Eigenspace conditions for homomorphic sensing

Manolis C. Tsakiris
School of Information Science and Technology, ShanghaiTech University, Shanghai, China

Abstract
Given two endomorphisms $\tau_1, \tau_2$ of $\mathbb{C}^m$, we provide eigenspace conditions under which $\tau_1(v_1) = \tau_2(v_2)$ for $v_1, v_2 \in V$ can only be true if $v_1 = v_2$, where $V$ is a general $n$-dimensional subspace of $\mathbb{C}^m$ for some $n \leq m/2$. As a special case, we show that these eigenspace conditions are true when the endomorphisms are permutations composed with coordinate projections, leading to an abstract proof of the recent unlabeled sensing theorem of [22].

Keywords: Homomorphic sensing, unlabeled sensing, shuffled linear regression, Jordan form, determinantal varieties, rational normal scroll

1. Introduction

In a fascinating line of research termed unlabeled sensing, it has been recently established that uniquely recovering a signal from shuffled and subsampled measurements is possible as long as the number of measurements is at least twice the intrinsic dimension of the signal [22]. In abstract terms, the result of [22] says that if $V$ is a general $n$-dimensional linear subspace of $\mathbb{C}^m$, for some $m \geq 2n$, $\pi_1, \pi_2$ permutations on the $m$ coordinates of $\mathbb{C}^m$ and $\rho_1, \rho_2$ coordinate projections viewed as endomorphisms, then $\rho_1 \pi_1(v_1) = \rho_2 \pi_2(v_2)$ for $v_1, v_2 \in V$ only if $v_1 = v_2$, provided that each of $\rho_1, \rho_2$ preserves at least $2n$ coordinates. Unlabeled sensing is in fact an even more challenging version of the already NP-hard problem of shuffled linear regression [21, 12, 11, 1, 13, 2, 16, 9, 18, 15], in which one aims at determining $v \in V$ from the data $\pi(v), V$, where $\pi$ is some unknown permutation. Interestingly, it has recently been shown that this can be done in linear complexity in terms of $m$ (but still exponential in $n$) by means of symmetric polynomials, resulting in Groebner basis based algorithms that are efficient for $n \leq 5$ and remain stable under small levels of noise [18]. Inspired by unlabeled sensing, in this paper we study the problem of homomorphic sensing, which in its simplest form can be stated as follows: given two endomorphisms $\tau_1, \tau_2$ of $\mathbb{C}^m$ and a general subspace $V$ of dimension $n$, under what conditions does the implication $\tau_1(v_1) = \tau_2(v_2) \Rightarrow v_1 = v_2$ hold true, whenever $v_1, v_2 \in V$?
2. Conventions

We adopt the language of abstract linear algebra and algebraic geometry, and refer the reader to [14] for the former and [6,14,18] for the latter. The reader not familiar with algebraic geometry is further referred to [13,19,20] for concise yet rigorous reviews of basic algebraic geometric notions in the context of machine learning problems, especially [18] for the notion of dimension of algebraic varieties and genericity.

We work over the field \( \mathbb{C} \) of complex numbers; an essential choice for the validity of our eigenspace conditions. If one is interested only in real vector spaces \( \mathcal{V} \), our results still hold in that case, assuming one computes the eigenspaces and their dimension over \( \mathbb{R} \). For an endomorphism \( \tau \) of a finite-dimensional vector space \( \mathcal{U} \), we denote by \( \mathcal{E}_{\tau,\lambda} \) the eigenspace of \( \tau \) corresponding to eigenvalue \( \lambda \), i.e., the set of all vectors \( v \in \mathcal{U} \) such that \( \tau(v) = \lambda v \). For two endomorphisms \( \tau_1, \tau_2 \) of \( \mathcal{U} \), \( \mathcal{E}_{(\tau_1,\tau_2),\lambda} \) denotes the corresponding eigenspace of the generalized eigenvalue problem \( \tau_1(v) = \lambda \tau_2(v) \). Given an endomorphism \( \tau \) of a vector space \( \mathcal{U} \) with eigenvalues \( \lambda_1, \ldots, \lambda_s \), \( \mathcal{U} \) admits a decomposition \( \mathcal{U} = \bigoplus_{k,i} \mathcal{C}_{k,\lambda_i} \) into \( \tau \)-invariant cyclic subspaces whose annihilators are generated by the elementary divisors of \( \tau \). Thus each \( \mathcal{C}_{k,\lambda_i} \) admits a basis \( w_1, \ldots, w_{d_{k,i}} \), where \( d_{k,i} \) is the dimension of \( \mathcal{C}_{k,\lambda_i} \), such that \( \tau(w_1) = \lambda_i w_1 \) and \( \tau(w_j) = \lambda_i w_j + w_{j-1}, \forall j = 2, \ldots, d_{k,i} \). Represented on this basis, the restriction of \( \tau \) on \( \mathcal{C}_{k,\lambda_i} \) is given by a Jordan block of size \( d_{k,i} \times d_{k,i} \) and of eigenvalue \( \lambda_i \). We refer to such a basis as a Jordan basis. By a projection \( \rho \) of \( \mathcal{U} \) we always mean an idempotent endomorphism. A coordinate projection is a projection that sets to zero a subset of the entries of every vector in \( \mathbb{C}^m \), and its rank is the number of entries that are preserved. A signed coordinate projection is a coordinate projection composed with a diagonal matrix whose diagonal entries take values in \( \{1,-1\} \).

By an algebraic variety or simply variety we mean the zero locus of a collection of polynomials with coefficients in \( \mathbb{C} \). If \( \mathcal{Y} \) is a variety \( \dim \mathcal{Y} \) denotes the affine dimension of \( \mathcal{Y} \). If \( \mathcal{R} \) is a ring \( \dim \mathcal{R} \) denotes the Krull dimension of \( \mathcal{R} \). If \( \mathcal{I} \) is an ideal of a polynomial ring \( \mathcal{R} \) over \( \mathbb{C} \), \( \codim \mathcal{I} \) denotes the height of the ideal \( \mathcal{I} \), and it is equal to \( \dim \mathcal{R} - \dim \mathcal{R}/\mathcal{I} \). By a general subspace \( \mathcal{V} \) of \( \mathbb{C}^m \) of dimension \( n \), we mean a non-empty open set in the Zariski topology of the Grassmannian variety of \( n \)-dimensional linear subspaces of \( \mathbb{C}^m \). For \( s \) an integer \([s]\) denotes the set \( \{1, \ldots, s\} \). A quasi-variety is an open subset of a variety. For \( I \subset [m] \) and \( A \) an \( m \times k \) matrix where \( k \) is any integer, \( A_I \) denotes the \((\#I) \times k\) row submatrix of \( A \) obtained by selecting the rows with index in \( I \), \( \#I \) denoting the cardinality of \( I \). For a real number \( \alpha \) we denote by \([\alpha]\) the largest integer smaller than \( \alpha \).

