Journal of Symbolic Computation 135 (2026) 102542

Contents lists available at ScienceDirect

Journal of Symbolic Computation

journal homepage: www.elsevier.com/locate/jsc

A field-theoretic view of unlabeled sensing

Hao Liang, Jingyu Lu, Manolis C. Tsakiris, Lihong Zhi

State Key Laboratory of Mathematics Mechanization, Academy of Mathematics and Systems Science, University of Chinese Academy of Sciences, Beijing, 100190, China

ARTICLE INFO

Article history:
Received 31 October 2024
Received in revised form 9 December 2025
Accepted 10 December 2025
Available online 10 December 2025

Keywords:
Unlabeled sensing
Determinantal variety
Birational morphism
Commutative algebra and algebraic geometry

ABSTRACT

Unlabeled sensing is the problem of solving a linear system of equations, where the right-hand-side vector is known only up to a permutation. In this work, we study fields of rational functions related to symmetric polynomials and their images under a linear projection of the variables; as a consequence, we establish that the solution to an n-dimensional unlabeled sensing problem with generic data can be obtained as the unique solution to a system of $n+1$ polynomial equations of degrees $1, 2, \dots, n+1$ in n unknowns. Besides the new theoretical insights, this development offers the potential for scaling up algebraic unlabeled sensing algorithms.

1. Introduction

1.1. Unlabeled sensing

In *unlabeled sensing* (Unnikrishnan et al., 2015, 2018) one is given a matrix $A^* \in \mathbb{R}^{m\times n}$, with $m > n$ and $\operatorname{rank}(A) = n$, and a vector $y^* \in \mathbb{R}^m$, such that for a permutation π of the coordinates of $\mathbb{R}^m$ the linear system of equations $A^*x = \pi(y^*)$ has a solution ξ^*; the problem then is to find ξ^* from A^* and y^*. The main theorem of unlabeled sensing asserts that this is a well-defined question when A is generic and $m \geq 2n$. This result has been generalized beyond permutations to arbitrary linear transformations (Tsakiris, 2023a; Peng and Tsakiris, 2021), as well as beyond linear spaces to unions

E-mail addresses: lianghao2020@amss.ac.cn (H. Liang), jingyulu@amss.ac.cn (J. Lu), manolis@amss.ac.cn (M.C. Tsakiris), lzhi@mmrc.iss.ac.cn (L. Zhi).

https://doi.org/10.1016/j.jsc.2025.102542
0747-7171/

of linear spaces (Peng and Tsakiris, 2021) and to spaces of bounded-rank matrices (Yao et al., 2021, 2024; Tsakiris, 2023b).

Unlabeled sensing is an extremely challenging computational problem, known to be NP-hard (Pananjady et al., 2018; Hsu et al., 2017), with brute-force (Elhami et al., 2017) or globally optimal approaches being tractable only for small dimensions; see Peng and Tsakiris (2020) for a brief account. Nevertheless, unlabeled sensing has a wealth of potential applications from biology (Abid and Zou, 2018; Ma et al., 2021) and neuroscience (Nejatbakhsh and Varol, 2021) to digital communications (Song et al., 2018), data mining (Slawski and Ben-David, 2019; Slawski et al., 2020; Zhang et al., 2021) and computer vision (Tsakiris and Peng, 2019; Li et al., 2023).

1.2. Motivation

In this paper we are concerned with algebraic aspects of unlabeled sensing (Song et al., 2018; Tsakiris et al., 2020; Melánová et al., 2022), for which we now set the context. Let

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

be polynomial rings in m and n variables respectively over the real numbers $\mathbb{R}$, and let

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

be the ℓ-th power sum of the y_i's; here and in the sequel $[t]$ denotes the set $\{1, 2, \dots, t\}$, whenever t is a positive integer. In Song et al. (2018) it was observed that ξ^* is a root of the polynomial

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

for any $\ell \in \mathbb{N}$; here and in the sequel x is the column vector containing $x_1, \dots, x_n$ in its entries. With A^* generic, it was proved in Tsakiris et al. (2020) that the square system

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

is zero-dimensional and thus has at most $n!$ solutions. An algorithm was also developed, which involved solving the square polynomial system for all of its roots via off-the-shelf solvers, isolating a root by a suitable criterion, and then using an expectation-maximization procedure to refine that root. An attractive feature of this algorithm is that it has linear complexity in m, while it has been empirically observed to be robust to low levels of noise: for SNR=40 dB, $m = 1000$ and $n = 4$, the algorithm took 25 milliseconds on a standard PC to produce a solution with a relative error of 0.4% with respect to the ground truth. On the other hand, this algorithm is not scalable with respect to n: as n increases, one would not even be able to store efficiently the $n!$ solutions of the square polynomial system, let alone solve it; indeed, in Tsakiris et al. (2020) it was possible to report results only for $n \leq 6$.

1.3. Contributions

Our object of study in this paper is the overdetermined system of $n + 1$ polynomial equations in n unknowns

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

Our main result reads:

Theorem 1. *Suppose that $A^* \in \mathbb{R}^{m \times n}$ and $\xi^* \in \mathbb{R}^{n \times 1}$ are generic, let π be any permutation of the coordinates of $\mathbb{R}^{m \times 1}$, and set $y^* = \pi(A^* \xi^*) \in \mathbb{R}^{m \times 1}$. Then ξ^* is the unique complex solution of the polynomial system $\mathcal{Q}_{n+1}$.*

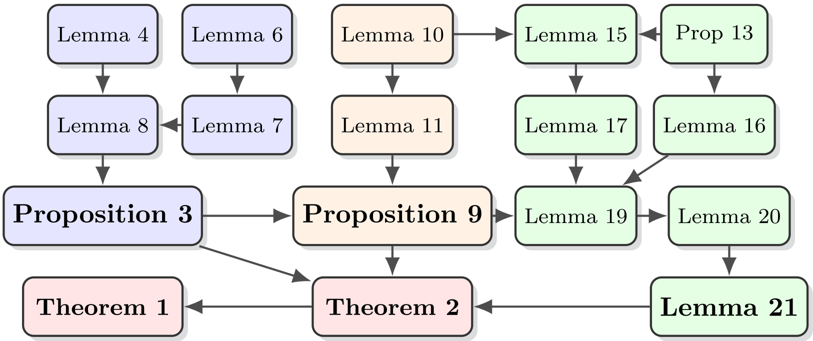

Fig. 1. The logical dependencies between the statements in this paper, the latter concerning integral ring extensions (purple), degrees of finite field extensions (orange), resultants (green), and the main results (red). (For interpretation of the colors in the figure, the reader is referred to the web version of this article.)

Theorem 1 settles an important open question in the theory of unlabeled sensing. Indeed, that $\mathscr{Q}_{n+1}$ has a unique solution for generic data was already experimentally observed in Song et al. (2018), and a more general unique recovery conjecture was formulated in Melánová et al. (2022) (Conjecture 6). But Theorem 1 also has significant implications for unlabeled sensing algorithms: no matter which method is used to obtain a root of $\mathscr{Q}_{n+1}$, Theorem 1 guarantees that this root is ξ^*; contrast this to the algorithm of Tsakiris et al. (2020) which relied on filtering all $n!$ solutions of $\mathscr{Q}_n$. Indeed, in Liang et al. (2024), for which the present manuscript partially serves as a rigorous theoretical foundation, we have proposed an algorithm for obtaining the unique solution of $\mathscr{Q}_{n+1}$ via rank-1 moment matrix completion, and reported encouraging results.

The proof of Theorem 1 relies on a careful analysis of a certain field of rational functions associated to the polynomials p_ℓ after a linear projection of the variables x has been applied, which is interesting on its own right (note that without the linear projection, the study of the field generated by the p_ℓ's for fixed given values of ℓ and the question of when this coincides with the field of symmetric rational functions on x, is an old and well-known topic in the literature, e.g. see Kakeya (1927); Nakamura (1927); Foulkes (1956); Dvornicich and Zannier (2009)). Let $A = (a_{ij})$ be an $m \times n$ matrix of variables so that all a_{ij}'s and x_j's are jointly algebraically independent over $\mathbb{R}$. Denote by $\mathscr{E} = \mathbb{R}(A, x)$ the field of rational functions in the variables A, x with coefficients in $\mathbb{R}$ and

$$\mathscr{F}_{n+1} = \mathbb{R}(A, p_1(Ax), \dots, p_{n+1}(Ax))$$

the subfield of $\mathscr{E}$ consisting of the rational functions in $A, p_1(Ax), \dots, p_{n+1}(Ax)$ with coefficients in $\mathbb{R}$. We prove:

Theorem 2. *The fields of rational functions $\mathscr{F}_{n+1}$ and $\mathscr{E}$ coincide.*

1.4. Organization

Theorem 2 is proved by a series of intermediate results, which occupy the core of this paper (§2 - §4). Once Theorem 2 is established at end of §4 (Theorem 22), Theorem 1 readily follows as shown in §5. The logical dependencies between the various statements in this paper are summarized in Fig. 1. The paper is concluded by giving some illustrative examples in §6.

