arXiv:2303.01175v3 [math.AC] 5 Nov 2024

无标签感知的域论视角

HAO LIANG JINGYU LU MANOLISC. TSAKIRIS LIHONG ZHI *

摘要。无标签感知是求解线性方程组的问题，其中右端向量仅在一个置换意义下已知。本文研究与对称多项式及其在变量的线性投影下的像相关的有理函数域；由此，我们证明，对于具有一般数据的 n 维无标签感知问题，其解可作为一个由 n 个未知数构成的系统的唯一解得到，该系统包含 $n+1$ 个次数为 1、2、.....、$n+1$ 的多项式方程。除了带来新的理论见解外，这一进展也为扩展代数无标签感知算法提供了可能。

1. 引言。

1.1. 无标签感知。 在无标签感知[33, 34] 给定一个高而满秩的矩阵 $A^* \in \mathbb{R}^{m\times n}$ 以及一个向量 $y^* \in \mathbb{R}^m$，使得对于 π 坐标 $\mathbb{R}^m$ 线性方程组 $A^*x = \pi(y^*)$，存在一个解 ξ^*；问题在于，如何根据 ξ^* 和 A^* 求出 y^*。无标签感知的主要定理断言，当 A 为一般的且 $m \geq 2n$时，这个问题是定义良好的。这一结果已推广到置换以外的任意线性变换[29, 25], ，也从线性空间推广到线性空间的并 [25] 以及有界秩矩阵空间 [36, 37, 30]。

无标签感知是一个极具挑战性的计算问题，已知为 NP难 [23, 12], ；蛮力法 [8] 或全局最优方法只有在维数较小时才可行；简要介绍见 [24] 。尽管如此，无标签感知有着众多潜在应用，涵盖生物学 [1, 17] 和神经科学 [22] ，以及数字通信 [28], 、数据挖掘 [26, 27, 38] 和计算机视觉 [31, 15]。

1.2. 研究动机。本文关注无标签感知的代数方面[28, 32, 20], ，下面我们将对此作背景介绍。令

$$\mathbb{R}[y_1, \dots, y_m] =: \mathbb{R}[y], \ \mathbb{R}[x_1, \dots, x_n] =: \mathbb{R}[x]$$

分别为实数 $\mathbb{R}$上的、具有 m 个和 n 个变量的多项式环，并令

$$p_\ell = \sum_{i\in[m]} y_i^\ell \in \mathbb{R}[y]$$

为 y_i的 ℓ次幂和；在下文中，只要 t 是正整数， $[t]$ 就表示集合 $\{1, 2, \dots, t\}$。在[28] 中，人们观察到 ξ^* 是多项式

$$q_\ell = p_\ell(A^*x) - p_\ell(y^*) \in \mathbb{R}[x]$$

对于任意 $\ell \in \mathbb{N}$；此处及下文中， x是一个列向量，其元素为 x_1、.....、x_n。当 A^* 为一般的时，文献 [32] 证明，方系统

$$\mathscr{Q}_n : q_1(x) = \cdots = q_n(x) = 0$$

*所有作者均隶属于中国科学院数学与系统科学研究院数学机械化重点实验室，北京，100190，中国。电子邮件：lianghao2020@amss.ac.cn，lujingyu@amss.ac.cn，manolis@amss.ac.cn，lzhi@mmrc.iss.ac.cn。

是零维的，因此至多有 $n!$ 个解。研究者还提出了一种算法：通过现成求解器求出方多项式系统的所有根，依据适当的准则隔离出一个根，然后利用期望最大化过程对该根进行精化。该算法的一个突出特点是，其复杂度关于 m呈线性；此外，经验观察表明，该算法在低噪声水平下具有鲁棒性：当信噪比为=40dB、 $m = 1000$ 且 $n = 4$ 时，该算法在标准个人电脑上耗时 25 毫秒，便可得到相对于真实值相对误差为 0.4 % 的解。另一方面，该算法在 n方面不可扩展：随着 n 增大，甚至无法高效存储方多项式系统的 $n!$ 个解，更不用说求解该系统了；事实上，文献[32] 中只能报告 $n \leq 6$ 的结果。

1.3. 贡献。本文研究的对象是超定 d
含有 n 个未知数的 $n+1$ 多项式方程系统

$$\mathscr{Q}_{n+1} : q_1(x) = \cdots = q_{n+1}(x) = 0.$$

我们的主要结果如下：

THEOREM 1.1. 假设 $A^* \in \mathbb{R}^{m\times n}$ 和 $\xi^* \in \mathbb{R}^{n\times 1}$ 是一般的，令 π 为 $\mathbb{R}^{m\times 1}$ 的坐标的任意置换，并设 $y^* = \pi(A^*\xi^*) \in \mathbb{R}^{m\times 1}$。那么， ξ^* 是多项式系统 $\mathscr{Q}_{n+1}$ 的唯一复数解。

定理1.1 解决了无标签感知理论中的一个重要开放问题。事实上， $\mathscr{Q}_{n+1}$ 对于一般数据具有唯一解这一点，早已通过实验观察到，见 [28], ；而更一般的唯一恢复猜想则见 [20]（猜想 6）。然而，定理1.1 对于无标签感知算法也有重要意义：无论采用何种方法求得 $\mathscr{Q}_{n+1}$的一个根，定理1.1 都保证该根是 ξ^*；相比之下， [32] 中的算法依赖于筛选 n个解 $\mathscr{Q}_n$。事实上，在 [16], 中（本文部分内容为其提供了严格的理论基础），我们提出了一种算法，通过秩一矩矩阵补全求得 $\mathscr{Q}_{n+1}$ 的唯一解，并报告了令人鼓舞的结果。

定理 1.1 的证明依赖于对一个与多项式 p_ℓ 相关的特定有理函数域进行细致分析；该分析是在变量 x 经线性投影后进行的，本身也颇有趣（请注意，若不进行线性投影，那么对于给定的 ℓ 值，研究由 p_ℓ 生成的域，以及该域何时与 x 上的对称有理函数域相同，是文献中一个历史悠久且广为人知的话题，例如参见 [13, 21, 9, 7]）。设 $A = (a_{ij})$ 是一个由变量构成的 $m \times n$ 矩阵，使得所有 a_{ij} 和 x_j 在 $\mathbb{R}$ 上联合代数独立。记 $\mathscr{E} = \mathbb{R}(A, x)$ 为变量 A、 x 上系数属于 $\mathbb{R}$ 的有理函数域，并记 $\mathscr{F}_{n+1} = \mathbb{R}(A, p_1(Ax) \ldots, p_{n+1}(Ax))$ 为 $\mathscr{E}$ 的子域，它由变量 A、 $p_1(Ax) \ldots, p_{n+1}(Ax)$ 上系数属于 $\mathbb{R}$ 的有理函数构成。我们证明：

THEOREM 1.2. 有理函数域 $\mathscr{F}_{n+1}$ 与 $\mathscr{E}$ 相同。

1.4. 致谢。感谢 Aldo Conca 阅读稿件并提出宝贵意见，也感谢 Matteo Varbaro 提供文献线索。Manolis C. Tsakiris 获得国家重点研发计划（2023YFA1009402）的资助。Lihong Zhi 获得国家重点研发计划（2023YFA1009401）和国家自然科学基金委员会（12071467）的资助。

2. 域 $\mathscr{F}_m$。本节及下一节所述内容均与基域无关，唯一的要求是基域的特征为零；因此，我们在全文中固定这样一个域 k；我们将多项式环 $k[A]$ 的分式域记为 $k(A)$。我们固定在域 $k(A)$ 上的多项式环

$$S := k(A)[z_1, \ldots, z_m],\ T := k(A)[y_1, \ldots, y_m],\ R := k(A)[x_1, \ldots, x_n],$$

