arXiv:2304.03846v1 [math.NT] 7 Apr 2023

函数域中的纯间隙全集

ALONSO S. CASTELLANOS、ERIK A. R. MENDOZA 和 GUILHERME TIZZIOTTI

Abstract. 本文提出了一种方法，可以完全确定有限域 $\mathbb{F}_q$ 上函数域 F 中两个有理点 P_1, P_2 处的纯间隙集合 $G_0(P_1, P_2)G_0$，以及该集合的基数。此外，我们给出了集合 $G_0(P_1, P_2)$ 基数的一个上界，在某些情况下优于 Homma 和 Kim 在 [11] 中给出的通用上界。由此，我们完全确定了两个函数域族中纯间隙的集合及其基数： GK 函数域和库默尔扩张。

1. 引言

Homma 和 Kim 于 2001 年引入了函数域F 在有限域 $\mathbb{F}_q$ 上的两个有理点 P_1, P_2 相关的纯间隙概念。该项工作依据相应点处的间隙序列描述了纯间隙集合，并利用这一新概念推导出由两个点支撑的代数几何码的最小距离下界。几年后，Carvalho 和 Torres [5] 将研究扩展到了多个点。此后，许多作者致力于刻画特殊曲线族中的魏尔斯特拉斯半群和纯间隙，例如 [1, 4,12, 14, 15, 19] 和 [21]。然而，即使对于特定曲线，明确描述纯间隙集合并确定其基数也颇为复杂。这一问题本身就具有挑战性和重要性，并且与有限域上曲线理论中的若干主题相关，例如限制有理点的数量，如 [3, 18]。不过，人们对纯间隙集合的兴趣主要源于其在代数几何码（AG codes）分析中的应用。尤其是，利用纯间隙有助于改进此类码的最小距离 Goppa 界。基于此，已有许多研究探讨这些应用，例如 [2, 6–8, 11]。

在 [11] Homma 和 Kim 还引入了魏尔斯特拉斯半群 $H(P_1, P_2)$ 中的一个特殊有限子集，该子集对应于一对有理点 P_1, P_2，包含整个半群以及间隙和纯间隙的信息。这个集合记为 $\Gamma(P_1, P_2)$，后来 Matthews 将其称为 $H(P_1, P_2)$ 的极小生成集 [16]。在这项工作中，我们利用极小生成集 $\Gamma(P_1, P_2)$，给出了一种方法，以完整确定有限域 $\mathbb{F}_q$ 上函数域 F 中两个有理点 P_1, P_2 处的纯间隙集合 $G_0(P_1, P_2)$ 及其基数。此外，我们还给出了集合 $G_0(P_1, P_2)$ 基数的一个上界；在本文研究的一些情形下，该上界优于一般上界

关键词：纯间隙、函数域、 GK 函数域、库默尔扩张。2010年数学主题分类：14H55、11G20。第一作者的部分研究经费由 FAPEMIG 资助。第二作者的部分研究经费由 FAPERJ/RJ-巴西 Grant 201.650/2021 资助。第三作者的部分研究经费由 CNPq 和 FAPEMIG 资助。1

由 Homma 和 Kim 在 [11] 中给出。因此，我们完整确定了两个函数域族的纯间隙集及其基数： GK 函数域和库默尔扩张。我们注意到，某些特殊情形下库默尔扩张的纯间隙集基数已在 [2] 和 [21], 中确定，但我们的结果能以更简单的方式得到这些情形下相同的基数。此外，我们证明，某些曲线族达到了本文给出的 $G_0(P_1, P_2)$ 基数界，也就是说，这些界是紧的。

本文的组织结构如下。第 2 节中，我们确立记号，并介绍关于两个有理点处的魏尔斯特拉斯半群 $H(P_1, P_2)$ 和纯间隙集$G_0(P_1, P_2)$ 的预备结果。第 3 节中，对于任意函数域 F 中的有理点 P_1, P_2，我们利用边长为 π 的正方形区域分解极小生成集 $\Gamma(P_1, P_2)$, 其中 π 是半群 $H(P_1, P_2)$ 的周期。基于这一分解，我们得到纯间隙集 $G_0(P_1, P_2)$ 的分解，进而完整描述 $G_0(P_1, P_2)$ 并给出其基数公式，见命题 3.4。此外，我们给出纯间隙集 $G_0(P_1, P_2)$ 的基数上界，见命题 3.7。第 4 节中，我们在两类函数域中阐明所得结果： GK 函数域和库默尔扩张，分别见定理 4.7 和定理 4.12。

2. Preliminaries and notation

设 q 为素数 p的幂， $\mathbb{F}_q$ 为含有 q 个元素的有限域， K 为 $\mathbb{F}_q$的代数闭包。给定亏格为 $g = g（F）$ 的一元函数域 F/K，记 $\mathcal{P}_F$ 为 F中的点集，Div(F)为 F中的因子群。对于函数 $z \in F$，我们分别用（z）、（z）$_\infty$ 和（z）$_0$ 表示函数 z 在 F 中的主因子、极点因子和零点因子。

对于因子 $D \in$ Div(F)，我们将与因子 D 相关联的黎曼-罗赫空间定义为

$$\mathcal{L}(D) = \{z \in F : (z) + D \geq 0\} \cup \{0\},$$

并记 ℓ(D)为其作为 K上向量空间的维数。令 $\mathbb{N}$ 为正整数集，并令 $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$。对于点 $P \in \mathcal{P}_F$， P处的魏尔斯特拉斯半群定义为

$$H(P) = \{s \in \mathbb{N}_0 : (z)_\infty = sP \text{ for some } z \in F\}.$$

非负整数 s 称为 P 处的非间隙，当且仅当 $s \in H(P)$。集合 $G(P) := \mathbb{N}_0 \setminus H(P)$中的元素称为 P处的间隙；对于亏格为 $g > 0$的函数域 F/K，$|G(P)| = g$。

由一个点定义的魏尔斯特拉斯半群 $H(P)$ 可以推广到两个点的情形。对于 F 中两个不同的点 P_1 和 P_2，我们将P_1、P_2 处的魏尔斯特拉斯半群定义为

$$H(P_1, P_2) = \{(s_1, s_2) \in \mathbb{N}_0^2 : (z)_\infty = s_1P_1 + s_2P_2 \text{ for some } z \in F\}.$$

与单个点的情形类似，集合 $G(P_1, P_2) := \mathbb{N}_0^2 \setminus H(P_1, P_2)$ 的元素称为 P_1, P_2 处的间隙，并可利用黎曼-罗赫空间刻画，即，a

对 (s_1, s_2), $\in \mathbb{N}_0^2$ 是 P_1, P_2 处的一个间隙，当且仅当

$$\ell(s_1P_1 + s_2P_2) = \ell(s_1P_1 + s_2P_2 - P_j) \text{ for some } j \in \{1, 2\}.$$

此外，如果满足以下条件，则称 (s_1, s_2) 在 P_1, P_2 处为纯间隙。

$$\ell(s_1P_1 + s_2P_2) = \ell(s_1P_1 + s_2P_2 - P_j) \text{ for all } j \in \{1, 2\}$$

或者，等价地，

$$\ell(s_1P_1 + s_2P_2) = \ell((s_1 - 1)P_1 + (s_2 - 1)P_2).$$

我们将 P_1、P_2 处的纯间隙集记为 $G_0(P_1, P_2)$。在 [11, 推论 2.2], 中，Homma 和 Kim 给出了 $G_0(P_1, P_2)$ 的基数的如下界:

$$|G_0(P_1, P_2)| \leq \frac{g(g-1)}{2}. \tag{1}$$

现在，令 $G(P_1)$ 和 $G(P_2)$ 分别为点 P_1 和 P_2 的间隙集。对于每个 $\beta \in G(P_1)$，我们令 $\tau_{P_1, P_2}(\beta) := \min\{\gamma \in \mathbb{N}_0 : (\beta, \gamma) \in H(P_1, P_2)\}$. 由 [13, 引理 2.6], 可得, $G(P_2) = \{\tau_{P_1,P_2}(\beta) : \beta \in G(P_1)\}$，因此

$$\begin{array}{rccc} \tau_{P_1,P_2}: & G(P_1) & \to & G(P_2) \\ & \beta & \mapsto & \min\{\gamma \in \mathbb{N}_0 : (\beta, \gamma) \in H(P_1, P_2)\} \end{array} \tag{2}$$

是一个双射。映射 $\tau_{P_1,\ P_2}$ 的图记作 $\Gamma(P_1, P_2)$，即,

$$\Gamma(P_1, P_2) := \{(\beta, \tau_{P_1,P_2}(\beta)) : \beta \in G(P_1)\}.$$

对于 $\mathbf{x} = (\beta_1, \gamma_1)$ 和 $\mathbf{y} = (\beta_2, \gamma_2)$，$\mathbf{x}$ 和 $\mathbf{y}$ 的最小上界与最大下界分别定义为 $\mathrm{lub}(\mathbf{x}, \mathbf{y}) = (\max\{\beta_1, \beta_2\}, \max\{\gamma_1, \gamma_2\})$ 和 $\mathrm{glb}(\mathbf{x}, \mathbf{y}) = (\min\{\beta_1, \beta_2\}, \min\{\gamma_1, \gamma_2\})$。令 $\preceq$ 为 $\mathbb{N}_0^2$中的自然偏序。若 $\beta_1 > \beta_2$ 或 $\gamma_1 > \gamma_2$，则记作 $\mathbf{x} \not\preceq \mathbf{y}$。

以下结果表明，只需确定 $\Gamma(P_1, P_2)$，即可计算魏尔斯特拉斯半群 $H(P_1, P_2)$。因此，集合 $\Gamma(P_1, P_2)$称为魏尔斯特拉斯半群 $H(P_1, P_2)$ 的极小生成集。

Lem引理 2.1. *[13, 引理 2.2]* 设 P_1 和 P_2 是 F中的两个不同的点。 n

$$H(P_1, P_2) = \{\mathrm{lub}(\mathbf{x}, \mathbf{y}) : \mathbf{x}, \mathbf{y} \in \Gamma(P_1, P_2) \cup (H(P_1) \times \{0\}) \cup (\{0\} \times H(P_2))\}.$$

下一个结果表明，集合 $\Gamma(P_1, P_2)$ 对于确定纯间隙集 $G_0(P_1, P_2)$ 也很重要。

引理 2.2。*[7, 命题 5.1]* 设 P_1 和 P_2 是 F 中的两个不同的点。那么

$$G_0(P_1, P_2) = \{\mathrm{glb}(\mathbf{x}, \mathbf{y}) : \mathbf{x}, \mathbf{y} \in \Gamma(P_1, P_2),\ \mathbf{x} \not\preceq \mathbf{y},\ \mathbf{y} \not\preceq \mathbf{x}\}.$$

3. Pure gap set at two places

设 P_1 和 P_2 是任意函数域 F/K 中不同的点，该函数域的亏格为 g。设 π 为半群 $H(P_1, P_2)$ 的周期，其中周期定义为：$\pi := \min\{k \in \mathbb{N} : k(P_1 - P_2) \text{ 是主因子}\}$。本节首先证明以下结果，该结果确立了周期 π 与式 (2) 中给出的双射 τ_{P_1,P_2} 之间的关系。

命题 3.1. 设 P_1 和 P_2 是 F中的不同点，且 π 是半群 $H(P_1, P_2)$的周期。对于 $\beta \in G(P_1)$ 和 $k \in \mathbb{N}$，以下陈述等价：

i) $\beta + k\pi \in G(P_1)$.
ii) $k\pi < \tau_{P_1,P_2}(\beta)$.