1.5. Acknowledgments

We thank Aldo Conca for reading the manuscript and giving us valuable comments, and Matteo Varbaro for a pointer in the literature. Hao Liang, Jingyu Lu and Lihong Zhi are supported by the National Key R&D Program of China (2023YFA1009401) and the National Natural Science Foundation of China (12071467). Manolis C. Tsakiris is supported by the National Key R&D Program of China (2023YFA1009402).

2. The field $\mathscr{F}_m$

Nothing of what we will say in this and the next section depends on the ground field, other than the requirement that it has characteristic zero; we thus fix throughout such a field k; we will denote by $k(A)$ the field of fractions of the polynomial ring $k[A]$. We fix polynomial rings over the field $k(A)$

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

and define $k(A)$-algebra homomorphisms $S \overset{\varphi}{\to} T \overset{\psi}{\to} R$, where $\varphi(z_i) = p_i$ and $\psi(y_i) = \sum_{j\in[n]} a_{ij} x_j$ for every $i \in [m]$. We let $\mathfrak{p} = I_{n+1}(A|y)$ be the ideal of T generated by all $(n+1)$-minors of the $m \times (n+1)$ matrix $[A|y]$; here y is the vector of variables $y_1, \dots, y_m$. Each such $(n+1)$-minor is a linear form of T and thus $\mathfrak{p}$ is a prime ideal of T whose height can be seen to be $m - n$. Since ψ is surjective, $\mathfrak{p} = \ker(\psi)$ and $R \cong T/\mathfrak{p}$.

Let $\mathfrak{q} = S \cap \mathfrak{p}$ be the contraction of $\mathfrak{p}$ to S under φ; this is a prime ideal of S whose residue field $S_\mathfrak{q}/\mathfrak{q}S_\mathfrak{q}$ we denote by $\kappa(\mathfrak{q})$. We have an inclusion of integral domains $S/\mathfrak{q} \hookrightarrow T/\mathfrak{p} \cong R = k(A)[x]$, which identifies $S/\mathfrak{q}$ with the $k(A)$-subalgebra $k(A)[p_1(Ax), \cdots, p_m(Ax)]$ of R; we denote the field of fractions of this subalgebra by $\mathscr{F}_m$. In turn, this induces the inclusion of fraction fields $\kappa(\mathfrak{q}) \cong \mathscr{F}_m \subseteq \mathscr{E} \cong \kappa(\mathfrak{p})$, where we recall that $\mathscr{E}$ is the field of fractions of the polynomial ring $k(A)[x]$ and $\kappa(\mathfrak{p}) = T_\mathfrak{p}/\mathfrak{p}T_\mathfrak{p}$. The main result of this section is:

Proposition 3. *We have an equality of fields $\mathscr{F}_m = \mathscr{E}$.*

Towards proving Proposition 3, we begin with a basic but important fact.

Lemma 4. *T is a free S-module of rank $m!$.*

Proof. By virtue of Newton's identities, the subalgebra $\varphi(S) = k(A)[p_1, \dots, p_m]$ of T coincides with the subalgebra $k(A)[s_1, \dots, s_m]$ generated by the m elementary symmetric functions $s_1, \dots, s_m$ on the variables y; it thus suffices to prove that T is a free module over $k(A)[s_1, \dots, s_m]$ of rank $m!$.

Consider the polynomial ring

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

of dimension $2m$, and the ideal J of P generated by all $w_i - s_i(y)$ for $i \in [m]$, where $s_i(y)$ is the i-th elementary symmetric function on the variables y. Under any monomial order on P with $y_1 > \cdots > y_m > w_1 > \cdots > w_m$, Proposition 5 in Section 1 of Chapter 7 of Cox et al. (2013) explicitly describes a Gröbner basis of J, consisting of m polynomials $g_1, \dots, g_m \in P$ such that the leading term of g_i is y_i^i. It immediately follows that a $k(A)$-vector space basis of P/J is given by all monomials of the form $y_2^{\ell_2} \cdots y_m^{\ell_m} w_1^{b_1} \cdots w_m^{b_m}$, where the b_i's range over the non-negative integers while $0 \le \ell_i < i$.

Now consider the $k(A)$-algebra epimorphism $\theta : P = k(A)[y, w] \to T = k(A)[y]$ defined by $\theta(w_i) = s_i(y)$ and $\theta(y_i) = y_i$ for every $i \in [m]$. We have $J = \ker(\theta)$ and so $T = P/J$; since P/J is generated over $k(A)$ by the $m!$ monomials $y_2^{\ell_2} \cdots y_m^{\ell_m}$ as above and all monomials in w, T is a fortiori generated over $k(A)[s_1(y), \dots, s_m(y)] \cong k(A)[w_1, \dots, w_m]$ by the $y_2^{\ell_2} \cdots y_m^{\ell_m}$'s. To show that these monomials are free generators, suppose that there is an algebraic relation $\sum_{0\le\ell_i<i} c_{\ell_2,\dots,\ell_m}(y) y_2^{\ell_2} \cdots y_m^{\ell_m} = 0$, with $c_{\ell_2,\dots,\ell_m}(y) \in k(A)[s_1(y), \dots, s_m(y)]$. Write $c_{\ell_2,\dots,\ell_m}(y) = f_{\ell_2,\dots,\ell_m}(s_1(y), \dots, s_m(y))$, where $f_{\ell_2,\dots,\ell_m}$ is a polynomial in m variables with coefficients in $k(A)$. Note $\theta(f_{\ell_2,\dots,\ell_m}(w)) = c_{\ell_2,\dots,\ell_m}(y)$, whence $\sum_{0\le\ell_i<i} f_{\ell_2,\dots,\ell_m}(w) y_2^{\ell_2} \cdots y_m^{\ell_m} \in \ker(\theta)$. Since $J = \ker(\theta)$ and the g_i's form a Gröbner basis of J, the leading term of $\sum_{0\le\ell_i<i} f_{\ell_2,\dots,\ell_m}(w) y_2^{\ell_2} \cdots y_m^{\ell_m}$ must be divisible by y_i^i for some $i \in [m]$; however, it is seen from the form of $\sum_{0\le\ell_i<i} f_{\ell_2,\dots,\ell_m}(w) y_2^{\ell_2} \cdots y_m^{\ell_m}$ that this is impossible, unless this is the zero

polynomial. Since all monomials in y freely generate $k(A)[y,w]$ as a module over $k(A)[w]$, we in turn have that all $f_{\ell_2,\dots,\ell_m}(w)$'s and thus all $c_{\ell_2,\dots,\ell_m}(y)$'s are zero. □

Remark 5. The fact that T is a free S-module is a special case of the well-known Chevalley-Shephard-Todd theorem.

The Lemma 4 implies that T is integral to $\varphi(S)$; this is a manifestation of a general fact:

Lemma 6 *(Exercises 12 & 13, Chapter 5, Atiyah and MacDonald (1969)). Let R be a commutative ring and Π a finite group acting on R; denote by R^{Π} the subring of R consisting of the invariant elements of R with respect to the action of Π. Then the ring extension $R^{\Pi} \subseteq R$ is integral, and for any prime ideal $\mathfrak{P}$ of R, the prime ideals of R that lie over $\mathfrak{P} \cap R^{\Pi}$ are the orbit $\{\pi(\mathfrak{P}) : \pi \in \Pi\}$ of $\mathfrak{P}$ under Π.*

We have:

Lemma 7. *The prime ideals of T that lie over $\mathfrak{q} = S \cap \mathfrak{p}$ are precisely of the form $\pi(\mathfrak{p})$, where π is a permutation of the variables $y_1, \dots, y_m$; these are $m!$ distinct prime ideals.*

Proof. That a prime ideal of T lies over $\mathfrak{q}$ if and only if it is of the form $\pi(\mathfrak{p})$, follows from Lemma 6. We prove that all $m!$ such prime ideals $\pi(\mathfrak{p})$ are distinct. For this, it suffices to prove that $\pi(\mathfrak{p}) \neq \mathfrak{p}$ as soon as π is not the identity permutation. Let $\sigma = \pi^{-1}$ and $\mathcal{J} = \{m-n+1, \dots, m\} = [m] \setminus [m-n]$.

