Homomorphic Sensing of Subspace Arrangements

Liangzu Peng[a], Manolis C. Tsakiris[a,*]

[a] *SIST, ShanghaiTech University, No. 393 Huaxia Middle Road, Pudong Area, Shanghai, China*

Abstract

This template helps you to create a properly formatted LaTeX manuscript.

Keywords: Homomorphic sensing

1. Introduction

1.1. Homomorphic sensing

The homomorphic sensing problem was posed by [1] in mathematical terms as follows. With $\mathbb{H}$ being $\mathbb{R}$ or $\mathbb{C}$ let $\mathcal{V} \subset \mathbb{H}^m$ be a linear subspace and $\mathcal{T}$ a finite set of linear maps $\mathbb{H}^m \to \mathbb{H}^r$, $r \leq m$. With $v^* \in \mathcal{V}$ and $\tau^* \in \mathcal{T}$ we observe $y := \tau^*(v^*)$. Given $\mathcal{V}, \mathcal{T}$, and y, then, can we *uniquely* determine v^* without knowing τ^*? In other words, with y fixed we want to know when the relations

$$y = \tau(v), \qquad \tau \in \mathcal{T}, \qquad v \in \mathcal{V} \tag{1}$$

necessarily imply that $v = v^*$. This motivates the following definition.

Definition 1 (hsp)**.** *Let $\mathscr{V}$ be a set of vectors and $\mathscr{T}$ a finite set of linear maps. We will say that $\mathscr{V}$ and $\mathscr{T}$ satisfy the "homomorphic sensing property", denoted by* $\operatorname{hsp}(\mathscr{V}, \mathscr{T})$*, whenever the following holds:*

$$\operatorname{hsp}(\mathscr{V}, \mathscr{T}): \quad \forall v_1, v_2 \in \mathscr{V}, \forall \tau_1, \tau_2 \in \mathscr{T}, \quad \tau_1(v_1) = \tau_2(v_2) \Rightarrow v_1 = v_2. \tag{2}$$

If $\tau_1(v_1) = \tau_2(v_2)$ only implies $v_1 = \pm v_2$, then we will use the notation $\operatorname{hsp}_{\pm}(\mathscr{V}, \mathscr{T})$*.*

The problem of interest to us is as follows.

Problem 1 (Homomorphic sensing [1, 2]). *Find conditions on a finite set $\mathcal{T}$ of linear maps $\mathbb{H}^m \to \mathbb{H}^r$ and an n-dimensional linear subspace $\mathcal{V} \subset \mathbb{H}^m$ that imply* $\operatorname{hsp}(\mathcal{V}, \mathcal{T})$ *or* $\operatorname{hsp}_{\pm}(\mathcal{V}, \mathcal{T})$*.*

To appreciate Problem1 we start by looking at several special cases which have been explored via different approaches in the last two decades, e.g., see [3, 4, 5, 6, 7, 8, 9]. The first example is *real phase retrieval* [9], a problem which dates back to the 1910s when the research on *X-ray crystallography* was launched; see [10] for a vivid account. In a mathematical formulation of this problem we let $\mathbb{H} = \mathbb{R}$ and consider the relation $y = B^* A x^*$, where y is a m-dimensional vector, $A \in \mathbb{R}^{m \times n}$ is a given matrix, and B^* is known only up to the set $\mathcal{B}_m$ of $m \times m$ sign matrices, i.e., diagonal matrices with ± 1 on the diagonal. Since uniquely recovering a nonzero x^* is impossible[1], we consider unique recovery of x^* up to sign. In other words, with $\mathcal{B}_m A := \{BA : B \in \mathcal{B}_m\}$ we consider the property $\operatorname{hsp}_{\pm}(\mathbb{R}^n, \mathcal{B}_m A)$. In 2006, it was proved by [3] in a frame-theoretical language that $m \geq 2n - 1$ is sufficient for a generic[2] $A \in \mathbb{R}^{m \times n}$ to enjoy $\operatorname{hsp}_{\pm}(\mathbb{R}^n, \mathcal{B}_m A)$,

⋆HI

*Corresponding author

Email addresses: `penglz@shanghaitech.edu.cn` (Liangzu Peng), `mtsakiris@shanghaitech.edu.cn` (Manolis C. Tsakiris)

[1] If x^* is nonzero then we have $B^* A x^* = -B^* A(-x^*)$ but $x^* \neq -x^*$.

[2] By a generic matrix in $\mathbb{R}^{m \times n}$ we mean a non-empty Zariski open subset of $\mathbb{R}^{m \times n}$; see also §2.2.

and this is necessary for any $A \in \mathbb{R}^{m\times n}$. If x^* is known to come from the set $\overline{\mathcal{K}_{\mathscr{I}}}$ of all k-sparse vectors of $\mathbb{R}^n$, a prior knowledege in *sparse real phase retrieval* [5], then [4] and [5] have independently showed that a sufficient and necessary condition for $\operatorname{hsp}_{\pm}(\overline{\mathcal{K}_{\mathscr{I}}}, \mathcal{B}_m A)$ for $A \in \mathbb{R}^{m\times n}$ generic is $m \geq \min\{2n-1, 2k\}$. Finally, those results are also true for the problem of *symmetric mixture of two linear regressions* [11], since it bears the same formulation as real phase retrieval in the noiseless case; see [12] and [13] for discussions that connect the two problems.

The next example involves the set $\mathcal{S}_{r,m}$ of all rank-r selection matrices, i.e., matrices whose rows are formed by r distinct standard basis vectors of $\mathbb{R}^m$. Motivated by signal processing applications, the property $\operatorname{hsp}(\mathbb{R}^n, \mathcal{S}_{r,m}A)$ was considered in [6, 7] under the name *unlabeled sensing*, and also independently in [8]. Specifically, they proved via different algebraic-combinatorial techniques that $r \geq 2n$ suffices to guarantee $\operatorname{hsp}(\mathbb{R}^n, \mathcal{S}_{r,m}A)$ for $A \in \mathbb{R}^{m\times n}$ generic. For the converse, [8] proved that $r \geq 2n-1$ is necessary for $\operatorname{hsp}(\mathbb{R}^n, \mathcal{S}_{r,m}A)$ and [6, 7] proved that, if m is odd with $m = r$ and $n \geq 2$, then $r \geq 2n$ is necessary. Finally, if $m = r$, then $\mathcal{S}_m := \mathcal{S}_{m,m}$ becomes the set of $m \times m$ permutation matrices and the unlabeled sensing problem becomes that of *linear regression without correspondences*. This special case has its origin in applications in statistics such as *record linkage* [14] and the *broken sample problem* [15] (see [16] for detailed discussions); recent development on this topic can be found in e.g. [17, 18, 19, 20, 21, 22, 23, 24, 25, 26].

An interesting generalization which we call *unsigned unlabeled sensing* was explored in [9] and is a combination of the above two, where we let $\mathcal{S}_{r,m}\mathcal{B}_m := \{SB : S \in \mathcal{S}_{r,m}, B \in \mathcal{B}_m\}$ and the interest is in $\operatorname{hsp}_{\pm}(\mathbb{R}^n, \mathcal{S}_{r,m}\mathcal{B}_m A)$. By extending the approach of [8], it was established in [9] that $r \geq 2n$ is sufficient for $\operatorname{hsp}_{\pm}(\mathbb{R}^n, \mathcal{S}_{r,m}\mathcal{B}_m A)$ for $A \in \mathbb{R}^{m\times n}$ generic and this is necessary if $n \geq 2$.

A further generalization termed *homomorphic sensing* (Problem 1) of all the above problems was considered in [1, 2], where, with $\mathcal{V} \subset \mathbb{H}^m$ an n-dimensional subspace and $\mathcal{T}$ a finite set of linear maps, the authors studied the property $\operatorname{hsp}(\mathcal{V}, \mathcal{T})$ using algebraic geometry. With linear maps τ_1, τ_2 of $\mathbb{H}^m$ let $\overline{\tau}_1, \overline{\tau}_2$ be their complexifications and let T_1, T_2 be their matrix representations[3]. Let ρ be a linear projection onto the image $\operatorname{im}(\tau_2)$ of τ_2 with matrix representation P and complexification $\overline{\rho}$. The 2×2 minors of the matrix $[PT_1 w \ T_2 w]$ are polynomials in entries of w, so their vanishing locus is a complex algebraic variety[4], say $\mathcal{Y}_{\rho\tau_1,\tau_2}$. Removing from $\mathcal{Y}_{\rho\tau_1,\tau_2}$ the union $\mathcal{Z}_{\rho\tau_1,\tau_2} := \ker(\overline{\rho}\overline{\tau}_1 - \overline{\tau}_2) \cup \ker(\overline{\rho}\overline{\tau}_1) \cup \ker(\overline{\tau}_2)$ of linear subspaces gives the quasi-variety (i.e., the set-theoretical difference between two algebraic varieties)

$$\mathcal{U}_{\rho\tau_1,\tau_2} = \mathcal{Y}_{\rho\tau_1,\tau_2} \backslash \mathcal{Z}_{\rho\tau_1,\tau_2}. \tag{3}$$

In [1, 2] it was proved that if for any $\tau_1, \tau_2 \in \mathcal{T}$ it holds that $\operatorname{rank}(\tau_1) := \operatorname{rank}(T_1) \geq 2n$ and $\operatorname{rank}(\tau_2) \geq 2n$, and that there exists a linear projection ρ onto $\operatorname{im}(\tau_2)$ satisfying $\dim(\mathcal{U}_{\rho\tau_1,\tau_2}) \leq m - n$,[5] then a generic subspace $\mathcal{V}$ of dimension n satisfies $\operatorname{hsp}(\mathcal{V}, \mathcal{T})$. They further specialized this result to unlabeled sensing, yielding the same sufficient conditions as in [7] and [8] mentioned above.

A limitation of this result is the presence of the projection ρ. It remains unknown whether such ρ that satisfies $\dim(\mathcal{U}_{\rho\tau_1,\tau_2}) \leq m - n$ exists, or even if so how to search for it. One of our main contributions is to dispense with ρ. To do so, we consider the complex algebraic variety $\mathcal{Y}_{\tau_1,\tau_2}$ defined by the vanishing of the 2×2 minors of $[T_1 w \ T_2 w]$, the union $\mathcal{Z}_{\tau_1,\tau_2} := \ker(\overline{\tau}_1 - \overline{\tau}_2) \cup \ker(\overline{\tau}_1) \cup \ker(\overline{\tau}_2)$, and the quasi-variety

$$\mathcal{U}_{\tau_1,\tau_2} = \mathcal{Y}_{\tau_1,\tau_2} \backslash \mathcal{Z}_{\tau_1,\tau_2}. \tag{4}$$

Then we have the following description of the homomorphic sensing phenomenon.

Theorem 1. *Suppose* $\operatorname{rank}(\tau) \geq 2n$ *for every* $\tau \in \mathcal{T}$. *Then* $\operatorname{hsp}(\mathcal{V}, \mathcal{T})$ *holds true for a generic subspace* $\mathcal{V}$ *of* $\mathbb{H}^m$ *of dimension* n *whenever*

$$\dim(\mathcal{U}_{\tau_1,\tau_2}) \leq m - n, \quad \forall \tau_1, \tau_2 \in \mathcal{T}. \tag{5}$$

[3]We always consider the matrix representation with respect to the standard basis. A linear map $\mathbb{R}^m \to \mathbb{R}^r$ and its complexification have the same matrix representation [27].

[4]We define (complex) algebraic varieties as the zero locus of finitely many polynomials. So they can be reducible. See §2.2.

[5]If $\mathcal{T} = \{\tau_1, \tau_2\}$ then the condition $\operatorname{rank}(\tau_1) \geq 2n$ can be relaxed to $\operatorname{rank}(\tau_1) \geq n$ [2]. See §2.2 for the definition of dimension.

Note that, by definition, $\mathcal{U}_{\tau_1,\tau_2}$ is a subset of $\mathcal{U}_{\rho\tau_1,\tau_2}$, so condition (5) is tighter than that of [1, 2]. Indeed, condition (5) is the tightest possible in the following sense.

Proposition 1. *Let $\mathbb{H} = \mathbb{C}$ and suppose that condition* (5) *is not true. Then* $\operatorname{hsp}(\mathcal{V}, \mathcal{T})$ *is violated for a generic subspace $\mathcal{V} \subset \mathbb{H}^m$ of dimension n.*

Using the proof technique of Theorem 1, we get the following extension for $\operatorname{hsp}_{\pm}(\mathcal{V}, \mathcal{T})$.

Proposition 2. *Suppose that for every $\tau \in \mathcal{T}$ we have* $\operatorname{rank}(\tau) \geq 2n$. *Let $\mathcal{U}^{\pm}_{\tau_1,\tau_2} := \mathcal{U}_{\tau_1,\tau_2} \setminus \ker(\overline{\tau}_1 + \overline{\tau}_2)$. Then $\operatorname{hsp}_{\pm}(\mathcal{V}, \mathcal{T})$ holds true for a generic subspace $\mathcal{V}$ of $\mathbb{H}^m$ of dimension n whenever*

$$\dim(\mathcal{U}^{\pm}_{\tau_1,\tau_2}) \leq m - n, \quad \forall \tau_1, \tau_2 \in \mathcal{T}. \tag{6}$$

In §1.2, we extend Theorem 1 from a single subspace $\mathcal{V}$ to a *subspace arrangement* (Theorem 2). In §1.3 we consider the local stability of the homomorphic sensing property under noise (Theorem 3). In §1.4, we specialize Theorems 1-3 to the aforementioned applications, e.g., real phase retrieval, unlabeled sensing variants, and their sparse versions. In §2 we give preliminaries. Proofs of all the statements are in §3.

1.2. Homomorphic sensing of subspace arrangements

We extend Theorem 1 from a single subspace $\mathcal{V}$ to a subspace arrangement $\mathcal{A} = (\mathcal{V}_1, \ldots, \mathcal{V}_\ell)$, the latter being an ordered set of subspaces $\mathcal{V}_i$'s of $\mathbb{H}^m$. If each subspace $\mathcal{V}_i$ has dimension n_i, we refer to $(n_1, \ldots, n_\ell)$ as the dimension configuration of $\mathcal{A}$. Thus, by a *generic* subspace arrangement $\mathcal{A}$ with dimension configuration $(n_1, \ldots, n_\ell)$ we mean a non-empty Zariski open subset of the product $\operatorname{Gr}_{\mathbb{H}}(n_1, m) \times \cdots \times \operatorname{Gr}_{\mathbb{H}}(n_\ell, m)$ of the Grassmannians (see also §2.2). Consider an ordered set $\mathscr{I} = (\mathcal{I}_1, \ldots, \mathcal{I}_s)$ of subsets of $[\ell] := \{1, \ldots, \ell\}$. Each $\mathcal{I}_j$ gives rise to a subspace $\mathcal{V}_{\mathcal{I}_j} := \sum_{i \in \mathcal{I}_j} \mathcal{V}_i$ with dimension upper bounded by $n_{\mathcal{I}_j} := \sum_{i \in \mathcal{I}_j} n_i$, where we define $\mathcal{V}_\varnothing := 0$. Thus the ordered set $\mathscr{I}$, together with $\mathcal{A}$, induces the *structured* subspace arrangement $\mathcal{A}_{\mathscr{I}} = (\mathcal{V}_{\mathcal{I}_1}, \ldots, \mathcal{V}_{\mathcal{I}_s})$. Clearly, the structured subspace arrangement $\mathcal{A}_{\mathscr{I}}$ becomes the original $\mathcal{A}$ when $\mathcal{I}_j = \{j\}$ and $s = \ell$, and if in addition $s = 1$, then $\mathcal{A}_{\mathscr{I}}$ becomes a single subspace. We write $\overline{\mathcal{A}_{\mathscr{I}}} := \cup_{j \in [s]} \mathcal{V}_{\mathcal{I}_j}$ and consider the property $\operatorname{hsp}(\overline{\mathcal{A}_{\mathscr{I}}}, \mathcal{T})$. We are ready to state the following result.