3. Main results

We need the following quasi-variety. For endomorphisms \( \tau_1, \tau_2 \) of \( \mathbb{C}^m \) let \( \rho \) be a projection onto \( \text{im}(\tau_2) \). Let \( \mathcal{Y}_{\rho \tau_1, \tau_2} \) be the set of all \( w \in \mathbb{C}^m \) for which \( \rho \tau_1(w), \tau_2(w) \) are linearly dependent. This is a determinantal variety defined by the vanishing of the \( 2 \times 2 \) minors of the matrix \( [\rho \tau_1(w), \tau_2(w)] \). In fact \( \mathcal{Y}_{\rho \tau_1, \tau_2} \) is the union of all generalized eigenspaces of the endomorphism pairs \( (\rho \tau_1, \tau_2) \) and \( (\tau_2, \rho \tau_1) \). Our quasi-variety is the complement in \( \mathcal{Y}_{\rho \tau_1, \tau_2} \) of the generalized eigenspaces corresponding to eigenvalues \( 0, 1 \): \( \mathcal{U}_{\rho \tau_1, \tau_2} = \mathcal{Y}_{\rho \tau_1, \tau_2} \setminus \ker(\rho \tau_1) \cup \ker(\tau_2) \cup \ker(\rho \tau_1 - \tau_2) \).
The main result of this paper reads:

**Theorem 1.** Let $\tau_1, \tau_2$ be endomorphisms of $\mathbb{C}^m$ with $\dim(\ker(\tau_1)) \leq m - n$ and $\dim(\im(\tau_2)) \geq 2n$, for some $n \leq m/2$. Let $\rho$ be any projection onto $\im(\tau_2)$. If $\dim(U_{\rho, \tau_1, \tau_2} \leq m - n$, then the following is true for a general $n$-dimensional subspace $V$ of $\mathbb{C}^m$: if $\tau_1(v_1) = \tau_2(v_2)$ with $v_1, v_2 \in V$, then $v_1 = v_2$.

Our second result shows that the eigenspace hypothesis of Theorem 1 is true for the special case of permutations composed with coordinate projections:

**Theorem 2.** Let $\pi_1, \pi_2$ be permutations on the $m$ coordinates of $\mathbb{C}^m$, and $\rho_1, \rho_2$ coordinate projections. Then $\dim(U_{\rho_1, \pi_1, \rho_2, \pi_2} \leq m - \lfloor \rank(\rho_2)/2 \rfloor$.

Using Theorems 1, 2 one obtains a generalization of the main theorem of [22]. The generalization consists in allowing one of the projections to preserve at least $n$ coordinates (and not $2n$ for both projections as in [22]) as well as considering sign changes:

**Theorem 3.** Let $\mathcal{P}_m$ be the group of permutations on the $m$ coordinates of $\mathbb{C}^m$, and $\mathcal{A}_n, \mathcal{A}_{2n}, \mathcal{J}_n, \mathcal{J}_{2n}$ the set of all coordinate projections ($\mathcal{A}_n$, $\mathcal{A}_{2n}$) and signed coordinate projections ($\mathcal{J}_n$, $\mathcal{J}_{2n}$) of $\mathbb{C}^m$, which preserve at least $n$ and $2n$ coordinates respectively, for some $n \leq m/2$. Then the following is true for a general $n$-dimensional subspace $V$: if $\rho_1 \pi_1(v_1) = \rho_2 \pi_2(v_2)$ for $v_1, v_2 \in V$ with $\rho_1, \rho_2 \in \mathcal{J}_{2n}$, $\pi_1, \pi_2 \in \mathcal{A}_n$, then $v_1 = v_2$ or $v_1 = -v_2$. Moreover, if $\rho_1 \in \mathcal{A}_n$ and $\rho_2 \in \mathcal{A}_{2n}$, then $v_1 = v_2$.

**Remark 1.** The proof given in [22] is in its essence algebraic geometric as well, yet different from our approach. It amounts to showing that certain determinants are non-zero by constructing suitable non-zero evaluations over a set of finitely many different possibilities. We also point out that the notion of cycle used in [22] is less standard than the one we use in this paper; the latter being that of a cyclic permutation.

**Remark 2.** The work of [7], which independently appeared online three days before the submission of the first version of the present manuscript, presented an eigenvalue condition of similar flavor as in Theorem 1 for the simpler case of invertible and diagonalizable endomorphisms.

**Remark 3.** The results of this paper substantiate the technical part of the expository paper [17], written for a computer science audience. The reader may also find there an application of these notions to the computer vision problem of image registration.

4. Proof of Theorem 1

The proof relies on two devices. The first one, given in Proposition 1 and proved in 4.1, gives eigenvalue conditions for a single endomorphism. The second device consists of reducing the case of two endomorphisms $\tau_1, \tau_2$ to the case of a single endomorphism $\tau$ and applying Proposition 1.

