PROJECTIONS AND PHASE RETRIEVAL

DAN EDIDIN

Abstract. We characterize collections of orthogonal projections for which it is possible to reconstruct a vector from the magnitudes of the corresponding projections. As a result we are able to show that in an \( M \)-dimensional real vector space a vector can be reconstructed from the magnitudes of its projections onto a generic collection of \( N \geq 2M - 1 \) subspaces. We also show that this bound is sharp when \( N = 2^k + 1 \). The results of this paper answer a number of questions raised in [4].

1. Introduction

The phase retrieval problem is an old one in mathematics and its applications. The author and his collaborators [1, 5] previously considered the problem of reconstructing a vector from the magnitudes of its frame coefficients. In this paper we answer questions raised in the paper [4] about phase retrieval from the magnitudes of orthogonal projections onto a collection of subspaces.

To state our result we introduce some notation. Given a collection of proper linear subspaces \( L_1, \ldots, L_N \) of \( \mathbb{R}^M \) we denote by \( P_1, \ldots, P_N \) the corresponding orthogonal projections onto the \( L_i \). Assuming that the linear span of the \( L_i \) is all of \( \mathbb{R}^M \) then any vector \( x \) can be recovered from vectors \( P_1x, \ldots, P_Nx \) since the linear map

\[
\mathbb{R}^M \to L_1 \times L_2 \times \cdots L_N, x \mapsto (P_1x, \ldots, P_Nx)
\]

is injective.

When the \( P_i \) are all rank 1 then a choice of generator for each line determines a frame and the inner products \( \langle P_i x, x \rangle \) are the frame coefficients with respect to this frame.

In this paper we consider the problem, originally raised in [4], of reconstructing a vector \( x \) (up to a global sign) from the magnitudes

\[
||P_1x||, ||P_2x||, \ldots, ||P_Nx||
\]

of the projection vectors \( P_1x, \ldots, P_Nx \).

Let \( \Phi = \{P_1, \ldots, P_N\} \) be a collection of projections of ranks \( k_1, \ldots, k_N \). Define a map \( \mathcal{A}_\Phi: (\mathbb{R}^M \setminus \{0\})/ \pm 1 \to \mathbb{R}_{\geq 0}^N \) by the formula

\[
x \mapsto (\langle P_1x, P_1x \rangle, \ldots, \langle P_Nx, P_Nx \rangle)
\]

As was the case for frames, phase retrieval by this collection of projections is equivalent to the map \( \mathcal{A}_\Phi \) being injective.

In [4], Cahill, Casazza, Peterson and Woodland proved that there exist collections of \( 2M - 1 \) projections which allow phase retrieval. They also proved that a collection \( \Phi = \{P_1, \ldots, P_N\} \) of projections admits phase retrieval if and only if for every orthonormal basis \( \{\phi_{i,d}\}_{d=1}^{k_d} \) of the linear subspace \( L_i \) determined by \( P_i \) the set of vectors \( \{\phi_{i,d}\}_{i=1}^{N_k} \) allows phase retrieval.

The author’s research was partially supported by a Simons Collaboration Grant.
Our first result is a more intrinsic characterization of collections of projections for which $A_{\Phi}$ is injective.

**Theorem 1.1.** The map $A_{\Phi}$ is injective if and only if for every non-zero $x \in \mathbb{R}^M$ the vectors $P_1x, \ldots, P_Nx$ span an $M$-dimensional subspace of $\mathbb{R}^N$, or equivalently the vectors $P_1x, \ldots, P_Nx$ form an $N$-element frame in $\mathbb{R}^M$.

As a corollary we obtain the following necessity result.

**Corollary 1.2.** If $N \leq 2M - 2$ and at least $M - 1$ of the $P_i$ have rank one, or if $N \leq 2M - 3$ and at least $M - 1$ of the $P_i$ have rank $M - 1$ then $A_{\Phi}$ is not injective.

**Remark 1.3.** We will see below that when the $P_i$ all have rank one the condition of the theorem is equivalent to the corresponding frame having the finite complement property of [1]

Using the characterization of Theorem 1.1 we show that when $N \geq 2M - 1$ any generic collection of projections admits phase retrieval. Note that this bound of $2M - 1$ is the same as that obtained in [1].

**Theorem 1.4.** If $N \geq 2M - 1$, then for a generic collection $\Phi = (P_1, \ldots, P_N)$ of ranks $k_1, \ldots, k_N$ with $1 \leq k_i \leq M - 1$, the map $A_{\Phi}$ is injective.