并定义 $k(A)$-代数同态 $S \xrightarrow{\varphi} T \xrightarrow{\psi} R$，其中 $\varphi(z_i) = p_i$ 和 $\psi(y_i) = \sum_{j\in[n]} a_{ij}x_j$ 对每个 $i \in [m]$均成立。令 $\mathfrak{p} = I_{n+1}(A|y)$ 为由 T 中的所有 $(n+1)$-子式生成的理想，其中 $m \times (n+1)$ 矩阵为 $[A|y]$；此处 y 是变量向量y_1、……、y_m。每个这样的 $(n+1)$-子式都是 T的线性形式，因此 $\mathfrak{p}$ 是 T 的素理想，其高度可见为 $m - n$。由于 ψ 是满射，$\mathfrak{p} = \ker(\psi)$且$R \cong T/\mathfrak{p}$。

令 $\mathfrak{q} = S \cap \mathfrak{p}$ 为 $\mathfrak{p}$ 在 φ 下收缩到 S 的理想；这是 S 的一个素理想，其剩余域 $S_\mathfrak{q}/\mathfrak{q}S_\mathfrak{q}$ 记为 $\kappa(\mathfrak{q})$。我们有整环 $S/\mathfrak{q} \hookrightarrow T/\mathfrak{p} \cong R = k(A)[x]$ 的包含关系，该关系将 $S/\mathfrak{q}$ 识别为 $k(A)$- 子代数 $k(A)[p_1(Ax)\ \cdots, p_m(Ax)]$ of R；我们将该子代数的分式域记为 $\mathscr{F}_m$。进而，这诱导出分式域的包含关系 $\kappa(\mathfrak{q}) \cong \mathscr{F}_m \subseteq \mathscr{E} \cong \kappa(\mathfrak{p})$，其中我们回顾一下，$\mathscr{E}$ 是多项式环 $k(A)[x]$ 的分式域，而$\kappa(\mathfrak{p}) = T_\mathfrak{p}/\mathfrak{p}T_\mathfrak{p}$。本节的主要结果是:

PROPOSITION 2.1. *We have an equality of fields $\mathscr{F}_m = \mathscr{E}$.*

为了证明命题2.1，我们先从一个基本但重要的事实入手。

LEMMA 2.2. T 是秩为 $m!$ 的自由 S-模。

证明。根据牛顿恒等式，T中的子代数 $\varphi(S) = k(A)[p_1, \ldots, p_m]$与由变量 y上的 m 初等对称函数 $s_1, \ldots, s_m$ 生成的子代数 $k(A)[s_1, \ldots, s_m]$ 相同；因此，只需证明 T是秩为 $m!$ 的 $k(A)[s_1, \ldots, s_m]$ 上的自由模。

考虑多项式环

$$P = k(A)[y, w] = k(A)[y_1, \ldots, y_m, w_1, \ldots, w_m]$$

其维数为 $2m$，以及由所有 $w_i - s_i(y)$（其中 $i \in [m]$）生成的 P 的理想 J，其中 $s_i(y)$是变量 y上的第 i 个初等对称函数。对于满足 $y_1 > \cdots > y_m > w_1 > \cdots > w_m$ 的 P上的任意单项式序，《代数》第 7 章命题 5 明确给出了 J的一个 Gr¨obner 基，它由 m个多项式 $g_1, \ldots, g_m \in P$组成，且 g_i的首项为 y_i^i。由此立即可得，P/J的 $k(A)$-向量空间基由所有形如 $y_2^{\ell_2} \cdots y_m^{\ell_m} w_1^{b_1} \cdots w_m^{b_m}$ 的单项式构成，其中 b_i's 取遍非负整数，且 $0 \le \ell_i < i$。

现在考虑由 $\theta(w_i) = s_i(y)$ 以及对每个 $i \in [m]$ 都有 $\theta(y_i) = y_i$ 所定义的 $k(A)$-代数满同态 θ：$P = k(A)[y, w] \to T = k(A)[y]$。我们有 $J = \ker(\theta)$，因此 $T = P/J$；由于 P/J 在 $k(A)$ 上由上述 $m!$ 单项式 $y_2^{\ell_2} \cdots y_m^{\ell_m}$ 以及

$$w\ \ T \qquad\qquad k\ A\ [s_1\ y\ \ \ldots\ \ s_m\ y\ ] \cong \text{中的所有单项式生成},$$

$k\ A$

所以它更可在 $(\,)(\,),(\,)(\,)[w_1, \ldots, w_m]$ 上由这些 $y_2^{\ell_2} \cdots y_m^{\ell_m}$ 生成。为证明这些单项式是自由生成元，假设存在一个关系

$$\sum_{0\le\ell_i<i} c_{\ell_2\ \ldots\ \ell_m}\ y\ y_2^{\ell_2} \cdots y_m^{\ell_m} = 0 \qquad T \qquad c_{\ell_2\ \ldots\ \ell_m}\ y\ \in, , ( )$$

$$k\ A\ [s_1\ y\ \ \ldots\ \ s_m\ y\ ] \qquad c_{\ell_2\ \ldots\ \ell_m}\ y\ = f_{\ell_2\ \ldots\ \ell_m}\ s_1\ y\ \ \ldots\ \ s_m\ y \qquad f_{\ell_2\ \ldots\ \ell_m}$$

in , with , , ( ) ( ) ( ) , ( ) 。写作 , , ( ) , , (( ) , ( )), 其中 , , 是一个关于 m 个变量、系数属于 $k(A)$ 的多项式。注意 $\theta(f_{\ell_2,\ldots,\ell_m}(w)) = c_{\ell_2,\ldots,\ell_m}(y)$，从而 $\sum_{0\le\ell_i<i} f_{\ell_2,\ldots,\ell_m}(w) y_2^{\ell_2} \cdots y_m^{\ell_m} \in \ker(\theta)$。由于 $J = \ker(\theta)$ 且

g_i 们构成 J 的 Gr¨obner 基，$\sum_{0\le \ell_i<i} f_{\ell_2,\ \ldots \ell_m}(w) y_2^{\ell_2}\cdots y_m^{\ell_m}$ 的首项必定能被某个 $i\in[m]$ 的 y_i^i 整除；然而，从 $\sum_{0\le \ell_i<i} f_{\ell_2,\ \ldots \ell_m}(w) y_2^{\ell_2}\cdots y_m^{\ell_m}$ 的形式可知，这是不可能的，除非它是零多项式。由于 y 中的所有单项式作为 $k(A)[w]$ 上的模自由生成 $k(A)[y,w]$，进而可得所有 $f_{\ell_2,\ \ldots \ell_m}(w)$ 都为零，因此所有 $c_{\ell_2,\ \ldots \ell_m}(y)$ 也都为零。

□

注 2.3. T 是自由的 S-模，这一事实是著名的谢泼德-托德-切瓦利定理的一个特例。

引理2.2 说明 T 是 $\varphi(S)$ 的整元；这体现了一个一般事实：

Lemma 2.4（习题 12 和 13，第 5, [2] 章）。设 R 是交换环，Π 是作用于 R 上的有限群；记 R^Π 为 R 的子环，它由 R 中关于 Π 的作用的不变元素组成。那么，环扩张$R^\Pi\subseteq R$ 是整的；对于 R 的任意素理想 $\mathfrak{p}$，R 中位于$\mathfrak{p}\cap R^\Pi$ 之上的素理想是 $\mathfrak{p}$ 在 Π 作用下的轨道 $\{\pi(\mathfrak{p}):\ \pi\in\Pi\}$。