**Proposition 1.** Let $U$ be a vector space of dimension $m \geq 2n$ and $\tau$ an endomorphism such that $\dim(E_{\tau, \lambda} \leq m - n$. Then the following is true for a general $n$-dimensional subspace $V$: if $\tau(v_1) = v_2$ with $v_1, v_2 \in V$, then $v_1 = v_2$. 
Let $k = \dim(\im(\tau_2))$. Since $V$ is a general $n$-dimensional subspace of $C^m$, we may as well view $V$ as a general $n$-dimensional subspace of a general $k$-dimensional subspace $H$ of $C^m$. Hence $\tau_1(v_1) = \tau_2(v_2)$ for $v_1, v_2 \in V$ implies $\tau_1|_H(v_1) = \tau_2|_H(v_2)$. This further implies $\rho\tau_1|_H(v_1) = \tau_2|_H(v_2)$, where $\rho$ is the given projection onto $\im(\tau_2)$. Since $H$ is general we have $H \cap \ker(\tau_2) = 0$ and so $\tau_2|_H$ establishes an isomorphism between $H$ and $\im(\tau_2)$. We denote by $(\tau_2|_H)^{-1} : \im(\tau_2) \to H$ the inverse of $\tau_2|_H$. Then $\tau_1(v_1) = \tau_2(v_2)$ implies $(\tau_2|_H)^{-1}\rho\tau_1|_H(v_1) = v_2$, and as per Proposition 1 we are done if $\dim E_{\tau_1, \lambda} \leq k - n$, where $\tau_1$ is the endomorphism of $H$ given by $(\tau_2|_H)^{-1}\rho\tau_1|_H$. Let $(y, \lambda)$ be an eigenpair of $\tau_1$; then $(\tau_2|_H)^{-1}\rho\tau_1|_H(y) = \lambda y$ and applying $\tau_2$ on both sides gives $\tau_2(\tau_2|_H)^{-1}\rho\tau_1|_H(y) = \lambda\tau_2(y)$. Clearly, $\tau_2(\tau_2|_H)^{-1}\rho = \rho$ whence $\rho\tau_1|_H(y) = \lambda\tau_2(y)$ or $\rho\tau_1(y) = \lambda\tau_2(y)$. In other words, the eigenpair $(y, \lambda)$ of $\tau_1$ is a generalized eigenpair for $(\rho\tau_1, \tau_2)$ and $E_{\tau_1, \lambda}$ is isomorphic to $E_{(\rho\tau_1, \tau_2), \lambda} \cap H$ via $\tau_2|_H$. Consequently, we are done if we can show that $\dim E_{(\rho\tau_1, \tau_2), \lambda} \cap H \leq k - n$. If $\dim E_{(\rho\tau_1, \tau_2), 0} \leq m - n$, we are done because $H$ is general of dimension $k$, thus $H$ intersects $U_{\rho\tau_1, \tau_2}$ at most at dimension $[(m - n) + k] - m = k - n$. If on the other hand $\dim E_{(\rho\tau_1, \tau_2), 0} = \dim \ker(\rho\tau_1) \geq m - n$, then $\im(\tau_2)$ will intersect any complement $C$ of $\im(\rho\tau_1)$ at dimension at least $[(m - n) + k] - m = k - n \geq n$. Let $\sigma$ be the projection onto $C \cap \im(\tau_2)$ along any complement that contains $\im(\rho\tau_1)$. Applying $\sigma$ on both sides of $\rho\tau_1(v_1) = \tau_2(v_2)$ gives $0 = \sigma\tau_2(v_2)$, i.e., $v_2 \in \ker(\sigma\tau_2)$. Since the codimension of the kernel of $\sigma\tau_2$ is at least $n$ and $\im(\sigma\tau_2)$ is general of dimension $n$, we must have $V \subseteq \ker(\sigma\tau_2)$, so that $v_2 = 0$. Then $\tau_1(v_1) = \tau_2(v_2)$ gives $\tau_1(v_1) = 0$, whence $v_1 = 0$ since by hypothesis the codimension of the kernel of $\tau_1$ is at least $n$.

4.1. Proof of Proposition 1

We prove the proposition in several stages, starting with the boundary situation described in the next lemma.

Lemma 1. Let $U$ be a vector space of dimension $2n$. Let $\tau$ be an endomorphism of $U$ such that $\dim E_{\tau, \lambda} = n$ for some eigenvalue $\lambda$ of $\tau$. Then there exists an $n$-dimensional subspace $V$ such that $U = V \oplus \tau(V)$.

Proof. Let $\lambda_1, \ldots, \lambda_n$ be the spectrum of $\tau$ and suppose that $\lambda_1 = \lambda$ is the said eigenvalue. Then there are exactly $n$ $\tau$-cyclic subspaces $C_1, \lambda_1, \ldots, C_n, \lambda_n$ associated to $\lambda_1$ each of them contributing a single eigenvector. If $u_1, \ldots, u_d$, is a fixed Jordan basis for $C_{k, \lambda_1}$, we let $v_1 = w_1$ be that eigenvector. We produce $n$ linearly independent vectors $u_1, \ldots, u_n$ to be taken as a basis for the claimed subspace $V$, by summing pairwise the $v_1, \ldots, v_n$ with the remaining Jordan basis vectors across all $C_{k, \lambda_i}$.

First, suppose that all $C_{k, \lambda_i}$ are 1-dimensional. Then $C_{1, \lambda_2}$ is a non-trivial subspace with Jordan basis $w_1, \ldots, w_d$, for some $d \geq 1$. We construct the first $d$ basis vectors $u_1, \ldots, u_d$ for $V$ as $u_j = v_j + w_j, \ j \in [d]$. A forward induction on the relations

$$\tau u_1 = \lambda_1 v_1 + \lambda_2 w_1; \ \tau u_2 = \lambda_1 v_2 + \lambda_2 w_j + w_{j-1}; \ \forall j = 2, \ldots, d,$$

together with $\lambda_1 \neq \lambda_2$, gives $\Span(u_1, \tau u_1, \ldots, u_d, \tau u_d) = (\oplus_{k \in [d]} C_{k, \lambda_1}) \oplus C_{1, \lambda_2}$. If $d = n$ we are done, otherwise either $C_{2, \lambda_2}$ or $C_{1, \lambda_3}$ is a non-trivial subspace and we inductively repeat the argument above until all $C_{k, \lambda_i}$ for $i > 1$ are exhausted.
Next, suppose that not all $C_{k, \lambda_1}$ are 1-dimensional. We may assume that there exists integer $0 \leq r < n$ such that $\dim C_{j, \lambda_1} = 1$ for every $j \leq r$ and $\dim C_{j, \lambda_1} = d_j > 1$ for every $j > r$. If $r = 0$, then each $C_{k, \lambda_1}$ is necessarily 2-dimensional and $\tau$ has only one eigenvalue $\lambda_1$. Letting $w_{1,k}, w_{2,k}$ be the Jordan basis for $C_{k, \lambda_1}$, we define $u_k = w_{2,k}, \forall k \in [n]$. Clearly, $\text{Span}(u_k, \tau u_k) = \text{Span}(w_{1,k}, w_{2,k})$, in which case $\text{Span} (\{ u_k, \tau u_k \}_{k=1}^n) = \bigoplus_{k=1}^n C_{k, \lambda_1} = \mathcal{U}$. So suppose $1 \leq r < n$. Let $w_1, \ldots, w_{d_{r+1}}$ be the Jordan basis for $C_{r+1, \lambda_1}$. Since

$$2(n - r - 1) \leq \dim \bigoplus_{k=r+2}^n C_{k, \lambda_1} \leq \text{codim} \bigoplus_{k=1}^{r+1} C_{k, \lambda_1} = 2n - r - d_{r+1},$$

we must have $d_{r+1} - 2 \leq r$. We may then assume that $w_1 = v_{r+1}$ and define $u_1 = v_{r+1} + w_{d_{r+1}}$ and $u_j = \tau u_{j-1} + w_j$, $j = 2, \ldots, d_{r+1} - 1$. Noting that \( \{ w_j : j \in [d_{r+1} - 1] \} = \{ \tau u_j - \lambda u_j : j \in [d_{r+1} - 1] \} \), we have

$$V' = \text{Span} (\{ u_j, \tau u_j \}_{j=1}^{d_{r+1}-1}) = \left( \bigoplus_{k=1}^{d_{r+1}-2} C_{k, \lambda_1} \right) \bigoplus C_{r+1, \lambda_1}.$$  

