Homomorphic Sensing of Subspace Arrangements

Liangzu Peng, Manolis C. Tsakiris

SIST, ShanghaiTech University, No. 393 Huaxia Middle Road, Pudong Area, Shanghai, China

---

Abstract

Homomorphic sensing is a recent algebraic-geometric framework that studies the unique recovery of points in a linear subspace from their images under a given collection of linear maps. It has been successful in interpreting such a recovery in the case of permutations composed by coordinate projections, an important instance in applications known as unlabeled sensing, which models data that are out of order and have missing values. In this paper, we provide tighter and simpler conditions that guarantee the unique recovery for the single-subspace case, extend the result to the case of a subspace arrangement, and show that the unique recovery in a single subspace is locally stable under noise. We specialize our results to several examples of homomorphic sensing such as real phase retrieval and unlabeled sensing. In so doing, in a unified way, we obtain conditions that guarantee the unique recovery for those examples, typically known via diverse techniques in the literature, as well as novel conditions for sparse and unsigned versions of unlabeled sensing. Similarly, our noise result also implies that the unique recovery in unlabeled sensing is locally stable.

Keywords: homomorphic sensing, unlabeled sensing, linear regression without correspondences, real phase retrieval, mixed linear regression, algebraic geometry.

---

1. Introduction

1.1. Homomorphic sensing

The homomorphic sensing problem, introduced in [1]-[2] and also in the expository paper [3], is posed 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 $\mathbb{H}^m \to \mathbb{H}^m$. 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

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

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

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

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

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

The problem of interest to us is as follows.

Problem 1 (Homomorphic sensing [1]-[2],[3]). *Find conditions on a finite set* $\mathcal{T}$ *of linear maps* $\mathbb{H}^m \to \mathbb{H}^m$ *and an* n*-dimensional linear subspace* $\mathcal{V} \subset \mathbb{H}^m$ *that imply* $\operatorname{hsp}(\mathcal{V}, \mathcal{T})$*.*

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

To appreciate Problem 1, we start by looking at several special cases of it, which have been explored via different approaches in the last two decades, e.g., see [4, 5, 6, 7, 8, 9, 10]. The first example is *real phase retrieval* [10], a problem which dates back to the 1910's, when the research on *X-ray crystallography* was launched; see [11] 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 an m-dimensional vector, $A \in \mathbb{R}^{m \times n}$ is a given matrix, and B^* is an element of 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, 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 $\operatorname{hsp}_{\pm}(\mathbb{R}^n, \mathcal{B}_m A)$. In 2006, it was proved by [4] in a frame-theoretical language that $m \geq 2n - 1$ suffices for a generic $A \in \mathbb{R}^{m \times n}$ to enjoy $\operatorname{hsp}_{\pm}(\mathbb{R}^n, \mathcal{B}_m A)$, and it is necessary for any $A \in \mathbb{R}^{m \times n}$. If x^* is from the set $\overline{\mathcal{K}_{\mathscr{I}}}$ of all k-sparse vectors of $\mathbb{R}^n$, a situation considered in *sparse real phase retrieval* [6], then [5] and [6] have independently showed that a sufficient and necessary condition for $\operatorname{hsp}_{\pm}(\overline{\mathcal{K}_{\mathscr{I}}}, \mathcal{B}_m A)$ is $m \geq \min\{2n - 1, 2k\}$ providing $A \in \mathbb{R}^{m \times n}$ is generic. Finally, those results also hold for the problem of *symmetric mixture of two linear regressions* [12], since it bears the same formulation as real phase retrieval; see [13], [14] for discussions that connect the two problems.

Our 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 [7, 8] under the name *unlabeled sensing*, and also independently in [9]. Specifically, they proved via different 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, [9] proved that $r \geq 2n - 1$ is necessary for $\operatorname{hsp}(\mathbb{R}^n, \mathcal{S}_{r,m} A)$ and [7, 8] proved that, if m is odd with $m = r$ and $n \geq 2$, then $r \geq 2n$ is necessary. Finally, when $m = r$, then $\mathcal{S}_m := \mathcal{S}_{m,m}$ is the group 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* [15] and the *broken sample problem* [16] (see [17] for detailed discussions); recent developments on this topic can be found in, e.g., [18, 19, 20, 21, 22, 24, 25, 26, 27, 28].

An interesting generalization which we call *unsigned unlabeled sensing* was explored in [10] 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 [9], it was established in [10] 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 $n \geq 2$.

The homomorphic sensing Problem 1 is an abstraction of the above examples. Even though its formulation is linear algebraic, its nature is inherently algebraic-geometric, because whenever $\tau_1(v_1) = \tau_2(v_2)$, we have that v_1, v_2 satisfy the quadratic relation $\tau_1(v_1) \wedge \tau_2(v_2) = 0$, with $\wedge$ being the exterior product. This was the main insight of [1]-[2],[3] leading to the following results. With linear maps $\tau_1, \tau_2 : \mathbb{H}^m \to \mathbb{H}^m$ let $\overline{\tau}_1, \overline{\tau}_2 : \mathbb{C}^m \to \mathbb{C}^m$ be their complexifications and let T_1, T_2 be their matrix representations with respect to the standard basis. Let ρ be a linear projection onto the image $\operatorname{im}(\tau_2)$ of τ_2 with matrix representation P and complexification $\overline{\rho}$. With w a vector of variables, the 2×2 minors of the $r \times 2$ matrix $[PT_1 w \;\; T_2 w]$ are polynomials in entries of w, so their vanishing locus in $\mathbb{C}^m$ is a complex algebraic variety, say $\mathcal{Y}_{\rho\tau_1,\tau_2}$. Removing from $\mathcal{Y}_{\rho\tau_1,\tau_2}$ the union of linear subspaces $\mathcal{Z}_{\rho\tau_1,\tau_2} := \ker(\overline{\rho\tau}_1 - \overline{\tau}_2) \cup \ker(\overline{\rho\tau}_1) \cup \ker(\overline{\tau}_2)$ gives

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

which is an open set in $\mathcal{Y}_{\rho\tau_1,\tau_2}$, also called quasi-variety. The following was proved in [1]-[2]: 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 if there exists a linear projection ρ onto $\operatorname{im}(\tau_2)$ satisfying $\dim(\mathcal{U}_{\rho\tau_1,\tau_2}) \leq m - n$, then a generic subspace $\mathcal{V}$ of dimension n satisfies $\operatorname{hsp}(\mathcal{V}, \mathcal{T})$; here generic is meant in the sense that $\operatorname{hsp}(\mathcal{V}, \mathcal{T})$ is true for every $\mathcal{V}$ in a dense open set of the Grassmannian $\operatorname{Gr}(n, m)$. In the same work, the dimension of the quasi-variety $\mathcal{U}_{\rho\tau_1,\tau_2}$ was calculated for the case of unlabeled sensing, leading to the same sufficient conditions as in [8] and [9], mentioned above.

A suboptimal feature of this result is the presence of the projection ρ. Even though for unlabeled sensing the obvious choice of ρ was good enough, it is in general unclear how to check that a ρ that satisfies $\dim(\mathcal{U}_{\rho\tau_1,\tau_2}) \leq m - n$ exists, or if so how to search for it. One of our main contributions in this paper 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

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

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*

$$\dim(\mathcal{U}_{\tau_1,\tau_2}) \leq m - n, \quad \forall \tau_1, \tau_2 \in \mathcal{T}. \tag{1}$$

Note that, by definition, $\mathcal{U}_{\tau_1,\tau_2}$ is a subset of $\mathcal{U}_{\rho\tau_1,\tau_2}$, so condition (1) is tighter than that of [1]-[2],[3]. Indeed, condition (1) is the tightest possible in the following sense.

Proposition 1. *Suppose* $\mathbb{H} = \mathbb{C}$ *and that* (1) *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*

$$\dim(\mathcal{U}^{\pm}_{\tau_1,\tau_2}) \leq m - n, \quad \forall \tau_1, \tau_2 \in \mathcal{T}. \tag{2}$$

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 obtain within a unified framework existing and new results for real phase retrieval and unlabeled sensing variants. In §2 we give preliminaries. Proofs of all the statements are in §3 and §4.

1.2. Homomorphic sensing of subspace arrangements

We extend Theorem 1 from a single subspace $\mathcal{V}$ to a subspace arrangement $\mathcal{A} = (\mathcal{V}_1, \dots, \mathcal{V}_\ell)$, the latter being an ordered set of subspaces $\mathcal{V}_i$, $i \in [\ell] := \{1, \dots, \ell\}$ of $\mathbb{H}^m$. With $n_i = \dim(\mathcal{V}_i)$, we refer to $(n_1, \dots, n_\ell)$ as the dimension configuration of $\mathcal{A}$. Thus, by a *generic* subspace arrangement $\mathcal{A}$ with dimension configuration $(n_1, \dots, n_\ell)$ 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 Grassmannians (see also §2). Consider an ordered set $\mathscr{I} = (\mathcal{I}_1, \dots, \mathcal{I}_s)$ of subsets of $[\ell]$. 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 $\mathcal{V}_{\varnothing} := 0$. Thus the ordered set $\mathscr{I}$, together with $\mathcal{A}$, induces the *structured* subspace arrangement $\mathcal{A}_{\mathscr{I}} = (\mathcal{V}_{\mathcal{I}_1}, \dots, \mathcal{V}_{\mathcal{I}_s})$. This construction allows various levels of flexibility that will be exploited later in the paper. For example, $\mathcal{A}_{\mathscr{I}}$ 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 $\overline{\mathcal{A}_{\mathscr{I}}} := \bigcup_{j \in [s]} \mathcal{V}_{\mathcal{I}_j}$ and consider the property $\operatorname{hsp}(\overline{\mathcal{A}_{\mathscr{I}}}, \mathcal{T})$. We have:

Theorem 2. *Suppose* $\operatorname{rank}(\tau) \geq 2n$ *for any* $\tau \in \mathcal{T}$. *Let* $(n_1, \dots, n_\ell)$ *be a dimension configuration and* $\mathscr{I} = (\mathcal{I}_1, \dots, \mathcal{I}_s)$ *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* $\mathcal{A} = (\mathcal{V}_1, \dots, \mathcal{V}_\ell)$ *with* $\dim(\mathcal{V}_i) = n_i$, *whenever* (1) *holds. Similarly,* $\operatorname{hsp}_{\pm}(\overline{\mathcal{A}_{\mathscr{I}}}, \mathcal{T})$ *holds for a generic subspace arrangement* $(\mathcal{V}_1, \dots, \mathcal{V}_\ell)$ *with* $\dim(\mathcal{V}_i) = n_i$, *whenever* (2) *holds.*

1.3. Noisy homomorphic sensing

For any (column) vector $v \in \mathbb{H}^m$, denote by v^H its Hermitian transpose. With $u, w \in \mathbb{H}^m$ define $\langle u, w \rangle := u^H w$, the standard inner product $\mathbb{H}^m \times \mathbb{H}^m \to \mathbb{H}$, and also $\|w\|_2 := \sqrt{\langle w, w \rangle} = \sqrt{w^H w}$.

