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 [5].

1. Introduction

The phase retrieval problem is an old one in mathematics and its applications. The author
and his collaborators [2, 6] 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
[5] 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 sub-
spaces $L_1, \ldots, L_N$ 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
$$\mathbb{R}^M \rightarrow L_1 \times L_2 \times \ldots L_N, x \mapsto (P_1x, \ldots, P_Nx)$$
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 [5], 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 $A_\Phi : (\mathbb{R}^M \setminus \{0\})/\pm 1 \rightarrow \mathbb{R}_{\geq 0}^N$ by the formula
$$x \mapsto (\langle P_1x, P_1x \rangle, \ldots, \langle P_Nx, P_Nx \rangle)$$
As was the case for frames, injectivity of the map $A_\Phi$ implies that phase retrieval by this
collection of projections is theoretically possible.

In [5], Cahill, Casazza, Peterson and Woodland proved that there exist collections of
$2M - 1$ projections of rank more than one 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 $\{\phi_{i,d}\}_{d=1}^{k_i}$ of the linear subspace $L_i$ determined by $P_i$ the set of
vectors $\{\phi_{i,d}\}_{i=1,d=1}^{N,k_d}$ 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 $\mathbb{R}^M$, 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 [2].

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 [2].

**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$^1$ of a product of real Grassmannians (which has the natural structure as an affine variety) whose complement has strictly smaller dimension. As noted in [3] 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 [5]. We refer the reader to the paper of Bachoc and Ehler [1] for results on the feasibility of phase retrieval using collections of random linear projections.

In [2] 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 [12].

**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 [8, 11] and [9, Chapter 1].

---

$^1$See Section 2 for the definition of the Zariski topology.
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 the intersections of $X$ with other algebraic subsets of $\mathbb{A}^n_{\mathbb{C}}$. An algebraic set is irreducible if and only if $I$ (resp. complex) projective space obtained from the radical of the ideal generated by $f_1, \ldots, f_m$. The dimension of an algebraic set is most naturally a local invariant. However, because varieties are irreducible, the local dimensions are constant.

### 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 $X$.

(ii) 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 [9, 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.** (Theorem on dimension of fibers) [11, Section 6.3, Theorem 7], [9, Chapter II, Exercise 3.22b] Let $f: X \to Y$ be a morphism of varieties such that $f(X)$ is dense in $Y$. If $n = \dim X$ and $m = \dim Y$ then $m \leq n$ and for every $y \in f(X)$ each irreducible component of the fiber $f^{-1}(y)$ has dimension at least $n - m$.

**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 $\dim X_R$ to be the maximum dimension of its irreducible components. When $X$ is smooth we can take its dimension as a manifold. For general $X$, a result in real algebraic geometry [4, Theorem 2.3.6] states that any real semi-algebraic subset of $\mathbb{R}^n$ is homeomorphic to a semi-algebraic set to a finite disjoint union of hypercubes. Thus we can define $\dim X_R$ to be the maximal dimension of a hypercube in this decomposition.

Now if $X \subset \mathbb{A}^n_R$ is a semi-algebraic set then [4, Corollary 2.8.9] implies that $\dim_R X$ 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 $\dim X_R \leq \dim X$ since $I(X_R) \supset I(X)$.

**Example 2.1.** If $f = x^2 + y^2 \in \mathbb{R}[x, y]$ then $\dim V(f) = 1$ but $\dim V(f)_R = 0$ since $V(f)_R = \{(0, 0)\}$. Note that in this case $I(V(f)_R)$ is the ideal $(x, y) \subset \mathbb{R}[x, y]$ and indeed $\dim V(x, y) = 0$ as predicted by [4, Corollary 2.8.9].

**3. Proof of Theorem 1.1**

To prove Theorem 1.1 we analyze the derivative of the map $\mathcal{A}_\phi$. Our argument is similar to an argument used by Murkerjee [10] to construct embeddings of complex projective spaces in Euclidean spaces. Recall that a map $f: X \to Y$ of differentiable manifolds is an

---

2A semi-algebraic subset of $\mathbb{R}^n$ is one defined by polynomial equations and inequalities. In particular any real algebraic set is semi-algebraic.
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 \( x \mapsto \langle P x, P x \rangle \). For any \( x \in \mathbb{R}^M \), \( df_x(y) = 2 \langle P x, y \rangle \) 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 \( \partial f / \partial x_i = 2x_i \) if \( i \leq k \) and \( \partial f / \partial x_i = 0 \) if \( i > k \). Thus the derivative at a point \( x = (a_1, \ldots, a_M) \in \mathbb{R}^M \) is the linear operator that maps \( y = (b_1, \ldots, b_M) \) to \( 2 \sum_{i=1}^k a_i b_i = 2 \langle P x, y \rangle \). \( \square \)

**Proposition 3.2.** The map \( A_\Phi \) is an immersion at \( \varpi \in (\mathbb{R}^M \setminus \{0\}) / \pm 1 \) 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 \( \varpi \) 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 \( A_\Phi \) 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 \( \mathbb{R}^M \). \( \square \)

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 \( (dA_\Phi)_x : \mathbb{R}^M \to \mathbb{R}^N, z \mapsto (\langle P_i(x - y), z \rangle)_{i=1}^M \) 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 \( x = -y \). \( \square \)
3.1. Proofs of the corollaries.