For $i_1, \dots, i_n, i_{n+1}$ distinct elements of m, we denote by $A_{i_1,\dots,i_n}$ the determinant of the $n \times n$ matrix, whose s-th row is the i_s-th row of A, and by $A_{i_1,\dots,\hat{i}_s,\dots,i_{n+1}}$ the determinant as above of the sub-matrix associated to rows $i_1, \dots, i_{s-1}, i_{s+1}, \dots, i_{n+1}$. For any monomial order on T with $y_1 > y_2 > \cdots > y_m$, the $m-n$ linear forms of T given by

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

are a reduced Gröbner basis of $\mathfrak{p}$. Similarly for $i \in [m-n]$, the linear forms

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

are a reduced Gröbner basis of $\pi(\mathfrak{p})$.

Since a reduced Gröbner basis is unique, if $\mathfrak{p} = \pi(\mathfrak{p})$, necessarily $\ell_i = \mu_i$ for every $i \in [m-n]$. In particular, for any $i \in [m-n]$ and any $s \in \mathcal{J}$, the coefficient of y_s in ℓ_i, must be equal to the coefficient of y_s in μ_i. Notice that $k(A)$ is the fraction field of the polynomial ring $k[A]$ which is a unique factorization domain (UFD), and the numerators and denominators of y_s's coefficients in ℓ_i and μ_i are irreducible polynomials in $k[A]$ with coefficients ± 1, we deduce that $A_{m-n+1,\dots,m} = \varepsilon A_{\sigma(m-n+1),\dots,\sigma(m)}$ and $A_{i,m-n+1,\dots,\hat{s},\dots,m} = \varepsilon A_{\sigma(i),\sigma(m-n+1),\dots,\widehat{\sigma(s)},\dots,\sigma(m)}$ for any $i \in [m-n]$, any $s \in \mathcal{J}$, and some $\varepsilon = \pm 1$. These equalities imply that $\sigma(\mathcal{J}) = \mathcal{J}$ and $\{i\} \sqcup \{m-n+1, \dots, \hat{s}, \dots, m\} = \{\sigma(i)\} \sqcup \{\sigma(m-n+1), \dots, \widehat{\sigma(s)}, \dots, \sigma(m)\}$ for any $i \in [m-n]$ and $s \in \mathcal{J}$. From $\sigma(\mathcal{J}) = \mathcal{J}$ we see that $\{m-n+1, \dots, \hat{s}, \dots, m\} = \mathcal{J} \setminus \{s\} \subset \mathcal{J}$ and $\{\sigma(m-n+1), \dots, \widehat{\sigma(s)}, \dots, \sigma(m)\} = \mathcal{J} \setminus \{\sigma(s)\} \subset \mathcal{J}$ for any $s \in \mathcal{J}$. Hence, from $i \notin \mathcal{J}$ we deduce that $\sigma(i) \notin \mathcal{J}$ and $\sigma(i) = i$ for any $i \in [m-n]$. Furthermore, from $\sigma(i) = i \notin \mathcal{J}$ we also see that $\mathcal{J} \setminus \{s\} = \mathcal{J} \setminus \{\sigma(s)\}$, which implies $\sigma(s) = s$ for any $s \in \mathcal{J}$. Therefore, $\sigma = \pi^{-1}$ is the identity permutation and $\varepsilon = 1$. □

The Proposition 3 is a special case of the following result for $\mathfrak{P} = \mathfrak{p}$:

Lemma 8. *Let $\mathfrak{P}$ be a prime ideal of T lying over $\mathfrak{q}$. Then $\kappa(\mathfrak{P}) = \kappa(\mathfrak{q})$.*

Proof. As T is a free S-module of rank $m!$ by Lemma 4, $T \otimes_S \kappa(\mathfrak{q})$ is a $\kappa(\mathfrak{q})$-vector space of dimension $m!$. Since $T \otimes_S \kappa(\mathfrak{q})$ is a finitely generated $\kappa(\mathfrak{q})$-algebra, which is also a finite-dimensional $\kappa(\mathfrak{q})$-vector space, it must be an Artinian ring. The prime ideals of $T \otimes_S \kappa(\mathfrak{q})$ correspond to the prime ideals of T lying over $\mathfrak{q}$. By Lemma 7, these are the $m!$ distinct prime ideals $\pi(\mathfrak{p})$, with π ranging over all permutations of the variables $y_1, \dots, y_m$. Quite generally, an Artinian ring is isomorphic to the product of its localizations at its prime ideals, hence

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

Now, each $T_{\pi(\mathfrak{p})} \otimes_S \kappa(\mathfrak{q}) = T_{\pi(\mathfrak{p})}/\mathfrak{q}T_{\pi(\mathfrak{p})}$ is an Artinian local ring and a finite $\kappa(\mathfrak{q})$-vector space. Since $T \otimes_S \kappa(\mathfrak{q})$ is an $m!$-dimensional $\kappa(\mathfrak{q})$-vector space and there are $m!$ factors in the product, it must be that each $T_{\pi(\mathfrak{p})} \otimes_S \kappa(\mathfrak{q})$ is a 1-dimensional $\kappa(\mathfrak{q})$-vector space, for every π. But $\kappa(\mathfrak{q})$ is contained in every $T_{\pi(\mathfrak{p})} \otimes_S \kappa(\mathfrak{q})$, so that $T_{\pi(\mathfrak{p})} \otimes_S \kappa(\mathfrak{q}) = \kappa(\mathfrak{q})$ for every π. Since $T_{\pi(\mathfrak{p})}/\mathfrak{q}T_{\pi(\mathfrak{p})} = T_{\pi(\mathfrak{p})} \otimes_S \kappa(\mathfrak{q}) = \kappa(\mathfrak{q})$ is a field, it must be that $\mathfrak{q}T_{\pi(\mathfrak{p})} = \pi(\mathfrak{p})T_{\pi(\mathfrak{p})}$ and so $T_{\pi(\mathfrak{p})}/\mathfrak{q}T_{\pi(\mathfrak{p})} = T_{\pi(\mathfrak{p})}/\pi(\mathfrak{p})T_{\pi(\mathfrak{p})} = \kappa(\pi(\mathfrak{p}))$. □

3. The field extension $\mathscr{F}_n \subseteq \mathscr{F}_m$

We denote by $\mathscr{F}_n$ the field of rational functions $k(A)(p_1(Ax), \dots, p_n(Ax))$; this is a subfield of $\mathscr{E} = k(A, x)$, this latter coinciding with $\mathscr{F}_m$ by Proposition 3. The main result of this section is:

Proposition 9. *The field extension $\mathscr{F}_n \subset \mathscr{F}_m$ is algebraic of degree $[\mathscr{F}_m : \mathscr{F}_n] = n!$.*

Towards proving Proposition 9, we prove a fundamental fact:

Lemma 10. *The polynomials $p_1(Ax), \dots, p_n(Ax)$ are a regular sequence of $R = k(A)[x]$.*

Proof. For a homogeneous ideal J in a polynomial ring P over a field, it follows from Serre's theorem on Hilbert functions (Bruns and Herzog, 1998, Theorem 4.4.3) that the Hilbert polynomial of P/J agrees with the Hilbert function of P/J at degrees greater than or equal to the Castelnuovo-Mumford (CM) regularity of J. It can be seen via the Koszul complex that the CM-regularity of an ideal J generated by a regular sequence of n elements of degrees $1, 2, 3, \dots, n$ is $\operatorname{reg}(J) = n(n-1)/2 + 1$.

Now let J be the ideal of R generated by $p_1(Ax), \dots, p_n(Ax)$. Then the sequence $p_1(Ax), \dots, p_n(Ax)$ is regular if and only if R/J has zero Krull dimension, if and only if the Hilbert polynomial of R/J is the zero polynomial, if and only if $[J]_a = [\mathfrak{m}]_a$; here $a = \operatorname{reg}(J) = n(n-1)/2 + 1$, $[J]_a$ denotes the degree-a homogeneous part of J, and $\mathfrak{m}$ is the ideal of R generated by $x_1, \dots, x_n$.