If $r = n - 1$, we have found a $(d_n - 1)$-dimensional subspace $V'$ such that $V' + \tau(V') = \bigoplus_{k=1}^d C_{k, \lambda_1}$. Otherwise if $r < n - 1$, $C_{r+2, \lambda_1}$ is a nontrivial subspace of dimension $d_{r+2} \geq 2$, which must satisfy

$$r + d_{r+1} + d_{r+2} + 2(n - r - 2) \leq 2n \iff d_{r+2} - 2 \leq r - (d_{r+1} - 2).$$

Letting $w_1, \ldots, w_{d_{r+2}}$ be the Jordan basis for $C_{r+2, \lambda_1}$ and recalling the convention $v_{r+1} = w_1$, we define $u_{d_{r+1}}, \ldots, u_{d_{r+2} + d_{r+2} - 2}$ as

$$u_{d_{r+1}} = v_{r+2} + w_{d_{r+2}}, \quad u_{d_{r+1} - 2 + j} = v_{d_{r+1} - 2 + j} + w_j, \quad \forall j = 2, \ldots, d_{r+2} - 1.$$  

Then one verifies that

$$\text{Span} (\{ u_{d_{r+1} - 2 + j} + \tau u_{d_{r+1} - 2 + j} \}_{j=1}^{d_{r+2} - 1}) = \left( \bigoplus_{k=1}^{d_{r+2} - 2} C_{d_{r+1} - 2 + k, \lambda_1} \right) \bigoplus C_{r+2, \lambda_1},$$

and in particular

$$\text{Span} (\{ u_j, \tau u_j \}_{j=1}^{d_{r+1} + d_{r+2} - 2}) = \left( \bigoplus_{k=1}^{d_{r+1} + d_{r+2} - 2} C_{k, \lambda_1} \right) \bigoplus \left( C_{r+1, \lambda_1} \bigoplus C_{r+2, \lambda_1} \right).$$

Continuing inductively like this we exhaust all higher-dimensional subspaces associated to $\lambda_1$, and obtain $V' = \text{Span} (\{ u_j : j = 1, \ldots, \sum_{k=1}^n d_k - n \})$ such that

$$V' + \tau(V') = \left( \bigoplus_{k=1}^{n-r} C_{k, \lambda_1} \right) \bigoplus \left( \bigoplus_{k=1}^{n-r} C_{r+k, \lambda_1} \right),$$

with $\sum_{j=1}^{n-r} (d_{r+j} - 2) \leq r$. If equality is achieved, then $s = 1$ and we are done. Otherwise, $\dim \bigoplus_{k \geq 1} C_{k, \lambda_1} = r - \sum_{j=1}^{n-r} (d_{r+j} - 2) =: \alpha$ and this is precisely the number of 1-dimensional subspaces associated to $\lambda_1$ that have not been used so far.
Letting $\xi_1, \ldots, \xi_\alpha$ be the union of all the Jordan basis of all $C_{k, \lambda_i}$ for $i > 1$, we define the remaining $\alpha$ basis vectors of $V$ as $u_{n-\alpha+j} = v_{\alpha-\alpha+j} + \xi_j$, for $j \in [\alpha]$, and since
\[
\text{Span} \left( \{u_{n-\alpha+j}, \tau(u_{n-\alpha+j})\}_{j=1}^{\alpha} \right) = \left( \bigoplus_{j=1}^{\alpha} C_{\alpha+j, \lambda_1} \right) \bigoplus \left( \bigoplus_{k,i>1} C_{k, \lambda_i} \right),
\]
the proof is complete. $\square$

We now use Lemma 1 to get a stronger statement for eigenspace dimensions less than or equal to half of the ambient dimension.

**Lemma 2.** Let $U$ be a vector space of dimension $2n$. Let $\tau$ be an endomorphism of $U$ such that $\dim \mathcal{E}_{\tau, \lambda} \leq n$ for every eigenvalue $\lambda$ of $\tau$. Then there exists an $n$-dimensional subspace $V$ such that $U = V \oplus \tau(V)$.

**Proof.** Let $\lambda_1, \ldots, \lambda_s$ be the eigenvalues of $\tau$ and proceed by induction on $n$. For $n = 1$ we have $s \leq 2$ and $\dim \mathcal{E}_{\tau, \lambda_i} = 1$, whence the claim follows from Lemma 1. So let $n > 1$. If $\dim \mathcal{E}_{\tau, \lambda_i} = n$ for some $i$, then we are done by Lemma 1. Hence suppose throughout that $\dim \mathcal{E}_{\tau, \lambda_i} < n$, $\forall i \in [s]$. Since the induction hypothesis applied on any $(2n-1)$-dimensional $\tau$-invariant subspace $S$ furnishes an $(n-1)$-dimensional subspace $V' \subset S$ such that $V' \oplus \tau(V') = S$, our strategy is to suitably select $S$ so that for a 2-dimensional complement $T$ there is a vector $u \in T$ such that $\text{Span}(u, \tau(u)) = T$. Then we can take $V = V' + \text{Span}(u)$.

If there are two 1-dimensional subspaces $C_{1, \lambda_1}, C_{1, \lambda_2}$ spanned by $v_1, v_2$ respectively, we let $S = \bigoplus_{(k,i) \neq (1,1),(1,2)} C_{k, \lambda_i}$ and $u = v_1 + v_2$. So suppose that there is at most one eigenvalue, say $\lambda_1$, that possibly contributes 1-dimensional subspaces $C_{k, \lambda_1}$ for some $k$. In that case, there exist $k', i'$ such that $d := \dim C_{k', \lambda_{i'}} > 1$. Let $w_1, \ldots, w_d$ be a Jordan basis for $C_{k', \lambda_{i'}}$. Define the $\tau$-invariant subspace $C_{k, \lambda_i} = \text{Span}(w_1, \ldots, w_{d-2})$, which is taken to be the zero subspace if $d = 2$. Then we let $S = \left( \bigoplus_{(k,i) \neq (k',i')} C_{k, \lambda_i} \right) \bigoplus C_{k, \lambda_{i'}}$ and $u = w_d$. $\square$

We take one step further by allowing ambient dimensions larger than $2n$.