我们有：

Lemma 2.5. T 中位于 $\mathfrak{q}=S\cap\mathfrak{p}$ 之上的素理想恰好具有 $\pi(\mathfrak{p})$ 的形式，其中 π 是变量 $y_1,\ \ldots,\ y_m$ 的一个置换；这些是 $m!$ 个互不相同的素理想。

证明。 的素理想 T 位于 $\mathfrak{q}$ 当且仅当它具有以下形式 $\pi(\mathfrak{p})$，这由引理 2.4 得出。我们证明所有 $m!$ 个这样的素理想 $\pi(\mathfrak{p})$ 彼此不同。为此，只需证明当 $\pi(\mathfrak{p})\neq\mathfrak{p}$ 成立，而 π 不是恒等置换时即可；不失一般性，可假设 $\sigma(\mathcal{J})\neq\mathcal{J}$对于 $\mathcal{J}=\{m-n+1,\ldots,m\}$成立，且 $\sigma=\pi^{-1}$。

对于 i_1、……、i_n、i_{n+1} 这些 m 中互不相同的元素，我们用 $A_{i_1,\ldots,i_n}$ 表示一个 $n\times n$ 矩阵的行列式，其中第 s 行是 A 的第 i_s 行；用 $A_{i_1,\ldots,\hat{i}_s,\ldots,i_{n+1}}$ 表示与上述行 i_1、……、i_{s-1}、i_{s+1}、……、i_{n+1} 对应的行列式。采用这一记号，对于 T 上任意满足 $y_1>y_2>\cdots>y_m$ 的单项式序，T 的线性形式为

$$\ell_i:=y_i+\sum_{s\in\mathcal{J}}(-1)^{s-m+n+1}\frac{\det(A_{i,m-n+1,\ldots,\hat{s},\ldots,m})}{\det(A_{m-n+1,\ldots,m})}y_s,\ \ i\in[m-n]$$

是 $\mathfrak{p}$的约化 Gr¨obner 基。类似地，对于 $i\in[m-n]$，这些线性形式

$$\mu_i:=y_i+\sum_{s\in\sigma(\mathcal{J})}(-1)^{s-m+n+1}\frac{\det(A_{\sigma(i),\sigma(m-n+1),\ldots,\hat{s},\ldots,\sigma(m)})}{\det(A_{\sigma(m-n+1),\ldots,\sigma(m)})}y_s$$

是 $\pi(\mathfrak{p})$ 的约化 Gr¨obner 基。由于约化 Gr¨obner 基是唯一的，若$\mathfrak{p}=\pi(\mathfrak{p})$，则必有 $\ell_i=\mu_i$ 对每个 $i\in[m-n]$都成立。特别地，对于任意 $i\in[m-n]$和任意 $s\in\mathcal{J}$，ℓ_i中 y_s 的系数必须等于 μ_i 中 y_s 的系数。

根据我们的假设 $\sigma(\mathcal{J})\neq\mathcal{J}$，存在 $s\in\mathcal{J}\setminus\sigma(\mathcal{J})$ 和 $i\in\sigma(\mathcal{J})\setminus\mathcal{J}\subseteq[m-n]$。$\ell_i$ 中 y_s 的系数为 $(-1)^{s-m+n+1}\det(A_{i,m-n+1,\ldots,\hat{s},\ldots,m})/\det(A_{m-n+1,\ldots,m})$。另一方面，由于 $i\in[m-n]$ 且 $s\neq i$，并且 $s\notin\sigma(\mathcal{J})$，$\mu_i$ 中 y_s 的系数为零。

□

命题 2.1 是以下关于 $\mathfrak{P}=\mathfrak{p}$的结果的一个特例：

Lemma 2.6. 设 $\mathfrak{P}$ 是 T 中位于 $\mathfrak{q}$之上的素理想。那么 $\kappa(\mathfrak{P})=\kappa(\mathfrak{q})$。

证明。根据引理 2.2， T 是秩为 $m!$ 的自由 S-模，因此 $T \otimes_S \kappa(\mathfrak{q})$ 是维数为 $m!$ 的 $\kappa(\mathfrak{q})$-向量空间。由于 $T \otimes_S \kappa(\mathfrak{q})$ 是有限生成的 $\kappa(q)$-代数，同时也是有限维的 $\kappa(\mathfrak{q})$-向量空间，所以它必定是一个阿廷环。 $T \otimes_S \kappa(\mathfrak{q})$ 的素理想与位于 $\mathfrak{q}$ 之上的 T 的素理想相对应。根据引理 2.5，这些是 $m!$ 个互不相同的素理想 $\pi(\mathfrak{p})$，其中 π 遍历变量 y_1、.....、 y_m 的所有排列。一般而言，阿廷环同构于其在各个素理想处的局部化之积，因此

$$T \otimes_S \kappa(\mathfrak{q}) = \prod_{\pi} T_{\pi(\mathfrak{p})} \otimes_S \kappa(\mathfrak{q}).$$

现在，每个 $T_{\pi(\mathfrak{p})} \otimes_S \kappa(\mathfrak{q}) = T_{\pi(\mathfrak{p})}/\mathfrak{q}T_{\pi(\mathfrak{p})}$ 都是一个阿廷局部环和一个有限的 $\kappa(\mathfrak{q})$-向量空间。由于 $T_{\pi(\mathfrak{p})} \otimes_S \kappa(\mathfrak{q})$ 是一个维数为 $m!$- 的 $\kappa(\mathfrak{q})$-向量空间，且乘积中有 $m!$ 个因子，因此对于每个 π，每个 $T_{\pi(\mathfrak{p})} \otimes_S \kappa(\mathfrak{q})$ 都必定是一个一维$\kappa(\mathfrak{q})$-向量空间。但 $\kappa(\mathfrak{q})$ 包含于每个 $T_{\pi(\mathfrak{p})} \otimes_S \kappa(\mathfrak{q})$ 中，因此对于每个 π，$T_{\pi(\mathfrak{p})} \otimes_S \kappa(\mathfrak{q}) = \kappa(\mathfrak{q})$。由于 $T_{\pi(\mathfrak{p})}/\mathfrak{q}T_{\pi(\mathfrak{p})}$ 是一个域，因此必有 $\mathfrak{q}T_{\pi(\mathfrak{p})} = \pi(\mathfrak{p})T_{\pi(\mathfrak{p})}$， 从而 $T_{\pi(\mathfrak{p})}/\mathfrak{q}T_{\pi(\mathfrak{p})} = T_{\pi(\mathfrak{p})}/\pi(\mathfrak{p})T_{\pi(\mathfrak{p})} = \kappa(\pi(\mathfrak{p}))$。□

3. 域扩张 $\mathscr{F}_n \subseteq \mathscr{F}_m$。 我们记 $\mathscr{F}_n$ 有理函数域 $k(A)(p_1(Ax)\ldots, p_n(Ax))$; 这是 $\mathscr{E} = k(A, x)$ 的一个子域，后者根据命题 $\mathscr{F}_m$ 2.1 与 一致。本节的主要结果是:

PROPOSITION 3.1. 域扩张 $\mathscr{F}_n \subset \mathscr{F}_m$ 是次数为 $[\mathscr{F}_m$ 的代数扩张: $\mathscr{F}_n] = n!$ 。

为了证明命题 3.1，我们先证明一个基本事实:

LEMMA 3.2. 多项式 $p_1(Ax) \ldots, p_n(Ax)$ 是 $R = k(A)[x]$ 的正则序列。

证明。对于域上的多项式环 P 中的齐次理想 J，由塞尔定理关于希尔伯特函数的结论 [4, 定理 4.4.3] 可知， P/J 的希尔伯特多项式在次数大于或等于 J 的 Castelnuovo-Mumford（CM）正则性时，与 P/J 的希尔伯特函数一致。通过 Koszul 复形可以看出，由 n 个次数分别为 1、2、3、. . .、 n 的元素组成的正则序列生成的理想 J 的 CM-正则性为 $\mathrm{reg}(J) = n(n-1)/2 + 1$。

现在令 J为由 $p_1(Ax) \ldots, p_n(Ax)$ 生成的 R的理想。那么，序列$p_1(Ax) \ldots, p_n(Ax)$ 是正则的，当且仅当 R/J的克鲁尔维数为零；当且仅当 R/J 的希尔伯特多项式是零多项式；当且仅当 $[J]_a = [\mathfrak{m}]_a$；这里 $a = \mathrm{reg}(J) = n(n-1)/2 + 1$， $[J]_a$ 表示 J的 a 次齐次部分，而 $\mathfrak{m}$ 是由 $x_1, \ldots, x_n$生成的 R的理想。

令 t 为 $[\mathfrak{m}]_a$ 作为 $k(A)$-向量空间的维数。通过将每个 $p_i(Ax)$ 乘以所有次数为 $a - i$ 的单项式，取 $[J]_a$ 的生成元。构造矩阵 H，其列包含 $[J]_a$ 的生成元在由所有次数为 a的单项式构成的 $[\mathfrak{m}]_a$ 基下的系数。当且仅当 H 的所有 $t \times t$ 子式不全为零时， $p_i(Ax)$ 构成正则序列。但若它们全为零，那么对任意 $A^* \in k^{m\times n}$，将 A 替换为 A^* 后，它们仍全为零；此处 k 表示 k 的代数闭包。然而，这与以下事实矛盾：根据 [32] 中的引理 4，对于 $A^* \in k^{m\times n}$ 的一般选择， $p_i(A^*x)$ 构成正则序列¯; 这里我们用到了这样的事实：当 $p_i(A^*x)$ 构成 $k[x]$ 的正则序列时，它们生成的理想 ¯ 的 CM- 正则性仍为 a，而 $k[x]$ 的次数为 a 的分次分量的 k- 向量空间维数仍等于 t；因此，当且仅当 $H|_{A^*}$ 的所有 $t \times t$ 子式不全为零时， $p_i(A^*x)$ 构成正则序列，其中 $H|_{A^*}$ 是将 H 中的 A 替换为 A^* 后得到的。

□

我们的下一个要素同样至关重要，而且本身也很有趣。

LEMMA 3.3. $R = k(A)[x]$ 是一个秩为 n 的自由 $k(A)[p_1(Ax) .. . , p_n(Ax)]$-模。

证明。我们首先证明 R 在 $R_n = k(A)[p_1(Ax) \dots , p_n(Ax)]$ 上是平坦的。一般而言，从 R_n 到 R 的包含映射是正分次环的同态，它将 R_n 的极大齐次理想映入 R 的极大齐次理想 $\mathfrak{m}$ 。根据 [19] 第 178 页备注的第 (3) 部分， R 在 R_n 上平坦，当且仅当 $R_{\mathfrak{m}}$ 在 R_n 上平坦。现在，根据引理 3.2 $p_1(Ax) \dots , p_n(Ax)$ 是 R 的正则序列；因此，它在 $R_{\mathfrak{m}}$ 中仍然是正则序列。因此，[11] 中的定理 1 表明 $R_{\mathfrak{m}}$ 在 R_n 上平坦；由此我们得出 R 在 R_n 上平坦。

接下来，我们论证 R 在 R_n上是有限生成的。令 J 为由 $p_i(Ax)\ \ i \in [n]$生成的 R 的理想，根据引理 3.2，它是一个正则序列。由此可知， R/J是阿廷的，并且作为 $k(A)$-向量空间的维数为 $n!$ ；对于后一个结论，我们使用了 R 关于由齐次元素组成的正则序列所得商环的希尔伯特级数的已知形式。令 $\mathcal{B}$ 为 R/J的一个 $k(A)$-向量空间基。若 $f \in R$ 是次数为 d的齐次多项式，则可写成 $f = \sum_{b\in\mathcal{B}} c_b\, b + f_1$，其中 $c_b \in k(A)$，而 f_1是 J 中次数为 d的齐次多项式。写作 $f_1 = \sum_{i\in[n]} g_i p_i(Ax)$，其中$g_i$ 是次数为 $d - i$的齐次多项式，我们有 $f = \sum_{b\in\mathcal{B}} c_b\, b + \sum_{i\in[n]} g_i p_i(Ax)$。将每个 g_i 写成 $k(A)$-线性组合（以 b's 为基）与 J中次数为 $d - i$ 的齐次多项式之和，归纳可知， R 由 $\mathcal{B}$在 R_n 上有限生成。

现在我们论证， R 是 R_n 上的有限秩自由模。由于 R 是有限生成的R_n-模，且 R_n 是多项式环，因此 R 在 R_n上有限表示；又因为 R 在 R_n上平坦，根据 [19] 第 53 页的推论可知， R 在R_n上是射影模。现在， R 是多项式环 R_n上的有限生成分次模，因此根据 [4] 中的定理 1.5.15(d)，它在 R_n 上是射影模，当且仅当它在 R_n上是自由模；由此得出， R 是有限秩的分次自由 R_n-模。

最后，我们论证 R 作为 R_n 上的自由模，其秩为 $n!$ 设 $\mathcal{U}$是 R 在 R_n上的齐次自由生成元；显然， $\mathcal{U}$ 张成 R/J这个 $k(A)$-向量空间。我们来证明 $\mathcal{U}$ 在 R/J中关于 $k(A)$ 线性无关。设对于 $c_u \in k(A)$，有$\sum_{u\in\mathcal{U}} c_u\, u \in J$ 。由于 J 是齐次理想，我们可以假设求和中所有满足 $c_u \neq 0$ 的 u都具有相同的次数 d。于是，对某个次数为 $d - i$的齐次 $f_i \in R$，有$\sum_{u\in\mathcal{U}} c_u\, u + \sum_{i\in[n]} f_i p_i(Ax) = 0$ 。由于$\mathcal{U}$ 生成了 R （作为 R_n-模），存在如下表达式：$f_i = \sum_{u\in\mathcal{U}} \rho_{i,u}\, u$，其中$\rho_{i,u} \in R_n$。代入后，得到一个关系

$$\sum_{u\in\mathcal{U}} \left(c_u + \sum_{i\in[n]} \rho_{i,u} p_i(Ax) \right) u = 0.$$

由于 u 在 R_n 上是自由的，我们必有 $c_u + \sum_{i\in[n]} \rho_{i,\ u} p_i(Ax) = 0$。左边是 R_n 中的一个多项式，其常数项为 c_u；由此可知 $c_u = 0$。 ∎

注记 3.4。引理 3.3 的证明可直接推广到任意正则序列h_1、.....、 h_n，其中 R由次数分别为 d_1、.....、 d_n的齐次元素组成；这表明 R是一个自由的 k（A）$[h_1, \dots , h_n]$-模，其秩为 $d_1 \cdots d_n$。