**Remark 1.5.** By generic we mean that $\Phi$ corresponds to a point in a non-empty Zariski open subset of a product of real Grassmannians (which has the natural structure as an affine variety) whose complement has strictly smaller dimension. As noted in [2] one consequence of the generic condition is that for any continuous probability distribution on this variety, $A_{\Phi}$ is injective with probability one. In particular Theorem 1.4 implies that phase retrieval can be done with $2M - 1$ random subspaces of $\mathbb{R}^M$. This answers Problems 5.2 and 5.6 of [4].

In [1] it was proved that $N \geq 2M - 1$ is a necessary condition for frames. However we obtain the following necessity result. This result was independently obtained by Zhiqiang Xu in his recent paper [10].

**Theorem 1.6.** If $M = 2^k + 1$ then $A_{\Phi}$ is not injective for any collection with $N \leq 2M - 2$ projections.

**Remark 1.7.** Xu also constructed an example of a collection of 6 projections in $\mathbb{R}^4$ which admit phase retrieval, which shows that the bound $N = 2M - 1$ is not in general sharp.

2. Background in algebraic geometry

In this section we give some brief background on some facts we will need from Algebraic Geometry. For a reference see [7] and [8, Chapter 1].

2.1. Real and complex varieties. Denote by $\mathbb{A}^n_{\mathbb{R}}$ (respectively $\mathbb{A}^n_{\mathbb{C}}$) the affine space of $n$-tuples of points in $\mathbb{R}$ (resp. $n$-tuples of points in $\mathbb{C}$). Given a collection of polynomials $f_1, \ldots, f_m \in \mathbb{C}[x_1, \ldots, x_n]$ let $V(f_1, \ldots, f_m)$ be the algebraic subset of $\mathbb{A}^n_{\mathbb{C}}$ defined by the simultaneous vanishing of the $f_i$. When the $f_i$ all have real coefficients then we denote by $V(f_1, \ldots, f_m)_{\mathbb{R}} \subset \mathbb{A}^n_{\mathbb{R}}$ the set of real points of the affine algebraic set $V(f_1, \ldots, f_m)$.

The relationship between the set of real and complex points of an algebraic set can be quite subtle. For example the algebraic subsets of $\mathbb{A}^2_{\mathbb{C}}$ defined by the equations $x^2 + y^2 = 0$
and $x^2 - y^2 = 0$ are isomorphic, since the complex linear transformation $(a, b) \mapsto (a, \sqrt{-1}b)$ maps one to the other. However, $V(x^2 + y^2)_\mathbb{R}$ consists of only the origin while $V(x^2 - y^2)_\mathbb{R}$ is the union of two lines.

Given an algebraic set $X = V(f_1, \ldots, f_m)$ we define the Zariski topology on $X$ by declaring closed sets to be the intersections of $X$ with other algebraic subsets of $\mathbb{A}^n_{\mathbb{C}}$. An algebraic set is irreducible if it is not the union of proper Zariski closed subsets. An irreducible algebraic set is called an algebraic variety. Every algebraic set has a decomposition into a finite union of irreducible algebraic subsets.

Note that the set of real points of an algebraic variety need not be irreducible. For example the affine curve $V(y^2 - x^3 + x)$ is irreducible, but $V(y^2 - x^3 + x)_\mathbb{R}$ is the disjoint union of two disconnected pieces.

Given a subset $X \subset \mathbb{A}^n_{\mathbb{C}}$ the ideal, $I(X)$, of $X$ is the set of all polynomials in $\mathbb{C}[x_1, \ldots, x_n]$ that vanish on $X$. Hilbert’s Nullstellensatz states that if $X = V(f_1, \ldots, f_n)$ then $I(X)$ is the radical of the ideal generated $f_1, \ldots, f_r$. A variety is irreducible if and only if $I(X)$ is a prime ideal. A key property of irreducible algebraic sets is that every non-empty Zariski open set is dense.

2.1.1. Homogeneous equations and projective algebraic sets. Denote by $\mathbb{P}^n_{\mathbb{R}}$ (resp. $\mathbb{P}^n_{\mathbb{C}}$) the real (resp. complex) projective space obtained from $\mathbb{R}^{n+1} \setminus \{0\}$ (resp. $\mathbb{C}^{n+1} \setminus \{0\}$) by identifying $(a_0, \ldots, a_n) \sim (\lambda a_0, \ldots, \lambda a_n)$ for any non-zero scalar $\lambda$.

Any collection of homogeneous polynomials $f_1, \ldots, f_m \subset \mathbb{C}[x_0, \ldots, x_n]$ defines a projective algebraic set $X = V(f_1, \ldots, f_r)$. When the polynomials $f_1, \ldots, f_r$ have real coefficients then we again let $V(f_1, \ldots, f_r)_\mathbb{R}$ denote the real points of $X$.

