arXiv:2301.05313v2 [cs.IT] 3 Nov 2023

加权射影平面上码的代数不变量

亚˘格穆尔·C、阿基罗·˘格鲁和梅苏特·S、阿欣

Abstract. 加权射影空间是射影空间的自然推广，具有丰富的结构。射影 Reed-Muller 码是一类纠错码，在通过数字通信信道可靠传输信息方面发挥了重要作用。在本案例研究中，我们探讨运用交换代数和同调代数技术，研究形如 $\mathbb{P}(1, 1, b)$ 的加权射影空间上的加权射影 Reed-Muller（WPRM）码。我们计算最小自由分解，从而得到 $\mathbb{F}_q$-有理点的消失理想的希尔伯特级数，并计算这些码的主要参数。

1. 引言

令 q 为素数幂，并令 $\mathbb{F}_q$ 表示含有 q 个元素的有限域。记 $\mathbb{K}$ 为 $\mathbb{F}_q$. 的代数闭包。设 $w_1, \ldots, w_r$ 为最大公因数为 1 的正整数。与权重 $w_1, \ldots, w_r$ 相关联的加权射影空间是商空间

$$\mathbb{P}(w_1, \ldots, w_r) = (\mathbb{K}^r \setminus \{0\})/\mathbb{K}^*$$

关于等价关系

$$(x_1, \ldots, x_r) \sim (\lambda^{w_1} x_1, \ldots, \lambda^{w_r} x_r) \text{ for } \lambda \in \mathbb{K}^*.$$

因此，空间 $X = \mathbb{P}(w_1, \ldots, w_r)$ 中的点是点 $(x_1, \ldots, x_r) \in \mathbb{K}^r \setminus \{0\}$. 的等价类 $[x_1 : \cdots : x_r]$。已知 $\mathbb{F}_q$-有理点 $X(\mathbb{F}_q)$ 中的元素 $[x_1 : \cdots : x_r]$ 有坐标为 $x_1, \ldots, x_r \in \mathbb{F}_q$ 的代表元，见 [2, 4]。

我们使用多项式环 $S = \mathbb{F}_q[x_1, \ldots, x_r]$，其分次由对所有 $i = 1, \ldots, r$ 都有 deg $x_i = w_i$ 给出。因此，我们有如下分解

$$S = \bigoplus_{d \in \mathbb{N}W} S_d$$

其中 S_d 是一个向量空间，其基由次数为 $d = m_1 w_1 + \cdots + m_r w_r$ 的单项式 $x_1^{m_1} \cdots x_r^{m_r}$ 组成，而 $\mathbb{N}W := \langle w_1, \ldots, w_r \rangle$ 是由权重生成的 $\mathbb{N}$ 的子半群。

任取 $Y = \{P_1, \ldots, P_N\} \subseteq X(\mathbb{F}_q)$ 的 $\mathbb{F}_q$-有理点的一个子集，并定义如下求值映射

2020 *Mathematics Subject Classification.* 主要分类号：14M25；14G05；次要分类号：94B27；11T71。*Key words and phrases.* 代数不变量、加权射影空间、纠错码、托里克码。作者获得 T ¨UB˙ITAK 项目资助，项目编号：119F177。

$$ev_Y : \begin{cases} S_d \to \mathbb{F}_q^N \\ f \mapsto (f(P_1), \ldots, f(P_N)) \end{cases} \tag{1.1}$$

像 $C_{d,Y}$ 是 $\mathbb{F}_q^N$ 的一个子空间，称为求值码。它是通过在 Y 的点处对次数为 d 的齐次多项式求值而得到的。线性码有三个主要参数 $[N, K, \delta]$。长度 N 在此处定义为子集的基数 $|Y|$。$C_{d,Y}$ 的维数（衡量效率的指标）记作 $K = \dim_{\mathbb{F}_q} C_{d,Y}$，即其作为 $\mathbb{F}_q^N$ 的子空间的维数。任意 $c \in C_{d,Y}$ 中非零项的个数称为其汉明重量，而 $C_{d,Y}$ 的最小距离 δ（衡量可靠性的指标）是所有码字 $c \in C_{d,Y} \setminus \{0\}$ 中最小的重量。研究这类码有一种代数方法，它依赖于 Y 的消失理想 $I(Y)$；该理想是由在 Y 的每个点处都取零的 S 中的齐次多项式生成的分次理想。由于式 (1.1) 中定义的求值映射的核等于次数为 d 的齐次部分 $I_d(Y)$，因此有同构 $S_d/I_d(Y) \cong C_{d,Y}$。由此，$C_{d,Y}$ 的维数就是定义 2.2 中定义的加权希尔伯特函数

$$\dim_{\mathbb{F}_q} C_{d,Y} = H_Y(d). \tag{1.2}$$

其长度 N 为 $C_{d,Y}$，给定为

$$N = q^{r-1} + q^{r-2} + \cdots + q + 1$$

当 $Y = X(\mathbb{F}_q)$ 时，参见 [2, 第 2.1] 节。

Lachaud 在论文 [11] 中引入了定义在有限域上的射影 Reed-Muller 码，它是经典广义 Reed-Muller 码的扩展。这些码通过在给定射影空间的所有 $\mathbb{F}_q$-有理点处对齐次多项式求值而得到。Lachaud [12] 给出了这些码的参数。Reed–Muller 码是纠错码，在通过数字通信信道可靠传输信息方面发挥了重要作用。射影 Reed-Muller 码是经过充分研究的码（参见 [16, 17, 12, 11, 1, 3]），并用于实际应用。

加权射影空间是经典射影空间的自然推广，具有丰富的结构，并展现出有趣的代数几何性质。在相关文献中，加权射影空间被视为构造有限域上线性码有趣类别的便利环境，而如上所定义的加权射影 Reed-Muller 码 $C_{d,Y}$ 首次在 [2] 中得到研究。文献[2]给出了加权射影平面 $\mathbb{P}(1, a, b)$ 上次数为 $d = k \cdot \mathrm{lcm}(a, b) \leq q$（其中 k 为某个正整数）的码的参数。尽管 Sørensen 在[17], 中引入了同名的码，但它们实际上并不相同，另见 [8]。Dias 和 Neves 研究了相关的码 [7]，他们关注 Y 为射影加权环面的 $\mathbb{F}_q$-有理点集的情形。他们证明，消失理想是一个特殊的二项式理想；后来，第二作者将这一结果推广到更一般的环面簇的 $\mathbb{F}_q$-有理点集的消失理想，见 [18]。Nardi 在论文 [15] 中提出，通过在全部 $\mathbb{F}_q$- 有理点集上进行求值，可以将环面码的长度扩展，这与将 Reed-Muller 码扩展为射影码是相对应的。当求值集为全部 $\mathbb{F}_q$-有理点集时，Hirzebruch 曲面上的码的参数由 Nardi 在此前的论文 [14] 中计算得到。

本文的主要目标是考察加权射影平面 $X = \mathbb{P}(1, a, b)$ 的 $\mathbb{F}_q$-有理点集的消失理想的代数不变量，以及它们与相应码的参数之间的关系；该码的次数不必像 [2] 中那样满足条件 $d = k \cdot \mathrm{lcm}(a, b) \leq q$。我们关注的代数不变量包括最小自由分解、贝蒂数、希尔伯特级数和正则性。我们特别关注 $\mathbb{P}(1, 1, b)$ 的情形，以获得更为明确的信息。这将得到希尔伯特函数（它给出码的维数）以及正则性集，而后者对于排除平凡码至关重要。

本文结构如下。我们在第 2 节给出代数不变量的定义。第 3 节介绍集合 $\mathbb{F}_q$-有理点 $Y = \mathbb{P}(1, 1, b)(\mathbb{F}_q)$ 的消失理想的代数不变量的主要结果。特别地，我们由此得到 $\mathbb{P}(1, 1, b)(\mathbb{F}_q)$ 的正则性集。我们还计算了对于任意次数 d，Y 上这些码的维数。在第 4 节，我们计算这些码的最小距离，并给出它们在$b = 2$、5、7 和 $q = 2$、5 时的主要参数表。

2. Preliminaries

本节给出陈述主要结果所需的一些定义。设 $X = \mathbb{P}(w_1, \ldots, w_r)$ 为一个加权射影空间，$Y = X(\mathbb{F}_q)$ 为 $\mathbb{F}_q$-有理点的集合。Y 的第一个代数不变量与对应于零码字的齐次多项式有着关键联系，它是以下理想。

定义 2.1。消失理想 $I(Y)$ 是环 $S = \mathbb{F}_q[x_1, \ldots, x_r]$ 的（齐次）理想，由在 Y 上消失的齐次多项式生成，因此

$$I(Y) = \bigoplus_{d \in \mathbb{N}W} I_d(Y),$$

其中，$I_d(Y)$ 是次数为 d 的齐次部分，而 $\mathbb{N}W$ 是由权重生成的 $\mathbb{N}$ 的子半群。

下面给出与 Y 的码参数相关的第二个代数不变量。

定义 2.2。设 S_d 是由次数为 $d = m_1 w_1 + \cdots + m_r w_r$ 的单项式 $x_1^{m_1} \cdots x_r^{m_r}$ 张成的向量空间，$I_d(Y)$ 是由次数为 d 且在 Y 上消失的齐次多项式构成的向量空间。Y 的（加权）希尔伯特函数定义如下：

$$H_Y(d) = \dim_{\mathbb{F}_q} S_d - \dim_{\mathbb{F}_q} I_d(Y).$$

此外，Y 的（加权）希尔伯特级数定义为

$$HS_Y(d) = \sum_{d \in \mathbb{N}W} H_Y(d) t^d.$$

用于消除平凡码的 Y 的最后一个代数不变量是以下集合。

定义 2.3。Y 的正则性集定义如下

$$\mathrm{reg}(Y) = \{d \in \mathbb{N}W : H_Y(d) = |Y|\}.$$

我们使用以下重要判据来证明消失理想的最小自由分解的正合性。

引理 2.4。 [6, 推论 2] 设

$$0 \to F_n \xrightarrow{\phi_n} F_{n-1} \xrightarrow{\phi_{n-1}} \cdots \xrightarrow{\phi_2} F_1 \xrightarrow{\phi_1} F_0$$

是诺特环 S 上的自由模复形。令 rank(ϕ_i) 为描述 ϕ_i 的矩阵中最大非零子式的阶数，并令 $I(\phi_i)$ 为由最高秩子式生成的理想。那么，该复形正合，当且仅当对所有 $1 \leq i \leq n$

(1) rank(ϕ_{i+1}) + rank(ϕ_i) = rank(F_i) (2) $I($
ϕ_i) 包含一个长度为 i 的 S-序列。

当正合复形中 ϕ_1 的余核 M

$$0 \to F_n \xrightarrow{\phi_n} F_{n-1} \xrightarrow{\phi_{n-1}} \cdots \xrightarrow{\phi_2} F_1 \xrightarrow{\phi_1} F_0$$

是一个分次模时，自由模具有如下形式

$$F_i = \bigoplus_{j=1}^{\operatorname{rank} F_i} S(-d_{ij}).$$

满足 $d_{ij} = d \in \mathbb{N}W$ 的指标 j 的个数称为 M 的分次 i-贝蒂数，记作 $\beta_{i,\ d}$(M)。除有限多个元素外， $d \in \mathbb{N}W$ 均对应于平凡的分次贝蒂数 $\beta_{i,\ d}(M) = 0$。

我们利用以下结果，根据 $I(Y)$ 的最小自由分解，将 Y 的希尔伯特级数表示为有理函数。

定理 2.5. [13, 定理 8.20，命题 8.23] 多项式环 $S = \mathbb{F}_q[x_1, \ldots, x_r]$ 上有限生成分次模 M 的希尔伯特级数是一个有理函数，其中该环由 $\mathbb{N}W$ 正分次，具体为:

$$HS_M(t) = \frac{\mathcal{K}_M(t)}{\prod_{i=1}^{r}(1 - t^{w_i})},$$

$_n$其中多项式 $\mathcal{K}_M(t) = \sum \quad \sum (-1)^i \beta_{i,d}(M) t^d$.
$i=0\ d\in\mathbb{N}W$

