q^3 k}{m(q+1)} \\
&= (q-1)\gamma + q(q-1)(q+1)\gamma - q^3\gamma \\
&= -\gamma \leqslant 0,
\end{aligned}$$

which contradicts to the fact $k \in G(P_0)$. So $\alpha + m\beta \neq 0$. There are two possibilities.

(i) If $\alpha = 0$, then $0 < \beta \leqslant q$. In this case, $k = m\beta + m(q+1)\gamma$ is a gap at P_0 if and only if

$$(q-1)\left\lceil \frac{k}{m(q+1)} \right\rceil + q(q-1)\left\lceil \frac{k}{m} \right\rceil > \frac{q^3 k}{m(q+1)},$$

or equivalently,

$$(q-1)(\gamma+1) + q(q-1)(\beta + (q+1)\gamma) > q^3\gamma + \frac{q^3\beta}{q+1},$$

leading to the first condition $0 \leqslant \gamma \leqslant q-1-\beta$ and $0 < \beta \leqslant q-1$.

(*ii*) If $0 < \alpha < m$, then $0 \leqslant \beta \leqslant q$. In this case, we have similarly that $k = \alpha + m\beta + m(q+1)\gamma$ is a gap at P_0 if and only if

$$(q-1)(\gamma+1) + q(q-1)(1+\beta+(q+1)\gamma) > q^3\gamma + \frac{q^3\alpha}{m(q+1)} + \frac{q^3\beta}{q+1},$$

which gives the second condition $0 \leqslant \gamma \leqslant q^2 - 1 - \beta + \left\lfloor \frac{\beta}{q+1} - \frac{q^3\alpha}{m(q+1)} \right\rfloor$. Note that

$$q^2 - 1 - \beta + \left\lfloor \frac{\beta}{q+1} - \frac{q^3\alpha}{m(q+1)} \right\rfloor \geqslant q^2 - 1 - q - 1 \geqslant 0.$$

The proof is finished. □

5 The floor of divisors

In this section, we investigate the floor of divisors of function fields. The significance of this concept is that it provides a useful tool for evaluating parameters of AG codes. We begin with general function fields.

Definition 2 ([22]) Given a divisor G of a function field $F/\mathbb{F}_q$ with $\ell(G) > 0$, the floor of G is the unique divisor G' of F of minimum degree such that $\mathcal{L}(G) = \mathcal{L}(G')$. The floor of G will be denoted by $\lfloor G \rfloor$.

The floor of a divisor can be used to characterize Weierstrass semigroups and pure gap sets. Let $G = s_1Q_1 + \cdots + s_lQ_l$. It is not hard to see that $(s_1, \cdots, s_l) \in H(Q_1, \cdots, Q_l)$ if and only if $\lfloor G \rfloor = G$. Moreover, $(s_1, \cdots, s_l)$ is a pure gap at $(Q_1, \cdots, Q_l)$ if and only if

$$\lfloor G \rfloor = \lfloor (s_1-1)Q_1 + \cdots + (s_l-1)Q_l \rfloor.$$

Maharaj, Matthews and Pirsic in [22] defined the floor of a divisor and characterized it by the basis of the Riemann-Roch space.

Theorem 3 ([22]) *Let G be a divisor of the function field $F/\mathbb{F}_q$ and let $b_1, \cdots, b_t \in \mathcal{L}(G)$ be a spanning set for $\mathcal{L}(G)$. Then*

$$\lfloor G \rfloor = -\gcd\left\{ \operatorname{div}(b_i) \middle| i = 1, \cdots, t \right\}.$$

The next theorem extends Theorem **??**, which shows the lower bound of minimum distance in a more general situation.