如果满足上述任一条件，则

$$\tau_{P_1,P_2}(\beta + k\pi) = \tau_{P_1,P_2}(\beta) - k\pi.$$

证明。令 $\beta \in G(P_1)$。对于 $k \in \mathbb{N}$ 我们知道存在一个函数 f 使得 $(f) = k\pi P_1 - k\pi P_2$。

i) $\Rightarrow$ *ii)*。假设 $\beta + k\pi \in G(P_1)$。若 $k\pi \geq \tau_{P_1,P_2}(\beta)$，由于 $(0, k\pi) \in H(P_1, P_2)$ 且 $(\beta, \tau_{P_1,P_2}(\beta)) \in H(P_1, P_2)$，我们有 $(\beta, k\pi) \in H(P_1, P_2)$。因此，存在函数 h_1，使得 $(h_1) = D - (\beta P_1 + k\pi P_2)$，其中 D 是有效因子，且 $P_1, P_2 \notin \text{支撑}(D)$。于是，$(h_1 f^{-1}) = D - \beta P_1 - k\pi P_2 - k\pi P_1 + k\pi P_2 = D - (\beta + k\pi)P_1$，从而我们有$\beta + k\pi \in H(P_1)$，矛盾。

ii) $\Rightarrow$ *i)*。现在，假设 $k\pi < \tau_{P_1,P_2}(\beta)$。若 $\beta + k\pi \in H(P_1)$，则存在一个函数 h_2，使得 $(h_2) = D' + \alpha P_2 - (\beta + k\pi)P_1$，其中 $\alpha \in \mathbb{N}_0$，且 D' 是一个有效因子，满足 $P_1, P_2 \notin \text{支撑}(D')$。因此，$(h_2 f) = D' + \alpha P_2 - (\beta + k\pi)P_1 + k\pi P_1 - k\pi P_2 = D' - \beta P_1 - (k\pi - \alpha)P_2$。注意，

- 若 $\alpha \geq k\pi$，则 $\beta \in H(P_1)$，这就产生矛盾；
- 若 $0 \leq \alpha < k\pi$，则有 $0 < k\pi - \alpha \leq k\pi < \tau_{P_1,P_2}(\beta)$，且 $(\beta, k\pi - \alpha) \in H(P_1, P_2)$，根据 $\tau_{P_1,P_2}(\beta)$ 的定义，这就产生矛盾。

为得到最后一部分中的等式，假设 $\beta + k\pi \in G(P_1)$。由于 $(\beta, \tau_{P_1,P_2}(\beta)) \in H(P_1, P_2)$，$k\pi < \tau_{P_1,P_2}(\beta)$ 且 $(f) = k\pi P_1 - k\pi P_2$，我们可以得到 $(\beta + k\pi, \tau_{P_1,P_2}(\beta) - k\pi) \in H(P_1, P_2)$。因此，$\tau_{P_1,P_2}(\beta) - k\pi \geq \tau_{P_1,P_2}(\beta + k\pi)$。另一方面，由于 $(\beta + k\pi, \tau_{P_1,P_2}(\beta + k\pi)) \in H(P_1, P_2)$ 且 $(f) = k\pi P_1 - k\pi P_2$，于是 $(\beta, \tau_{P_1,P_2}(\beta + k\pi) + k\pi) \in H(P_1, P_2)$。根据 $\tau_{P_1,P_2}(\beta)$ 的定义，我们得出 $\tau_{P_1,P_2}(\beta) - k\pi \leq \tau_{P_1,P_2}(\beta + k\pi)$，结论得证。□

令 $\Gamma(P_1, P_2)$为半群 $H(P_1, P_2)$ 的极小生成集。对于 $k_1, k_2 \in \mathbb{N}_0$，定义集合

$$\begin{aligned}\Gamma_{k_1,k_2} &:= \Gamma(P_1, P_2) \cap ((k_1\pi, (k_1 + 1)\pi] \times (k_2\pi, (k_2 + 1)\pi]) \\ &= \{(\beta, \tau_{P_1,P_2}(\beta)) : \beta \in G(P_1),\ k_1\pi < \beta < (k_1 + 1)\pi,\ k_2\pi < \tau_{P_1,P_2}(\beta) < (k_2 + 1)\pi\}.\end{aligned}$$

因此,

$$\Gamma(P_1,P_2)=\bigcup_{\substack{0\le k_1\\0\le k_2}}\Gamma_{k_1,k_2}. \tag{3}$$

注记 3.2。注意，如果 $(k_1,k_2)\neq(j_1,j_2)$，那么 $\Gamma_{k_1,\ k_2}\cap\Gamma_{j_1,\ j_2}=\emptyset$。因此，上述并集互不相交。此外，魏尔斯特拉斯半群理论（参见例如 *[13,* 引理 2.*1]* 以及 *[17]*中的黎曼-罗赫定理）中众所周知，$(a,b)\in H(P_1,P_2)$ 当$a+b\geq 2g$时。因此，我们有，若 $k_1+k_2\geq\left\lceil\frac{2g-1}{\pi}\right\rceil$，则 $\Gamma_{k_1,\ k_2}=\emptyset$。

接下来，作为命题 3.1 的推论，我们证明，要确定 $\Gamma(P_1,P_2)$，只需确定 $k\geq 0$ 的 $\Gamma_{k,0}$ 形式的集合。

对于每个 $j\in\mathbb{N}_0$，定义

$$\mathbf{w}_j:=(-j\pi,j\pi)\in\mathbb{Z}^2.$$

命题 3.3。对于 i、$j\geq 0$,

$$\Gamma_{i,j}=\Gamma_{i+j,0}+\mathbf{w}_j.$$

特别地,

$$\sum_{0\le k}(k+1)|\Gamma_{k,0}|=g. \tag{4}$$

证明。设 $(\beta,\tau_{P_1,P_2}(\beta))$ 是 $\Gamma_{i+j,0}$ 中的一个元素。则 $\beta\in G(P_1)$、$(i+j)\pi<\beta<(i+j+1)\pi$以及 $0<\tau_{P_1,P_2}(\beta)<\pi$。根据周期 π 的定义，我们有 $\pi\in H(P_1)$，因此 $\beta-j\pi\in G(P_1)$ 且 $i\pi<\beta-j\pi<(i+1)\pi$。此外，由命题 3.1 可得 $\tau_{P_1,P_2}(\beta-j\pi)=\tau_{P_1,P_2}(\beta)+j\pi$。因此 $j\pi<\tau_{P_1,P_2}(\beta-j\pi)<(j+1)\pi$ 并且

$$(\beta,\tau_{P_1,P_2}(\beta))+\mathbf{w}_j=(\beta-j\pi,\tau_{P_1,P_2}(\beta-j\pi))\in\Gamma_{i,j}.$$

这意味着 $\Gamma_{i+j,\ 0}+\mathbf{w}_j\subseteq\Gamma_{i,\ j}$。另一个包含关系的证明类似。最后，利用 (3) 以及上面的等式，我们得到

$$g=|\Gamma(P_1,P_2)|=\sum_{\substack{0\le i\\0\le j}}|\Gamma_{i,j}|=\sum_{\substack{0\le i\\0\le j}}|\Gamma_{i+j,0}|=\sum_{0\le k}(k+1)|\Gamma_{k,0}|.$$

□

类似地，对于 $k_1,k_2\in\mathbb{N}_0$ 定义集合

$$G_{k_1,k_2}:=G_0(P_1,P_2)\cap((k_1\pi,(k_1+1)\pi]\times(k_2\pi,(k_2+1)\pi]).$$

因此,

$$G_0(P_1,P_2)=\bigcup_{\substack{0\le k_1\\0\le k_2}}G_{k_1,k_2}. \tag{5}$$

与 $\Gamma_{k_1,\ k_2}$ 的情况一样，上述并集是互不相交的；若 $k_1+k_2\geq\left\lceil\frac{2g-1}{\pi}\right\rceil$，则有 $G_{k_1,\ k_2}=\emptyset$。

由引理 2.2，我们可以将集合 G_{k_1,k_2} 重写为

$$G_{k_1,k_2} = \{\mathrm{glb}(\mathbf{u},\mathbf{v}) : \mathbf{u} \in \Gamma_{k_1,l_2},\, \mathbf{v} \in \Gamma_{l_1,k_2}, \mathbf{u} \not\preceq \mathbf{v},\, \mathbf{v} \not\preceq \mathbf{u},\, k_1 \le l_1,\, k_2 \le l_2\}. \tag{6}$$

以下结果表明，要确定 $G_0(P_1,P_2)$，只需确定形如 $G_{k,\,0}$ 的集合，其中 $k \ge 0$。

命题 3.4. 对于 $i,j \ge 0$,

$$G_{i,j} = G_{i+j,0} + \mathbf{w}_j.$$

特别是,

$$|G_0(P_1,P_2)| = \sum_{k=0}^{\lceil \frac{2g-1}{\pi} \rceil - 1} (k+1)|G_{k,0}|. \tag{7}$$

证明. 设 $\mathbf{u} \in G_{i+j,\,0}$。由 (6)，存在元素 $\mathbf{u}_1 \in \Gamma_{i+j,\,u}$ 和 $\mathbf{u}_2 \in \Gamma_{v,\,0}$，使得 $\mathbf{u}_1 \not\preceq \mathbf{u}_2$ 且 $\mathbf{u}_2 \not\preceq \mathbf{u}_1$, ，从而

$$\mathbf{u} = \mathrm{glb}(\mathbf{u}_1, \mathbf{u}_2),$$

其中 $u \ge 0$ 和 $v \ge i+j$。由命题 3.3 可得

$$\mathbf{v}_1 := \mathbf{u}_1 + \mathbf{w}_j \in \Gamma_{i,u+j} \quad \text{and} \quad \mathbf{v}_2 := \mathbf{u}_2 + \mathbf{w}_j \in \Gamma_{v-j,j},$$