3. Algebraic Invariants relevant to Weighted Projective Reed-Muller codes

本节中，我们计算消失理想的代数不变量。具体而言，我们求出该理想的最小自由分解及其希尔伯特级数，并利用它们得到希尔伯特函数的取值。由此可得 $Y = \mathbb{P}(1, 1, b)(\mathbb{F}_q)$ 的正则性集；它在消除平凡（全）码方面起着关键作用。本节最后给出这些码的维数。

定理 3.1. [19, 推论 5.8] 设 a, b 为正整数，且 gcd(a, b) =1，并且 $X = \mathbb{P}(1, a, b)$ 是有限域上的加权射影平面。那么， $X(\mathbb{F}_q)$ 的消失理想 $I(X(\mathbb{F}_q))$ 的极小生成元为

$$f_1 = x_2^{(q-1)b+1} x_3 - x_2 x_3^{(q-1)a+1}, f_2 = x_1^{(q-1)b+1} x_3 - x_1 x_3^q \text{ and } f_3 = x_1^{(q-1)a+1} x_2 - x_1 x_2^q.$$

推论 3.2. 设 a 为正整数，且 $X = \mathbb{P}(1, 1, b)$ 是有限域上的加权射影空间。那么，集合 $X(\mathbb{F}_q)$ 的理想为 $I(X(\mathbb{F}_q)) = \langle f_1, f_2, f_3\rangle$，其中

$$f_1 = x_2^{(q-1)b+1}x_3 - x_2x_3^q, f_2 = x_1^{(q-1)b+1}x_3 - x_1x_3^q \text{ and } f_3 = x_1^qx_2 - x_1x_2^q.$$

定理 3.3. 记加权射影平面 $X = \mathbb{P}(1, a, b)$ 上由定理 3.1 给出的理想 $I(X(\mathbb{F}_q))$ 为 I。那么，以下复形是 S/I 的分次极小自由分解

$$0 \to \bigoplus_{j=1}^{2} S(-\sigma_j) \xrightarrow{\begin{bmatrix} x_1 & 0 \\ A_1 & f_3/x_1 \\ A_2 & -f_2/x_1 \end{bmatrix}} \bigoplus_{j=1}^{3} S(-\lambda_j) \xrightarrow{\begin{bmatrix} f_1 & f_2 & f_3 \end{bmatrix}} S \to S/I \to 0$$

其中 $\lambda_1 = (q-1)ab + a + b, \quad \lambda_2 = qb + 1, \quad \lambda_3 = qa + 1,$

$$A_1 = -\sum_{i=1}^{a} x_1^{(i-1)(q-1)b}x_2x_3^{(q-1)a-iq+i}, \quad A_2 = \sum_{i=1}^{b} x_1^{(i-1)(q-1)a}x_2^{(q-1)b-iq+i}x_3,$$
$$\sigma_1 = (q-1)ab + a + b + 1, \qquad \sigma_2 = qb + qa + 1.$$

推论 3.4. 设 I 为加权射影空间 $X = \mathbb{P}(1, 1, b)$ 上由推论 3.2 给出的 $X(\mathbb{F}_q)$ 的理想。那么，以下复形是 S/I的分次极小自由分解

$$0 \to \bigoplus_{j=1}^{2} S(-\sigma_j) \xrightarrow{\begin{bmatrix} x_1 & 0 \\ -x_2x_3^{q-1} & f_3/x_1 \\ A & -f_2/x_1 \end{bmatrix}} \bigoplus_{j=1}^{3} S(-\lambda_j) \xrightarrow{\begin{bmatrix} f_1 & f_2 & f_3 \end{bmatrix}} S \to S/I \to 0$$

其中

$$A = \sum_{i=1}^{b} x_1^{(i-1)(q-1)}x_2^{(q-1)b-iq+i}x_3, \qquad \sigma_1 = qb + 2, \qquad \sigma_2 = qb + q + 1,$$
$$\lambda_1 = qb + 1, \qquad \lambda_2 = qb + 1, \quad 0 \quad \lambda_3 = q + 1.$$

定理 3.3 的证明 设 $\phi_1 := \begin{bmatrix} f_1 & f_2 & f_3 \end{bmatrix}$ 和 $\phi_2 := \begin{bmatrix} x_1 & 0 \\ A_1 & f_3/x_1 \\ A_2 & -f_2/x_1 \end{bmatrix}$，其中

$f_1 = x_2^{(q-1)b+1}x_3 - x_2x_3^{(q-1)a+1}$, $f_2 = x_1^{(q-1)b+1}x_3 - x_1x_3^q$, $f_3 = x_1^{(q-1)a+1}x_2 - x_1x_2^q$ 和

$$A_1 = -\sum_{i=1}^{a} x_1^{(i-1)(q-1)b}x_2x_3^{(q-1)a-iq+i}, \quad A_2 = \sum_{i=1}^{b} x_1^{(i-1)(q-1)a}x_2^{(q-1)b-iq+i}x_3.$$

我们将使用引理 2.4 来证明以下分次模复形的正合性。

$$0 \to F_2 \xrightarrow{\phi_2} F_1 \xrightarrow{\phi_1} S \to S/I \to 0, \tag{3.1}$$

其中 $F_2 = S(-\sigma_1) \oplus S(-\sigma_2)$, $F_1 = S(-\lambda_1) \oplus S(-\lambda_2) \oplus S(-\lambda_3)$。容易看出，秩$(\phi_2) = 2$，秩$(\phi_1) = 1$ 且秩$(S^3) = 3$。因此我们得到

$$\operatorname{rank}(S^3) = \operatorname{rank}(\phi_2) + \operatorname{rank}(\phi_1).$$

现在我们需要验证引理 2.4 中的第二项。 $I(\phi_1)$ 显然是 $I = \langle f_1, f_2, f_3\rangle$，其中包含一个在 S 上不是零因子的多项式。 ϕ_2 的子式为

$$\begin{vmatrix} A_1 & f_3/x_1 \\ A_2 & -f_2/x_1 \end{vmatrix} = -f_1 \neq 0, \begin{vmatrix} x_1 & 0 \\ A_2 & -f_2/x_1 \end{vmatrix} = -f_2 \neq 0 \text{ and } \begin{vmatrix} x_1 & 0 \\ A_1 & f_3/x_1 \end{vmatrix} = f_3 \neq 0.$$

因此， $I(\phi_2)$ 仍然是理想 $I = \langle f_1, f_2, f_3\rangle$ ，它包含正则序列$\{f_1 + f_2, f_2 + f_3\}$。这是因为，如果 $f_2 + f_3$ 是 $S/\langle f_1 + f_2\rangle$中的零因子，那么就存在 $g \in S \setminus \langle f_1 + f_2\rangle$ 使得 $(f_2 + f_3)g \in \langle f_1 + f_2\rangle$，也就是说，存在 $h \in S$使得 $h(f_1 + f_2) = g(f_2 + f_3)$，这显然是不可能的。因为如果存在满足此条件的 $h \in S$ ，那么这两个多项式 $f_1 + f_2$和 $f_2 + f_3$ 就会有一个公因子。但这两个多项式没有公因子。因此，根据引理 2.4，定理 3.3 中给出的自由分解是一个正合序列。

现在我们来证明这个分解是分次的，也就是说，映射 ϕ_1 和 ϕ_2 保持次数。若对所有 $d \in \mathbb{N}W$，都有 $\phi(M_d) \subseteq N_d$，则称 $\phi\colon M = \bigoplus M_d \to N = \bigoplus N_d$ 是分次的（或保次数的）（参见 [13, 定义 8.12，第 153] 页）。因此，我们需要证明 $\phi_1((F_1)_d) \subseteq (F_0)_d$。回忆

$$\phi_1 : \quad F_1 = \bigoplus_{j=1}^{3} S(-\lambda_j) \xrightarrow{\begin{bmatrix} f_1 & f_2 & f_3 \end{bmatrix}} F_0 = S$$
$$(m_1, m_2, m_3) \to m_1 f_1 + m_2 f_2 + m_3 f_3.$$

若 $(m_1, m_2, m_3) \in (F_1)_d = S_{d-\lambda_1} \oplus S_{d-\lambda_2} \oplus S_{d-\lambda_3}$ 对所有 $d \in \mathbb{N}W$ 都成立，则有

$$\deg(m_j f_j) = (d - \lambda_j) + \deg(f_j) = d, \text{ since } \lambda_j = \deg(f_j) \text{ for all } j = 1, 2, 3.$$

因此， ϕ_1 是分次的。现在考虑下面这个映射。

$$\phi_2 : \qquad F_2 = \bigoplus_{j=1}^{2} S(-\sigma_j) \xrightarrow{\begin{bmatrix} x_1 & 0 \\ A_1 & f_3/x_1 \\ A_2 & -f_2/x_1 \end{bmatrix}} F_1 = \bigoplus_{j=1}^{3} S(-\lambda_j)$$
$$(m_1, m_2) \to (x_1 m_1 + 0 m_2, A_1 m_1 + m_2 f_3/x_1, A_2 m_1 - m_2 f_2/x_1)$$

为了证明 $\phi_2((F_2)_d) \subseteq (F_1)_d$，我们取 $(m_1, m_2) \in (F_2)_d = S_{d-\sigma_1} \oplus S_{d-\sigma_2}$。根据映射 ϕ_2 的定义，有

$$\deg(x_1 m_1) = \deg(x_1) + \deg(m_1) = 1 + d - ((q-1)ab + q + b + 1) = d - \lambda_1.$$

此外，

$$\deg(A_1 m_1) = \deg(m_2 f_3/x_1) = qa + d - (qb + qa + 1) = d - (qb + 1) = d - \lambda_2.$$

同样地，我们有

$$\deg(A_2 m_2) = \deg(-m_2 f_2/x_1) = qb + d - (qa + qb + 1) = d - (qa + 1) = d - \lambda_3.$$

因此，我们得到，

$$\phi_2((F_2)_d) = \phi_2(S_{d-\sigma_1} \oplus S_{d-\sigma_2}) \subseteq S_{d-\lambda_1} \oplus S_{d-\lambda_2} \oplus S_{d-\lambda_3} = (F_1)_d$$

这证明了 ϕ_2 是分次的，从而完成证明。 □

命题 3.5。 $Y = \mathbb{P}(1, a, b)(\mathbb{F}_q)$的希尔伯特级数公式如下。

$$HS_Y(t) = \frac{1 - t^{qa+1} - t^{qb+1} - t^{(q-1)ab+a+b} + t^{qa+qb+1} + t^{(q-1)ab+a+b+1}}{(1-t)(1-t^a)(1-t^b)}.$$

由命题 3.5 可直接得到以下结果。

推论 3.6。 $Y = \mathbb{P}(1, 1, b)(\mathbb{F}_q)$ 的希尔伯特级数公式如下。

$$HS_Y(t) = \frac{1 - t^{q+1} - 2t^{qb+1} + t^{qb+2} + t^{qb+q+1}}{(1-t)(1-t)(1-t^b)}. \tag{3.2}$$

命题 3.5 的证明 由定理 2.5 和定理 3.3 中给出的分次自由分解可得

$$\mathcal{K}_M(t) = \sum_{d \in \mathbb{N}W} (-1)^0 \beta_{0,d}(M) t^d + \sum_{d \in \mathbb{N}W} (-1)^1 \beta_{1,d}(M) t^d + \sum_{d \in \mathbb{N}W} (-1)^2 \beta_{2,d}(M) t^d,$$

其中，$\beta_{0,\ 0}(F_0) = 1, \beta_{1,\ \lambda_1}(F_1) = 1, \beta_{1,\ \lambda_2}(F_1) = 1, \beta_{1,\ \lambda_3}(F_1) = 1$ 以及 $\beta_{2,\ \sigma_1}(F_2) = 1, \beta_{2,\ \sigma_2}(F_2) = 1$. 因此，我们得到

$$\mathcal{K}_M(t) = 1 - t^{qa+1} - t^{qb+1} - t^{(q-1)ab+a+b} + t^{qa+qb+1} + t^{(q-1)ab+a+b+1}.$$