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

$$(\hat{\tau}, \hat{v}) \in \underset{v \in \mathcal{V}, \tau \in \mathcal{T}}{\operatorname{argmin}} \|\overline{y} - \tau(v)\|_2. \tag{3}$$

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

For a subspace $\mathcal{W} \subset \mathbb{H}^m$ and a non-zero $u \in \mathbb{H}^m$ define

$$\cos(u, \mathcal{W}) := \max\Big\{ \frac{\langle u, w \rangle + \langle w, u \rangle}{2\|u\|_2} : w \in \mathcal{W} \text{ and } \|w\|_2 = 1 \Big\}.$$

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

Theorem 3. *Let $\mathcal{V} \subset \mathbb{H}^m$ be a subspace of dimension n that satisfies* $\operatorname{hsp}(\mathcal{V}, \mathcal{T})$ *and let $A \in \mathbb{H}^{m\times n}$ be a matrix that has $\mathcal{V}$ as its column-space. Let $(\hat{\tau}, \hat{v})$ be a solution to* (3) *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*

$$2\|\epsilon\|_2 < \|y\|_2\Big(1 - \max_{\tau\in\mathcal{T}\setminus\mathcal{T}_1} \cos\big(y, \tau(\mathcal{V})\big)\Big), \tag{4}$$

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 column space of A. Also $\mathcal{S}_{r,m} \subset \mathbb{R}^{r\times m}$ can be viewed as a finite set of linear maps $\mathbb{H}^m \to \mathbb{H}^m$ (via an obvious injection). We then check whether $\mathcal{S}_{r,m}$ satisfies condition (1). Interestingly, whenever the rank constraint $r \geq 2n$ of Theorem 1 on $\mathcal{S}_{r,m}$ is fulfilled, condition (1) is automatically satisfied by $\mathcal{S}_{r,m}$, and similarly for the other types of transformations discussed:

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.*

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

Combining Proposition 3 with Theorem 1 we get the following results, which have already been obtained in a diverse literature via diverse methods:

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

- *i)* $m \geq 2n \Rightarrow \operatorname{hsp}(\mathbb{R}^n, \mathcal{S}_mA)$ *[3, 8, 9, 24].*
- *ii)* $r \geq 2n \Rightarrow \operatorname{hsp}(\mathbb{R}^n, \mathcal{S}_{r,m}A)$ *[3, 8, 9].*
- *iii)* $m \geq 2n \Rightarrow \operatorname{hsp}_\pm(\mathbb{R}^n, \mathcal{B}_mA)$ *[4, 24].*
- *iv)* $r \geq 2n \Rightarrow \operatorname{hsp}_\pm(\mathbb{R}^n, \mathcal{S}_{r,m}\mathcal{B}_mA)$ *[3, 10].*

Next we consider the sparse counterpart of Corollary 1. This is mostly unexplored territory in prior work and the main player here is Theorem 2. Consider the standard basis $e_1, \dots, e_n$ of $\mathbb{R}^n$ and the subspace arrangement $\mathcal{K} = (\mathcal{V}_1, \dots, \mathcal{V}_n)$ of $\mathbb{R}^n$ with $\mathcal{V}_i = \operatorname{Span}(e_i)$. Let $s = \binom{n}{k}$ and consider the set $\mathscr{I} = (\mathcal{I}_1, \dots, \mathcal{I}_s)$ of all subsets of $[n]$ of cardinality k, ordered, say, in the lexicographic order. 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 of subspaces $\overline{\mathcal{K}_{\mathscr{I}}} := \cup_{j\in[s]}\mathcal{V}_{\mathcal{I}_j}$ is the set of all k-sparse vectors of $\mathbb{R}^n$. With this notation, sparse real phase retrieval is equivalent to $\operatorname{hsp}_\pm(\overline{\mathcal{K}_{\mathscr{I}}}, \mathcal{B}_mA)$, and this has been studied by [5] and [6], while sparse unlabeled sensing ($\operatorname{hsp}(\overline{\mathcal{K}_{\mathscr{I}}}, \mathcal{S}_{r,m}A)$) and sparse unsigned unlabeled sensing ($\operatorname{hsp}_\pm(\overline{\mathcal{K}_{\mathscr{I}}}, \mathcal{S}_{r,m}\mathcal{B}_mA)$) have not been considered yet, to the best of our knowledge. Theorem 2 and Proposition 3 give:

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

- *i)* $m \geq 2k \Rightarrow \operatorname{hsp}(\overline{\mathcal{K}_{\mathscr{I}}}, \mathcal{S}_mA)$.
- *ii)* $r \geq 2k \Rightarrow \operatorname{hsp}(\overline{\mathcal{K}_{\mathscr{I}}}, \mathcal{S}_{r,m}A)$.

iii) $m \geq 2k \Rightarrow \operatorname{hsp}_{\pm}(\overline{\mathcal{K}_{\mathscr{I}}}, \mathcal{B}_m A)$ *[5, 6].*

iv) $r \geq 2k \Rightarrow \operatorname{hsp}_{\pm}(\overline{\mathcal{K}_{\mathscr{I}}}, \mathcal{S}_{r,m}\mathcal{B}_m A)$.

Our final result is a corollary of Theorem 3. 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 (3) is

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

Corollary 3. *If* (4) *holds with* $\mathcal{T} = \mathcal{S}_{r,m}$ *and if* A *satisfies* $\operatorname{hsp}(\mathbb{R}^n, \mathcal{S}_{r,m}A)$, *then* $\hat{x} - x^* = (\hat{T}A)^{\dagger}\epsilon$.

We note that condition (4) of Corollary 3 defines a non-asymptotic regime, where the local stability of estimating x^* is guaranteed, and this implies the asymptotic result of [8].

2. Preliminaries

Let $\mathbb{H}$ be equal to $\mathbb{R}$ or $\mathbb{C}$. For $k = 1, 2$ let τ_k be an $\mathbb{H}$-linear map $\mathbb{H}^m \to \mathbb{H}^m$ and write $T_k \in \mathbb{H}^{m \times m}$ for its matrix representation on the canonical basis of $\mathbb{H}^m$. Denote by $\overline{\tau}_k : \mathbb{C}^m \to \mathbb{C}^m$ the complexification of τ_k. That is $\overline{\tau}_k := \tau_k$ if $\mathbb{H} = \mathbb{C}$, and $\overline{\tau}_k(u + iv) := \tau_k(u) + i\tau_k(v)$ for every $u, v \in \mathbb{R}^m$ if $\mathbb{H} = \mathbb{R}$; here $i = \sqrt{-1}$. Note that if $\mathbb{H} = \mathbb{R}$, then T_k is also a matrix representation for $\overline{\tau}_k$. With $\lambda \in \mathbb{C}$, denote by $\mathscr{E}_{(\tau_1,\tau_2),\lambda}$ the set of all $w \in \mathbb{C}^m$ satisfying $\overline{\tau}_1(w) = \lambda\overline{\tau}_2(w)$. This is a $\mathbb{C}$-subspace of $\mathbb{C}^m$. If $\lambda \in \mathbb{R}$, then $\mathscr{E}_{(\tau_1,\tau_2),\lambda} \cap \mathbb{R}^m$ is an $\mathbb{R}$-subspace of $\mathbb{R}^m$ and we have $\dim_{\mathbb{R}}\left(\mathscr{E}_{(\tau_1,\tau_2),\lambda} \cap \mathbb{R}^m\right) = \dim_{\mathbb{C}}\left(\mathscr{E}_{(\tau_1,\tau_2),\lambda}\right)$, where $\dim_{\mathbb{R}}, \dim_{\mathbb{C}}$ denote real and complex vector space dimension respectively. In the sequel, we will drop the subscript indicating the field, with the convention that by $\dim(\mathcal{W})$ we mean $\dim_{\mathbb{H}}(\mathcal{W})$ whenever $\mathcal{W}$ is a $\mathbb{H}$-subspace of $\mathbb{H}^m$, while $\mathcal{V} \cap \mathscr{E}_{(\tau_1,\tau_2),\lambda}$ will always be treated as an $\mathbb{R}$-subspace whenever $\mathcal{V}$ is such. For simplicity, we write $\mathscr{E}_{\tau_k,\lambda} := \mathscr{E}_{(\tau_k,\mathrm{id}),\lambda}$ for the eigenspace of τ_k corresponding to eigenvalue λ, where id is the identity map. For a map of sets $\tau : \mathcal{X} \to \mathcal{Y}$ we let $\tau^{-1}(Q)$ be the inverse image of $\mathcal{Q} \subset \mathcal{Y}$ under τ. Denote by 0 the trivial subspace, the zero vector, and the number zero, to be made clear by the context. We say that two subspaces $\mathcal{V}, \mathcal{W}$ do not intersect if $\mathcal{V} \cap \mathcal{W} = 0$.

An algebraic variety is a subset of $\mathbb{H}^m$ defined as the common zero locus of a set of polynomials in m variables with coefficients in $\mathbb{H}$. The *Zariski topology* on $\mathbb{H}^m$ is defined by identifying closed sets with algebraic varieties of $\mathbb{H}^m$. Hence Zariski open sets arise as loci in $\mathbb{H}^m$ of non-simultaneous vanishing of sets of polynomials. An irreducible algebraic variety is one which can not be written as the union of two proper subvarieties of it. Here by subvariety we mean a closed set in the subspace topology. By a *generic* point of an irreducible algebraic variety having some property of interest, we mean that there is a non-empty Zariski open (and thus necessarily dense) subset in the variety, each element of which satisfies the property. We denote by $\mathrm{Gr}_{\mathbb{H}}(n, m)$ the Grassmannian of n-dimensional $\mathbb{H}$-subspaces of $\mathbb{H}^m$. One defines a Zariski topology in projective space in a similar fashion as above and under the Plücker embedding [29] $\mathrm{Gr}_{\mathbb{H}}(n, m)$ becomes an irreducible projective variety of dimension $n(m - n)$. For integers $1 \leq n_1, \dots, n_\ell \leq m - 1$ the product $\mathrm{Gr}_{\mathbb{H}}(n_1, m) \times \cdots \times \mathrm{Gr}_{\mathbb{H}}(n_\ell, m)$ is also an irreducible projective variety. Since the affine space $\mathbb{H}^{m \times n}$ is irreducible as well, we have justified what we mean by a generic $m \times n$ matrix over $\mathbb{H}$ or a generic n-dimensional $\mathbb{H}$-subspace of $\mathbb{H}^m$ or a generic subspace arrangement $(\mathcal{V}_1, \dots, \mathcal{V}_\ell)$ with $\mathcal{V}_i \in \mathrm{Gr}_{\mathbb{H}}(n_i, m)$. Another classical irreducible variety that will play a role is the *flag variety* $\mathrm{F}_{\mathbb{H}}(n_0, n, m)$. This lives in the product $\mathrm{Gr}_{\mathbb{H}}(n_0, m) \times \mathrm{Gr}_{\mathbb{H}}(n, m)$ and consists of those pairs $(\mathcal{V}_0, \mathcal{V})$ that satisfy $\mathcal{V}_0 \subset \mathcal{V}$. The following fact about projections, proved in §4.1, will be needed in the proof of Theorem 1:

Lemma 1. *Let* $\phi : \mathrm{F}_{\mathbb{H}}(n_0, n, m) \to \mathrm{Gr}_{\mathbb{H}}(n, m)$ *be the canonical projection that sends* $(\mathcal{V}_0, \mathcal{V})$ *to* $\mathcal{V}$. *If* $\mathscr{U}$ *is a non-empty Zariski open subset of* $\mathrm{F}_{\mathbb{H}}(n_0, n, m)$, *then the image* $\phi(\mathscr{U})$ *contains a non-empty Zariski open subset of* $\mathrm{Gr}_{\mathbb{H}}(n, m)$.