现在我们可以证明命题3.1。

证明。（命题 3.1）为方便起见，我们设 $R_n = k(A)[p_1(Ax) \dots , p_n(Ax)]$。我们有整环 $R_n \subset R$ 的一个包含关系，其分式域分别记为 $K(R_n)$ 和 $K(R)$。现在， $K(R_n)$ 只是 R_n 的一个局部化，因此它在 R_n 上是平坦的。于是我们有环的包含关系 $K(R_n) \subset R \otimes_{R_n} K(R_n) \subset K(R)$。由

引理 3.3， R 是一个有限生成的 R_n-模，因此环扩张 $R_n \subset R$ 是整的。由此可知，环扩张 $K(R_n) \subset R \otimes_{R_n} K(R_n)$ 也是整的；两个环的克鲁尔维数必定相等，因此 $R \otimes_{R_n} K(R_n)$ 是阿廷的，因为 $K(R_n)$ 是一个域。一般而言，包含在整环中的阿廷环必定是域；因此 $R \otimes_{R_n} K(R_n)$ 是一个域。这个域包含 R，并且由于它包含于 $K(R)$，必有 $R \otimes_{R_n} K(R_n) = K(R)$。由于根据引理 3.3， R 是一个秩为 $n!$ 的自由 R_n-模，因此 $K(R)$ 是一个 $K(R_n)$-向量空间，其维数为 $n!$。最后，回顾一下，域 $K(R_n)$ 和 $K(R)$ 分别就是域 $\mathscr{F}_n$ 和 $\mathscr{F}_m$。 □

4. 域扩张 $\mathscr{F}_{n+1} \subseteq \mathscr{F}_m$。在本节中，我们将证明域 $\mathscr{F}_{n+1} = k(A)(p_1(Ax)\dots, p_{n+1}(Ax))$ 与域 $\mathscr{F}_m = \mathscr{E}$ 相同；定理1.2 将作为 $k = \mathbb{R}$ 的特例得出。

我们有域 $\mathscr{F}_n \subseteq \mathscr{F}_{n+1} \subseteq \mathscr{F}_m$。由命题 3.1，域扩张 $\mathscr{F}_n \subset \mathscr{F}_m$ 的次数为 $n!$；因此，要证明 $\mathscr{F}_{n+1} = \mathscr{F}_m$ ，只需证明域扩张 $\mathscr{F}_n \subseteq \mathscr{F}_{n+1}$ 的次数为 $n!$ 。注意， $\mathscr{F}_{n+1}$ 正是由 $p_{n+1}(Ax)$ 在 $\mathscr{F}_n$ 上生成的域 $\mathscr{F}_n(p_{n+1}(Ax))$；因此，只需证明 $p_{n+1}(Ax)$ 在 $\mathscr{F}_n$ 上的最小多项式 $\mu_{n+1} \in \mathscr{F}_n[t]$ 的次数为 $n!$ 。我们将通过使用多维结式 [18, 35, 10, 14]，来证明这一点。为方便读者，我们现在按照 [18] 简要回顾一下这些结式。

对于正整数 a 和特征零域 $\mathscr{K}$，设 $l_1, \dots, l_a$ 为正整数，并用 $\mathcal{M}(t, l_i)$ 表示变量 $t = t_1, \dots, t_a$ 中所有次数为 l_i 的单项式组成的集合。对于每个 $i \in [a]$ 以及每个单项式 $w \in \mathcal{M}(t, l_i)$，我们考虑一个变量 $c(i, w)$，并定义 $f_i = \sum_{w \in \mathcal{M}(t,l_i)} c(i, w)\, w$；这可以视为变量 t 上的一个次数为 l_i、系数属于多项式环 $C = \mathscr{K}[c(i, w)$ 的齐次多项式： $w \in \mathcal{M}(t, l_i)$ $i \in [a]]$。令 $l = l_1 + \cdots + l_a - a + 1$，并设 H 为一个元素属于环 C 的矩阵，定义如下：固定 $w \in \mathcal{M}(t, l - l_i)$ 和 $i \in [m]$ 后，考虑由 wf_i 关于 $\mathcal{M}(t, l)$ 展开所得的系数在 C 中的列向量；然后， H 的列由所有此类向量构成，其中 i 和 w 分别遍历 $[a]$ 和 $\mathcal{M}(t, l - l_i)$。Macaulay 将 $\mathcal{R}(f_1, \dots, f_a)$ 的结式定义为 H 的所有极大子式的最大公因式；他证明了该结式具有以下我们将用到的性质：

Proposition 4.1（[18], §6—§10，第一章）。令 $L = l_1 \cdots l_a$ 和 $L_i = L/l_i$。则

1. 对于 $i \in [a]$， $c(i, t_i^{l_i})$ 在 $\mathcal{R}(f_1, .., f_a)$ 中的次数为 L_i，而 $c(a, t_a^{l_a})^{L_a}$ 的系数为 $\mathcal{R}(\bar{f}_1, \dots, \bar{f}_{a-1})^{l_a}$，其中 $\bar{f}_i = f_i|_{t_a=0}$。 2. 对于任意 $i \in [a]$，都有 $\mathcal{R}(f_1, .., f_a)$ 关于变量 $(c(i, w))_{w \in \mathcal{M}(t,l_i)}$ 是次数为 L_i 的齐次式。3. 令 $f_1^*, \dots, f_a^* \in \mathscr{K}[t] = \mathscr{K}[t_1, \dots, t_a]$ 为 $f_1, \dots, f_a$ 的任意特化，即将每个 $c(i, w)$ 替换为 $\mathscr{K}$ 中的一个元素，并令 $\mathcal{R}(f_1^*, \dots, f_a^*)$ 为 $\mathcal{R}(f_1, \dots, f_a)$ 的相应特化。则当且仅当 $f_1^*, \dots, f_a^*$ 除零以外在 $\mathscr{K}^a$ 中有一个公共根时， $\mathcal{R}(f_1^*, \dots, f_a^*) = 0$；其中 $\mathscr{K}$ 是 $\mathscr{K}$ 的代数闭包。

注记 4.2. 一个基本观察是，在维数为 n 、基于 n 的多项式环中， $\mathscr{K}$一组齐次多项式构成正则序列，当且仅当它们生成的理想是极大齐次理想的原初理想；这等价于¯这些多项式在 $\mathscr{K}^n$ 中除零点外没有公共根。事实上，矩阵 H 在引理 3.2 的证明中出现的，恰好是与结式相关联的 Macaulay 矩阵 $p_1(Ax)\dots, p_n(Ax)$。

现在我们回到目标，即证明 μ_{n+1} 在$p_{n+1}(Ax)$上的最小多项式在 $\mathscr{F}_n$ 上次数为 $n!$。我们将上述表述应用于 $a = n+1$，令 t 为分量是 $t_1, \ldots, t_n$的列向量，并引入新变量$r_1, \ldots, r_{n+1}$。对于 $i \in [n+1]$，我们定义 $f_i^* = p_i(At) - r_i t_{n+1}^i$；这是一个关于变量 $t_1, \ldots, t_{n+1}$的 i 次齐次多项式，其系数属于多项式环 $k(A)[r] := k(A)[r_1, \ldots, r_{n+1}]$。我们将 $\mathcal{R}(f_1^*, \ldots, f_{n+1}^*) \in k(A)[r]$记作命题 4.1 的结式 $\mathcal{R}(f_1, \ldots, f_m)$ 的特化，其中变量 $c(i,w)$ 被替换为 w 在 f_i^*中的对应系数。类似地，将上述表述应用于 $a = n$，我们令 $\mathcal{R}(p_1(At) \ldots, p_n(At))$ 为 $\mathcal{R}(f_1, \ldots, f_n)$ 的特化，其中变量 $c(i,w)$ 被替换为 w 在 $p_i(At)$中的对应系数。明确指出$\mathcal{R}(f_1^*, \ldots, f_{n+1}^*) \in k(A)[r]$对变量 A和 $r = r_1, \ldots, r_{n+1}$的依赖将很有用；为此，我们记作 $\rho(A, r_1, \ldots, r_{n+1}) := \mathcal{R}(f_1^*, \ldots, f_{n+1}^*)$。接下来，我们将进行一系列关键观察。

