3-24-2016

Generalized Phase Retrieval: Isometries in Vector Spaces

Josiah Park

Generalized Phase Retrieval: Isometries in Vector Spaces

by

Josiah Park

A thesis submitted in partial fulfillment
of the requirements for the degree of
Master of Arts
Department of Mathematics & Statistics
College of Arts and Sciences
University of South Florida

Major Professor: Boris Shekhtman, Ph.D.
Mohamed Elhamdadi, Ph.D.
Razvan Teodorescu, Ph.D.

Date of Approval:
March 24, 2016

Keywords: Phase Retrieval, Isometry, Lie Group, Inverse Problem, Algebraic Variety

Acknowledgments

The contents of this thesis were inspired by discussion held with members of the IMA summer graduate program hosted at the University of Maryland in College Park. My thesis advisor, Boris Shekhtman, provided also the encouraging atmosphere from which many of the ideas presented here were fostered.

Table of Contents

Abstract

In this thesis we generalize the problem of phase retrieval of vector to that of multi-vector. The identification of the multi-vector is done up to some special classes of isometries in the space. We give some upper and lower estimates on the minimal number of multi-linear operators needed for the retrieval. The results are preliminary and far from sharp.

Chapter 1

Injectivity Results related to phase retrieval

Consider the following problem: Suppose one is given the magnitude of the coefficients of some vector $x \in \mathbb{R}^2$ against some frame of vectors from $\mathbb{R}^2$, $\Phi = \{\varphi_n\}_{n=1}^N$. That is, one is given measurements, $\{|\langle x, \varphi_n \rangle|^2\}_{n=1}^N$. Can x be recovered from these measurements? In other words is the mapping sending x to the magnitude squared of its coefficients against some frame injective?

Since replacing x with $-x$ in $\{|\langle x, \varphi_n \rangle|^2\}_{n=1}^N$ does not change the measurements, the answer to the second question can be answered "No". However, rewording the question and generalizing the problem to one about the injectivity of the mapping $\mathcal{A} :\mathbb{R}^M/\{\pm 1\} \to \mathbb{R}^N$, $x \mapsto \{|\langle\, x, \varphi_n \rangle|^2\}_{n=1}^N$ changes the answer to "Yes." Qualifying, the answer is yes if Φ is chosen carefully.

Let $x, y \in \mathbb{R}^2$ be given, $x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$, $y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ and $\Phi = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$ where φ_n are taken to be the column vectors of Φ.

Then the conditions $\{|\langle x, \varphi_n \rangle|^2\}_{n=1}^3 = \{|\langle y, \varphi_n \rangle|^2\}_{n=1}^3$ give the following:

$$\begin{aligned} x_1^2 = y_1^2 \qquad &\Rightarrow x_1 = \pm y_1 \\ x_2^2 = y_2^2 \qquad &\Rightarrow x_2 = \pm y_2 \\ (x_1 + x_2)^2 = (y_1 + y_2)^2 &\Rightarrow x_1 x_2 = y_1 y_2 \end{aligned}$$

Together these conditions imply $x = \pm y$ and so Φ gives injective measurements and x may be recovered from the magnitude of its coefficients against Φ up to a multiple of a unit-modular constant in $\mathbb{R}$.

In what follows let now $x_k, y_k \in \mathbb{C}$, $x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$, $y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$, and $\Phi = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$ as before. Then corresponding to the question presented above, we may ask for complex valued vectors: Is the mapping $\mathcal{B} :\mathbb{C}^M/\mathbb{T} \to \mathbb{R}^N$, $y \mapsto \{|\langle\, y, \varphi_n \rangle|^2\}_{n=1}^N$ injective? In this case one may check that $x = \begin{pmatrix} 1 \\ i \end{pmatrix}$ and $y = \begin{pmatrix} -1 \\ i \end{pmatrix}$ satisfy $\{|\langle x, \varphi_n \rangle|^2\}_{n=1}^3 = \{|\langle y, \varphi_n \rangle|^2\}_{n=1}^3$ as $\mathcal{B}(x) = (1, 1, 2)$ and

$\mathcal{B}(y) = (1,1,2)$ however $x \neq cy$ for $c \in \mathbb{T} = \{z \in \mathbb{C} \mid |z| = 1\}$. Hence we conclude $\mathcal{B}$ is not injective. However, if $\Phi = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & i \end{pmatrix}$, for example, then x is recoverable from the magnitude of its coefficients against Φ up to a multiple of a unit-modular constant in $\mathbb{C}$ (see [3] for a proof).

