arXiv:2303.04757v1 [cs.IT] 8 Mar 2023

来自一般线性群的纠错码

Mahir Bilen Can[1]

[1] 杜兰大学，新奥尔良，路易斯安那州，mahirbilencan@gmail.com

2023年3月9日

摘要

确定了一般线性群上的代数几何码的参数，并找出了具有最少（或最多）有理点数的超平面截面。

关键词：代数几何码、良好滤过、超平面截面 MSC：14G50，94B27

1 引言

本文分析有限域上一般线性群的超平面截面。本文的主要目标是研究我们利用良好滤过构造的一族线性纠错码中最简单的情形。令 $GL_n(F)$ 表示定义在有限域 F 上的 $n \times n$ 矩阵的一般线性群。为引出本文的讨论，我们先考察在含两个元素的域 $F = \mathbb{F}_2$ 上的 2×2 矩阵情形。令

$$GL_2(F) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : \{a, b, c, d\} \subseteq F \text{ and } ad - bc = 1 \right\}. \tag{1.1}$$

$GL_2(F)$ 的定义表示是二维向量空间 $V := F^2$。这是一个简单的 $GL_2(F)$-模。令 $S(V^*)$ 表示对偶向量空间 V^* 上的对称代数。用 $S^r(V^*)$ 表示 $S(V^*)$ 中次数为 r 的齐次部分。每个简单的 $GL_2(F)$-模都包含在某个空间 $S^r(V^*)$ 中，其中 $r \in \{1, 2, \dots\}$ 为某个值。令 $M_2(F)$ 表示所有元素取自 F 的 2×2 矩阵所构成的空间。这样，我们可以将张量积 $V_1 := S^1(V^*) \otimes S^1(V)$ 与 $M_2(F)$ 上所有次数为 1 的齐次多项式函数所构成的空间等同起来。本文主要关注以下（F-线性）求值映射的像，记作 C：

$$\begin{aligned} ev_1 : V_1 &\longrightarrow F^{|GL_2(F)|} \\ f &\longmapsto (f(A) | A \in GL_2(F)), \end{aligned}$$

这里我们对群 $GL_2(F)$ 的元素采用一个固定全序。经过直接计算可得

$$|V_1| = 2^4 \text{ and } |GL_2(F)| = 6.$$

此外，很容易验证

$$C = \left\{ \begin{array}{llll} (1,1,1,1,0,0), & (1,0,0,0,1,0), & (0,1,0,0,0,1), & (0,0,1,0,1,0), \\ (0,0,0,1,0,1), & (0,0,1,1,1,1), & (0,1,1,0,1,1), & (1,0,0,1,1,1), \\ (1,1,0,0,1,1), & (1,0,1,0,0,0), & (0,1,0,1,0,0), & (1,1,1,0,0,1), \\ (1,1,0,1,1,0), & (1,0,1,1,0,1), & (0,1,1,1,1,0), & (0,0,0,0,0,0) \end{array} \right\}.$$

通过观察可知， C 中的非零向量所达到的最小汉明重量为 2。因此，我们的码的参数为 $[6,4,2]_2$。具有这些参数的码是 F上长度为 6 的重复码的对偶码的子码。

现在，令 V表示 $GL_n(F)$ 的定义表示，其中 $n \geq 2$，且 F 是一个含有 q 个元素的有限域。于是， $S^1(V^*) \otimes S^1(V)$ 可与所有以 F为元素的 $n \times n$ 矩阵所构成的空间上的线性泛函空间等同。我们将通过在 $GL_n(F)$ 的点上对 $S^1(V^*) \otimes S^1(V)$ 中的元素求值而得到的代数几何码记为 C。最后，对于正整数 r，我们定义 r 的 q模拟为 $[r]_q := 1 + q + \cdots + q^{n-1} = \frac{q^n-1}{q-1}$。作为约定，令 $[0]_q := 1$。阶乘模拟现在表示为 $[r]_q! := [r]_q[r-1]_q \cdots [2]_q[1]_q$。采用这一记号，本文的第一个主定理如下。

定理1. 设 $F = \mathbb{F}_q$。令 C 表示通过在簇 $GL_n(F)$ 上对向量空间 $M_n(F)$ 的所有齐次线性多项式求值而得到的求值码。那么 C 的参数为

1. $\mathtt{n} = q^{\binom{n}{2}}(q-1)^n[n]_q!$,
2. $\mathtt{k} = n^2$,
3. $\mathtt{d} = q^{\binom{n}{2}-1}(q-1)^{n-1}\left((q-1)^2[n]_q! - [n-2]_q!\right)$.