因此，由定理 2.5 可得以下有理函数，

$$HS_M(t) = \frac{1 - t^{qa+1} - t^{qb+1} - t^{(q-1)ab+a+b} + t^{qa+qb+1} + t^{(q-1)ab+a+b+1}}{(1-t)(1-t^a)(1-t^b)}. \tag{3.3}$$

从而完成证明。 □

考虑推论 3.6 中给出的 $\mathbb{P}(1, 1, b)(\mathbb{F}_q)$ 的希尔伯特级数公式。将和式 $1 - t^{q+1} - 2t^{qb+1} + t^{qb+2} + t^{qb+q+1}$ 乘以 $1/(1-t)$ 两次，我们得到以下多项式 $p(t)$，

$$1+2t+\cdots+qt^{q-1}+(q+1)t^q+\cdots+(q+1)t^{qb}+(q-1)t^{qb+1}+\cdots+2t^{qb+q-2}+t^{qb+q-1}.$$

将这个和式乘以 $1/(1-t^b)$，我们得到以下希尔伯特级数 $HS_M(t)$。

$$\sum_{i=0}^{\infty} t^{ib} p(t) = \sum_{i=0}^{\infty} t^{ib} \left(\sum_{j=0}^{q} (j+1)t^j + \sum_{k=q+1}^{qb} (q+1)t^k + \sum_{s=1}^{q-1} (q-s)t^{qb+s} \right). \tag{3.4}$$

由于希尔伯特级数的形式为

$$\sum_{d \in \mathbb{N}W} H_Y(d) t^d = \sum_{i=0}^{\infty} t^{ib} p(t), \tag{3.5}$$

$H_Y(d)$ 的值是多项式 $p(t)$ 中 t^{d-ib} 的系数。因此，我们将这个系数记为 $C_i(d)$，并仔细实现这一想法，得到以下结果。注意， $p(t)$ 中 t^j 的系数为

$$\begin{cases} j+1, & \text{if } 0 \le j \le q-1 \\ q+1, & \text{if } q \le j \le qb \\ qb+q-j, & \text{if } qb+1 \le j \le qb+q-1. \end{cases} \tag{3.6}$$

定理 3.7. 设 $d = d_0 b + r_0$，其中 $0 \le r_0 < b$。若 $q \le b$，则 $Y = \mathbb{P}(1,1,b)(\mathbb{F}_q)$ 的希尔伯特函数如下

$$H_Y(d) = \begin{cases} d_0(q+1) + r_0 + 1, & \text{if } 0 \le d_0 \le q-1 \text{ and } 0 \le r_0 \le q-1 \\ (d_0+1)(q+1), & \text{if } 0 \le d_0 \le q-1 \text{ and } q \le r_0 < b \\ q(q+1), & \text{if } d_0 \ge q \text{ and } 0 < r_0 < b \\ q(q+1)+1, & \text{if } d_0 \ge q \text{ and } r_0 = 0. \end{cases} \tag{3.7}$$

证明。回顾一下，$H_Y(d)$是式（3.4）所给无穷和中 t^d 的系数。因此，我们着重考察多项式中 t^{d-ib} 的系数 $C_i(d)$

$$p(t) = \sum_{j=0}^{q}(j+1)t^j + \sum_{k=q+1}^{qb}(q+1)t^k + \sum_{s=1}^{q-1}(q-s)t^{qb+s} = \sum_{i=0}^{d_0} C_i(d)t^{d-ib}$$

d_0对于 $0 \le i \le d_0$. 因此，$H_Y(d) = \sum C_i(d)$。回顾一下，$d - ib = (d_0 - i)b + r_0$.$i=0$

情形 I：设 $0 \le d_0 \le q-1$.
对于 $i = d_0$，我们有 $d - ib = r_0$，并得到 $p(t)$中 t^{r_0} 的系数为

$$C_i(d) = \begin{cases} r_0 + 1, & \text{if } 0 \le r_0 \le q-1 \\ q+1, & \text{if } q \le r_0 < b. \end{cases} \tag{3.8}$$

每当 $0 \le i \le d_0 - 1$时，我们有 $q \le b \le (d_0 - i)b + r_0 \le (d_0 + 1)b \le qb$。因此，$d - ib = (d_0 - i)b + r_0$ 介于 q 和 qb之间，从而根据式（3.6），对所有$0 \le i \le d_0 - 1$，$C_i(d) = q + 1$。因此，

$$H_Y(d) = \sum_{i=0}^{d_0} C_i(d) = d_0(q+1) + \begin{cases} r_0 + 1, & \text{if } 0 \le r_0 \le q-1 \\ q+1, & \text{if } q \le r_0 < b. \end{cases} \tag{3.9}$$

情形 II：令 $d_0 = q$。因此，$d = qb + r_0$ 和 $d - ib = (q - i)b + r_0$。首先，考虑 $i = 0$ 的情形。于是我们得到以下公式。

$$C_i(d) = \begin{cases} q+1 & \text{if } r_0 = 0, \\ q - r_0 & \text{if } 0 < r_0 \le q-1, \\ 0 & \text{if } q \le r_0 < b. \end{cases} \tag{3.10}$$

现在考虑 $1 \le i \le q-1$ 的情形。于是，

$$q \le b \le (q-i)b \le (q-1)b \Rightarrow q \le (q-i)b + r_0 \le (q-1)b + r_0 < qb \Rightarrow C_i(d) = q+1.$$

对于情形 $i = q$，我们得到以下公式。

$$C_i(d) = \begin{cases} 1 & \text{if } r_0 = 0, \\ r_0 + 1 & \text{if } 0 < r_0 \le q-1, \\ q+1 & \text{if } q \le r_0 < b. \end{cases} \tag{3.11}$$

因此，将这些结果相加，我们得到

$$H_Y(d) = \begin{cases} q(q+1)+1 & \text{if } r_0 = 0, \\ q(q+1) & \text{if } 0 < r_0 \le q-1, \\ q(q+1) & \text{if } q \le r_0 < b. \end{cases} \tag{3.12}$$

情形 III：令 $d_0 > q$。因此， $d_0 - q > 0$。
对于情形 $0 \le i < d_0 - q$，我们有 $C_i(d) = 0$，因为

$$q + 1 \le d_0 - i \Rightarrow (q+1)b \le (d_0 - i)b \Rightarrow qb + (q-1) < qb + b \le (d_0 - i)b \le d - ib.$$

对于 $d_0 - q \le i < d_0$ 的情形，我们有

$$0 < d_0 - i \le q \Rightarrow q \le b \le (d_0 - i)b \le qb.$$

因此， $d - ib = (d_0 - i)b + r_0$ 所在的区间取决于 r_0。
若 $r_0 = 0$，则对所有 $d_0 - q \le i \le d_0 - 1$，我们得到 $C_i(d) = q + 1$ 为 $d - ib = (d_0 - i)b$。若 $r_0 > 0$ 且 $i = d_0 - q$，则得到 $d - ib = qb + r_0$，因此

$$C_i(d) = \begin{cases} q - r_0 & \text{if } 1 \le r_0 \le q-1, \\ 0 & \text{if } q \le r_0 < b. \end{cases} \tag{3.13}$$

若 $r_0 > 0$ 且 $i > d_0 - q$，则得到 $d_0 - i < q \Rightarrow d_0 - i \le q - 1$，因此

$$d - ib = (d_0 - i)b + r_0 \le (q-1)b + r_0 = qb - b + r_0 < qb.$$

因此，对所有 $d_0 - (q-1) \le i \le d_0 - 1$，我们有 $C_i(d) = q + 1$。
最后，对于 $i = d_0$ 的情形，我们有 $d - ib = r_0$，因此

$$C_i(d) = \begin{cases} r_0 + 1 & \text{if } 0 \le r_0 \le q-1, \\ q + 1 & \text{if } q \le r_0 < b. \end{cases} \tag{3.14}$$

综上，对所有 $d_0 - (q-1) \le i \le d_0 - 1$，我们有 $C_i(d) = q + 1$，并且

$$C_{d_0-q}(d) + C_{d_0}(d) = \begin{cases} (q+1) + 1 & \text{if } r_0 = 0, \\ q + 1 & \text{if } 0 < r_0 < b. \end{cases} \tag{3.15}$$

因此，我们得到

$$H_Y(d) = \begin{cases} q(q+1) + 1 & \text{if } r_0 = 0, \\ q(q+1) & \text{if } 0 < r_0 < b, \end{cases} \tag{3.16}$$

证明完成。 □

定理 3.8. 设 $d = d_0 b + r_0$ 满足 $0 \le r_0 < b$。当 $d > q$ 时，我们还设 $d = q + kb + r$ 满足 $0 \le r < b$。若 $q > b$，则 $Y = \mathbb{P}(1, 1, b)(\mathbb{F}_q)$ 的希尔伯特函数如下

$$H_Y(d) = \begin{cases} d + 1 & \text{if } 0 \le d \le b-1, \\ (d_0 + 1)(d + 1 - bd_0/2) & \text{if } b \le d \le q, \\ (d_0 - k)(d - (d_0 + k + 1)b/2) + q(k+1) + 1 & \text{if } q + 1 \le d \le qb \\ (k+q)(k - q + 1)b/2 + q(k + d + 1) - dk - bd_0 + \kappa & \text{if } d > qb \text{ and } k < q, \\ q^2 + r_0 + \kappa & \text{if } d > qb \text{ and } k \ge q, \end{cases}$$

其中

$$\kappa = \begin{cases} q - r_0, & \text{if } 0 < r_0 < q, \\ q + 1 & \text{if } r_0 = 0. \end{cases}$$

证明。令 $d = d_0 b + r_0$ 对于 $0 \le r_0 < b < q$. 回忆一下，(3.5) 中的希尔伯特级数为

$$\sum_{i=0}^{\infty} t^{ib} \left(\sum_{j=0}^{q} (j+1)t^j + \sum_{k=q+1}^{qb} (q+1)t^k + \sum_{s=1}^{q-1} (q-s)t^{qb+s} \right) = \sum_{i=0}^{\infty} t^{ib} p(t) \tag{3.17}$$

并且 $C_i(d)$ 是前一个证明中多项式 $p(t)$ 中 t^{d-ib} 的系数，其中 $0 \le i \le d_0$。将 $j = d - ib$ 代入 (3.6)，得到

$$C_i(d) = \begin{cases} d - ib + 1 & \text{if } 0 \le d - ib \le q, \\ q + 1 & \text{if } q + 1 \le d - ib \le qb, \\ q + (qb - d + ib) & \text{if } qb + 1 \le d - ib \le qb + q - 1. \end{cases} \tag{3.18}$$

情形 I：令 $0 \le d \le b-1$. 因此，我们有 $d_0 = 0$。那么 $i = 0$。因此， $H_Y(d) = d+1$.