The problem of characterizing Φ for which the mappings $\mathcal{A}$ and $\mathcal{B}$ are injective is a problem related to phase retrieval. In [2], Balan, Casazza, and Edidin asked the following question, interested in its theoretical implications for phase retrieval, a method by which intensity measurements $\{|\langle y, \varphi_n \rangle|^2\}_{n=1}^N$ may be used to recover signal y up to a unit-modular constant. (For details on how y may be recovered from these measurements, see the work of Candès, Strohmer, Voroninski, [6]).

What is the minimal size, N, of a frame $\Phi = \{\varphi_n\}_{n=1}^N$ for which the mapping $\mathcal{A}$ or $\mathcal{B}$ is injective? How does one choose $\{\varphi_n\}$ so that Φ gives *injective measurements*, that is, so that the corresponding mapping $\mathcal{A}$ or $\mathcal{B}$ is injective?

Balan et al in [2], gave an upper bound in the complex case for N, $N \leq 4M - 2$, non-constructively using methods in algebraic geometry, proving that generically, $4M - 2$ vectors suffice for the corresponding mapping $\mathcal{B}$ to be injective. The term generic is algebraic and in this context means the frames for which corresponding mapping $\mathcal{B}$ is injective, forms a Zariski-open set, that is, they form the complement of a proper algebraic variety in $\mathbb{C}^{MN}$. In addition, for the real case, $x \in \mathbb{R}^N$, the authors of [2] solved the problem in full, giving $N = 2M - 1$. Their argument for this case is presented in Chapter 2.

Previous work by Heinosaari, Mazzarella, Wolf in [9], used results in differential geometry to give lower bounds for N, $N \geq 4M - \alpha(M-1) - 3$ (see [9] for exact results), where $\alpha(M)$ is the number of one's in the binary representation of M.

Together the results in [2] and [9] gave an asymptotic expression $N = 4M + o(n)$. Influenced by the authors' of [2] work, successive researchers Bandeira, Cahill, Mixon, and Nelson in [3] suggesed a precise value of N, $N = 4M - 4$, this suggestion being coined the "$4M - 4$ conjecture". In [3], the authors verified the conjecture in the cases $M = 2, 3$ and argued via heuristics that in general $N = 4M - 4$.

One part of the conjecture was later confirmed by Conca, Edidin, and Vinzant in [7], again using methods in algebraic geometry. Generically, frames of vectors Φ of size $|\Phi| = N = 4M - 4$ suffice for $\mathcal{B}$ to be injective. (An explicit construction of such frames of size $N = 4M - 4$ is presented in a paper of Bodmann and Hammen, [4].) The authors of [7] showed that for M of the form $M = 2^n + 1$ the $4M - 4$ conjecture holds, that is they showed for such M that any frame of smaller size does not give injective measurements.

Recently, Vinzant gave the first bit of evidence against the $4M - 4$ conjecture. In [14], a frame of 11 vectors in $\mathbb{C}^4$ (presented here for convenience):

$$\Phi^T = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 9i & -5-7i & -6-7i \\ 1 & 1-i & -5-2i & -1-8i \\ 1 & -2+4i & -4-2i & 3+8i \\ 1 & -3+i & 1-8i & 7-6i \\ 1 & 3-3i & -8+7i & -6-2i \\ 1 & -3+5i & 5+6i & 2i \\ 1 & -3+8i & 5-5i & -6-4i \end{pmatrix}$$

was verified to give $\mathcal{B}$ injective, using computational methods in algebraic geometry, thereby renewing interest in calculating explicit values of N.