其中 $u+j \ge j$ 和 $v-j \ge i \ge 0$。此外，由于 $\mathbf{v}_1 \not\preceq \mathbf{v}_2$ 和 $\mathbf{v}_2 \not\preceq \mathbf{v}_1$，我们得到

$$\mathbf{u} + \mathbf{w}_j = \mathrm{glb}(\mathbf{u}_1,\mathbf{u}_2) + \mathbf{w}_j = \mathrm{glb}(\mathbf{u}_1 + \mathbf{w}_j, \mathbf{u}_2 + \mathbf{w}_j) = \mathrm{glb}(\mathbf{v}_1,\mathbf{v}_2) \in G_{i,j}.$$

因此，$G_{i+j,\,0} + \mathbf{w}_j \subseteq G_{i,\,j}$。另一包含关系可类似地证明。为完成证明，根据（5）及上述等式，我们有

$$|G_0(P_1,P_2)| = \sum_{\substack{0\le i\\ 0\le j}} |G_{i,j}| = \sum_{\substack{0\le i\\ 0\le j}} |G_{i+j,0}| = \sum_{0\le k} (k+1)|G_{k,0}|.$$

结论成立，这是因为 $G_{k,\,0} = \emptyset$ 当 $k \ge \lceil \frac{2g-1}{\pi} \rceil$ 时。 □

注意，由（5）和命题 3.4 可知，我们有

$$G_0(P_1,P_2) = \bigcup_{\substack{0\le i,j\\ i+j<\lceil \frac{2g-1}{\pi} \rceil}} (G_{i+j,0} + \mathbf{w}_j) = \bigcup_{0\le j\le k<\lceil \frac{2g-1}{\pi} \rceil} (G_{k,0} + \mathbf{w}_j)\,. \tag{8}$$

现在，我们将了解如何使用集合Γ_{k_1,k_2}来确定集合 $G_{k,0}$。为此，固定 $k \in \mathbb{N}_0$并注意到

$$\begin{aligned}
G_{k,0} &= \{\mathrm{glb}(\mathbf{u},\mathbf{v}) : \mathbf{u} \in \Gamma_{k,k_2},\, \mathbf{v} \in \Gamma_{k_1,0},\, \mathbf{u} \not\preceq \mathbf{v},\, \mathbf{v} \not\preceq \mathbf{u},\, k \le k_1,\, 0 \le k_2\} \\
&= \{\mathrm{glb}(\mathbf{u},\mathbf{v}) : \mathbf{u} \in \Gamma_{k,k_2},\, \mathbf{v} \in \Gamma_{k_1,0},\, \mathbf{u} \not\preceq \mathbf{v},\, \mathbf{v} \not\preceq \mathbf{u},\, k < k_1,\, 0 < k_2\} \\
&\quad \cup \{\mathrm{glb}(\mathbf{u},\mathbf{v}) : \mathbf{u},\mathbf{v} \in \Gamma_{k,0},\, \mathbf{u} \not\preceq \mathbf{v},\, \mathbf{v} \not\preceq \mathbf{u}\} \\
&\quad \cup \{\mathrm{glb}(\mathbf{u},\mathbf{v}) : \mathbf{u} \in \Gamma_{k,0},\, \mathbf{v} \in \Gamma_{k_1,0},\, \mathbf{u} \not\preceq \mathbf{v},\, \mathbf{v} \not\preceq \mathbf{u},\, k < k_1\} \\
&\quad \cup \{\mathrm{glb}(\mathbf{u},\mathbf{v}) : \mathbf{u} \in \Gamma_{k,k_2},\, \mathbf{v} \in \Gamma_{k,0},\, \mathbf{u} \not\preceq \mathbf{v},\, \mathbf{v} \not\preceq \mathbf{u},\, 0 < k_2\} \\
&= \{\mathrm{glb}(\mathbf{u},\mathbf{v}) : \mathbf{u} \in \Gamma_{k,k_2},\, \mathbf{v} \in \Gamma_{k_1,0},\, k < k_1,\, 0 < k_2\} \\
&\quad \cup \{\mathrm{glb}(\mathbf{u},\mathbf{v}) : \mathbf{u},\mathbf{v} \in \Gamma_{k,0},\, \mathbf{u} \not\preceq \mathbf{v},\, \mathbf{v} \not\preceq \mathbf{u}\} \\
&\quad \cup \{\mathrm{glb}(\mathbf{u},\mathbf{v}) : \mathbf{u} \in \Gamma_{k,0},\, \mathbf{v} \in \Gamma_{k_1,0},\, \mathbf{u} \not\preceq \mathbf{v},\, k < k_1\} \\
&\quad \cup \{\mathrm{glb}(\mathbf{u},\mathbf{v}) : \mathbf{u} \in \Gamma_{k,k_2},\, \mathbf{v} \in \Gamma_{k,0},\ \mathbf{v} \not\preceq \mathbf{u},\, 0 < k_2\}.
\end{aligned}$$

为简化记号，记

$$\begin{aligned}
G^1_{k,0} &= \{\mathrm{glb}(\mathbf{u},\mathbf{v}) : \mathbf{u} \in \Gamma_{k,k_2},\, \mathbf{v} \in \Gamma_{k_1,0},\, k < k_1,\, 0 < k_2\}, \\
G^2_{k,0} &= \{\mathrm{glb}(\mathbf{u},\mathbf{v}) : \mathbf{u},\mathbf{v} \in \Gamma_{k,0},\, \mathbf{u} \not\preceq \mathbf{v},\, \mathbf{v} \not\preceq \mathbf{u}\}, \\
G^3_{k,0} &= \{\mathrm{glb}(\mathbf{u},\mathbf{v}) : \mathbf{u} \in \Gamma_{k,0},\, \mathbf{v} \in \Gamma_{k_1,0},\, \mathbf{u} \not\preceq \mathbf{v},\, k < k_1\},\ \text{and} \\
G^4_{k,0} &= \{\mathrm{glb}(\mathbf{u},\mathbf{v}) : \mathbf{u} \in \Gamma_{k,k_2},\, \mathbf{v} \in \Gamma_{k,0},\ \mathbf{v} \not\preceq \mathbf{u},\, 0 < k_2\}.
\end{aligned}$$

因此，对于每个 $k \in \mathbb{N}_0$，我们有

$$G_{k,0} = G^1_{k,0} \cup G^2_{k,0} \cup G^3_{k,0} \cup G^4_{k,0}. \tag{9}$$

注意，根据定义，这样的并集两两不交；并且由 (8) 可知，若确定了$G^i_{k,\ 0}$、 $i = 1$、2、3、4 对应的集合，就能确定 $G_0(P_1, P_2)$。下面给出这些集合的一些信息。

引理 3.5. $|G^1_{k,\ 0}| = \left(\sum_{k<k_1} |\Gamma_{k_1,\ 0}|\right)^2$。

证明. 注意，对于 $\mathbf{u}_1,\mathbf{u}_2 \in \Gamma_{k,\ k_2}$ 和 $\mathbf{v}_1,\mathbf{v}_2 \in \Gamma_{k_1,\ 0}$，其中 $k < k_1$ 和 $0 < k_2$，我们有 $\mathrm{glb}(\mathbf{u}_1, \mathbf{v}_1) = \mathrm{glb}(\mathbf{u}_2,\mathbf{v}_2)$ 当且仅当 $\mathbf{u}_1 = \mathbf{u}_2$ 且 $\mathbf{v}_1 = \mathbf{v}_2$。因此，

$$|G^1_{k,0}| = |\{\mathrm{glb}(\mathbf{u},\mathbf{v}) : \mathbf{u} \in \Gamma_{k,k_2},\, \mathbf{v} \in \Gamma_{k_1,0},\, k < k_1,\, 0 < k_2\}| = \left(\sum_{k<k_1} |\Gamma_{k_1,0}|\right)\left(\sum_{0<k_2} |\Gamma_{k,k_2}|\right).$$

此外，由命题 3.3 可得 $\Gamma_{k,k_2} = \Gamma_{k+k_2,0} + \mathbf{w}_{k_2}$。因此，$|\Gamma_{k,k_2}| = |\Gamma_{k+k_2,0}|$并且

$$|G^1_{k,0}| = \left(\sum_{k<k_1} |\Gamma_{k_1,0}|\right)\left(\sum_{0<k_2} |\Gamma_{k,k_2}|\right) = \left(\sum_{k<k_1} |\Gamma_{k_1,0}|\right)\left(\sum_{0<k_2} |\Gamma_{k+k_2,0}|\right) = \left(\sum_{k<k_1} |\Gamma_{k_1,0}|\right)^2.$$

□

注 3.6。根据定义可得

$$\begin{array}{l} 0 \leq |G^2_{k,0}| \leq |\Gamma_{k,0}|(|\Gamma_{k,0}|-1) = |\Gamma_{k,0}|^2 - |\Gamma_{k,0}|, \\ 0 \leq |G^3_{k,0}| \leq |\Gamma_{k,0}| \left(\sum_{k<k_1} |\Gamma_{k_1,0}|\right), \ and \\ 0 \leq |G^4_{k,0}| \leq |\Gamma_{k,0}| \left(\sum_{0<k_2} |\Gamma_{k,k_2}|\right) = |\Gamma_{k,0}| \left(\sum_{k<k_1} |\Gamma_{k_1,0}|\right). \end{array} \tag{10}$$

在下一个结果中，我们给出了 $G_0(P_1, P_2)$ 的基数界。

命题 3.7。设 P_1 和 P_2 是函数域 F/K 中两个不同的点，其亏格为 g。则

$$\sum_{0\leq k}(k+1)\left(\sum_{k<k_1}|\Gamma_{k_1,0}|\right)^2 \leq |G_0(P_1,P_2)| \leq \sum_{0\leq k}(k+1)\left(\sum_{k\leq k_1}|\Gamma_{k_1,0}|\right)^2 - g.$$

证明。由引理 3.5 和注 3.6 可得

$$|G_{k,0}| \leq \left(\sum_{k<k_1}|\Gamma_{k_1,0}|\right)^2 + |\Gamma_{k,0}|^2 - |\Gamma_{k,0}| + 2|\Gamma_{k,0}|\left(\sum_{k<k_1}|\Gamma_{k_1,0}|\right) = \left(\sum_{k\leq k_1}|\Gamma_{k_1,0}|\right)^2 - |\Gamma_{k,0}|.$$

因此，由公式（7），

$$\sum_{0\leq k}(k+1)\left(\sum_{k<k_1}|\Gamma_{k_1,0}|\right)^2 \leq |G_0(P_1,P_2)|$$

and

$$\begin{aligned} |G_0(P_1,P_2)| &\leq \sum_{0\leq k}(k+1)\left[\left(\sum_{k\leq k_1}|\Gamma_{k_1,0}|\right)^2 - |\Gamma_{k,0}|\right] \\ &= \sum_{0\leq k}(k+1)\left(\sum_{k\leq k_1}|\Gamma_{k_1,0}|\right)^2 - \sum_{0\leq k}(k+1)|\Gamma_{k,0}| \\ &= \sum_{0\leq k}(k+1)\left(\sum_{k\leq k_1}|\Gamma_{k_1,0}|\right)^2 - g. \qquad \text{(from Equation (4))} \end{aligned}$$