Theorem 2. *Suppose* $\operatorname{rank}(\tau) \geq 2n$ *for any $\tau \in \mathcal{T}$. Let $(n_1, \ldots, n_\ell)$ be a dimension configuration and $\mathscr{I} = (\mathcal{I}_1, \ldots, \mathcal{I}_s)$ an ordered set of subsets of $[\ell]$ satisfying $n_{\mathcal{I}_j} \leq n$ for any $j \in [s]$. Then $\operatorname{hsp}(\overline{\mathcal{A}_{\mathscr{I}}}, \mathcal{T})$ holds for a generic subspace arrangement $\mathcal{A} = (\mathcal{V}_1, \ldots, \mathcal{V}_\ell)$ with $\dim(\mathcal{V}_i) = n_i$ whenever* (5) *holds. Similarly, $\operatorname{hsp}_{\pm}(\overline{\mathcal{A}_{\mathscr{I}}}, \mathcal{T})$ holds for a generic subspace arrangement $(\mathcal{V}_1, \ldots, \mathcal{V}_\ell)$ with $\dim(\mathcal{V}_i) = n_i$ whenever* (6) *holds.*

1.3. Noisy homomorphic sensing

We consider the homomorphic sensing problem with $\mathbb{H} = \mathbb{R}$ in the presence of additive noise $\epsilon \in \mathbb{R}^m$. For $v^* \in \mathcal{V}$ and $\tau^* \in \mathcal{T}$ set $y = \tau^*(v^*)$ and $\overline{y} = y + \epsilon$. Consider the optimization problem

$$(\hat{\tau}, \hat{v}) \in \operatorname*{argmin}_{v \in \mathcal{V}, \tau \in \mathcal{T}} \|\overline{y} - \tau(v)\|_2. \tag{7}$$

What can we say about the optimal solution $\hat{v}$? Under what conditions is $\hat{v}$ close to v^*?

For a nonzero vector $u \in \mathbb{R}^m$ and a subspace $\mathcal{W} \subset \mathbb{R}^m$ we define

$$\cos(u, \mathcal{W}) := \max\big\{\langle u, w\rangle / \|u\|_2 : w \in \mathcal{W} \text{ and } \|w\|_2 = 1\big\}. \tag{8}$$

Denote by $\sigma(X)$ the largest singular value of a real matrix X. Then we have the following stability result.

Theorem 3. *Suppose* $\operatorname{rank}(\tau) \geq 2n$ *for every $\tau \in \mathcal{T}$ and that* (5) *holds. Let $\mathcal{V} \subset \mathbb{R}^m$ be a subspace of dimension n that satisfies* $\operatorname{hsp}(\mathcal{V}, \mathcal{T})$ *and let $A \in \mathbb{R}^{m \times n}$ be a matrix that has $\mathcal{V}$ as its column space. Let $(\hat{\tau}, \hat{v})$ be a solution to* (7) *with $\hat{T}$ the matrix representation of $\hat{\tau}$. Set $\mathcal{T}_1 := \{\tau \in \mathcal{T} : y \in \tau(\mathcal{V})\}$. If $\mathcal{T} = \mathcal{T}_1$ or*

$$2\|\epsilon\|_2 < \|y\|_2 \Big(1 - \max_{\tau \in \mathcal{T} \setminus \mathcal{T}_1} \cos\big(y, \tau(\mathcal{V})\big)\Big), \tag{9}$$

then $\hat{v} - v^* = A(\hat{T}A)^\dagger \epsilon$, where $(\hat{T}A)^\dagger$ is the pseudoinverse of $\hat{T}A$. In particular $\|\hat{v} - v^*\|_2 \leq \sigma(A(\hat{T}A)^\dagger)\|\epsilon\|_2$.

1.4. Applications of homomorphic sensing theory

We now consider the applications of Theorems 1-3 to problems mentioned in §1.1, namely linear regression without correspondences ($\mathcal{S}_m$), unlabeled sensing ($\mathcal{S}_{r,m}$), real phase retrieval ($\mathcal{B}_m$), and unsigned unlabeled sensing ($\mathcal{S}_{r,m}\mathcal{B}_m$). Taking $\mathcal{S}_{r,m}$ for example we see that, if A is of full column rank, then $\operatorname{hsp}(\mathbb{R}^n, \mathcal{S}_{r,m}A)$ is equivalent to $\operatorname{hsp}(R(A), \mathcal{S}_{r,m})$, where $R(A)$ is the range space of A. We then check whether $\mathcal{S}_{r,m}$ satisfies condition (5). Interestingly, whenever the rank constraint $r \geq 2n$ of Theorem 1 on $\mathcal{S}_{r,m}$ is fulfilled, condition (5) is automatically satisfied by $\mathcal{S}_{r,m}$, as presented next.

Proposition 3. *Let $\Pi_1, \Pi_2 \in \mathcal{S}_m$, $S_1, S_2 \in \mathcal{S}_{r,m}$, and $B_1, B_2 \in \mathcal{B}_m$ be permutations, rank-r selections, and sign matrices, respectively.*

- $m \geq 2n \Rightarrow \dim(\mathcal{U}_{\Pi_1,\Pi_2}) \leq m - n$.
- $r \geq 2n \Rightarrow \dim(\mathcal{U}_{S_1,S_2}) \leq m - n$.
- $m \geq 2n \Rightarrow \dim(\mathcal{U}^{\pm}_{B_1,B_2}) \leq m - n$.
- $r \geq 2n \Rightarrow \dim(\mathcal{U}^{\pm}_{S_1B_1,S_2B_2}) \leq m - n$.

Combining Proposition 3 with Theorem 1, we get the following corollary.

Corollary 1. *For a generic matrix A of $\mathbb{R}^{m\times n}$, it holds that*

- $m \geq 2n \Rightarrow \operatorname{hsp}(\mathbb{R}^n, \mathcal{S}_mA)$ *[1, 7, 8, 22].*
- $r \geq 2n \Rightarrow \operatorname{hsp}(\mathbb{R}^n, \mathcal{S}_{r,m}A)$ *[1, 7, 8].*
- $m \geq 2n \Rightarrow \operatorname{hsp}_{\pm}(\mathbb{R}^n, \mathcal{B}_mA)$ *[3, 22].*
- $r \geq 2n \Rightarrow \operatorname{hsp}_{\pm}(\mathbb{R}^n, \mathcal{S}_{r,m}\mathcal{B}_mA)$ *[1, 9].*

Next we consider the applications of Theorem 2. If given the standard basis $e_1, \dots, e_n$ of $\mathbb{R}^n$ we are also given $\mathcal{V}_i = \operatorname{Span}(e_i)$ and the subspace arrangement $\mathcal{K} = (\mathcal{V}_1, \dots, \mathcal{V}_n)$. Let $s = \binom{n}{k}$ and consider the ordered set $\mathscr{I} = (\mathcal{I}_1, \dots, \mathcal{I}_s)$ of all subsets of $[n]$ of cardinality k. It gives the structured subspace arrangement $\mathcal{K}_{\mathscr{I}} = (\mathcal{V}_{\mathcal{I}_1}, \dots, \mathcal{V}_{\mathcal{I}_s})$ where $\mathcal{V}_{\mathcal{I}_j} = \sum_{i\in\mathcal{I}_j} \mathcal{V}_i$. By construction, the union $\overline{\mathcal{K}_{\mathscr{I}}} := \cup_{j\in[s]}\mathcal{V}_{\mathcal{I}_j}$ of subspaces is the set of all k-sparse vectors of $\mathbb{R}^n$. As mentioned in §1.1, the property $\operatorname{hsp}_{\pm}(\overline{\mathcal{K}_{\mathscr{I}}}, \mathcal{B}_mA)$ for sparse real phase retrieval was studied in [4] and [5]. However, the properties $\operatorname{hsp}(\overline{\mathcal{K}_{\mathscr{I}}}, \mathcal{S}_{r,m}A)$ and $\operatorname{hsp}_{\pm}(\overline{\mathcal{K}_{\mathscr{I}}}, \mathcal{S}_{r,m}\mathcal{B}_mA)$ for sparse variants of unlabeled sensing have not been considered, to the best of our knowledge. By Theorem 2 and Proposition 3 we get conditions that guarantee those properties at once.

Corollary 2. *For a generic matirx A of $\mathbb{R}^{m\times n}$ and $k \leq n$, it holds that*

- $m \geq 2k \Rightarrow \operatorname{hsp}(\overline{\mathcal{K}_{\mathscr{I}}}, \mathcal{S}_mA)$.
- $r \geq 2k \Rightarrow \operatorname{hsp}(\overline{\mathcal{K}_{\mathscr{I}}}, \mathcal{S}_{r,m}A)$.
- $m \geq 2k \Rightarrow \operatorname{hsp}_{\pm}(\overline{\mathcal{K}_{\mathscr{I}}}, \mathcal{B}_mA)$ *[4, 5].*
- $r \geq 2k \Rightarrow \operatorname{hsp}_{\pm}(\overline{\mathcal{K}_{\mathscr{I}}}, \mathcal{S}_{r,m}\mathcal{B}_mA)$.

Our final result is a corollary of Theorem 3. For brevity we only state the result for unlabeled sensing, where $y = S^*Ax^*$ for some $S^* \in \mathcal{S}_{r,m}$, $\overline{y} = y + \epsilon$, and the objective function of interest as a special case of (7) is

$$(\hat{S}, \hat{x}) \in \underset{x\in\mathbb{R}^n, S\in\mathcal{S}_{r,m}}{\operatorname{argmin}} \|\overline{y} - SAx\|_2. \tag{10}$$

Corollary 3. *Suppose $r \geq 2n$ and that (9) holds for $\mathcal{T} = \mathcal{S}_{r,m}$ and $A \in \mathbb{R}^{m\times n}$ generic. Then $\hat{x} - x^* = (\hat{T}A)^{\dagger}\epsilon$.*

We note that condition (9) of Corollary 3 defines a non-asymptotic regime where stablity of estimating x^* is guaranteed, and this implies the asymptotic result of [7].

2. Preliminaries

2.1. Notations and facts

Given two linear maps τ_1, τ_2 of $\mathbb{H}^m$, we write T_1, T_2 for their matrix representations and $\overline{\tau}_1, \overline{\tau}_2$ for their complexifications, respectively. With $\lambda \in \mathbb{C}$, denote by $\mathscr{E}_{(\tau_1,\tau_2),\lambda}$ the set of all w's of $\mathbb{C}^m$ satisfying $\overline{\tau}_1(w) = \lambda\overline{\tau}_2(w)$. Write $\mathscr{E}_{\tau_1,\lambda} := \mathscr{E}_{(\tau_1,\mathrm{id}),\lambda}$ where id is the identity map. Clearly $\mathscr{E}_{\tau_1,\lambda}$ is the eigenspace of τ_1 corresponding to eigenvalue λ. For a linear map $\tau : X \to Y$ denote by $\tau^{-1}(Q)$ the inverse image of $Q \subset Y$ under τ. Denote by 0 the trivial subspace, the zero vector, and the number zero. Let $\mathrm{Gr}_{\mathbb{H}}(n,m)$ be the set of n-dimensional subspaces of $\mathbb{H}^m$, which is known as the Grassmannian. Lemma 1 will be useful.

Lemma 1. *For a linear map τ of $\mathbb{C}^m$ and B, C subspaces of $\mathbb{C}^m$, we have*

$$B \cap \ker(\tau) = 0,\ \ \tau(B) \cap C = 0 \Leftrightarrow B \cap \tau^{-1}(C) = 0. \tag{11}$$

PROOF. ($\Rightarrow$) Let $b \in B \cap \tau^{-1}(C)$. So there is some $c \in C$ such that $\tau(b) = c$. But $\tau(B) \cap C = 0$ implies that $\tau(b) = c = 0$. This gives $b = 0$ because $B \cap \ker(\tau) = 0$. This proves $B \cap \tau^{-1}(C) = 0$.

($\Leftarrow$) Since $\ker(\tau) \subset \tau^{-1}(C)$, we get $B \cap \ker(\tau) = 0$. Let $c \in \tau(B) \cap C$. For some $b \in B$ we have

$$\tau(b) = c \Rightarrow b \in \tau^{-1}(c) \Rightarrow b \in \tau^{-1}(C). \tag{12}$$

But $B \cap \tau^{-1}(C) = 0$ implies $b = 0$. So $c = 0$. This proves $\tau(B) \cap C = 0$.

2.2. Algebraic geometry background

A (complex) algebraic variety is a subset of $\mathbb{C}^m$ defined by the common zero locus of finitely many polynomials in m variables with coefficients in $\mathbb{C}$. The *Zariski topology* is defined by letting algebraic varieties be closed subsets of $\mathbb{C}^m$, and so a Zariski open set is the complement of some variety. An irreducible algebraic variety is the one which can not be written as the union of two proper subvarieties of it. By a *generic* point of an irreducible algebraic variety having some property we mean that there is a non-empty Zariski open subset in this variety satisfying this property. Since $\mathbb{R}^{m\times n}$ and $\mathrm{Gr}_{\mathbb{H}}(n,m)$ are both irreducible, we justfied what we mean by a generic matrix of $\mathbb{R}^{m\times n}$ or a generic subspace of $\mathbb{H}^m$ of dimension n.

Our proof relies heavily on the notion of dimension of algebraic varieties. Specifically, the dimension $\dim(\mathcal{Q})$ of an algebraic variety $\mathcal{Q}$ is the maximal length t of the chains $\mathcal{Q}_0 \subset \mathcal{Q}_1 \subset \cdots \subset \mathcal{Q}_t$ of distinct irreducible algebraic varieties contained in $\mathcal{Q}$. The dimension of any set is the dimension of its *closure*, i.e., the smallest algebraic variety which contains it. The following lemma will be useful and proved in §4.