**Lemma 3.** Let $U$ be a vector space of dimension $m \geq 2n$. Let $\tau$ be an endomorphism of $U$ such that $\dim \mathcal{E}_{\tau, \lambda} \leq m - n$ for every eigenvalue $\lambda$ of $\tau$. Then there exists an $n$-dimensional subspace $V$ such that $\dim(V + \tau(V)) = 2n$.

**Proof.** Let $U = \bigoplus_{k,i} C_{k, \lambda_i}$ be the decomposition of $U$ into $\tau$-cyclic subspaces. The strategy of the proof is to find a 2$n$-dimensional $\tau$-invariant subspace $S \subset U$ for which $\dim \mathcal{E}_{\tau, \lambda_i} \leq n$; then the claim will follow from Lemma 2. We obtain $S$ by suitably truncating the $C_{k, \lambda_i}$. We proceed by induction on $\mu = \max_i \dim \mathcal{E}_{\tau, \lambda_i}$. If $\mu = 1$ then $\tau$ has $m$ distinct eigenvalues and we may take $S = \bigoplus_{i=1}^{2n} C_{1, \lambda_i}$. Suppose that $1 < \mu \leq n$. If there is some $C_{k', \lambda_{i'}}$ with $d = \dim C_{k', \lambda_{i'}} \geq c$, let $w_1, \ldots, w_d$ be a Jordan basis for $C_{k', \lambda_{i'}}$ and take $S = \left( \bigoplus_{(k,i) \neq (k',i')} C_{k, \lambda_i} \right) \bigoplus \text{Span}(w_1, \ldots, w_{d-c})$. Otherwise, let $t > 1$ be the smallest number of subspaces $C_{k_1, \lambda_{i_1}}, \ldots, C_{k_t, \lambda_{i_t}}$ for which $\dim \bigoplus_{j=1}^{t} C_{k_j, \lambda_{i_j}} = c + \ell$ for some $\ell \geq 0$. Then by the minimality of $t$ we must have
that \( \dim \mathcal{C}_{k_1, \lambda_1} \geq \ell \). Now replace \( \mathcal{C}_{k_1, \lambda_1} \) by an \( \ell \)-dimensional \( \tau \)-invariant subspace \( \tilde{\mathcal{C}}_{k_1, \lambda_1} \) obtained as the span of the first \( \ell \) vectors of a Jordan basis of \( \mathcal{C}_{k_1, \lambda_1} \), and take \( \mathcal{S} = \left( \bigoplus_{(k,i) \neq (k_j, \lambda_j), j \in [\ell]} \mathcal{C}_{k, \lambda} \right) \oplus \tilde{\mathcal{C}}_{k_1, \lambda_1} \).

Next, suppose that \( \mu > n \) and we may assume that \( \dim \mathcal{E}_{\tau, \lambda_1} = \mu = n + c_1 \) with \( 0 < c_1 \leq c \). We first treat the case \( c_1 = c \). In such a case \( \dim \mathcal{E}_{\tau, \lambda_1} \leq n \) for any \( i > 1 \). Let \( \Sigma \) be the number of 1-dimensional \( \mathcal{C}_{k, \lambda_1} \), say \( \mathcal{C}_{1, \lambda_1}, \ldots, \mathcal{C}_{1, \lambda_1} \). Then we must have that \( \Sigma + 2(n + c - \Sigma) \leq 2n + c \) and we can take \( \mathcal{S} = \left( \bigoplus_{k=1}^{n+c} \mathcal{C}_{k, \lambda_1} \right) \oplus \left( \bigoplus_{k=1}^{\Sigma} \mathcal{C}_{k, \lambda_1} \right) \). Next, suppose that \( c_1 < c \). If \( \dim \mathcal{C}_{k, \lambda_1} = 1 \) for every \( k, i \), then there are \( n + c - c_1 \) 1-dimensional subspaces associated to eigenvalues other than \( \lambda_1 \). In that case we can take \( \mathcal{S} \) to be the sum of \( n \) subspaces associated to \( \lambda_1 \) and any other subspaces associated to eigenvalues different than \( \lambda_1 \). If on the other hand \( \dim \mathcal{C}_{k, \lambda_1} > 1 \) for some \( k, i \), then we replace \( \mathcal{U} \) by \( \mathcal{U}_1 \), the latter being the sum of all cyclic subspaces with the exception that \( \mathcal{C}_{k, \lambda_1} \) has been replaced by a \( \tau \)-cyclic subspace \( \tilde{\mathcal{C}}_{k, \lambda_1} \) of dimension one less. Notice that this replacement does not change \( \mu \). If \( c - 1 = c_1 \) or all cyclic subspaces of \( \mathcal{U}_1 \) are 1-dimensional, we are done by proceeding as above. If on the other hand \( c - 1 > c_1 \) and there is a cyclic subspace \( \mathcal{C} \) of \( \mathcal{U}_1 \) of dimension larger than one, then replace \( \mathcal{U}_1 \) by \( \mathcal{U}_2 \), where the latter is the sum of all \( \tau \)-cyclic subspaces of \( \mathcal{U}_1 \) except the said subspace \( \mathcal{C} \), which is replaced by a \( \tau \)-cyclic subspace of \( \mathcal{C} \) of dimension one less. Continuing inductively like this furnishes \( \mathcal{S} \).  

We are now in a position to complete the proof of Proposition 1. Suppose first that \( \dim \mathcal{E}_{\tau, 1} \leq n - n \). Then for any \( n \)-dimensional \( \mathcal{V} \) we have \( \dim (\mathcal{V} + \tau(\mathcal{V})) \leq 2n \), with equality on an open set \( \mathcal{W}_1 \) which is not empty as per Lemma 3. Hence for every \( \mathcal{V} \in \mathcal{W}_1 \) we have \( \mathcal{V} \cap \tau(\mathcal{V}) = 0 \), so that \( \tau(v_1) = v_2 \) gives \( v_2 = 0 \) and \( v_1 \in \ker(\tau) \). Then on a non-empty set \( \mathcal{W}_2 \) \( \mathcal{V} \) does not intersect \( \ker(\tau) \) so that for every \( \mathcal{V} \in \mathcal{W}_1 \setminus \mathcal{W}_2 \) we must have \( v_1 = v_2 = 0 \). Next, suppose that \( \dim \mathcal{E}_{\tau, 1} \geq n \). Working on a basis on which the matrix representation of \( \tau \) is in Jordan canonical form \( J \in \mathbb{C}^{m \times m} \), the relation \( \tau(v_1) = v_2 \) can be written as \( JA_1 = A_2 \), where \( A \in \mathbb{C}^{m \times n} \) is a matrix containing in its columns the representation of a basis of \( \mathcal{V} \), and \( A_1 \) is the representation of \( v_1 \). Since \( \dim \mathcal{E}_{\tau, 1} \geq n \), there are at least \( n \) Jordan blocks in \( J \) associated to eigenvalue 1, so that there are indices \( i_1, \ldots, i_n \) for which the \( i_k \) row of \( J \) is the vector \( e_i \) of all zeros except \( a_1 \) at position \( i_k \). Letting \( A_{i_1, \ldots, i_n} \in \mathbb{C}^{n \times n} \) be the row submatrix of \( A \) indexed by rows \( i_1, \ldots, i_n \), we have \( A_{i_1, \ldots, i_n} \xi_1 = A_{i_1, \ldots, i_n} \xi_2 \). Since \( \mathcal{V} \) is general \( A_{i_1, \ldots, i_n} \) is invertible whence \( \xi_1 = \xi_2 \), i.e., \( v_1 = v_2 \).