Let t be the dimension of $[\mathfrak{m}]_a$ as a $k(A)$-vector space. Take generators for $[J]_a$ by multiplying every $p_i(Ax)$ by all monomials of degree $a - i$. Make a matrix H whose columns contain the coefficients of the generators of $[J]_a$ on the basis of $[\mathfrak{m}]_a$ of all monomials of degree a. Then the $p_i(Ax)$'s are a regular sequence if and only if not all $t \times t$ minors of H are zero. But if they were zero, they would also be zero upon substitution of A by A^*, for any $A^* \in \bar{k}^{m \times n}$; here $\bar{k}$ denotes the algebraic closure of k. However, this would contradict the fact that the $p_i(A^*x)$'s are a regular sequence for a generic choice of $A^* \in \bar{k}^{m \times n}$, as per Lemma 4 in Tsakiris et al. (2020); here we have used the fact that when the $p_i(A^*x)$'s are a regular sequence of $\bar{k}[x]$, the CM-regularity of the ideal they generate is still a, while the $\bar{k}$-vector space dimension of the degree-a graded component of $\bar{k}[x]$ is still equal to t, so that the $p_i(A^*x)$'s are a regular sequence if and only if not all $t \times t$ minors of $H|_{A^*}$ are zero, where $H|_{A^*}$ is obtained from H by replacing A by A^*. □

Our next ingredient is fundamental as well and interesting in its own right.

Lemma 11. *$R = k(A)[x]$ is a free graded $k(A)[p_1(Ax), \dots, p_n(Ax)]$-module of rank $n!$.*

Proof. We first prove that R is flat over $R_n = k(A)[p_1(Ax), \dots, p_n(Ax)]$. Quite generally, the inclusion of R_n into R is a homomorphism of positively graded rings, which takes the maximal homogeneous ideal of R_n into the maximal homogeneous ideal $\mathfrak{m}$ of R. By part (3) of the Remark at page 178 in Matsumura (1989), R is flat over R_n if and only if $R_{\mathfrak{m}}$ is flat over R_n. By Lemma 10, $p_1(Ax), \dots, p_n(Ax)$ is a regular sequence of R; as such it remains a regular sequence in $R_{\mathfrak{m}}$. Consequently, Theorem 1 in Hartshorne (1966) gives that $R_{\mathfrak{m}}$ is flat over R_n; we conclude that R is flat over R_n.

Next, we argue that R is finitely generated graded R_n-module. Let J be the ideal of R generated by $p_i(Ax)$, $i \in [n]$, which is a regular sequence by Lemma 10. It follows that R/J is Artinian and of $k(A)$-vector space dimension $n!$; for the latter statement, we used the known form for the Hilbert series of the quotient of R by a regular sequence of homogeneous elements. As J is a homogeneous ideal, R/J is a graded $k(A)$-vector space, thus admitting a homogeneous $k(A)$-vector space basis $\{b + J : b \in \mathcal{B}\}$, where $\mathcal{B}$ is a set of $n!$ homogeneous polynomials in R. If $f \in R$ is a homogeneous polynomial of degree d, then we can write $f = \sum_{b\in\mathcal{B}} c_b\, b + f_1$, where $c_b \in k(A)$ and f_1 is a homogeneous polynomial of J of degree d. Writing $f_1 = \sum_{i\in[n]} g_i p_i(Ax)$, where g_i is homogeneous of degree $d - i$, we have $f = \sum_{b\in\mathcal{B}} c_b\, b + \sum_{i\in[n]} g_i p_i(Ax)$. Writing each g_i as a $k(A)$-linear combination of the b's plus a homogeneous polynomial of degree $d - i$ in J, we inductively see that R is finitely generated over R_n by $\mathcal{B}$.

We now argue that R is free of finite rank as a graded R_n-module. As R is a finite (i.e., finitely generated) R_n-module and R_n is a polynomial ring, R is finitely presented over R_n; since R is flat over R_n, it follows by the Corollary at page 53 in Matsumura (1989) that R is a projective R_n-module. Hence, with $\mathfrak{n}$ the maximal homogeneous ideal of R_n, we have that $R_{\mathfrak{n}}$ is a projective $(R_n)_{\mathfrak{n}}$-module. Now, Theorem 1.5.15(e) in Bruns and Herzog (1998) asserts that the projective dimension of R as a graded module over R_n is equal to the projective dimension of $R_{\mathfrak{n}}$ over the local ring $(R_n)_{\mathfrak{n}}$; it follows that R is a finite projective graded R_n-module. Finally, Theorem 1.5.15(d) in Bruns and Herzog (1998) asserts that R is a finite projective graded R_n-module if and only if it is a finite free graded R_n-module.

It remains to argue that the rank of R as a free graded module over R_n is $n!$. We have seen that R is free of finite rank, say ℓ, as a graded R_n-module via the inclusion of graded rings $R_n \to R$. It follows that $R \otimes_{R_n} R_n/\mathfrak{n}$ is an $R_n/\mathfrak{n}$-vector space of dimension ℓ. But $R \otimes_{R_n} R_n/\mathfrak{n} = R/\mathfrak{n}R = R/J$ and we have already seen that R/J has vector space dimension $n!$ over the field $k(A) = R_n/\mathfrak{n}$. Hence $\ell = n!$ (it can further be argued that $\mathcal{B}$ is in fact a set of free homogeneous generators of R over R_n). □

Remark 12. The proof of Lemma 11 directly generalizes to any regular sequence $h_1, \dots, h_n$ of R consisting of homogeneous elements of degrees $d_1, \dots, d_n$; this yields that R is a free $k(A)[h_1, \dots, h_n]$-module of rank $d_1 \cdots d_n$.

We can now prove Proposition 9.

Proof. (Proposition 9) For convenience we set $R_n = k(A)[p_1(Ax), \dots, p_n(Ax)]$. We have an inclusion of integral domains $R_n \subset R$, whose fields of fractions we denote respectively by $K(R_n)$ and $K(R)$. Now $K(R_n)$ is just a localization of R_n and so it is flat over R_n. We thus have an inclusion of rings $K(R_n) \subset R \otimes_{R_n} K(R_n) \subset K(R)$. By Lemma 11, R is a finitely generated R_n-module and so the ring extension $R_n \subset R$ is integral. It follows that the ring extension $K(R_n) \subset R \otimes_{R_n} K(R_n)$ is also integral; the Krull dimensions of both rings must be equal, whence $R \otimes_{R_n} K(R_n)$ is Artinian because $K(R_n)$ is a field. Quite generally, an Artinian ring contained in an integral domain must be a field; this implies that $R \otimes_{R_n} K(R_n)$ is a field. This field contains R and, since it is contained in $K(R)$, it must be that $R \otimes_{R_n} K(R_n) = K(R)$. As R is a free R_n-module of rank $n!$ by Lemma 11, it follows that $K(R)$ is a $K(R_n)$-vector space of dimension $n!$. Finally, recall that the fields $K(R_n)$ and $K(R)$ are just the fields $\mathscr{F}_n$ and $\mathscr{F}_m$, respectively. □

4. The field extension $\mathscr{F}_{n+1} \subseteq \mathscr{F}_m$

In this section, we will prove that the field

$$\mathscr{F}_{n+1} = k(A)(p_1(Ax), \dots, p_{n+1}(Ax))$$

coincides with the field $\mathscr{F}_m = \mathscr{E}$; Theorem 2 will follow as a special case for $k = \mathbb{R}$.

We have fields $\mathscr{F}_n \subseteq \mathscr{F}_{n+1} \subseteq \mathscr{F}_m$. By Proposition 9 the degree of the field extension $\mathscr{F}_n \subset \mathscr{F}_m$ is $n!$; hence to prove $\mathscr{F}_{n+1} = \mathscr{F}_m$ it suffices to prove that the degree of the field extension $\mathscr{F}_n \subseteq \mathscr{F}_{n+1}$ is $n!$. Note that $\mathscr{F}_{n+1}$ is just the field $\mathscr{F}_n(p_{n+1}(Ax))$ generated over $\mathscr{F}_n$ by $p_{n+1}(Ax)$; thus it suffices to prove that the minimal polynomial $\mu_{n+1} \in \mathscr{F}_n[t]$ of $p_{n+1}(Ax)$ over $\mathscr{F}_n$ has degree $n!$. We will achieve this by using multidimensional resultants (Macaulay, 1916; van der Waerden, 1950; Gelfand et al., 1994; Lang, 2012), which for the convenience of the reader we now briefly review following (Macaulay, 1916).