Chapter 2

Phase Retrieval: Real and Complex

The following examples coming from injectivity results in phase retrieval provide motivation for the problem which this thesis introduces (see Chapter 3).

First we develop notation. In the following it will be useful to introduce the following term, used in [2] the characterize injectivity of the mapping $\mathcal{A}$. A frame $\Phi = \{\varphi_n\}_{n=1}^N$ of real or complex vectors, $\varphi_n \in \mathbb{R}^M$ or $\mathbb{C}^M$, is said to have the *complement property* if for any $P \subset [N] = 1, 2, ..., N$ either $\{\varphi_n\}_{n\in P}$ or $\{\varphi_n\}_{n\in P^C}$ forms a spanning set for $\mathbb{R}^M$ or $\mathbb{C}^M$ respectively. Recall that the problem of determining N in the real case, concerns conditions on $\Phi = \{\varphi_n\}_{n=1}^N$ which guarantee the injectivity of the mapping $\mathcal{A}$:$\mathbb{R}^M/\{\pm 1\}\rightarrow \mathbb{R}^N$, given by:

$$\mathcal{A}(x) = \{|\langle\, x, \varphi_n\rangle|^2\}_{n=1}^N$$

Using the terms and notation developed we introduce the following result from [2], presented here for convenience.

PROPOSITION 1 $\mathcal{A}$ is injective if and only if Φ has the complement property.

Proof. ($\Rightarrow$) Suppose there is a set $P \subset [N]$ for which neither $\{\varphi_n\}_{n\in P}$ nor $\{\varphi_n\}_{n\in P^C}$ spans $\mathbb{R}^M$. Then there exists $u \neq 0 \in \{\varphi_n\}_{n\in P}^{\perp}$ and $v \neq 0 \in \{\varphi_n\}_{n\in P^C}^{\perp}$. Consider the two vectors $u + v, u - v \in \mathbb{R}^M$. Note that $|\langle\, u + v, \varphi_n\rangle|^2 = |\langle\, v, \varphi_n\rangle|^2$ and $|\langle\, u - v, \varphi_n\rangle|^2 = |\langle\, v, \varphi_n\rangle|^2$ for $n \in P$. When the corresponding measurements are considered for $n \in P^C$ combined with the preceding remark, one has $\mathcal{A}(u+v) = \mathcal{A}(u-v)$. However $u+v \neq \pm(u-v)$ for otherwise $u = 0$ or $v = 0$, contrary to assumption.

($\Leftarrow$) Suppose $\mathcal{A}(u) = \mathcal{A}(v)$ for $u \neq \pm v$, that is $|\langle\, u, \varphi_n\rangle|^2 = |\langle\, v, \varphi_n\rangle|^2$ for $n = 1, ..., N$. Since $u, v,$ and, φ_n are real valued, $\langle\, u, \varphi_n\rangle = \pm\langle\, v, \varphi_n\rangle$. Let P be the set of n for which equality holds. Consider then vectors $u+v, u-v \neq 0$. $|\langle\, u-v, \varphi_n\rangle|^2 = 0$ for $n \in P$ while $|\langle\, u+v, \varphi_n\rangle|^2 = 0$ for $n \in P^C$. Hence neither $\{\varphi_n\}_{n\in P}$ nor $\{\varphi_n\}_{n\in P^C}$ spans $\mathbb{R}^M$. So Φ does not have the complement property. $\square$

Proposition 1 gives then that if Φ is taken to consist of $N = 2M - 1$ vectors that are *full spark*, that is so that every sub-collection of M vectors is linearly independent, the corresponding map $\mathcal{A}$ is injective. Since any frame of smaller size cannot have the complement property, we have:

COROLLARY 2.0.1 *In the real case,* $N(M) = 2M - 1$*.*

As an aside, full spark frames are abundant. A Vandermonde construction of such frames is given by taking the first M rows of the Vandermonde matrix, for $M < N$. Such a Vandermonde matrix is given as follows:

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_N \\ x_1^2 & x_2^2 & \cdots & x_N^2 \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{N-1} & x_2^{N-1} & \cdots & x_N^{N-1} \end{pmatrix}$$

Full spark frames are well documented, see the paper [1].