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 $\mathcal{Q}$ is the dimension of its *closure* $\mathcal{Q}^{\mathrm{cl}}$, i.e., $\mathcal{Q}^{\mathrm{cl}}$ is the smallest algebraic variety which contains $\mathcal{Q}$. Linear subspaces are algebraic varieties and their linear algebra dimension coincides with their algebraic-geometric dimension. By convention $\dim \mathcal{Q} = -1$ if and only if $\mathcal{Q}$ is empty, while over $\mathbb{C}$ we have that $\dim(\mathcal{Q}) = 0$ if and only if $\mathcal{Q}$ is a finite set of points. A polynomial p is called homogeneous if, writing p as a linear combination of distinct monomials, all monomials that appear with non-zero coefficient have the same degree. For instance, $\mathcal{Y}_{\tau_1,\tau_2}$ is clearly defined by homogeneous polynomials, while so is any union of linear subspaces such as $\mathcal{Z}_{\tau_1,\tau_2}$. Let $\mathcal{Y}, \mathcal{Z}$ be two algebraic varieties defined by homogeneous polynomials and set $\mathcal{U} = \mathcal{Y} \setminus \mathcal{Z}$. Then $\mathcal{U}^{\mathrm{cl}}$ is also defined by homogeneous polynomials [30]. The next statement is a folklore fact in commutative algebra and algebraic geometry and we will use it often:

Lemma 2. *Given algebraic varieties $\mathcal{Q}_1, \dots, \mathcal{Q}_t$ in $\mathbb{C}^m$ of dimensions $r_1, \dots, r_t$, each defined by homogeneous polynomials, there exists a $\mathbb{C}$-subspace $\mathcal{V} \in \mathrm{Gr}_{\mathbb{C}}(d, m)$ with $\dim(\mathcal{Q}_j \cap \mathcal{V}) = \max\{r_j + d - m, 0\}$ for any $j \in [t]$.*

Another fact that will play a role in the proof of Proposition 1, proved in §4.2, is:

Lemma 3. *Let $0 \subsetneq \mathcal{Z} \subset \mathcal{Y}$ be two algebraic varieties of $\mathbb{C}^m$ defined by homogeneous polynomials. If $\dim(\mathcal{Y} \backslash \mathcal{Z}) > m - n$, then a generic subspace $\mathcal{V} \subset \mathbb{C}^m$ of dimension n intersects $\mathcal{Y} \backslash \mathcal{Z}$.*

We close with an important fact, Lemma 5 of [2], used in the proof of Theorem 1:

Lemma 4. *Let m, n be positive integers with $m \geq 2n$. Let $\tau : \mathbb{C}^m \to \mathbb{C}^m$ be a $\mathbb{C}$-linear map with $\dim(\mathscr{E}_{\tau,\lambda}) \leq m - n$ for every $\lambda \in \mathbb{C}$. Then there is a $\mathbb{C}$-subspace $\mathcal{V}$ of $\mathbb{C}^m$ of dimension n such that $\dim(\mathcal{V} + \tau(\mathcal{V})) = 2n$.*

3. Proofs

3.1. Proof of Theorem 1

It suffices that for arbitrary $\tau_1, \tau_2 \in \mathcal{T}$ we exhibit a non-empty Zariski open subset of $\mathrm{Gr}_{\mathbb{H}}(n, m)$ on which every subspace $\mathcal{V}$ satisfies $\mathrm{hsp}(\mathcal{V}, \{\tau_1, \tau_2\})$. This 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 divide the proof in two cases, $\dim(\mathscr{E}_{(\tau_1,\tau_2),1}) \leq m - n$ and $\dim(\mathscr{E}_{(\tau_1,\tau_2),1}) > m - n$. 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 $\dim(\mathscr{E}_{(\tau_1,\tau_2),1}) \leq m - n$. Then there is an n-dimensional 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 $\mathscr{U}_1$ of subspaces $\mathcal{V} \in \mathrm{Gr}_{\mathbb{H}}(n, m)$ for which $\dim(\tau_1(\mathcal{V}) + \tau_2(\mathcal{V})) = 2n$ is non-empty. Moreover, $\mathscr{U}_1$ is open. To see this, let $A \in \mathbb{H}^{m \times n}$ have $\mathcal{V} \in \mathscr{U}_1$ as its column space. Then $\dim(\tau_1(\mathcal{V}) + \tau_2(\mathcal{V})) = 2n$ is equivalent to $\mathrm{rank}[T_1 A \ T_2 A] = 2n$, which in turn is equivalent to the non-vanishing of some $2n \times 2n$ minor of $[T_1 A \ T_2 A]$. Each such minor is a quadratic polynomial in the Plücker coordinates of $\mathcal{V}$, so that their non-simultaneous vanishing indeed gives an open set of $\mathrm{Gr}_{\mathbb{H}}(n, m)$. We next show that $\mathrm{hsp}(\mathcal{V}, \{\tau_1, \tau_2\})$ holds for every $\mathcal{V} \in \mathscr{U}_1$. 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 $\tau_1(\mathcal{V}) \cap \tau_2(\mathcal{V}) = 0$ and also $\dim(\tau_1(\mathcal{V})) = \dim(\tau_2(\mathcal{V})) = \dim(\mathcal{V}) = n$. 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 $\dim(\mathscr{E}_{(\tau_1,\tau_2),1}) > m - n$ by the following proposition, proved in §3.1.2.

Proposition 5. *In addition to the hypotheses of Theorem 1, suppose $\dim(\mathscr{E}_{(\tau_1,\tau_2),1}) = m - n_0 > m - n$. There are two subspaces $\mathcal{V}_0^* \subset \mathcal{V}^*$ of $\mathbb{H}^m$ of dimension n_0 and n respectively so that $\dim(\tau_1(\mathcal{V}_0^*) + \tau_2(\mathcal{V}^*)) = n_0 + n$.*

With $\mathcal{V}_0^*$ and $\mathcal{V}^*$ of Proposition 5 we know that

$$\mathscr{U}_2 := \{(\mathcal{V}_0, \mathcal{V}) \in \mathrm{F}_{\mathbb{H}}(n_0, n, m) : \dim_{\mathbb{H}}(\tau_1(\mathcal{V}_0) + \tau_2(\mathcal{V})) = n_0 + n\}$$

is not empty. By a similar argument that showed $\mathscr{U}_1$ is open, $\mathscr{U}_2$ is also open in $\mathrm{F}_{\mathbb{H}}(n_0, n, m)$. Now, Lemma 1 shows that $\mathscr{U}_2$ induces a non-empty open set $\mathscr{U}_3 \subset \mathrm{Gr}_{\mathbb{H}}(n, m)$ such that for every $\mathcal{V} \in \mathscr{U}_3$ there exists a

$\mathcal{V}_0 \in \mathrm{Gr}_{\mathbb{H}}(n_0, m)$ with $(\mathcal{V}_0, \mathcal{V}) \in \mathscr{U}_2$. We show that $\mathrm{hsp}(\mathcal{V}, \{\tau_1, \tau_2\})$ holds for any $\mathcal{V} \in \mathscr{U}_3$. So suppose that $\tau_1(v_1) = \tau_2(v_2)$ with $v_1, v_2 \in \mathcal{V}$ and let $\mathcal{V}_0$ be as above. Thus $\dim(\tau_1(\mathcal{V}_0) + \tau_2(\mathcal{V})) = n_0 + n$ and in particular $\dim(\tau_1(\mathcal{V}_0) + \tau_2(\mathcal{V}_0)) = 2n_0$. Necessarily $\mathcal{V}_0 \cap \mathscr{E}_{(\tau_1,\tau_2),1} = 0$. Now by hypothesis, $\mathcal{V} \cap \mathscr{E}_{(\tau_1,\tau_2),1}$ has dimension at least $n + m - n_0 - m = n - n_0$. In fact, we must have $\dim(\mathcal{V} \cap \mathscr{E}_{(\tau_1,\tau_2),1}) = n - n_0$ otherwise the subspaces $\mathcal{V}_0$ and $\mathcal{V} \cap \mathscr{E}_{(\tau_1,\tau_2),1}$ of $\mathcal{V}$ must intersect, contradicting the fact $\mathcal{V}_0$ does not intersect $\mathscr{E}_{(\tau_1,\tau_2),1}$. We conclude that $\mathcal{V}_0$ and $\mathcal{V} \cap \mathscr{E}_{(\tau_1,\tau_2),1}$ are subspace complements in $\mathcal{V}$. Write v_1 as a sum of two vectors v_0 and w in $\mathcal{V}_0$ and $\mathcal{V} \cap \mathscr{E}_{(\tau_1,\tau_2),1}$ respectively. Then $\tau_1(v_1) = \tau_2(v_2)$ implies $\tau_1(v_0) = \tau_2(v_2) - \tau_1(w) = \tau_2(v_2 - w)$. Since $v_0 \in \mathcal{V}_0$, $(v_2 - w) \in \mathcal{V}$ and $(\mathcal{V}_0, \mathcal{V}) \in \mathscr{U}_2$, the definition of $\mathscr{U}_2$ implies that $v_0 = 0$ and $v_2 - w = 0$. That is, $v_1 = w = v_2$. □

3.1.1. Proof of Proposition 4

For $\mathbb{H} = \mathbb{R}$ we have $T_1, T_2 \in \mathbb{R}^{m \times m}$ and it suffices to show that $\mathrm{rank}[T_1 A \; T_2 A] = 2n$ for some $A \in \mathbb{R}^{m \times n}$. This is equivalent to showing some $2n \times 2n$ minor of $[T_1 A \; T_2 A]$ is a nonzero polynomial in the entries of A. This is certainly true if the evaluation of that minor is non-zero for some $A^* \in \mathbb{C}^{m \times n}$. Hence it suffices to prove Proposition 4 for $\mathbb{H} = \mathbb{C}$, which will be the field of choice for the rest of this section.

We start by introducing a sequence of subspaces and study some useful properties. Set $\mathcal{R}_0, \mathcal{F}_0$ equal to $\mathbb{C}^m$. For any non-negative integer j define

$$\begin{aligned} \mathcal{G}_{j+1} &= \tau_1(\mathcal{R}_j \cap \mathcal{F}_j) \cap \tau_2(\mathcal{R}_j \cap \mathcal{F}_j), \\ \mathcal{R}_{j+1} &= \tau_1^{-1}(\mathcal{G}_{j+1}) \cap \mathcal{R}_j \cap \mathcal{F}_j, \\ \mathcal{F}_{j+1} &= \tau_2^{-1}(\mathcal{G}_{j+1}) \cap \mathcal{R}_j \cap \mathcal{F}_j. \end{aligned} \tag{5}$$

Part iv) of the next lemma gives some motivation behind the definition of recursions[1] (5):

Lemma 5. *For any non-negative integer j we have i) $\mathcal{R}_{j+1} \subset \mathcal{R}_j \cap \mathcal{F}_j \subset \mathcal{R}_j$, ii) $\mathcal{F}_{j+1} \subset \mathcal{R}_j \cap \mathcal{F}_j \subset \mathcal{F}_j$, iii) $\mathcal{G}_{j+2} \subset \mathcal{G}_{j+1}$ and iv) $\tau_1(\mathcal{R}_{j+1}) = \tau_2(\mathcal{F}_{j+1}) = \mathcal{G}_{j+1}$.*

Proof. i) and ii) are directly by definition and so is $\mathcal{R}_{j+1} \cap \mathcal{F}_{j+1} \subset \mathcal{R}_j \cap \mathcal{F}_j$. This latter implies

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

We now show that $\tau_1(\mathcal{R}_{j+1}) = \mathcal{G}_{j+1}$. From $\mathcal{R}_{j+1} \subset \tau_1^{-1}(\mathcal{G}_{j+1})$ we have $\tau_1(\mathcal{R}_{j+1}) \subset \tau_1(\tau_1^{-1}(\mathcal{G}_{j+1})) \subset \mathcal{G}_{j+1}$. For the reverse direction $\mathcal{G}_{j+1} \subset \tau_1(\mathcal{R}_{j+1})$ 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 $w \in \mathcal{R}_j \cap \mathcal{F}_j$ with $\tau_1(w) = z$. 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 so $w \in \tau_1^{-1}(\mathcal{G}_{j+1}) \cap \mathcal{R}_j \cap \mathcal{F}_j = \mathcal{R}_{j+1}$. Hence $z \in \tau_1(\mathcal{R}_{j+1})$. A similar derivation gives $\tau_2(\mathcal{F}_{j+1}) = \mathcal{G}_{j+1}$. □