作为这一结果的一个特例，我们得到以下推论。

推论1。设 C 是通过在 $GL_2(F)$ 上取线性形式的值定义的码，其中 $F = \mathbb{F}_q$。那么， C 的长度（记为 n）、维数（记为 k）和最小距离（记为 d）由以下公式给出

1. $\mathtt{n} = q^4 - q^3 - q^2 + q$,
2. $\mathtt{k} = 4$,
3. $\mathtt{d} = q^4 - 2q^3 + q$.

为证明定理1，我们找出 $GL_n(F)$ 中包含最多 F-有理点的超平面截面。本文的另一个目标是证明， $GL_n(F)$ 中包含最少 F-有理点的超平面截面由 Borel 子群的双陪集导出。

令 B 表示 $GL_n(F)$ 中所有上三角矩阵构成的 Borel 子群。 B 的对向 Borel 子群记为 B^-。换言之， B^- 是 $GL_n(F)$ 中所有下三角矩阵构成的 Borel 子群。众所周知， $GL_n(F)$ 中只有有限多个 (B^-, B)-双陪集。切瓦利大胞腔定理 $[1, \text{Part II, §1.9}]$ 告诉我们， B^-B 这个双陪集的几何点在 $GL_n(F)$ 中稠密（关于 Zariski 拓扑）， $\bar{}$其中 F 表示 F 的代数闭包。本文的第二个主要结果将该集合的补集刻画为一个超平面截面。

定理 2. 令 Y 表示 $GL_n(F)$ 中的 (B^-, B)-双陪集 B^-B。那么 $GL_n(F) \setminus Y$ 是具有最少 F-有理点的超平面截面，位于 $GL_n(F)$ 中。

本文的结构如下。在下一节中，我们将介绍所用的记号。在第 3 节中，我们注意到：当 F是一个有限域时， $GL_n(F)$ 的一般超平面截面的 F-有理点数，等于经过 $M_n(F)$ 原点的 $GL_n(F)$ 超平面截面的 F-有理点数。在第 4 节中，我们证明第一个主要结果。在第 5 节中，我们证明第二个主要结果。最后，我们将讨论 $GL_n(F)$- 码的缺陷。

2 预备知识与记号

正整数集记为 $\mathbb{Z}_+$。对于 $n \in \mathbb{Z}_+$，所有元素取自域 F 的 $n \times n$ 矩阵构成的幺半群记为 $M_n(F)$。

设 F 是一个含有 q 个元素的有限域，其中 q 是某个素数的幂。若 X 是定义在 F 上的代数簇，则用记号 $|X|$ 表示 X 的 F-有理点数。当需要强调 q 时，我们将使用 $\mathbb{F}_q$ 而不是 F。

$\bar{}$ $\bar{}$一般线性群 $G := GL_n(F)$，其中 F 是 F的代数闭包，是一个定义在 F 上的代数簇。 G的 F-有理点的数量等于$GL_n(F)$的基数，记作 $\gamma(n, q)$。众所周知， $[3,$ 命题 1.10.1$]$,$\gamma(n, q) = \prod_{i=0}^{n-1} (q^n - q^i)$。我们将这个乘积写成 $q^{\binom{n}{2}}(q-1)^n[n]_q!$ 以下递推关系立刻可得：

$$\gamma(n, q) = q^{n-1}(q^n - 1)\gamma(n-1, q) \qquad \text{for } n \geq 2.$$

由于这对我们的研究很有用，下面我们遵循 $[4]$, 回顾一下 q-元线性码的一种众所周知的改写。一个 $[\mathtt{n}, \mathtt{k}, \mathtt{d}]_q$ 系统是一个有限序列 $\mathcal{P} = (v_1, \ldots, v_\mathtt{n})$，其中$v_1, \ldots, v_\mathtt{n}$是来自一个 F-向量空间 V的向量，但不一定彼此不同，使得