情形 II：令 $b \le d \le q$. 显然， $d_0 > 0$. 然后 $d - ib \le q$. 因此，$C_i = d - ib + 1$. 因此，

$$H_Y(d) = \sum_{i=0}^{d_0}(d-ib+1) = (d_0+1)(d+1) - b\sum_{i=0}^{d_0} i = (d_0+1)(d+1) - b\left(\frac{d_0(d_0+1)}{2}\right).$$

情形 III：令 $q+1 \le d < qb$ 并且 $d = q + kb + r$ 满足 $0 \le r < b$。由于$d > q$ 我们有 $d - q = kb + r$。首先，令 $k = 0$. 如果 $i = 0$ 我们得到 $C_i = q + 1$. 令$i > 0$。因此， $d - d_0 b < \cdots < d - 2b < d - b < q$. 然后我们得到 $C_i = d - ib + 1$ 对于$_{d_0} i = 1$, 2, ..., d_0. 因此， $H_Y(d) = q + 1 + \sum(d - ib + 1)$。$_{i=1}$

如果 $i = 0$，我们得到 $C_i = q + 1$.。设 $1 \le i \le k$.。显然， $q \le d - b < (q - 1)$ a，因此我们有 $q \le d - kb \le d - ib \le d \le qb$。接着，对于 $1 \le i \le k$.，我们得到 $C_i = q + 1$。设 $k + 1 \le i \le d_0$.。由于 $-i \le -k - 1$，我们有 $d - ib \le d - kb - b$。又由于$d = q + kb + r$ 且 $r < b$，我们得到 $d - ib \le d - kb - b \le q + r - b < q$.。因此，$_{d_0} H_Y(d) = (k + 1)(q + 1) + \sum(d - ib + 1)$。整理等式后，我们得到：$_{i=k+1}$

$$H_Y(d) = (k+1)(q+1) + (d_0 - k)(d+1) - b\left(\frac{d_0(d_0+1)}{2} - \frac{k(k+1)}{2}\right).$$

情形 IV：设 $qb < d$ 且 $k < q$.。由于 $d = d_0 b + r_0$，我们有 $d_0 \ge q$.

设 $0 \le i < d_0 - q$. 如果我们考虑 $i < d_0 - q$，则得到 $d - ib > qb$. 因此，我们得到，

$$C_i = q + qb - d + ib.$$

设 $d_0 - q < i \le d_0 - k$. 如果我们考虑 $d_0 - q < i$，利用情形 V 中的论证，可得 $d - ib < qb$. 此外，如果我们考虑 $i \le d_0 - k$，则有 $d - ib \ge d - d_0 b + kb =$ $r_0 + kb > kb = d - q - r > qb - q - r > qb - 2q = q(b - 2)$。由于 $b \ge 2$，我们有$d - ib > q($ $b - 2) \ge q$. 于是得到，

$$C_i = q + 1.$$

设 $d_0 - k < i \le k$. 如果我们考虑 $d_0 - k < i$，则有 $d - ib \le d - d_0 b + kb - b =$ $r_0 - b + kb < qb + r_0 - b$. 由于 $r_0 < b$，可得 $d - ib < qb$. 并且，如果我们考虑 $i \le k$，则有 $d - ib \ge d - kb = q + r > q$. 因此得到，

$$C_i = q + 1.$$

令 $k + 1 \le i \le d_0$. 根据情形 V 中的论证，我们得到，

$$C_i = d - ib + 1.$$

考虑 $i = d_0 - q$。若 $i = d_0 - q$，我们有 $d - ib = d - d_0 b + qb = r_0 + qb$.。由于 $0 < r_0 < q$，我们有 $qb < d - ib \le qb + q - 1$。因此，我们得到

$$C_i = q - r_0 \text{ for } 0 < r_0 < q.$$

此外，若考虑 $r_0 = 0$，我们得到 $d - ib = d - d_0b + qb = r_0 + qb = qb$。因此，

$$C_i = q + 1 \text{ for } r_0 = 0.$$

因此，我们得到：

$$H_Y(d) = \sum_{i=0}^{d_0-q-1} (q + qb - d + ib) + (q + k - d_0)(q + 1) + \sum_{i=k+1}^{d_0} (d + 1 - ib) + \kappa$$

其中

$$\kappa = \begin{cases} q - r_0, & \text{if } 0 < r_0 < q, \\ q + 1 & \text{if } r_0 = 0. \end{cases}$$

将 $d > qb$ 和 $k < q$ 的所有等式排列起来，我们得到：

$$\begin{aligned} H_Y(d) &= (d_0 - q)(q + qb - d) + \frac{b}{2}\left((d_0 - q - 1)(d_0 - q)\right) + (q + k - d_0)(q + 1) \\ &\quad + (d + 1)(d_0 - k) - \frac{b}{2}\left(d_0(d_0 + 1) - k(k + 1)\right) + \kappa. \\ &= qd - \frac{q^2b}{2} - bd_0 + \frac{bq}{2} + q + kq - dk + \frac{bk^2}{2} + \frac{bk}{2} + \kappa \\ &= \frac{b}{2}\left((k + q)(k - q + 1)\right) + q(d + 1 + k) - bd_0 - kd + \kappa \begin{cases} q - r_0, & \text{if } r_0 < q, \\ q + 1 & \text{if } r_0 = 0. \end{cases} \end{aligned}$$

情形 V：设 $qb < d$ 和 $k \geq q.$。回想 $d = d_0b + r_0$，且我们有 $d_0 \geq q.$

设 $0 \leq i \leq k-q.$。那么，我们得到 $d-ib \geq d-kb+qb = q+r+qb \geq qb+q > qb+q-1$。由于 $d - ib > qb + q - 1$，我们得到

$$C_i = 0.$$

设 $k - q < i < d_0 - q.$。首先，若考虑 $i < d_0 - q$，我们得到 $-i > q - d_0 \Rightarrow d - ib > d + qb - d_0b = r_0 + qb > qb.$。此外，若考虑 $i > k - q$，我们得到 $-i \leq -k + q - 1 \Rightarrow d - ib \leq d - kb + qb - b.$。由于 $d = q + kb + r$ 且 $r < b$，我们得到 $d-ib \leq d-kb+qb-b \leq q+r+qb-b \leq qb+q-1.$。因此，我们得到 $qb < d-ib \leq qb+q-1$，然后得到

$$C_i = q + qb - d + ib.$$

令 $d_0-q < i \leq k.$那么，由于 $d = kb+q+r$，我们有 $d-ia \geq d-kb = q+r \geq q.$。此外，我们有 $i \geq d_0-q+1 \Rightarrow -i \leq q-1-d_0 \Rightarrow d-ib \leq d+qb-b-d_0b = qb+r_0-b.$。由于 $r_0 < b$，可得 $d - ib < qb.$。因此，

$$C_i = q + 1.$$

令 $k + 1 \leq i \leq d_0.$。利用情形 IV 中的论证，可得

$$C_i = d - ib + 1.$$

令 $i = d_0 - q$，与情形 IV 中相同。于是，我们有 $d - ib = d - d_0b + qb = r_0 + qb.$。由于$0 < r_0 < q$，我们有 $qb < d - ib \leq qb + q - 1$。因此，可得

$$C_i = q - r_0 \text{ for } 0 < r_0 < q.$$

此外，如果考虑 $r_0 = 0$，可得 $d - ib = d - d_0b + qb = r_0 + qb = qb$。因此，

$$C_i = q + 1 \text{ for } r_0 = 0.$$

因此，如果我们将关于 $d > qb$ 和 $k \geq q$ 的所有等式排列起来，就能得到所需的结论。□

根据定理 3.7 和定理 3.8，我们将在下面的推论中描述 $\mathbb{F}_q$-有理点 $Y = \mathbb{P}(1, 1, b)(\mathbb{F}_q)$ 的正则性集。

推论 3.9. 设 b 为正整数。 $Y = \mathbb{P}(1, 1, b)(\mathbb{F}_q)$ 的正则性集如下。

$$\mathrm{reg}(Y) = \{d_0 b \in \mathbb{N} : d_0 \geq (q + \lfloor (q-1)/b \rfloor)\} = (q + \lfloor (q-1)/b \rfloor)b + \mathbb{N}b.$$

证明. $d = d_0 b + r_0$，其中 $0 \leq r_0 < b$ 与前文相同。

情形 A：首先，设 $q \leq b$。对于此情形，由于 $\lfloor (q-1)/b \rfloor = 0$，只需证明以下等式。

$$\mathrm{reg}(Y) = \{d \in \mathbb{N} : d = d_0 b \text{ with } d_0 \geq q\} = qb + \mathbb{N}b.$$

情形 A.I：设 $0 \leq d_0 \leq q-1$ 和 $0 \leq r_0 \leq q-1$. 。根据 3.7 中给出的结果，我们得到希尔伯特函数的值为 $H_Y(d) = d_0(q+1) + r_0 + 1$. 因此，

$$H_Y(d) \leq (q-1)(q+1) + q = q^2 - 1 + q < q^2 + q + 1.$$

因此，对于 $0 \leq d_0 \leq q-1$ 和 $0 \leq r_0 \leq q-1$，我们有 $d \notin \mathrm{reg}(Y)$。

情形 A.II：设 $0 \leq d_0$ 和 $q \leq r_0 < b$. 类似地，若考虑 3.7 中给出的结果，可得 $H_Y(d) = (d_0+1)(q+1) \leq q(q+1)$。显然，$H_Y(d) < q^2 + q + 1$. 因此，我们得到 $d \notin \mathrm{reg}(Y)$。

情形 A.III：设 $d_0 \geq q$ 和 $0 < r_0 < b$。根据 3.7 中给出的结果，可得 $H_Y(d) = q(q+1)$。显然，$H_Y(d) < q^2 + q + 1$. 因此，对于 $d_0 \geq q$ 和 $0 < r_0 < b$，我们得到 $d \notin \mathrm{reg}(Y)$。

情形 A.IV：设 $d_0 \geq q$ 和 $r_0 = 0$。根据 3.7 中给出的结果，我们知道，对于 $d_0 \geq q$ 和 $r_0 = 0$，$H_Y(d) = q^2 + q + 1$ 。因此，在这种情形下，$d = d_0 b \in \mathrm{reg}(Y)$。

由于上述情况中只有一种可能，因此我们得到

$$\mathrm{reg}(Y) = \{d \in \mathbb{N} : d = d_0 b \text{ with } d_0 \geq q\} = qb + \mathbb{N}b.$$

情形 B：令 $q > b$。

情形 B.I：令 $0 \leq d \leq b-1$. 我们根据 3.8 中给出的结果得到 $H_Y(d) = d+1$。显然，$H_Y(d) < q^2 + q + 1$. 因此，对于 $0 \leq d \leq b-1$，我们得到 $d \notin \mathrm{reg}(Y)$。

情形 B.II：令 $b \leq d \leq q$。我们有 $d_0 \geq 1$，否则便会得到矛盾$d = d_0 b + r_0 = r_0 < b$。于是得到以下不等式，

$$H_Y(d) = (d_0+1)(d+1) - b\left(\frac{d_0(d_0+1)}{2}\right) < (d_0+1)(d+1) \leq q(q+1).$$

因此我们得到 $H_Y(d) < q^2 + q + 1$. 所以，对于 $b \leq d \leq q$，我们得到 $d \notin \mathrm{reg}(Y)$。

情形 B.III：设 $q+1 \leq d \leq qb$。考虑以下求和式：

$$H_Y(d) = (k+1)(q+1) + (d_0 - k)(d+1) - b\sum_{i=k+1}^{d_0} i.$$

整理该求和式可得,

$$\begin{aligned}
&= kq + q + 1 + d_0 d + d_0 - kd - \frac{bd_0^2}{2} - \frac{bd_0}{2} + \frac{bk^2}{2} + \frac{bk}{2} \\
&= kq + q + 1 + bd_0^2 + d_0 r_0 + d_0 - kd - \frac{bd_0^2}{2} - \frac{bd_0}{2} + \frac{k^2 b}{2} + \frac{kb}{2} \\
&< kq + q + 1 + \frac{bd_0^2}{2} + \frac{bd_0}{2} + d_0 - kd + \frac{k^2 b}{2} + \frac{kb}{2} \\
&= kq + q + 1 + \frac{bd_0^2}{2} + \frac{bd_0}{2} + d_0 - kq - k^2 b - kr + \frac{k^2 b}{2} + \frac{kb}{2} \\
&= q + 1 + \frac{bd_0^2}{2} + \frac{bd_0}{2} + d_0 - \frac{k^2 b}{2} - kr + \frac{kb}{2}.
\end{aligned}$$