Lemma 5 gives two subspace chains $\cdots \subset \mathcal{R}_{j+1} \subset \mathcal{R}_j \subset \cdots \subset \mathcal{R}_0$ and $\cdots \subset \mathcal{F}_{j+1} \subset \mathcal{F}_j \subset \cdots \subset \mathcal{F}_0$. These stabilize at a common subspace:

Lemma 6. *There is a non-negative integer α such that $\mathcal{R}_j = \mathcal{F}_j$ for every $j \geq \alpha$ and $\tau_1(\mathcal{R}_\alpha) = \tau_2(\mathcal{R}_\alpha) = \mathcal{G}_\alpha$.*

Proof. Since the subspaces $\mathcal{R}_0$ and $\mathcal{F}_0$ are of finite dimension m, both chains stabilize, that is, there exist non-negative integers α_1 and α_2 such that for any $j_1 \geq \alpha_1$ and $j_2 \geq \alpha_2$ we have $\mathcal{R}_{j_1} = \mathcal{R}_{j_1+1}$ 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 $\mathcal{F}_\alpha = \mathcal{F}_{\alpha+1}$. Lemma 5 and the definition of α give $\mathcal{R}_{\alpha+1} \subset \mathcal{R}_\alpha \cap \mathcal{F}_\alpha \subset \mathcal{R}_\alpha = \mathcal{R}_{\alpha+1}$. 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 $\mathcal{R}_\alpha = \mathcal{F}_\alpha$. The equality $\tau_1(\mathcal{R}_\alpha) = \tau_2(\mathcal{R}_\alpha) = \mathcal{G}_\alpha$ is immediate from Lemma 5. □

The strategy of the proof is to make use of the $\mathcal{R}$ chain ascending from $\mathcal{R}_\alpha$

$$\mathcal{R}_\alpha \subset \mathcal{R}_{\alpha-1} \cap \mathcal{F}_{\alpha-1} \subset \mathcal{R}_{\alpha-1} \subset \cdots \subset \mathcal{R}_1 \subset \mathcal{R}_0 \cap \mathcal{F}_0 \subset \mathcal{R}_0 = \mathbb{C}^m \tag{6}$$

---

[1] Our recursions bear some resemblance with the somewhat less complicated Wong sequence [31], which for example was used in [32, 33]. A detailed comparison of the two constructions is left as future work.

in the following fashion. First we show that there is always a j_0, such that either there is a subspace $\mathcal{W}_{j_0} \subset \mathcal{R}_{j_0}$ of dimension $[\dim(\mathcal{R}_{j_0}) - (m-n)]$ with $\dim(\tau_1(\mathcal{W}_{j_0}) + \tau_2(\mathcal{W}_{j_0})) = 2\dim(\mathcal{W}_{j_0})$ or there is a subspace $\mathcal{Z}_{j_0} \subset \mathcal{R}_{j_0} \cap \mathcal{F}_{j_0}$ of dimension $[\dim(\mathcal{R}_{j_0} \cap \mathcal{F}_{j_0}) - (m-n)]$ with $\dim(\tau_1(\mathcal{Z}_{j_0}) + \tau_2(\mathcal{Z}_{j_0})) = 2\dim(\mathcal{Z}_{j_0})$. Then we describe devices to pass either from $\mathcal{W}_{j_0}$ to $\mathcal{Z}_{j_0-1}$ or from $\mathcal{Z}_{j_0}$ to $\mathcal{W}_{j_0-1}$, all the while preserving the properties i) $\dim(\tau_1(\mathcal{Z}_{j_0-1}) + \tau_2(\mathcal{Z}_{j_0-1})) = 2\dim(\mathcal{Z}_{j_0-1})$ and $\dim(\mathcal{Z}_{j_0-1}) = [\dim(\mathcal{R}_{j_0-1} \cap \mathcal{F}_{j_0-1}) - (m-n)]$ or ii) $\dim(\tau_1(\mathcal{W}_{j_0-1}) + \tau_2(\mathcal{W}_{j_0-1})) = 2\dim(\mathcal{W}_{j_0-1})$ and $\dim(\mathcal{W}_{j_0-1}) = [\dim(\mathcal{R}_{j_0-1}) - (m-n)]$. Then inductively $\mathcal{V}^* := \mathcal{W}_0$ will satisfy the statement of the proposition since $\mathcal{R}_0 = \mathbb{C}^m$. Below, we distinguish between three cases, in two out of which the existence of a $\mathcal{W}_{j_0}$ is proved while the third one proves the existence of a $\mathcal{Z}_{j_0}$. The next lemma handles the case where j_0 can be taken to be α.

Lemma 7 ($\mathcal{W}_\alpha$-Initialization). *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. By Lemma 6 and the rank-plus-nullity theorem we have

$$\dim(\ker(\tau_1|_{\mathcal{R}_\alpha})) = \dim(\mathcal{R}_\alpha) - \dim(\mathcal{G}_\alpha) = \dim(\ker(\tau_2|_{\mathcal{R}_\alpha}))$$

Moreover, by hypothesis $\operatorname{rank}(\tau_1|_{\mathcal{R}_\alpha}) \geq \dim(\mathcal{R}_\alpha) - (m-2n) > n$. Hence

$$(m-n) + \dim(\mathcal{G}_\alpha) - \dim(\mathcal{R}_\alpha) = \operatorname{rank}(\tau_1|_{\mathcal{R}_\alpha}) - n > 0$$

Since $\dim(\mathcal{U}^{\mathrm{cl}}_{\tau_1,\tau_2}) = \dim(\mathcal{U}_{\tau_1,\tau_2}) \leq m-n$ and $\dim(\mathscr{E}_{(\tau_1,\tau_2),1}) \leq m-n$ as well, Lemma 2 gives a subspace $\mathcal{H}$ of $\mathcal{R}_\alpha$ of dimension $\dim(\mathcal{G}_\alpha)$, such that $\mathcal{H} \cap \ker(\tau_1|_{\mathcal{R}_\alpha}) = \mathcal{H} \cap \ker(\tau_2|_{\mathcal{R}_\alpha}) = 0$ and

$$\dim(\mathcal{U}^{\mathrm{cl}}_{\tau_1,\tau_2} \cap \mathcal{H}) \leq (m-n) + \dim(\mathcal{G}_\alpha) - \dim(\mathcal{R}_\alpha) \tag{7}$$
$$\dim(\mathscr{E}_{(\tau_1,\tau_2),1} \cap \mathcal{H}) \leq (m-n) + \dim(\mathcal{G}_\alpha) - \dim(\mathcal{R}_\alpha) \tag{8}$$

Since $\tau_1(\mathcal{H}) = \mathcal{G}_\alpha = \tau_2(\mathcal{H})$ we have that $\tau_{\mathcal{H}} := (\tau_1|_{\mathcal{H}})^{-1}\tau_2|_{\mathcal{H}}$ is an isomorphism of $\mathcal{H}$. We are going to get our subspace $\mathcal{W}_\alpha$ by applying Lemma 4 with ambient space $\mathcal{H}$, $\mathbb{C}$-linear map $\tau_{\mathcal{H}}$ and subspace dimension $[\dim(\mathcal{R}_\alpha) - (m-n)]$, this number being positive by hypothesis. There are two things we need to check, the first being that $\dim(\mathcal{H}) \geq 2[\dim(\mathcal{R}_\alpha) - (m-n)]$. Indeed, this is true because

$$\begin{aligned}
\dim(\mathcal{H}) \geq 2[\dim(\mathcal{R}_\alpha) - (m-n)] &\Leftrightarrow 2m - 2n \geq \dim(\mathcal{R}_\alpha) + \dim(\mathcal{R}_\alpha) - \dim(\mathcal{G}_\alpha) \\
&\Leftrightarrow 2m - 2n \geq \dim(\mathcal{R}_\alpha) + \dim(\ker(\tau_1|_{\mathcal{R}_\alpha})) \\
&\Leftarrow 2m - 2n \geq \dim(\mathcal{R}_\alpha) + \dim(\ker(\tau_1)) \\
&\Leftrightarrow (\operatorname{rank}(\tau_1) - 2n) + (m - \dim(\mathcal{R}_\alpha)) \geq 0
\end{aligned}$$

and the last inequality is true by hypothesis. The second thing that we need to check is that for any $\lambda \in \mathbb{C}$

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

When $\lambda = 0$, we have $\mathscr{E}_{\tau_{\mathcal{H}},0} = \ker(\tau_{\mathcal{H}}) = 0$, because $\tau_{\mathcal{H}}$ is an isomorphism. When $\lambda \neq 0$, $v \in \mathscr{E}_{\tau_{\mathcal{H}},\lambda}$ is equivalent to $\tau_1|_{\mathcal{H}}(v) = \lambda\tau_2|_{\mathcal{H}}(v)$ or equivalently $v \in (\mathcal{U}_{\tau_1,\tau_2} \cap \mathcal{H}) \cup (\mathscr{E}_{(\tau_1,\tau_2),1} \cap \mathcal{H})$. This shows that $\mathscr{E}_{\tau_{\mathcal{H}},\lambda}$ lives in $(\mathcal{U}^{\mathrm{cl}}_{\tau_1,\tau_2} \cap \mathcal{H}) \cup (\mathscr{E}_{(\tau_1,\tau_2),1} \cap \mathcal{H})$ and as per (7) and (8) that latter set has dimension at most $\dim(\mathcal{H}) - [\dim(\mathcal{R}_\alpha) - (m-n)]$.

Now Lemma 4 gives a subspace $\mathcal{W}_\alpha$ of $\mathcal{H}$ of dimension $[\dim(\mathcal{R}_\alpha) - (m-n)]$ such that $\dim(\mathcal{W}_\alpha + \tau_{\mathcal{H}}(\mathcal{W}_\alpha)) = 2\dim(\mathcal{W}_\alpha)$. 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 have that $\mathcal{W}_\alpha + \tau_{\mathcal{H}}(\mathcal{W}_\alpha) \cong \tau_1|_{\mathcal{H}}(\mathcal{W}_\alpha + \tau_{\mathcal{H}}(\mathcal{W}_\alpha)) = \tau_1(\mathcal{W}_\alpha) + \tau_2(\mathcal{W}_\alpha)$. That is, $\dim(\tau_1(\mathcal{W}_\alpha) + \tau_2(\mathcal{W}_\alpha)) = 2\dim(\mathcal{W}_\alpha)$. □

If $\alpha = 0$, then Proposition 4 is proved by Lemma 7, so we assume $\alpha > 0$ for the sequel. If $\dim(\mathcal{R}_\alpha) \leq m-n$, and since $\dim(\mathcal{R}_0) = m$, then necessarily one of the two following cases must occur in the chain (6). Either there is a β with $\dim(\mathcal{R}_\beta \cap \mathcal{F}_\beta) \leq m-n < \dim(\mathcal{R}_\beta)$ or there is a γ with $\dim(\mathcal{R}_{\gamma+1}) \leq m-n < \dim(\mathcal{R}_\gamma \cap \mathcal{F}_\gamma)$. The next two lemmas show how to choose $\mathcal{W}_\beta \subset \mathcal{R}_\beta$ and $\mathcal{Z}_\gamma \subset \mathcal{R}_\gamma \cap \mathcal{F}_\gamma$, respectively.