As in the affine case we can define the Zariski topology on a projective algebraic set $X$ by declaring the intersection of $X$ with another projective algebraic set to be closed. An irreducible projective algebraic set is called a projective variety. If $X \subset \mathbb{P}^n$ then we define $I(X)$ to be the ideal generated by all homogeneous polynomials vanishing on $X$. A projective algebraic set is irreducible if and only if $I(X)$ is a homogeneous prime ideal.

A subset of $\mathbb{P}^n$ is called quasi-projective if it is a Zariski open subset of a projective algebraic set. Since $\mathbb{A}^n_{\mathbb{C}}$ is the complement of the hyperplane $V(x_0) \subset \mathbb{P}^n$, any affine algebraic set is quasi-projective. Following [8], Section I.3] we will use the term variety to refer to any affine, quasi-affine (open in an affine), quasi-projective or projective variety.

2.1.2. Dimension of a complex variety. The dimension of an algebraic set is most naturally a local invariant. However, because varieties are irreducible, the local dimensions are constant. There are several equivalent definitions of the dimension of a variety $X$:

(i) (Krull dimension) The length of the longest descending chain of proper, irreducible Zariski closed subsets of $X$.

(i') If $X \subset \mathbb{A}^n$ is affine then (i) is equal to the length of the longest ascending chain of prime ideals in the coordinate ring, $\mathbb{C}[x_1, \ldots, x_n]/I(X)$ of $X$.

(ii) The transcendence dimension over $\mathbb{C}$ of the field of rational functions on $X$.
(iii) The dimension of the analytic tangent space to a general point of $X$. (This definition uses the fact that a complex variety contains a dense Zariski open complex submanifold.)

Since an arbitrary algebraic set $X$ can decomposed into a finite union of irreducible components we can define $\dim X$ to be the maximum dimension of its irreducible components.

In the proof of Theorem 1.4 we will make use of several facts in dimension theory.

**Theorem. (Krull’s Hauptidealsatz § Chapter I, Theorem 1.11A) Let $X \subset \mathbb{A}^n$ is an affine variety of dimension $d$. If $f \in \mathbb{C}[x_1, \ldots, x_n]$ is any polynomial, then $X \cap V(f)$ is either empty, all of $X$, or every irreducible component of $X \cap V(f)$ has dimension exactly $d - 1$.

**Theorem. (Semi-continuity of fiber dimension § Chapter I, Theorem 11.12) Let $f : X \to Y$ be a morphism of varieties. For any $p \in X$ let $\mu(p) = \dim f^{-1}(f(p))$. Then $\mu(p)$ is an upper-semicontinuous function in the Zariski topology on $X$ - that is, for any $m$ the locus of points $p \in X$ such that $\dim(f^{-1}(f(p))) \geq m$ is closed in $X$. Moreover, if $\mu$ is the minimum value of $\mu(p)$ then $\dim X = \dim f(X) + \mu$.

2.1.3. The dimension of the set of real points of a variety. If $X$ is a variety defined by real equations then we can also define the dimension of $X_\mathbb{R}$ as a subset of $\mathbb{A}^n_\mathbb{R} = \mathbb{R}^n$ (or $\mathbb{P}^n_\mathbb{R}$). When $X_\mathbb{R}$ is smooth we can take its dimension as a manifold. For general $X$, a result in real algebraic geometry [3] Theorem 2.3.6] states that any real semi-algebraic subset of $\mathbb{R}^n$ is homeomorphic as a semi-algebraic set to a finite disjoint union of hypercubes. Thus we can define $\dim_\mathbb{R} X_\mathbb{R}$ to be the maximal dimension of a hypercube in this decomposition.

Now if $X \subset \mathbb{A}^n_\mathbb{R}$ is a semi-algebraic set then [3] Corollary 2.8.9 implies that $\dim_\mathbb{R} X$ equals to the Krull dimension of the algebraic set $V(I(X))$. As a consequence we obtain the important fact that if $f_1, \ldots, f_m$ are real polynomials and $X = V(f_1, \ldots, f_m)$ then $\dim_\mathbb{R} X_\mathbb{R} \leq \dim X$ since $I(X_\mathbb{R}) \supset I(X)$.

**Example 2.1.** If $f = x^2 + y^2 \in \mathbb{R}[x, y]$ then $\dim V(f) = 1$ but $\dim V(f)_\mathbb{R} = 0$ since $V(f)_\mathbb{R} = \{(0,0)\}$. Note that in this case $I(V(f)_\mathbb{R})$ is the ideal $(x, y) \subset \mathbb{R}[x, y]$ and indeed $\dim V(x, y) = 0$ as predicted by [3] Corollary 2.8.9].