5. Proof of Theorems 2, 3

We first need two lemmas.

Lemma 4. Let \( \Pi \) be an \( \ell \times \ell \) permutation matrix consisting of a single cycle, and let \( \Sigma \) be an \( \ell \times \ell \) diagonal matrix with its diagonal entries taking values in \( \{1, -1\} \). Let \( \mathcal{Q} \) be the ideal generated by the 2 \( \times \) 2 minors of the matrix \( [z, \Sigma \Pi z] \) over the \( \ell \)-dimensional polynomial ring \( \mathbb{C}[z] = \mathbb{C}[z_1, \ldots, z_\ell] \). Then \( \text{codim} \mathcal{Q} = \ell - 1 \).

Proof. Let \( \sigma_i \in \{1, -1\} \) be the \( i \)th diagonal element of \( \Sigma \). Let \( \mathcal{V} \subset \mathbb{C}^\ell \) be the variety defined by the vanishing of all generators of \( \mathcal{Q} \). Since \( \dim \mathcal{V} = \dim \mathbb{C}[z]/\mathcal{Q} \), it is
enough to show that \( \dim \mathcal{Y} = 1 \). Clearly, \( v \in \mathcal{Y} \) if and only if \( v \) is an eigenvector of \( \Sigma \Pi \). Hence \( \mathcal{Y} \) is the union of the eigenspaces of \( \Sigma \Pi \), the latter being the irreducible components of \( \mathcal{Y} \). Since the eigenvalues of \( \Sigma \Pi \) are the \( \ell \) distinct roots of the equation \( x^\ell = \sigma_1 \cdots \sigma_\ell \), \( \Sigma \Pi \) is diagonalizable with \( \ell \) distinct eigenvalues, i.e., each eigenspace has dimension 1.

\[ \text{Lemma 5.} \] Let \( \Pi \) be an \( m \times m \) permutation matrix consisting of \( c \) cycles, and let \( \Sigma \) be an \( m \times m \) diagonal matrix with its diagonal entries taking values in \( \{1,-1\} \). For every \( i \in [c] \) let \( I_i \subseteq [m] \) be the indices that are cycled by cycle \( i \). Let \( I \subseteq [m] \) be such that \( I_i \not\subseteq I \) for every \( i \in [c] \). Let \( \mathcal{Q} \) be the ideal generated by the \( 2 \times 2 \) minors of the row-submatrix \( \Phi \) of \( [x \ \Sigma \Pi x] \) indexed by \( I \). Viewing \( \mathcal{Q} \) as an ideal of the polynomial ring over the indeterminates that appear in \( \Phi \), we have that \( \text{codim} \mathcal{Q} = \#I - 1 \).

\[ \text{Proof.} \] Let \( \Phi = [x \ \Sigma \Pi x]_I \) be the said submatrix. Let \( k \in [c] \) be such that \( I \cap I_k \neq \emptyset \). Since \( I_k \not\subseteq I \), we can partition \( I \cap I_k \) into subsets \( I_{kj} \) for \( j \in [s] \) for some \( s \), such that each \( \Phi_{kj} = [x \ \Sigma \Pi x]_{I_{kj}} \) has (up to a permutation of the rows) the form

\[
\Phi_{kj} = \begin{bmatrix}
  x_\alpha & \sigma_\beta x_\beta \\
  x_{\alpha+1} & \sigma_\alpha x_\alpha \\
  \vdots & \vdots \\
  x_{\alpha+\ell-2} & \sigma_{\alpha+\ell-3} x_{\alpha+\ell-3} \\
  x_\gamma & \sigma_{\alpha+\ell-2} x_{\alpha+\ell-2}
\end{bmatrix},
\]

where the \( \alpha, \beta, \gamma, \ell, \sigma \) depend on \( k, j \), with \( \sigma \in \{1, -1\} \) and \( x_\alpha, \ldots, x_{\alpha+\ell-3}, x_\beta, x_\gamma \) distinct variables appearing only in \( \Phi_{kj} \). Define \( s = \sum_k s_k \) and let \( T \) be the \( (\#I + s) \)-dimensional polynomial subring of \( \mathbb{C}[x] = \mathbb{C}[x_1, \ldots, x_m] \) generated by the variables that appear in \( \Phi_{kj} \). Next, let \( \mathbb{C}[y] = \mathbb{C}[y_1, \ldots, y_{2(\#I)}] \) be a \( 2(\#I) \)-dimensional polynomial ring and let \( \Psi \) be a \((\#I) \times 2\) matrix with \((i,j)\)th entry equal to \( y_{2(i-1)+j} \), where \( i = 1, \ldots, (\#I) \) and \( j = 1, 2 \). Let \( \mathcal{P} \subseteq \mathbb{C}[y] \) be the ideal generated by the \( 2 \times 2 \) minors of the matrix \( \Psi \). Then it is well-known that \( \dim \mathbb{C}[y]/\mathcal{P} = \#I + 1 \). Now, there exist \( \sum_{k,j}(s_{I_{kj}} - 1) = \#I - s \) linear forms in \( \mathbb{C}[y] \), say generating an ideal \( \mathcal{L} \), such that \( \mathcal{L}/\mathcal{Q} \cong \mathbb{C}[y]/(\mathcal{P} + \mathcal{L}) \). Moreover, we may add \( s \) linear forms to \( \mathcal{L} \) and obtain an ideal \( \mathcal{L}' \supset \mathcal{L} \) generated by \( \#I \) linear forms, such that \( \mathbb{C}[y]/(\mathcal{P} + \mathcal{L}') \cong \mathbb{C}[z]/\mathcal{Q}' \), where \( \mathbb{C}[z] = \mathbb{C}[z_1, \ldots, z_{\#I}] \) is a \( \#I \)-dimensional polynomial ring and \( \mathcal{Q}' \) is the ideal of \( \mathbb{C}[z] \) generated by the \( 2 \times 2 \) minors of the matrix \( [z \ \Sigma \Pi' \ z] \), where \( \Sigma' \) is a diagonal matrix with diagonal entries in \( \{1, -1\} \) and \( \Pi' \) a cycle of length \( \#I \). Then Lemma \[ \text{Remark 4.} \] If the matrix \( \Sigma \) in Lemma 5 is the identity, the ideal \( \mathcal{Q} \) is the vanishing ideal of an \( s \)-fold rational normal scroll \( \mathcal{Y}^{(s)}_{\text{RNS}} \). Since such a variety is known to have affine dimension \( s + 1 \), it follows directly that \( \text{codim} \mathcal{Q} = \dim \mathcal{T} - \dim \mathcal{Y}^{(s)}_{\text{RNS}} = (\#I + s) - (s + 1) = \#I - 1 \). Our argument then reduces to yet another algebraic device.
for computing the dimension of $Y^{(s)}_{RNS}$, which geometrically relies on specializing the general determinantal variety to the union of the eigenspaces of a cyclic permutation through a sequence of hyperplane sections of rational normal scrolls. 