□

注意，我们可以用集合 $\Gamma_{k_1,0}$来改写集合 $G^1_{k,0}$、 $G^2_{k,0}$、 $G^3_{k,0}$ 和 $G^4_{k,0}$ 。事实上，

$$\begin{array}{l} G^1_{k,0} = \{\mathrm{glb}(\mathbf{u}+\mathbf{w}_{k_2-k}, \mathbf{v}) : \mathbf{u} \in \Gamma_{k_2,0},\ \mathbf{v} \in \Gamma_{k_1,0},\ k<k_1,\ k<k_2\}, \\ G^2_{k,0} = \{\mathrm{glb}(\mathbf{u}, \mathbf{v}) : \mathbf{u}, \mathbf{v} \in \Gamma_{k,0},\ \mathbf{u} \not\preceq \mathbf{v},\ \mathbf{v} \not\preceq \mathbf{u}\}, \\ G^3_{k,0} = \{\mathrm{glb}(\mathbf{u}, \mathbf{v}) : \mathbf{u} \in \Gamma_{k,0},\ \mathbf{v} \in \Gamma_{k_1,0},\ \mathbf{u} \not\preceq \mathbf{v},\ k<k_1\}, \text{ and} \\ G^4_{k,0} = \{\mathrm{glb}(\mathbf{u}+\mathbf{w}_{k_2-k}, \mathbf{v}) : \mathbf{u} \in \Gamma_{k_2,0},\ \mathbf{v} \in \Gamma_{k,0},\ \mathbf{v} \not\preceq \mathbf{u}+\mathbf{w}_{k_2-k},\ k<k_2\}. \end{array} \tag{11}$$

注 3.8。由注记 3.2 可知，若 $k \geq \left\lceil \frac{2g-1}{\pi} \right\rceil$ 则 $G^i_{k,\ 0} = \emptyset$ 对每个 $i = 1,\ 2,\ 3,\ 4$ 都成立。此外，根据定义，若 $k = \left\lceil \frac{2g-1}{\pi} \right\rceil - 1$ 则 $G^1_{k,\ 0} = G^3_{k,\ 0} = G^4_{k,\ 0} = \emptyset$。

为结束本节，我们给出以下结果。

引理 3.9. 若对每个 $\beta \in G(P_1)$，$\beta \equiv \tau_{P_1,P_2}(\beta) \pmod{\pi}$，则

$$G^2_{k,0} = \emptyset \quad and \quad G^4_{k,0} = \{(b,a) \in \mathbb{N}^2 : (a,b) \in G^3_{k,0}\} - \mathbf{w}_k$$

对每个 $k \in \mathbb{N}_0$ 都成立。特别地，$|G^3_{k,0}| = |G^4_{k,0}|$。

证明。假设对每个 $\beta \in G(P_1)$，$\beta \equiv \tau_{P_1,P_2}(\beta) \pmod{\pi}$。令 $\mathbf{u} = (\beta_1, \tau_{P_1,P_2}(\beta_1))$ 和 $\mathbf{v} = (\beta_2, \tau_{P_1,P_2}(\beta_2))$ 属于 $\Gamma_{k,0}$。因此，$\beta_1 = \tau_{P_1,P_2}(\beta_1) + \ell_1\pi$，且 $\beta_2 = \tau_{P_1,P_2}(\beta_2) + \ell_2\pi$，其中 $\ell_1, \ell_2 \in \mathbb{Z}$。由于 $k\pi < \beta_1, \beta_2 < (k+1)\pi$ 且 $0 < \tau_{P_1,P_2}(\beta_1)\, \tau_{P_1,P_2}(\beta_2) < \pi$，我们有 $\ell_1 = \ell_2 = k$。因此，若 $\beta_1 \le \beta_2$（或 $\beta_2 \le \beta_1$），则 $\tau_{P_1,P_2}(\beta_1) \le \tau_{P_1,P_2}(\beta_2)$（或 $\tau_{P_1,P_2}(\beta_2) \le \tau_{P_1,P_2}(\beta_1)$）。因此，对每个 $\mathbf{u}, \mathbf{v} \in \Gamma_{k,0}$，都有 $\mathbf{u} \preceq \mathbf{v}$ 或 $\mathbf{v} \preceq \mathbf{u}$。这意味着 $G^2_{k,0} = \emptyset$。

另一方面，设 $(a,b) \in G^3_{k,0}$。由 (11) 可知，存在元素 $\mathbf{u} = (k\pi + j, j) \in \Gamma_{k,0}$ 和 $\mathbf{v} = (k_1\pi + j_1, j_1) \in \Gamma_{k_1,0}$，其中 $k < k_1$，使得 $0 < j_1 < j < \pi$ 且 $(a,b) = \mathrm{glb}(\mathbf{u}, \mathbf{v}) = (k\pi + j, j_1)$。由命题 3.3，$\mathbf{v} + \mathbf{w}_{k_1-k} \in \Gamma_{k,k_1-k}$。此外，$\mathbf{u} \not\preceq \mathbf{v} + \mathbf{w}_{k_1-k}$。因此，由 (11) 可得

$$(b,a) - \mathbf{w}_k = (k\pi + j_1, j) = \mathrm{glb}(\mathbf{u}, \mathbf{v} + \mathbf{w}_{k_1-k}) \in G^4_{k,0}.$$

这证明了一个包含关系。另一个包含关系的证明类似。 □

4. Pure gap set of some function fields

本节作为上一节所述结果的一个应用，将完整确定若干类函数域的纯间隙集及其基数。

4.1. GK 函数域。

考虑 Giulietti 和 Korchmáros[10]通过下列方程引入的曲线

$$\mathcal{GK} : \begin{cases} Z^{q^2-q+1} = Y \sum_{i=0}^{q} (-1)^{i+1} X^{i(q-1)} \\ Y^{q+1} = X^q + X \end{cases}.$$

该曲线在 $\mathbb{F}_{q^6}$ 上是极大的，并且是第一个不被厄米特曲线覆盖的极大曲线例子。令 K 为 $\mathbb{F}_{q^6}$ 的代数闭包，并考虑具有 $z^{q^2-q+1} = y\sum_{i=0}^{q}(-1)^{i+1}x^{i(q-1)}$ 且 $y^{q+1} = x^q + x$ 为 $\mathcal{GK}$ 在 K 上的函数域的 $GK = K(x,y,z)$。该 GK 函数域在 $\mathbb{F}_{q^6}$ 上有 $q^8 - q^6 + q^5 + 1$ 个有理点、一个记作 P_∞ 的无穷远点，其亏格为 $g = \frac{1}{2}(q^3+1)(q^2-2) + 1$。

令 $GK(\mathbb{F}_{q^6})$ 为 GK 中有理点的集合。对于 $j = 0, \dots, q-1$，取 $P_j = (a_j, 0, 0) \in GK(\mathbb{F}_{q^6})$，使得 $a_j^q + a_j = 0$，其中 $a_0 = 0$，因此 $P_0 = (0,0,0)$。对于 $\ell = 1, \dots, q^3 - q$，取 $Q_\ell = (a_\ell, b_\ell, 0) \in GK(\mathbb{F}_{q^6})$，使得 $b_\ell \neq 0$ 且 $a_\ell^q + a_\ell = b_\ell^{q+1}$。下文中，$P_\infty$, P_j（对于 $j = 0, \dots, q-1$）以及 Q_ℓ（对于 $\ell = 1, \dots, q^3 - q$）均表示上述给出的点。对于每个 $j = 0, \dots, q-1$，我们有如下主因子

$$(x - a_j) = (q^3+1)P_j - (q^3+1)P_\infty. \tag{12}$$

定理 4.1. *[10, 定理 7]* $GK(\mathbb{F}_{q^6})$，即 GK 的有理点集合，在 Aut(GK) 的作用下分成两个轨道。一个轨道（记作 $\mathcal{O}_1$）的大小为 q^3+1，由上述点 P_j 和 Q_ℓ 以及无穷远点 P_∞组成。另一个轨道的大小为 $q^3(q^3+1)(q^2-1)$，由满足 $c \neq 0$ 的点 $P=(a,b,c) \in GK(\mathbb{F}_{q^6})$ 组成。此外，Aut(GK) 在 $\mathcal{O}_1$ 上的作用为 PGU(3, q) 的双重传递置换表示。

命题 4.2. *[10, 命题 1]* 设 P_j 和 Q_ℓ 如上所述。则，对每个 $j=1,\ldots,q-1$ 以及 $\ell=1,\ldots,q^3-q$，$H(P_\infty) = H(P_j) = H(Q_\ell) = \langle q^3-q^2+q, q^3, q^3+1\rangle$。

以下结果明确给出了极小生成集$\Gamma(P_0,P_\infty)$。我们将重点讨论 $P_1 = P_0$ 和 $P_2 = P_\infty$ 的情形，但根据定理 4.1，对于任意点 $P_{(a,b,0)} \in GK(\mathbb{F}_{q^6})$，这些结果同样成立。也就是说，我们可以将点 P_0 和 P_∞ 替换为定理 4.1 中给出的轨道 $\mathcal{O}_1$ 上的任意点。

定理 4.3. *[8, 定理 3.4]* 令 $q \geq 3$ 并定义集合

$$A_1 = \{\gamma_{i,j,k} : 1 \leq k \leq q-1,\ 0 \leq i \leq k,\ k-i+1 \leq j \leq q^2-q\},$$
$$A_2 = \{\gamma_{i,j,k} : 1 \leq k \leq q-1,\ k+1 \leq i \leq q,\ 0 \leq j \leq q^2-q\},$$
$$A_3 = \{\gamma_{i,j,k} : q \leq k \leq q^2-q-2,\ 0 \leq i \leq q,\ k-i+1 \leq j \leq q^2-q\},\ \textit{and}$$
$$A_4 = \{\gamma_{i,j,k} : q^2-q-1 \leq k \leq q^2-1,\ k-q^2+q+1 \leq i \leq q,\ k-i+1 \leq j \leq q^2-q\},$$

其中

$$\gamma_{i,j,k} = ((k-1)(q^3+1)+(q+1-i)(q^2-q+1)-j,\ (i+j-k-1)(q^3+1)+(q+1-i)(q^2-q+1)-j).$$

Then

$$\Gamma(P_0,P_\infty) = A_1 \cup A_2 \cup A_3 \cup A_4.$$

为了计算纯间隙集 $G_0(P_0,P_\infty)$，我们将重写集合$\Gamma(P_0,P_\infty)$。使用定理 4.3 中引入的记号，注意到

$$A_1 \cup A_2 = \{\gamma_{i,j,k} : 1 \leq k \leq q-1,\ 0 \leq i \leq q,\ \max\{0,k-i+1\} \leq j \leq q^2-q\},$$

$$A_1 \cup A_2 \cup A_3 = \{\gamma_{i,j,k} : 1 \leq k \leq q^2-q-2,\ 0 \leq i \leq q,\ \max\{0,k-i+1\} \leq j \leq q^2-q\},$$