Lemma 2. *Given t algebraic varieties $\mathcal{Q}_1, \dots, \mathcal{Q}_t$ in $\mathbb{C}^m$ of dimension $r_1, \dots, r_t$ passing through the origin, there exists a non-empty Zariski open subset of $\mathrm{Gr}_{\mathbb{C}}(d,m)$ on which every subspace $\mathcal{V}$ satisfies $\dim(\mathcal{Q}_j \cap \mathcal{V}) \le \max\{r_j + d - m, 0\}$ for any $j \in [t]$, and we have $\mathcal{Q}_j \cap \mathcal{V} = 0$ if in addition $r_j + d \le m$.*

3. Proofs

3.1. Proof of Theorem 1

For every $\tau_1, \tau_2 \in \mathcal{T}$ it suffices to exhibit a non-empty Zariski open subset of $\mathrm{Gr}_{\mathbb{H}}(n,m)$ on which every subspace $\mathcal{V}$ satisfies $\mathrm{hsp}(\mathcal{V}, \{\tau_1, \tau_2\})$, which will imply $\mathrm{hsp}(\mathcal{V}, \mathcal{T})$ since $\mathcal{T}$ is a finite set and the intersection of finitely many non-empty Zariski open subsets of $\mathrm{Gr}_{\mathbb{H}}(n,m)$ is also non-empty and open.

We will divide the proof of Theorem 1 into two cases say $\dim(\mathscr{E}_{\tau_1,\tau_2}) \le m - n$ and $\dim(\mathscr{E}_{\tau_1,\tau_2}) > m - n$. Assume that we are in the first case. Then we have the following proposition whose proof is placed at §3.1.1.

Proposition 4. *In addition to the hypotheses of Theorem 1, further assume $\dim(\mathscr{E}_{(\tau_1,\tau_2),1}) \le m - n$. Then there is a subspace $\mathcal{V}$ of $\mathbb{H}^m$ which satisfies $\dim(\tau_1(\mathcal{V}) + \tau_2(\mathcal{V})) = 2n$.*

With the subspace $\mathcal{V}$ of Proposition 4 we get that the set $\mathbb{U}_1$ of subspaces of $\mathrm{Gr}_{\mathbb{H}}(n,m)$ on which $\dim(\tau_1(\mathcal{V}')+\tau_2(\mathcal{V}'))=2n$ for every $\mathcal{V}'\in\mathbb{U}_1$ is non-empty. Let $A\in\mathbb{H}^{m\times n}$ have this $\mathcal{V}$ as its column space. Then we see that $\dim(\tau_1(\mathcal{V})+\tau_2(\mathcal{V}))=2n$ is equivalent to $\mathrm{rank}[T_1A\ T_2A]=2n$. It follows that $\mathbb{U}_1$ is a Zariski open subset of $\mathrm{Gr}_{\mathbb{H}}(n,m)$ implicitly defined by the non-vanishing of some $2n\times 2n$ minor of $[T_1A\ T_2A]$. With this non-empty Zariski open $\mathbb{U}_1$ we next show that $\mathrm{hsp}(\mathcal{V},\{\tau_1,\tau_2\})$ holds for every $\mathcal{V}\in\mathbb{U}_1$. Indeed, let $v_1,v_2\in\mathcal{V}$ be such that $\tau_1(v_1)=\tau_2(v_2)$. But $\dim(\tau_1(\mathcal{V})+\tau_2(\mathcal{V}))=2n$ implies that $\tau_1(\mathcal{V})\cap\tau_2(\mathcal{V})=0$ and that $\dim(\tau_1(\mathcal{V}))=\dim(\tau_2(\mathcal{V}))=\dim(\mathcal{V})=n$. So $\ker(\tau_1)\cap\mathcal{V}=0$ and $\ker(\tau_2)\cap\mathcal{V}=0$. We conclude that $\tau_1(v_1)=\tau_2(v_2)=0$ and moreover $v_1=v_2=0$.

We tackle the second case $\dim(\mathscr{E}_{\tau_1,\tau_2})>m-n$ by the following proposition.

Proposition 5. *In addition to the hypotheses of Theorem 1, further suppose* $\dim(\mathscr{E}_{(\tau_1,\tau_2),1})=m-\overline{n}>m-n$. *There are two subspaces* $\overline{\mathcal{V}}\subset\mathcal{V}$ *of* $\mathbb{H}^m$ *of dimension* $\overline{n}$ *and* n *respectively such that* $\dim(\tau_1(\overline{\mathcal{V}})+\tau_2(\mathcal{V}))=\overline{n}+n$.

Proof (Proposition 5). Note that $\mathrm{rank}(\tau_1)\geq 2n>2\overline{n}$ and $\mathrm{rank}(\tau_2)\geq 2n>2\overline{n}$ and $\dim(\mathcal{U}_{\tau_1,\tau_2})\leq m-n<m-\overline{n}$. Invoking Proposition 4, we get a subspace $\overline{\mathcal{V}}$ of $\mathrm{Gr}_{\mathbb{H}}(\overline{n},m)$ which satisfies $\dim(\tau_1(\overline{\mathcal{V}})+\tau_2(\overline{\mathcal{V}}))=2\overline{n}$. The dimension of the subspace $\tau_2^{-1}(\tau_1(\overline{\mathcal{V}})+\tau_2(\overline{\mathcal{V}}))$ is at most $(m-\mathrm{rank}(\tau_2))+2\overline{n}$, and

$$(n-\overline{n})+[(m-\mathrm{rank}(\tau_2))+2\overline{n}]=m+(n+\overline{n}-\mathrm{rank}(\tau_2))<m+2n-\mathrm{rank}(\tau_2)\leq m. \tag{13}$$

Thus, there is a subspace $\mathcal{W}$ of $\mathbb{C}^m$ of dimension $n-\overline{n}$ such that $\mathcal{W}$ intersects the subspace $\tau_2^{-1}(\tau_1(\overline{\mathcal{V}})+\tau_2(\overline{\mathcal{V}}))$ only at zero (e.g., see Lemma 2). With Lemma 1 we get $\mathcal{W}\cap\ker(\tau_2)=0$ and $\tau_2(\mathcal{W})\cap[\tau_1(\overline{\mathcal{V}})+\tau_2(\overline{\mathcal{V}})]=0$. Hence $\mathcal{W}$ intersects $\overline{\mathcal{V}}$ only at zero, $\dim(\mathcal{W}+\overline{\mathcal{V}})=n$, and

$$\dim(\tau_1(\overline{\mathcal{V}})+\tau_2(\mathcal{W}+\overline{\mathcal{V}}))=\dim(\tau_2(\mathcal{W}))+\dim(\tau_1(\overline{\mathcal{V}})+\tau_2(\overline{\mathcal{V}}))=n-\overline{n}+2\overline{n}=n+\overline{n}. \tag{14}$$

Letting $\mathcal{V}=\mathcal{W}+\overline{\mathcal{V}}$ we are done. □

The product $\mathrm{Gr}_{\mathbb{H}}(\overline{n},n)\times\mathrm{Gr}_{\mathbb{H}}(n,m)$ of the Grassmannians contains what is known as the *flag variety* $\mathrm{F}_{\mathbb{H}}(\overline{n},n,m)$ on which every element $(\overline{\mathcal{V}}',\mathcal{V}')$ satisfies $\overline{\mathcal{V}}'\subset\mathcal{V}'$. With $\overline{\mathcal{V}}$ and $\mathcal{V}$ of Proposition 5 we know that

$$\mathbb{U}_2:=\{(\overline{\mathcal{V}},\mathcal{V})\in\mathrm{F}_{\mathbb{H}}(\overline{n},n,m):\dim_{\mathbb{H}}(\tau_1(\overline{\mathcal{V}})+\tau_2(\mathcal{V}))=\overline{n}+n\} \tag{15}$$

is not empty. Similar to the argument that $\mathbb{U}_1$ is Zariski open, $\mathbb{U}_2$ is also Zariski open.

We then show that for ϕ the canonical projection from $\mathrm{F}_{\mathbb{H}}(\overline{n},n,m)$ onto $\mathrm{Gr}_{\mathbb{H}}(n,m)$, the image $\phi(\mathbb{U}_2)$ contains a non-empty Zariski open subset of $\mathrm{Gr}_{\mathbb{H}}(n,m)$. It is not empty. Assume $\phi(\mathbb{U}_2)\neq\mathrm{Gr}_{\mathbb{H}}(n,m)$ and assume for the sake of contradiction that $\phi(\mathbb{U}_2)$ is contained in some proper closed subset of $\mathrm{Gr}_{\mathbb{H}}(n,m)$. Then there is a non-empty open set of $\mathrm{Gr}_{\mathbb{H}}(n,m)$ which does not intersect $\phi(\mathbb{U}_2)$, and thus its inverse image is also a non-empty open set of $\mathrm{F}_{\mathbb{H}}(\overline{n},n,m)$ not intersecting $\mathbb{U}_2$. This implies that $\mathrm{F}_{\mathbb{H}}(\overline{n},n,m)$ can be written as a union of two proper closed sets, contradicting to the fact that $\mathrm{F}_{\mathbb{H}}(\overline{n},n,m)$ is irreducible.

The last step is to show we have $\mathrm{hsp}(\mathcal{V},\{\tau_1,\tau_2\})$ for any $\mathcal{V}\in\phi(\mathbb{U}_2)$. Let $\tau_1(v_1)=\tau_2(v_2)$ with $v_1,v_2\in\mathcal{V}$. There is some $\overline{\mathcal{V}}$ such that $(\overline{\mathcal{V}},\mathcal{V})\in\mathbb{U}_2$. So $\dim(\tau_1(\overline{\mathcal{V}})+\tau_2(\mathcal{V}))=\overline{n}+n$, and in particular $\dim(\tau_1(\overline{\mathcal{V}})+\tau_2(\overline{\mathcal{V}}))=2\overline{n}$, which indicates $\overline{\mathcal{V}}\cap\mathscr{E}_{(\tau_1,\tau_2),1}=0$. Thus $\overline{\mathcal{V}}\cap\mathscr{E}_{(\tau_1,\tau_2),1}\cap\mathcal{V}=0$. Consequently, $\mathcal{V}$ is a direct sum of $\overline{\mathcal{V}}$ and $\mathscr{E}_{(\tau_1,\tau_2),1}\cap\mathcal{V}$. Write v_1 as a sum of two vectors $\overline{v}$ and w in $\overline{\mathcal{V}}$ and $\mathcal{V}\cap\mathscr{E}_{(\tau_1,\tau_2),1}$ respectively. Then $\tau_1(v_1)=\tau_2(v_2)$ implies $\tau_1(\overline{v})=\tau_2(v_2)-\tau_1(w)=\tau_2(v_2-w)$. Since $\overline{v}\in\overline{\mathcal{V}}$ and $(v_2-w)\in\mathcal{V}$ and $(\overline{\mathcal{V}},\mathcal{V})\in\mathbb{U}_2$, the definition of $\mathbb{U}_2$ implies that $\overline{v}=v_2-w=0$. That is, $v_1=w+\overline{v}=w=v_2$. The proof is complete. □

3.1.1. Proof of Proposition 4

For $\mathbb{H}=\mathbb{R}$ it suffices to show that $\mathrm{rank}[T_1A\ T_2A]=2n$ with $T_1,T_2\in\mathbb{R}^{m\times m}$ for some $A\in\mathbb{R}^{m\times n}$, that is, some $2n\times 2n$ minor of $[T_1A\ T_2A]$ is a nonzero polynomial with real coefficients in entries of A. This holds true whenever there is some $A^*\in\mathbb{C}^{m\times n}$ at which the evaluation of some $2n\times 2n$ minor of $[T_1A\ T_2A]$ is non-zero. Hence it suffices to prove Proposition 4 for $\mathbb{H}=\mathbb{C}$.

Let us first define a series of subspaces and discover their properties. Write $\mathcal{R}_0 := \mathbb{C}^m$, $\mathcal{F}_0 := \mathbb{C}^m$. For any non-negative integer j define

$$\begin{aligned} \mathcal{G}_{j+1} &= \tau_1(\mathcal{R}_j \cap \mathcal{F}_j) \cap \tau_2(\mathcal{R}_j \cap \mathcal{F}_j), \\ \mathcal{R}_{j+1} &= \tau_1^{-1}(\mathcal{G}_{j+1}) \cap \mathcal{R}_j \cap \mathcal{F}_j, \\ \mathcal{F}_{j+1} &= \tau_2^{-1}(\mathcal{G}_{j+1}) \cap \mathcal{R}_j \cap \mathcal{F}_j. \end{aligned} \tag{16}$$

The next lemma shows that what were defined in (16) are three chains of subspaces.

Lemma 3. *We have $\mathcal{R}_{j+1} \subset \mathcal{R}_j \cap \mathcal{F}_j \subset \mathcal{R}_j$ and $\mathcal{F}_{j+1} \subset \mathcal{R}_j \cap \mathcal{F}_j \subset \mathcal{F}_j$ and $\mathcal{G}_{j+2} \subset \mathcal{G}_{j+1}$ and $\tau_1(\mathcal{R}_{j+1}) = \tau_2(\mathcal{F}_{j+1}) = \mathcal{G}_{j+1}$ for any non-negative integer j.*

Proof. By definition (16) we have $\mathcal{R}_{j+1} \subset \mathcal{R}_j \cap \mathcal{F}_j \subset \mathcal{R}_j$ and $\mathcal{F}_{j+1} \subset \mathcal{R}_j \cap \mathcal{F}_j \subset \mathcal{F}_j$. Note also $\mathcal{R}_{j+1} \cap \mathcal{F}_{j+1} \subset \mathcal{R}_j \cap \mathcal{F}_j$. This further implies that

$$\mathcal{G}_{j+2} = \tau_1(\mathcal{R}_{j+1} \cap \mathcal{F}_{j+1}) \cap \tau_2(\mathcal{R}_{j+1} \cap \mathcal{F}_{j+1}) \subset \tau_1(\mathcal{R}_j \cap \mathcal{F}_j) \cap \tau_2(\mathcal{R}_j \cap \mathcal{F}_j) = \mathcal{G}_{j+1}. \tag{17}$$

Also noting that $\mathcal{G}_{j+1} \subset \tau_1(\mathcal{R}_j \cap \mathcal{F}_j) \subset \operatorname{im}(\tau_1)$ and $\mathcal{R}_{j+1} \subset \tau_1^{-1}(\mathcal{G}_{j+1})$ for any non-negative integer j, we have $\tau_1(\mathcal{R}_{j+1}) \subset \tau_1(\tau_1^{-1}(\mathcal{G}_{j+1})) = \mathcal{G}_{j+1}$. To show $\mathcal{G}_{j+1} \subset \tau_1(\mathcal{R}_{j+1})$ we let $z \in \mathcal{G}_{j+1} = \tau_1(\mathcal{R}_j \cap \mathcal{F}_j) \cap \tau_2(\mathcal{R}_j \cap \mathcal{F}_j)$. In particular $z \in \tau_1(\mathcal{R}_j \cap \mathcal{F}_j)$. So there is some $w \in \mathcal{R}_j \cap \mathcal{F}_j$ such that $\tau_1(w) = z$. Then $w \in \tau_1^{-1}(z) \cap \mathcal{R}_j \cap \mathcal{F}_j$. But $\tau_1^{-1}(z) \subset \tau_1^{-1}(\mathcal{G}_{j+1})$, and this suggests $w \in \tau_1^{-1}(\mathcal{G}_{j+1}) \cap \mathcal{R}_j \cap \mathcal{F}_j = \mathcal{R}_{j+1}$. With $\tau_1(w) = z$ we see that $z \in \tau_1(\mathcal{R}_{j+1})$. To conclude, we get $\tau_1(\mathcal{R}_{j+1}) = \mathcal{G}_{j+1}$. A similar derivation gives $\tau_2(\mathcal{F}_{j+1}) = \mathcal{G}_{j+1}$. □

It is expected that those chains will be stable eventually at some point and yield some special property.