3. Proof of Theorem 1.1

To prove Theorem 1.1 we analyze the derivative of the map $A_\mathbb{R}$. Our argument is similar to an argument used by Murkherjee [9] to construct embeddings of complex projective spaces in Euclidean spaces. Recall that a map $f : X \to Y$ of differentiable manifolds is an immersion at $x \in M$ if the induced map of tangent spaces $df_x : T_x X \to T_{f(x)} Y$ is injective (so necessarily $\dim X \leq \dim Y$).

**Lemma 3.1.** Let $P : \mathbb{R}^M \to \mathbb{R}^M$ be a rank $k$ projection and let $f : \mathbb{R}^M \to \mathbb{R}$ be defined by $x \mapsto (P x, P x)$. For any $x \in \mathbb{R}^M$, $df_x(y) = 2(P x, y)$ where we identify $T_x \mathbb{R}^M = \mathbb{R}^M$ and $T_{f(x)} \mathbb{R} = \mathbb{R}$.

**Proof.** Since $P$ is a projection there is an orthonormal basis of eigenvectors for $P$. With respect to this basis $P = \text{diag}(1, \ldots, 1, 0, \ldots, 0)$ where there are $k$ ones and $M - k$ zeroes. If we choose coordinates determined by this basis then $f(x_1, \ldots, x_M) = x_1^2 + x_2^2 + \ldots + x_k^2$, so $\partial f / \partial x_i = 2 x_i$ if $i \leq k$ and $\partial f / \partial x_i = 0$ if $i > k$. Thus the derivative at a point $x = A_{\text{semi-algebraic subset of } \mathbb{R}^n}$ is one defined by polynomial equations and inequalities. In particular any real algebraic set is semi-algebraic.
(a_1, \ldots, a_M) \in \mathbb{R}^M is the linear operator that maps \( y = (b_1, \ldots, b_M) \) to \( 2 \sum_{i=1}^{k} a_i b_i = 2 \langle P x, y \rangle \)

**Proposition 3.2.** The map \( A_\Phi \) is an immersion at \( \Phi \in (\mathbb{R}^M \setminus \{0\}) / \pm 1 \) if and only if \( P_1 x, \ldots, P_N x \) span an \( M \)-dimensional subspace of \( \mathbb{R}^M \) where \( x \) is either lift of \( \Phi \) to \( \mathbb{R}^N \setminus \{0\} \).

**Proof.** Consider the map \( B_\Phi : \mathbb{R}^M \setminus \{0\} \to \mathbb{R}^N \), \( x \mapsto (\langle P_1 x, P_1 x \rangle, \ldots, \langle P_N x, P_N x \rangle) \). The map \( B_\Phi \) is the composition of the map \( A_\Phi \) with the double cover \( \mathbb{R}^M \setminus \{0\} \to (\mathbb{R}^M \setminus \{0\}) / \pm 1 \). Since the derivative of a covering map is an isomorphism, it suffices to prove the proposition for the map \( B_\Phi \). Applying Lemma 3.1 to each component of \( B_\Phi \) we see that \( dB_\Phi \) is the linear transformation \( y \mapsto 2(\langle P_1 x, y \rangle, \ldots, \langle P_N x, y \rangle) \). Hence \( (dB_\Phi)_x \) and thus \((dA_\Phi)_x \) is injective if and only if there is no non-zero vector \( y \) which is orthogonal to each \( P_i x \), or equivalently the vectors \( P_i x \) span all of \( \mathbb{R}^M \).

The proof of the theorem now follows from the following proposition.

**Proposition 3.3.** The map \( A_\Phi \) is injective if and only if it is a global immersion.

**Proof.** First assume that \( A_\Phi \) is not an immersion. By Proposition 3.2 there exists an \( x \neq 0 \) such that \( P_1 x, \ldots, P_N x \) fail to span \( \mathbb{R}^M \). Let \( y \) be a non-zero vector orthogonal to all the \( P_i x \) and consider the vectors \( x' = x + y \) and \( y' = x - y \).

Then

\[
|P_i x'|^2 = \langle P_i x', x' \rangle \quad \text{since } P_i \text{ is an orthogonal projection}
\]

\[
= \langle P_i x, x \rangle + \langle P_i y, y \rangle + \langle P_i y, x \rangle + \langle P_i x, y \rangle
\]

\[
= ||P_i x||^2 + ||P_i y||^2
\]

where the last equality holds because

\[
\langle P_i y, x \rangle = \langle P_i y, P_i x \rangle = \langle P_i x, P_i y \rangle = \langle P_i x, y \rangle = 0.
\]

Likewise \( ||P_i y'||^2 = ||P_i x||^2 + ||P_i y||^2 \). Hence, either \( A_\Phi \) is not injective or \( x' = \pm y' \).

However, if \( x' = \pm y' \) then either \( x = 0 \) or \( y = 0 \) which is not the case. Thus \( A_\Phi \) is not injective.