5.1. Proof of Theorem 2

Working with matrices, we let $P_1, P_2$ be the matrix representations of the coordinate projections $\rho_1, \rho_2$, and $\Pi_1, \Pi_2$ the permutation matrices representing the permutations $\pi_1, \pi_2$. Since $(v, \lambda)$ is a generalized eigenpair of $(P_2P_1 \Pi_1, P_2 \Pi_2)$ if and only if $(\Pi_2 v, \lambda)$ is a generalized eigenpair of $(P_2P_1 \Pi_1 \Pi_2^{-1}, P_2)$, it is enough to show that the dimension of the generalized eigenspace of the matrix pair $(P_2P_1 \Pi_1, P_2)$ has the required upper bound for any permutation $\Pi$. Now, if $P_2P_1 \Pi v = \lambda P_2 v$, then $v$ lies in the variety $Y \subset \mathbb{C}^m$ defined by the vanishing of all the $2 \times 2$ minors of the matrix $[P_2 \ x \ P_2P_1 \Pi x]$, where $\mathbb{C}[x] = \mathbb{C}[x_1, \ldots, x_m]$ is the $m$-dimensional polynomial ring over $\mathbb{C}$. Contrary though to ordinary eigenspaces, there may be infinitely many generalized eigenvalues, so that the union of the eigenspaces $Y' = \bigcup_{\lambda \neq 0, 1} \mathcal{E}(P_2P_1 \Pi, \lambda)$ need not be closed. Instead, since each $\mathcal{E}(P_2P_1 \Pi, \lambda)$ is closed, it is enough to show that $Y'$ lies inside a subvariety $Y''$ of $Y$ of dimension at most $m - \lceil \text{rank}(P_2)/2 \rceil$.

Suppose that $v \in \mathcal{E}(P_2P_1 \Pi, \lambda), \lambda \neq 0, 1$, i.e., $P_2P_1 \Pi v = \lambda P_2 v$, for some $\lambda \neq 0, 1$. For $i = 1, 2$, let $I_i \subset [m]$ be the indices that correspond to $\text{Im}(P_i)$, and similarly $K_i$, the indices that correspond to $\ker(P_i)$. If $i \in I_2 \cap K_1$, then it is clear that $v_i$ must be zero, because $\lambda \neq 0$. If $\pi(i) \in I_2 \cap K_1$, then we must also have $v_{\pi(i)} = 0$ for the same reason. If $\pi(i) \in I_2 \cap K_1$, then again $v_{\pi(i)} = 0$ because we already have $v_i = 0$ and $\lambda \neq 0$. This domino effect either forces $v$ to be zero in the entire orbit of $i$, or until an index $j$ in the orbit of $i$ is reached such that $\pi(j) \in K_2 \cap K_1$. Let $I_{\text{domino}} \subset I_2$ be the coordinates of $v$ that are forced to zero by the union of the domino effects for every $i \in I_2 \cap K_1$. Clearly $I_2 \setminus I_{\text{domino}} \subset I_2 \cap I_1$. Let $i \in I_2 \setminus I_{\text{domino}}$; if it so happens that $\pi(i) = i$, then we must have that $v_i = 0$ because $\lambda \neq 1$. Consequently the coordinates of $v$ that correspond to fixed points of $\pi$ and lie in $I_2 \setminus I_{\text{domino}}$ must be zero. Letting $I_{\text{fixed}} \subset I_2 \setminus I_{\text{domino}}$ be the set containing these indices, $v$ must lie in the linear variety defined by the vanishing of the coordinates indexed by $I_{\text{domino}} \cup I_{\text{fixed}}$.

Next, let $\pi_1, \ldots, \pi_c'$ be all the $c' \geq 0$ cycles of $\pi$ of length at least two that lie entirely in $I_2 \setminus (I_{\text{domino}} \cup I_{\text{fixed}})$. Let $C_i \subset [m]$ be the indices cyclic by $\pi_i$. Since $\lambda \neq 0$, it is clear that $v_{C_i}$ must be an eigenvector of $\pi_i$, and so by Lemma 4, $v_{C_i}$ must lie in a codimension-$(\#C_i - 1)$ variety. Adding codimensions over $i \in [c']$, and letting $I_{\text{cycles}} = \bigcup_{i \in [c']}(\#C_i - 1)$, we get that $v_{I_{\text{cycles}}}$ must lie in a variety of codimension $\sum_{i \in [c']}((\#C_i - 1))$. Moreover, we may assume that the set $I_{\text{incomplete}} = I_2 \setminus (I_{\text{domino}} \cup I_{\text{fixed}} \cup I_{\text{cycles}})$ does not contain any complete cycles, and if $I_{\text{incomplete}} \neq \emptyset$ Lemma 5 gives that $v_{I_{\text{incomplete}}}$ must lie in a codimension-$(\#I_{\text{incomplete}} - 1)$ variety.