Lemma 4. *There is a non-negative integer α for which $\mathcal{R}_\alpha = \mathcal{F}_\alpha$ and $\tau_1(\mathcal{R}_\alpha) = \tau_2(\mathcal{R}_\alpha)$.*

Proof (Lemma 4). From Lemma 3 we see two chains $\cdots \subset \mathcal{R}_{j+1} \subset \mathcal{R}_j \subset \cdots \subset \mathcal{R}_0$ and $\cdots \subset \mathcal{F}_{j+1} \subset \mathcal{F}_j \subset \cdots \subset \mathcal{F}_0$. Since the subspaces $\mathcal{R}_0$ and $\mathcal{F}_0$ are of finite dimension m, these two chains stabilize respectively, that is, there exist some non-negative integers α_1 and α_2 such that for any integers $j_1 \geq \alpha_1$ and $j_2 \geq \alpha_2$ it holds that $\mathcal{R}_{j_1} = \mathcal{R}_{j_1+1}$ and $\mathcal{F}_{j_2} = \mathcal{F}_{j_2+1}$. Let $\alpha := \max\{\alpha_1, \alpha_2\}$. We then have $\mathcal{R}_\alpha = \mathcal{R}_{\alpha+1}$ and $\mathcal{F}_\alpha = \mathcal{F}_{\alpha+1}$. With Lemma 3 we obtain $\mathcal{R}_{\alpha+1} \subset \mathcal{R}_\alpha \cap \mathcal{F}_\alpha \subset \mathcal{R}_\alpha = \mathcal{R}_{\alpha+1}$. This implies $\mathcal{R}_\alpha = \mathcal{R}_\alpha \cap \mathcal{F}_\alpha$. Similarly we get $\mathcal{F}_\alpha = \mathcal{R}_\alpha \cap \mathcal{F}_\alpha$. It follows that $\mathcal{R}_\alpha = \mathcal{F}_\alpha$. Lemma 3 then gives $\tau_1(\mathcal{R}_\alpha) = \tau_2(\mathcal{R}_\alpha)$. □

Lemma 4 suggests to focus on the chain acsending from $\mathcal{R}_\alpha$ say

$$\mathcal{R}_\alpha \subset \mathcal{R}_{\alpha-1} \cap \mathcal{F}_{\alpha-1} \subset \mathcal{R}_{\alpha-1} \subset \cdots \subset \mathcal{R}_1 \subset \mathcal{R}_0 \cap \mathcal{F}_0 \subset \mathcal{R}_0 = \mathbb{C}^m. \tag{18}$$

Our proof rests on chain (18) and the strategy is as follows. We start by exhibiting a subspace say $\mathcal{W}_j$ inside some subspace $\mathcal{R}_j$ on chain (18) such that $\dim(\tau_1(\mathcal{W}_j) + \tau_2(\mathcal{W}_j)) = 2\dim(\mathcal{W}_j)$. While $\mathcal{W}_j$ may have smaller dimension than the required n, we provide devices with which we are capable of ascending the chain and recursively extending $\mathcal{W}_j$ to a larger subspace say $\mathcal{W}_{j-1}$ contained in $\mathcal{R}_{j-1}$, and at the same time keeping the property $\dim(\tau_1(\mathcal{W}_{j-1}) + \tau_2(\mathcal{W}_{j-1})) = 2\dim(\mathcal{W}_{j-1})$, eventually obtaining the desired subspace $\mathcal{V} = \mathcal{W}_0$.

The first step is to find some subspace $\mathcal{W}_j$ to start with. The next lemma provides such one.

Lemma 5. *In addition to the hypotheses of Proposition 4, suppose $\dim(\mathcal{R}_\alpha) > m - n$, then there is a subspace $\mathcal{W}_\alpha$ of $\mathcal{R}_\alpha$ of dimension $[\dim(\mathcal{R}_\alpha) - (m-n)]$ such that $\dim(\tau_1(\mathcal{W}_\alpha) + \tau_2(\mathcal{W}_\alpha)) = 2\dim(\mathcal{W}_\alpha)$.*

Proof (Lemma 5). The first implication of $\mathcal{R}_\alpha = \mathcal{F}_\alpha$ and $\tau_1(\mathcal{R}_\alpha) = \tau_2(\mathcal{R}_\alpha) = \mathcal{G}_\alpha$ is that

$$\dim(\ker(\tau_1) \cap \mathcal{R}_\alpha) = \dim(\mathcal{R}_\alpha) - \dim(\mathcal{G}_\alpha) = \dim(\ker(\tau_2) \cap \mathcal{R}_\alpha). \tag{19}$$

This implies that $(m-n) + \dim(\mathcal{G}_\alpha) - \dim(\mathcal{R}_\alpha) = \operatorname{rank}(\tau_1) - n > 0$. From Lemma ?? we know that $\mathcal{U}_{\tau_1,\tau_2}$ has the same dimension as its closure $\overline{\mathcal{U}}_{\tau_1,\tau_2}$. Hence $\overline{\mathcal{U}}_{\tau_1,\tau_2}$ and $\mathscr{E}_{(\tau_1,\tau_2),1}$ are both of dimensions at most

$(m-n)$. By Lemma 2 there is a subspace $\mathcal{H}$ of $\mathcal{R}_\alpha$ of dimension $\dim(\mathcal{G}_\alpha)$ which intersects both $\ker(\tau_1)$ and $\ker(\tau_2)$ only at zero, and such that

$$\dim(\overline{\mathcal{U}}_{\tau_1,\tau_2} \cap \mathcal{H}) \le (m-n) + \dim(\mathcal{G}_\alpha) - \dim(\mathcal{R}_\alpha), \tag{20}$$

$$\dim(\mathscr{E}_{(\tau_1,\tau_2),1} \cap \mathcal{H}) \le (m-n) + \dim(\mathcal{G}_\alpha) - \dim(\mathcal{R}_\alpha). \tag{21}$$

Let $\tau_1|_\mathcal{H}$ and $\tau_2|_\mathcal{H}$ be restrictions of τ_1 and τ_2 on $\mathcal{H}$ respectively. Since $\ker(\tau_1) \cap \mathcal{H} = \ker(\tau_2) \cap \mathcal{H} = 0$, we have that $\tau_1|_\mathcal{H}$ and $\tau_2|_\mathcal{H}$ are isomorphisms from $\mathcal{H}$ to $\mathcal{G}_\alpha$. Recalling that $\mathcal{H}$ is a subspace of $\mathcal{R}_\alpha$ and $\tau_1(\mathcal{R}_\alpha) = \tau_2(\mathcal{R}_\alpha)$, we have $\tau_1(\mathcal{H}) = \mathcal{G}_\alpha = \tau_2(\mathcal{H})$. So $\tau_\mathcal{H} := (\tau_1|_\mathcal{H})^{-1}\tau_2|_\mathcal{H}$ is an isomorphism of $\mathcal{H}$. Since $\dim(\mathcal{H}) = \dim(\mathcal{G}_\alpha) = \dim(\mathcal{R}_\alpha) - \dim(\ker(\tau_1) \cap \mathcal{R}_\alpha) \ge \dim(\mathcal{R}_\alpha) - (m - \operatorname{rank}(\tau_1)) > \dim(\mathcal{R}_\alpha) - (m-n)$, $\mathcal{H}$ can contain a subspace of dimension $[\dim(\mathcal{R}_\alpha) - (m-n)]$. Recalling that $\mathscr{E}_{\tau,\lambda}$ denotes the eigenspace of a linear map τ of $\mathbb{C}^m$ corresponding to the eigenvalue $\lambda \in \mathbb{C}$, we will need Lemma 3 of [2].

Lemma 6 (Lemma 5 of [2], restated). *Suppose for any $\lambda \in \mathbb{C}$ and some linear map τ of $\mathcal{H}$ we have $\dim(\mathscr{E}_{\tau,\lambda}) \le \dim(\mathcal{H}) - [\dim(\mathcal{R}_\alpha) - (m-n)]$ and $\dim(\mathcal{H}) \ge 2[\dim(\mathcal{R}_\alpha) - (m-n)]$. There is a subspace $\mathcal{W}_\alpha$ of $\mathcal{H}$ of dimension $[\dim(\mathcal{R}_\alpha) - (m-n)]$ such that $\dim(\mathcal{W}_\alpha + \tau(\mathcal{W}_\alpha)) = 2\dim(\mathcal{W}_\alpha)$.*

Next we will show that $\tau_\mathcal{H}$ satisfies the conditions of Lemma 6. First note that

$$\begin{aligned}
\dim(\mathcal{H}) \ge 2[\dim(\mathcal{R}_\alpha) - (m-n)] &\Leftrightarrow 2m - 2n \ge \dim(\mathcal{R}_\alpha) + \dim(\mathcal{R}_\alpha) - \dim(\mathcal{G}_\alpha) && (22)\\
&\Leftrightarrow 2m - 2n \ge \dim(\mathcal{R}_\alpha) + \dim(\ker(\tau_1) \cap \mathcal{R}_\alpha) && (23)\\
&\Leftarrow 2m - 2n \ge \dim(\mathcal{R}_\alpha) + \dim(\ker(\tau_1)) && (24)\\
&\Leftrightarrow (\operatorname{rank}(\tau_1) - 2n) + (m - \dim(\mathcal{R}_\alpha)) \ge 0. && (25)
\end{aligned}$$

Another condition of Lemma 6 is that for any $\lambda \in \mathbb{C}$ it holds that

$$\dim(\mathscr{E}_{\tau_\mathcal{H},\lambda}) \le \dim(\mathcal{H}) - [\dim(\mathcal{R}_\alpha) - (m-n)], \tag{26}$$

which is true for the following reason. When $\lambda = 0$, the eigenspace $\mathscr{E}_{\tau_\mathcal{H},0}$ is exactly $\ker(\tau_\mathcal{H})$, which is zero since $\tau_\mathcal{H}$ is an isomorphism. When $\lambda \ne 0$, note that $\mathscr{E}_{\tau_\mathcal{H},\lambda}$ is exactly the set of all points v's of $\mathbb{C}^m$ satisfying $\tau_1|_\mathcal{H}(v) = \lambda\tau_2|_\mathcal{H}(v)$. That is, $\tau_1(v) = \lambda\tau_2(v)$ and $v \in \mathcal{H}$. Recalling the definition of $\mathcal{Y}_{\tau_1,\tau_2}$ we get $v \in \mathcal{Y}_{\tau_1,\tau_2} \cap \mathcal{H}$. But the definitions of $\mathcal{H}$ and $\mathcal{U}_{\tau_1,\tau_2}$ imply $v \in \overline{\mathcal{U}}_{\tau_1,\tau_2} \cap \mathcal{H}$ or $v \in \mathscr{E}_{(\tau_1,\tau_2),1} \cap \mathcal{H}$. It follows that $\mathscr{E}_{\tau_\mathcal{H},\lambda}$ is a subset of $\overline{\mathcal{U}}_{\tau_1,\tau_2} \cap \mathcal{H}$ or $\mathscr{E}_{(\tau_1,\tau_2),1} \cap \mathcal{H}$, both of which have dimension at most $(m-n) + \dim(\mathcal{G}_\alpha) - \dim(\mathcal{R}_\alpha)$ as per (20) and (21). Together, we have proved (26) for any $\lambda \in \mathbb{C}$. Then Lemma 6 is applicable and we get the subspace $\mathcal{W}_\alpha \subset \mathcal{H}$ of dimension $[\dim(\mathcal{R}_\alpha) - (m-n)]$ such that $\mathcal{W}_\alpha + \tau_\mathcal{H}(\mathcal{W}_\alpha)$ has dimension $2[\dim(\mathcal{R}_\alpha) - (m-n)]$.

Since $\tau_1|_\mathcal{H}$ is an isomorphism from $\mathcal{H}$ to $\mathcal{G}_\alpha$ and $\mathcal{W}_\alpha + \tau_\mathcal{H}(\mathcal{W}_\alpha)$ is a subspace of $\mathcal{H}$, we see that $\tau_1|_\mathcal{H}(\mathcal{W}_\alpha + \tau_\mathcal{H}(\mathcal{W}_\alpha)) = \tau_1|_\mathcal{H}(\mathcal{W}_\alpha) + \tau_2|_\mathcal{H}(\mathcal{W}_\alpha)$ also has dimension $2[\dim(\mathcal{R}_\alpha) - (m-n)]$. But note that $\tau_1|_\mathcal{H}(\mathcal{W}_\alpha) + \tau_2|_\mathcal{H}(\mathcal{W}_\alpha) = \tau_1(\mathcal{W}_\alpha) + \tau_2(\mathcal{W}_\alpha)$. We finished the proof. $\square$

Note that Lemma 5 places in addition the dimension constraint $\dim(\mathcal{R}_\alpha) > m - n$ on $\mathcal{R}_\alpha$. When $\alpha = 0$ we get $\dim(\mathcal{R}_\alpha) = m$, and we finished the proof of Proposition 4 by Lemma 5. Assume $\alpha > 0$ in what follows.

Then, this dimension constraint on $\mathcal{R}_\alpha$ might be voilated because by construction (Lemma 4) it is quite possible for $\mathcal{R}_\alpha$ to be the trivial subspace 0. On the other hand, the converse $\dim(\mathcal{R}_\alpha) \le m - n$ implies a dimension transition on chain (18) in the sense that there exist some non-negative integers β or γ satisfying $\dim(\mathcal{R}_{\beta+1}) \le m - n < \dim(\mathcal{R}_\beta \cap \mathcal{F}_\beta)$ or $\dim(\mathcal{R}_\gamma \cap \mathcal{F}_\gamma) \le m - n < \dim(\mathcal{R}_\gamma)$. It is at this transition that we can obtain the subspace of interest as an alternative starting point, via the next two lemmas.