- V中不存在包含所有向量 v_1、……、 $v_\mathtt{n}$的超平面（因此， $\mathtt{n} \geq$维数$_F\, V$）；

- $\mathtt{k} =$ 维数$_F V$;
- $\mathtt{d} = \mathtt{n} - \max_H |\mathcal{P} \cap H|$，其中最大值取遍所有超平面 $H \subseteq V$，并按重数计算各点。（假设 $\mathtt{d} \geq 1$。）

根据 [4, 命题 1.1, 4], 类$[\mathtt{n}, \mathtt{k}, \mathtt{d}]_q$系统与线性 $[\mathtt{n}, \mathtt{k}, \mathtt{d}]_q$码的集合之间存在一一对应关系 φ。在此对应关系下， $\varphi(\mathcal{P})$ 是通过在 $\mathcal{P}$ 的各项上对 V 上的线性泛函求值而得到的码。

3 超平面截面

设 F 是一个域。设 $n \in \mathbb{Z}_+$。除非另有说明，以下均假设 $n \geq 2$。超平面 $H \subset M_n(F)$ 是线性映射 $B^\vee$: $M_n(F) \to F$ 的核沿元素 $C \in M_n(F)$ 平移所得。这意味着存在一个矩阵 $B \in M_n(F)$ 和一个标量 $c \in F$，使得

$$H := \{A \in M_n(F) : \ \mathrm{tr}(AB^\top) = c\}. \tag{3.1}$$

注意，除非标量 c 为零，否则 H 不包含 $M_n(F)$ 中的零元。本节旨在分析交集的基数，

$$H \cap GL_n(F).$$

引理 1. 设 $B \in M_n(F)$ 和 $c \in F$。令 H表示超平面， $H := \{A \in M_n(F) : \mathrm{tr}(AB^\top) = c\}$。那么存在 $r \in [n]$，以及 $GL_n(F)$ 中的两个可逆矩阵 E 和 D，使得

$$GL_n(F) \cap H = \left\{ A \in GL_n(F) : \ tr\left(EAD^{-1} \begin{bmatrix} \mathbf{1}_r & 0 \\ 0 & 0 \end{bmatrix} \right) = c \right\}.$$

证明。首先注意，迹形式在 $GL_n(F)$ 的元素作用下共轭不变:

$$\mathrm{tr}(ECE^{-1}) = \mathrm{tr}(C) \tag{3.2}$$

对于每个 $E \in GL_n(F)$ 和 $C \in M_n(F)$ 都成立。我们将 (3.2) 应用于 H 的定义方程:

$$H = \{A \in M_n(F) : \ \mathrm{tr}(EAB^\top E^{-1}) = c\}.$$

令 $M_n^r(F)$ 表示 $M_n(F)$ 中所有秩为 r 的矩阵构成的集合。接下来假设 $B \in M_n^r(F)$。那么 $B^\top$ 也是 $M_n^r(F)$ 的一个元素。

群 G $L_n(F) \times GL_n(F)$ 通过左右乘法在 $M_n^r(F)$ 上传递作用 ,

$$(D, E) \cdot A = DAE^{-1}, \qquad \text{where} \qquad (D, E) \in GL_n(F) \times GL_n(F), \ A \in M_n^r(F).$$

换句话说，存在 $(D, E) \in GL_n(F) \times GL_n(F)$，使得

$$DB^{\top}E^{-1} = \begin{bmatrix} \mathbf{1}_r & 0 \\ 0 & 0 \end{bmatrix},$$

其中 $\mathbf{1}_r$ 是 $r \times r$ 单位矩阵。因此，对于如 (3.1) 中的 H，存在两个可逆矩阵 E 和 D，使得每个元素 $A \in H$ 都满足

$$\operatorname{tr}\left(EAD^{-1}\begin{bmatrix} \mathbf{1}_r & 0 \\ 0 & 0 \end{bmatrix}\right) = c.$$

这就完成了对我们断言的证明。 □

记号 3.3. 下文中，我们用 e_r表示秩为 r 的幂等矩阵 $\begin{bmatrix} \mathbf{1}_r & 0 \\ 0 & 0 \end{bmatrix}$。