Let $Y_{\text{domino}}, Y_{\text{fixed}}, Y_{\text{cycles}}, Y_{\text{incomplete}}$ be the varieties defined by the vanishing of the coordinates in $I_{\text{domino}}$, the vanishing of the coordinates in $I_{\text{fixed}}$, as well as the vanishing of the $2 \times 2$ minors of the matrix $[x \ | \ x]_{\Pi x}$ indexed by $I_{\text{cycles}}$ and $I_{\text{incomplete}}$ respectively. Noting that these varieties are all associated with disjoint polynomial rings and that $\#I_{\text{domino}} + \#I_{\text{fixed}} + \#I_{\text{cycles}} + \#I_{\text{incomplete}} = \#I_2$, the above analysis gives that $v$ must
lie in a variety $Y'' = Y_{\text{domino}} \times Y_{\text{fixed}} \times Y_{\text{cycles}} \times Y_{\text{incomplete}}$ so that

$$\text{codim } Y'' \geq \#I_{\text{domino}} + \#I_{\text{fixed}} + \sum_{i \in [c']} (#C_i - 1) + \max\{\#I_{\text{incomplete}} - 1, 0\}$$

$$= \#I_2 - c' - \#I_{\text{incomplete}} + \max\{\#I_{\text{incomplete}} - 1, 0\}.$$ 

If $I_{\text{incomplete}} = \emptyset$, then $\text{codim } Y'' \geq \#I_2 - c'$. Since $c' \leq \#I_2/2$, we have that $\text{codim } Y' \geq \#I_2/2 \geq \lfloor \#I_2/2 \rfloor$. If on the other hand $I_{\text{incomplete}} \neq \emptyset$, then $c' \leq \lfloor (#I_2 - 1)/2 \rfloor$, so that $\text{codim } Y'' \geq \#I_2 - \lfloor (#I_2 - 1)/2 \rfloor - 1 \geq \lfloor #I_2/2 \rfloor$, with the last inequality separately verified for $#I_2$ odd or even.

5.2. Proof of Theorem

If $\rho_1 \in \mathcal{B}_n$ and $\rho_2 \in \mathcal{B}_{2n}$, then the claim is a direct corollary of Theorems and the proof of Theorem establishes that $\dim \mathcal{U}_{\rho_2 \rho_1 \pi_1, \rho_2 \pi_2} \leq m - \lfloor \text{rank}(\rho_2)/2 \rfloor$, where now $\mathcal{U}_{\rho_2 \rho_1 \pi_1, \rho_2 \pi_2} = \mathcal{U}_{\rho_2 \rho_1 \pi_1, \rho_2 \pi_2} \setminus \ker(\rho_1 \tau + \tau_2)$. Moreover, an identical argument as in the end of the proof of Proposition shows that we can reformulate that proposition as follows: “Let $\mathcal{U}$ be a vector space of dimension $m \geq 2n$ and $\tau$ such that $\dim \delta_{\tau, \lambda \neq 1, -1} \leq m - n$. Then the following is true for a general $n$-dimensional subspace $\mathcal{V}$: if $\tau(v_1) = v_2$ with $v_1, v_2 \in \mathcal{V}$, then either $v_1 = v_2$ or $v_1 = -v_2$.” Combining everything together establishes the claim.

Acknowledgement

The author is grateful to Prof. Aldo Conca, Department of Mathematics, University of Genova, for suggesting to study the abstraction of the unlabeled sensing problem, pointing out initial eigenspace conditions in the form of Proposition for diagonalizable endomorphisms, as well as for many inspiring subsequent discussions.

References

[1] A. Abid, A. Poon, J. Zou, Linear regression with shuffled labels, Tech. Rep., arXiv:1705.01342v2 [stat.ML], 2017.

[2] A. Abid, J. Zou, Stochastic EM for shuffled linear regression, Tech. Rep., arXiv:1804.00681v1 [stat.ML], 2018.

[3] W. Bruns, U. Vetter, Determinantal Rings, Springer, Berlin/Heidelberg, 1988.

[4] M. L. Catalano-Johnson, The resolution of the ideal of 2x2 minors of a 2xn matrix of linear forms, Journal of Algebra 187 (1997) 39–48.

[5] A. Conca, D. Faenzi, A remark on hyperplane sections of rational normal scrolls, Bull. Math. Soc. Sci. Math. Roumanie 60 (108) (4) (2017) 337–349.

[6] D. Cox, J. Little, D. O’Shea, Ideals, Varieties, and Algorithms, Springer, 2007.

[7] I. Dokmanic, Permutations unlabeled beyond sampling unknown, Tech. Rep., arXiv:1812.00498v1 [cs.IT], 2018.
[8] D. Eisenbud, Commutative Algebra with a View Toward Algebraic Geometry, Springer, 2004.

[9] S. Haghighatshoar, G. Caire, Signal recovery from unlabeled samples, IEEE Transaction on Signal Processing 66 (5) (2018) 1242–1257.

[10] J. Harris, Algebraic Geometry: A First Course, Springer-Verlag, 1992.

[11] D. J. Hsu, K. Shi, X. Sun, Linear regression without correspondence, in: Advances in Neural Information Processing Systems (NIPS), 1531–1540, 2017.

[12] A. Pananjady, M. J. Wainwright, T. A. Courtade, Linear regression with shuffled data: Statistical and computational limits of permutation recovery, in: 54th IEEE Annual Allerton Conference on Communication, Control and Computing, 417–424, 2016.

[13] A. Pananjady, M. J. Wainwright, T. A. Courtade, Linear regression with shuffled data: Statistical and computational limits of permutation recovery, IEEE Transactions on Information Theory 64 (5) (2018) 3286–3300.

[14] S. Roman, Advanced Linear Algebra, Springer, 2008.

[15] M. Slawski, E. Ben-David, Linear regression with sparsely permuted data, Electronic Journal of Statistics 13 (1) (2019) 1–36.

[16] X. Song, H. Choi, Y. Shi, Permutated linear model for header-free communication via symmetric polynomials, in: International Symposium on Information Theory (ISIT), 2018.

[17] M. C. Tsakiris, L. Peng, Homomorphic sensing, Tech. Rep., arXiv:1901.07852 [cs.IT], 2019.

[18] M. C. Tsakiris, L. Peng, A. Conca, L. Kneip, Y. Shi, H. Choi, An algebraic-geometric approach to shuffled linear regression, arXiv:1810.05440 [cs.LG].

[19] M. C. Tsakiris, R. Vidal, Filtrated algebraic subspace clustering, SIAM Journal on Imaging Sciences 10 (1) (2017) 372–415.

[20] M. C. Tsakiris, R. Vidal, Algebraic clustering of affine subspaces, IEEE Transactions on Pattern Analysis and Machine Intelligence 2 (40) (2018) 482–489.

[21] J. Unnikrishnan, S. Haghighatshoar, M. Vetterli, Unlabeled sensing: solving a linear system with unordered measurements, in: 53rd IEEE Annual Allerton Conference on Communication, Control and Computing, 2015.

[22] J. Unnikrishnan, S. Haghighatshoar, M. Vetterli, Unlabeled sensing with random linear measurements, IEEE Transactions on Information Theory 64 (5) (2018) 3237–3253.