For a positive integer a and a field $\mathscr{K}$ of characteristic zero, let $l_1, \dots, l_a$ be positive integers and denote by $\mathcal{M}(t, l_i)$ the set of all monomials of degree l_i in the variables $t = t_1, \dots, t_a$. For every $i \in [a]$ and every monomial $w \in \mathcal{M}(t, l_i)$ we consider a variable $c(i, w)$ and define $f_i = \sum_{w \in \mathcal{M}(t,l_i)} c(i, w)\, w$; this can be viewed as a homogeneous polynomial of degree l_i in the variables t with coefficients in the polynomial ring $C = \mathscr{K}[c(i, w) : w \in \mathcal{M}(t, l_i),\ i \in [a]]$. Set $l = l_1 + \cdots + l_a - a + 1$ and let H be the matrix with entries in the ring C defined as follows: with $w \in \mathcal{M}(t, l - l_i)$ and $i \in [m]$ fixed, we consider the column-vector that gives the coefficients in C of $w f_i$ with respect to $\mathcal{M}(t, l)$; then H has as its columns all such vectors as i and w range in $[a]$ and $\mathcal{M}(t, l - l_i)$ respectively. Macaulay defined the resultant $\mathcal{R}(f_1, \dots, f_a)$ of $f_1, \dots, f_a$ as the greatest common divisor of all maximal minors of H; he proved that it has the following properties that we shall need:

Proposition 13 *((Macaulay, 1916), §6-§10, Chapter I). Set $L = l_1 \cdots l_a$ and $L_i = L/l_i$. Then*

1. *For $i \in [a]$ the degree of $c(i, t_i^{l_i})$ in $\mathcal{R}(f_1, \dots, f_a)$ is L_i and the coefficient of $c(a, t_a^{l_a})^{L_a}$ is $\mathcal{R}(\bar{f}_1, \dots, \bar{f}_{a-1})^{l_a}$, where $\bar{f}_i = f_i|_{t_a=0}$.*
2. *For every $i \in [a]$, we have that $\mathcal{R}(f_1, \dots, f_a)$ is homogeneous in the variables $(c(i, w))_{w \in \mathcal{M}(t,l_i)}$ of degree L_i.*
3. *Let $f_1^*, \dots, f_a^* \in \mathscr{K}[t] = \mathscr{K}[t_1, \dots, t_a]$ be any specialization of $f_1, \dots, f_a$, obtained by replacing each $c(i, w)$ by an element of $\mathscr{K}$, and $\mathcal{R}(f_1^*, \dots, f_a^*)$ the corresponding specialization of $\mathcal{R}(f_1, \dots, f_a)$. Then $\mathcal{R}(f_1^*, \dots, f_a^*) = 0$ if and only if $f_1^*, \dots, f_a^*$ have a common root in $\bar{\mathscr{K}}$ besides zero; here $\bar{\mathscr{K}}$ is the algebraic closure of $\mathscr{K}$.*

Remark 14. It is a basic observation that a set of n homogeneous polynomials in a polynomial ring of dimension n over $\mathscr{K}$ is a regular sequence if and only if the ideal they generate is primary to the maximal homogeneous ideal, which is equivalent to the polynomials admitting no common root in $\bar{\mathscr{K}}^n$ other than zero. Indeed, the matrix H that appeared in the proof of Lemma 10 is precisely Macaulay's matrix associated to the resultant of $p_1(Ax), \dots, p_n(Ax)$.

We now return to our objective of showing that the minimal polynomial μ_{n+1} of $p_{n+1}(Ax)$ over $\mathscr{F}_n$ has degree $n!$. We apply the formulation above with $a = n + 1$, letting t be the column vector with entries $t_1, \dots, t_n$, and introducing new variables $r_1, \dots, r_{n+1}$. For $i \in [n + 1]$ we define $f_i^* = p_i(At) - r_i t_{n+1}^i$; this is a homogeneous polynomial of degree i in the variables $t_1, \dots, t_{n+1}$ with coefficients in the polynomial ring $k(A)[r] := k(A)[r_1, \dots, r_{n+1}]$. We denote by $\mathcal{R}(f_1^*, \dots, f_{n+1}^*) \in k(A)[r]$ the specialization of the resultant $\mathcal{R}(f_1, \dots, f_m)$ of Proposition 13 with the variable $c(i, w)$ replaced by the corresponding coefficient of w in f_i^*. Similarly, applying the formulation above with $a = n$, we let $\mathcal{R}(p_1(At), \dots, p_n(At))$ be the specialization of $\mathcal{R}(f_1, \dots, f_n)$ with the variable $c(i, w)$ replaced by the corresponding coefficient of w in $p_i(At)$. It will be convenient to explicitly indicate the dependence of $\mathcal{R}(f_1^*, \dots, f_{n+1}^*) \in k(A)[r]$ on the variables A and $r = r_1, \dots, r_{n+1}$; for this we shall write $\rho(A, r_1, \dots, r_{n+1}) := (-1)^{n!}\mathcal{R}(f_1^*, \dots, f_{n+1}^*)$. We next proceed with a series of key observations.

Lemma 15. *$\rho(A, r_1, \dots, r_{n+1}) \in k(A)[r]$ is a non-zero polynomial of degree $n!$ in the variable r_{n+1}. The coefficient of $r_{n+1}^{n!}$ is $\mathcal{R}(p_1(At), \dots, p_n(At))^{n+1} \neq 0$.*

Proof. By Lemma 10 $p_1(Ax), \dots, p_n(Ax)$ is a regular sequence of $R = k(A)[x]$. Part (3) of Proposition 13 and Remark 14 give that $\mathcal{R}(p_1(At), \dots, p_n(At))$ is a non-zero element of $k(A)$. The statement now follows from part (1) of Proposition 13, because the resultant commutes with specialization. □

Lemma 16. *We have $\rho\,(A, p_1(Ax), \dots, p_{n+1}(Ax)) = 0$.*

Proof. After substituting r_i with $p_i(Ax)$ in the polynomials f_i^* for every $i \in [n+1]$, it is evident that the point $(x_1, \dots, x_n, 1) \in \mathscr{E}^{n+1}$ is a common root; thus the resultant of these polynomials vanishes by part (4) of Proposition 13. □

Lemma 17. *We have that $\rho\,(A, p_1(Ax), \dots, p_n(Ax), r_{n+1}) \neq 0$.*

Proof. This follows immediately from Lemma 15. □

Remark 18. As by Lemma 10 the polynomials $p_1(Ax), \dots, p_n(Ax)$ are a regular sequence of $k(A)[x]$, they are algebraically independent over $k(A)$. Hence the polynomials $p_1(Ax), \dots, p_n(Ax), r_{n+1}$ are algebraically independent over $k(A)$. Therefore, $\rho\,(A, p_1(Ax), \dots, p_n(Ax), r_{n+1})$ is an irreducible polynomial in the ring $k(A)[p_1(Ax), \dots, p_n(Ax), r_{n+1}]$ if and only if $\rho\,(A, r_1, \dots, r_{n+1})$ is irreducible in $k(A)[r_1, \dots, r_{n+1}]$.

We will prove that $\rho\,(A, r_1, \dots, r_{n+1})$ is irreducible in $k[A, r_1, \dots, r_{n+1}]$. We do this by first proving the special case $m = n+1$, where all the difficulty concentrates.