因此

$$\Gamma(P_0,P_\infty) = \{\gamma_{i,j,k} : 1 \leq k \leq q^2-1,\ \max\{0,k-q^2+q+1\} \leq i \leq q,\ \text{and}\ \max\{0,k-i+1\} \leq j \leq q^2-q\}. \tag{13}$$

我们注意到，对情形 $q=2$ 而言，极小生成集 $\Gamma(P_0,P_\infty)$ 的这一新描述同样成立，因为所得结果与 [8,第三节]中给出的结果一致。

命题 4.4. 半群 $H(P_0,P_\infty)$ 的周期为 $\pi = q^3+1$。

证明. 由 (12) 可得 $(x) = (q^3+1)(P_0 - P_\infty)$，因此 $\pi \le q^3+1$。假设 $1 \le \pi \le q^3$，并令 $w \in \mathbb{F}_{q^6}(GK)$ 为满足 $(w) = \pi(P_0 - P_\infty)$ 的函数。由命题 4.2，$H(P_\infty)$ 的最小非零元素为 $q^3 - q^2 + q$，且由于$\pi \in H(P_\infty)$，我们得到 $q^3 - q^2 + q \le \pi \le q^3$。此外，由于

$$(xw^{-1}) = (q^3 + 1 - \pi)(P_0 - P_\infty),$$

我们得出 $q^3 + 1 - \pi \in H(P_\infty)$，其中 $0 < q^3 + 1 - \pi \le q^2 - q + 1 < q^3 - q^2 + q$，这与假设矛盾。这意味着 $\pi = q^3 + 1$。□

根据前面的结果和注记 3.2，我们有 $\Gamma_{k,\,0} = \emptyset$，对于 $k \ge q^2 - 1$。此外，根据 $\gamma_{i,\,j,\,k}$ 的定义以及命题 4.4，我们有 $\gamma_{i,\,j,\,k} \in \Gamma_{k-1,\,0}$ 当且仅当 $j = k - i + 1$。因此，对于 $1 \le k \le q^2 - 1$,

$$\begin{aligned}\Gamma_{k-1,0} &= \{\gamma_{i,j,k} : \max\{0, k-q^2+q+1\} \le i \le q,\ \max\{0, k-i+1\} \le j \le q^2-q\} \\ &= \{\gamma_{i,j,k} : \max\{0, k-q^2+q+1\} \le i \le q,\ k-q^2+q+1 \le i \le k+1\} \\ &= \{\gamma_{i,k-i+1,k} : \max\{0, k-q^2+q+1\} \le i \le \min\{q, k+1\}\}.\end{aligned}$$

Thus

$$\Gamma_{k,0} = \{\gamma_{i,k-i+2,k+1} : \max\{0, k-q^2+q+2\} \le i \le \min\{q, k+2\}\} \text{ for } 0 \le k \le q^2-2.$$

So,

$$|\Gamma_{k,0}| = \begin{cases} k+3, & \text{if } 0 \le k \le q-2, \\ q+1, & \text{if } q-1 \le k \le q^2-q-3, \\ q^2-1-k, & \text{if } q^2-q-2 \le k \le q^2-2. \end{cases} \tag{14}$$

那么，根据命题 3.7，我们有

$$\begin{aligned}|G_0(P_0,P_\infty)| &\le \sum_{0\le k}(k+1)\left(\sum_{k\le k_1}|\Gamma_{k_1,0}|\right)^2 - g \\ &= \sum_{k=0}^{q-2}(k+1)\left(\sum_{k_1=k}^{q-2}(k_1+3) + \sum_{k_1=q-1}^{q^2-q-3}(q+1) + \sum_{k_1=q^2-q-2}^{q^2-2}(q^2-1-k_1)\right)^2 \\ &\quad + \sum_{k=q-1}^{q^2-q-3}(k+1)\left(\sum_{k_1=k}^{q^2-q-3}(q+1) + \sum_{k_1=q^2-q-2}^{q^2-2}(q^2-1-k_1)\right)^2 \\ &\quad + \sum_{k=q^2-q-2}^{q^2-2}(k+1)\left(\sum_{k_1=q^2-q-2}^{q^2-2}(q^2-1-k_1)\right)^2 \\ &\quad - \left(\frac{1}{2}(q^3+1)(q^2-2)+1\right) \\ &= \frac{10q^{10}-15q^8-4q^7+20q^6-56q^5-35q^4+124q^3-40q^2-4q}{120}.\end{aligned}$$

最后一个等式是利用SageMath程序 [9]得到的。我们注意到，对于 $q \geq 3$，这个界优于（1）中给出的界。

现在，利用集合 $\Gamma_{k,\ 0}$ 的描述、关系 (9) 和命题 3.4，在以下引理中，我们将完全确定式 (11) 给出的集合 $G^1_{k,\ 0}$、$G^2_{k,\ 0}$、$G^3_{k,\ 0}$ 和 $G^4_{k,\ 0}$，从而得到 $G_0(P_0, P_\infty)$。注意，根据注 3.8，若 $k \geq q^2-2$，则 $G^1_{k,\ 0} = G^3_{k,\ 0} = G^4_{k,\ 0} = \emptyset$；若 $k \geq q^2-1$，则 $G^2_{k,\ 0} = \emptyset$。

引理 4.5。对于 $0 \leq k \leq q^2-3$，我们有

$$G^1_{k,0} = \left\{ \gamma^{i_2,k_2-i_2+2,k+1}_{i_1,k_1-i_1+2,1} : \begin{array}{l} \max\{0, k_s - q^2 + q + 2\} \leq i_s \leq \min\{q, k_s + 2\} \\ and\ k < k_s \leq q^2 - 2\ for\ s = 1, 2 \end{array} \right\}\ and$$

$$G^3_{k,0} = \left\{ \gamma^{i_2,k-i_2+2,k+1}_{i_1,k_1-i_1+2,1} : \begin{array}{l} \max\{0, k_1 - q^2 + q + 2\} \leq i_1 \leq \min\{q, k_1 + 2\}, \\ \max\{0, k - q^2 + q + 2\} \leq i_2 \leq \min\{q, k + 2\}, \\ i_2 \leq i_1\ and\ k < k_1 \leq q^2 - 2 \end{array} \right\},$$

其中

$$\gamma^{a_2,b_2,c_2}_{a_1,b_1,c_1} = ((c_2-1)(q^3+1)+(q+1-a_2)(q^2-q+1)-b_2, (c_1-1)(q^3+1)+(q+1-a_1)(q^2-q+1)-b_1).$$

证明。我们首先计算集合 $G^1_{k,\ 0}$。设 k_1, k_2 为正整数，使得$k < k_1, k_2 \leq q^2-2$。对于 $\gamma_{i_1,\ k_1-i_1+2,\ k_1+1} \in \Gamma_{k_1,\ 0}$ 以及 $\gamma_{i_2,\ k_2-i_2+2,\ k_2+1} \in \Gamma_{k_2,\ 0}$，我们有

$$\mathrm{glb}(\gamma_{i_2,k_2-i_2+2,k_2+1} + \mathbf{w}_{k_2-k}, \gamma_{i_1,k_1-i_1+2,k_1+1}) = \gamma^{i_2,k_2-i_2+2,k+1}_{i_1,k_1-i_1+2,1}.$$

由 (11)，我们得出

$$G^1_{k,0} = \left\{ \gamma^{i_2,k_2-i_2+2,k+1}_{i_1,k_1-i_1+2,1} : \begin{array}{l} \max\{0, k_s - q^2 + q + 2\} \leq i_s \leq \min\{q, k_s + 2\} \\ \text{and } k < k_s \leq q^2 - 2 \text{ for } s = 1, 2 \end{array} \right\}.$$

现在，设 k_1 为正整数，使得 $k < k_1 \leq q^2 - q$。对于 $\gamma_{i_2,\ k-i_2+2,\ k+1} \in \Gamma_{k,\ 0}$ 以及$\gamma_{i_1,\ k_1-i_1+2,\ k_1+1} \in \Gamma_{k_1,\ 0}$，我们得到

$$\begin{aligned} \gamma_{i_2,k-i_2+2,k+1} \not\preceq \gamma_{i_1,k_1-i_1+2,k_1+1} &\Leftrightarrow (i_2 - i_1)(q^2 - q) < k_1 - k \\ &\Leftrightarrow i_2 \leq i_1. \end{aligned}$$

假设 $i_2 \leq i_1$，我们可推出

$$\mathrm{glb}(\gamma_{i_2,k-i_2+2,k+1}, \gamma_{i_1,k_1-i_1+2,k_1+1}) = \gamma^{i_2,k-i_2+2,k+1}_{i_1,k_1-i_1+2,1}$$

因此

$$G^3_{k,0} = \left\{ \gamma^{i_2,k-i_2+2,k+1}_{i_1,k_1-i_1+2,1} : \begin{array}{l} \max\{0, k_1 - q^2 + q + 2\} \leq i_1 \leq \min\{q, k_1 + 2\}, \\ \max\{0, k - q^2 + q + 2\} \leq i_2 \leq \min\{q, k + 2\}, \\ i_2 \leq i_1 \text{ and } k < k_1 \leq q^2 - 2 \end{array} \right\}.$$

□

引理 4.6。以下陈述成立：

(i) 对于 $0 \leq k \leq q^2-2$, $G^2_{k,\ 0} = \emptyset$。(ii) 对于 $0 \leq k \leq q^2-3$, $G^4_{k,\ 0} = \{(b, a) \in \mathbb{N}^2 : (a, b) \in G^3_{k,\ 0}\} - \mathbf{w}_k$，其中 $G^3_{k,\ 0}$ 如前一引理中所给出。

证明。F rom 由 (13) 和命题 4.4 中给出的 $\Gamma(P_0, P_\infty)$ 的描述，我们有

$$\beta \equiv \tau_{P_0,P_\infty}(\beta) \pmod{q^3+1} \text{ for each } \beta \in G(P_0).$$

该结果可直接由引理 3.9 得出。 □

定理 4.7。设上述引理中给出的 $G^1_{k,0}$,$G^3_{k,0}$ 和 $G^4_{k,0}$ 。则

$$G_0(P_0,P_\infty) = \bigcup_{0\le j\le k\le q^2-3} \left((G^1_{k,0}\cup G^3_{k,0}\cup G^4_{k,0}) + \mathbf{w}_j\right)$$

and

$$|G_0(P_0,P_\infty)| = \frac{q(q-1)(10q^8+10q^7-25q^6-9q^5+71q^4-111q^3-86q^2+128q-12)}{120}.$$