由于 $k > 1 \Rightarrow -k < -1$、$d = q + kb + r \leq qb \Rightarrow k \leq q - \frac{q+r}{b}$，我们得到以下不等式。

$$\begin{aligned}
&< q + 1 + \frac{bd_0^2}{2} + \frac{bd_0}{2} + d_0 + \frac{b}{2} - r + \frac{kb}{2} \\
&= q + 1 + d_0 + \frac{b}{2}\left(d_0(d_0+1)\right) + \frac{b}{2}(k+1) - r \\
&\leq q + 1 + d_0 + \frac{bd_0}{2}(d_0+1) + \frac{b}{2}\left(q - \frac{q+r}{b} + 1\right) - r \\
&= q + 1 + d_0 + \frac{bd_0}{2}(d_0+1) + \frac{qb}{2} - \frac{qb}{2b} - \frac{rb}{2b} + \frac{b}{2} - r \\
&= \frac{q}{2} + 1 + d_0 + \frac{bd_0}{2}(d_0+1) + \frac{qb}{2} + \frac{b}{2} - \frac{3r}{2}.
\end{aligned}$$

由于我们知道 $q + 1 \leq d = d_0 b + r_0$，因此有 $q \leq d_0 b + r_0 - 1$. 而且,

$$d_0 \leq q \leq d_0 b + r_0 - 1 \Rightarrow d_0 \leq d_0 b + r_0 - 1 \Rightarrow d_0 \leq \frac{r_0 - 1}{1 - b}.$$

如果我们使用所有这些不等式，就得到,

$$\begin{aligned}
&\leq \frac{bd_0 + r_0}{2} + \frac{1}{2} + \frac{r_0 - 1}{1 - b} + \frac{bd_0}{2}\left(\frac{r_0 - 1 + 1 - b}{1 - b}\right) + \frac{qb}{2} + \frac{b}{2} - \frac{3r}{2} \\
&< \frac{bd_0}{2} + b + \frac{1}{2} + \frac{b - 1}{1 - b} + \frac{qb}{2} - \frac{3r}{2} \\
&= \frac{bd_0}{2} + b - \frac{1}{2} + \frac{qb}{2} - \frac{3r}{2} \\
&\leq qb + b - \frac{(3r+1)}{2} \\
&< q^2 + q < q^2 + q + 1.
\end{aligned}$$

因此我们得到 $H_Y(d) < q^2 + q + 1$. 所以，对于 $q + 1 \leq d \leq qb$，$d \notin \mathbf{reg}(Y)$。情形 B.IV：设 $d > qb$ 和 $k < q$. 考虑以下求和：

$$H_Y(d) = \frac{b}{2}\left((k+q)(k-q+1)\right) + q(k+d+1) - dk - bd_0 + \kappa.$$

上面关于 $H_Y(d)$ 的公式取决于公式 $d = q+kb+r$ 中 k 的值。当 $k = q-1$ 时，我们得到

$$\begin{aligned} H_Y(d) &= \frac{b}{2}\left((q-1+q)(q-1-q+1)\right) + q(q-1+d+1) - qd + d - bd_0 + \kappa \\ &= q^2 + d - bd_0 + \kappa = q^2 + r_0 + \kappa. \end{aligned}$$

- 若 $0 < r_0 < q$，则 $\kappa = q - r_0$ 因此 $H_Y(d) = q^2 + q < q^2 + q + 1$。由此可得，对于 $d > qb$、$k = q-1$ 和 $0 < r_0 < q$.，$d \notin \mathrm{reg}(Y)$
- 设 $r_0 = 0$.。则 $\kappa = q+1$ 因此 $H_Y(d) = q^2 + q + 1$。因此，对于 $d > qb$、$k = q-1$ 和 $r_0 = 0$，$d \in \mathrm{reg}(Y)$。

由于，对于 $k < q-1$，$H_Y(q+kb+r) < H_Y(q+(q-1)b+r)$，因此若 $k < q-1$，则 $d \notin \mathrm{reg}(Y)$。

情形 B.V：设 $d > qb$ 和 $k \geq q$.

- 令 $0 < r_0 < q$. 因此，$\kappa = q - r_0$. 于是，我们有

$$H_Y(d) = q^2 + d - bd_0 + \kappa = q^2 + q < q^2 + q + 1.$$

因此，对于 $d > qb$、$k \geq q$ 和 $0 < r_0 < q$.，我们得到 $d \notin \mathrm{reg}(Y)$

- L令 r_0 =。0 S因此，$\kappa = q$1+。Th于是，我们 have

$$H_Y(d) = q^2 + d - bd_0 + \kappa = q^2 + q + 1.$$

因此，在这种情况下，$d \in \mathrm{reg}(Y)$。

所有这些情形都表明，当且仅当 $d = d_0 b$、$d_0 > q$ 和 $k \geq q-1$ 时，$d \in \mathrm{reg}(Y)$。为了确定 $\mathrm{reg}(Y)$ 中的最小元素，我们取 $k = q-1$，并寻找使 $d = d_0 b \in \mathrm{reg}(Y)$ 成立的 r 的值。由于 $0 \leq r \leq b-1$，我们有

$$q + (q-1)b \leq q + kb + r = d \leq q + qb - b + b - 1 = qb + q - 1.$$

因此，我们得到 $qb + q - b \leq d = d_0 b \leq qb + q - 1$。由于该区间内有 b 个整数，下面区间中的唯一整数

$$q + (q-b)/b \leq d_0 \leq q + (q-1)/b$$

是 $d_0 = q + \lfloor q - 1/b \rfloor$。因此，

$$\begin{aligned} \mathrm{reg}(Y) &= \{d \in \mathbb{N} : d = d_0 b = q + kb + r \text{ with } d_0 \leq q + (q-1)/b, d_0 > q \text{ and } k \geq q-1\} \\ &= (q + \lfloor q - 1/b \rfloor)b + \mathbb{N}b \end{aligned}$$

□

定理 3.10。 [5, 定理 4.3。5] 设 R 是一个正分次的 $\mathbb{K}$-代数，且 $M \neq 0$ 是一个有限（又称有限生成的）分次的 R-模。则，

i. 存在唯一确定的拟多项式 P_M，使得对于所有 $d \gg 0$.，有 $H_M(d) = P_M(d)$；ii. 有 $\deg\left(HS_M(t)\right) = \max\{d : H_M(d) \neq P_M(d)\}$

这里，$\deg(H_M(t))$ 表示有理函数 $HS_M(t)$ 的次数，也称为 M 的 a-不变量，记作 $a(M)$。

注 3.11. 由定理 3.10 可知，对于所有 $d > a(Y)$，Y 的希尔伯特函数都与希尔伯特准多项式 P_Y 一致；也就是说，存在一个正整数 g（周期）以及多项式 P_0, ..., P_{g-1}，使得对于 $d > a(Y)$ 且 $d \equiv i \mod g$.，$H_Y(d) = P_i(d)$。

作为上述结果的直接推论，我们现在给出 Y的希尔伯特准多项式。

推论 3.12. 设 $Y = \mathbb{P}(1,1,b)(\mathbb{F}_q)$。那么 Y的希尔伯特准多项式为

$$P_Y(d_0b + r_0) = \begin{cases} q(q+1)+1 & if\ d_0 \in \mathbb{Z}\ and\ r_0 = 0 \\ q(q+1) & if\ d_0 \in \mathbb{Z}\ and\ 1 \le r_0 \le b-1. \end{cases}$$

证明。我们需要证明，对于所有情况， $H_Y(d) = P_Y(d)$

$$d \ge a(Y) + 1 = (q-1)(b+1) + 1 = (q-1)b + q = qb + q - b.$$

推论 3.9 的证明表明，对于所有 $d \le a(Y)$， $H_Y(d) < q(q+1)$，并且当且仅当 $d = (q-1)b + r_0$，其中 $q \le r_0 < b$ 或 $d = d_0b + r_0$，且 $d_0 \ge q$ 和 $0 < r_0 < b$ 时，$H_Y(d) = q(q+1)$；在情形 A 中，我们有 $q \le b$。最后，若 $d = d_0b$，其中 $d_0 \ge q$，则 $H_Y(d) = q(q+1) + 1$，从而证明了情形 A 的断言。至于情形 B，我们有 $q > b$，可得 $d \ge a(Y) + 1 = qb + q - b > qb$。因此，当 $0 < r_0 < q$ 且 $d > qb$ 时，正如推论 3.9 的证明所示，$H_Y(d) = q^2 + q$。类似地，若 $d_0 > q$，则 $H_Y(d_0b) = q(q+1) + 1$。因此，在这种情况下，我们也得到所需的 $H_Y(d) = P_Y(d)$。□

根据 (1.2) 中给出的码的维数与 Y和 Y 的希尔伯特函数之间的关系，我们得到以下结果。

推论 3.13. 设 $d = d_0b + r_0$，其中 $0 \le r_0 < b$且 $Y = \mathbb{P}(1,1,b)(\mathbb{F}_q)$。若$q \le b$，则码 $C_{d,\ Y}$ 的维数如下。

(3.19)

$$\dim_{\mathbb{F}_q}(C_{d,Y}) = \begin{cases} d_0(q+1) + r_0 + 1 & if\ 0 \le d_0 \le q-1\ and\ 0 \le r_0 \le q-1 \\ (d_0+1)(q+1) & if\ 0 \le d_0 \le q-1\ and\ q \le r_0 < b \\ q(q+1) & if\ d_0 \ge q\ and\ 0 < r_0 < b \\ q(q+1)+1 & if\ d_0 \ge q\ and\ r_0 = 0 \end{cases}$$

推论 3.14. 设 $d = d_0b + r_0$，对于所有情形均有 $0 \le r_0 < b$，且在 $d > q$的情形下有 $d = q + kb + r$和 $0 \le r < b$。若 $q > b$，则

$$\dim_{\mathbb{F}_q}(C_{d,Y}) = \begin{cases} d+1 & \text{若 } 0 \le d \le b-1, \\ (d_0+1)(d+1-bd_0/2) & \text{若 } b \le d \le q, \\ (d_0-k)(d-(d_0+k+1)b/2) + q(k+1) + 1 & \text{若 } q+1 \le d \le qb \\ (k+q)(k-q+1)b/2 + q(k+d+1) - dk - bd_0 + \kappa & \text{若 } d > qb, \quad k < q, \\ q^2 + r_0 + \kappa & \text{若 } d > qb, \quad k \ge q, \end{cases}$$

其中

$$\kappa = \begin{cases} q - r_0, & if\ 0 < r_0 < q, \\ q+1 & if\ r_0 = 0. \end{cases}$$

3.1. 正则性集和维数示例。本节将给出本文主要结果之一： $Y = \mathbb{P}(1,1,b)(\mathbb{F}_q)$的希尔伯特函数值。本节所列的表格中，我们特别强调正则性集的第一个元素；正则性集是希尔伯特函数达到其最大值时对应的次数集合。

例 3.15。设 $q = 5$、 $X = \mathbb{P}(1,1,b)$ 和 $Y = X(\mathbb{F}_q)$。对于 $b = 2$、5、7，我们将在下表中分别给出 Y 的希尔伯特函数值。根据推论 3.13 和推论 3.14，这些值将分别是域 Y 上的码的维数。我们注意到，这些值是使用 Macaulay2 [10] 计算得到的。

TABLE 1. $\mathbb{P}(1,1,2)$ 上 $\mathbb{F}_5$的希尔伯特函数值

d	0	1	2	3	4	5	6	7	8	9	10	11	12	
$H_Y(d)$	1	2		4	6	9	12	15	18	21	24	27	28	30
d	13	**14**	15	16	17	18	19	20	21	22	23	24	25	
$H_Y(d)$	30	31	30	31	30	31	30	31	30	31	30	31	30	

TABLE 2. $\mathbb{P}(1,1,5)$ 在 $\mathbb{F}_5$ 上的希尔伯特函数值

d	0	1	2	3	4	5	6	7	8	9	10	11	12		
$H_Y(d)$	1		2	3	4		5	7	8	9	10	11	13	14	15
d	13	14	15	16	17	18	19	20	21	22	23	24	**25**		
$H_Y(d)$	16	17	19	20	21	22	23	25	26	27	28	29	31		
d	26	27	28	29	30	31	32	33	34	35	36	37	38		
$H_Y(d)$	30	30	30	30	31	30	30	30	30	31	30	30	30		