LEMMA 4.3. $\rho(A, r_1, \ldots, r_{n+1}) \in k(A)[r]$ 是关于变量 r_{n+1} 的非零 n 次多项式！此外， $r_{n+1}^{n!}$ 的系数为 $\mathcal{R}(p_1(Ax) \ldots, p_n(Ax))^{n+1}$。

证明。根据引理 3.2 $p_1(Ax) \ldots, p_n(Ax)$ 是一个正则序列，其长度为 $R = k(A)[x]$。命题 4.1 的第（3）部分以及备注 4.2 表明 $\mathcal{R}(p_1(Ax) \ldots, p_n(Ax))$ 是 $k(A)$ 中的非零元素。由命题 4.1的第（1）部分即可得出结论，因为结式与特化可交换。 □

LEMMA 4.4. 我们有 $\rho(A, p_1(Ax) \ldots, p_{n+1}(Ax)) = 0$。

证明。 将 r_i 替换为 $p_i(Ax)$，代入多项式 f_i^*对每个 $i \in [n+1]$，显然点 $(x_1, \ldots, x_n, 1) \in \mathscr{E}^{n+1}$ 是一个公共根；因此，根据命题4.1的第 (4) 部分，这些多项式的结式为零。 □

LEMMA 4.5. 我们有 $\rho(A, p_1(Ax) \ldots, p_n(Ax)\ r_{n+1}) \neq 0$。

证明。 这可由引理 4.3立即得出。 □

注 4.6. 由引理 3.2， 多项式 $p_1(Ax) \ldots, p_n(Ax)$ 是 $k(A)[x]$ 的正则序列，因此它们在 $k(A)$ 上代数独立。于是，多项式 $p_1(Ax) \ldots, p_n(Ax)\ r_{n+1}$ 在 $k(A)$ 上代数独立。因此，$\rho(A, p_1(Ax) \ldots, p_n(Ax)\ r_{n+1})$ 在 $k(A)[p_1(Ax) \ldots, p_n(Ax)\ r_{n+1}]$ 中不可约，当且仅当 $\rho(A, r_1, \ldots, r_{n+1})$ 在 $k(A)[r_1, \ldots, r_{n+1}]$ 中不可约。

我们将证明 $\rho(A, r_1, \ldots, r_{n+1})$ 在 $k[A, r_1, \ldots, r_{n+1}]$ 中不可约。我们首先证明特殊情形 $m = n+1$，其中集中了所有难点。

LEMMA 4.7. 假设 $m = n+1$，那么 $\rho(A, r_1, \ldots, r_{n+1})$ 作为关于 $k[A, r_1, \ldots, r_{n+1}]$ 的多项式是不可约的。

证明。当 $m = n+1$ 时，我们有 $\mathscr{F}_m = \mathscr{F}_{n+1}$，且由命题 3.1 可知，域扩张 $\mathscr{F}_n \subseteq \mathscr{F}_{n+1}$ 的次数为 $n!$。由于 $\mathscr{F}_{n+1} = \mathscr{F}_n(p_{n+1}(Ax))$，因此 $p_{n+1}(Ax)$ 在 $\mathscr{F}_n$ 上的最小多项式 μ_{n+1} 的次数为 $n!$。另一方面，由引理 4.5 可知，多项式 $\rho(A, p_1(Ax) \ldots, p_n(Ax)\ r_{n+1}) \in \mathscr{F}_n[r_{n+1}]$ 的次数为 $n!$，且由引理 4.4 可知，其根为 $p_{n+1}(Ax)$。因此， $p_{n+1}(Ax)$ 在 $\mathscr{F}_n$ 上的最小多项式 μ_{n+1} （相差一个 $\mathscr{F}_n$ 中元素的乘数）为 $\rho(A, p_1(Ax) \ldots, p_n(Ax)\ r_{n+1}) \in \mathscr{F}_n[r_{n+1}]$。根据注 4.6， $\rho(A, r_1, \ldots, r_{n+1}) \in k(A)(r_1, \ldots, r_n)[r_{n+1}]$ 是不可约的，其中 $k(A)(r_1, \ldots, r_n)$ 表示多项式环 $k(A)[r_1, \ldots, r_n]$ 的分式域。由不可约多项式的高斯引理，只需证明

$\rho(A, r_1, \ldots, r_{n+1})$ 在 $k[A, r_1, \ldots, r_n][r_{n+1}]$ 中是本原的。

$\rho(A, r_1, \ldots, r_{n+1})$ 的系数的任何公因子都必须整除 $r_{n+1}^{n!}$ 的系数；根据引理 4.3，该系数为 $\mathcal{R}(p_1(Ax)\ldots, p_n(Ax))^{n+1} \in k[A]$。因此，只需证明没有非恒定多项式 $p(A) \in k[A]$ 整除 $\rho(A, r_1, \ldots, r_{n+1})$。反设 $p(A) \in k[A]$ 是 $\mathcal{R}(A, r_1, \ldots, r_{n+1})$ 的一个非恒定因子，并令 $A^* \in k^{m\times n}$ $p\ A$ $r_1^* \ \ldots \ r_{n+1}^* \in \bar{k}^{n+1}$ $\mathcal{R}\ A^*$ $\ldots$ $= 0$ 3 $4\ 1$ 为 ( ) 的一个根。由此可知, $\ldots$ 对于任意选择 (, ,), 都有 (, r_1^*, , r_{n+1}^*) , 因此根据命题 . 的第 ( ) 部分，多项式 $f_i^*(x) = p_i(A^*x) - r_i^* x_{n+1}^i \in \bar{k}[x_1, \ldots, x_{n+1}]$, $i \in [n+1]$ 有一个公共根 $0 \neq (\xi_1, \ldots, \xi_{n+1}) \in \bar{k}^{n+1}$。下面区分 rank$(A^*) = n$和 rank$(A^*) < n$两种情况。

假设 rank$(A^*) = n$。如果 $\xi_{n+1} = 0$，令 ξ 为列向量 $(\xi_1, \ldots, \xi_n) \in k^n$，则我们有 $A^*\xi \in k^m$ 是多项式 $p_1(z)$ .., $p_m(z) \in k[z] = k[z_1, \ldots, z_m]$ 的公共根（回忆 $m = n+1$）。由于 p_i's 是 $k[z]$ 中的正则序列，我们必有 $A^*\xi = 0$。根据假设，rank$(A^*) = n$ ，因此$\xi = 0$；然而，这与我们关于并非所有 ξ_1, $\ldots$, ξ_{n+1} 均为零的假设相矛盾。因此，必有 $\xi_{n+1} \neq 0$；又由于 f_i^*'s 是齐次的，我们可以假设$\xi_{n+1} = 1$；进而，对于每个 $i \in [n+1]$，都有 $r_i^* = p_i(A^*\xi)$。由于 r_i^*'s 是任意选取的，多项式映射 $\bar{k}^n \to \bar{k}^{n+1}$ （它将 $\beta^* \in \bar{k}^n$ 映射到 $(p_1(A^*\beta^*)\ldots, p_{n+1}(A^*\beta^*)) \in \bar{k}^{n+1}$）的像必定是整个 $\bar{k}^{n+1}$。这意味着，该映射的闭包的仿射坐标环，即 $k[p_1(A^*x)\ldots, p_{n+1}(A^*x)]$，必须具有克鲁尔维数 $n+1$。但这是不可能的，因为它是 $k[x] = k[x_1, \ldots, x_n]$的子环。