Proof of Corollary 1.2. Suppose that $P_1, \ldots, P_{M-1}$ have rank 1. Then there is a vector $x$ such that $P_ix = 0$ for $i = 1, \ldots, M-1$, so $P_1x, \ldots, P_{M-1}x, \ldots, P_Nx$ 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 $P_iy = y$ for $i = 1, \ldots, M-1$. In this case $P_1x, \ldots, P_Nx$ fail to span $\mathbb{R}^M$ if $M \leq 2M-3$. \[ \blacksquare \]

Corollary 3.4 (Complement property [2]). If $P_1, \ldots, P_N$ all have rank 1 corresponding to lines $L_1, \ldots, L_N$ then $\mathcal{A}_\phi$ 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 $\mathbb{R}^M$.

Proof. Suppose $S \bigcup S'$ is a partition of $\{1, \ldots, N\}$ such that neither subset of lines $\{L_i\}_{i \in S}$ or $\{L_i\}_{i \in S'}$ spans. Let $x$ be a vector orthogonal to the lines $\{L_i\}_{i \in S}$. Thus the span of the vectors $P_ix$ is contained in the span of the lines $\{L_j\}_{j \in S'}$ which by assumption do not span $\mathbb{R}^M$.

Conversely, suppose that for some vector $P_1x, \ldots, P_Nx$ fail to span $\mathbb{R}^M$. Let $S = \{i | P_ix = 0\}$ and let $S' = \{j | P_jx \neq 0\}$. Since the vectors $\{P_jx\}_{j \in S'}$ are parallel to the lines $\{L_j\}_{j \in S'}$ we see that these vectors cannot span $\mathbb{R}^M$. On the other hand the non-zero vector $x$ is orthogonal to each line in the collection $\{L_i\}_{i \in S}$ so these vectors cannot span either. \[ \blacksquare \]

3.2. An example. We revisit [5, Example 5.3] in the context of Theorem 1.1. Let $\{\phi_i\}_{i=1}^3$ and $\{\psi_i\}_{i=1}^3$ be orthonormal bases for $\mathbb{R}^3$ such that $\{\phi_i\} \cup \{\psi_i\}$ is full spark (meaning that any 3 element subset spans). Since $M = 2+1$ at least 5 projections are required for phase retrieval by Theorem 1.6. Cahill, Casazza, Peterson and Woodland consider two collections of subspaces.

$$
\begin{align*}
W_1 &= \text{span}\{\phi_1, \phi_3\} & W_1^\perp &= \text{span}\{\phi_2\} \\
W_2 &= \text{span}\{\phi_2, \phi_3\} & W_2^\perp &= \text{span}\{\phi_1\} \\
W_3 &= \text{span}\{\phi_3\} & W_3^\perp &= \text{span}\{\phi_1, \phi_2\} \\
W_4 &= \text{span}\{\psi_1\} & W_4^\perp &= \text{span}\{\psi_2, \psi_3\} \\
W_5 &= \text{span}\{\psi_2\} & W_5^\perp &= \text{span}\{\psi_1, \psi_3\}
\end{align*}
$$

and showed the collection of orthogonal projections onto $\{W_i\}_{i=1}^5$ admits phase retrieval while the collection of orthogonal projections onto $\{W_i^\perp\}_{i=1}^5$ does not.

Using Theorem 1.1 it is easy to see that the orthogonal projections corresponding to $\{W_i^\perp\}$ do not admit phase retrieval since the vector $\phi_3$ is orthogonal to $W_1^\perp, W_2^\perp, W_3^\perp$. Thus, the images of the vector $\phi_3$ under the 5 projections cannot span $\mathbb{R}^3$.