Conversely, suppose that \( A_\Phi \) is an immersion and suppose that there exist \( x \) and \( y \) such that \( ||P_i x|| = ||P_i y|| \) for all \( i \). We wish to show that \( x = \pm y \). Suppose that \( x \neq y \). Then \( x - y \neq 0 \). Thus the linear transformation \((dA_\Phi)_{x-y} : \mathbb{R}^M \to \mathbb{R}^N, z \mapsto (\langle P_i (x - y), z \rangle)_{i=1}^M \) is injective. On the other hand

\[
\langle P_i (x - y), x + y \rangle = \langle P_i x, x \rangle - \langle P_i y, y \rangle = ||P_i x||^2 - ||P_i y||^2 = 0.
\]

(Here we again use the fact that \( P_i \) is an orthogonal projection so \( \langle P_i x, x \rangle = \langle P_i x, P_i x \rangle \)). Hence \( x + y = 0 \), ie \( x = -y \).

3.1. **Proofs of the corollaries.**

**Proof of Corollary 3.4.** Suppose that \( P_1, \ldots, P_{M-1} \) have rank 1. Then there is a vector \( x \) such that \( P_i x = 0 \) for \( i = 1, \ldots, M-1 \), so \( P_1 x, \ldots, P_{M-1} x, \ldots, P_N x \) cannot span \( \mathbb{R}^M \) if \( N \leq 2M - 2 \). Likewise if \( P_1, \ldots, P_{M-1} \) have rank \( M - 1 \) then there exists a vector \( y \) such that \( P_i y = y \) for \( i = 1, \ldots, M - 1 \). In this case \( P_1 x, \ldots, P_N x \) fail to span \( \mathbb{R}^M \) if \( M \leq 2M - 3 \).

**Corollary 3.4** (Complement property). If \( P_1, \ldots, P_N \) all have rank 1 corresponding to lines \( L_1, \ldots, L_N \) then \( A_\Phi \) is injective if and only if for every partition of \( \{1, \ldots, N\} \) into two set \( S, S' \) one of the sets of lines \( \{L_i\}_{i \in S} \) or \( \{L_j\}_{j \in S'} \) spans \( \mathbb{R}^M \).
Proposition 4.1. There is an affine irreducible subvariety $\mathcal{P}_k(M) \subset \mathbb{A}^{M \times M}$ of complex dimension $k(M - k)$ whose real points are the set of orthogonal projections of rank $k$.

Remark 4.2. It is crucial for our proof that $\mathcal{P}_k(M)$ be irreducible since will need to know that any proper subvariety has strictly smaller dimension.
Proof. Let $\mathcal{P}_k(M)$ be the algebraic subset of $A^{M \times M}$ defined by the equations $P^2 = P$, $P = P^t$ and trace$(P) = k$. A real matrix satisfies these equations if and only it is an orthogonal projection. So $\mathcal{P}_k(M)_{\mathbb{R}}$ is the set of orthogonal projections.

We now show that $\mathcal{P}_k(M)$ is an irreducible variety of dimension $k(M-k)$.

Let $P$ be a matrix representing a point of $\mathcal{P}_k(M)$. Since $P^2 = P$ the eigenvalues of $P$ lie in the set $\{0, 1\}$ and $P$ is diagonalizable. Thus $P$ is a symmetric and diagonalizable matrix. Finally the condition that trace $P = k$ implies that $P$ is conjugate to the diagonal matrix $E_k = \text{diag}(1,1,\ldots,1,0,\ldots,0)$ where there are $k$ ones and $M-k$ zeros. Conversely, any matrix of the form $P = AE_kA^t$ with $A \in SO(M,\mathbb{C})$ satisfies $P^2 = P$, $P = P^t$ and trace $P = k$.

Thus $\mathcal{P}_k(M)$ can be identified with the $SO(M,\mathbb{C})$ orbit of the matrix $E_k$ under the conjugation. Since $SO(M,\mathbb{C})$ is an irreducible algebraic group, so is the orbit. Finally, the stabilizer of $E_k$ is isomorphic to the subgroup $SO(k) \times SO(M-k)$. The dimension of the algebraic group $SO(M,\mathbb{C})$ is $\binom{M}{2}$. Thus the dimension of $\mathcal{P}_k(M)$ is $\binom{M}{2} - \binom{k}{2} - \binom{M-k}{2} = k(M-k)$.