由引理 1 可知，重要的不是矩阵 B 本身，而是它的秩。

引理 2. 设 H 是引理 1 假设中的 $M_n(F)$ 的一个超平面。那么存在一个超平面 $H_0 \subset M_n(F)$，使得 $\mathbf{0} \in H_0$ 和

$$|H \cap GL_n(F)| = |H_0 \cap GL_n(F)|.$$

证明. 我们沿用引理 1（证明）中的记号。由于映射 $A \mapsto EAD^{-1}$,$A \in GL_n(F)$ 是单射，我们可知

$$|GL_n(F) \cap H| = |\{X \in GL_n(F) : \operatorname{tr}(Xe_r) = c\}|.$$

接下来只需证明我们可以将标量 c 替换为 0。为此，我们将对 $GL_n(F)$ 应用一个仿射变换。

令 C 表示矩阵 $-ce_r$。映射 $\mathsf{s}_C\colon M_n(F) \to M_n(F)$ $Z \mapsto C + Z$ 是 $M_n(F)$ 的一个仿射变换。容易验证

$$|\{X \in GL_n(F) : \operatorname{tr}(Xe_r) = c\}| = |\{X \in GL_n(F) : \operatorname{tr}(\mathbf{s}_C(X)e_r) = 0\}|. \tag{3.4}$$

注意，s_C 是 $M_n(F)$ 的集合自同构。令 $GL_n(F)$ 表示 $GL_n(F)$ 在 s_C 下的像，

$$\widetilde{GL_n}(F) := \{C + X : X \in GL_n(F)\}.$$

容易验证乘积

$$\begin{aligned} \widetilde{GL_n}(F) \times \widetilde{GL_n}(F) &\longrightarrow \widetilde{GL_n}(F) \\ (C + X, C + Y) &\longmapsto C + XY \end{aligned}$$

使 $GL_n(F)$ 成为一个与 $GL_n(F)$ 同构的群。

Let

$$\varphi : \{X \in GL_n(F) : \ \mathrm{tr}\,(\mathbf{s}_C(X)e_r) = 0\} \longrightarrow \{\mathbf{s}_C(X) \in \widetilde{GL_n}(F) : \ \mathrm{tr}\,(\mathbf{s}_C(X)e_r) = 0\}$$
$$X \longmapsto \mathbf{s}_C(X).$$

由于 $\mathbf{s}_C(X)$ 是一个双射，我们可知 φ 是一个双射。因此，根据 (3.4)，我们证明了

$$|\{X \in GL_n(F) : \ \mathrm{tr}\,(Xe_r) = c\}| = \left|\{\mathbf{s}_C(X) \in \widetilde{GL_n}(F) : \ \mathrm{tr}\,(\mathbf{s}_C(X)e_r) = 0\}\right|. \tag{3.5}$$

令 H 表示超平面 $H = \{\mathbf{s}_C(Z) \in M_n(F) : \mathrm{tr}(\mathbf{s}_C(Z)e_r) = 0\}$。那么，式 (3.5) 的右端给出了交集 $GL_n(F) \cap H$ 的基数。换言之，我们证明了 $|GL_n(F) \cap H| = |GL_n(F) \cap H|$。由于 $\mathbf{0} \in H$，且由于 $GL_n(F) \cap H$ 是 $GL_n(F)$ 的一个超平面截面，我们的断言便得证。 □

命题 1。设 H 是 $GL_n(F)$ 的一个超平面截面。那么，无论 $\mathbf{0} \in H$ 是否成立，都存在 $r \in [n]$ 使得

$$|H| = \left|\left\{\begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} \in GL_n(F) : \ A_{11} \in M_r(F) \ and \ tr(A_{11}) = 0\right\}\right|.$$

证明。利用引理 2，我们得到存在 $r \in [n]$ 使得

$$|GL_n(F) \cap H| = |\{A \in GL_n(F) : \ \mathrm{tr}(Ae_r) = 0\}|.$$

将 A 按 $A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix}$ 中的分块形式写出，其中 $A_{11} \in M_r(F)$ 且 $A_{22} \in M_{n-r}(F)$，我们发现

$$|GL_n(F) \cap H| = \left|\left\{\begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} \in GL_n(F) : \ A_{11} \in M_r(F) \text{ and } \mathrm{tr}(A_{11}) = 0\right\}\right|.$$

至此，我们的断言得证。 □

4 主定理

现在我们可以证明主定理了。为方便起见，我们先回顾其陈述。

设 $F = \mathbb{F}_q$。令 C 表示通过在簇 $GL_n(F)$ 上对向量空间 $M_n(F)$ 的所有齐次线性多项式求值而得到的求值码。那么 C 的参数为

1. $\mathtt{n} = q^{\binom{n}{2}}(q-1)^n[n]_q!$,
2. $\mathtt{k} = n^2$,

3. $\mathtt{d} = q^{\binom{n}{2}-1}(q-1)^{n-1}\left((q-1)^2[n]_q! - [n-2]_q!\right)$.