The following examples serve to introduce the problem considered in this thesis through its relation to real and complex phase retrieval.

2.0.1 The Real Case: Example 1

Let $u = (u_1, ..., u_M)$ and $v = (v_1, ..., v_M) \in \mathbb{R}^M$ and to each member of Φ, split it into M functions, $\varphi_n = \varphi_{n,k}, k = 1, ..., M$ thereby creating linear functions $\varphi_{n,k} : \mathbb{R} \to \mathbb{R}$ by which one may rewrite

$$\mathcal{A}(u) = \{|\langle u, \varphi_n\rangle|^2\}_{n=1}^N = \{|\sum_{k=1}^M \varphi_{n,k}(u_k)|^2\}_{n=1}^N$$

So that $\mathcal{A}(u) = \mathcal{A}(v)$ if and only if

$$|\sum_{k=1}^M \varphi_{n,k} u_k|^2 = |\sum_{k=1}^M \varphi_{n,k} v_k|^2 \text{ for all } n = 1, ..., N.$$

If Φ is taken to be full spark and of size $|\Phi| = 2M - 1$, $\mathcal{A}(u) = \mathcal{A}(v) \implies u = \pm v$. That is, every v_k is the image of u_k under either the identity mapping T_1 or isometry $T_2 : \mathbb{R} \to \mathbb{R}$, $T_2(x) = -x$. Of course, if $Tu_k = v_k$, for all $k = 1, ..., M$, then $\mathcal{A}(u) = \mathcal{A}(v)$ for,

$$|\sum_{k=1}^{M}\varphi_{n,k}v_k|^2 = |\sum_{k=1}^{M}\varphi_{n,k}T_2u_k|^2 = |\sum_{k=1}^{M}\varphi_{n,k}(-u_k)|^2 = |-\sum_{k=1}^{M}\varphi_{n,k}u_k|^2$$

$$|-\sum_{k=1}^{M}\varphi_{n,k}u_k|^2 = |T_2(\sum_{k=1}^{M}\varphi_{n,k}u_k)|^2 = |\sum_{k=1}^{M}\varphi_{n,k}u_k|^2$$

So if Φ is chosen to be of size $N = 2M - 1$ and full spark, we have for $u, v \in \mathbb{R}^M$ if

$$|\sum_{k=1}^{M}\varphi_{n,k}u_k|^2 = |\sum_{k=1}^{M}\varphi_{n,k}v_k|^2 \text{ for all } n = 1, ..., N$$

then there exists isometry $T = T_1$ or T_2, commuting with each $\varphi_{n,k}$, for which $Tu_k = v_k$ for $k = 1, ..., M$. Further, the preceding proposition gives that this is the smallest sized collection of linear functions $\{\varphi_{n,k}\}_{n=1,k=1}^{N,M}$ with this property.

The next example focuses on the complex case once more.

2.0.2 The Complex Case: Example 2

Consider $u = (u_1, ..., u_M), v = (v_1, ..., v_M) \in \mathbb{C}^M$. Each of u and v, $u_k = a_k + ib_k, v_k = c_k + id_k$ where $a_k, b_k, c_k, d_k \in \mathbb{R}$ are in correspondence with members of $\mathbb{R}^2$, (a_k, b_k), and (c_k, d_k) respectively. This correspondence gives way to a representation of $\varphi_{n,k} = x_{n,k} + iy_{n,k}$ as linear operators $A_{n,k} : \mathbb{R}^2 \to \mathbb{R}^2$ where

$$A_{n,k}(u) = \begin{pmatrix} x_{n,k} & y_{n,k} \\ -y_{n,k} & x_{n,k} \end{pmatrix} \begin{pmatrix} a_k \\ b_k \end{pmatrix} = \begin{pmatrix} x_{n,k}a_k - y_{n,k}b_k \\ x_{n,k}b_k + y_{n,k}a_k \end{pmatrix}$$

So $A_{n,k}(u)$ is computed by carrying out the matrix multiplication presented above.