TABLE 3. $\mathbb{P}(1,1,7)$ 在 $\mathbb{F}_5$ 上的希尔伯特函数值

d	0	1	2	3	4	5	6	7	8	9		10	11	12
$H_Y(d)$	1	2	3	4		5	6	6	7	8	9		10	11	12
d	13	14	15	16	17	18	19	20	21	22	23	24	25	
$H_Y(d)$	12	13	14	15	16	17	18	18	19	20	21	22	23	
d	26	27	28	29	30	31	32	33	34	**35**	36	37	38	
$H_Y(d)$	24	24	25	26	27	28	29	30	30	31	30	30	30	
d	39	40	41	42	43	44	45	46	47	48	49	50	51	
$H_Y(d)$	30	30	30	31	30	30	30	30	30	30	31	30	30	

注 3.16。请注意，在这些表格中，我们用粗体红色强调正则性集的第一个元素 d 。

4. MINIMUM DISTANCE

回顾一下， $Y = \{[1 : y_2 : y_3] : y_2, y_3 \in \mathbb{F}_q\} \cup \{[0 : y_2 : 1] : y_2 \in \mathbb{F}_q\} \cup \{[0 : 1 : 0]\}$ 是加权射影空间 $X = \mathbb{P}(1,1,b)$ 中在代数闭域 $\overline{\mathbb{F}}_q$ 上的 $\mathbb{F}_q$-有理点集合，其中 b 是一个正整数。

引理 4.1. 如果 $0 < d < b$ ，那么 $\delta(C_{d,\ Y}) \geq q$。

证明. 设 $F \in S_d \backslash \{0\}$。由于 $\deg(x_3) = b$ 且 $d < b$，显然 $F \in \mathbb{F}_q[x_1, x_2]$。因此，我们假设 $F = x_1^{\ell} F'(x_1, x_2)$，其中 $F' \in \mathbb{F}_q[x_1, x_2]$ 是次数为 $d - \ell$、不能被 x_1整除的齐次多项式。因此， $F'(x_1, x_2) = x_1 F_1(x_1, x_2) + F_2(x_2)$，其中 F_1 和 F_2 分别是次数为 $d - \ell - 1$ 和$d - \ell$的齐次多项式。因此，对于某个 $c \in \mathbb{F}_q^*$，有 $F_2(x_2) = cx_2^{d-\ell}$。所以，

$$F(x_1, x_2, x_3) = x_1^{\ell}[x_1 F_1(x_1, x_2) + cx_2^{d-\ell}]. \tag{4.1}$$

情形 I：设 $\ell > 0$。那么， F 有 $q + 1$ 个根 $[y_1 : y_2 : y_3]$ ，满足 $y_1 = 0$。由于 $f(x_2) := F(1, x_2, x_3) \in \mathbb{F}_q[x_2] \backslash \{0\}$ 是一元式，它至多有 q 个根 $y_2 \in \mathbb{F}_q$。如果 f 有 q 个根，那么 F 在 Y 中的 $q^2 + q + 1$ 个点处为零，因此 $F \in I(Y)$。因此，码字 $\mathrm{ev}_{d,\ Y}(F) = 0$。于是，为了得到非平凡码字，$f$ 至多有 $q - 1$ 个根，而 F至多有 $(q-1)q$ 个根，其中 $y_1 = 1, y_2 \in V(f) \subset \mathbb{F}_q$ 且 $y_3 \in \mathbb{F}_q$。因此， F在 Y中至多有 $q + 1 + (q-1)q = q^2 + 1$个根。

情形 II：设 $\ell = 0$。若 $F(0, y_2, y_3) = 0$，则由 (4.1) 得到 $y_2 = 0$。因此， F在 Y 中只有一个根 $[0 : 0 : 1]$ ，其中 $y_1 = 0$。

为了研究 $y_1 = 1$ 处的根，我们再次考虑一元多项式$f(x_2) = F(1, x_2, x_3)$。由于 $f(x_2)$ 至多有 q 个根， F在 Y 中至多有 q^2 个根 $[1 : y_2 : y_3]$。总之， F在 Y 中至多有 $q^2 + 1$ 个根。

因此，在两种情形下，码字 $\mathrm{ev}_{d,\ Y}(F) = (F(P_1) \ldots, F(P_N))$（其中 $N = q^2 + q + 1$）都至少有 $q = N - (q^2 + 1)$ 个非零分量，从而得到$\delta(C_{d,\ Y}) \geq q$。□

定理 4.2. 码 $C_{d,\ Y}$ 的最小距离由 (4.2) 给出

$$\delta = \begin{cases} q & \text{if } q \leq d < b \\ q(q-d+1) & \text{if } d < q \leq b \\ q(q-d+1) & \text{if } d < b < q \\ q(q-d+1) & \text{if } b \leq d < q \\ q-k & \text{if } b \leq q \leq d, d = q + kb + r \text{ with } 0 \leq r < b \text{ and } 0 \leq k \leq q-2 \\ q-k & \text{if } q < b \leq d, d = q + kb + r \text{ with } 0 \leq r < b \text{ and } 0 \leq k \leq q-2 \\ 1 & \text{if } d = q + kb + r \text{ with } 0 \leq r < b \text{ and } k \geq q-1 \end{cases}$$

证明。情形 I：$\mathrm{q} \leq \mathrm{d} < \mathrm{b}$：多项式

$$F_0 = x_1 x_2^{d-q} \prod_{y_2 \in \mathbb{F}_q^*} (x_2 - y_2 x_1) \in S_d,$$

有 $q+1$ 个根 $[y_1 : y_2 : y_3]$，其中 $y_1 = 0$ 以及 $q(q-1)$ 个根位于 $y_1 = 1$ 中 X。总计， F在 Y 中有 $q^2 + 1$ 个根。我们知道 $N = q^2 + q + 1$。因此，我们得到 $\delta \leq N - (q^2 + 1) = q$. 所以，根据引理 4.1，我们得到 $\delta = q$。

情形 II：$\mathrm{d} < \mathrm{q} \leq \mathrm{b}$：对于非零的 $F \in S_d$，令 $F = x_1^\ell F'(x_1, x_2)$，其中 F'是次数为 $d - \ell$的齐次多项式，形式为 $F'(x_1, x_2) = x_1 F_1' + c x_2^{d-\ell}$，且 $c \in \mathbb{F}_q^*$，如引理 4.1 的证明中所示。注意，一元多项式$f(x_2) = F(1, x_2)$ 的次数为 $d - \ell$，因此至多可以有 $d - \ell$ 个根 $y_2 \in \mathbb{F}_q$。

如果 $\ell > 0$，那么 F将有 $q+1$个根满足 $y_1 = 0$，并且至多有 $q(d-\ell)$ 个根满足 $y_1 = 1$。总之，由于 $\ell \geq 1$， F至多有 $qd + 1 + q(1-\ell)$ 个 $\leq qd + 1$ 根。

如果 $\ell = 0$，那么 F 将有 1 个根满足 $y_1 = 0$，并且至多有 qd 个根满足 $y_1 = 1$。总之， F至多有 $qd + 1$ 个根。

多项式

$$F_0 = x_1 \prod_{y_2=1}^{d-1} (x_2 - y_2 x_1) \in S_d,$$

有 $q+1$ 个根 $[y_1 : y_2 : y_3]$ 满足 $y_1 = 0$，以及 $q(d-1)$ 个根满足 $y_1 = 1$，位于 X 中。因此，它在 Y中有 $qd + 1$ 个根。因此， $\delta = q^2 + q + 1 - (qd + 1) = q(q + 1 - d)$。

情形 III：$\mathrm{d} < \mathrm{b} < \mathrm{q}$：此处可沿用前一种情形证明中的论证，得到 $\delta = q(q - d + 1)$。

情形 IV：$\mathrm{b} \leq \mathrm{d} < \mathrm{q}$：设 $d = d_0 b + r_0$，其中 $0 \leq r_0 < b$。对于非零的 $F \in S_d$，我们考虑以下关键子集

$$J = \{y_3 \in \mathbb{F}_q : y_3 x_1^b - x_3 \text{ divides } F\}.$$

显然， $|J| \leq d_0$。由此可知，只要 $y_3 \in J$，就有 $F(1, y_2, y_3) = 0$，且在 Y 中存在 $q|J|$ 个这样的点满足 $y_1 = 1$。

另一方面，当 $y_3 \notin J$时，多项式 $f(x_2) = F(1, x_2, y_3) \in \mathbb{F}_q[x_2]\backslash\{0\}$。这是因为一般而言，对于某个 $H \in \mathbb{F}_q[x_1, x_2, x_3]$，以及非零齐次多项式，我们有 $F(x_1, x_2, x_3) = (y_3x_1^b - x_3)H + r(x_1, x_2)$。

$$r(x_1, x_2) = \sum_{i=0}^{d} r_i x_1^i x_2^{d-i}$$

次数为 d。因此，如果 $f \equiv 0$，那么 $r(1, x_2) = \sum_{i=0}^{d} r_i x_2^{d-i}$是一个零多项式，即 $r_i = 0$ 对所有 i都成立，这意味着 $r = 0$ 作为多项式是一个矛盾。因此，如果$y_3 \notin J$，那么 f至多有 $\deg_{x_2}(F)$ $= \deg(f)$ 个根。因此， F至多有$|\mathbb{F}_q\backslash J|$ $\deg_{x_2}(F) = (q - |J|) \deg_{x_2}(F)$ 个这样的根。于是，我们有

$$|V_Y(F) \cap U_1| \leq q|J| + (q - |J|) \deg_{x_2}(F), \tag{4.3}$$

其中 $V_Y(F) = \{P \in Y\colon F(P) = 0\}$，且 $U_1 = \{[x_1\colon x_2\colon x_3] \in Y\colon x_1 = 1\}$。

现在考虑以下对次数为 $d = d_0b + r_0$ 的齐次多项式的一般描述，其中 $0 \leq r_0 < b$:

$$F(x_1, x_2, x_3) = x_1^{\ell} \prod_{y_3 \in J} (y_3x_1^b - x_3)F'(x_1, x_2, x_3) \text{ where } F' = x_1F_1 + F_2,$$

且 $F_2(x_2, x_3)$ 是一个次数为 $d - \ell - |J|b$ 的齐次多项式，其中 $x_1 \nmid F_2$。下面估计满足 $x_1 = 0$ 的 F 的根。

若 $\ell > 0$，则满足 $x_1 = 0$ 的 F 有 $q + 1$ 个根。因此，我们有

$$\begin{aligned} |V_Y(F)| &\leq q + 1 + q|J| + (q - |J|) \deg_{x_2}(F) \\ &\leq q + 1 + q|J| + (q - |J|)(d - \ell - |J|b). \\ &= q + 1 + q(d - \ell) + |J|(q - qb - d + \ell + |J|b) \\ &\leq q + 1 + q(d - \ell) \leq qd + 1, \end{aligned}$$

因为我们现在证明 $q - qb - d + \ell + |J|b \leq 0$ 成立：若 $b = 1$，则有

$$q - qb - d + \ell + |J|b = \ell - d + |J| \leq 0;$$

且若 $b \geq 2$，则 $q + \ell \leq 2q \leq qb$，从而得到以下结果

$$q - qb - d + \ell + |J|b \leq q - qb - d + \ell + d_0b \leq q - qb + \ell \leq 0.$$

若 $\ell = 0$，则 $F(0, y_2, 1) = 0$ 蕴含 $F'(0, y_2, 1) = 0$，即 $F' \in I([0\colon y_2\colon 1])$。根据命题 3.4], , 由 [19, 可得

$$x_1F_1 + F_2 = F' \in I([0 : y_2 : 1]) = \langle x_1, x_2^b - y_2^b x_3 \rangle$$