证明。回顾一下，$\gamma(n,q)$ 表示基数，$|GL_n(F)| = q^{\binom{n}{2}}(q-1)^n[n]_q!$ 这给出了长度 $\mathtt{n}$。码的维数由 $M_n(F)$ 上齐次线性形式空间的维数给出。显然，这个数为 n^2。最后，为了求最小距离，我们使用命题 1 和 R. Stanley 的一个结果。在他的著作 [3,第 1 章习题 196 (a) 和 (b)], 中，Stanley 指出了以下事实。

对于 $k \in \{0,1,\ldots,n\}$，令 $f_k(n)$ 表示满足以下条件的矩阵 $A = (a_{ij}) \in GL_n(F)$ 的数量：

$$a_{11} + a_{22} + \cdots + a_{kk} = 0.$$

换言之，$f_k(n)$ 是交集 $GL_n(F)$ 与由方程 $a_{11}+a_{22}+\cdots+a_{kk}=0$ 定义的超平面 $H \subset M_n(F)$ 的 F-有理点的数量。于是，Stanley 公式为

$$f_k(n) = \frac{1}{q}\left(\gamma(n,q) + (-1)^k(q-1)q^{\frac{1}{2}k(2n-k-1)}\gamma(n-k,q)\right). \tag{4.1}$$

由于 q 和 n 是固定的，我们希望找到满足以下条件的 k_0：

$$f_{k_0}(n) = \max\{f_k(n) : k \in [n]\}. \tag{4.2}$$

我们断言 $k_0 = 2$。

我们将证明分为两部分。首先，我们将证明，对于来自 $\{2,3,\ldots\}$ 的每个 n 和 q，都有 $\frac{q}{q-1}(f_2(n) - f_1(n)) \geq 0$。然后，我们将证明，对于每个 $\{n,q\} \subset \{2,3,\ldots\}$，以及 $j \in \{3,\ldots,n\}$，都有 $\frac{q}{q-1}(f_2(n) - f_j(n)) \geq 0$。

在前一种情况下，我们有

$$\frac{q}{q-1}(f_2(n) - f_1(n)) = q^{2n-3}\gamma(n-2,q) + q^{n-1}\gamma(n-1,q). \tag{4.3}$$

显然，(4.3) 的右端是非负的。

在后一种情况下，我们有

$$\frac{q}{q-1}(f_2(n) - f_j(n)) = q^{2n-3}\gamma(n-2,q) + (-1)^j q^{\frac{1}{2}j(2n-j-1)}\gamma(n-j,q). \tag{4.4}$$

在 (4.4) 中，与前一种情况类似，如果 j 为偶数，则无需进行任何处理。我们假设 j 为奇数。令 $j = 2m+1$，其中某个 $m \in \{1,\ldots,\lfloor\frac{n}{2}\rfloor\}$。于是我们有

$$\frac{q}{q-1}(f_2(n) - f_j(n)) = q^{2n-3}\gamma(n-2,q) - q^{(2m+1)(n-m-1)}\gamma(n-2m-1,q). \tag{4.5}$$

由于 $\gamma(n,q) = q^{\binom{n}{2}}(q-1)^n[n]_q!$ 我们将 (4.5) 的右端识别如下：

$$q^{2n-3+\binom{n-2}{2}}(q-1)^{n-2}[n-2]_q! - q^{(2m+1)(n-m-1)+\binom{n-2m-1}{2}}(q-1)^{n-2m-1}[n-2m-1]_q!$$

由于我们有不等式 $(q-1)^{n-2m-1} \leq (q-1)^{n-2}$ 和 $[n-2m-1]_q! \leq [n-2]_q!$，我们的任务归结为比较项 $q^{2n-3+\binom{n-2}{2}}$ 和 $q^{(2m+1)(n-m-1)+\binom{n-2m-1}{2}}$。但通过直接计算即可证明

$$2n-3+\binom{n-2}{2}=\binom{n}{2} \text{ and } (2m+1)(n-m-1)+\binom{n-2m-1}{2}=\binom{n}{2}.$$