Lemma 19. *Suppose $m = n+1$, then $\rho\,(A, r_1, \dots, r_{n+1})$ is irreducible as a polynomial in $k[A, r_1, \dots, r_{n+1}]$.*

Proof. When $m = n+1$ we have $\mathscr{F}_m = \mathscr{F}_{n+1}$ and the degree of the field extension $\mathscr{F}_n \subseteq \mathscr{F}_{n+1}$ is $n!$ by Proposition 9. Since $\mathscr{F}_{n+1} = \mathscr{F}_n(p_{n+1}(Ax))$, we have that the minimal polynomial μ_{n+1} of $p_{n+1}(Ax)$ over $\mathscr{F}_n$ is of degree $n!$. On the other hand, by Lemma 17 the polynomial $\rho\,(A, p_1(Ax), \dots, p_n(Ax), r_{n+1}) \in \mathscr{F}_n[r_{n+1}]$ is a polynomial of degree $n!$, which by Lemma 16 has $p_{n+1}(Ax)$ as its root. Consequently, $\rho\,(A, p_1(Ax), \dots, p_n(Ax), r_{n+1}) \in \mathscr{F}_n[r_{n+1}]$ is the minimal polynomial μ_{n+1} of $p_{n+1}(Ax)$ over $\mathscr{F}_n$ up to multiplication by an element of $\mathscr{F}_n$. In view of Remark 18, we have that $\rho\,(A, r_1, \dots, r_{n+1}) \in k(A)(r_1, \dots, r_n)[r_{n+1}]$ is irreducible, where $k(A)(r_1, \dots, r_n)$ denotes the field of fractions of the polynomial ring $k(A)[r_1, \dots, r_n]$. By Gauss's lemma on irreducible polynomials, it suffices to prove that $\rho\,(A, r_1, \dots, r_{n+1})$ is primitive in $k[A, r_1, \dots, r_n][r_{n+1}]$.

Any common factor of the coefficients of $\rho\,(A, r_1, \dots, r_{n+1})$ must divide the coefficient of $r_{n+1}^{n!}$, which by Lemma 15 is $\mathcal{R}(p_1(At), \dots, p_n(At))^{n+1} \in k[A]$. Hence, it suffices to show that no non-constant polynomial $p(A) \in k[A]$ divides $\rho\,(A, r_1, \dots, r_{n+1})$. Suppose otherwise, that is $p(A) \in k[A]$ is a non-constant factor of $\mathcal{R}(A, r_1, \dots, r_{n+1})$ and let $A^* \in \bar{k}^{m \times n}$ be a root of $p(A)$. It follows that for any choice $(r_1^*, \dots, r_{n+1}^*) \in \bar{k}^{n+1}$ we have $\rho(A^*, r_1^*, \dots, r_{n+1}^*) = 0$, so that by part (3) of Proposition 13 the polynomials $f_i^*(x) = p_i(A^*x) - r_i^* x_{n+1}^i \in \bar{k}[x_1, \dots, x_{n+1}]$, $i \in [n+1]$ have a common root $0 \neq (\xi_1, \dots, \xi_{n+1}) \in \bar{k}^{n+1}$. Let us distinguish between the case $\operatorname{rank}(A^*) = n$ and $\operatorname{rank}(A^*) < n$.

Suppose that $\operatorname{rank}(A^*) = n$. If $\xi_{n+1} = 0$, letting ξ be the column vector $(\xi_1, \dots, \xi_n) \in \bar{k}^n$, we have that $A^*\xi \in \bar{k}^m$ is a common root of the polynomials $p_1(z), .., p_m(z) \in \bar{k}[z] = \bar{k}[z_1, \dots, z_m]$ (recall $m = n+1$). Since the p_i's are a regular sequence in $\bar{k}[z]$, we must have that $A^*\xi = 0$. By hypothesis $\operatorname{rank}(A^*) = n$ so that $\xi = 0$; however, this contradicts our assumption that not all $\xi_1, \dots, \xi_{n+1}$ are zero. Hence, it must be that $\xi_{n+1} \neq 0$, and since the f_i^*'s are homogeneous, we may assume $\xi_{n+1} = 1$; in turn, this gives $r_i^* = p_i(A^*\xi)$ for every $i \in [n+1]$. As the r_i^*'s were chosen arbitrarily, the image of the polynomial map $\bar{k}^n \to \bar{k}^{n+1}$ that takes $\beta^* \in \bar{k}^n$ to $(p_1(A^*\beta^*), \dots, p_{n+1}(A^*\beta^*)) \in \bar{k}^{n+1}$ must be the entire $\bar{k}^{n+1}$. This implies that the affine coordinate ring of the closure of this map, which is

$\bar{k}[p_1(A^*x), \dots, p_{n+1}(A^*x)]$, must have Krull dimension $n+1$. But this is impossible because this is a subring of $\bar{k}[x] = \bar{k}[x_1, \dots, x_n]$.

We have concluded that $\operatorname{rank}(A^*) < n$ for any root A^* of $p(A)$. In other words, the hypersurface of $\bar{k}^{m\times n}$ defined by the polynomial $p(A)$ must lie in the determinantal variety defined by the ideal $I_n(A)$ of maximal minors of A. But this is impossible, because the dimension of the former is $(n+1)n-1 = n^2+n-1$, while the dimension of the latter is well-known to be $(n-1)(n+2) = n^2+n-2$ (Bruns and Vetter, 1988; Bruns et al., 2022). □

We now treat the general case.

Lemma 20. *$\rho\,(A, r_1, \dots, r_{n+1})$ is irreducible in $k[A, r_1, \dots, r_{n+1}]$.*

Proof. The case $m = n+1$ has been proved in Lemma 19, hence we assume $m > n+1$. Let us denote by $\bar{A}$ the matrix obtained from A by replacing all a_{ij}'s for which $i > n+1$ with zero; this induces a k-algebra homomorphism $\vartheta : k[A, r] \to k[\bar{A}, r]$ which takes A to $\bar{A}$. As the resultant commutes with specialization, $\vartheta\,(\rho\,(A, r_1, \dots, r_{n+1})) = \rho\left(\bar{A}, r_1, \dots, r_{n+1}\right)$. In view of Lemma 15, the degrees of r_{n+1} in $\rho\,(A, r_1, \dots, r_{n+1})$ and $\rho\left(\bar{A}, r_1, \dots, r_{n+1}\right)$ are the same integer $n!$, and the coefficients of $r_{n+1}^{n!}$ are respectively $\mathcal{R}(p_1(At), \dots, p_n(At))^{n+1}$ and $\vartheta\left(\mathcal{R}(p_1(At), \dots, p_n(At))^{n+1}\right) = \mathcal{R}(p_1(\bar{A}t), \dots, p_n(\bar{A}t))^{n+1}$, the latter being non-zero as it corresponds to the statement of Lemma 15 for the special case $m = n+1$. Now suppose $\rho\,(A, r_1, \dots, r_{n+1}) = gh$ with g, h non-constant polynomials in $k[A, r]$; then $\rho\left(\bar{A}, r_1, \dots, r_{n+1}\right) = \vartheta(g)\vartheta(h)$ with $\vartheta(g), \vartheta(h) \in k[\bar{A}, r_1, \dots, r_{n+1}]$. By Lemma 19, the polynomial $\rho\left(\bar{A}, r_1, \dots, r_{n+1}\right)$ is irreducible in $k[\bar{A}, r_1, \dots, r_{n+1}]$, so we may assume that $\vartheta(g) = 1$. It follows that the degree of r_{n+1} in $\vartheta(h)$ is $n!$, whence the degree of r_{n+1} in h is $n!$ as well. In turn, this gives that g divides the coefficient of $r_{n+1}^{n!}$ in $\rho\,(A, r_1, \dots, r_{n+1})$, which by Lemma 15 is $\mathcal{R}(p_1(At), \dots, p_n(At))^{n+1} \in k[A]$. By part (2) of Proposition 13 and the construction of $\mathcal{R}(p_1(At), \dots, p_n(At))$, we have $\mathcal{R}(p_1(At), \dots, p_n(At))$ is a multi-homogeneous polynomial in the coefficients of $p_1(At), \dots, p_n(At)$ of multi-degree $(n!/1, \dots, n!/n)$. Now, the coefficients of $p_i(At)$ are homogeneous polynomials themselves in the variables A of degree i. We conclude that $\mathcal{R}(p_1(At), \dots, p_n(At))$ is a homogeneous polynomial in the variables A of total degree $nn!$. Since g divides $\mathcal{R}(p_1(At), \dots, p_n(At))^{n+1}$ it must also be homogeneous, and the fact that $\vartheta(g) = 1$ shows that g is indeed a constant polynomial. □

We have arrived at the following crucial fact:

Lemma 21. *The minimal polynomial μ_{n+1} of $p_{n+1}(Ax)$ over $\mathscr{F}_n$ is up to multiplication by an element of $\mathscr{F}_n$ equal to $\rho(A, p_1(Ax), \dots, p_n(Ax), r_{n+1})$, and thus has degree $n!$.*