我们已经得出结论：对于 $p(A)$ 的任意根 A^*，秩$(A^*) < n$。换言之，由多项式 $p(A)$ 定义的超曲面必须包含在由 A 的极大子式所生成的理想 $I_n(A)$ 定义的行列式簇中。但这是不可能的，因为前者的维数为 $(n+1)n - 1 = n^2 + n - 1$，而众所周知，后者的维数为 $(n-1)(n+2) = n^2 + n - 2$ [5, 3]。 □

现在我们讨论一般情形。

LEMMA 4.8. $\rho(A, r_1, \ldots, r_{n+1})$ 在 $k[A, r_1, \ldots, r_{n+1}]$ 中不可约。

证明。情形 $m = n+1$ 已在引理 4.7 中证明，因此我们假设$m > n+1$。记 A 为从 A 中将所有满足 $i > n+1$ 的 a_{ij} 替换为零后得到的矩阵；这诱导出一个 k-代数同态 $\vartheta : k[A, r] \to k[A, r]$，它将 A 映为 A。由于结式与特化可交换，$\vartheta(\rho(A, r_1, \ldots, r_{n+1})) = \rho\left(\bar{A}, r_1, \ldots, r_{n+1}\right)$。现在假设 $\rho(A, r_1, \ldots, r_{n+1}) = gh$，其中 g, h 是 $k[A, r]$ 中的非恒定多项式；那么 $\rho\left(\bar{A}, r_1, \ldots, r_{n+1}\right) = \vartheta(g)\vartheta(h)$，其中 $\vartheta(g)$ $\vartheta(h) \in k[\bar{A}, r_1, \ldots, r_{n+1}]$。根据引理 4.7 $\rho\left(\bar{A}, r_1, \ldots, r_{n+1}\right)$ 在 $k[A, r_1, \ldots, r_{n+1}]$ 中不可约，因此我们可以假设 $\vartheta(g) = 1$。由此可知，r_{n+1} 在 $\vartheta(h)$ 中的次数为 $n!$，因此 r_{n+1} 在 h 中的次数也为 $n!$。进而可得，g 整除 $\rho(A, r_1, \ldots, r_{n+1})$ 中 $r_{n+1}^{n!}$ 的系数；根据引理 4.3，该系数为 $\mathcal{R}(p_1(Ax)\ldots, p_n(Ax))^{n+1} \in k[A]$。根据命题 4.1 的第 (2) 部分，对于每个$i \in [n]$，$\mathcal{R}(p_1(Ax)\ldots, p_n(Ax))$ 是关于 $p_i(Ax)$ 的系数的齐次多项式，次数为 $n!/i$；这些系数本身是关于变量 A 的次数为 i 的齐次多项式。因此我们得出结论：$\mathcal{R}(p_1(Ax)\ldots, p_n(Ax))$ 是关于变量 A 的齐次多项式，次数为 $nn!$。由于 g 整除$\mathcal{R}(p_1(Ax)\ldots, p_n(Ax))^{n+1}$，它也必定是齐次的；又因 $\vartheta(g) = 1$，可知 g 确为一个常数多项式。 □

我们得出了以下关键事实：

LEMMA 4.9. $\mathscr{F}_n$ 上的 $p_{n+1}(Ax)$ 的最小多项式 μ_{n+1} 除了乘以 LEMMA 4 中的元素外，等于

$\rho(A, p_1(Ax) \ldots, p_n(Ax)\ r_{n+1})$，因此次数为 $n!$。

证明。由引理 4.8 和备注 4.6 ρ，$A(p_1(Ax) \ldots, p_n(Ax)\ r_{n+1})$ 作为关于 $k[A, p_1(Ax) \ldots, p_n(Ax)][r_{n+1}]$ 的多项式是不可约的。根据唯一分解整环上不可约多项式的高斯引理，$\rho(A, p_1(Ax) \ldots, p_n(Ax)\ r_{n+1})$ 在 $k(A)(p_1(Ax) \ldots, p_n(Ax))[r_{n+1}] = \mathscr{F}_n[r_{n+1}]$ 中也不可约。由引理 4.3，它关于 r_{n+1} 的次数为 $n!$；由引理 4.4，它以 $p_{n+1}(Ax)$ 为根。 □

现在我们可以陈述并证明本文的主要技术定理:

THEOREM 4.10. 我们有域等式 $\mathscr{F}_{n+1} = \mathscr{F}_m$。

证明。我们有 $[\mathscr{F}_m : \mathscr{F}_n] = n!$ 根据命题 3.1以及 $[\mathscr{F}_{n+1} : \mathscr{F}_n] = n!$ 根据引理 4.9；由于 $\mathscr{F}_n \subseteq \mathscr{F}_{n+1} \subseteq \mathscr{F}_m$，我们必有 $\mathscr{F}_{n+1} = \mathscr{F}_m$。 □

作为定理 4.10的推论，我们可以证明定理 1.1。

证明。（定理 1.1）根据定理 4.10，我们有 $\mathscr{F}_{n+1} = \mathscr{F}_m$，根据命题 2.1，我们有 $\mathscr{F}_m = \mathscr{E}$；也就是说 $\mathscr{F}_{n+1} = \mathscr{E}$。具体而言，$k(A)(p_1(Ax) \ldots, p_{n+1}(Ax)) = k(A)(x)$。由此等式立即可得，每个 x_i 都是 k 上关于 A、$p_1(Ax) \ldots, p_{n+1}(Ax)$ 的有理函数。特别地，对于每个 $i \in [n]$，存在多项式

$$f_i\big(A, p_1(Ax), \ldots, p_{n+1}(Ax)\big), g_i\big(A, p_1(Ax), \ldots, p_{n+1}(Ax)\big)$$

在 $k[A][p_1(Ax) \ldots, p_{n+1}(Ax)]$ 使得 $x_i = f_i/g_i$；事实上，由于这对每个特征零域 k 都成立，可知 $f_i, g_i \in \mathbb{Z}[A][p_1(Ax) \ldots, p_n(Ax)]$.

现在令 $A^* \in k^{m\times n}$ 和 $x^* \in k^n$ 为一般的，即将 A 和 x 分别代入 A^* 和 x^*后，没有一个 g_i取值为零。假设，$\xi \in k^n$ 是多项式 $q_i(x) = p_i(A^*x) - p_i(A^*x^*)$ $i \in [n+1]$的一个公共根；也就是说，对于每个 $i \in [n+1]$，都有 $p_i(A^*\xi) = p_i(A^*x^*)$。因此，

$$0 \neq g_i\big(A^*, p_1(A^*x^*), \ldots, p_{n+1}(A^*x^*)\big) = g_i\big(A^*, p_1(A^*\xi), \ldots, p_{n+1}(A^*\xi)\big)$$

$\forall i \in [n]$，因此有理函数 $x_i = f_i/g_i$ 的相等关系给出了 k中的一个等式

$$\xi_i = \frac{f_i\big(A^*, p_1(A^*\xi), \ldots, p_{n+1}(A^*\xi)\big)}{g_i\big(A^*, p_1(A^*\xi), \ldots, p_{n+1}(A^*\xi)\big)} = \frac{f_i\big(A^*, p_1(A^*x^*), \ldots, p_{n+1}(A^*x^*)\big)}{g_i\big(A^*, p_1(A^*x^*), \ldots, p_{n+1}(A^*x^*)\big)} = x_i^*$$