Now consider the other collection of orthogonal projections onto $W_1, \ldots, W_5$ which we denote by $P_1, \ldots, P_5$. Since $\{\phi_1, \phi_2, \phi_3, \psi_1, \psi_2, \psi_3\}$ is full spark the vectors $\{\phi_3, \psi_1, \psi_2\}$ span. Thus if $x \in \mathbb{R}^3$ is not orthogonal to any of $\phi_3, \psi_1, \psi_2$ then $P_3x, P_4x, P_5x$ span. If $x$ is orthogonal to $\phi_3$ then it lies in the plane spanned by $\phi_1$ and $\phi_2$ and is also not orthogonal to one of $\psi_1$ or $\psi_2$, say $\psi_1$. If $P_3x = 0$ then $x$ is orthogonal to $\psi_2$ which means that it cannot be orthogonal to either of $\phi_1$ or $\phi_2$ for otherwise $\psi_2$ would have to be parallel to one of the $\psi_i$. It would then follow that the vectors $P_1x, P_2x, P_4x$ span. If $P_5x \neq 0$ then either $P_1x, P_4x, P_5x$ or $P_2x, P_3x, P_5x$ span. If $P_3x \neq 0$ then $P_1x, P_2x, P_3x$ span if $x$ isn’t orthogonal to either $\phi_1$ or $\phi_2$. If $x$ is orthogonal to both $\phi_1, \phi_2$ then $P_3x, P_4x, P_5x$ span.
4. Proof of Theorem 1.4

Our proof is similar to previous proofs of generic sufficiency bounds for frames [2, 6] where an incidence variety is considered. However, the proof here is more intricate because the natural complex variety parametrizing orthogonal projections is affine rather than projective.

4.1. An affine variety whose real points are the space of orthogonal projections.

The set of orthogonal projections of rank \(k\) in \(\mathbb{R}^M\) can be identified with the Grassmann manifold of \(k\) dimensional linear subspaces of \(\mathbb{R}^M\). This manifold has (real) dimension \(k(M - k)\) [4, Section 3.4.2].

Proposition 4.1. There is an affine 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. Since we show that the complex dimension of \(\mathcal{P}_k(M)\) is \(k(M - k)\) our proposition implies that \(\mathcal{P}_k(M)_{\mathbb{R}}\) has the maximal dimension which we is needed in the proof of Theorem 1.4. It is also crucial for our proof that \(\mathcal{P}_k(M)\) be irreducible since we will need to know that any proper subvariety has strictly smaller dimension.

Proof. Let \(\mathcal{P}_k(M)\) be the algebraic subset of \(\mathbb{A}^{M \times M}\) defined by the equations \(P^2 = P, P = P^t\) and \(\text{trace}(P) = k\). 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 the algebraic set \(\mathcal{P}_k(M)\) is irreducible 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\(^3\) matrix. Thus it is conjugate by an element of the complex orthogonal group \(SO(M, \mathbb{C})\) to a diagonal matrix. Finally the condition that \(\text{trace}(P) = k\) 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 \(P^t = P\), \(P^2 = P\) and \(\text{trace}(P) = k\).

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 \(\binom{M}{2} - \binom{k}{2} - \binom{M - k}{2} = k(M - k)\). \(\square\)

4.2. Completion of the Proof of theorem 1.4. 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 \(P_i \in \mathcal{P}(M)_{k_i}\) 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

\[\mathcal{I} = \mathcal{I}_{k_1, \ldots, k_N}(M) \subset \mathcal{P}_{k_1}(M) \times \ldots \times \mathcal{P}_{k_N}(M) \times \mathbb{P}^{M-1} \times \mathbb{P}^{M-1}.\]

\(^3\)Note that a complex symmetric matrix need not be diagonalizable. For example the matrix

\[
\begin{pmatrix}
1 & i \\
-1 & -i
\end{pmatrix}
\]

is non-diagonalizable.
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 1.1 if $(P_1, \ldots, P_N, x, y) \in \mathcal{I}_\mathbb{R}$ then the map $A_\Phi$ isn’t injective for the collection of projections $\Phi = (P_1, \ldots, P_N)$.

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

**Lemma 4.3.** For each point $(x, y) \in \mathbb{P}_\mathbb{R}^{M-1} \times \mathbb{P}_\mathbb{R}^{M-1}$ then every irreducible component of the algebraic subset $\mathcal{P}_{k,x,y}$ of $\mathcal{P}_k(M)$ defined by the equation $y^tPx = 0$ has complex dimension $k(M-k) - 1$.

**Proof of Lemma 4.3.** The fiber $\mathcal{P}_{x,y}$ is defined by a single equation in the affine variety $\mathcal{P}_k(M)$. Therefore, by Krull’s Hauptidealsatz every irreducible component of $\mathcal{P}_{k,x,y}$ has dimension $k(M-k) - 1$ unless the equation $y^tPx$ vanishes identically on $\mathcal{P}_k$ or the equation $y^tPx$ does not vanish at all in which case $\mathcal{P}_{x,y}$ is empty.

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

To find $P$ such that $y^tPx = 0$ 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 $P_Lx = 0$ and so $y^tP_Lx = 0$ as well.