4.2. Completion of the Proof of theorem 1.1. Since the vectors $P_1x,\ldots,P_Nx$ fail to span $\mathbb{R}^M$ if an only if there is a non-zero vector $y$ which is orthogonal to each $P_ix$, a collection $\mathcal{A}_\Phi$ fails to be injective if and only there are non-zero vectors $x,y$ such that

$$y^tP_1x = y^tP_2x = \ldots = y^tP_Mx = 0.$$

Consider the incidence set of tuples $\{(P_1,\ldots,P_N,x,y)|y^tP_ix = 0\}$ where $P_i \in \mathcal{P}_{k_i}$ and $x,y \in \mathbb{C}^M \setminus \{0\}$. Since the equations $y^tP_ix = 0$ are homogeneous in $x$ and $y$ there is a corresponding incidence set

$$\mathcal{I} = \mathcal{I}_{k_1,\ldots,k_N,M} \subset \mathcal{P}_{k_1} \times \ldots \times \mathcal{P}_{k_N} \times \mathbb{P}^{N-1} \times \mathbb{P}^{N-1}.$$

The real points of the algebraic set $\mathcal{I}$ parametrize tuples of orthogonal projections and non-zero vectors $(P_1,\ldots,P_N,x,y)$ such that $P_ix$ is orthogonal to $y$ for each $i$. By Theorem 4.1 if $(P_1,\ldots,P_N,x,y) \in \mathcal{I}_\mathbb{R}$ then the map $\mathcal{A}_\Phi$ isn’t injective for the collection of projections $\Phi = (P_1,\ldots,P_N)$.

We will show that when $N \geq 2M - 1$ the variety $\mathcal{I}$ contains an open set of complex dimension less than that of $\mathcal{P}_{k_1} \times \ldots \times \mathcal{P}_{k_N}$, that contains all of the real points of $\mathcal{I}$. This means that $\mathcal{I}_\mathbb{R}$ has real dimension less than $\sum_{i=1}^{M} k_i(M-k_i)$. Hence for generic projections $P_1,\ldots,P_N$ there are no non-zero real vectors $x,y$ such that $\langle P_ix,y \rangle = 0$ for all $i$. In other words $\mathcal{A}_\Phi$ is injective for generic collections of projections $P_1,\ldots,P_N$ with $N \geq 2M - 1$.

**Proposition 4.3.** There is an open subset of $\mathcal{I}$ which contains $\mathcal{I}_\mathbb{R}$ and has dimension $\sum_{i=1}^{N} k_i(M-k_i) + 2M - 2 - N$. In particular if $N \geq 2M - 1$ this open set has dimension strictly smaller than $\dim \prod_{i=1}^{N} \mathcal{P}_{k_i}$.

**Remark 4.4.** Note that since we do not know that $\mathcal{I}$ is irreducible we are not asserting that $\mathcal{I}$ has dimension $\sum_{i=1}^{N} k_i(M-k_i) + 2M - 2 - N$. Instead, we are proving that the union of the irreducible components of $\mathcal{I}$ that contain all of the real points has this dimension.

---

2 Note that a complex symmetric matrix need not be diagonalizable. For example the matrix

$$\begin{pmatrix} 1 & i \\ i & -1 \end{pmatrix}$$

is non-diagonalizable.
Proof. We show that the image of the projection $p_2 : \mathcal{I} \to \mathbb{P}^{N-1} \times \mathbb{P}^{N-1}$ contains a dense open set $U \subset \mathbb{P}^{M-1} \times \mathbb{P}^{M-1}$ which contains $\mathbb{P}^{M-1} \times \mathbb{P}^{M-1}$ such that for each $x, y \in U$ the fiber $p_2^{-1}(x, y)$ is non-empty and has dimension $\sum_{i=1}^{N} (k_i(M - k_i) - 1)$. It follows that the incidence $\mathcal{I}$ contains an open set of dimension $\sum_{i=1}^{N} k_i(M - k_i) + 2M - 2 - N$ and that this open set contains $\mathcal{I}_{\mathbb{R}}$.

Observe that the fiber $p_2^{-1}(x, y)$ is the algebraic subset

$$\mathcal{I}_{x,y} \subset \prod_{i=1}^{N} \mathcal{P}_{k_i}$$

defined by the linear equations $y^tP_1 x = 0, \ldots, y^tP_N x = 0$. This algebraic subset is the product $\prod_{i=1}^{N} (I_{x,y})_i$ where $(I_{x,y})_i$ is the algebraic subset of $\mathcal{P}_{k_i}$ defined by the linear equation $y^tP_i x = 0$.

Lemma 4.5. For each $k$ with $1 \leq k \leq M - 1$ there is a dense open subset $U_k \subset \mathbb{P}^{M-1} \times \mathbb{P}^{M-1}$ containing $\mathbb{P}^{M-1} \times \mathbb{P}^{M-1}$ such that for $x, y \in U_k$ the algebraic subset $\mathcal{P}_{x,y}$ of $\mathcal{P}_k$ defined by the equation $y^tP x = 0$ has complex dimension $k(M - k) - 1$.