证明。由式 (14) 和引理 3.5，可得

$$|G^1_{k,0}| = \begin{cases} \frac{1}{4}(2q^3-k^2-7k-10)^2, & \text{if } 0\le k\le q-2,\\ \frac{1}{4}(2q^3-2(k+4)q+q^2-2k+3q-4)^2, & \text{if } q-1\le k\le q^2-q-3,\\ \frac{1}{4}(q^4-(2k+3)q^2+k^2+3k+2)^2, & \text{if } q^2-q-2\le k\le q^2-3. \end{cases}$$

另一方面，根据引理 4.5 中对 $G^3_{k,0}$ 的描述，我们可以推得，对于每个 $0\le k\le q^2-3$,

$$|G^3_{k,0}| = \sum_{i_2=\max\{0,k-q^2+q+2\}}^{\min\{q,k+2\}} \sum_{k_1=k+1}^{q^2-3} (\min\{q,k_1+2\} - \max\{i_2,k_1-q^2+q+2\}+1).$$

因此，为了确定 $|G^3_{k,\ 0}|$ 我们将分三种情况进行计算。

◇ 对于 $0\le k\le q-2$,

$$\begin{aligned} |G^3_{k,0}| &= \sum_{i_2=0}^{k+2}\sum_{k_1=k+1}^{q^2-3} (\min\{q,k_1+2\} - \max\{i_2,k_1-q^2+q+2\}+1)\\ &= \sum_{i_2=0}^{k+2}\left(\sum_{k_1=k+1}^{q-2}(k_1+3-i_2) + \sum_{k_1=q-1}^{q^2-q-2+i_2}(q+1-i_2) + \sum_{k_1=q^2-q-1+i_2}^{q^2-3}(q^2-1-k_1)\right)\\ &= (k+3)\left(q^3-5-\frac{2k^2+39k+10}{12} - \frac{(2q^2-2q-5)(k+2)}{4}\right). \end{aligned}$$

◇ 对于 $q-1 \leq k \leq q^2-q-3$,

$$\begin{aligned}|G^3_{k,0}| &= \sum_{i_2=0}^{q} \sum_{k_1=k+1}^{q^2-3} (\min\{q, k_1+2\} - \max\{i_2, k_1-q^2+q+2\}+1) \\ &= \sum_{i_2=0}^{q} \left(\sum_{k_1=k+1}^{q^2-q-2+i_2} (q+1-i_2) + \sum_{k_1=q^2-q-1+i_2}^{q^2-3} (q^2-1-k_1) \right) \\ &= (q+1)\left(\frac{3q^3+5q^2-8q-12}{6} - \frac{k(q+2)}{2}\right).\end{aligned}$$

◇ 对于 $q^2-q-2 \leq k \leq q^2-3$,

$$\begin{aligned}|G^3_{k,0}| &= \sum_{i_2=k-q^2+q+2}^{q} \sum_{k_1=k+1}^{q^2-3} (\min\{q, k_1+2\} - \max\{i_2, k_1-q^2+q+2\}+1) \\ &= \sum_{i_2=k-q^2+q+2}^{q} \left(\sum_{k_1=k+1}^{q^2-q-2+i_2} (q+1-i_2) + \sum_{k_1=q^2-q-1+i_2}^{q^2-3} (q^2-1-k_1) \right) \\ &= \frac{q^2(q^4-3q^2+2)}{3} - \frac{k^2(k-3q^2+3)}{3} - \frac{k(3q^4-6q^2+2)}{3}.\end{aligned}$$

现在，根据引理 4.6，$|G^4_{k,\ 0}| = |G^3_{k,\ 0}|$。由于 $|G_{k,\ 0}| = |G^1_{k,\ 0}| + 2|G^3_{k,\ 0}|$ 对每个 $0 \leq k \leq q^2-3$ 都成立，因此由 (7) 并使用 SageMath 程序进行一些计算后，我们得到

$$|G_0(P_0, P_\infty)| = \frac{q(q-1)(10q^8+10q^7-25q^6-9q^5+71q^4-111q^3-86q^2+128q-12)}{120}.$$

□

例 4.8. 对于 $q=2$，GK 曲线的纯间隙集 $G_0(P_0, P_\infty)$ 为

$$\begin{aligned}G_0(P_0,P_\infty) \ = \ & \left(G^1_{0,0} \cup G^3_{0,0} \cup G^4_{0,0}\right) \\ \bigcup \ & \left(G^1_{1,0} \cup G^3_{1,0} \cup G^4_{1,0}\right) \\ \bigcup \ & \left(G^1_{1,0} \cup G^3_{1,0} \cup G^4_{1,0}\right) + (-9, 9),\end{aligned}$$

其中

$$\begin{aligned}G^1_{0,0} &= \{(1,1),(1,2),(1,4),(2,1),(2,2),(2,4),(4,1),(4,2),(4,4)\} \\ G^3_{0,0} &= \{(3,1),(3,2),(5,1),(5,2),(5,4),(7,1),(7,2),(7,4)\} \\ G^4_{0,0} &= \{(1,3),(1,5),(1,7),(2,3),(2,5),(2,7),(4,5),(4,7)\} \\ G^1_{1,0} &= \{(10,1)\} \\ G^3_{1,0} &= \{(11,1),(13,1)\} \\ G^4_{1,0} &= \{(10,2),(10,4)\}.\end{aligned}$$

因此，我们得到

$$G_0(P_0,P_\infty)=\left\{\begin{array}{l}(1,1),(1,2),(1,3),(1,4),(1,5),(1,7),(1,10),(1,11),(1,13),(2,1),\\(2,2),(2,3),(2,4),(2,5),(2,7),(2,10),(3,1),(3,2),(4,1),(4,2),\\(4,4),(4,5),(4,7),(4,10),(5,1),(5,2),(5,4),(7,1),(7,2),(7,4),\\(10,1),(10,2),(10,4),(11,1),(13,1)\end{array}\right\},$$

其基数为 $|G_0(P_0,P_\infty)|=35$。

4.2. 库默尔扩张。设 K 为 $\mathbb{F}_q$ 的代数闭包，并考虑由方程定义的库默尔扩张

$$\mathcal{X}:\quad Y^m=f(X)^\lambda,$$

其中，$\lambda\in\mathbb{N}$, $m\geq 2$ 是一个整数，满足 $\mathrm{Char}(K)=p\nmid m$，且 $f(X)\in K[X]$ 是一个次数为 $r\geq 2$、满足 $\gcd(m,\lambda r)=1$的可分多项式。设 $K(\mathcal{X})$ 为其函数域，其亏格为 $g=\frac{1}{2}(m-1)(r-1)$。记 P_∞ 为唯一的无穷远点，并设P_1,P_2为扩张 $K(\mathcal{X})/K(x)$ 中不同于 P_∞ 的全分歧点。纯间隙集 $G_0(P_1,P_2)$ 已在 [12, 推论 3] 中得到明确确定。在本小节中，我们将给出 $G_0(P_1,P_2)$ 的另一种显式描述，并计算其基数。

设 α_1 和 α_2 是与点 P_1 和 P_2 分别对应的 $f(X)$ 的根，则对于 $i=1,\ 2$，我们有主因子 $(x-\alpha_i)=m(P_i-P_\infty)$。因此，

$$\left(\frac{x-\alpha_1}{x-\alpha_2}\right)=m(P_1-P_2). \tag{15}$$

命题 4.9. 半群 $H(P_1,P_2)$ 的周期为 $\pi=m$。

证明. 由 (15)，我们有 $\pi\leq m$。设 $1\leq\pi\leq m-1$，并令 $z\in K(\mathcal{X})$ 满足 $(z)=\pi(P_1-P_2)$。由命题 3.3], , $H(P_2)$ 的最小非零元素为 $m-\lfloor m/r\rfloor$，因此 $m-\lfloor m/r\rfloor\leq\pi\leq m-1$。由于

$$\left(\frac{x-\alpha_1}{z(x-\alpha_2)}\right)=(m-\pi)(P_1-P_2)\ ,$$

我们得到 $m-\pi\in H(P_2)$ 且 $0<m-\pi\leq m-(m-\lfloor m/r\rfloor)=\lfloor m/r\rfloor<m-\lfloor m/r\rfloor$，矛盾。这意味着 $\pi=m$。□

由注记 3.2 可知，对于 $k\geq r-1-\lfloor r/m\rfloor$，有 $\Gamma_{k,\ 0}=\emptyset$。为了确定 $k\leq r-2-\lfloor r/m\rfloor$ 的 $\Gamma_{k,\ 0}$，我们将使用 [20, 定理 8] 中给出的极小生成集 $\Gamma(P_1,P_2)$ 的如下描述:

$$\Gamma(P_1,P_2)=\left\{(mk_1+j,mk_2+j)\in\mathbb{N}^2:1\leq j\leq m-1-\left\lfloor\frac{m}{r}\right\rfloor,\ k_1\geq 0,\ k_2\geq 0,\right.\\ \left.\text{and } k_1+k_2=r-2-\left\lfloor\frac{rj}{m}\right\rfloor\right\}. \tag{16}$$

所以，我们得到以下结果。

命题 4.10。对于 $0 \leq k \leq r-2-\lfloor r/m \rfloor$,

$$\Gamma_{k,0} = \left\{ (mk+j, j) \in \mathbb{N}^2 : \max\left\{1, m - \left\lfloor \frac{m(k+2)}{r} \right\rfloor\right\} \leq j \leq m-1-\left\lfloor \frac{m(k+1)}{r} \right\rfloor \right\}$$

and

$$|\Gamma_{k,0}| = \left\lceil \frac{m(k+2)}{r} \right\rceil - \left\lceil \frac{m(k+1)}{r} \right\rceil.$$

证明。由 (16) 和命题 4.9，我们推得，对于 $0 \leq k \leq r-2-\lfloor r/m \rfloor$,

$$\begin{aligned}
\Gamma_{k,0} &= \left\{ (mk+j, j) : 1 \leq j \leq m-1-\left\lfloor \frac{m}{r} \right\rfloor,\ k = r-2-\left\lfloor \frac{rj}{m} \right\rfloor \right\} \\
&= \left\{ (mk+j, j) : 1 \leq j \leq m-1-\left\lfloor \frac{m}{r} \right\rfloor,\ m - \left\lfloor \frac{m(k+2)}{r} \right\rfloor \leq j \leq m-1-\left\lfloor \frac{m(k+1)}{r} \right\rfloor \right\} \\
&= \left\{ (mk+j, j) : \max\left\{1, m - \left\lfloor \frac{m(k+2)}{r} \right\rfloor\right\} \leq j \leq m-1-\left\lfloor \frac{m(k+1)}{r} \right\rfloor \right\}.
\end{aligned}$$

这意味着

$$|\Gamma_{k,0}| = m - \left\lfloor \frac{m(k+1)}{r} \right\rfloor - \max\left\{1, m - \left\lfloor \frac{m(k+2)}{r} \right\rfloor\right\}.$$