To find $Q$ such that $y^tQx \neq 0$ requires more care. Since $x$ and $y$ are real vectors $(x, x) \neq 0$ and $(y, y) \neq 0$. Hence $(x + \lambda y, y)$ and $(x + \lambda y, x)$ 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 $y^tQ_{L_1}x = (Q_{L_1}x, y) \neq 0$ 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. \hfill $\square$

We now conclude the proof of Theorem 1.4.

Consider the projection $p_2: \mathcal{I} \to \mathbb{P}_\mathbb{R}^{N-1} \times \mathbb{P}_\mathbb{R}^{N-1}$ onto the last two factors. For each point $(x, y) \in \mathbb{P}_\mathbb{R}^{M-1} \times \mathbb{P}_\mathbb{R}^{M-1}$ the fiber $p_2^{-1}(x, y)$ is the product $\prod_{i=1}^N \mathcal{P}_{k_i,x,y}$. By Lemma 4.3 every irreducible component of this product has dimension $\sum_{i=1}^N (k_i(M-k_i) - 1)$ when $(x, y) \in \mathbb{P}_\mathbb{R}^{M-1} \times \mathbb{P}_\mathbb{R}^{M-1}$.

Let $\mathcal{J}$ be an irreducible component of $\mathcal{I}$ that contains a real point. Since $p_2(\mathcal{I}_\mathbb{R}) \subset \mathbb{P}_\mathbb{R}^{M-1} \times \mathbb{P}_\mathbb{R}^{M-1}$ we see that $p_2(\mathcal{J})$ necessarily contains a point of $\mathbb{P}_\mathbb{R}^{M-1} \times \mathbb{P}_\mathbb{R}^{M-1}$. Since the image of an irreducible set is irreducible, the closure of $p_2(\mathcal{J})$ in $\mathbb{P}_\mathbb{R}^{M-1} \times \mathbb{P}_\mathbb{R}^{M-1}$ is a subvariety. In particular $\dim p_2(\mathcal{J}) \leq 2M - 2$. By construction $p_2(\mathcal{J})$ has a real point, so there is a point where the fiber of the map $\mathcal{J} \to p_2(\mathcal{J})$ has dimension $\sum_{i=1}^N (k_i(M-k_i) - 1)$. Applying the theorem
on dimension of the fibers to the map of $\mathcal{J} \to \overline{p_2(\mathcal{J})}$ we conclude\textsuperscript{4} that $\dim \mathcal{J} \leq 2M - 2 + \sum_{i=1}^{N} (k_i(M - k_i) - 1)$. Therefore, when $N > 2M - 2$, $\dim \mathcal{J} < \dim \mathcal{P}_{k_1}(M) \times \ldots \times \mathcal{P}_{k_N}(M)$.

Remark 4.4. Note that since we do not know that $\mathcal{I}$ is irreducible we are not asserting that $\mathcal{I}$ has dimension less than or equal to $\sum_{i=1}^{N} k_i(M - k_i) + 2M - 2 - N$. Instead, we have proved this bound for the union of the irreducible components of $\mathcal{I}$ that contain real points.

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 bihomogenous of degree 1 in $x$ and $y$ e, 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 the 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 $\mathbb{P}^{M-1}_\mathbb{R} \times \mathbb{P}^{M-1}_\mathbb{R}$. \hfill $\square$

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 $Z \subset \mathbb{P}^{N-1} \times \mathbb{P}^{N-1}$ must be divisible by 4. On the other hand by [7, Examples 13.2, 13.3] the degree of the intersection cycle supported on $Z$ is $(2M-2)_{M-1}$. When $M = 2^k + 1$, Legendre’s formula [6, cf. Proof of Lemma 5.3] for the highest power of a prime dividing a factorial shows that $(2M-2)_{M-1}$ 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 $P_i$. Since the system of linear equations

\[ \langle y, v_1 \rangle = \ldots = \langle y, v_{M-1} \rangle = \langle x, v_M \rangle = \ldots = \langle x, v_{2M-2} \rangle = 0 \]

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

\textsuperscript{4}The image of an algebraic set need not be algebraic. Thus, the irreducible set $p_2(\mathcal{J}) \subset \mathbb{P}^{M-1}_\mathbb{R} \times \mathbb{P}^{M-1}_\mathbb{R}$ need not be algebraic. To apply the theorem on dimension of fibers we replace $p_2(\mathcal{J})$ with its closure in the Zariski topology which is an irreducible algebraic set. Although the map of varieties $\mathcal{J} \to \overline{p_2(\mathcal{J})}$ need not be surjective, it does have dense image which allows us to apply the theorem.
**Acknowledgements.** The author is grateful to Pete Casazza for suggesting that he look at the paper [5]. The author is also grateful to the referee for helpful comments and suggestions.

**References**


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