Proof. By Lemma 20 and Remark 18 $\rho(A, p_1(Ax), \dots, p_n(Ax), r_{n+1})$ is irreducible as a polynomial in $k[A, p_1(Ax), \dots, p_n(Ax)][r_{n+1}]$, which is a unique factorization domain (UFD). By Gauss's lemma on irreducible polynomials over a UFD, the polynomial $\rho(A, p_1(Ax), \dots, p_n(Ax), r_{n+1})$ is also irreducible in $k(A)(p_1(Ax), \dots, p_n(Ax))[r_{n+1}] = \mathscr{F}_n[r_{n+1}]$. By Lemma 15 it has degree $n!$ in r_{n+1} and by Lemma 16 it has $p_{n+1}(Ax)$ as its root. □

We can now state and prove the main technical theorem of this paper (Theorem 2 in the introduction):

Theorem 22. *We have an equality of fields $\mathscr{F}_{n+1} = \mathscr{F}_m$.*

Proof. We have $[\mathscr{F}_m : \mathscr{F}_n] = n!$ by Proposition 9 and $[\mathscr{F}_{n+1} : \mathscr{F}_n] = n!$ by Lemma 21; since $\mathscr{F}_n \subseteq \mathscr{F}_{n+1} \subseteq \mathscr{F}_m$, we must have $\mathscr{F}_{n+1} = \mathscr{F}_m$. □

5. Proof of Theorem 1

As a corollary to Theorem 22, we now prove Theorem 1.

We have $\mathscr{F}_{n+1} = \mathscr{F}_m$ by Theorem 22 and $\mathscr{F}_m = \mathscr{E}$ by Proposition 3; that is $\mathscr{F}_{n+1} = \mathscr{E}$. Concretely, $k(A)(p_1(Ax), \dots, p_{n+1}(Ax)) = k(A)(x)$. It immediately follows from this equality that each x_i is a rational function over k in $A, p_1(Ax), \dots, p_{n+1}(Ax)$. In particular, for every $i \in [n]$, there exist polynomials

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

in $k[A][p_1(Ax), \dots, p_{n+1}(Ax)]$ such that $x_i = f_i/g_i$; in fact, since this holds for every field k of characteristic zero, one sees that $f_i, g_i \in \mathbb{Z}[A][p_1(Ax), \dots, p_n(Ax)]$.

Now let $A^* \in \bar{k}^{m\times n}$ and $x^* \in \bar{k}^n$ be generic in the sense that none of the g_i's evaluates to zero upon substitution of A and x with A^* and x^*, respectively. Suppose that $\xi \in \bar{k}^n$ is a common root of the polynomials $q_i(x) = p_i(A^*x) - p_i(A^*x^*)$, $i \in [n+1]$; that is, $p_i(A^*\xi) = p_i(A^*x^*)$ for every $i \in [n+1]$. As a consequence,

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

$\forall i \in [n]$, and thus the equality of rational functions $x_i = f_i/g_i$ gives an equality in $\bar{k}$

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

for every $i \in [n]$.

6. Examples

In this section, we illustrate Theorem 2 for $n = 1, 2$. When $n = 1$, A is a column vector of length m. Hence, for any positive integer ℓ we have $p_\ell(Ax) = p_\ell(A)x_1$; in particular $x_1 = p_1(Ax)/p_1(A)$.

When $n = 2$, the situation becomes significantly more involved. Let us write

$$p_\ell(Ax) = \sum_{j=0}^{\ell} c_{j,\ell-j} x_1^j x_2^{\ell-j},$$

where the coefficients $c_{j,\ell-j}$ are given by the binomial theorem as

$$c_{j,\ell-j} = \binom{\ell}{j} \sum_{i=1}^{m} a_{i1}^j a_{i2}^{\ell-j}.$$

By an elementary calculation, we obtain relations in the field of fractions of $k(A)[x_1, x_2]$

$$x_1 = \left[-\frac{c_{01}}{c_{10}}\right] \cdot x_2 + \left[\frac{p_1(Ax)}{c_{10}}\right] \cdot 1 \quad (*)$$

$$x_2^2 = \left[\frac{(-c_{10}c_{11} + 2c_{01}c_{20})p_1(Ax)}{c_{10}^2 c_{02} - c_{10}c_{01}c_{11} + c_{01}^2 c_{20}}\right] \cdot x_2 + \left[\frac{c_{10}^2 p_2(Ax) - c_{20}p_1(Ax)^2}{c_{10}^2 c_{02} - c_{10}c_{01}c_{11} + c_{01}^2 c_{20}}\right] \cdot 1, \quad (**)$$

where, indeed, one verifies that

$$c_{10}^2 c_{02} - c_{10}c_{01}c_{11} + c_{01}^2 c_{20} = \sum_{1 \leqslant i < j \leqslant m} (a_{i1}a_{j2} - a_{i2}a_{j1})^2 \neq 0.$$

From this it follows that the algebra $k(A)[x_1, x_2]$ is freely generated as a module over its subalgebra $k(A)[p_1(Ax), p_2(Ax)]$ by the elements 1 and x_2. Hence there exist $h_1, h_2 \in k(A)[p_1(Ax), p_2(Ax)]$ such that $p_3(Ax) = h_1 + h_2 x_2$. The calculation of h_1 and h_2 is done by first replacing x_1 in $p_3(Ax)$ by the right-hand-side of $(*)$ and then successively using $(**)$ to reduce the degree in x_2. The explicit formulas are found via the help of Maple to be

$$\begin{aligned}
h_1 =& \frac{u_1(A)p_1(Ax)^3 + u_2(A)p_2(Ax)p_1(Ax)}{c_{10}^3(c_{10}^2c_{02} - c_{10}c_{01}c_{11} + c_{01}^2c_{20})^2}\\
h_2 =& \frac{v_1(A)p_1(Ax)^2 + v_2(A)p_2(Ax)}{c_{10}^3(c_{10}^2c_{02} - c_{10}c_{01}c_{11} + c_{01}^2c_{20})^2}, \quad \text{with}\\
u_1(A) =& -6c_{01}^4c_{20}^2c_{30} + 6c_{01}^3c_{10}c_{11}c_{20}c_{30} + 4c_{01}^3c_{10}c_{20}^2c_{21} - 5c_{01}^2c_{02}c_{10}^2c_{20}c_{30}\\
& - c_{01}^2c_{10}^2c_{11}^2c_{30} - 3c_{01}^2c_{10}^2c_{11}c_{20}c_{21} - 3c_{01}^2c_{10}^2c_{12}c_{20}^2 + 2c_{01}c_{02}c_{10}^3c_{11}c_{30}\\
& + 2c_{01}c_{02}c_{10}^3c_{20}c_{21} + 2c_{01}c_{03}c_{10}^3c_{20}^2 + 2c_{01}c_{10}^3c_{11}c_{12}c_{20} - c_{02}^2c_{10}^4c_{30}\\
& - c_{02}c_{10}^4c_{12}c_{20} - c_{03}c_{10}^4c_{11}c_{20},\\
u_2(A) =& c_{10}^2(5c_{01}^4c_{20}c_{30} - 4c_{01}^3c_{10}c_{11}c_{30} - 4c_{01}^3c_{10}c_{20}c_{21} + 3c_{01}^2c_{02}c_{10}^2c_{30}\\
& + 3c_{01}^2c_{10}^2c_{11}c_{21} + 3c_{01}^2c_{10}^2c_{12}c_{20} - 2c_{01}c_{02}c_{10}^3c_{21} - 2c_{01}c_{03}c_{10}^3c_{20}\\
& - 2c_{01}c_{10}^3c_{11}c_{12} + c_{02}c_{10}^4c_{12} + c_{03}c_{10}^4c_{11}),\\
v_1(A) =& 14c_{01}^5c_{20}^2c_{30} - 20c_{01}^4c_{10}c_{11}c_{20}c_{30} - 10c_{01}^4c_{10}c_{20}^2c_{21} + 13c_{01}^3c_{02}c_{10}^2c_{20}c_{30}\\
& + 7c_{01}^3c_{10}^2c_{11}^2c_{30} + 13c_{01}^3c_{10}^2c_{11}c_{20}c_{21} + 7c_{01}^3c_{10}^2c_{12}c_{20}^2 - 9c_{01}^2c_{02}c_{10}^3c_{11}c_{30}\\
& - 7c_{01}^2c_{02}c_{10}^3c_{20}c_{21} - 5c_{01}^2c_{03}c_{10}^3c_{20}^2 - 4c_{01}^2c_{10}^3c_{11}^2c_{21} - 8c_{01}^2c_{10}^3c_{11}c_{12}c_{20}\\
& + 3c_{01}c_{02}^2c_{10}^4c_{30} + 4c_{01}c_{02}c_{10}^4c_{11}c_{21} + 3c_{01}c_{02}c_{10}^4c_{12}c_{20}\\
& + 5c_{01}c_{03}c_{10}^4c_{11}c_{20} + 2c_{01}c_{10}^4c_{11}^2c_{12} - c_{02}^2c_{10}^5c_{21} - c_{02}c_{03}c_{10}^5c_{20}\\
& - c_{02}c_{10}^5c_{11}c_{12} - c_{03}c_{10}^5c_{11}^2,\\
v_2(A) =& c_{10}^2(c_{03}c_{10}^3 - c_{01}c_{10}^2c_{12} + c_{01}^2c_{10}c_{21} - c_{01}^3c_{30})(c_{01}^2c_{20} - c_{01}c_{10}c_{11} + c_{02}c_{10}^2).
\end{aligned}$$