Theorem 4 ([22]) *Assume that $F/\mathbb{F}_q$ is a function field with genus g. Let $D := Q_1 + \cdots + Q_N$ where $Q_1, \cdots, Q_N$ are distinct rational places of F, and let $G := H + \lfloor H \rfloor$ be a divisor of F such that H is an effective divisor whose support does not contain any of the places $Q_1, \cdots, Q_N$. Then the minimum distance of $C_\Omega(D, G)$ satisfies*

$$d_\Omega \geqslant 2\deg(H) - (2g-2).$$

The following theorem provides a characterization of the floor over GGS curves, which can be viewed as a generalization of Theorem 3.9 in [22] related to Hermitian function fields.

Theorem 5 *Let $H := \sum_{\mu=0}^{q-1} r_\mu P_\mu + \sum_{\nu=1}^{q^2-1} s_\nu Q_\nu + tP_\infty$ be a divisor of GGS curve given by (1). Then the floor of H is given by*

$$\lfloor H \rfloor = \sum_{\mu=0}^{q-1} r'_\mu P_\mu + \sum_{\nu=1}^{q^2-1} s'_\nu Q_\nu + t' P_\infty,$$

where

$$\begin{aligned} r'_0 &= \max\left\{ -i \,\middle|\, (i,\boldsymbol{j},\boldsymbol{k}) \in \Omega_{\boldsymbol{r},\boldsymbol{s},t} \right\}, \\ r'_\mu &= \max\left\{ -i - m(q+1)j_\mu \,\middle|\, (i,\boldsymbol{j},\boldsymbol{k}) \in \Omega_{\boldsymbol{r},\boldsymbol{s},t} \right\} \text{ for } \mu = 1,\cdots,q-1, \\ s'_\nu &= \max\left\{ -i - mk_\nu \,\middle|\, (i,\boldsymbol{j},\boldsymbol{k}) \in \Omega_{\boldsymbol{r},\boldsymbol{s},t} \right\} \text{ for } \nu = 1,\cdots,q^2-1, \\ t' &= \max\left\{ q^3 i + m(q+1)|\boldsymbol{j}| + mq|\boldsymbol{k}| \,\middle|\, (i,\boldsymbol{j},\boldsymbol{k}) \in \Omega_{\boldsymbol{r},\boldsymbol{s},t} \right\}. \end{aligned}$$

Proof Let $H = \sum_{\mu=0}^{q-1} r_\mu P_\mu + \sum_{\nu=1}^{q^2-1} s_\nu Q_\nu + tP_\infty$. It follows from Theorem 1 that the elements $E_{i,\boldsymbol{j},\boldsymbol{k}}$ of Equation (2) with $(i,\boldsymbol{j},\boldsymbol{k}) \in \Omega_{\boldsymbol{r},\boldsymbol{s},t}$ form a basis for the Riemann-Roch space $\mathcal{L}(H)$. Note that the divisor of $E_{i,\boldsymbol{j},\boldsymbol{k}}$ is

$$\begin{aligned} &iP_0 + \sum_{\mu=1}^{q-1} (i + m(q+1)j_\mu) P_\mu + \sum_{\nu=1}^{q^2-1} (i + mk_\nu) Q_\nu \\ &- \left(q^3 i + m(q+1)|\boldsymbol{j}| + mq|\boldsymbol{k}|\right) P_\infty \end{aligned}$$

By Theorem 3, we get that

$$\lfloor H \rfloor = -\gcd\left\{ \operatorname{div}(E_{i,\boldsymbol{j},\boldsymbol{k}}) \,\middle|\, (i,\boldsymbol{j},\boldsymbol{k}) \in \Omega_{\boldsymbol{r},\boldsymbol{s},t} \right\}.$$