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

Proof. We have

$$[\dim(\mathcal{R}_\beta)-(m-n)] + \dim(\ker(\tau_1)) = \dim(\mathcal{R}_\beta) + (n-\operatorname{rank}(\tau_1)) \leq \dim(\mathcal{R}_\beta)$$

and a similar inequality for τ_2. Moreover,

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

Consequently, by Lemma 2 there exists a subspace $\mathcal{W}_\beta$ of $\mathcal{R}_\beta$ of dimension $[\dim(\mathcal{R}_\beta)-(m-n)]$ which does not intersect $\ker(\tau_1), \ker(\tau_2)$ and $\mathcal{R}_\beta\cap\mathcal{F}_\beta$. Clearly $\beta > 0$ and Lemma 5 gives $\tau_1(\mathcal{W}_\beta) \subset \tau_1(\mathcal{R}_\beta) = \mathcal{G}_\beta$. Recalling definition (5), we have

$$\begin{aligned}
\mathcal{W}_\beta \cap \tau_2^{-1}(\tau_1(\mathcal{W}_\beta)) &\subset \mathcal{W}_\beta \cap \tau_2^{-1}(\mathcal{G}_\beta)\\
&= \mathcal{W}_\beta \cap \tau_2^{-1}(\mathcal{G}_\beta) \cap \mathcal{R}_\beta\\
&= \mathcal{W}_\beta \cap \tau_2^{-1}(\mathcal{G}_\beta) \cap \tau_1^{-1}(\mathcal{G}_\beta) \cap \mathcal{R}_{\beta-1} \cap \mathcal{F}_{\beta-1}\\
&= \mathcal{W}_\beta \cap \tau_1^{-1}(\mathcal{G}_\beta) \cap \mathcal{F}_\beta\\
&\subset \mathcal{W}_\beta \cap \mathcal{F}_\beta = \mathcal{W}_\beta \cap \mathcal{R}_\beta \cap \mathcal{F}_\beta = 0.
\end{aligned}$$

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

Lemma 9 ($\mathcal{Z}_\gamma$-Initialization). *In addition to the hypotheses of Proposition 4, suppose that* $\dim(\mathcal{R}_{\gamma+1}) \leq m-n < \dim(\mathcal{R}_\gamma\cap\mathcal{F}_\gamma)$ *for some non-negative integer* γ. *Then there exists a subspace* $\mathcal{Z}_\gamma$ *of* $\mathcal{R}_\gamma\cap\mathcal{F}_\gamma$ *of dimension* $[\dim(\mathcal{R}_\gamma\cap\mathcal{F}_\gamma)-(m-n)]$, *such that* $\dim(\tau_1(\mathcal{Z}_\gamma)+\tau_2(\mathcal{Z}_\gamma)) = 2\dim(\mathcal{Z}_\gamma)$.

Proof. We have

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

and a similar inequality for τ_2. Moreover,

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

Thus Lemma 2 implies the existence of a subspace $\mathcal{Z}_\gamma$ of $\mathcal{R}_\gamma\cap\mathcal{F}_\gamma$ of dimension $[\dim(\mathcal{R}_\gamma\cap\mathcal{F}_\gamma)-(m-n)]$ which does not intersect $\ker(\tau_1), \ker(\tau_2)$ and $\mathcal{R}_{\gamma+1}$. This gives $\dim(\tau_1(\mathcal{Z}_\gamma)) = \dim(\tau_2(\mathcal{Z}_\gamma)) = \dim(\mathcal{Z}_\gamma)$. It now suffices to prove $\tau_1(\mathcal{Z}_\gamma)\cap\tau_2(\mathcal{Z}_\gamma) = 0$. Let $\tau_1(v_1) = \tau_2(v_2)$ for some $v_1, v_2 \in \mathcal{Z}_\gamma$. Then

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

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

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

Thus $v_1 = 0$ and we have proved $\tau_1(\mathcal{Z}_\gamma)\cap\tau_2(\mathcal{Z}_\gamma) = 0$. ☐

Table 1 summarizes the three different types of initialization, two giving $\mathcal{W}_\alpha, \mathcal{W}_\beta$ and the third one $\mathcal{Z}_\gamma$. With μ either α or β, we have that subspace $\mathcal{W}_\mu$ of $\mathcal{R}_\mu$ satisfies

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

Table 1: Three different types of initialization.

$\mathcal{W}_\alpha: \; m-n<\dim(\mathcal{R}_\alpha)$	Lemma 7
$\mathcal{W}_\beta: \; \dim(\mathcal{R}_\beta \cap \mathcal{F}_\beta) \leq m-n<\dim(\mathcal{R}_\beta)$	Lemma 8
$\mathcal{Z}_\gamma: \; \dim(\mathcal{R}_{\gamma+1}) \leq m-n<\dim(\mathcal{R}_\gamma \cap \mathcal{F}_\gamma)$	Lemma 9

On the other hand, $\mathcal{Z}_\gamma$ is a subspace of $\mathcal{R}_\gamma \cap \mathcal{F}_\gamma$ and satisfies

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

Thus, either we have a chain of the form

$$\mathcal{W}_\mu \subset \mathcal{R}_\mu \subset \mathcal{R}_{\mu-1} \cap \mathcal{F}_{\mu-1} \subset \cdots \subset \mathcal{R}_0=\mathbb{C}^m$$

or a chain of the form

$$\mathcal{Z}_\gamma \subset \mathcal{R}_\gamma \cap \mathcal{F}_\gamma \subset \mathcal{R}_\gamma \subset \cdots \subset \mathcal{R}_0=\mathbb{C}^m.$$

The next two lemmas show that we can always extend $\mathcal{W}_\mu$ to $\mathcal{Z}_{\mu-1}$ or $\mathcal{Z}_\gamma$ to $\mathcal{W}_{\gamma-1}$ and so on, thus enabling induction and thus concluding the proof of the proposition. The proof of Lemma 11 follows an identical argument as in the proof of Lemma 10 and is thus omitted.

Lemma 10 ($\mathcal{W}_j$-Extension). *In addition to the hypotheses of Proposition 4, suppose for some 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*

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

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

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

Proof. If $\mathcal{R}_j \cap \mathcal{F}_j=\mathcal{R}_j$, then we are done by letting $\mathcal{W}_j=\mathcal{Z}_j$. In what follows we assume $\dim(\mathcal{R}_j)>\dim(\mathcal{R}_j \cap \mathcal{F}_j)$, in particular $j>0$. The subspace $\tau_1^{-1}(\tau_1(\mathcal{Z}_j)+\tau_2(\mathcal{Z}_j))$ has dimension at most $(m-\operatorname{rank}(\tau_1))+2[\dim(\mathcal{R}_j \cap \mathcal{F}_j)-(m-n)]$. Hence

$$\begin{aligned}[\dim(\mathcal{R}_j)-\dim(\mathcal{R}_j \cap \mathcal{F}_j)]+\dim(\tau_1^{-1}(\tau_1(\mathcal{Z}_j)+\tau_2(\mathcal{Z}_j))) &\leq \dim(\mathcal{R}_j)+[2n-\operatorname{rank}(\tau_1)]+[\dim(\mathcal{R}_j \cap \mathcal{F}_j)-m] \\ &\leq \dim(\mathcal{R}_j).\end{aligned}$$

By hypothesis it is also true that $[\dim(\mathcal{R}_j)-\dim(\mathcal{R}_j \cap \mathcal{F}_j)]+\dim(\ker(\tau_1)) \leq \dim(\mathcal{R}_j)$ and similarly for τ_2. 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 does not intersect the subspaces $\mathcal{R}_j \cap \mathcal{F}_j$, $\tau_1^{-1}(\tau_1(\mathcal{Z}_j)+\tau_2(\mathcal{Z}_j))$, $\ker(\tau_1)$, $\ker(\tau_2)$. In particular $\tau_1(\mathcal{W}_j') \cap [\tau_1(\mathcal{Z}_j)+\tau_2(\mathcal{Z}_j)]=0$. This together with the hypothesis gives $\dim(\tau_1(\mathcal{Z}_j)+\tau_2(\mathcal{Z}_j)+\tau_1(\mathcal{W}_j'))=2[\dim(\mathcal{R}_j \cap \mathcal{F}_j)-(m-n)]+[\dim(\mathcal{R}_j)-\dim(\mathcal{R}_j \cap \mathcal{F}_j)]$. Equivalently,

$$\dim(\tau_1(\mathcal{Z}_j+\mathcal{W}_j')+\tau_2(\mathcal{Z}_j))=\dim(\mathcal{R}_j)+\dim(\mathcal{R}_j \cap \mathcal{F}_j)-2(m-n). \tag{9}$$

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 subspace of $\mathcal{G}_j$, and consequently

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

In short, we have $\mathcal{W}'_j \cap \tau_2^{-1}(\tau_1(\mathcal{Z}_j + \mathcal{W}'_j) + \tau_2(\mathcal{Z}_j)) = 0$ and so $\tau_2(\mathcal{W}'_j) \cap [\tau_1(\mathcal{Z}_j + \mathcal{W}'_j) + \tau_2(\mathcal{Z}_j)] = 0$. Recalling (9), 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,

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

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

Lemma 11 ($\mathcal{Z}_j$-Extension). *In addition to the hypotheses of Proposition 4, suppose for some 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*

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

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

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

□

3.1.2. Proof of Proposition 5

Note that $\operatorname{rank}(\tau_1), \operatorname{rank}(\tau_2) \geq 2n > 2n_0$ and $\dim(\mathcal{U}_{\tau_1,\tau_2}) \leq m - n < m - n_0$. Invoking Proposition 4, we get a subspace $\mathcal{V}_0$ of $\operatorname{Gr}_{\mathbb{H}}(n_0, m)$ which satisfies $\dim(\tau_1(\mathcal{V}_0) + \tau_2(\mathcal{V}_0)) = 2n_0$. The dimension of the subspace $\tau_2^{-1}(\tau_1(\mathcal{V}_0) + \tau_2(\mathcal{V}_0))$ is at most $(m - \operatorname{rank}(\tau_2)) + 2n_0$, and

$$(n - n_0) + [(m - \operatorname{rank}(\tau_2)) + 2n_0] = m + (n + n_0 - \operatorname{rank}(\tau_2)) < m + 2n - \operatorname{rank}(\tau_2) \leq m.$$

By Lemma 2, there is a subspace $\mathcal{W}$ of $\mathbb{H}^m$ of dimension $n - n_0$ such that $\mathcal{W}$ does not intersect the subspaces $\tau_2^{-1}(\tau_1(\mathcal{V}_0) + \tau_2(\mathcal{V}_0))$, $\mathcal{V}_0$ and $\ker(\tau_2)$. Hence $\dim(\mathcal{W} + \mathcal{V}_0) = n$, $\tau_2(\mathcal{W}) \cap (\tau_1(\mathcal{V}_0) + \tau_2(\mathcal{V}_0)) = 0$ and

$$\dim(\tau_1(\mathcal{V}_0) + \tau_2(\mathcal{W} + \mathcal{V}_0)) = \dim(\tau_2(\mathcal{W})) + \dim(\tau_1(\mathcal{V}_0) + \tau_2(\mathcal{V}_0)) = n - n_0 + 2n_0 = n + n_0.$$

Letting $\mathcal{V} = \mathcal{W} + \mathcal{V}_0$ we are done. □

3.2. Proof of Proposition 1

Any $\mathcal{V} \in \operatorname{Gr}_{\mathbb{C}}(n, m)$ that intersects $\mathcal{U}_{\tau_1,\tau_2}$ violates $\operatorname{hsp}(\mathcal{V}, \mathcal{T})$. So it suffices to show $\mathcal{V} \cap \mathcal{U}_{\tau_1,\tau_2}$ is not empty for a generic $\mathcal{V} \in \operatorname{Gr}_{\mathbb{C}}(n, m)$. This follows from Lemma 3, proved in §4.2, and the fact that $\mathcal{U}_{\tau_1,\tau_2} = \mathcal{Y}_{\tau_1,\tau_2} \setminus \mathcal{Z}_{\tau_1,\tau_2}$, with both $\mathcal{Y}_{\tau_1,\tau_2}$ and $\mathcal{Z}_{\tau_1,\tau_2}$ defined by homogeneous polynomials. □