由此可知，(4.5) 中的不等式成立，因此 (4.4) 中的不等式也总是成立。这就完成了对断言 $k_0=2$ 的证明。令 $H_0 \subset M_n(F)$ 表示由 $\{(a_{ij}) \in M_n(F): \ a_{11}+a_{22}=0\}$ 定义的超平面。因此， H_0 的 F-有理点数由 $f_2(n)$ 给出。根据这一观察和命题 1，我们得到

$$\max_H |GL_n(F)\cap H| = |H_0|,$$

其中，最大值取遍 $M_n(F)$ 的所有超平面。

现在我们可以证明关于 $\mathtt{d}$ 的公式了：

$$\begin{aligned}\mathtt{d} &= \mathtt{n} - \max_H |GL_n(F)\cap H| \\ &= \mathtt{n} - f_2(n) \\ &= \left(1-\frac{1}{q}\right)\gamma(n,q) - \frac{1}{q}(q-1)q^{2n-3}\gamma(n-2,q) \\ &= q^{\binom{n}{2}-1}(q-1)^{n+1}[n]_q! - q^{\binom{n}{2}-1}(q-1)^{n-1}[n-2]_q!.\end{aligned}$$

通过将 $q^{\binom{n}{2}-1}(q-1)^{n-1}$ 提出，我们完成了定理的证明。 □

5 $B^- \times B$-稳定边界

本节的目标是证明， $GL_n(F)$ 中具有最少 F-有理点的超平面截面由 $GL_n(F)$ 的一个 $B^- \times B$稳定除子给出，其中 B 表示 $GL_n(F)$ 的一个 Borel 子群。为此，我们先介绍代数群论记号。本部分的基本参考文献是 Jantzen 的著作，尤其是 [1, 第二部分，§1.9]。

令 F 为一个域。令 G 为定义在 F上的一个（分裂）连通约化代数群。我们固定 G中的一个（分裂）极大环面 T，并固定 G 的一个 Borel 子群 B，使得 $T \subseteq B$。(G,T) 的 Weyl群记为 W。它由 $N_G(T)/T$ 给出，其中 $N_G(T)$ 是 G中 T的正规化子。对于 $w \in W$，我们用 $\dot{w}$表示 w在 $N_G(T)$ 中的一个代表元。 G 的 Bruhat分解是将 G 划分为 B的双陪集，具体如下：

$$G = \bigsqcup_{w\in W} B\dot{w}B. \tag{5.1}$$

于是，Weyl群 W 在双陪集的扎里斯基闭包上的包含序下成为一个偏序集：

$$v \leq w \iff B\dot{v}B \subseteq \overline{B\dot{w}B} \qquad (w, v \in W).$$

这个序称为 W 上的布鲁哈-谢瓦莱序。它是一个分次偏序集，其秩函数为：

$$\begin{aligned} \ell : W &\longrightarrow \mathbb{Z} \\ w &\longmapsto \dim B\dot{w}B - \dim B. \end{aligned}$$

元素 $w \in W$ 在 ℓ 下的值称为 w 的长度。存在唯一的最大长度元素 $w_0 \in W$。它具有以下优良性质：

- $\overline{B\dot{w}_0B} = G$,
- $w_0^2 = id$,
- $\dot{w}_0 B \dot{w}_0 \cap B = T$。

Borel 子群 $\dot{w}_0 B \dot{w}_0$，记作 B^-，称为 B 的对偶（相对于 W）。容易看出，Bruhat分解等价于以下分解：

$$G = \bigsqcup_{w \in W} B^- \dot{w} B. \tag{5.2}$$

现在我们聚焦于最重要的线性代数群，即 $G := GL_n(F)$。G 中的所有可逆上三角矩阵构成一个 Borel 子群。为简便起见，我们将其记为 B。G 中的可逆对角矩阵群记为 T。显然，T是包含于 B中的一个极大环面。(G, T) 的 Weyl群自然同构于对称群 S_n。 B的对向 Borel 子群记为 B^-，它是 G中下三角矩阵构成的 Borel 子群。于是，Bruhat分解 $G = \bigsqcup_{w \in W} B^- w B$ 无非就是可逆矩阵的 LPU分解，其中 L 表示下三角矩阵，P 表示置换，U 表示上三角矩阵。请注意，我们有意省略了记号中 w上方的点，因为对称群 S_n 实际上是 G的一个子群。