Let $U$ be the intersection of all of the $U_k$ in $\mathbb{P}^{M-1} \times \mathbb{P}^{M-1}$. By Lemma 4.5 the inverse image of $U$ under the projection $\mathcal{I} \to \mathbb{P}^{M-1} \times \mathbb{P}^{M-1}$ has dimension equal to $\sum_{i=1}^{N} k_i(M - k_i) + 2M - 2 - N$ and contains all of the real points. □

Proof of Lemma 4.5. The fiber $\mathcal{P}_{x,y}$ is defined by a single equation in the affine variety $\mathcal{P}_k$. Therefore, by Krull’s Hauptidealsatz $\mathcal{P}_{x,y}$ has dimension $k(M - k) - 1$ unless the equation $y^tP x$ vanishes identically on $\mathcal{P}_k$ or the equation $y^tP x$ does not vanish at all in which case $\mathcal{P}_{x,y}$ is empty.

We first show that if $x, y$ are non-zero vectors in $\mathbb{R}^M$ we can find $P, Q \in \mathcal{P}_k$ such that $y^tP x = 0$ and $y^tQ x \neq 0$. This implies that $\mathcal{P}_{x,y}$ is non-empty and not all of $\mathcal{P}_{x,y}$.

To find $P$ such that $y^tP x = 0$ observe that given any non-zero real vector $x$ we can find a linear subspace $L$ of dimension $k < M$ which is orthogonal to $x$. If $P_L$ is the orthogonal projection onto $L$ then $P_L x = 0$ and so $y^tP_L x = 0$ as well.

To find $Q$ such that $y^tQ x \neq 0$ requires more care. Since $x$ and $y$ are real vectors $\langle x, x \rangle \neq 0$ and $\langle y, y \rangle \neq 0$. Hence $\langle x + \lambda y, y \rangle$ and $\langle x + \lambda y, x \rangle$ are non-zero for all but finitely many values of $\lambda$. Choose $\lambda$ such that the above inner products are non-zero and let $L_1$ be the line spanned by $x + \lambda y$. Let $Q_{L_1}$ be the orthogonal projection onto this line. Then $Q_{L_1} x$ is non-zero and parallel to $x + \lambda y$ so $y^tQ_{L_1} x = \langle Q_{L_1} x, y \rangle \neq 0$ since we also chose $\lambda$ so that $x + \lambda y$ is not orthogonal to $y$.

Now let $L_{k-1}$ be any $(k - 1)$-dimensional linear subspace in the orthogonal complement of the linear subspace spanned by $x$ and $y$ and let $Q_{L_{k-1}}$ be the orthogonal projection onto this subspace. Then $Q = Q_{L_1} + Q_{L_{k-1}}$ is the desired projection.

By the theorem on the dimension of the fibers applied to the morphism

$$\mathcal{I}_k = \{(P, x, y)|y^tP x = 0\} \subset \mathcal{P}_k \times \mathbb{P}^{M-1} \times \mathbb{P}^{M-1} \to \mathbb{P}^{M-1} \times \mathbb{P}^{M-1}$$

then there is a dense open subset $U_k \subset \mathbb{P}^{M-1} \times \mathbb{P}^{M-1}$ where the dimension of the fiber is constant. Since the set of real points of $\mathbb{P}^{M-1} \times \mathbb{P}^{M-1}$ has maximal dimension it is dense, and therefore $U_k$ contains real points. On the other hand we showed that the dimension of $\mathcal{P}_{x,y}$ is constant for all real points $(x, y)$ of $\mathbb{P}^{M-1} \times \mathbb{P}^{M-1}$. Therefore $U_k$ contains $\mathbb{P}^{M-1} \times \mathbb{P}^{M-1}$. □
5. The case of fewer measurements

Here we prove that if $M = 2^k + 1$ and $N \leq 2M - 2$ then for any collection of projections $P_1, \ldots, P_N$ the map $\mathcal{A}_\phi$ is not injective. Since we can always add projections to a collection we may assume that $N = 2M - 2$.

By Theorem 1.1, the map $\mathcal{A}_\phi$ is not injective if and only there is a pair $(x, y) \in \mathbb{P}^{M-1}_\mathbb{R} \times \mathbb{P}^{M-1}_\mathbb{R}$ such that $y^t P_i x = 0$ for all $i$. The equation $y^t P_i x = 0$ is bihomegenous of degree 1 in $x$ and $y$, so we can consider the subvariety $Z \subset \mathbb{P}^{M-1}_\mathbb{R} \times \mathbb{P}^{M-1}_\mathbb{R}$ defined by the vanishing of the $2M - 2$ bilinear forms $\{y^T P_i x\}_{i=1}^{2M-2}$. We wish to show that if $M = 2^k + 1$ then $Z$ has a real point.