3.3. Proof of Theorem 2

Set $\mathscr{G} = \operatorname{Gr}_{\mathbb{H}}(n_1, m) \times \cdots \times \operatorname{Gr}_{\mathbb{H}}(n_\ell, m)$ and for every $\mathcal{I} \subset [\ell]$ denote by $\mathscr{G}_{\mathcal{I}}$ the product of the factors of $\mathscr{G}$ indexed by $\mathcal{I}$. It is clear that an open set of $\mathscr{G}_{\mathcal{I}}$ gives rise to an open set of $\mathscr{G}$, with the closed locus in $\mathscr{G}$ to be avoided defined by equations involving only the Plücker coordinates of the factors indexed by $\mathcal{I}$. To show that $\operatorname{hsp}(\overline{\mathcal{A}_{\mathscr{I}}}, \mathcal{T})$ holds true for every subspace arrangement $(\mathcal{V}_1, \ldots, \mathcal{V}_\ell)$ on a non-empty open set $\mathscr{U}$ of $\mathscr{G}$, it suffices to show that $\operatorname{hsp}(\mathcal{V}_{\mathcal{I}_i} \cup \mathcal{V}_{\mathcal{I}_j}, \{\tau_\alpha, \tau_\beta\})$ holds true on a non-empty open set $\mathscr{U}_{i,j,\alpha,\beta}$ of $\mathscr{G}_{\mathcal{I}_i \cup \mathcal{I}_j}$ for every $\mathcal{I}_i, \mathcal{I}_j \in \mathscr{I}$ and for every $\tau_\alpha, \tau_\beta \in \mathcal{T}$. For then $\mathscr{U}$ will be the intersection of all $\mathscr{U}_{i,j,\alpha,\beta}$'s, viewed as open sets of $\mathscr{G}$. With i, j, α, β fixed, we show the existence of such a $\mathscr{U}_{i,j,\alpha,\beta}$.

The dimension of the subspace $\tau_\alpha(\mathcal{V}_{\mathcal{I}_i}) + \tau_\beta(\mathcal{V}_{\mathcal{I}_j})$ attains its maximum possible value, say c, on a non-empty open set $\mathscr{U}_{\mathcal{I}_i \cup \mathcal{I}_j}$ of $\mathscr{G}_{\mathcal{I}_i \cup \mathcal{I}_j}$. To see this, let A_k be an $m \times n_k$ matrix with a basis of $\mathcal{V}_k$ in its columns. Let $A_{\mathcal{I}_i}$ be the column-wise concatenation of those A_k's with $k \in \mathcal{I}_i$. Define similarly $A_{\mathcal{I}_i}$ and $A_{\mathcal{I}_i \cup \mathcal{I}_j}$. Let us view the entries of the A_k's as polynomial variables and consider the polynomial ring $\mathbb{H}[A_{\mathcal{I}_i \cup \mathcal{I}_j}]$ whose elements are polynomials in the variables $A_{\mathcal{I}_i \cup \mathcal{I}_j}$ and coefficients in $\mathbb{H}$. Let $\mathbb{H}(A_{\mathcal{I}_i \cup \mathcal{I}_j})$ be the field of fractions of $\mathbb{H}[A_{\mathcal{I}_i \cup \mathcal{I}_j}]$, that is every element of $\mathbb{H}(A_{\mathcal{I}_i \cup \mathcal{I}_j})$ is of the form f/g with $f, g \in \mathbb{H}[A_{\mathcal{I}_i \cup \mathcal{I}_j}]$ and $g \neq 0$. Then the matrix $[T_\alpha A_{\mathcal{I}_i}\ \ T_\beta A_{\mathcal{I}_i \cap \mathcal{I}_j}]$ is an element of $\mathbb{H}(A_{\mathcal{I}_i \cup \mathcal{I}_j})^{m \times (n_{\mathcal{I}_i} + n_{\mathcal{I}_j})}$ and c coincides with its rank over

$\mathbb{H}(A_{\mathcal{I}_i\cup\mathcal{I}_j})$. Moreover, $\mathscr{U}_{\mathcal{I}_i\cup\mathcal{I}_j}$ is defined by the non-simultaneous vanishing of all $c\times c$ determinants of that matrix, which are polynomials in the Plücker coordinates of the A_k's.

We claim that for every subspace arrangement $(\mathcal{V}_k)_{k\in\mathcal{I}_i\cup\mathcal{I}_j}\in\mathscr{U}_{\mathcal{I}_i\cup\mathcal{I}_j}$ the subspace $\tau_\beta(\mathcal{V}_{\mathcal{I}_j\backslash\mathcal{I}_i})$ does not intersect $\tau_\alpha(\mathcal{V}_{\mathcal{I}_i})+\tau_\beta(\mathcal{V}_{\mathcal{I}_i\cap\mathcal{I}_j})$. To see this, note $\tau_\alpha(\mathcal{V}_{\mathcal{I}_i})+\tau_\beta(\mathcal{V}_{\mathcal{I}_j})=\tau_\alpha(\mathcal{V}_{\mathcal{I}_i})+\tau_\beta(\mathcal{V}_{\mathcal{I}_i\cap\mathcal{I}_j})+\tau_\beta(\mathcal{V}_{\mathcal{I}_j\backslash\mathcal{I}_i})$ and

$$\begin{aligned}c=\dim(\tau_\alpha(\mathcal{V}_{\mathcal{I}_i})+\tau_\beta(\mathcal{V}_{\mathcal{I}_i\cap\mathcal{I}_j})+\tau_\beta(\mathcal{V}_{\mathcal{I}_j\backslash\mathcal{I}_i}))=&\dim(\tau_\alpha(\mathcal{V}_{\mathcal{I}_i})+\tau_\beta(\mathcal{V}_{\mathcal{I}_i\cap\mathcal{I}_j}))+\dim(\tau_\beta(\mathcal{V}_{\mathcal{I}_j\backslash\mathcal{I}_i}))\\&-\dim((\tau_\alpha(\mathcal{V}_{\mathcal{I}_i})+\tau_\beta(\mathcal{V}_{\mathcal{I}_i\cap\mathcal{I}_j}))\cap\tau_\beta(\mathcal{V}_{\mathcal{I}_j\backslash\mathcal{I}_i}))\end{aligned}$$

By hypothesis $n_{\mathcal{I}_i},n_{\mathcal{I}_j}\le n\le m/2$ and $\operatorname{rank}(\tau_\beta)\ge 2n$, thus

$$\dim(\tau_\alpha(\mathcal{V}_{\mathcal{I}_i})+\tau_\beta(\mathcal{V}_{\mathcal{I}_i\cap\mathcal{I}_j}))\le n_{\mathcal{I}_i}+n_{\mathcal{I}_i\cap\mathcal{I}_j}\le 2n-n_{\mathcal{I}_j\backslash\mathcal{I}_i}\le\operatorname{rank}(\tau_\beta)-n_{\mathcal{I}_j\backslash\mathcal{I}_i}$$

Now, if $\tau_\beta(\mathcal{V}_{\mathcal{I}_j\backslash\mathcal{I}_i})$ intersects $\tau_\alpha(\mathcal{V}_{\mathcal{I}_i})+\tau_\beta(\mathcal{V}_{\mathcal{I}_i\cap\mathcal{I}_j})$, there is another arrangement obtained by setting $\mathcal{V}'_k=\mathcal{V}_k$ for every $k\in\mathcal{I}_i$ and replacing the $\mathcal{V}_k$'s with $k\in\mathcal{I}_j\backslash\mathcal{I}_i$ by suitable $\mathcal{V}'_k$, $k\in\mathcal{I}_j\backslash\mathcal{I}_i$, such that i) $\dim\tau_\beta(\mathcal{V}'_{\mathcal{I}_j\backslash\mathcal{I}_i})=n_{\mathcal{I}_j\backslash\mathcal{I}_i}$ and ii) $\tau_\beta(\mathcal{V}'_{\mathcal{I}_j\backslash\mathcal{I}_i})$ does not intersect $\tau_\alpha(\mathcal{V}_{\mathcal{I}_i})+\tau_\beta(\mathcal{V}_{\mathcal{I}_i\cap\mathcal{I}_j})$. Such a replacement is always possible. But then $\dim(\tau_\alpha(\mathcal{V}'_{\mathcal{I}_i})+\tau_\beta(\mathcal{V}'_{\mathcal{I}_j}))>\dim(\tau_\alpha(\mathcal{V}_{\mathcal{I}_i})+\tau_\beta(\mathcal{V}_{\mathcal{I}_j}))$, a contradiction on the maximality of c. A similar argument shows that the same property is true if we interchange the roles of i and j. In the sequel, we will obtain $\mathscr{U}_{i,j,\alpha,\beta}$ by intersecting $\mathscr{U}_{\mathcal{I}_i\cup\mathcal{I}_j}$ with several other suitable non-empty open sets.

By dimension considerations, there is a non-empty open set $\mathscr{U}'_{\mathcal{I}_i\cup\mathcal{I}_j}$ of $\mathscr{G}_{\mathcal{I}_i\cup\mathcal{I}_j}$ such that the $\mathcal{V}_k$'s are independent subspaces for every subspace arrangement in $\mathscr{U}'_{\mathcal{I}_i\cup\mathcal{I}_j}$, that is $\dim(\mathcal{V}_{\mathcal{I}_i\cup\mathcal{I}_j})=n_{\mathcal{I}_i\cup\mathcal{I}_j}=\sum_{k\in\mathcal{I}_i\cup\mathcal{I}_j}n_k$. Hence we have a surjective map $\varphi_i:\mathscr{U}'_{\mathcal{I}_i\cup\mathcal{I}_j}\to\operatorname{Gr}_{\mathbb{H}}(n_{\mathcal{I}_i},m)$, which sends $(\mathcal{V}_k)_{k\in\mathcal{I}_i\cup\mathcal{I}_j}$ to $\mathcal{V}_{\mathcal{I}_i}$. By Theorem 1 there is a non-empty open set $\mathscr{U}_{\mathcal{I}_i}$ of $\operatorname{Gr}_{\mathbb{H}}(n_{\mathcal{I}_i},m)$ such that $\operatorname{hsp}(\mathcal{V},\{\tau_\alpha,\tau_\beta\})$ holds true for every $\mathcal{V}\in\mathscr{U}_{\mathcal{I}_i}$. Similarly, there is a non-empty open set $\mathscr{U}_{\mathcal{I}_j}$ of $\operatorname{Gr}_{\mathbb{H}}(n_{\mathcal{I}_j},m)$ such that $\operatorname{hsp}(\mathcal{V},\{\tau_\alpha,\tau_\beta\})$ holds true for every $\mathcal{V}\in\mathscr{U}_{\mathcal{I}_j}$. Now, intersect $\mathscr{U}_{\mathcal{I}_i\cup\mathcal{I}_j}$ with $f_i^{-1}(\mathscr{U}_{\mathcal{I}_i})\cap f_j^{-1}(\mathscr{U}_{\mathcal{I}_j})\cap\mathscr{U}''_{\mathcal{I}_i\cup\mathcal{I}_j}$ and call the result again $\mathscr{U}_{\mathcal{I}_i\cup\mathcal{I}_j}$, here $\mathscr{U}''_{\mathcal{I}_i\cup\mathcal{I}_j}$ is the open set where $\mathcal{V}_{\mathcal{I}_i},\mathcal{V}_{\mathcal{I}_j}$ do not intersect $\ker(\tau_\alpha),\ker(\tau_\beta)$.