每个Weyl群都带有一组（不一定唯一的）考克斯特生成元系统。对于对称群 S_n ，一组考克斯特生成系由简单换位组成

$$S := \{s_i : \ i = 1, \ldots, n-1\}, \tag{5.3}$$

其中， $s_i (i \in \{1, \ldots, n-1\})$ 是 $\{1, \ldots, n\}$ 的置换，它交换 i 和 $i+1$，并保持其他所有元素不变。于是，元素 $w \in S_n$ 的长度 $\ell(w)$ 等于

表示 w 为这些简单换位之积所需的最少数量。由 Matsumoto交换条件 [2] 可知，对于每个 $s \in S$，我们有

$$\ell(w_0 s) = \ell(w_0) - 1 \qquad \text{and} \qquad w_0 s \leq w_0.$$

换言之，集合 $\overline{Bw_0sB}$ ($s \in S$) 是 $GL_n(F)$ 的一个余维一子簇。顺便指出，

$$\overline{Bw_0sB} = \overline{w_0 w_0 B w_0 s B} = w_0 \overline{B^- s B}. \tag{5.4}$$

由于 w_0 在 G 上传递作用，我们看到，对于每个 $s \in S$，都有 $\dim \overline{Bw_0sB} = \dim \overline{B^-sB}$。

引理3。令 H_0 表示超平面 $H_0 = \{(a_{ij})_{i,j=1,\ldots,n} \in M_n(F) : \ a_{11} = 0\}$。那么我们有

$$H_0 \cap GL_n(F) = \bigsqcup_{s \in S} \overline{B^- s B},$$

其中 S 表示 S_n 中所有简单换位的集合。

证明。根据其定义， H_0 由所有形如以下形式的 $n \times n$ 矩阵 $x \in M_n(F)$ 构成

$$x = \begin{bmatrix} 0 & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \cdots & a_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & a_{n3} & \cdots & a_{nn} \end{bmatrix}. \tag{5.5}$$

通过直接进行矩阵乘法，我们可得

$$b^- x b \in H_0 \qquad \text{for every} \qquad (b^-, b) \in B^- \times B, \ x \in H_0.$$

换言之， H_0 在 $B^- \times B$的双边作用下保持不变。同时，根据Bruhat分解， $GL_n(F)$在 $B^- \times B$ 的双边作用下也保持不变。因此，交集

$$\mathcal{D} := H_0 \cap GL_n(F)$$

是 $GL_n(F)$中的一个 $B^- \times B$稳定子集。由于 H_0 是 $M_n(F)$中的一个超平面， $\mathcal{D}$ 是 $GL_n(F)$中的一个超曲面。下面我们来分析其不可约分支。

设 $s \in S$。我们断言 $\overline{B^-sB}$ 包含于 $\mathcal{D}$。显然，要证明这一断言，只需证明 $B^-sB \subseteq \mathcal{D}$。设 b^- （分别为 b）是 B^- （分别是 B）中的一个元素。容易验证，若 $s = s_i$，其中 $i \in \{2, 3, \ldots, n-1\}$，则 $b^- s b \in \mathcal{D}$。接下来证明 $b^- s_1 b \in \mathcal{D}$。这里，不妨假设 $n = 2$。于是我们有

$$\begin{aligned} b^- s_1 b &= \begin{bmatrix} b'_{11} & 0 \\ b'_{21} & b'_{22} \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} b_{11} & b_{12} \\ 0 & b_{22} \end{bmatrix} \\ &= \begin{bmatrix} b'_{11} & 0 \\ b'_{21} & b'_{22} \end{bmatrix} \begin{bmatrix} 0 & b_{22} \\ b_{11} & b_{12} \end{bmatrix} \\ &= \begin{bmatrix} 0 & b'_{11} b_{22} \\ b_{11} b'_{21} & b'_{21} b_{22} + b'_{22} b_{12} \end{bmatrix}, \end{aligned}$$