Lemma 7 (Dimension Transition-1). *In addition to the hypotheses of Proposition 4, suppose for some non-negative integer β that $\dim(\mathcal{R}_{\beta+1}) \le m - n < \dim(\mathcal{R}_\beta \cap \mathcal{F}_\beta)$, then there exists a subspace $\mathcal{Z}_\beta$ of $\mathcal{R}_\beta \cap \mathcal{F}_\beta$ of dimension $[\dim(\mathcal{R}_\beta \cap \mathcal{F}_\beta) - (m-n)]$ such that $\dim(\tau_1(\mathcal{Z}_\beta) + \tau_2(\mathcal{Z}_\beta)) = 2\dim(\mathcal{Z}_\beta)$.*

Lemma 8 (Dimension Transition-2). *In addition to the hypotheses of Proposition 4, suppose for some non-negative integer γ that $\dim(\mathcal{R}_\gamma \cap \mathcal{F}_\gamma) \le m - n < \dim(\mathcal{R}_\gamma)$. Then there exists a subspace $\mathcal{W}_\gamma$ of $\mathcal{R}_\gamma$ of dimension $[\dim(\mathcal{R}_\gamma) - (m-n)]$ such that $\dim(\tau_1(\mathcal{W}_\gamma) + \tau_2(\mathcal{W}_\gamma)) = 2\dim(\mathcal{W}_\gamma)$.*

Proof (Lemma 7). Note that we have

$$[\dim(\mathcal{R}_\beta \cap \mathcal{F}_\beta) - (m-n)] + \dim(\ker(\tau_1)) = \dim(\mathcal{R}_\beta \cap \mathcal{F}_\beta) + (n - \operatorname{rank}(\tau_2)) < \dim(\mathcal{R}_\beta \cap \mathcal{F}_\beta) \tag{27}$$

and similarly

$$[\dim(\mathcal{R}_\beta \cap \mathcal{F}_\beta) - (m-n)] + \dim(\ker(\tau_2)) \leq \dim(\mathcal{R}_\beta \cap \mathcal{F}_\beta). \tag{28}$$

Also note that

$$[\dim(\mathcal{R}_\beta \cap \mathcal{F}_\beta) - (m-n)] + \dim(\mathcal{R}_{\beta+1}) = \dim(\mathcal{R}_\beta \cap \mathcal{F}_\beta) + [\dim(\mathcal{R}_{\beta+1}) - (m-n)] \leq \dim(\mathcal{R}_\beta \cap \mathcal{F}_\beta). \tag{29}$$

Lemma 2implies that there is a subspace $\mathcal{Z}_\beta$ of $\mathcal{R}_\beta \cap \mathcal{F}_\beta$ of dimension $[\dim(\mathcal{R}_\beta \cap \mathcal{F}_\beta) - (m-n)]$ which intersects $\ker(\tau_1)$ and $\ker(\tau_2)$ and $\mathcal{R}_{\beta+1}$ only at zero, respectively. This gives $\dim(\tau_1(\mathcal{Z}_\beta)) = \dim(\tau_2(\mathcal{Z}_\beta)) = \dim(\mathcal{Z}_\beta)$.

It now suffices to prove $\tau_1(\mathcal{Z}_\beta) \cap \tau_2(\mathcal{Z}_\beta) = 0$. Let $\tau_1(v_1) = \tau_2(v_2)$ for some $v_1, v_2 \in \mathcal{Z}_\beta$. Hence $\tau_1(v_1)$ is contained in $\tau_1(\mathcal{R}_\beta \cap \mathcal{F}_\beta)$ and $\tau_1(v_1) = \tau_2(v_2)$ is contained in $\tau_2(\mathcal{R}_\beta \cap \mathcal{F}_\beta)$. In sum we have

$$\tau_1(v_1) \in \tau_1(\mathcal{R}_\beta \cap \mathcal{F}_\beta) \cap \tau_2(\mathcal{R}_\beta \cap \mathcal{F}_\beta) = \mathcal{G}_{\beta+1}. \tag{30}$$

This implies $v_1 \in \tau_1^{-1}(\mathcal{G}_{\beta+1})$ and so

$$v_1 \in \mathcal{Z}_\beta \cap \tau_1^{-1}(\mathcal{G}_{\beta+1}) = \mathcal{Z}_\beta \cap \tau_1^{-1}(\mathcal{G}_{\beta+1}) \cap \mathcal{R}_\beta \cap \mathcal{F}_\beta = \mathcal{R}_{\beta+1} \cap \mathcal{Z}_\beta = 0. \tag{31}$$

That is, $v_1 = 0$. Then $0 = \tau_2(v_2)$, which implies $v_2 \in \ker(\tau_2) \cap \mathcal{Z}_\beta = 0$. We proved $\tau_1(\mathcal{Z}_\beta) \cap \tau_2(\mathcal{Z}_\beta) = 0$. □

Proof (Lemma 8). Clearly $\gamma \neq 0$. Note that we have

$$[\dim(\mathcal{R}_\gamma) - (m-n)] + \dim(\ker(\tau_1)) = \dim(\mathcal{R}_\gamma) + (m - \operatorname{rank}(\tau_1)) - (m-n) < \dim(\mathcal{R}_\gamma) \tag{32}$$

and similarly

$$[\dim(\mathcal{R}_\gamma) - (m-n)] + \dim(\ker(\tau_2)) \leq \dim(\mathcal{R}_\gamma). \tag{33}$$

Also note that

$$[\dim(\mathcal{R}_\gamma) - (m-n)] + \dim(\mathcal{R}_\gamma \cap \mathcal{F}_\gamma) \leq \dim(\mathcal{R}_\gamma) + [\dim(\mathcal{R}_\gamma \cap \mathcal{F}_\gamma) - (m-n)] \leq \dim(\mathcal{R}_\gamma). \tag{34}$$

Consequently, by Lemma 2, there exists a subspace $\mathcal{W}_\gamma$ of $\mathcal{R}_\gamma$ of dimension $[\dim(\mathcal{R}_\gamma) - (m-n)]$ which intersects $\ker(\tau_1)$ and $\ker(\tau_2)$ and $\mathcal{R}_\gamma \cap \mathcal{F}_\gamma$ only at zero, respectively. By Lemma 3 we get $\tau_1(\mathcal{W}_\gamma) \subset \tau_1(\mathcal{R}_\gamma) = \mathcal{G}_\gamma$. Recalling definition (16) and $\mathcal{W}_\gamma \subset \mathcal{R}_\gamma$ we obtain

$$\begin{aligned}
\mathcal{W}_\gamma \cap \tau_2^{-1}(\tau_1(\mathcal{W}_\gamma)) &\subset \mathcal{W}_\gamma \cap \tau_2^{-1}(\mathcal{G}_\gamma) && (35)\\
&= \mathcal{W}_\gamma \cap \tau_2^{-1}(\mathcal{G}_\gamma) \cap \mathcal{R}_\gamma && (36)\\
&= \mathcal{W}_\gamma \cap \tau_2^{-1}(\mathcal{G}_\gamma) \cap \tau_1^{-1}(\mathcal{G}_\gamma) \cap \mathcal{R}_{\gamma-1} \cap \mathcal{F}_{\gamma-1} && (37)\\
&= \mathcal{W}_\gamma \cap \tau_1^{-1}(\mathcal{G}_\gamma) \cap \mathcal{F}_\gamma && (38)\\
&\subset \mathcal{W}_\gamma \cap \mathcal{F}_\gamma = \mathcal{W}_\gamma \cap \mathcal{R}_\gamma \cap \mathcal{F}_\gamma = 0. && (39)
\end{aligned}$$

In short $\mathcal{W}_\gamma \cap \tau_2^{-1}(\tau_1(\mathcal{W}_\gamma)) = 0$, and it follows from Lemma 1 that $\tau_2(\mathcal{W}_\gamma) \cap \tau_1(\mathcal{W}_\gamma) = 0$. Recalling that $\mathcal{W}_\gamma \cap \ker(\tau_1) = 0$ and $\mathcal{W}_\gamma \cap \ker(\tau_2) = 0$, we conclude with $\dim(\tau_1(\mathcal{W}_\gamma) + \tau_2(\mathcal{W}_\gamma)) = 2\dim(\mathcal{W}_\gamma)$. □

As summarized in Table 1, we have obtained three subspaces $\mathcal{W}_\alpha$, $\mathcal{Z}_\beta$, and $\mathcal{W}_\gamma$ contained in $\mathcal{R}_\alpha$, $\mathcal{R}_\beta \cap \mathcal{F}_\beta$, and $\mathcal{R}_\gamma$, respectively, depending on whether the aformentioned dimension transition exists (Lemma 5) or if so where it happens (Lemmas 7 and 8). Note that $\mathcal{Z}_\beta$ is a subspace of $\mathcal{Z}_\beta \subset \mathcal{R}_\beta \cap \mathcal{F}_\beta$ satisfying

$$\mathscr{P}(\mathcal{Z}_\beta): \ \dim(\mathcal{Z}_\beta) = [\dim(\mathcal{R}_\beta \cap \mathcal{F}_\beta) - (m-n)] \quad \text{and} \quad \dim(\tau_1(\mathcal{Z}_\beta) + \tau_2(\mathcal{Z}_\beta)) = 2\dim(\mathcal{Z}_\beta). \tag{40}$$

Table 1: Three different cases and Lemmas that address them.

Cases	Lemmas
$m-n<\dim(\mathcal{R}_\alpha)$	Lemma 5
$\dim(\mathcal{R}_{\beta+1})\le m-n<\dim(\mathcal{R}_\beta\cap\mathcal{F}_\beta)$	Lemma 7
$\dim(\mathcal{R}_\gamma\cap\mathcal{F}_\gamma)\le m-n<\dim(\mathcal{R}_\gamma)$	Lemma 8

Let μ be either α or γ then we see that the subspace $\mathcal{W}_\mu$ of $\mathcal{R}_\mu$ satisfies

$$\mathscr{P}(\mathcal{W}_\mu):\ \dim(\mathcal{W}_\mu)=[\dim(\mathcal{R}_\mu)-(m-n)]\ \text{ and }\ \dim(\tau_1(\mathcal{W}_\mu)+\tau_2(\mathcal{W}_\mu))=2\dim(\mathcal{W}_\mu). \tag{41}$$

Thus the three cases in Table 1 give rise to two possible chains say

$$\begin{array}{l}\mathcal{R}_\beta\cap\mathcal{F}_\beta\subset\mathcal{R}_\beta\subset\cdots\subset\mathcal{R}_0=\mathbb{C}^m\\ \quad\cup\\ \quad\mathcal{Z}_\beta\end{array} \tag{42}$$

and

$$\begin{array}{l}\mathcal{R}_\mu\subset\mathcal{R}_{\mu-1}\cap\mathcal{F}_{\mu-1}\subset\cdots\subset\mathcal{R}_0=\mathbb{C}^m\\ \cup\\ \mathcal{W}_\mu\end{array} \tag{43}$$

where we added $\mathcal{Z}_\beta$ or $\mathcal{W}_\mu$ into chain (18).

The next step is to extend $\mathcal{Z}_\beta$ or $\mathcal{W}_\gamma$ in chain (42) or (43), recursively if necessary.

Lemma 9 (Extension-1). *In addition to the hypotheses of Proposition 4, suppose for some non-negative integer j that $\dim(\mathcal{R}_j\cap\mathcal{F}_j)>m-n$ and that there exists a subspace $\mathcal{Z}_j$ of $\mathcal{R}_j\cap\mathcal{F}_j$ satisfying*

$$\mathscr{P}(\mathcal{Z}_j):\ \dim(\mathcal{Z}_j)=[\dim(\mathcal{R}_j\cap\mathcal{F}_j)-(m-n)]\ \text{ and }\ \dim(\tau_1(\mathcal{Z}_j)+\tau_2(\mathcal{Z}_j))=2\dim(\mathcal{Z}_j). \tag{44}$$

Then there exists a subspace $\mathcal{W}_j$ of $\mathcal{R}_j$ satisfying $\mathcal{Z}_j\subset\mathcal{W}_j$ and

$$\mathscr{P}(\mathcal{W}_j):\ \dim(\mathcal{W}_j)=[\dim(\mathcal{R}_j)-(m-n)]\ \text{ and }\ \dim(\tau_1(\mathcal{W}_j)+\tau_2(\mathcal{W}_j))=2\dim(\mathcal{W}_j). \tag{45}$$

Lemma 10 (Extension-2). *In addition to the hypotheses of Proposition 4, suppose for some non-negative integer j that $\dim(\mathcal{R}_{j+1})>m-n$, and that there exists a subspace $\mathcal{W}_{j+1}$ of $\mathcal{R}_{j+1}$ satisfying*

$$\mathscr{P}(\mathcal{W}_{j+1}):\ \dim(\mathcal{W}_{j+1})=[\dim(\mathcal{R}_{j+1})-(m-n)]\ \text{ and }\ \dim(\tau_1(\mathcal{W}_{j+1})+\tau_2(\mathcal{W}_{j+1}))=2\dim(\mathcal{W}_{j+1}). \tag{46}$$

Then there exists a subspace $\mathcal{Z}_j$ of $\mathcal{R}_j\cap\mathcal{F}_j$ satisfying $\mathcal{W}_{j+1}\subset\mathcal{Z}_j$ and

$$\mathscr{P}(\mathcal{Z}_j):\ \dim(\mathcal{Z}_j)=[\dim(\mathcal{R}_j\cap\mathcal{F}_j)-(m-n)]\ \text{ and }\ \dim(\tau_1(\mathcal{Z}_j)+\tau_2(\mathcal{Z}_j))=2\dim(\mathcal{Z}_j). \tag{47}$$

Proof (Lemma 9). Clearly $\mathcal{R}_j\cap\mathcal{F}_j\subset\mathcal{R}_j$. If $\mathcal{R}_j\cap\mathcal{F}_j=\mathcal{R}_j$ we are done by letting $\mathcal{W}_j=\mathcal{Z}_j$. In what follows we assume $\dim(\mathcal{R}_j)>\dim(\mathcal{R}_j\cap\mathcal{F}_j)$. This implies $j\neq 0$.

Note that $[\dim(\mathcal{R}_j)-\dim(\mathcal{R}_j\cap\mathcal{F}_j)]+\dim(\mathcal{R}_j\cap\mathcal{F}_j)=\dim(\mathcal{R}_j)$. The inverse image $\tau_1^{-1}(\tau_1(\mathcal{Z}_j)+\tau_2(\mathcal{Z}_j))$ has dimension at most $(m-\operatorname{rank}(\tau_1))+2[\dim(\mathcal{R}_j\cap\mathcal{F}_j)-(m-n)]$. So the summation $[\dim(\mathcal{R}_j)-\dim(\mathcal{R}_j\cap\mathcal{F}_j)]+\dim(\tau_1^{-1}(\tau_1(\mathcal{Z}_j)+\tau_2(\mathcal{Z}_j)))$ is at most

$$\dim(\mathcal{R}_j)+[2n-\operatorname{rank}(\tau_1)]+[\dim(\mathcal{R}_j\cap\mathcal{F}_j)-m]\le\dim(\mathcal{R}_j). \tag{48}$$

Hence, by Lemma 2, there is a subspace $\mathcal{W}_j'$ of $\mathcal{R}_j$ of dimension $[\dim(\mathcal{R}_j)-\dim(\mathcal{R}_j\cap\mathcal{F}_j)]$ which intersects both $\mathcal{R}_j\cap\mathcal{F}_j$ and $\tau_1^{-1}(\tau_1(\mathcal{Z}_j)+\tau_2(\mathcal{Z}_j))$ only at zero, respectively. The latter with Lemma 1 implies that

$\tau_1(\mathcal{W}_j') \cap [\tau_1(\mathcal{Z}_j) + \tau_2(\mathcal{Z}_j)] = 0$ and $\mathcal{W}_j' \cap \ker(\tau_1) = 0$. So $[\tau_1(\mathcal{Z}_j) + \tau_2(\mathcal{Z}_j)] + \tau_1(\mathcal{W}_j')$ is of dimension $2[\dim(\mathcal{R}_j \cap \mathcal{F}_j) - (m-n)] + [\dim(\mathcal{R}_j) - \dim(\mathcal{R}_j \cap \mathcal{F}_j)]$. In other words,

$$\dim(\tau_1(\mathcal{Z}_j + \mathcal{W}_j') + \tau_2(\mathcal{Z}_j)) = \dim(\mathcal{R}_j) + \dim(\mathcal{R}_j \cap \mathcal{F}_j) - 2(m-n). \tag{49}$$