因此，当 $y_2 \neq 0$ 时， $x_2^b - y_2^b x_3$ 是 F_2 的一个因子。此外， F_2 至多有 $d_0 - |J|$ 个这样的因子，因为 d 中至多有 d_0b 个，且 $\deg_{x_2}(F_2) = d - |J|b$。因此，形如 $[0\colon y_2\colon 1]$ 的根至多有 $d_0 - |J|$ 个。在这种情况下，我们有

$$F(x_1, x_2, x_3) = \prod_{y_3 \in J} (y_3x_1^b - x_3)[x_1F_1 + x_2^{r_0} \prod_{y_2=1}^{d_0-|J|} (x_2^b - y_2^b x_3)].$$

但是 $I([0 : 0 : 1]) = \langle x_1, x_2 \rangle$ 且当 $r_0 > 0$, $F'(0, 0, 1) = 0$.
当 $J \neq \emptyset$ 时，点 $[0 : 1 : 0]$ 也是一个根，因为 $y_3x_1^b - x_3$ 是 F 的因子。

总而言之，当 $x_1 = 0$ 时，至多有 $2 + d_0 - |J|$ 个根。因此，我们有

$$\begin{aligned} |V_Y(F)| &\leq 1 + d_0 + 1 - |J| + q|J| + (q - |J|)\deg_{x_2}(F) \\ &\leq 1 + d_0 + q|J| + (q - |J|)(d - |J|b) \\ &= 1 + d_0 + qd + |J|(q - qb - d + |J|b) \\ &\leq 1 + qd + |J|(d_0 + q - qb - d + |J|b) \\ &\leq qd + 1, \end{aligned}$$

由于 $b > 1$ 蕴含 $d_0 + q \leq qb$，因此我们有 $d_0 + q - qb - d + |J|b \leq 0$。
设 $J = \emptyset$。由于 $\deg_{x_2}(F) \leq d$，F 至多有 qd 个 $[1$ 型的根：$y_2 :\ y_3]$，由 (4.3) 可知。接下来，我们计算满足 $x_1 = 0$ 的根的数量。若 $\deg_{x_2}(F) = d$，则 x_2^d 会出现在 F 中，因此 $F \notin I(0, 1, 0) = \langle x_1,\ x_3\rangle$. 因此，$F(0, 1, 0) \neq 0.$。同理，$F$ 不能属于 $I(0, y_2, 1) = \langle x_1,\ y_2^b x_3 - x_2^b\rangle$ 对任意 $y_2 \in \mathbb{F}_q^*$. 都成立。因此，F 唯一可能的根是 $[0 :\ 0 :\ 1]$，当 $x_1 = 0.$ 时。综上，F 至多有$qd + 1$个根。若 $\deg_{x_2}(F) \leq d - 1$，则由 (4.3) 可知，F至多有 $q(d - 1)$ 个满足 $x_1 = 1$ 的根。由于 F 至多有 $q + 1$ 个满足 $x_1 = 0$ 的根，因此我们有

$$|V_Y(F)| \leq q(d - 1) + q + 1 = qd + 1.$$

因此，无论哪种情况，我们都得到 $|V_Y(F)| \leq qd + 1$，其中 $\ell = 0$。

现在考虑多项式

$$F_0(x_1, x_2, x_3) = \prod_{y_2=1}^{d} (x_2 - y_2 x_1) \in S_d.$$

F_0 在 $[1 :\ y_2 :\ y_3]$ 处为零，其中 d 属于 $y_2 \in \mathbb{F}_q$ 且 $y_3 \in \mathbb{F}_q$，因此它有 qd 个根。此外，$F_0(0, x_2, y_3) = x_2^d = 0$ 意味着 $x_2 = 0$，也就是说，当$x_1 = 0$时，它只有一个根 $[0 : 0 :\ 1]$。因此，F_0 恰有 $qd + 1$ 个根。于是，最终得到以下等式，

$$\delta = N - (qd + 1) = q^2 + q + 1 - qd - 1 = q(q - d + 1),$$

正如所需。

情形 V：$\mathsf{b} \leq \mathsf{q} \leq \mathsf{d}$：令 $d = q + kb + r$ 为满足 $0 \leq r < b$的集合。一个非零的 $F \in S_d$具有如下形式

$$F = x_1^{\ell} \prod_{y_3 \in J} (y_3 x_1^b - x_3) F'(x_1, x_2, x_3) \tag{4.4}$$

对于如情形 IV 中的子集 $J \subseteq \mathbb{F}_q$，以及次数为$\mu = d - \ell - |J|b$的齐次多项式 F'。

设 $0 \leq |J| \leq k$。利用以下事实：$f_3 = x_1^q x_2 - x_1 x_2^q \in I(Y)$ 且 $|V_Y(F)| \neq |V_Y(\bar{F})|$ 当 $F - \bar{F} \in I(Y)$ 时，我们可以在 F 中用 $x_1^q x_2$ 替换 $x_1 x_2^q$，并假设 F 不含可被 $x_1 x_2^q$ 整除的项。若 $\ell > 0$，则 x_1 整除 F，因此 $\deg_{x_2}(F) < q$，这表明一元多项式 $f(x_2) := F(1, x_2, y_3) \in \mathbb{F}_q[x_2] \setminus \{0\}$ 至多有 $q - 1$ 个根，对每个 $y_3 \in \mathbb{F}_q \setminus J$ 都成立。若 $\ell = 0$ 且 $f(x_2)$ 有 q 个根 $y_2 \in \mathbb{F}_q$，则 $x_2 - y_2$ 整除 f，这意味着 $\deg_{x_2}(F) \geq q$，因为 $x_2 - y_2$ 本可以由 $x_2 - y_2 x_1$ 或 $y_3 x_2^b - y_2^b x_3$ 整除 F 得到。将 $F' = x_1 F_1 + F_2$ 写为 $x_1 \nmid F_2$，我们注意到 $F_1 = 0$，因为对所有 $y_2 \in \mathbb{F}_q$，$x_2 - y_2$ 都整除 f，且 F 不含可被 $x_1 x_2^q$ 整除的项。因此，当 $y_2 \neq 0$ 时，$x_2 - y_2 x_1$ 不可能整除 $F' = F_2$，这意味着对所有 $y_2 \in \mathbb{F}_q^*$，$y_3 x_2^b - y_2^b x_3$ 都整除 F'。因此，我们得到

$$d - |J|b = \deg_{x_2}(F) = \deg_{x_2}(F') \geq (q - 1)(q - |J|)b,$$

因为这样的 $y_3 \in \mathbb{F}_q \setminus J$ 有 $q-|J|$ 个。由 $k \le q-2$ 和 $r < b$ 可得

$$\begin{aligned} q+(q-1)b > d = q+kb+r &\ge |J|b+(q-1)(q-|J|)b \\ &= 2|J|b+q^2b-q|J|b-qb \\ &= (2|J|+q^2-q|J|-q)b \\ &= (2-q)|J|b+q(q-1)b. \end{aligned}$$

于是，我们有 $q > (2-q)|J|b+(q(q-1)-(q-1))b = (2-q)|J|b+(q-1)^2b$. 因此，$q+(q-2)|J|b > (q-1)^2b$. 由于 $0 \le |J| \le k \le q-2$，我们有

$$q+(q-2)^2b > (q-1)^2b \Rightarrow q > (q-1)^2b-(q-2)^2b = (2q-3)b$$

由于 $b \ge 2$，我们得到 $q > (2q-3)b \ge 4q-6$，从而导致矛盾，即 $2 > q$。因此，f 至多有 $q-1$ 个根。因此，若 $0 \le |J| \le k$，则得到以下不等式:

$$\begin{aligned} |V_Y(F)| &\le q+1+q|J|+(q-|J|)(q-1) \\ &\le q+1+q|J|+q^2-q-q|J|+|J| \\ &\le q^2+k+1. \end{aligned}$$

另一方面，若 $|J| > k$，则我们可以写成 $|J| = k+j_0$，其中 $j_0 \ge 1$。我们先考虑情形 $\ell > 0$。在这种情况下，$|J| < q$，因为若 $|J| = q$，则有 $F \in I(Y)$，这是因为下列等式成立

$$|V_Y(F)| = q+1+q|J|+(q-|J|)\deg_{x_2}(F) = q^2+q+1.$$

由此可得

$$\begin{aligned} d-\ell-b|J| &= d-\ell-bk-b(j_0-1+1) \\ &= q+r-b-b(j_0-1)-\ell \quad (\text{ as } d-bk = q+r) \\ &\le q-1-\ell-b(j_0-1) \quad (\text{ as } r-b \le -1) \\ &\le q-2-b(j_0-1) \quad (\text{ as } -\ell \le -1). \end{aligned}$$

因此，我们有:

$$\begin{aligned} |V_Y(F)| &\le q+1+q|J|+(q-|J|)(d-\ell-|J|b) \\ &\le q+1+q|J|+(q-|J|)(q-2-b(j_0-1)) \\ &= q+1+q|J|+q^2-2q-qbj_0+qb-q|J|+2|J|+bj_0|J|-b|J| \\ &= q+1+q^2-2q-qb(j_0-1)+2|J|+b|J|(j_0-1) \\ &= q^2+1-q+(j_0-1)b(|J|-q)+2|J|+k-k \\ &= q^2+k+1+(j_0-1)b(|J|-q)+|J|-k+|J|-q \\ &\le q^2+k+1+(j_0-1)b(-1)+j_0-1 \quad (\text{ as } |J|-q \le -1.) \\ &= q^2+k+1-(j_0-1)(b+1) \\ &\le q^2+k+1. \end{aligned}$$

设 $|J|>k$ 和 $\ell=0$. 为 $|J|=k+j_0$，其中 $j_0\geq 1$，我们有

$$\begin{aligned} d-bj &= d-bk-bj_0 \\ &= q+r-b(j_0+1-1) \\ &= q+r-b-b(j_0-1) \\ &\leq q-1-b(j_0-1) \end{aligned}$$

在这种情况下，可得

$$\begin{aligned} |V_Y(F)| &\leq q+1+q|J|+(q-|J|)(q-1-b(j_0-1)) \\ &= q+1+q|J|+q^2-q-q|J|+|J|+(|J|-q)b(j_0-1)+k-k \\ &= q^2+k+1+(|J|-q)b(j_0-1)+|J|-k \\ &\leq q^2+k+1-b(j_0-1)+j_0 \quad (\text{ if } |J|-q\leq -1) \\ &\leq q^2+k+1 \quad (\text{ if } j_0\geq 2 \text{ as } b\geq 2). \end{aligned}$$

因此，只需证明当 $j_0=1$ 或 $|J|=q$ 时，同一不等式仍成立。令 $j_0=1$，则有 $|J|=k+1$。回忆一下，形如 $[0\colon y_2\colon 1]$ 且满足$y_2\in\mathbb{F}_q^*$的根的数量至多为 $d_0-|J|=d_0-k-1<q-1$，因为 $d_0<k+q$。再加上 $[0:1:0]$和 $[0:0:1],$，满足 $x_1=0.$ 的根至多有 q 个。因此，我们有

$$\begin{aligned} |V_Y(F)| &\leq q+q(k+1)+(q-(k+1))(d-b(k+1)) \\ &\leq q+qk+q+(q-k-1)(q-1) \quad (\text{ as } q+r-b\leq q-1) \\ &\leq q+qk+q+q^2-q-qk+k-q+1=q^2+k+1. \end{aligned}$$

另一方面，若 $|J|=q$，则显然有

$$\begin{aligned} |V_Y(F)| &\leq 2+d_0-|J|+q|J|+(q-|J|)(d-|J|b) \\ &= 2+d_0-q+q^2 \\ &\leq q^2+k+1 \quad (\text{ as } d_0<k+q) \end{aligned}$$

因此，对于所有 ℓ 以及所有 $|J|$，都有 $|V_Y(F)|\leq q^2+k+1.$。现在考虑以下次数为 $d=q+kb+r$ 且满足 $0\leq r<b$ 的多项式，

$$F_0(x_1,x_2,x_3)=x_1^{r+1}\prod_{y_3=1}^{k}(y_3x_1^b-x_3)\prod_{y_2\in\mathbb{F}_q^*}(x_2-y_2x_1)\in S_d.$$