Note that $\varphi_{n,k}$, by representation by $A_{n,k}$, may be viewed as isometries (rotations) $A_{n,k} : \mathbb{R}^2 \to \mathbb{R}^2$. Then, mapping $\mathcal{B} : \mathbb{C}^M/\mathbb{T} \to \mathbb{R}^N$ is given alternatively as:

$$\mathcal{B}(u) = \{|\langle u, \varphi_n\rangle|^2\}_{n=1}^N = \{||\sum_{k=1}^{M} A_{n,k}u_k||^2\}_{n=1}^N$$

So for generic $\Phi \subset \mathbb{C}^M$, of size $N = 4M - 4$, by [7], if

$$\{||\sum_{k=1}^{M} A_{n,k}u_k||^2\}_{n=1}^N = \{||\sum_{k=1}^{M} A_{n,k}v_k||^2\}_{n=1}^N \text{ for } n = 1, ..., N$$

then there exists a rotation (isometry) T, necessarily commuting with all $A_{n,k}$, (as T and $A_{n,k}$ are rotations $\mathbb{R}^2 \to \mathbb{R}^2$) for which $Tu_k = v_k$ for $k = 1, ..., M$.

2.0.3 Introduction of Parameter $S(M,N)$

Again, we develop terminology for what follows. Let $\mathscr{A} = \{(A_{1,1},...,A_{1,M}),...,(A_{S,1},...,A_{S,M})\}$ be an ensemble of linear operators $A_{n,k} : \mathbb{R}^N \to \mathbb{R}^N$. For u and $v \in (\mathbb{R}^N)^M$, if

$$||\sum_{k=1}^{M} A_{n,k}u_k||^2 = ||\sum_{k=1}^{M} A_{n,k}v_k||^2 \text{ for } n = 1,...,N$$

then u and v will be said to be $\mathscr{A}$-equivalent, denoted by $u \simeq_{\mathscr{A}} v$. Lastly, isometry $T : \mathbb{R}^N \to \mathbb{R}^N$ is $\mathscr{A}$-admissable if T commutes with all members of $\mathscr{A}$.

The previous example suggests the following question as a generalization of the one considered by the authors in [2].

What is the smallest sized ensemble $\mathscr{A} = \{(A_{1,1},...,A_{1,M}),...,(A_{S,1},...,A_{S,M})\}$, $|\mathscr{A}| = S$, of linear operators, such that for any pair of tuples $u, v \in (\mathbb{R}^N)^M$

$$||\sum_{k=1}^{M} A_{n,k}u_k||^2 = ||\sum_{k=1}^{M} A_{n,k}v_k||^2 \text{ for all } n = 1,...,N$$

implies u and v belong to the same orbit of some $\mathscr{A}$-admissable isometry, T, that is $Tu_k = v_k$ for all $k = 1,...,M$ for some $\mathscr{A}$-admissable isometry T?

For M,N given, let $S(M,N)$ denote the size of such $\mathscr{A}$. Then Example 1 of Section 2.2 demonstrates the following result:

PROPOSITION 2 $S(M,1) = 2M - 1$

While Example 2 yields:

PROPOSITION 3 $S(M,2) \leq 4M - 4$

Results in phase retrieval in the complex case give upper bounds for $S(M,2)$, however the restriction of phase retrieval to linear operators that are rotations only, allows for $S(M,2)$ to be less than $N(M)$ theoretically. This is in fact confirmed by results given in the following section.