The desired conclusion then follows. □

6 The AG codes from GGS curves

In this section, we will we study the linear code $C_{\mathcal{L}}(D,G)$ with $D := \sum_{\substack{\alpha,\beta,\gamma \\ \gamma \neq 0}} \mathcal{P}_{\alpha,\beta,\gamma}$ and $G := \sum_{\mu=0}^{q-1} r_\mu P_\mu + \sum_{\nu=1}^{q^2-1} s_\nu Q_\nu + tP_\infty$. The length of $C_{\mathcal{L}}(D,G)$ is

$$N := \deg(D) = q^{n+2}(q^n - q + 1) - q^3.$$

It is well known that the dimension of $C_{\mathcal{L}}(D,G)$ is given by

$$\dim C_{\mathcal{L}}(D,G) = \ell(G) - \ell(G-D). \tag{8}$$

Set $R := N + 2g - 2$. Since $\deg(G) > R$, then we deduce from the Riemann-Roch Theorem and (8) that

$$\begin{aligned}\dim C_{\mathcal{L}}(D,G) &= (1-g+\deg(G)) - (1-g+\deg(G-D)) \\ &= \deg(G) - \deg(G-D) = N,\end{aligned}$$

which implies that $C_{\mathcal{L}}(D,G)$ is trivial. So we only consider the case $0 \leqslant \deg(G) \leqslant R$.

Now, we use the following lemmas to calculate the dual of $C_{\mathcal{L}}(D,G)$.

Lemma 11 (Proposition 2.2.10, [27]) *Let τ be an element of the function field of the curve $\mathcal{X}$ such that $v_{P_i}(\tau) = 1$ for all rational places P_i contained in the divisor D. Then the dual of $C_{\mathcal{L}}(D,G)$ is*

$$C_{\mathcal{L}}(D,G)^{\perp} = C_{\mathcal{L}}(D, D - G + \mathrm{div}(d\tau) - \mathrm{div}(\tau)).$$

Lemma 12 (Proposition 2.2.14, [27]) *Suppose G_1 and G_2 are divisors with $G_1 = G_2 + div(\rho)$ for some $\rho \in F\backslash\{0\}$ and $\operatorname{supp} G_1 \cap \operatorname{supp} D = \operatorname{supp} G_2 \cap \operatorname{supp} D = \varnothing$. Let $N := \deg(D)$ and $\varrho := (\rho(P_1), \cdots, \rho(P_N))$ with $P_i \in D$. Then the codes $C_{\mathcal{L}}(D,G_1)$ and $C_{\mathcal{L}}(D,G_2)$ are equivalent and*

$$C_{\mathcal{L}}(D,G_2) = \varrho \cdot C_{\mathcal{L}}(D,G_1).$$

Theorem 6 *Let $A := (q^n+1)(q-1)-1$, $B := mq^2(q^n-q^3)+(q^n+1)(q^2-1)-1$ and $\rho := 1 + \sum_{i=1}^{\frac{n-3}{2}} z^{(q^n+1)(q-1)\sum_{j=1}^{i} q^{2j}}$. Then the dual code of $C_{\mathcal{L}}(D,G)$ is given as follows.*

(i) The dual of $C_{\mathcal{L}}(D,G)$ is represented as

$$C_{\mathcal{L}}(D,G)^{\perp} = \varrho \cdot C_{\mathcal{L}}(D, \sum_{\mu=0}^{q-1}(A - r_{\mu})P_{\mu} + \sum_{\nu=1}^{q^2-1}(A - s_{\nu})Q_{\nu} + (B-t)P_{\infty}),$$

where $\varrho := (\rho(\mathcal{P}_{\alpha_1,\beta_1,\gamma_1}), \cdots, \rho(\mathcal{P}_{\alpha_N,\beta_N,\gamma_N}))$ with $\mathcal{P}_{\alpha_i,\beta_i,\gamma_i} \in D$.

(ii) In particular, for $n = 3$, we have $\rho = 1$ and

$$C_{\mathcal{L}}(D,G)^{\perp} = C_{\mathcal{L}}(D, \sum_{\mu=0}^{q-1}(A - r_{\mu})P_{\mu} + \sum_{\nu=1}^{q^2-1}(A - s_{\nu})Q_{\nu} + (B-t)P_{\infty}).$$

Proof Define

$$H := \left\{ z \in \mathbb{F}_{q^{2n}}^{*} \,\middle|\, \exists y \in \mathbb{F}_{q^{2n}} \text{ with } y^{q^2} - y = z^m \right\}.$$