Lemma 5.1. If $Z$ has a non-empty intersection with diagonal in $\mathbb{P}^{M-1}_\mathbb{R} \times \mathbb{P}^{M-1}_\mathbb{R}$ then $\mathcal{A}_\phi$ is not injective.

Remark 5.2. Note that Lemma 5.1 holds whether or not $M = 2^k + 1$.

Proof of Lemma 5.1. Let $(z, z)$ be a point of $Z$ on the diagonal. Write $z = x + \sqrt{-1} y$ so the condition $z^t P_i z = 0$ implies that $x^t P_i x - y^t P_i y = 0$ and $y^t P_i x = 0$ for all $i$. If $x$ and $y$ are both non-zero then $(x, y)$ is a real point of $Z$. If $x$ or $y$ is 0 then $z$ is either real or pure imaginary. In this case, either $z$ is a real vector or $\sqrt{-1} z$ is a real vector so $(z, z)$ also represents a real point of product $\mathbb{P}^{M-1}_\mathbb{R} \times \mathbb{P}^{M-1}_\mathbb{R}$. □

Now suppose that $Z$ has no real points. Then by Lemma 5.1 $Z$ misses the diagonal. Since the equations $x^t P_i y = 0$ are symmetric in $x$ and $y$, we see that $(x, y) \in Z$ if and only if $(y, x) \in Z$ and $(x, y) \neq (y, x)$. Also if $(x, y) \in Z$ is not real then the complex conjugate $(\overline{x}, \overline{y})$ is also a distinct point of $Z$. It follows that the degree of the intersection cycle supported on the variety $Z \subset \mathbb{P}^{N-1}_\mathbb{R} \times \mathbb{P}^{N-1}_\mathbb{R}$ must be divisible by 4. On the other hand by [6, Examples 13.2, 13.3] the degree of the intersection cycle supported on $Z$ is $\binom{2M-2}{M-1}$. When $M = 2^k + 1$, Legendre’s formula [5, cf. Proof of Lemma 5.3] for the highest power of a prime dividing a factorial shows that $\binom{2M-2}{M-1}$ is not divisible by 4.

Remark 5.3. If the $P_i$ all have rank one then the bilinear equation $y^t P_i x = 0$ factors as a product $\langle y, v_i \rangle \langle x, v_i \rangle = 0$ where $v_i$ is a unit norm vector generating the line determined by $v_i$. Since the system of linear equations

$\langle y, v_i \rangle = \ldots = \langle y, v_{M-1} \rangle = \langle x, v_M \rangle = \ldots \langle x, v_{2M-2} \rangle = 0$

has a non-trivial real solution, we obtain another proof that the bound $N = 2M - 1$ is sharp for rank one projections.

Acknowledgements. The author is grateful to Pete Casazza for suggesting that he look at the paper [4].

References

[1] Radu Balan, Pete Casazza, and Dan Edidin. On signal reconstruction without phase. Appl. Comput. Harmon. Anal., 20(3):345–356, 2006.
[2] Afonso S. Bandeira, Jameson Cahill, Dustin G. Mixon, and Aaron A. Nelson. Saving phase: injectivity and stability for phase retrieval. Appl. Comput. Harmon. Anal., 37(1):106–125, 2014.
[3] Jacek Bochnak, Michel Coste, and Marie-Françoise Roy. Real algebraic geometry, volume 36 of Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]. Springer-Verlag, Berlin, 1998. Translated from the 1987 French original, Revised by the authors.
[4] J. Cahill, P. Casazza, J. Peterson, and L. Woodland. Phase retrieval by projections. arXiv:1305.6226, 2013.

[5] Aldo Conca, Dan Edidin, Milena Hering, and Cynthia Vinzant. An algebraic characterization of injectivity in phase retrieval. Appl. Comput. Harmon. Anal., 38(2):346–356, 2015.

[6] William Fulton. Intersection theory. Springer-Verlag, Berlin, 1984.

[7] Joe Harris. Algebraic geometry, volume 133 of Graduate Texts in Mathematics. Springer-Verlag, New York, 1992. A first course, Corrected reprint of the 1992 original.

[8] Robin Hartshorne. Algebraic geometry. Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[9] Amiya Mukherjee. Embedding complex projective spaces in Euclidean space. Bull. London Math. Soc., 13(4):323–324, 1981.

[10] Z. Xu. The minimal measurement number for low-rank matrices recovery. arxiv:150507204, May 2015.

Dan Edidin (edidind@missouri.edu)
Department of Mathematics,
University of Missouri,
Columbia, Missouri 65211 USA