$\diamond$ 如果 $k < r-2-\lfloor r/m \rfloor$ 那么 $1 < m - \lfloor m(k+2)/r \rfloor$ 并且

$$|\Gamma_{k,0}| = \left\lfloor \frac{m(k+2)}{r} \right\rfloor - \left\lfloor \frac{m(k+1)}{r} \right\rfloor = \left\lceil \frac{m(k+2)}{r} \right\rceil - \left\lceil \frac{m(k+1)}{r} \right\rceil.$$

$\diamond$ 如果 $k = r-2-\lfloor r/m \rfloor$ 那么 $m - \lfloor m(k+2)/r \rfloor \leq 1$ 并且

$$|\Gamma_{k,0}| = m - \left\lfloor \frac{m(r-1)}{r} \right\rfloor - 1 = m - \left\lceil \frac{m(r-1)}{r} \right\rceil.$$

至此证明完毕。 □

现在，利用前述命题，我们将计算 $i = 1$、2、3、4 对应的集合 $G^i_{k,0}$。我们注意到，根据注 3.8，若 $k \geq r-2-\lfloor r/m \rfloor$，则 $G^1_{k,0} = G^3_{k,0} = G^4_{k,0} = \emptyset$；若 $k \geq r-1-\lfloor r/m \rfloor$，则 $G^2_{k,0} = \emptyset$。

引理 4.11. 对于 $0 \leq k \leq r-3-\lfloor r/m \rfloor$,

$$\begin{aligned}
G^1_{k,0} &= \{(mk+j_2, j_1) : 1 \leq j_i \leq m-1-\lfloor m(k+2)/r \rfloor \text{ for } i = 1, 2\}, \\
G^3_{k,0} &= \left\{ (mk+j, j_1) : \begin{array}{l} m-\lfloor m(k+2)/r \rfloor \leq j \leq m-1-\lfloor m(k+1)/r \rfloor \\ \text{and } 1 \leq j_1 \leq m-1-\lfloor m(k+2)/r \rfloor \end{array} \right\}, \text{ and} \\
G^4_{k,0} &= \{(b, a) \in \mathbb{N}^2 : (a, b) \in G^3_{k,0}\} - \mathbf{w}_k.
\end{aligned}$$

此外，$G^2_{k,0} = \emptyset$ 对于 $0 \leq k \leq r-2-\lfloor r/m \rfloor$。

证明. 我们首先注意到，根据式 (16) 中对 $\Gamma(P_1,P_2)$ 的描述，对于每个 $\beta\in G(P_1)$，有 $\beta\equiv\tau_{P_1,P_2}(\beta)\pmod m$。因此，由引理 3.9，我们得到集合 $G^2_{k,0}$ 和$G^4_{k,0}$的结果。

对于每个 $0\le k\le r-3-\lfloor r/m\rfloor$，令 $\mathbf{u}=(mk_2+j_2,j_2)\in\Gamma_{k_2,\,0}$ 且 $\mathbf{v}=(mk_1+j_1,j_1)\in\Gamma_{k_1,\,0}$，其中 $k<k_i\le r-2-\lfloor r/m\rfloor$ 对于 $i=1,\ 2$。于是 $\mathbf{u}+\mathbf{w}_{k_2-k}=(mk+j_2,m(k_2-k)+j_2)$，因此

$$\mathrm{glb}(\mathbf{u}+\mathbf{w}_{k_2-k},\mathbf{v})=(mk+j_2,j_1).$$

因此，由 (11) 和命题 4.10 可得，

$$G^1_{k,0}=\left\{(mk+j_2,j_1):\ \begin{array}{l}\max\{1,m-\lfloor m(k_i+2)/r\rfloor\}\le j_i\le m-1-\lfloor m(k_i+1)/r\rfloor\\ \text{and } k<k_i\le r-2-\lfloor r/m\rfloor \text{ for } i=1,2\end{array}\right\}.$$

注意，对于 $i=1,\ 2$，$\max\{1,m-\lfloor m(k_i+2)/r\rfloor\}=1$ 当且仅当 $k_i=r-2-\lfloor r/m\rfloor$。因此，考虑上述集合 $G^1_{k,0}$ 中的区间，对于每个 $i=1,\ 2$，我们有

$$\text{for } k_i=k+1:\quad m-\left\lfloor\frac{m(k+3)}{r}\right\rfloor\le j_i\le m-1-\left\lfloor\frac{m(k+2)}{r}\right\rfloor;$$

$$\text{for } k_i=k+2:\quad m-\left\lfloor\frac{m(k+4)}{r}\right\rfloor\le j_i\le m-1-\left\lfloor\frac{m(k+3)}{r}\right\rfloor;$$

$$\vdots$$

$$\text{for } k_i=r-3-\lfloor r/m\rfloor:\quad m-\left\lfloor\frac{m(r-1-\lfloor r/m\rfloor)}{r}\right\rfloor\le j_i\le m-1-\left\lfloor\frac{m(r-2-\lfloor r/m\rfloor)}{r}\right\rfloor;$$

$$\text{for } k_i=r-2-\lfloor r/m\rfloor:\quad 1\le j_i\le m-1-\left\lfloor\frac{m(r-1-\lfloor r/m\rfloor)}{r}\right\rfloor.$$

因此，我们有 $1\le j_i\le m-1-\lfloor m(k+2)/r\rfloor$，并得到

$$G^1_{k,0}=\left\{(mk+j_2,j_1):1\le j_i\le m-1-\lfloor m(k+2)/r\rfloor \text{ for } i=1,2\right\}.$$

现在，为了计算集合 $G^3_{k,\,0}$，令 $\mathbf{u}=(mk+j,j)\in\Gamma_{k,\,0}$ 以及 $\mathbf{v}=(mk_1+j_1,j_1)\in\Gamma_{k_1,\,0}$，其中 $k<k_1\le r-2-\lfloor r/m\rfloor$。于是，由命题 4.10，

$$m-\left\lfloor\frac{m(k+2)}{r}\right\rfloor\le j\le m-1-\left\lfloor\frac{m(k+1)}{r}\right\rfloor$$

and

$$\max\left\{1,m-\left\lfloor\frac{m(k_1+2)}{r}\right\rfloor\right\}\le j_1\le m-1-\left\lfloor\frac{m(k_1+1)}{r}\right\rfloor.$$

由于 $k<k_1$，我们得到 $mk+j<mk_1+j_1$ 且

$$j_1\le m-1-\left\lfloor\frac{m(k_1+1)}{r}\right\rfloor\le m-1-\left\lfloor\frac{m(k+2)}{r}\right\rfloor\le j-1<j.$$

这意味着 $\mathbf{u} \not\equiv \mathbf{v}$，并且由 (11) 可得

$$G^3_{k,0} = \{\mathrm{glb}(\mathbf{u},\mathbf{v}) : \mathbf{u} \in \Gamma_{k,0},\ \mathbf{v} \in \Gamma_{k_1,0},\ k < k_1\}$$
$$= \left\{ (mk+j, j_1) : \begin{array}{l} m - \lfloor m(k+2)/r \rfloor \le j \le m-1-\lfloor m(k+1)/r \rfloor, \\ \max\{1, m-\lfloor m(k_1+2)/r \rfloor\} \le j_1 \le m-1-\lfloor m(k_1+1)/r \rfloor, \\ \text{and } k < k_1 \le r-2-\lfloor r/m \rfloor \end{array} \right\}.$$

通过类似的方法确定上面的集合 $G^1_{k,0}$，可得

$$G^3_{k,0} = \left\{ (mk+j, j_1) : \begin{array}{l} m - \lfloor m(k+2)/r \rfloor \le j \le m-1-\lfloor m(k+1)/r \rfloor \\ \text{and } 1 \le j_1 \le m-1-\lfloor m(k+2)/r \rfloor \end{array} \right\}.$$

□

定理 4.12. 设 P_1 和 P_2 是扩张 $K(\mathcal{X})/K(x)$ 的全分歧点，且与 P_∞ 不同。设 $G^1_{k,0}$、$G^3_{k,0}$ 和 $G^4_{k,0}$ 是上引理中给出的集合。则

$$G_0(P_1,P_2) = \bigcup_{0 \le j \le k \le r-3-\lfloor r/m \rfloor} \left((G^1_{k,0} \cup G^3_{k,0} \cup G^4_{k,0}) + \mathbf{w}_j \right)$$

and

$$|G_0(P_1,P_2)| = \sum_{k=1}^{r-2-\lfloor r/m \rfloor} k \left[\left(m - \left\lceil \frac{mk}{r} \right\rceil \right)^2 - \left(\left\lceil \frac{m(k+1)}{r} \right\rceil - \left\lceil \frac{mk}{r} \right\rceil \right)^2 \right].$$

证明. 由引理 4.11，我们推得 $|G^2_{k,0}| = 0$, $|G^3_{k,0}| = |G^4_{k,0}|$ 和

$$|G^3_{k,0}| = |\{\mathrm{glb}(\mathbf{u},\mathbf{v}) : \mathbf{u} \in \Gamma_{k,0},\ \mathbf{v} \in \Gamma_{k_1,0},\ k < k_1\}| = |\Gamma_{k,0}| \left(\sum_{k<k_1} |\Gamma_{k_1,0}| \right)$$

对每个 $0 \le k \le r-3-\lfloor r/m \rfloor$。注意，在这种情况下，$|G^3_{k,0}|$ 和 $|G^4_{k,0}|$ 达到了式 (10) 给出的上界。此外，由式 (9) 和引理 3.5，我们得到

$$|G_{k,0}| = \left(\sum_{k<k_1} |\Gamma_{k_1,0}| \right)^2 + 2|\Gamma_{k,0}| \left(\sum_{k<k_1} |\Gamma_{k_1,0}| \right) = \left(\sum_{k \le k_1} |\Gamma_{k_1,0}| \right)^2 - |\Gamma_{k,0}|^2.$$

最后，由式 (7) 和命题 4.10，

$$\begin{aligned}
|G_0(P_1,P_2)| &= \sum_{0\le k}(k+1)|G_{k,0}| \\
&= \sum_{k=0}^{r-3-\lfloor r/m\rfloor}(k+1)\left[\left(\sum_{k_1=k}^{r-2-\lfloor r/m\rfloor}|\Gamma_{k_1,0}|\right)^2-|\Gamma_{k,0}|^2\right] \\
&= \sum_{k=0}^{r-3-\lfloor r/m\rfloor}(k+1)\left[\left(m-\left\lceil\frac{m(k+1)}{r}\right\rceil\right)^2-\left(\left\lceil\frac{m(k+2)}{r}\right\rceil-\left\lceil\frac{m(k+1)}{r}\right\rceil\right)^2\right] \\
&= \sum_{k=1}^{r-2-\lfloor r/m\rfloor}k\left[\left(m-\left\lceil\frac{mk}{r}\right\rceil\right)^2-\left(\left\lceil\frac{m(k+1)}{r}\right\rceil-\left\lceil\frac{mk}{r}\right\rceil\right)^2\right].
\end{aligned}$$