Consider the element

$$\tau := \prod_{\gamma \in H} (z - \gamma).$$

Then τ is a prime element for all places $\mathcal{P}_{\alpha,\beta,\gamma}$ in D and its divisor is

$$\operatorname{div}(\tau) = \sum_{\gamma \in H} \operatorname{div}(z-\gamma) = D - \deg(D) P_\infty,$$

where $D = \sum_{\substack{\alpha,\beta,\gamma \\ \gamma \neq 0}} \mathcal{P}_{\alpha,\beta,\gamma}$ and $N = \deg(D) = q^{n+2}(q^n - q + 1) - q^3$. Moreover by a same discussion as in the proof of Lemma 2 in [1], we have

$$\tau = 1 + \sum_{i=0}^{k-1} w^{\sum_{j=0}^{i} q^{2j} + \sum_{j=0}^{k-1} q^{2j+1}} + \sum_{i=0}^{k-1} w^{\sum_{j=0}^{i} q^{2j+1}},$$

where $n = 2k+1$ (note that $n > 1$ is odd) and $w = z^{(q^n+1)(q-1)}$. Then a straightforward computation shows

$$\begin{aligned} d\tau &= w^{\sum_{j=0}^{k-1} q^{2j+1}} \Big(1 + \sum_{i=1}^{k-1} w^{\sum_{j=1}^{i} q^{2j}}\Big) dw \\ &= w^{\frac{q^n - q}{q^2-1}} \Big(1 + \sum_{i=1}^{k-1} w^{\sum_{j=1}^{i} q^{2j}}\Big) dw, \\ dw &= -z^{(q^n+1)(q-1)-1} dz. \end{aligned}$$

Let $\rho := 1 + \sum_{i=1}^{k-1} w^{\sum_{j=1}^{i} q^{2j}}$ and denote its divisor by $\operatorname{div}(\rho)$. Set

$$\begin{aligned} A &:= m(q^n - q) + (q^n + 1)(q-1) - 1, \\ S &:= q^3 A - 2g + 2. \end{aligned}$$

Since $\operatorname{div}(dz) = (2g-2)P_\infty$ (see Lemma 3.8 of [13]), it follows from Proposition 1 that

$$\begin{aligned} \operatorname{div}(d\tau) &= A \cdot \operatorname{div}(z) + \operatorname{div}(dz) + \operatorname{div}(\rho) \\ &= A \sum_{\beta \in \mathbb{F}_{q^2}} Q_\beta - \Big(q^3 A - 2g + 2\Big) P_\infty + \operatorname{div}(\rho) \\ &= A \sum_{\mu=0}^{q-1} P_\mu + A \sum_{\nu=1}^{q^2-1} Q_\nu - S P_\infty + \operatorname{div}(\rho). \end{aligned}$$

Let $\eta := d\tau/\tau$ be a Weil differential. The divisor of η is

$$\begin{aligned} \operatorname{div}(\eta) &= \operatorname{div}(d\tau) - \operatorname{div}(\tau) \\ &= A \sum_{\mu=0}^{q-1} P_\mu + A \sum_{\nu=1}^{q^2-1} Q_\nu - D + \Big(\deg(D) - S\Big) P_\infty + \operatorname{div}(\rho). \end{aligned}$$

By writing $B := \deg(D) - S = mq^2(q^n - q^3) + (q^n + 1)(q^2 - 1) - 1$, we establish from Lemma 11 that the dual of $C_{\mathcal{L}}(D, G)$ is

$$C_{\mathcal{L}}(D, G)^\perp = C_{\mathcal{L}}(D, D - G + \operatorname{div}(\eta))$$

$$= C_{\mathcal{L}}(D, \sum_{\mu=0}^{q-1}(A-r_\mu)P_\mu + \sum_{\nu=1}^{q^2-1}(A-s_\nu)Q_\nu + (B-t)P_\infty + \mathrm{div}(\rho)).$$