2.0.4 $S(2,2)$ Example

Let $x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$, $y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$, $\varphi_n = \begin{pmatrix} \varphi_{n_1} \\ \varphi_{n_2} \end{pmatrix}$. where $x, y, \varphi_n \in \mathbb{C}^2$. Then $N(2) = 4(2) - 4 = 4$, and there exists $\varphi_1, \varphi_2, \varphi_3, \varphi_4$ such that if

$$(*)\ \ |\langle x,\varphi_n\rangle|^2 = |x_1\overline{\varphi_{n_1}} + x_2\overline{\varphi_{n_2}}|^2 = |y_1\overline{\varphi_{n_1}} + y_2\overline{\varphi_{n_2}}|^2 = |\langle y,\varphi_n\rangle|^2$$

for $n = 1, ..., 4$, then $x = cy$ for some $c \in \mathbb{T} = \{z \in \mathbb{C} \ | \ |z| = 1\}$.

For instance taking φ_n for $n = 1, ..., 4$ to be the columns of the matrix $\Phi = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & i \end{pmatrix}$ then φ_n will have the property given in (*).

Instead of members of $\mathbb{C}^2$, we take x, y to now be members of $(\mathbb{R}^2)^2$. A family $\mathscr{A}$ with less than 3-tuples of linear operators cannot give injective measurements with respect to equivalence class members. That is, there does not exist $\mathscr{A} = \{(A_{1,1}, A_{1,2}), (A_{2,1}, A_{2,2})\}$ such that the conditions:

$$||A_{1,1}x_1 + A_{1,2}x_2||^2 = ||A_{1,1}y_1 + A_{1,2}y_2||^2$$
$$||A_{2,1}x_1 + A_{2,2}x_2||^2 = ||A_{2,1}y_1 + A_{2,2}y_2||^2$$

guarantee that there is an isometry T, commuting with all $A_{j,k}$, such that $Tx_k = y_k$ for $k = 1, 2$.

However there is a 3-tuple of linear operators distinguishing two tuples of vectors from $\mathbb{R}^2$. Take $\mathscr{A} = \{(I, 0), (0, I), (I, I)\}$. Then

$$||\sum_{k=1}^{M} A_{j,k}x_k||^2 = ||\sum_{k=1}^{M} A_{j,k}y_k||^2 \text{ for } j = 1, 2, 3, \text{ gives}$$

$$||x_1||^2 = ||y_1||^2$$
$$||x_2||^2 = ||y_2||^2$$
$$||x_1 + x_2||^2 = ||y_1 + y_2||^2$$

So that $\langle x_j, x_k\rangle = \langle y_j, y_k\rangle$ for all $j, k = 1, 2$. This last condition by the proposition and its corollary (to follow) imply that there exists an isometry, $T : \mathbb{R}^2 \to \mathbb{R}^2$, trivially commuting with the members of $\mathscr{A}$ (as the members are identity operators hence commuting with all linear operators/isometries) for which $Tx_k = y_k$ for $k = 1, 2$.

Chapter 3

Upper and Lower Bounds on $S(M,N)$

In aims of establishing a general bounds on $S(M,N)$ for $N > 2$ the following result, phrased in the context of a separable Hilbert space $\mathcal{H}$, proves useful. By Corollary 3.02 it gives an initial upper bound for $S(M,N)$ quadratic in M.

PROPOSITION 4 *Let* $u = (u_1,...,u_M), v = (v_1,...,v_M) \in \mathcal{H}^M$ *be given with the property:* $\langle u_j, u_k\rangle = \langle v_j, v_k\rangle$, $\forall j,k = 1,...,M$. *Then there exists an isometry* $T : \mathcal{H} \to \mathcal{H}$ *such that* $Tu_j = v_j$ *for* $j = 1,...,M$.

Proof. The proof proceeds by induction on M. For base case $M = 1$,
consider $u, v \in \mathcal{H}$ given such that $||u|| = ||v|| = 1$, without loss of generality.
Let $A = \{\psi_n\}_n$, and $B = \{\phi_n\}_n$ be Orthonormal Bases (ONB's) for $\mathcal{H}$ with $\psi_1 = u$ and $\phi_1 = v$.