Since $\mathcal{Z}_j \subset \mathcal{R}_j \cap \mathcal{F}_j$ we see that $\tau_2(\mathcal{Z}_j) \subset \tau_2(\mathcal{F}_j) = \mathcal{G}_j$. With $\tau_1(\mathcal{Z}_j + \mathcal{W}_j') \subset \tau_1(\mathcal{R}_j) = \mathcal{G}_j$, we obtain that $\tau_1(\mathcal{Z}_j + \mathcal{W}_j') + \tau_2(\mathcal{Z}_j)$ is a subset of $\mathcal{G}_j$, and consequently

$$\begin{aligned}
\mathcal{W}_j' \cap \tau_2^{-1}(\tau_1(\mathcal{Z}_j + \mathcal{W}_j') + \tau_2(\mathcal{Z}_j)) &\subset \mathcal{W}_j' \cap \tau_2^{-1}(\mathcal{G}_j) && (50)\\
&= \mathcal{W}_j' \cap \tau_2^{-1}(\mathcal{G}_j) \cap \mathcal{R}_j && (51)\\
&= \mathcal{W}_j' \cap \tau_2^{-1}(\mathcal{G}_j) \cap \tau_1^{-1}(\mathcal{G}_j) \cap \mathcal{R}_{j-1} \cap \mathcal{F}_{j-1} && (52)\\
&= \mathcal{W}_j' \cap \tau_1^{-1}(\mathcal{G}_j) \cap \mathcal{F}_j && (53)\\
&\subset \mathcal{W}_j' \cap \mathcal{F}_j && (54)\\
&= \mathcal{W}_j' \cap \mathcal{F}_j \cap \mathcal{R}_j = 0. && (55)
\end{aligned}$$

From (50) to (51) we used that $\mathcal{W}_j'$ is a subset of $\mathcal{R}_j$, and from (51) to (53) we used the definitions of $\mathcal{R}_j$ and $\mathcal{F}_j$. In short we have $\mathcal{W}_j' \cap \tau_2^{-1}(\tau_1(\mathcal{Z}_j + \mathcal{W}_j') + \tau_2(\mathcal{Z}_j)) = 0$, which with Lemma 1 yields $\tau_2(\mathcal{W}_j') \cap [\tau_1(\mathcal{Z}_j + \mathcal{W}_j') + \tau_2(\mathcal{Z}_j)] = 0$ and $\mathcal{W}_j' \cap \ker(\tau_2) = 0$. Recalling (49) it follows that $[\tau_1(\mathcal{Z}_j + \mathcal{W}_j') + \tau_2(\mathcal{Z}_j)] + \tau_2(\mathcal{W}_j')$ is of dimension $[\dim(\mathcal{R}_j) + \dim(\mathcal{R}_j \cap \mathcal{F}_j) - 2(m-n)] + [\dim(\mathcal{R}_j) - \dim(\mathcal{R}_j \cap \mathcal{F}_j)]$, that is,

$$\dim(\tau_1(\mathcal{Z}_j + \mathcal{W}_j') + \tau_2(\mathcal{Z}_j + \mathcal{W}_j')) = 2\dim(\mathcal{R}_j) - 2(m-n). \tag{56}$$

By letting $\mathcal{W}_j = \mathcal{Z}_j + \mathcal{W}_j'$ we finished the proof. □

Proof (Lemma 10). Recalling $\mathcal{R}_{j+1} = \tau_1^{-1}(\mathcal{G}_{j+1}) \cap \mathcal{R}_j \cap \mathcal{F}_j$, we see that $\mathcal{R}_{j+1} \subset \mathcal{R}_j \cap \mathcal{F}_j$. If $\mathcal{R}_{j+1} = \mathcal{R}_j \cap \mathcal{F}_j$ we are done by letting $\mathcal{Z}_j = \mathcal{W}_{j+1}$. Hence we assume $\dim(\mathcal{R}_j \cap \mathcal{F}_j) > \dim(\mathcal{R}_{j+1})$ in what follows.

Note that $[\dim(\mathcal{R}_j \cap \mathcal{F}_j) - \dim(\mathcal{R}_{j+1})] + \dim(\mathcal{R}_{j+1}) = \dim(\mathcal{R}_j \cap \mathcal{F}_j)$. Since the inverse image $\tau_2^{-1}(\tau_1(\mathcal{W}_{j+1}) + \tau_2(\mathcal{W}_{j+1}))$ has dimension at most $(m - \mathrm{rank}(\tau_2)) + 2[\dim(\mathcal{R}_{j+1}) - (m-n)]$, we can see that $[\dim(\mathcal{R}_j \cap \mathcal{F}_j) - \dim(\mathcal{R}_{j+1})] + \dim(\tau_2^{-1}(\tau_1(\mathcal{W}_{j+1}) + \tau_2(\mathcal{W}_{j+1})))$ is no more than

$$\dim(\mathcal{R}_j \cap \mathcal{F}_j) + [\dim(\mathcal{R}_{j+1}) - m] + [2n - \mathrm{rank}(\tau_2)] \le \dim(\mathcal{R}_j \cap \mathcal{F}_j). \tag{57}$$

Consequently, by Lemma 2, there exists a subspace $\mathcal{Z}_j'$ of $\mathcal{R}_j \cap \mathcal{F}_j$ of dimension $[\dim(\mathcal{R}_j \cap \mathcal{F}_j) - \dim(\mathcal{R}_{j+1})]$ which intersects both $\mathcal{R}_{j+1}$ and $\tau_2^{-1}(\tau_1(\mathcal{W}_{j+1}) + \tau_2(\mathcal{W}_{j+1}))$ only at zero, respectively. The later with Lemma 1 implies that $\mathcal{Z}_j' \cap \ker(\tau_2) = 0$ and $\tau_2(\mathcal{Z}_j') \cap [\tau_1(\mathcal{W}_{j+1}) + \tau_2(\mathcal{W}_{j+1})] = 0$. Hence $\tau_1(\mathcal{W}_{j+1}) + \tau_2(\mathcal{W}_{j+1} + \mathcal{Z}_j') = [\tau_1(\mathcal{W}_{j+1}) + \tau_2(\mathcal{W}_{j+1})] + \tau_2(\mathcal{Z}_j')$ is of dimension $2[\dim(\mathcal{R}_{j+1}) - (m-n)] + [\dim(\mathcal{R}_j \cap \mathcal{F}_j) - \dim(\mathcal{R}_{j+1})]$. Simplifying it, we get

$$\dim(\tau_1(\mathcal{W}_{j+1}) + \tau_2(\mathcal{W}_{j+1} + \mathcal{Z}_j')) = \dim(\mathcal{R}_{j+1}) + \dim(\mathcal{R}_j \cap \mathcal{F}_j) - 2(m-n). \tag{58}$$

Since $\mathcal{W}_{j+1}$ is a subspace of $\mathcal{R}_{j+1}$, we have $\tau_1(\mathcal{W}_{j+1}) \subset \tau_1(\mathcal{R}_{j+1}) = \mathcal{G}_{j+1} \subset \tau_2(\mathcal{R}_j \cap \mathcal{F}_j)$. Since $\mathcal{W}_{j+1} + \mathcal{Z}_j'$ is a subspace of $\mathcal{R}_j \cap \mathcal{F}_j$, we get $\tau_2(\mathcal{W}_{j+1} + \mathcal{Z}_j') \subset \tau_2(\mathcal{R}_j \cap \mathcal{F}_j)$. Together we obtain that $\tau_1(\mathcal{W}_{j+1}) + \tau_2(\mathcal{W}_{j+1} + \mathcal{Z}_j') \subset \tau_2(\mathcal{R}_j \cap \mathcal{F}_j)$ and thus $\tau_1^{-1}(\tau_1(\mathcal{W}_{j+1}) + \tau_2(\mathcal{W}_{j+1} + \mathcal{Z}_j'))$ is a subspace of $\tau_1^{-1}(\tau_2(\mathcal{R}_j \cap \mathcal{F}_j))$. Since $\mathcal{Z}_j'$ is a subspace of $\mathcal{R}_j \cap \mathcal{F}_j$, we see that

$$\begin{aligned}
\mathcal{Z}_j' \cap \tau_1^{-1}(\tau_2(\mathcal{R}_j \cap \mathcal{F}_j)) &= \mathcal{Z}_j' \cap \tau_1^{-1}(\tau_2(\mathcal{R}_j \cap \mathcal{F}_j)) \cap \mathcal{R}_j \cap \mathcal{F}_j && (59)\\
&= \mathcal{Z}_j' \cap \tau_1^{-1}(\tau_1(\mathcal{R}_j \cap \mathcal{F}_j) \cap \tau_2(\mathcal{R}_j \cap \mathcal{F}_j)) \cap \mathcal{R}_j \cap \mathcal{F}_j && (60)\\
&= \mathcal{Z}_j' \cap \tau_1^{-1}(\mathcal{G}_{j+1}) \cap \mathcal{R}_j \cap \mathcal{F}_j = \mathcal{Z}_j' \cap \mathcal{R}_{j+1} = 0. && (61)
\end{aligned}$$

This in particular implies $\mathcal{Z}_j' \cap \tau_1^{-1}(\tau_1(\mathcal{W}_{j+1}) + \tau_2(\mathcal{W}_{j+1} + \mathcal{Z}_j')) = 0$, which with Lemma 1 we know that $\tau_1(\mathcal{Z}_j') \cap [\tau_1(\mathcal{W}_{j+1}) + \tau_2(\mathcal{W}_{j+1} + \mathcal{Z}_j')] = 0$ and $\ker(\tau_1) \cap \mathcal{Z}_j' = 0$. With (58) it follows that $\tau_1(\mathcal{W}_{j+1} + \mathcal{Z}_j') +$

$\tau_2(\mathcal{W}_{j+1}+\mathcal{Z}_j')$ has dimension $[\dim(\mathcal{R}_{j+1})+\dim(\mathcal{R}_j\cap\mathcal{F}_j)-2(m-n)]+[\dim(\mathcal{R}_j\cap\mathcal{F}_j)-\dim(\mathcal{R}_{j+1})]$. After simplification we get

$$\dim(\tau_1(\mathcal{W}_{j+1}+\mathcal{Z}_j')+\tau_2(\mathcal{W}_{j+1}+\mathcal{Z}_j'))=2[\dim(\mathcal{R}_j\cap\mathcal{F}_j)-(m-n)]. \tag{62}$$

Letting $\mathcal{Z}_j=\mathcal{W}_{j+1}+\mathcal{Z}_j'$ we finished the proof. $\square$

We are ready to summarize the proof of Proposition 4. To repeat we can construct a chain of subspaces say (42) or (43), where $\mathcal{Z}_\beta$ or $\mathcal{W}_\mu$ satisfies $\mathscr{P}(\mathcal{Z}_\beta)$ or $\mathscr{P}(\mathcal{W}_\mu)$, respectively. Lemmas 9 and 10 can then be used iteratively to extend chain (42) or (43), with (42) yielding the chain

$$\begin{array}{ccccccccc}
\mathcal{R}_\beta\cap\mathcal{F}_\beta & \subset & \mathcal{R}_\beta & \subset & \mathcal{R}_{\beta-1}\cap\mathcal{F}_{\beta-1} & \subset & \cdots & \subset & \mathcal{R}_0=\mathbb{C}^m\\
\cup & & \cup & & \cup & & & & \cup\\
\mathcal{Z}_\beta & \subset & \mathcal{W}_\beta & \subset & \mathcal{Z}_{\beta-1} & \subset & \cdots & \subset & \mathcal{W}_0\\
\uparrow & & \uparrow & & \uparrow & & & & \uparrow\\
\mathscr{P}(\mathcal{Z}_\beta) & & \mathscr{P}(\mathcal{W}_\beta) & & \mathcal{P}(\mathcal{Z}_{\beta-1}) & & \cdots & & \mathscr{P}(\mathcal{W}_0)
\end{array} \tag{63}$$

or (43) giving rise to

$$\begin{array}{ccccccccc}
\mathcal{R}_\gamma & \subset & \mathcal{R}_{\gamma-1}\cap\mathcal{F}_{\gamma-1} & \subset & \mathcal{R}_{\gamma-1} & \subset & \cdots & \subset & \mathcal{R}_0=\mathbb{C}^m\\
\cup & & \cup & & \cup & & & & \cup\\
\mathcal{W}_\gamma & \subset & \mathcal{Z}_{\gamma-1} & \subset & \mathcal{W}_{\gamma-1} & \subset & \cdots & \subset & \mathcal{W}_0\\
\uparrow & & \uparrow & & \uparrow & & & & \uparrow\\
\mathscr{P}(\mathcal{W}_\gamma) & & \mathscr{P}(\mathcal{Z}_{\gamma-1}) & & \mathcal{P}(\mathcal{W}_{\gamma-1}) & & \cdots & & \mathscr{P}(\mathcal{W}_0)
\end{array} \tag{64}$$

where both in (63) and (64) each $\mathcal{W}_j$ satisfies $\mathscr{P}(\mathcal{W}_j)$ defined in (41). In both cases $\mathcal{W}_0$ satisfies $\dim(\mathcal{W}_0)=[\dim(\mathcal{R}_0)-(m-n)]=n$ and $\dim(\tau_1(\mathcal{W}_0)+\tau_2(\mathcal{W}_0))=2\dim(\mathcal{W}_0)=2n$. The proof is complete. $\square$

3.2. Proof of Proposition 1

3.3. Proof of Theorem 2

The following lemma is elementary.

Lemma 11. *For $\mathcal{I}\subset[\ell]$ with $n_{\mathcal{I}}\le m$, there is a non-empty Zariski open subset of $\prod_{t\in\mathcal{I}}\mathrm{Gr}_{\mathbb{H}}(n_t,m)$ whose element $(\mathcal{V}_1,\dots,\mathcal{V}_{|\mathcal{I}|})$ consists of independent subspaces, i.e., $\mathcal{V}_j\cap\mathcal{V}_{\mathcal{I}\setminus\{j\}}=0$, $\forall j\in\mathcal{I}$.*

Similar to the proof of Theorem 1 it suffices to consider two linear maps τ_1 and τ_2 of $\mathcal{T}$ and prove $\mathrm{hsp}(\mathcal{A}_{\mathscr{I}},\{\tau_1,\tau_2\})$. And for the same reason we need only to prove $\mathrm{hsp}(\mathcal{V}_{\mathcal{I}_1}\cup\mathcal{V}_{\mathcal{I}_2},\{\tau_1,\tau_2\})$.