By writing $\varrho := (\rho(\mathcal{P}_{\alpha_1,\beta_1,\gamma_1}), \cdots, \rho(\mathcal{P}_{\alpha_N,\beta_N,\gamma_N}))$ with $\mathcal{P}_{\alpha_i,\beta_i,\gamma_i} \in D$, we deduce the first statement from Lemma 12. The second statement then follows immediately. □

Theorem 7 *Suppose that* $0 \leqslant \deg(G) \leqslant R$. *Then the dimension of* $C_{\mathcal{L}}(D, G)$ *is given by*

$$\dim C_{\mathcal{L}}(D,G) = \begin{cases} \#\Omega_{\boldsymbol{r},\boldsymbol{s},t} & \text{if } 0 \leqslant \deg(G) < N, \\ N - \#\Omega^{\perp}_{\boldsymbol{r},\boldsymbol{s},t} & \text{if } N \leqslant \deg(G) \leqslant R, \end{cases}$$

where $\Omega^{\perp}_{\boldsymbol{r},\boldsymbol{s},t} := \Omega_{\boldsymbol{r'},\boldsymbol{s'},B-t}$ *with* $\boldsymbol{r'} = (A - r_0, \cdots, A - r_{q-1})$ *and* $\boldsymbol{s'} = (A - s_1, \cdots, A - s_{q^2-1})$.

Proof For $0 \leqslant \deg(G) < N$, we have by Theorem 1 and Equation (8) that

$$\dim C_{\mathcal{L}}(D,G) = \ell(G) = \#\Omega_{\boldsymbol{r},\boldsymbol{s},t}.$$

For $N \leqslant \deg(G) \leqslant R$, Theorem 6 yields that

$$\dim C_{\mathcal{L}}(D,G) = N - \dim C_{\mathcal{L}}(D,G)^{\perp} = N - \#\Omega^{\perp}_{\boldsymbol{r},\boldsymbol{s},t}.$$

So the proof is completed. □

7 Examples of codes on GGS curves

In this section we treat several examples of codes to illustrate our results. The codes in the next example will give new records of better parameters than the corresponding ones in MinT's tables [25].

Example 1 Now, we study codes arising from GK curves, that is, we let $q = 2$ and $n = 3$ in (1) given at the beginning of Section 3. This curve has 225 $\mathbb{F}_{64}$-rational points and its genus is $g = 10$. Here we will study multi-point AG codes from this curve by employing our previous results. Let us take $H = 3P_0 + 4P_1 + 11P_\infty$ for example. Then it can be computed from Equation (4) that the elements $(-i, -i-m(q+1)j_1, -i-mk_1, -i-mk_2, -i-mk_3, q^3 i + m(q+1)j_1 + mq(k_1+k_2+k_3))$, with $(i, j_1, k_1, k_2, k_3) \in \Omega_{3,4,0,0,0,11}$, are as follows

$$\begin{aligned}
&(\ \ 3,\ \ 3,\ \ 0,\ \ 0,\ \ 0, -6),\\
&(\ \ 2,\ \ 2, -1, -1, -1,\ \ 2),\\
&(\ \ 1,\ \ 1, -2, -2, -2, 10),\\
&(\ \ 0,\ \ 0,\ \ 0,\ \ 0,\ \ 0,\ \ 0),\\
&(-1, -1, -1, -1, -1,\ \ 8),
\end{aligned}$$

$$\begin{array}{l}(-3,-3,\ \ 0,\ \ 0,\ \ 0,\ 6),\\(-6,\ \ 3,\ \ 0,\ \ 0,\ \ 0,\ 3),\\(-7,\ \ 2,-1,-1,-1,11),\\(-9,\ \ 0,\ \ 0,\ \ 0,\ \ 0,\ 9).\end{array}$$