Moreover, one can check that $h_2 \neq 0$ using Maple, and obtain a rational expression $x_2 = (p_3(Ax) - h_1)/h_2$, which upon substitution to $(*)$ gives a rational expression of x_1 in terms of elements of $k(A)[p_1(Ax), p_2(Ax)]$.

CRediT authorship contribution statement

Hao Liang: Writing – review & editing, Writing – original draft, Validation, Methodology, Investigation, Formal analysis, Conceptualization. **Jingyu Lu:** Writing – review & editing, Writing – original draft, Validation, Software, Investigation, Formal analysis, Data curation. **Manolis C. Tsakiris:** Writing – review & editing, Supervision, Software, Methodology, Formal analysis. **Lihong Zhi:** Writing – review & editing, Validation, Supervision, Software, Resources, Project administration, Funding acquisition, Data curation.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

References

Atiyah, M.F., MacDonald, I.G., 1969. Introduction to Commutative Algebra. Addison-Wesley Series in Mathematics. CRC Press.

Abid, A., Zou, J., 2018. A stochastic expectation-maximization approach to shuffled linear regression. In: Annual Allerton Conference on Communication, Control, and Computing, pp. 470–477.

Bruns, W., Conca, A., Raicu, C., Varbaro, M., 2022. Determinants, Gröbner Bases and Cohomology. Springer.

Bruns, W., Herzog, J., 1998. Cohen-Macaulay Rings. Cambridge Studies in Advanced Mathematics, vol. 39. Cambridge University Press.

Bruns, W., Vetter, U., 1988. Determinantal Rings, vol. 1327. Springer.

Cox, D.A., Little, J., O'Shea, D., 2013. Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra. Springer Science & Business Media.

Dvornicich, R., Zannier, U., 2009. Newton functions generating symmetric fields and irreducibility of Schur polynomials. Adv. Math. 222 (6), 1982–2003.

Elhami, G., Scholefield, A., Béjar Haro, B., Vetterli, M., 2017. Unlabeled sensing: reconstruction algorithm and theoretical guarantees. In: IEEE International Conference on Acoustics, Speech and Signal Processing, pp. 4566–4570.

Foulkes, H.O., 1956. Theorems of Kakeya and Pólya on power-sums. Math. Z. 65, 345–352.

Gelfand, I.M., Kapranov, M.M., Zelevinsky, A.V., 1994. Discriminants, Resultants, and Multidimensional Determinants. Birkhäuser, Boston, MA.

Hartshorne, R., 1966. A property of A-sequences. Bull. Soc. Math. Fr. 94, 61–65.

Hsu, D., Shi, K., Sun, X., 2017. Linear regression without correspondence. Adv. Neural Inf. Process. Syst. 30.

Kakeya, S., 1927. On fundamental systems of symmetric functions-II. Jpn. J. Math. 4, 77–85.

Lang, S., 2012. Algebra, vol. 211. Springer Science & Business Media.

Li, F., Fujiwara, K., Okura, F., Matsushita, Y., 2023. Shuffled linear regression with outliers in both covariates and responses. Int. J. Comput. Vis. 131 (3), 732–751.

Liang, H., Lu, J., Tsakiris, M.C., Zhi, L., 2024. Unlabeled sensing using rank-one moment matrix completion. In: ISSAC '24: Proceedings of the 2024 International Symposium on Symbolic and Algebraic Computation, pp. 46–55.

Macaulay, F.S., 1916. The Algebraic Theory of Modular Systems. Cambridge Tracts in Mathematics and Mathematical Physics. Cambridge University Press, Cambridge.

Matsumura, H., 1989. Commutative Ring Theory. Cambridge Studies in Advanced Mathematics, vol. 8. Cambridge University Press.

Ma, R., Cai, T.T., Li, H., 2021. Optimal estimation of bacterial growth rates based on a permuted monotone matrix. Biometrika 108 (3), 693–708.

Melánová, H., Sturmfels, B., Winter, R., 2022. Recovery from power sums. Exp. Math., 1–10.

Nakamura, K., 1927. On the representation of symmetric functions by power-sums which form the fundamental system. Jpn. J. Math. 4, 87–92.

Nejatbakhsh, A., Varol, E., 2021. Neuron matching in C. elegans with robust approximate linear regression without correspondence. In: Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision, pp. 2837–2846.

Peng, L., Tsakiris, M.C., 2020. Linear regression without correspondences via concave minimization. IEEE Signal Process. Lett. 27, 1580–1584.

Peng, L., Tsakiris, M.C., 2021. Homomorphic sensing of subspace arrangements. Appl. Comput. Harmon. Anal. 55, 466–485.

Pananjady, A., Wainwright, M.J., Courtade, T.A., 2018. Linear regression with shuffled data: statistical and computational limits of permutation recovery. IEEE Trans. Inf. Theory 64 (5), 3286–3300.

Slawski, M., Ben-David, E., 2019. Linear regression with sparsely permuted data. Electron. J. Stat. 13 (1), 1–36.

Slawski, M., Ben-David, E., Li, P., 2020. Two-stage approach to multivariate linear regression with sparsely mismatched data. J. Mach. Learn. Res. 21 (204), 1–42.

Song, X., Choi, H., Shi, Y., 2018. Permuted linear model for header-free communication via symmetric polynomials. In: IEEE International Symposium on Information Theory, pp. 661–665.

Tsakiris, M.C., Peng, L., 2019. Homomorphic sensing. In: International Conference on Machine Learning, pp. 6335–6344.

Tsakiris, M.C., Peng, L., Conca, A., Kneip, L., Shi, Y., Choi, H., 2020. An algebraic-geometric approach for linear regression without correspondences. IEEE Trans. Inf. Theory 66 (8), 5130–5144.

Tsakiris, M.C., 2023a. Determinantal conditions for homomorphic sensing. Linear Algebra Appl. 656, 210–223.

Tsakiris, M.C., 2023b. Matrix recovery from permutations: an algebraic geometry approach. In: IEEE International Symposium on Information Theory (ISIT). IEEE, pp. 2511–2516.

Unnikrishnan, J., Haghighatshoar, S., Vetterli, M., 2015. Unlabeled sensing: solving a linear system with unordered measurements. In: Annual Allerton Conference on Communication, Control, and Computing, pp. 786–793.

Unnikrishnan, J., Haghighatshoar, S., Vetterli, M., 2018. Unlabeled sensing with random linear measurements. IEEE Trans. Inf. Theory 64 (5), 3237–3253.

van der Waerden, B.L., 1950. Modern Algebra II, 1 edition. Frederick Ungar.

Yao, Y., Peng, L., Tsakiris, M.C., 2021. Unlabeled principal component analysis. Adv. Neural Inf. Process. Syst. 34, 30452–30464.

Yao, Y., Peng, L., Tsakiris, M.C., 2024. Unlabeled principal component analysis and matrix completion. J. Mach. Learn. Res. 25 (77), 1–38.

Zhang, H., Slawski, M., Li, P., 2021. The benefits of diversity: permutation recovery in unlabeled sensing from multiple measurement vectors. IEEE Trans. Inf. Theory 68 (4), 2509–2529.