We now show that $\mathscr{U}_{\mathcal{I}_i\cup\mathcal{I}_j}$ is the required $\mathscr{U}_{i,j,\alpha,\beta}$. Note that, by the definition of $\mathscr{U}_{\mathcal{I}_i\cup\mathcal{I}_j}$, we only need to consider the case $\tau_\alpha(v_i)=\tau_\beta(v_j)$ with $v_i\in\mathcal{V}_{\mathcal{I}_i}$ and $v_j\in\mathcal{V}_{\mathcal{I}_j}$. Write $v_j=v_{j\backslash i}+v_{i\cap j}$ where $v_{j\backslash i}\in\mathcal{V}_{\mathcal{I}_j\backslash\mathcal{I}_i}$ and $v_{i\cap j}\in\mathcal{V}_{\mathcal{I}_j\cap\mathcal{I}_i}$. We have $\tau_\beta(v_{j\backslash i})=\tau_\alpha(v_i)-\tau_\beta(v_{j\cap i})$. That is, $\tau_\beta(v_{j\backslash i})$ is in the intersection of $\tau_\beta(\mathcal{V}_{\mathcal{I}_j\backslash\mathcal{I}_i})$ with $\tau_\alpha(\mathcal{V}_{\mathcal{I}_i})+\tau_\beta(\mathcal{V}_{\mathcal{I}_i\cap\mathcal{I}_j})$. By what we have said above, $\tau_\beta(v_{j\backslash i})=0$. Thus $v_{j\backslash i}\in\ker(\tau_\beta)$ and by the definition of $\mathscr{U}_{\mathcal{I}_i\cup\mathcal{I}_j}$ we further have $v_{j\backslash i}=0$. Hence $v_j\in\mathcal{V}_{\mathcal{I}_i}$ and the equation $\tau_\alpha(v_i)=\tau_\beta(v_j)$ implies $v_i=v_j$ by the definition of $\mathscr{U}_{\mathcal{I}_i\cup\mathcal{I}_j}$. □

3.4. Proof of Theorem 3

We first rewrite (3) into the following convenient form.

$$\begin{aligned}\hat{\tau}&=\operatorname*{argmin}_{\tau\in\mathcal{T}}\min_{v\in\mathcal{V}}\|\overline{y}-\tau(v)\|_2\\&=\operatorname*{argmin}_{\tau\in\mathcal{T}}\min_{w\in\tau(\mathcal{V})}\|\overline{y}-w\|_2^2\\&=\operatorname*{argmin}_{\tau\in\mathcal{T}}\min_{w\in\tau(\mathcal{V})}\{\|w\|_2^2-\langle\overline{y},w\rangle-\langle w,\overline{y}\rangle\}\\&=\operatorname*{argmin}_{\tau\in\mathcal{T}}\min_{\lambda>0}\min_{w\in\tau(\mathcal{V}):\|w\|_2=\lambda}\{\lambda^2-\langle\overline{y},w\rangle-\langle w,\overline{y}\rangle\}\\&=\operatorname*{argmin}_{\tau\in\mathcal{T}}\min_{\lambda>0}\{\lambda^2-2\lambda\|\overline{y}\|_2\max_{w\in\tau(\mathcal{V}):\|w\|_2=\lambda}\frac{\langle\overline{y},w\rangle+\langle w,\overline{y}\rangle}{2\|\overline{y}\|_2\|w\|_2}\}\\&=\operatorname*{argmin}_{\tau\in\mathcal{T}}\min_{\lambda>0}\{\lambda^2-2\lambda\|\overline{y}\|_2\cos(\overline{y},\tau(\mathcal{V}))\}\\&=\operatorname*{argmax}_{\tau\in\mathcal{T}}\cos(\overline{y},\tau(\mathcal{V})).\end{aligned}$$

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

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

which surely holds, if the following stronger condition

$$\frac{\langle \overline{y}, y\rangle + \langle y, \overline{y}\rangle}{2\|\overline{y}\|_2\|y\|_2} > \cos(\overline{y}, \tau_2(\mathcal{V})) \tag{10}$$

is satisfied. Letting $w_2 \in \tau_2(\mathcal{V})$ with $\|w_2\|_2 = 1$ be such that $(\langle \overline{y}, w_2\rangle + \langle w_2, \overline{y}\rangle)/\|\overline{y}\|_2 = \cos(\overline{y}, \tau_2(\mathcal{V}))$ and recalling that $\overline{y} = y + \epsilon$, condition (10) is equivalent to

$$\begin{aligned}\frac{\langle \overline{y}, y\rangle + \langle y, \overline{y}\rangle}{\|\overline{y}\|_2\|y\|_2} > \frac{\langle \overline{y}, w_2\rangle + \langle w_2, \overline{y}\rangle}{\|\overline{y}\|_2} &\Leftrightarrow \frac{\langle \overline{y}, y\rangle + \langle y, \overline{y}\rangle}{\|y\|_2^2} > \frac{\langle \overline{y}, w_2\rangle + \langle w_2, \overline{y}\rangle}{\|y\|_2} \\ &\Leftrightarrow 2 > \frac{\langle y, w_2\rangle + \langle w_2, y\rangle}{\|y\|_2} + \frac{\langle \epsilon, w_2\rangle + \langle w_2, \epsilon\rangle}{\|y\|_2} - \frac{\langle \epsilon, y\rangle + \langle y, \epsilon\rangle}{\|y\|_2^2}. \\ &\Leftarrow 2 > 2\cos(y, \tau_2(\mathcal{V})) + \frac{2\|\epsilon\|_2}{\|y\|_2} + \frac{2\|\epsilon\|_2}{\|y\|_2} \\ &\Leftrightarrow \|y\|_2(1 - \cos(y, \tau_2(\mathcal{V}))) > 2\|\epsilon\|_2\end{aligned}$$

which is already fulfilled by (4). 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 (3), we have

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

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

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

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

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

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

3.5. Proof of Proposition 3

With $S_1, S_2 \in \mathcal{S}_{r,m}$, it was proved in [2] that there is always a projection P onto the column space of S_2 such that $\dim(\mathcal{U}_{PT_1,T_2}) \leq m - \lfloor r/2 \rfloor$. Since $\dim(\mathcal{U}_{S_1,S_2}) \leq \dim(\mathcal{U}_{PS_1,S_2})$, we have $\dim(\mathcal{U}_{S_1,S_2}) \leq m - r$ which proves i), ii) and with a small modification iv). For iii) it is easy to see that $\mathcal{U}_{B_1,B_2} = \varnothing$.

3.6. Proof of Corollary 1

Part i) is a special case of ii) and we prove the latter. By Theorem 1 and Proposition 3 there is a non-empty open set $\mathscr{U}$ of $\operatorname{Gr}_{\mathbb{R}}(n, m)$ such that $\operatorname{hsp}(\mathcal{V}, \mathcal{S}_{r,m})$ holds true for every $\mathcal{V} \in \mathscr{U}$. Now let $\mathscr{V}$ be the non-empty open set of $\mathbb{R}^{m\times n}$ consisting of full-rank matrices. There is a surjective polynomial map $f : \mathscr{V} \to \operatorname{Gr}_{\mathbb{R}}(n, m)$, defined in the same way as the Plücker embedding, which sends $A \in \mathscr{V}$ to its column space $\mathrm{R}(A)$. Now $f^{-1}(\mathscr{U})$ is a non-empty open set of $\mathbb{R}^{m\times n}$ such that for every $A \in f^{-1}(\mathscr{U})$ we have $\operatorname{hsp}(\mathrm{R}(A), \mathcal{S}_{r,m})$. Since every $A \in f^{-1}(\mathscr{U})$ is of full column rank, we also have $\operatorname{hsp}(\mathbb{R}^n, A)$. Parts iii) and iv) follow from Propositions 2 and 3 in a similar fashion.

3.7. Proof of Corollary 2

We only prove ii), which implies i). Parts iii) and iv) follow similarly. With $r \geq 2k$, Proposition 3 gives $\dim(\mathcal{U}_{S,S'}) \leq m - k$ for any rank-r selections $S, S' \in \mathcal{S}_{r,m}$. Let $s = \binom{n}{k}$ and let $\mathscr{I} = (\mathcal{I}_1, \ldots, \mathcal{I}_s)$ be the set of all subsets of $[n]$ of cardinality k, say, ordered in the lexicographic order. Then Theorem 2 gives a non-empty open set $\mathscr{U}$ of $\prod_{j\in[n]} \operatorname{Gr}_{\mathbb{R}}(1, m)$, such that for any $\mathcal{A} = (\mathcal{V}_1, \ldots, \mathcal{V}_n) \in \mathscr{U}$, the property $\operatorname{hsp}(\overline{\mathcal{A}_{\mathscr{I}}}, \mathcal{S}_{r,m})$ holds true. Let $\mathscr{V}$ be the open set of $\mathbb{R}^{m\times n}$ on which for every $A \in \mathscr{V}$ and every $j \in [n]$ the j-th column of A is non-zero. We have a surjective map $f : \mathscr{V} \to \prod_{j\in[n]} \operatorname{Gr}_{\mathbb{R}}(1, m)$ which sends $A = [a_1 \cdots a_n]$ to the subspace arrangement $(\operatorname{Span}(a_1), \dots, \operatorname{Span}(a_n))$. Let $\mathscr{V}'$ be the set of $A \in \mathbb{R}^{m\times n}$ for which any $\min\{n, 2k\}$ distinct columns of A are linearly independent. Then $\mathscr{V}'' = f^{-1}(\mathscr{U}) \cap \mathscr{V}'$ is a non-empty open set of $\mathbb{R}^{m\times n}$.

We show that $\operatorname{hsp}(\overline{\mathcal{K}_{\mathscr{I}}}, \mathcal{S}_{r,m}A)$ holds true for every $A \in \mathscr{V}''$. Let us view A as the linear map $\tau_A : \mathbb{R}^n \to \mathbb{R}^m$ defined by $\tau_A(x) = Ax$. By the definition of $\mathscr{V}''$ we have 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 $Ax = Ax'$. But $A(x - x') = 0$ is a linear dependence relation involving at most $2k$ columns of A and thus again by the definition of $\mathscr{V}''$ we must have $x = x'$. □

4. Appendix

4.1. Proof of Lemma 1

We assume familiarity with basic topological considerations in algebraic geometry on the level of schemes, e.g. see [34]. We first treat the case $\mathbb{H} = \mathbb{C}$, where classical arguments suffice. By Chevalley's theorem [29] $\phi(\mathscr{U})$ is constructible, that is $\phi(\mathscr{U}) = \cup_\nu \mathscr{Y}_\nu \cap \mathscr{U}_\nu$ where the $\mathscr{Y}_\nu$'s are closed in $\operatorname{Gr}_{\mathbb{C}}(n, m)$, the $\mathscr{U}_\nu$'s are open in $\operatorname{Gr}_{\mathbb{C}}(n, m)$, and ν takes finitely many values. If $\phi(\mathscr{U})$ does not contain any non-empty open set, then necessarily it is contained in the proper closed subset $\mathscr{Y} = \cup_\nu \mathscr{Y}_\nu$. The complement of $\mathscr{Y}$ is a non-empty open subset of $\operatorname{Gr}_{\mathbb{C}}(n, m)$ which does not intersect $\phi(\mathscr{U})$, and thus its inverse image under ϕ is also a non-empty open subset of $\operatorname{F}_{\mathbb{C}}(n_0, n, m)$ not intersecting $\mathscr{U}$. This implies that $\operatorname{F}_{\mathbb{C}}(n_0, n, m)$ can be written as a union of two proper closed sets. This is a contradiction because $\operatorname{F}_{\mathbb{C}}(n_0, n, m)$ is irreducible.