So we obtain from Theorem 5 that $\lfloor H \rfloor = 3P_0 + 3P_1 + 11P_\infty$. Let D be a divisor consisting of $N = 216$ rational places away from the places P_0, P_1, Q_1, Q_2, Q_3 and P_∞. According to Theorem 4, if we let $G = H + \lfloor H \rfloor = 6P_0 + 7P_1 + 22P_\infty$, then the code $C_\Omega(D, G)$ has minimum distance at least $2\deg(H) - (2g - 2) = 18$. Since $2g - 2 < \deg(G) < N$, the dimension of $C_\Omega(D, G)$ is $k_\Omega = N + g - 1 - \deg(G) = 190$. In other words, the code $C_\Omega(D, G)$ has parameters $[216, 190, \geqslant 18]$. One can verify that our resulting code improve the minimum distance with respect to MinT's Tables. Up to equivalence, by Theorem 6 the code $C_\Omega(D, G)$ is dual to $C_\mathcal{L}(D, G')$, where $G' = 2P_0 + P_1 + 8Q_1 + 8Q_2 + 8Q_3 + 4P_\infty$.

Additionally, we remark that more AG codes with excellent parameters can be found by taking $H = aP_0 + bP_1 + 7P_\infty$, where $a, b \in \{4, 5, 6\}$ and $9 \leqslant a+b \leqslant 12$. The floor of such H is computed to be $\lfloor H \rfloor = aP_0 + bP_1 + 6P_\infty$. Let D be as before. If we take $G = H + \lfloor H \rfloor = 2aP_0 + 2bP_1 + 13P_\infty$, then we can produce AG codes $C_\Omega(D, G)$ with parameters $[216, 212-2a-2b, \geqslant 2a+2b-4]$. All of these codes improve the records of the corresponding ones found on MinT's Tables.

Example 2 Consider the curve $\mathrm{GGS}(q, n)$ of (1) with $q = 2$ and $n = 5$. This curve has 3969 $\mathbb{F}_{2^{10}}$-rational points and its genus is $g = 46$. It follows from Theorem 2 that

$$\left\{(57, j, 3)\middle| 1 \leqslant j \leqslant 3\right\} \subseteq G_0(P_0, P_1, P_\infty).$$

Let D be a divisor consisting of $N = 3960$ rational places except P_0, P_1, Q_1, Q_2, Q_3 and P_∞. Applying Theorem 3.4 of [4] (see also Theorem 1, [16]), if we take $G = 113P_0 + 3P_1 + 5P_\infty$, then the three-point code $C_\Omega(D, G)$ has length $N = 3960$, dimension $N - 76 = 3884$ and minimum distance at least 36. Thus we produce an AG code with parameters $[3960, 3884, \geqslant 36]$. Unfortunately, this $\mathbb{F}_{2^{10}}$-code cannot be compared with the one on MinT's Tables because the alphabet size given is at most 256.

Acknowledgements This work is partially supported by the NSFC (Grant No.11271381), the NSFC (Grant No.11431015), the NSFC (Grant No.61472457) and China 973 Program (Grant No.2011CB808000). This work is also partially supported by Guangdong Natural Science Foundation (Grant No. 2014A030313161) and the Natural Science Foundation of Shandong Province of China (ZR2016AM04).

References

1. Abdón, M., Bezerra, J., Quoos, L.: Further examples of maximal curves. Journal of Pure and Applied Algebra **213**, 1192–1196 (2009)