□

纯间隙集 $G_0(P_1,P_2)$ 的基数，在 $m=ur+1$ 的情形下由 [2, 定理 3.2] 的证明确定，其中 u 是正整数；在 $m=(q+1)/N$ 的情形下，则由 [21, 推论 12] 确定，其中 N 是 $q+1$ 的因子，且满足 $q-2-N\ge 0$ 和 $r=q$。下面我们将验证，对于这些情形，定理 4.12 也能以比上述参考文献作者所用方法更简单的方式得到相同的基数。

◇ 对于某个正整数 $u\in\mathbb{N}$ 的情形 $m=ur+1$。根据定理 4.12，我们有

$$\begin{aligned}
|G_0(P_1,P_2)| &= \sum_{k=1}^{r-2-\lfloor r/m\rfloor}k\left[\left(m-\left\lceil\frac{mk}{r}\right\rceil\right)^2-\left(\left\lceil\frac{m(k+1)}{r}\right\rceil-\left\lceil\frac{mk}{r}\right\rceil\right)^2\right] \\
&= \sum_{k=1}^{r-2}k\left[\left(ur+1-\left\lceil\frac{(ur+1)k}{r}\right\rceil\right)^2-\left(\left\lceil\frac{(ur+1)(k+1)}{r}\right\rceil-\left\lceil\frac{(ur+1)k}{r}\right\rceil\right)^2\right] \\
&= \sum_{k=1}^{r-2}k\left[(ur+1-(uk+1))^2-((u(k+1)+1)-(uk+1))^2\right] \\
&= u^2\left((r^2-1)\sum_{k=1}^{r-2}k-2r\sum_{k=1}^{r-2}k^2+\sum_{k=1}^{r-2}k^3\right) \\
&= u^2(r-1)(r-2)\left(\frac{r^2-1}{2}-\frac{r(2r-3)}{3}+\frac{(r-2)(r-1)}{4}\right) \\
&= \frac{u^2(r-1)(r-2)r(r+3)}{12}.
\end{aligned}$$

注意，对于 $u=1$，我们有

$$|G_0(P_1,P_2)|=\frac{(r-1)(r-2)r(r+3)}{12}.$$

现在，由命题 4.10 可得，

$$|\Gamma_{k,0}| = \left\lceil \frac{(r+1)(k+2)}{r} \right\rceil - \left\lceil \frac{(r+1)(k+1)}{r} \right\rceil = k+2-(k+1) = 1,$$

因此

$$\begin{aligned}
\sum_{k=0}^{r-2}(k+1)\left(\sum_{k_1=k}^{r-2}|\Gamma_{k_1,0}|\right)^2 - g &= \sum_{k=0}^{r-2}(k+1)\,(r-1-k)^2 - \frac{r(r-1)}{2} \\
&= \sum_{k=1}^{r-1} k\,(r-k)^2 - \frac{r(r-1)}{2} \\
&= r^2\sum_{k=1}^{r-1}k - 2r\sum_{k=1}^{r-1}k^2 + \sum_{k=1}^{r-1}k^3 - \frac{r(r-1)}{2} \\
&= \frac{(r-1)r^3}{2} - \frac{(r-1)r^2(2r-1)}{3} + \frac{(r-1)^2r^2}{4} - \frac{r(r-1)}{2} \\
&= \frac{(r-1)(r-2)r(r+3)}{12}.
\end{aligned}$$

因此，对于 $m = r+1$， $G_0(P_1,P_2)$ 的基数达到命题 3.7 给出的上界，所以我们得出该上界是紧的。

◇ 情形 $m = (q+1)/N$，其中 N 是 $q+1$ 的一个因子，使得 $q-2-N \geq 0$ 且 $r = q$。因此，$r-2-\lfloor r/m \rfloor = q-1-N = (m-2)N+N-2$。写作 $k = N\ell_k + j$，其中 $0 \leq \ell_k \leq m-2$ 且 $0 \leq j \leq N-1$，我们有

$$\left\lceil \frac{mk}{r} \right\rceil = \ell_k + 1, \text{ if } 0 \leq \ell_k \leq m-2 \text{ and } 0 \leq j \leq N-1\,,$$

and

$$\left\lceil \frac{m(k+1)}{r} \right\rceil = \begin{cases} \ell_k+1, & \text{if } 0 \leq \ell_k \leq m-2 \text{ and } 0 \leq j \leq N-2, \\ \ell_k+2, & \text{if } 0 \leq \ell_k \leq m-3 \text{ and } j = N-1. \end{cases}$$

现在，对每个 $1 \leq k \leq q-1-N$，定义

$$h(k) = k\left[\left(m - \left\lceil \frac{mk}{r} \right\rceil\right)^2 - \left(\left\lceil \frac{m(k+1)}{r} \right\rceil - \left\lceil \frac{mk}{r} \right\rceil\right)^2\right].$$

因此，由定理 4.12 可得

$$
\begin{aligned}
|G_0(P_1,P_2)| &= \sum_{k=1}^{r-2-\lfloor r/m\rfloor} h(k)\\
&= \sum_{j=1}^{N-1} h(j) + \sum_{\ell_k=1}^{m-3}\sum_{j=0}^{N-1} h(N\ell_k+j) + \sum_{j=0}^{N-2} h(N(m-2)+j)\\
&= \sum_{j=1}^{N-2} h(j) + h(N-1) + \sum_{\ell_k=1}^{m-3}\sum_{j=0}^{N-2} h(N\ell_k+j) + \sum_{\ell_k=1}^{m-3} h(N\ell_k+N-1)\\
&\quad + \sum_{j=0}^{N-2} h(N(m-2)+j)\\
&= \sum_{j=1}^{N-2} j(m-1)^2 + (N-1)((m-1)^2-1) + \sum_{\ell_k=1}^{m-3}\sum_{j=0}^{N-2}(N\ell_k+j)(m-\ell_k-1)^2\\
&\quad + \sum_{\ell_k=1}^{m-3}(N(\ell_k+1)-1)[(m-\ell_k-1)^2-1] + \sum_{j=0}^{N-2}(N(m-2)+j)\\
&= \frac{(q+1)(m-1)}{12}((q+1)(m-1)-2m+N+7) - q(m-1).
\end{aligned}
$$

这个关于 $|G_0(P_1,P_2)|$ 的公式与 [21, 推论 12] 中给出的公式相同。

References

[1] D. Bartoli、A. M. Masuda、M. Montanucci 和 L. Quoos。具有大量有理点的曲线上的纯间隙。Finite Fields Appl., 53:287–308，2018。[2] D. Bartoli、L. Quoos 和 G. Zini。来自库默尔扩张的多点代数几何码。Finite Fields Appl., 52:319–335，2018。[3] P. Beelen 和 D. Ruano。利用魏尔施特拉斯半群的一种推广界定曲线上的点数。Des. Codes Cryptogr., 66(1-3):221–230，2013。[4] H. M. Borges Filho 和 G. Duran Cunha。具有三个指定点的曲线上的魏尔施特拉斯纯间隙。IEEE Trans. Inform. Theory, 68(5):3062–3069，2022。[5] C. Carvalho 和 F. Torres。关于多个点处的 Goppa 码和魏尔施特拉斯间隙。Des. Codes Cryptogr., 35(2):211–225，2005。[6] A. S. Castellanos、A. M. Masuda 和 L. Quoos。库默尔扩张上的单点码与双点码。IEEE Trans. Inform. Theory, 62(9):4867–4872，2016。[7] A. S. Castellanos、E. A. R. Mendoza 和 L. Quoos。库默尔扩张上的魏尔斯特拉斯半群、纯间隙与码。预印本，2023。ArXiv:2304.02128。[8] A. S. Castellanos 和 G. C. Tizziotti。GK 极大曲线上的双点代数几何码。IEEE Trans. Inform. Theory, 62(2):681–686，2016。[9] B. Er¨ocal 和 W. Stein。Sage 数学软件（9.8 版），Sage 开发团队，2010。载于《数学软件——ICMS 2010》，计算机科学讲义第 6327 卷，第 12–27 页。Springer，柏林，2010。

[10] M. Giulietti 和 G. Korchm´aros. 有限域上的一个新的极大曲线族. Math. Ann., 343(1):229–245, 2009.[11] M. Homma 和 S. J. Kim. 具有魏尔斯特拉斯点对的 Goppa 码. J. Pure Appl. Algebra, 162(2-3):273– 290, 2001.[12] C. Hu 和 S. Yang. 库默尔扩张上的多点码. Des. Codes Cryptogr., 86(1):211–230, 2018.[13] S. J. Kim. 曲线上一对点的魏尔斯特拉斯半群的指标. Arch. Math. (Basel), 62(1):73–82, 1994.[14] G. L. Matthews. 魏尔斯特拉斯点对与 Goppa 码的最小距离. Des. Codes Cryptogr., 22(2):107–121, 2001.[15] G. L. Matthews. Suzuki 函数域上的码. IEEE Trans. Inform. Theory, 50(12):3298– 3302, 2004.[16] G. L. Matthews. 厄米特曲线上一组共线点的魏尔斯特拉斯半群. 收录于《有限域及其应用》, Lecture Notes in Comput. Sci. 第 2948 卷, 第 12–24 页. Springer, Berlin, 2004.[17] H. Stichtenoth. 代数函数域与码, Graduate Texts in Mathematics 第 254 卷. Springer-Verlag, Berlin, 第二版, 2009.[18] K.-O. St¨ohr 和 J. F. Voloch. 有限域上的魏尔斯特拉斯点与曲线. Proc. London Math. Soc. (3), 52(1):1–19, 1986.[19] W. Ten´orio 和 G. Tizziotti. 多个点处的魏尔斯特拉斯间隙. Bull. Braz. Math. Soc. (N.S.), 50(2):543–559, 2019.[20] S. Yang 和 C. Hu. 库默尔扩张所产生的魏尔斯特拉斯半群. Finite Fields Appl., 45:264– 284, 2017.[21] S. Yang 和 C. Hu. 厄米特曲线商曲线所产生的纯魏尔斯特拉斯间隙. Finite Fields Appl., 50:251–271, 2018.

Faculdade de Matemática, Universidade Federal de Uberlândia, Campus Santa Mônica, CEP 38400-902, Uberlândia, Brazil电子邮箱：alonso.castellanos@ufu.br
Instituto de Matemática, Universidade Federal do Rio de Janeiro, Cidade Universitária, CEP 21941-909, Rio de Janeiro, Brazil电子邮箱：erik@im.ufrj.br
Faculdade de Matemática, Universidade Federal de Uberlândia, Campus Santa Mônica, CEP 38400-902, Uberlândia, Brazil电子邮箱：guilhermect@ufu.br