Next, we treat the case $\mathbb{H} = \mathbb{R}$. Then the arguments in the previous paragraph apply without change providing we treat ϕ as a morphism of finite type of Noetherian schemes over $\mathbb{R}$; see [34, 35, 36]. Thus we write $\overline{\phi} : \overline{\operatorname{F}}_{\mathbb{R}}(n_0, n, m) \to \overline{\operatorname{Gr}}_{\mathbb{R}}(n, m)$, where the overline indicates the scheme structure. By the Jacobson property, the restriction of $\overline{\phi}$ on the k-valued points is just ϕ. The polynomials that define $\mathscr{U}$ also define a corresponding scheme $\overline{\mathscr{U}} \subset \overline{\operatorname{F}}_{\mathbb{R}}(n_0, n, m)$, and the above arguments applied to $\overline{\phi}$ show that $\overline{\phi}(\overline{\mathscr{U}})$ contains a non-empty open subscheme $\overline{\mathscr{V}}$ of $\overline{\operatorname{Gr}}_{\mathbb{R}}(n, m)$. Now $\overline{\operatorname{Gr}}_{\mathbb{R}}(n, m)$ is locally isomorphic to the affine space $\mathbb{A}^{n(m-n)} = \operatorname{Spec}(\mathbb{R}[Z])$, where Z is an $n \times (m - n)$ matrix of variables z_{ij} and $\mathbb{R}[Z]$ is the polynomial ring in the z_{ij}'s with coefficients over $\mathbb{R}$. So let $\overline{\mathscr{V}'}$ be an open subscheme of $\overline{\operatorname{Gr}}_{\mathbb{R}}(n, m)$ isomorphic to $\mathbb{A}^{n(m-n)}$. Then $\overline{\mathscr{V}''} = \overline{\mathscr{V}'} \cap \overline{\mathscr{V}}$ is also open in $\overline{\operatorname{Gr}}_{\mathbb{R}}(n, m)$ and in fact non-empty because $\overline{\operatorname{Gr}}_{\mathbb{R}}(n, m)$ is irreducible. Under the isomorphism $\overline{\mathscr{V}'} \cong \mathbb{A}^{n(m-n)}$ we view $\overline{\mathscr{V}''}$ as a non-empty open subscheme of $\mathbb{A}^{n(m-n)}$. Now $\overline{\mathcal{V}''}$ can be written as $\bigcup_p \operatorname{Spec}(k[Z])_p$, with $p \in k[Z]$ and $(k[Z])_p$ the localization of $k[Z]$ at the multiplicatively closed set $\{1, p, p^2, \dots\}$. Since $\overline{\mathscr{V}''}$ is non-empty, not all p's are zero. Hence there is some non-zero p for which $\overline{\mathscr{V}'''} = \operatorname{Spec}(k[Z])_p$ is a non-empty open subscheme of $\mathbb{A}^{n(m-n)}$. Let $\mathscr{U}'$ be the open set of points in $\mathbb{R}^{n(m-n)}$ which are not roots of p. Since $\mathbb{R}$ is infinite, $\mathscr{U}'$ is non-empty. Finally, $\mathscr{U}'$ lies in the image of ϕ. □

4.2. Proof of Lemma 3

We assume familiarity with basic dimension theory in commutative algebra and algebraic geometry, for example see [34] and [36] respectively. Let $\mathfrak{R} := \mathbb{C}[w_1, \dots, w_m]$ be a polynomial ring associated with $\mathbb{C}^m$ and let J and I be the vanishing ideals of $\mathcal{Z}$ and $\mathcal{Y}$, respectively. Since $\mathcal{Z} \neq \{0\}$ we have that J is properly contained in the ideal $(w_1, \dots, w_m)$ generated by the w_i's. Let $\mathcal{U} = \mathcal{Y} \backslash \mathcal{Z}$. Then the vanishing ideal of the closure $\mathcal{U}^{\mathrm{cl}}$ of $\mathcal{U}$ is $\mathfrak{a} := I : J^\infty$, where $\mathfrak{a}$ is the saturation of I with respect to J. Hence we have $\dim(\mathfrak{R}/\mathfrak{a}) = \dim(\mathcal{U}^{\mathrm{cl}}) = \dim(\mathcal{U}) > m - n$. Since I, J are homogeneous so is $\mathfrak{a}$. Then for $m - n$ generic linear forms $\ell_1, \dots, \ell_{m-n}$ of $\mathfrak{R}$ we have

$$\dim(\mathfrak{R}/\mathfrak{a} + (\ell_1, \dots, \ell_{m-n})) = \dim(\mathfrak{R}/\mathfrak{a}) - (m - n) > 0. \tag{11}$$

Geometrically, this means that the generic linear subspace $\mathcal{V}$ defined as the common vanishing locus of the linear forms $\ell_1, \dots, \ell_{m-n}$ intersects $\mathcal{U}^{\mathrm{cl}}$ at positive dimension, that is $\mathcal{V} \cap \mathcal{U}^{\mathrm{cl}} \supsetneq \{0\}$. If $\mathcal{U} = \mathcal{U}^{\mathrm{cl}}$ we are done, so assume that $\mathcal{X} := \mathcal{U}^{\mathrm{cl}} \backslash \mathcal{U}$ is not empty. Since $\mathcal{U}$ is open in $\mathcal{Y}$, we have that $\mathcal{X}$ is closed in $\mathcal{U}^{\mathrm{cl}}$. Suppose that $\dim(\mathcal{X}) = \dim(\mathcal{U}^{\mathrm{cl}})$. Let $\mathcal{X}'$ be a maximal irreducible closed subset in $\mathcal{X}$. Then necessarily $\mathcal{X}'$ is an irreducible component of $\mathcal{U}^{\mathrm{cl}}$. But $\mathcal{X}' \cap \mathcal{U} = \varnothing$, which contradicts the fact that $\mathcal{U}^{\mathrm{cl}}$ is the smallest closed set that contain $\mathcal{U}$. We conclude that $\dim(\mathcal{X}) < \dim(\mathcal{U}^{\mathrm{cl}})$. With $\mathfrak{b}$ the vanishing ideal of $\mathcal{X}$, we have $\dim(\mathfrak{R}/\mathfrak{a}) > \dim(\mathfrak{R}/\mathfrak{b})$. Let us show that $\mathfrak{b}$ is homogeneous. For any $z \in \mathcal{X} \subset \mathcal{U}^{\mathrm{cl}} \subset \mathcal{Y}$, we have $\lambda z \in \mathcal{U}^{\mathrm{cl}}$ for any $\lambda \in \mathbb{C}$. Assume for the sake of contradiction that $\lambda' z \in \mathcal{U}$ for some $\lambda' \in \mathbb{C}$. Note that λ' can not be zero because $0 \in \mathcal{Z}$. But $z \notin \mathcal{U}$ implies $z \in \mathcal{Z}$ and so $\lambda' z \in \mathcal{Z}$, a contradiction. Taking again quotient by $m-n$ generic linear forms we have

$$\dim(\mathfrak{R}/\mathfrak{b} + (\ell_1, \dots, \ell_{m-n})) = \max\{\dim(\mathfrak{R}/\mathfrak{b}) - (m-n), 0\}. \tag{12}$$

Combining (11), (12) with $\dim(\mathfrak{R}/\mathfrak{a}) > \dim(\mathfrak{R}/\mathfrak{b})$ we get

$$\dim(\mathfrak{R}/\mathfrak{a} + (\ell_1, \dots, \ell_{m-n})) > \dim(\mathfrak{R}/\mathfrak{b} + (\ell_1, \dots, \ell_{m-n})).$$

This implies $\dim(\mathcal{U}^{\mathrm{cl}} \cap \mathcal{V}) > \dim(\mathcal{X} \cap \mathcal{V})$ for a generic $\mathcal{V} \in \mathrm{Gr}_{\mathbb{C}}(n, m)$. Thus $\mathcal{V}$ necessarily intersects $\mathcal{U}$. ☐

Acknowledgments

This work was funded by ShanghaiTech start-up grant 2017F0203-000-16. The authors thank Boshi Wang for useful discussions.

References

[1] M. C. Tsakiris, Eigenspace conditions for homomorphic sensing, arXiv:1812.07966v1, 2018.

[2] M. C. Tsakiris, Determinantal conditions for homomorphic sensing, arXiv:1812.07966v6, 2020.

[3] M. C. Tsakiris, L. Peng, Homomorphic sensing, International Conference on Machine Learning, 2019.

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

[5] M. Akçakaya, V. Tarokh, New conditions for sparse phase retrieval, arXiv:1310.1351v2, 2013.

[6] Y. Wang, Z. Xu, Phase retrieval for sparse signals, Applied and Computational Harmonic Analysis 37 (3) (2014) 531 – 544.

[7] J. Unnikrishnan, S. Haghighatshoar, M. Vetterli, Unlabeled sensing: Solving a linear system with unordered measurements, Annual Allerton Conference on Communication, Control, and Computing, 2015.

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

[9] D. Han, F. Lv, W. Sun, Recovery of signals from unordered partial frame coefficients, Applied and Computational Harmonic Analysis 44 (1) (2018) 38 – 58.

[10] F. Lv, W. Sun, Real phase retrieval from unordered partial frame coefficients, Advances in Computational Mathematics 44 (3) (2018) 879–896.

[11] P. Grohs, S. Koppensteiner, M. Rathmair, Phase retrieval: uniqueness and stability, SIAM Review 62 (2) (2020) 301–350.

[12] S. Balakrishnan, M. J. Wainwright, B. Yu, Statistical guarantees for the em algorithm: from population to sample-based analysis, Annals of Statistics 45 (1) (2017) 77–120.

[13] 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.

[14] 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.

[15] I. P. Fellegi, A. B. Sunter, A theory for record linkage, J. Am. Stat. Assoc. 64 (328) (1969) 1183–1210.

[16] M. H. DeGroot, P. K. Goel, Estimation of the correlation coefficient from a broken random sample, Annals of Statistics 8 (2) (1980) 264–278.

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

[18] D. Hsu, K. Shi, X. Sun, Linear regression without correspondence, Advances in Neural Information Processing Systems 30, 2017.

[19] 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.

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

[21] M. Slawski, G. Diao, E. Ben-David, A pseudo-likelihood approach to linear regression with partially shuffled data, arXiv:1910.01623, 2019.

[22] M. Slawski, M. Rahmani, P. Li, A sparse representation-based approach to linear regression with partially shuffled labels, The Conference on Uncertainty in Artificial Intelligence, 2019.

[23] M. Slawski, E. Ben-David, P. Li, Two-stage approach to multivariate linear regression with sparsely mismatched data, Journal of Machine Learning Research 21 (204) (2020) 1–42.

[24] I. Dokmanic, Permutations unlabeled beyond sampling unknown, IEEE Signal Processing Letters 26 (6) (2019) 823–827.

[25] H. Zhang, M. Slawski, P. Li, Permutation recovery from multiple measurement vectors in unlabeled sensing, arXiv:1909.02496, 2019.

[26] 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 66 (8) (2020) 5130–5144.

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

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

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

[30] D. Cox, J. Little, D. OShea, Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra, Springer Science & Business Media, 2013.

[31] K.-T. Wong, The eigenvalue problem $\lambda tx + sx$, Journal of Differential Equations 16 (2) (1974) 270 – 280.

[32] T. Berger, A. Ilchmann, S. Trenn, The quasi-weierstraß form for regular matrix pencils, Linear Algebra and its Applications 436 (10) (2012) 4052 – 4069, special Issue dedicated to Heinrich Voss's 65th birthday.

[33] T. Berger, S. Trenn, The quasi-kronecker form for matrix pencils, SIAM Journal on Matrix Analysis and Applications 33 (2) (2012) 336–368.

[34] R. Vakil, The Rising Sea: Foundations of Algebraic Geometry, 2017.

[35] R. Hartshorne, Algebraic Geometry, Vol. 52, Springer Science & Business Media, 1977.

[36] D. Eisenbud, Commutative Algebra with a View toward Algebraic Geometry, Springer, 1995.