2. Bartoli, D., Montanucci, M., Zini, G.: AG codes and AG quantum codes from the GGS curve. arXiv:1703.03178 (2017)
3. Bartoli, D., Montanucci, M., Zini, G.: Multi point AG codes on the GK maximal curve. Des. Codes Cryptogr (2017). DOI 10.1007/s10623-017-0333-9
4. Carvalho, C., Torres, F.: On Goppa codes and Weierstrass gaps at several points. Designs, Codes and Cryptography **35**, 211–225 (2005)
5. Castellanos, A.S., Masuda, A.M., Quoos, L.: One-and two-point codes over Kummer extensions. IEEE Transactions on Information Theory **62**(9), 4867–4872 (2016)
6. Castellanos, A.S., Tizziotti, G.C.: Two-Point AG Codes on the GK Maximal Curves. IEEE Transactions on Information Theory **62**(2), 681–686 (2016)
7. Fanali, S., Giulietti, M.: One-Point AG Codes on the GK Maximal Curves. IEEE Transactions on Information Theory **56**(1), 202–210 (2010)
8. Garcia, A., Güneri, C., Stichtenoth, H.: A generalization of the Giulietti-Korchmáros maximal curve. Advances in Geometry **10**(3), 427–434 (2010)
9. Garcia, A., Kim, S.J., Lax, R.F.: Consecutive Weierstrass gaps and minimum distance of Goppa codes. Journal of Pure and Applied Algebra **84**, 199–207 (1993)
10. Garcia, A., Lax, R.F.: Goppa codes and Weierstrass gaps. In: Coding Theory and Algebraic Geometry, pp. 33–42. Springer Berlin (1992)
11. Giulietti, M., Korchmáros, G.: A new family of maximal curves over a finite field. Mathematische Annalen **343**, 229–245 (2008)
12. Goppa, V.D.: Codes associated with divisors. Problemy Peredachi Informatsii **13**, 33–39 (1977)
13. Güneri, C., Özdemiry, M., Stichtenoth, H.: The automorphism group of the generalized Giulietti-Korchmáros function field. Advances in Geometry **13**, 369–380 (2013)
14. Guruswami, V., Sudan, M.: Improved decoding of Reed-Solomon and algebraic-geometric codes. IEEE Transactions on Information Theory **45**(6), 1757–1768 (1999)
15. Homma, M., Kim, S.J.: Goppa codes with Weierstrass pairs. Journal of Pure and Applied Algebra **162**, 273–290 (2001)
16. Hu, C., Yang, S.: Multi-point codes over Kummer extensions. Des. Codes Cryptogr (2017). DOI 10.1007/s10623-017-0335-7
17. Kim, S.J.: On the index of the Weierstrass semigroup of a pair of points on a curve. Archiv der Mathematik **62**, 73–82 (1994)
18. Kirfel, C., Pellikaan, R.: The minimum distance of codes in an array coming from telescopic semigroups. IEEE Transactions on Information Theory **41**(6), 1720–1732 (1995)
19. Korchmáros, G., Nagy, G.: Hermitian codes from higher degree places. Journal of Pure and Applied Algebra **217**, 2371–2381 (2013)
20. Maharaj, H.: Code construction on fiber products of Kummer covers. IEEE Transactions on Information Theory **50**(9), 2169–2173 (2004)
21. Maharaj, H., Matthews, G.L.: On the floor and the ceiling of a divisor. Finite Fields and Their Applications **12**, 38–55 (2006)
22. Maharaj, H., Matthews, G.L., Pirsic, G.: 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**, 261–280 (2005)
23. Matthews, G.L.: The Weierstrass semigroup of an m-tuple of collinear points on a Hermitian curve. Finite Fields and Their Applications pp. 12–24 (2004)
24. Matthews, G.L.: Weierstrass semigroups and codes from a quotient of the Hermitian curve. Designs, Codes and Cryptography **37**, 473–492 (2005)
25. MinT: Online database for optimal parameters of (t, m, s)-nets, (t, s)-sequences, orthogonal arrays, and linear codes. (Accessed on 2017-01-10.). URL `http://mint.sbg.ac.at.`
26. Stichtenoth, H.: Algebraic Function Fields and Codes, vol. 254. Springer-Verlag, Berlin, Heidelberg (2009)
27. Stichtenoth, H.: Algebraic function fields and codes, vol. 254. Springer Science & Business Media (2009)
28. Yang, K., Kumar, P.V.: On the true minimum distance of Hermitian codes. In: Coding Theory and Algebraic Geometry, pp. 99–107. Springer (1992)
29. Yang, K., Kumar, P.V., Stichtenoth, H.: On the weight hierarchy of geometric Goppa codes. IEEE Transactions on Information Theory **40**(3), 913–920 (1994)