这也是 $\mathcal{D}$ 的一个元素。总之，我们证明了

$$\bigsqcup_{s\in S}\overline{B^-sB}\subseteq\mathcal{D}.$$

由 (5.4) 可知， $\overline{B^-sB}$ 是 $GL_n(F)$ 中一个 $B^-\times B$ 稳定的素除子。事实上，根据Bruhat分解，我们知道 $GL_n(F)$ 中的每个 $B^-\times B$ 稳定素除子都是某个 $s\in S$ 的轨道闭包。由于 $\mathcal{D}$ 是 $B^-\times B$ 稳定的，且包含每个 $\overline{B^-sB}$，其中 $s\in S$，因此可知 $\mathcal{D}$ 由它们的并集给出。这就完成了我们断言的证明。 □

现在我们可以证明本文的第二个主要结果了。

定理 2 的证明。回顾定理1的证明， $GL_n(F)$ 与超平面 $H=\{A=(a_{ij})\in M_n(F):a_{11}+\cdots a_{kk}=0\}$ 的交集中的 F-有理点数为

$$f_k(n)=\frac{1}{q}\left(\gamma(n,q)+(-1)^k(q-1)q^{\frac{1}{2}k(2n-k-1)}\gamma(n-k,q)\right).$$

我们将 $f_k(n)$ 视为一个 $\mathbb{Z}$ 值函数。容易验证（沿用定理1证明中的思路），最小值 $_{k\in[n]}f_k(n)$ 在 $f_1(n)$ 处取得。引理3表明， $f_1(n)$ 是 $B^-\times B$ 稳定除子 $\bigsqcup_{s\in S}\overline{B^-sB}$ 上的 F-有理点数。但此除子恰好是“切瓦利的大胞腔” B^-B 的补集。这就完成了定理的证明。

□

6 最后说明

每个线性 $[\mathtt{n},\mathtt{k},\mathtt{d}]_q$ 码都满足 Singleton界，即不等式 $\mathtt{d}\le\mathtt{n}-\mathtt{k}+1$。同样，每个线性 $[\mathtt{n},\mathtt{k},\mathtt{d}]_q$ 码都满足 Griesmer界，即不等式 $\sum_{i=0}^{\mathtt{k}}\lceil\frac{\mathtt{d}}{q^i}\rceil\le\mathtt{n}$。我们将差值 $(\mathtt{n}-\mathtt{k}+1)-\mathtt{d}$ 和 $\mathtt{n}-\left(\sum_{i=0}^{\mathtt{k}}\lceil\frac{\mathtt{d}}{q^i}\rceil\right)$ 分别称为 Singleton缺陷和 Griesmer缺陷。MDS码是 Singleton缺陷为 0 的线性码。这类码备受青睐。 $GL_n(F)$-码远非 MDS码。对于 $n=2$，我们观察到以下事实，其证明显而易见。

命题2. 设 $F=\mathbb{F}_q$。令 C 表示这样一个求值码：将向量空间 $M_2(F)$中的所有齐次线性多项式在簇 $GL_2(F)$上求值而得到。则以下结论成立：

1. C 的Singleton缺陷为 q^3-q^2-3。
2. C 的Griesmer缺陷为 $q-1$。

在二元域上，我们有如下对应关系 $GL_n(\mathbb{F}_2)=SL_n(\mathbb{F}_2)$。因此，我们的所有结果都自动适用于 $SL_n(\mathbb{F}_2)$。对于非二元域 F，可以用类似的方法求得 $SL_n(F)$-码的参数。在即将发表的稿件中，我们将给出其他经典群的类似计算。

致谢

本研究部分由路易斯安那州摄政委员会的拨款资助（合同编号 LEQSF(2021-22)-ENH-DE-26）。

参考文献

[1] Jens Carsten Jantzen。《代数群表示》，数学调查与专著第107卷。美国数学学会，罗得岛州普罗维登斯，第二版，2003年。[2] Hideya Matsumoto。《广义魏尔群的生成元与关系》。巴黎科学院院刊，258:3419–3422，1964年。[3] Richard P. Stanley。《枚举组合学》。第1卷，剑桥高等数学研究第49卷。剑桥大学出版社，剑桥，第二版，2012年。[4] Michael Tsfasman、Serge Vlˇadut、和Dmitry Nogin。《代数几何码：基本概念》，数学调查与专著第139卷。美国数学学会，罗得岛州普罗维登斯，2007年。