Since $n_{\mathcal{I}_1}+n_{\mathcal{I}_2}\le 2n\le m$, by Lemma 11 there is a non-empty Zariski open subset $\mathbb{U}_0$ of $\prod_{t\in\mathcal{I}_1\cup\mathcal{I}_2}\mathrm{Gr}_{\mathbb{H}}(n_t,m)$ whose element consists of independent subspaces. Let $\mathbb{U}_1$ contain all elements $(\mathcal{V}_t)_{t\in\mathcal{I}_1\cup\mathcal{I}_2}$ of $\mathbb{U}_0$ satisfying

$$\dim(\tau_2^{-1}(\tau_1(\mathcal{V}_{\mathcal{I}_1}))+\mathcal{V}_{\mathcal{I}_1\cap\mathcal{I}_2}+\mathcal{V}_{\mathcal{I}_2\setminus\mathcal{I}_1})=\dim(\tau_2^{-1}(\tau_1(\mathcal{V}_{\mathcal{I}_1}))+\mathcal{V}_{\mathcal{I}_1\cap\mathcal{I}_2})+n_{\mathcal{I}_2\setminus\mathcal{I}_1}. \tag{65}$$

Note that $\mathbb{U}_1$ is Zariski open since it is defined by the non-vanishing of the maximal minors of $[A_1,A_2]$, where A_1 and A_2 are basis matrices of $\tau_2^{-1}(\tau_1(\mathcal{V}_{\mathcal{I}_1}))+\mathcal{V}_{\mathcal{I}_1\cap\mathcal{I}_2}$ and $\mathcal{V}_{\mathcal{I}_2\setminus\mathcal{I}_1}$ respectively. Moreover, This Zariski open subset $\mathbb{U}_1$ of $\mathbb{U}_0$ is not-empty since the right-hand side of (65) is at most

$$m-r_2+n_{\mathcal{I}_1}+n_{\mathcal{I}_1\cap\mathcal{I}_2}+n_{\mathcal{I}_2\setminus\mathcal{I}_1}\le m-r_2+n_{\mathcal{I}_1}+n_{\mathcal{I}_2}\le m-r_2+2n\le m, \tag{66}$$

and thus we can always choose a $\mathcal{V}_{\mathcal{I}_2\setminus\mathcal{I}_1}$ such that it intersects $\tau_2^{-1}(\tau_1(\mathcal{V}_{\mathcal{I}_1}))+\mathcal{V}_{\mathcal{I}_1\cap\mathcal{I}_2}$ only at zero. Consequently $\mathbb{U}_1$ is a non-empty Zariski open subset of $\prod_{t\in\mathcal{I}_1\cup\mathcal{I}_2}\mathrm{Gr}_{\mathbb{H}}(n_t,m)$, on which every element $(\mathcal{V}_t)_{t\in\mathcal{I}_1\cup\mathcal{I}_2}$ satisfies (65), which implies $\mathcal{V}_{\mathcal{I}_2\setminus\mathcal{I}_1}\cap[\tau_2^{-1}(\tau_1(\mathcal{V}_{\mathcal{I}_1}))+\mathcal{V}_{\mathcal{I}_1\cap\mathcal{I}_2}]=0$. Changing the role of $\mathcal{I}_1$ and $\mathcal{I}_2$ we obtain another non-empty Zariski open subset $\mathbb{U}_2\in\prod_{t\in\mathcal{I}_1\cup\mathcal{I}_2}\mathrm{Gr}_{\mathbb{H}}(n_t,m)$, on which every element $(\mathcal{V}_t)_{t\in\mathcal{I}_1\cup\mathcal{I}_2}$ satisfies $\mathcal{V}_{\mathcal{I}_1\setminus\mathcal{I}_2}\cap[\tau_2^{-1}(\tau_1(\mathcal{V}_{\mathcal{I}_2}))+\mathcal{V}_{\mathcal{I}_1\cap\mathcal{I}_2}]=0$. Denote by $\mathbb{U}_3$ the intersection of $\mathbb{U}_1$ and $\mathbb{U}_2$, which is non-empty open.

Then we show that, for any $(\mathcal{V}_t)_{t\in\mathcal{I}_1\cup\mathcal{I}_2} \in \mathbb{U}_3$, the relation $\tau_1(v_1) = \tau_2(v_2)$ where $v_1 \in \mathcal{V}_{\mathcal{I}_1}$ and $v_2 \in \mathcal{V}_{\mathcal{I}_1} \cup \mathcal{V}_{\mathcal{I}_2}$ implies $v_2 \in \mathcal{V}_{\mathcal{I}_1}$. Suppose for the sake of contradiction that $v_2 \in \mathcal{V}_{\mathcal{I}_2}\backslash\mathcal{V}_{\mathcal{I}_1}$. Since $\mathcal{V}_{\mathcal{I}_2} = \mathcal{V}_{\mathcal{I}_1\cap\mathcal{I}_2} + \mathcal{V}_{\mathcal{I}_2\backslash\mathcal{I}_1}$, we get $v_2 = w_0 + w_2$ for some $w_0 \in \mathcal{V}_{\mathcal{I}_1\cap\mathcal{I}_2}$ and $w_2 \in \mathcal{V}_{\mathcal{I}_2\backslash\mathcal{I}_1}$. This implies $w_0 + w_2 \in \tau_2^{-1}(\tau_1(\mathcal{V}_{\mathcal{I}_1}))$ and $w_2 \in \tau_2^{-1}(\tau_1(\mathcal{V}_{\mathcal{I}_1})) + \mathcal{V}_{\mathcal{I}_1\cap\mathcal{I}_2}$. By the definition of $\mathbb{U}_3$ we have $w_2 = 0$. That is, $v_2 = w_0 \in \mathcal{V}_{\mathcal{I}_1\cap\mathcal{I}_2} \subset \mathcal{V}_{\mathcal{I}_1}$, a contradiction. Similarly we can prove for any $(\mathcal{V}_t)_{t\in\mathcal{I}_1\cup\mathcal{I}_2} \in \mathbb{U}_3$ that the relation $\tau_1(v_1) = \tau_2(v_2)$ where $v_1 \in \mathcal{V}_{\mathcal{I}_2}$ and $v_2 \in \mathcal{V}_{\mathcal{I}_1} \cup \mathcal{V}_{\mathcal{I}_2}$ implies $v_2 \in \mathcal{V}_{\mathcal{I}_2}$. To conclude, for any $(\mathcal{V}_t)_{t\in\mathcal{I}_1\cup\mathcal{I}_2} \in \mathbb{U}_3$, the property $\operatorname{hsp}(\mathcal{V}_{\mathcal{I}_1} \cup \mathcal{V}_{\mathcal{I}_2}, \{\tau_1, \tau_2\})$ reduces to $\operatorname{hsp}(\mathcal{V}_{\mathcal{I}_1}, \{\tau_1, \tau_2\})$ and $\operatorname{hsp}(\mathcal{V}_{\mathcal{I}_2}, \{\tau_1, \tau_2\})$, we next show the former for $(\mathcal{V}_t)_{t\in\mathcal{I}_1\cup\mathcal{I}_2}$ in some non-empty Zariski open subset of $\mathbb{U}_3$, from which the latter will follow by symmetry.

Since $n_{\mathcal{I}_1} \leq n \leq m/2$, Theorem 1 implies that there is a non-empty Zariski open set $\mathbb{O}_1$ of $\operatorname{Gr}_{\mathbb{H}}(n_{\mathcal{I}_1}, m)$ on which every $\mathcal{V} \in \mathbb{O}_1$ satisfies $\operatorname{hsp}(\mathcal{V}, \{\tau_1, \tau_2\})$. Consider the surjective polynomial map from $\mathbb{U}_0$ to $\operatorname{Gr}_{\mathbb{H}}(n_{\mathcal{I}_1}, m)$ which sends the independent subspaces $(\mathcal{V}_t)_{t\in\mathcal{I}_1\cup\mathcal{I}_2}$ to the sum $\mathcal{V}_{\mathcal{I}_1}$. The inverse image of $\mathbb{O}_1$ under this surjective polynomial map is also Zariski open and non-empty. The intersection $\mathbb{U}$ of this inverse image with $\mathbb{U}_3$ is non-empty Zariski open in $\prod_{t\in\mathcal{I}_1} \operatorname{Gr}_{\mathbb{H}}(n_t, m)$, and $\operatorname{hsp}(\mathcal{V}_{\mathcal{I}_1}, \{\tau_1, \tau_2\})$ holds for $(\mathcal{V}_t)_{t\in\mathcal{I}_1\cup\mathcal{I}_2} \in \mathbb{U}$.

3.4. Proof of Proposition 3

It has been shown in [1, 2] that for every $S_1, S_2 \in \mathcal{S}_{r,m}$ there is some projection P onto the range space of S_2 satisfying $\dim(\mathcal{U}_{PT_1,T_2}) \leq m - \lfloor r/2 \rfloor$. With $r \geq 2n$ we have $\dim(\mathcal{U}_{S_1,S_2}) \leq \dim(\mathcal{U}_{PS_1,S_2}) \leq m - r$, and this proves the first two statements of Proposition 3. The last statment follows similarly from [2]. For the third statement, let $B_1, B_2 \in \mathcal{B}_m$. Then for every $w \in \mathcal{U}^{\pm}_{B_1,B_2}$ we have $B_1 w = \lambda B_2 w$ for some λ, that is, $Bw = \lambda w$ where $B = (B_2)^{-1} B_1$ is a sign matrix. Hence w is an eigenvector of B corresponding to the eigenvalue λ. The only possibility is that $\lambda = \pm 1$. That is, w is in the null space of $B_1 \pm B_2$, which does not intersect $\mathcal{U}_{B_1,B_2}$. It is only possible that $\mathcal{U}_{B_1,B_2} = \varnothing$.

3.5. Proof of Corollary 1

The first statement is a special case of the second, and here we prove the second. Theorem 1 and Proposition 3 imply that when $r \geq 2n$ there is a non-empty Zariski open subset $\mathbb{O}$ of $\operatorname{Gr}_{\mathbb{R}}(n, m)$ on which every subspace $\mathcal{V}$ satisfies $\operatorname{hsp}(\mathcal{V}, \mathcal{S}_{r,m})$. The inverse image $\mathbb{U}$ of $\mathbb{O}$ under the polynomial map from the non-empty set of all full column rank matrices of $\mathbb{R}^{m\times n}$ to $\operatorname{Gr}_{\mathbb{R}}(n, m)$ that sends a matrix A to (the Plücker coordinates of) its column space $R(A)$ is also non-empty and Zariski open. Then for every $m \times n$ matrix $A \in \mathbb{U}$ we have $\operatorname{hsp}(R(A), \mathcal{S}_{r,m})$. Since every $A \in \mathbb{U}$ is of full column rank, we also have $\operatorname{hsp}(\mathbb{R}^n, A)$. We proved the first two statements. Using Propositions 2 and 3 the last two statements can be proved similarly.

3.6. Proof of Corollary 2

We present the proof for the second statement, which implies the first, and from which the last two statements follow similarly. Let $r \geq 2k$. Then Propositon 3 implies that $\dim(\mathcal{U}_{S_1,S_2}) \leq m - k$ for any rank-r selections $S_1, S_2 \in \mathcal{S}_{r,m}$. Let $s = \binom{n}{k}$ and let $\mathscr{I} = (\mathcal{I}_1, \ldots, \mathcal{I}_s)$ be an ordered set of all subsets of $[n]$ of cardinality k. Applying Theorem 2 we get a non-empty Zariski open subset $\mathbb{O}$ of $\prod_{j\in[n]} \operatorname{Gr}_{\mathbb{R}}(1, m)$ such that for any $\mathcal{A} = (\mathcal{V}_1, \ldots, \mathcal{V}_n) \in \mathbb{O}$, the property $\operatorname{hsp}(\overline{\mathcal{A}_{\mathscr{I}}}, \mathcal{S}_{r,m})$ holds.

Consider the map from $\mathbb{R}^{m\times n}$ to $\prod_{j\in[n]} \operatorname{Gr}_{\mathbb{R}}(1, m)$ which sends the j-th column of a matrix to (the Plücker coordinates of) its column space. This map is surjective, and so the inverse image $\mathbb{U}_1$ of $\mathbb{O}$ under this map is also non-empty Zariski open. Let $\mathbb{U}_2$ be the set of matrices A's of $\mathbb{R}^{m\times n}$ such that any $2k$ different columns of A are linearly independent (if $n < 2k$ then let $\mathbb{U}_2$ be the set of all full column rank matrices of $\mathbb{R}^{m\times n}$). Let $\mathbb{U} = \mathbb{U}_1 \cap \mathbb{U}_2$. Then $\mathbb{U}$ is a non-empty Zariski open subset of $\mathbb{R}^{m\times n}$.

Let $A \in \mathbb{U}$. We will show $\operatorname{hsp}(\overline{\mathcal{K}_{\mathscr{I}}}, \mathcal{S}_{r,m} A)$. Let us view A as a linear map τ_A such that $\tau_A(x) = Ax$. The choice of $\mathbb{U}_1$ (and so of $\mathbb{U}$) implies that $\operatorname{hsp}(\tau_A(\overline{\mathcal{K}_{\mathscr{I}}}), \mathcal{S}_{r,m})$ holds true. That is, for any k-sparse vectors $x, x' \in \overline{\mathcal{K}_{\mathscr{I}}}$ and $S, S' \in \mathcal{S}_{r,m}$ satisfying $SAx = S'Ax'$, we have $Ax = Ax'$. For some $J \subset [n]$ use $A_J \in \mathbb{R}^{m\times|J|}$ to denote the sub-matrix of A formed by $|J|$ columns of A indexed by J, and also write x_J and x'_J for the sub-vectors of x and x' indexed by J, respectively. Then, for J_1 and J_2 two index sets corresponding to the locations of nonzero entries of x and x' respectively, we have that $A_{J_1} x_{J_1} = A_{J_2} x'_{J_2}$. That is, $A_{J_1\cap J_2}(x_{J_1\cap J_2} - x'_{J_1\cap J_2}) + A_{J_1-J_2} x_{J_1-J_2} - A_{J_2-J_1} x'_{J_2-J_1} = 0$. But $|J_1 \cap J_2| + |J_1 - J_2| + |J_2 - J_1| \leq 2k$ and any $2k$ distinct columns of A are linearly independent, so we must have $x_{J_1\cap J_2} = x'_{J_1\cap J_2}$ and $x_{J_1-J_2} = 0$ and $x'_{J_2-J_1} = 0$. That is, $x = x'$. We finished the proof. □

3.7. Proof of Theorem 3

Since the conditions of Theorem 1 are fulfilled, there is a non-empty Zariski open subset of $\mathrm{Gr}_{\mathbb{R}}(n, m)$ on which every subspace $\mathcal{V}'$ satisfies $\mathrm{hsp}(\mathcal{V}', \mathcal{T})$. Let $\mathcal{V}$ be a subspace in that Zariski open set. We first rewrite (7) into a convenient form. Note that

$$\hat{\tau} = \operatorname*{argmin}_{\tau\in\mathcal{T}} \min_{v\in\mathcal{V}} \|\overline{y} - \tau(v)\|_2 \tag{67}$$

$$= \operatorname*{argmin}_{\tau\in\mathcal{T}} \min_{w\in\tau(\mathcal{V})} \|\overline{y} - w\|_2^2 \tag{68}$$

$$= \operatorname*{argmin}_{\tau\in\mathcal{T}} \min_{w\in\tau(\mathcal{V})} \{\|w\|_2^2 - 2\langle \overline{y}, w\rangle\} \tag{69}$$

$$= \operatorname*{argmin}_{\tau\in\mathcal{T}} \min_{\lambda>0} \min_{w\in\tau(\mathcal{V}):\|w\|_2=\lambda} \{\lambda^2 - 2\langle \overline{y}, w\rangle\} \tag{70}$$

$$= \operatorname*{argmin}_{\tau\in\mathcal{T}} \min_{\lambda>0} \{\lambda^2 - 2\lambda\|\overline{y}\|_2 \max_{w\in\tau(\mathcal{V}):\|w\|_2=\lambda} \frac{\langle \overline{y}, w\rangle}{\|\overline{y}\|_2\|w\|_2}\} \tag{71}$$

$$= \operatorname*{argmin}_{\tau\in\mathcal{T}} \min_{\lambda>0} \{\lambda^2 - 2\lambda\|\overline{y}\|_2 \cos(\overline{y}, \tau(\mathcal{V}))\} \tag{72}$$

$$= \operatorname*{argmax}_{\tau\in\mathcal{T}} \cos(\overline{y}, \tau(\mathcal{V})). \tag{73}$$