对每个 $i \in [n]$均成立。 □

参考文献

[1] A. ABID AND J. ZOU, *A stochastic expectation-maximization approach to shuffled linear regres-sion*，载于 Allerton通信、控制与计算年会，2018年，第470–477页。[2] M. ATIYAH AND I. G. MACDONALD, *Introduction to Commutative Algebra*，《Addison-Wesley数学丛书》，CRC出版社，1969年。[3] W. BRUNS, A. CONCA, C. RAICU, AND M. VARBARO, *Determinants Gröbner Bases and Co-homology*，Springer。2022

[4] W. BRUNS AND J. HERZOG, *Cohen-Macaulay Rings*，第39号，剑桥大学出版社，1998年。

[5] W. BRUNS AND U. VETTER, *Determinantal Rings*，第1327卷，Springer，1988年。[6] D. COX, J. LITTLE, AND D. OSHEA, *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic geometry and Commutative Algebra*，Springer Science & Business Media，2013年。

[7] R. Dvornicich and U. Zannier, *Newton functions generating symmetric fields and irreducibility of schur polynomials* 222 2009 1982 2003, , 《数学进展》, （ ）, 第–页, https:// doi.org/https://doi.org/10.1016/j.aim.2009.06.021。[8] G. Elhami, A. Scholefield, B. B. Haro, and M. Vetterli, *Unlabeled sensing: Reconstruction algorithm and theoretical guarantees*, 载于IEEE声学、语音与信号处理国际会议, 2017年3月, 第4566–4570页。[9] H. O. Foulkes, *Theorems of kakeya and pólya on power-sums*, 《数学杂志》, 65（1956年）, 第345–352页, https://doi.org/https://doi.org/10.1007/BF01473887。[10] I. M. Gelfand, M. M. Kapranov, and A. V. Zelevinsky, *Discriminants Resultants and* , , *Multidimensional Determinants* ¨ 1994, 10 1007 Birkhauser, 波士顿, MA, https://doi.org/ 。 / 978-0-8176-4771-1。[11] R. Hartshorne, *A property of a-sequences*, 《法国数学学会通报》, 94（1966年）, 第61–65页。[12] D. Hsu, K. Shi, and X. Sun, *Linear regression without correspondence*, 载于《神经信息处理系统进展》, 第30卷, 2017年。[13] S. Kakeya, *On fundamental systems of symmetric functions-ii*, 《日本数学杂志：论著与摘要》, 4（1927年）, 第77–85页, https://doi.org/10.4099/jjm1924. 4.0 77。[14] S. Lang, *Algebra*, 第211卷, Springer Science & Business Media, 2012年。[15] F. Li, K. Fujiwara, F. Okura, and Y. Matsushita, *Shuffled linear regression with outliersin both covariates and responses*, 《国际计算机视觉杂志》, 131（2023年）, 第732–751页。[16] H. Liang, J. Lu, M. C. Tsakiris, and L. Zhi, *Unlabeled Sensing Using Rank-One MomentMatrix Completion*, 即将发表于第49届国际符号与代数计算研讨会论文集, arXiv预印本arXiv:2405.16407 (2024)。[17] R. Ma, T. T. Cai, and H. Li, *Optimal estimation of bacterial growth rates based on a permuted monotone matrix* 108 2021 693 708 , 《生物计量学》, （ ）, 第–页。[18] F. Macaulay, *The Algebraic Theory of Modular Systems*, 《剑桥数学与数理物理丛书》, 剑桥, 1916年。[19] H. Matsumura, *Commutative Ring Theory*, 第8号, 剑桥大学出版社, 1989年。[20] H. Melánová, B. Sturmfels, and R. Winter, *Recovery from power sums*, 《实验数学》, （2022年）, 第1–10页。[21] K. Nakamura, *On the representation of symmetric functions by power-sums which formthe fundamental system*, 《日本数学杂志：论著与摘要》, 4（1927年）, 第87–92页, https://doi.org/10.4099/jjm1924.4.0 87。[22] A. Nejatbakhsh and E. Varol, *Neuron matching in c. elegans with robust approximate linear regression without correspondence*, 载于IEEE/CVF冬季计算机视觉应用会议论文集, 2021年, 第2837–2846页。[23] A. Pananjady, M. J. Wainwright, and T. A. Courtade, *Linear regression with shuffleddata: Statistical and computational limits of permutation recovery*, IEEE 信息论汇刊, 64（2018年）, 第3286–3300页。[24] L. Peng and M. C. Tsakiris, *Linear Regression Without Correspondences via Concave Minimization* 27 2020 1580 1584, 10 , 《IEEE信号处理快报》, （ ）, 第–页, https://doi.org/ 。 1109/LSP.2020.3019693。[25] L. Peng and M. C. Tsakiris, *Homomorphic sensing of subspace arrangements*, 《应用与计算调和分析》, 55（2021年）, 第466–485页。[26] M. Slawski and E. Ben-David, *Linear regression with sparsely permuted data*, 《电子统计学杂志》, 13（2019年）, 第1–36页。[27] M. Slawski, E. Ben-David, and P. Li, *Two-stage approach to multivariate linear regression with sparsely mismatched data* 21 2020 1 42 , 《机器学习研究杂志》, （ ）, 第–页。[28] X. Song, H. Choi, and Y. Shi, *Permuted linear model for header-free communication viasymmetric polynomials*, 载于IEEE信息论国际研讨会, 2018年, 第661–665页。[29] M. C. Tsakiris, *Determinantal conditions for homomorphic sensing*, 《线性代数及其应用》, 656（2023年）, 第210–223页, https://doi.org/https://doi.org/10.1016/j.laa.2022. 09.026, https://www.sciencedirect.com/science/article/pii/S0024379522003512。[30] M. C. Tsakiris, *Matrix recovery from permutations: An algebraic geometry approach*, 载于IEEE信息论国际研讨会（ISIT）, IEEE, 2023年, 第2511–2516页。[31] M. C. Tsakiris and L. Peng, *Homomorphic sensing*, 载于国际机器学习会议, 2019年, 第6335–6344页。[32] M. C. Tsakiris, L. Peng, A. Conca, L. Kneip, Y. Shi, and H. Choi, *An algebraic-geometricapproach for linear regression without correspondences*, IEEE 信息论汇刊

理论，66（2020年），第 5130–5144 页。[33] J. Unnikrishnan, S. Haghighatshoar, and M. Vetterli, *Unlabeled sensing: Solving a linearsystem with unordered measurements*，载于 2015 年 Allerton通信、控制与计算年会，第 786–793 页。[34] J. Unnikrishnan, S. Haghighatshoar, and M. Vetterli, *Unlabeled sensing with random linear measurements* 64 2018 3237 3253 ，《IEEE 信息论汇刊》， （），第 – 页。[35] B. L. van der Waerden, *Modern Algebra II*，Frederick Ungar，第一版，1950 年。[36] Y. Yao, L. Peng, and M. C. Tsakiris, *Unlabeled principal component analysis*，载于《神经信息处理系统进展》，34（2021年），第 30452–30464 页。[37] Y. Yao, L. Peng, and M. C. Tsakiris, *Unlabeled Principal Component Analysis and Matrix Completion* 25 2024 1 38 ，《机器学习研究杂志》， （），第 – 页。[38] H. Zhang, M. Slawski, and P. Li, *The benefits of diversity: Permutation recovery in unlabeledsensing from multiple measurement vectors*，《IEEE 信息论汇刊》，68（2021年），第 2509–2529 页。