F_0 在 $[1:y_2:y_3]$ 处消失，其中 k 属于 y_3，且对所有 $y_2\in\mathbb{F}_q$ 也成立；它还在 $[1:y_2:y_3]$ 处消失，其中剩余的 $q-k$ 属于 y_3，且对所有 $y_2\in\mathbb{F}_q^*$也成立。因此它有$qk+(q-1)(q-k)$ 个 $=q^2-q+k$ 根。此外，由于 $r+1\geq 1$， F_0 在$[0\colon y_2\colon 1]$ 处对所有 $y_2\in\mathbb{F}_q$ 都消失，并且在 $[0:1:0].$ 处消失。总之， F_0 恰有 q^2+k+1 个根。

因此，最终得到以下等式，

$$\delta=N-(q^2+k+1)=q^2+q+1-q^2-k-1=q-k,$$

正如所需。

情形 VI: $\mathbf{q<b\leq d}$: 由于此论证不依赖于 q 大于还是小于 b，因此前一种情形证明中使用的论证在此同样适用，并得到 $\delta=q-k$，正如所需。

情形 VII: $\mathbf{d=q+kb+r}$，且 $\mathbf{0\leq r<b}$，$\mathbf{k\geq q-1}$:

$$F_0 = x_1^{\ell_0} \prod_{y_3 \in \mathbb{F}_q^*} (y_3 x_1^b - x_3) \prod_{y_2 \in \mathbb{F}_q^*} (y_2 x_1 - x_2) \in S_d$$

恰好在 $q^2 + q = q + 1 + (q-1)q +$(q − 1) 个点处消失，因为幂$l_0 := d - q -$ ($q-1)b+1 \geq r+1 \geq 1$。这意味着相应的码字$ev_Y(F_0)$ 的重量为 1。□

注 4.3。 [2] 的猜想 2.3 对集合 $Y = \mathbb{P}(1, w_1, \ldots, w_n)(\mathbb{F}_q)$ 中的 $|V_Y(F)|$ 给出了一个上界，并适用于任何次数为 d 且是 lcm$(w_1, \ldots, w_n)$ 的倍数的齐次多项式；定理 2.4 在 $m = 2$ 的情形下证明了这一点。定理 4.2 的情形 4 在 $r_0 = 0$ 的条件下完成了证明。

4.1. 主要参数示例。本小节展示加权射影空间$X = \mathbb{P}(1, 1, b)$上各码的主要参数表。本部分旨在展示本文所完成的工作，并提供将所得的码与 http://codetables.de/ 上的记录进行比较的机会（见 [9]）。表中以红色标出的次数表示正则性集合的首个元素。表中以蓝色标出的次数表示，对于每个 b 次数，码的大小均等于码的长度。

TABLE 4. 加权射影平面 $Y = \mathbb{P}(1, 1, b)(\mathbb{F}_2)$ 上的码的主要参数

b	次数 N K δ		b	次数 N K δ		b	次数 N K δ	
$b=2$	$d=2$	7 4 2	$b=5$	$d=2$	7 3 2	$b=7$	$d=2$	7 3 2
	$d=3$	7 5 2		$d=3$	7 3 2		$d=3$	7 3 2
	$d=4$	7 7 1		$d=4$	7 3 2		$d=4$	7 3 2
	$d=5$	7 6 1		$d=5$	7 4 2		$d=5$	7 3 2
	$d=6$	7 7 1		$d=6$	7 5 1		$d=6$	7 3 2
	$d=7$	7 6 1		$d=7$	7 6 1		$d=7$	7 4 1
	$d=8$	7 7 1		$d=8$	7 6 1		$d=8$	7 5 1
	$d=9$	7 6 1		$d=9$	7 6 1		$d=9$	7 6 1
	$d=10$	7 7 1		$d=10$	7 7 1		$d=10$	7 6 1
	$d=11$	7 6 1		$d=11$	7 6 1		$d=11$	7 6 1
	$d=12$	7 7 1		$d=12$	7 6 1		$d=12$	7 6 1
	$d=13$	7 6 1		$d=13$	7 6 1		$d=13$	7 6 1
	$d=14$	7 7 1		$d=14$	7 6 1		$d=14$	7 7 1
	$d=15$	7 6 1		$d=15$	7 7 1		$d=15$	7 6 1

TABLE 5. $Y = \mathbb{P}(1, 1, b)(\mathbb{F}_5)$上的码的主要参数

b	次数	N	K	δ
$b = 2$	$d = 2$	31	4	20
	$d = 3$	31	6	15
	$d = 4$	31	9	10
	$d = 5$	31	12	5
	$d = 6$	31	15	5
	$d = 7$	31	18	4
	$d = 8$	31	21	4
	$d = 9$	31	24	3
	$d = 10$	31	27	3
	$d = 11$	31	28	2
	$d = 12$	31	30	2
	$d = 13$	31	30	1
	$d = 14$	31	31	1
	$d = 15$	31	30	1
	$d = 16$	31	31	1
	$d = 17$	31	30	1
	$d = 18$	31	31	1
	$d = 19$	31	30	1
	$d = 20$	31	31	1
	$d = 21$	31	30	1
	$d = 22$	31	31	1
	$d = 23$	31	30	1
	$d = 24$	31	31	1
	$d = 25$	31	30	1
	$d = 26$	31	31	1
	$d = 27$	31	30	1
	$d = 28$	31	31	1
	$d = 29$	31	30	1
	$d = 30$	31	31	1
	$d = 31$	31	30	1
	$d = 32$	31	31	1
	$d = 33$	31	30	1
	$d = 34$	31	31	1
	$d = 35$	31	30	1

b	次数	N	K	δ
$b = 5$	$d = 2$	31	3	20
	$d = 3$	31	4	15
	$d = 4$	31	5	10
	$d = 5$	31	7	5
	$d = 6$	31	8	5
	$d = 7$	31	9	5
	$d = 8$	31	10	5
	$d = 9$	31	11	5
	$d = 10$	31	13	4
	$d = 11$	31	14	4
	$d = 12$	31	15	4
	$d = 13$	31	16	4
	$d = 14$	31	17	4
	$d = 15$	31	19	3
	$d = 16$	31	20	3
	$d = 17$	31	21	3
	$d = 18$	31	22	3
	$d = 19$	31	23	3
	$d = 20$	31	25	2
	$d = 21$	31	26	2
	$d = 22$	31	27	2
	$d = 23$	31	28	2
	$d = 24$	31	29	2
	$d = 25$	31	31	1
	$d = 26$	31	30	1
	$d = 27$	31	30	1
	$d = 28$	31	30	1
	$d = 29$	31	30	1
	$d = 30$	31	31	1
	$d = 31$	31	30	1
	$d = 32$	31	30	1
	$d = 33$	31	30	1
	$d = 34$	31	30	1
	$d = 35$	31	31	1

b	次数	N	K	δ
$b = 7$	$d = 2$	31	3	20
	$d = 3$	31	4	15
	$d = 4$	31	5	10
	$d = 5$	31	6	5
	$d = 6$	31	6	5
	$d = 7$	31	7	5
	$d = 8$	31	8	5
	$d = 9$	31	9	5
	$d = 10$	31	10	5
	$d = 11$	31	11	5
	$d = 12$	31	12	4
	$d = 13$	31	12	4
	$d = 14$	31	13	4
	$d = 15$	31	14	4
	$d = 16$	31	15	4
	$d = 17$	31	16	4
	$d = 18$	31	17	4
	$d = 19$	31	18	3
	$d = 20$	31	18	3
	$d = 21$	31	19	3
	$d = 22$	31	20	3
	$d = 23$	31	21	3
	$d = 24$	31	22	3
	$d = 25$	31	23	3
	$d = 26$	31	24	2
	$d = 27$	31	24	2
	$d = 28$	31	25	2
	$d = 29$	31	26	2
	$d = 30$	31	27	2
	$d = 31$	31	28	2
	$d = 32$	31	29	2
	$d = 33$	31	30	1
	$d = 34$	31	30	1
	$d = 35$	31	31	1

ACKNOWLEDGEMENTS

作者感谢 Jade Nardi 对稿件提出的宝贵意见。作者受到土耳其科学技术研究理事会（TÜBİTAK）项目编号：119F177 的资助。第一作者受到 TÜBİTAK-2211/A 的资助。本文是第一作者在第二作者指导下完成的博士论文的一部分。

References

[1] Yves Aubry。与射影代数簇相关的 Reed-Muller 码。载于 *Coding theory and algebraic geometry (Luminy, 1991)* 1518 *Lecture Notes in Math.* 4 17 ，第 卷，页码 –。施普林格出版社，柏林，1992 年。[2] Yves Aubry 、 Wouter Castryck 、 Sudhir R. Ghorpade、Gilles Lachaud、Michael E. O'Sullivan 和 Samrith Ram。有限域上加权射影空间中的超曲面及其在编码理论中的应用。载于 *Algebraic geometry for coding theory and cryptography*, *Assoc. Women Math. Ser.*第9卷，页码25–61。施普林格，尚，2017年。[3] Daniele Bartoli、Adnen Sboui 和 Leo Storme。有限域上代数超曲面有理点数的界及其在射影 Reed-Muller 码中的应用。*Adv. Math. Commun.*，10(2):355–365，2016年。[4] Mauro Beltrametti 和 Lorenzo Robbiano。加权射影空间理论导论。 *Exposition. Math.*，4(2):111–162，1986年。[5] Winfried Bruns 和 J ¨ *Cohen-Macaulay rings* 39 *Cambridge Studies in Advanced Mathematics* 1993 urgen Herzog。[6] ，第 卷。剑桥大学出版社，剑桥，。[6] David A Buchsbaum 和 David Eisenbud。是什么使一个复形成为正合复形？ *Journal of Algebra*，25 2 259( ): –268，1973年。[7] Eduardo Dias 和 Jorge Neves。加权环面上的码。 *Finite Fields Appl.*，33 79，2015 66: –。[8] Olav Geil 和 Casper Thomsen。重新审视加权 Reed–Muller 码。 *Des. Codes Cryptogr.*，66 1 3 195(-): –220，2013年。[9] Markus Grassl。线性码和量子码的最小距离界。在线可查: `http://www.codetables.de`，2007年。访问日期: 2023年6月12日。[10] Daniel R. Grayson 和 Michael E. Stillman。Macaulay2，一款用于代数几何研究的软件系统。[11] Gilles Lachaud。射影 Reed-Muller 码。载于 *Coding theory and applications (Cachan, 1986)* 311 *Lecture Notes in Comput. Sci.* 125 129 1988 ，第 卷，页码 –。施普林格出版社，柏林，。[12] Gilles Lachaud。射影 Reed-Muller 码的参数。 *Discrete Math.*，81(2):217–221，1990年。[13] Ezra Miller 和 Bernd Sturmfels。 *Combinatorial commutative algebra* 227 *Grad-* ，第 *uate Texts in Mathematics* 2005 卷。施普林格出版社，纽约，。[14] Jade Nardi。极小 Hirzebruch 曲面上的代数几何码。 *J. Algebra*，535:556–597，2019年。[15] Jade Nardi。射影托里克码。 *Int. J. Number Theory*，18(1):179–204，2022年。[16] Anders Bjært Sørensen。射影 Reed-Muller 码。 *IEEE Trans. Inform. Theory*，37 6 1567 1576，1991 ( ): –。[17] Anders Bjært Sørensen。加权 Reed–Muller 码与代数几何码。 *IEEE Trans. Inform. Theory* 38 6 1821 1826, 1992 ，( ): –。[18] Mesut S¸ahin。托里克码与格理想。 *Finite Fields Appl.*，52:243–260，2018 年。[19] Mesut S¸ahin。计算托里克码的消失理想，2022年，https://arxiv.org/abs/2207.01061。

Department of Mathematics, Hacettepe University, Ankara, TURKEY
Email address: `yagmur.cakiroglu@hacettepe.edu.tr`

Department of Mathematics, Hacettepe University, Ankara, TURKEY
Email address: `mesut.sahin@hacettepe.edu.tr`