We then prove $\hat{\tau} \in \mathcal{T}_1$. It suffices to show for any $\tau_2 \in \mathcal{T} \setminus \mathcal{T}_1$ that there is some $\tau_1 \in \mathcal{T}_1$ so that

$$\cos(\overline{y}, \tau_1(\mathcal{V})) > \cos(\overline{y}, \tau_2(\mathcal{V})), \tag{74}$$

which surely holds, if the following stronger condition

$$\frac{\langle \overline{y}, y\rangle}{\|\overline{y}\|_2\|y\|_2} > \cos(\overline{y}, \tau_2(\mathcal{V})) \tag{75}$$

is satisfied. Letting $w_2 \in \tau_2(\mathcal{V})$ with $\|w_2\|_2 = 1$ be such that $\langle \overline{y}, w_2\rangle/\|\overline{y}\|_2 = \cos(\overline{y}, \tau_2(\mathcal{V}))$ and noticing that $\overline{y} = y + \epsilon$, condition (75) is equivalent to

$$\frac{\langle \overline{y}, y\rangle}{\|\overline{y}\|_2\|y\|_2} > \frac{\langle \overline{y}, w_2\rangle}{\|\overline{y}\|_2} \Leftrightarrow \frac{\langle \overline{y}, y\rangle}{\|y\|_2^2} > \frac{\langle \overline{y}, w_2\rangle}{\|y\|_2} \Leftrightarrow 1 > \frac{\langle y, w_2\rangle}{\|y\|_2} + \frac{\langle \epsilon, w_2\rangle}{\|y\|_2} - \frac{\langle \epsilon, y\rangle}{\|y\|_2^2}. \tag{76}$$

Note that $\frac{\langle y, w_2\rangle}{\|y\|_2} \leq \cos(y, \tau_2(\mathcal{V}))$, $\langle \epsilon, w_2\rangle \leq \|\epsilon\|_2$, and $-\langle \epsilon, y\rangle \leq \|\epsilon\|_2\|y\|_2$. For (76) to be true, it is enough to satisfy the following condition

$$1 > \cos(y, \tau_2(\mathcal{V})) + 2\frac{\|\epsilon\|_2}{\|y\|_2} \Leftrightarrow \|y\|_2(1 - \cos(y, \tau_2(\mathcal{V}))) > 2\|\epsilon\|_2, \tag{77}$$

which is already fulfilled by (9). Hence $\hat{\tau} \in \mathcal{T}_1$. So we have $y = \tau^*(v^*) = \hat{\tau}(v)$ for some $v \in \mathcal{V}$. This implies $v = v^*$, and thus $y = \hat{\tau}(v^*)$. On the other hand, according to (7), we have

$$\hat{v} = \operatorname*{argmin}_{v\in\mathcal{V}} \|y + \epsilon - \hat{\tau}(v)\|_2. \tag{78}$$

Thus, for $\hat{x} \in \mathbb{R}^n$ and $x^* \in \mathbb{R}^n$ satisfying $\hat{v} = A\hat{x}$ and $v^* = Ax^*$, we get that

$$\hat{x} = \operatorname*{argmin}_{x\in\mathbb{R}^n} \|y + \epsilon - \hat{T}Ax\|_2 = (\hat{T}A)^\dagger(y + \epsilon), \tag{79}$$

where we used the fact that $\hat{T}A$ is of full column rank. Recalling $y = \hat{\tau}(v^*) = \hat{T}Ax^*$, we obtain

$$\hat{x} = (\hat{T}A)^\dagger(\hat{T}Ax^* + \epsilon) = x^* + (\hat{T}A)^\dagger\epsilon, \tag{80}$$

and consequently $\hat{v} = v^* + A(\hat{T}A)^\dagger\epsilon$. $\square$

4. Appendix: Proof of Lemma 2

Here we provide a proof for Lemma 2. This follows from Lemma 12 (whose proof relies on Lemmas 13 and 14) and the fact that the intersection of t non-empty Zariski open subsets is also non-empty and open in the Grassmannian $\mathrm{Gr}_{\mathbb{C}}(d, m)$.

Lemma 12. *For an algebraic variety $\mathcal{Q}$ of $\mathbb{C}^m$ of dimension r passing through the origin, there is a non-empty Zariski open subset of $\mathrm{Gr}_{\mathbb{C}}(m-1, m)$ on which every hyperplane $\mathcal{H}$ satisfies $\dim(\mathcal{Q} \cap \mathcal{H}) \leq \max\{r-1, 0\}$. Moreover, there is another non-empty Zariski open subset of $\mathrm{Gr}_{\mathbb{C}}(d, m)$ on which every subspace $\mathcal{V}$ satisfies $\dim(\mathcal{Q} \cap \mathcal{V}) \leq \max\{r+d-m, 0\}$.*

Proof. Consider $\mathcal{Q} = \cup_{j\in[s]} \mathcal{Q}_j$ the irreducible decomposition of $\mathcal{Q}$ with $\dim(\mathcal{Q}_1) \leq \cdots \leq \dim(\mathcal{Q}_s) = r$. If there is some component being $\{0\}$, say $\mathcal{Q}_1 = \{0\}$, then $\mathcal{Q}_j \neq \{0\}$ for $j > 1$ and $\mathcal{Q}_1 \cap \mathcal{H} = \{0\}$ for any hyperplane $\mathcal{H}$. By Lemma 13 there is a non-empty Zariski open subset of $\mathrm{Gr}_{\mathbb{C}}(m-1, m)$ on which every hyperplane $\mathcal{H}$ does not contain $\mathcal{Q}_j$, $\forall j \in [s]\backslash\{1\}$. If $[s] = \{1\}$ or $r = 0$ we are done since $\mathcal{Q} \cap \mathcal{H} = \{0\}$ and thus $\dim(\mathcal{Q} \cap \mathcal{H}) \leq \max\{r-1, 0\}$. It remains to consider the case $s > 1$ and $r > 0$. Using Lemma 14 we get that for $j \in [s]\backslash\{1\}$ all irreducible components of $\mathcal{Q}_j \cap \mathcal{H}$ have dimension $\dim(\mathcal{Q}_j) - 1$, from which it follows that $\dim(\mathcal{Q}_j \cap \mathcal{H}) \leq r-1$. Hence $\dim(\mathcal{Q} \cap \mathcal{H}) \leq \max\{r-1, 0\}$. If $\mathcal{Q}$ does not contain $\{0\}$ as one of its irreducible components, similarly we get $\dim(\mathcal{Q} \cap \mathcal{H}) \leq \max\{r-1, 0\}$. Running this process $(m-d)$ times yields the second statement.

Lemma 13. *For a non-empty algebraic variety $\mathcal{Q}$ of $\mathbb{C}^m$ with irreducible components $\mathcal{Q}_j$'s, there is a non-empty Zariski open subset of $\mathrm{Gr}_{\mathbb{C}}(m-1, m)$ on which every hyperplane through the origin does not contain $\mathcal{Q}_j \neq \{0\}$.*

Proof. Consider all irreducible components $\{\mathcal{Q}_j\}_{j\in[s]}$ appearing in the irreducible decomposition of $\mathcal{Q}$ with $\mathcal{Q}_j \neq \{0\}$. For any $j \in [s]$ take $q_j \in \mathcal{Q}_j$ with $q_j \neq 0$. There exists a non-empty Zariski open subset $\mathbb{U}_j$ of $\mathrm{Gr}_{\mathbb{C}}(m-1, m)$ on which every hyperplane does not contain q_j. Since $\mathrm{Gr}_{\mathbb{C}}(m-1, m)$ is irreducible, the intersection $\mathbb{U} := \bigcap_{j\in[s]} \mathbb{U}_j$ is also non-empty and Zariski open. So any hyperplane of $\mathbb{U}$ does not contain $\mathcal{Q}_j$.

Lemma 14 (Exercise 1.8 in [28]). *Let $\mathcal{Q}$ be an irreducible algebraic variety of dimension r in $\mathbb{C}^m$ and $\mathcal{F}$ a hypersurface not containing $\mathcal{Q}$. Then every irreducible component of $\mathcal{Q} \cap \mathcal{F}$ has dimension $r-1$.*

References

[1] M. C. Tsakiris, L. Peng, Homomorphic sensing, in: Proc. the 36th Int. Conf. Mach. Learning, Long Beach, California, USA, 2019.

[2] M. C. Tsakiris, Determinantal conditions for homomorphic sensing (arXiv:1812.07966v5 [math.CO], Tech. Rep., 2020).

[3] R. Balan, P. Casazza, D. Edidin, On signal reconstruction without phase, Applied and Computational Harmonic Analysis 20 (3) (2006) 345 – 356.

[4] M. Akçakaya, V. Tarokh, New conditions for sparse phase retrieval, arXiv preprint arXiv:1310.1351 (2013).

[5] Y. Wang, Z. Xu, Phase retrieval for sparse signals, Applied and Computational Harmonic Analysis 37 (3) (2014) 531 – 544. doi:https://doi.org/10.1016/j.acha.2014.04.001.
URL http://www.sciencedirect.com/science/article/pii/S1063520314000517

[6] J. Unnikrishnan, S. Haghighatshoar, M. Vetterli, Unlabeled sensing: Solving a linear system with unordered measurements, in: 2015 53rd Annual Allerton Conference on Communication, Control, and Computing (Allerton), 2015, pp. 786–793.

[7] J. Unnikrishnan, S. Haghighatshoar, M. Vetterli, Unlabeled sensing with random linear measurements, IEEE Trans. Inf. Theory 64 (5) (2018) 3237–3253. doi:10.1109/TIT.2018.2809002.

[8] D. Han, F. Lv, W. Sun, Recovery of signals from unordered partial frame coefficients, Applied and Computational Harmonic Analysis 44 (1) (2018) 38 – 58. doi:https://doi.org/10.1016/j.acha.2016.04.002.
URL http://www.sciencedirect.com/science/article/pii/S1063520316300021

[9] F. Lv, W. Sun, Real phase retrieval from unordered partial frame coefficients, Advances in Computational Mathematics 44 (3) (2018) 879–896. doi:10.1007/s10444-017-9566-4.
URL https://doi.org/10.1007/s10444-017-9566-4

[10] P. Grohs, S. Koppensteiner, M. Rathmair, Phase retrieval: Uniqueness and stability, SIAM Review 62 (2) (2020) 301–350. arXiv:https://doi.org/10.1137/19M1256865, doi:10.1137/19M1256865.
URL https://doi.org/10.1137/19M1256865

[11] S. Balakrishnan, M. J. Wainwright, B. Yu, Statistical guarantees for the em algorithm: From population to sample-based analysis, Ann. Statist. 45 (1) (2017) 77–120. doi:10.1214/16-AOS1435.
URL https://doi.org/10.1214/16-AOS1435

[12] Y. Chen, Y. Chi, J. Fan, C. Ma, Gradient descent with random initialization: fast global convergence for nonconvex phase retrieval, Mathematical Programming 176 (1) (2019) 5–37. doi:10.1007/s10107-019-01363-6.
URL https://doi.org/10.1007/s10107-019-01363-6

[13] J. M. Klusowski, D. Yang, W. D. Brinda, Estimating the coefficients of a mixture of two linear regressions by expectation maximization, IEEE Transactions on Information Theory 65 (6) (2019) 3515–3524. doi:10.1109/TIT.2019.2891628.

[14] I. P. Fellegi, A. B. Sunter, A theory for record linkage, Journal of the American Statistical Association 64 (328) (1969) 1183–1210. doi:10.1080/01621459.1969.10501049.

[15] M. H. DeGroot, P. K. Goel, Estimation of the correlation coefficient from a broken random sample, Ann. Statist. 8 (2) (1980) 264–278. doi:10.1214/aos/1176344952.
URL https://doi.org/10.1214/aos/1176344952

[16] M. Slawski, E. Ben-David, Linear regression with sparsely permuted data, Electron. J. Statist. 13 (1) (2019) 1–36. doi:10.1214/18-EJS1498.

[17] D. Hsu, K. Shi, X. Sun, Linear regression without correspondence, in: Advances in Neural Inf. Process. Syst. 30 (NeurIPS), 2017.

[18] A. Pananjady, M. J. Wainwright, T. A. Courtade, Linear regression with shuffled data: Statistical and computational limits of permutation recovery, IEEE Trans. Inf. Theory 64 (5) (2018) 3286–3300. doi:10.1109/TIT.2017.2776217.

[19] S. Haghighatshoar, G. Caire, Signal recovery from unlabeled samples, IEEE Trans. Signal Process. 66 (5) (2018) 1242–1257. doi:10.1109/TSP.2017.2786276.

[20] M. Slawski, G. Diao, E. Ben-David, A Pseudo-Likelihood Approach to Linear Regression with Partially Shuffled Data (arXiv:1910.01623 [stat.ME], Tech. Rep., 2019). arXiv:1910.01623.

[21] M. Slawski, M. Rahmani, P. Li, A sparse representation-based approach to linear regression with partially shuffled labels, in: Proceedings of the Thirty-Fifth Conference on Uncertainty in Artificial Intelligence, UAI 2019, 2019, pp. 38–48.

[22] I. Dokmanic, Permutations unlabeled beyond sampling unknown, IEEE Signal Process. Lett. 26 (6) (2019) 823–827. doi:10.1109/LSP.2019.2908505.

[23] H. Zhang, M. Slawski, P. Li, Permutation Recovery from Multiple Measurement Vectors in Unlabeled Sensing, arXiv e-prints (2019) arXiv:1909.02496arXiv:1909.02496.

[24] M. C. Tsakiris, L. Peng, A. Conca, L. Kneip, Y. Shi, H. Choi, An algebraic-geometric approach for linear regression without correspondences, IEEE Transactions on Information Theory (2020) 1–1doi:10.1109/TIT.2020.2977166.

[25] L. Peng, M. C. Tsakiris, Linear regression without correspondences via concave minimization, IEEE Signal Processing Letters 27 (2020) 1580–1584.

[26] Z. Wang, E. Ben-David, M. Slawski, Estimation in exponential family Regression based on linked data contaminated by mismatch error, arXiv e-prints (2020) arXiv:2010.00181arXiv:2010.00181.

[27] S. Roman, Advanced linear algebra, Springer, New York, 2008.

[28] R. Hartshorne, Algebraic geometry, Springer Science+Business Media, Inc., New York, 2010.