Consider the mapping, $T : \mathcal{H} \to \mathcal{H}, x \mapsto \sum\limits_n \langle x, \psi_n\rangle\phi_n$, and note T is an isometry of $\mathcal{H}$ as $||T(x)||_2^2 = \sum\limits_n |\hat{x}_A(n)|^2 = ||x||_2^2$. Also, $T(u) = \sum\limits_n \langle u, \psi_n\rangle\phi_n = \langle u, u\rangle v + \langle u, \psi_2\rangle\phi_2 + ... = v$ as desired, since $\langle u, \psi_n\rangle = 0, \forall n \geq 2$.

Suppose the proposition holds for $x, y \in \mathcal{H}^k$ for $k < M$. Consider $u, v \in \mathcal{H}^M$. Without loss of generality, suppose $||u_1|| = ||v_1|| = 1$. As in the previous case, let $A = \{\psi_n\}_n$, and $B = \{\phi_n\}_n$ be ONB's for $\mathcal{H}$ with $\psi_1 = u_1$ and $\phi_1 = v_1$. Consider the coefficient maps:

$$\begin{array}{ll} T_1 : \mathcal{H} \to \ell^2(A) & T_2 : \mathcal{H} \to \ell^2(B) \\ \quad x \mapsto \{\langle x, \psi_n\rangle\}_n & \quad x \mapsto \{\langle x, \phi_n\rangle\}_n \end{array}$$

The image of the $u_j's$ and $v_j's$ under these maps are given as follows:

$a = (T_1(u_1),...,T_1(u_M)) = ((1,0,...),(\langle u_2,\psi_1\rangle,\langle u_2,\psi_2\rangle,...),...,(\langle u_M,\psi_1\rangle,\langle u_M,\psi_2\rangle,...))$

$b = (T_2(v_1),...,T_2(v_M)) = ((1,0,...),(\langle v_2,\phi_1\rangle,\langle v_2,\phi_2\rangle,...),...,(\langle v_M,\phi_1\rangle,\langle v_M,\phi_2\rangle,...))$

Letting $u', v' \in \mathcal{H}^{M-1}$ denote the restriction to the last $M-1$ entries of a and b respectively, one notes:

$$\langle u_j', u_k'\rangle = \sum_l \langle u_j, \psi_l\rangle \overline{\langle u_k, \psi_l\rangle} = \sum_p \sum_l \langle u_j, \psi_l\rangle\langle \psi_l, \psi_p\rangle \overline{\langle u_k, \psi_l\rangle}$$
$$=\langle \sum_l \langle u_j, \psi_l\rangle \psi_l, \sum_p \langle u_k, \psi_p\rangle \psi_p\rangle = \langle u_j, u_k\rangle$$

Similar calculations with $\langle v_j', v_k'\rangle$ and the assumption $\langle u_j, u_k\rangle = \langle v_j, v_k\rangle$, give $\langle u_j', u_k'\rangle = \langle v_j', v_k'\rangle$. Hence by the inductive hypothesis, there exists an isometry $S : \mathcal{H} \to \mathcal{H}$ such that $Su_j' = v_j'$ for $j = 1, ..., M-1$.

Now, since the coefficient maps T_1, T_2 preserve inner products, we have:

$\langle u_1, u_j\rangle = \langle T_1(u_1), T_1(u_j)\rangle = (u_j')_1, \quad \langle v_1, v_j\rangle = \langle T_2(v_1), T_2(v_j)\rangle = (v_j')_1$

Using the assumption $\langle u_1, u_j\rangle = \langle v_1, v_j\rangle$ and $Su_j' = v_j'$, give that S restricted to the first Fourier coefficient with respect to ONB, $A = \{\psi_n\}_n$, is the identity map. Hence:

$(ST_1(u_1), ..., ST_1(u_M)) = (S(1,0,...), ..., Su_M') = ((1,0,...), ...v_M')$

and so $ST_1(u_j) = T_2(v_j)$ for $j = 1, ..., M$ and so by letting $U = T_2^{-1}ST_1$, there exists an isometry $U : \mathcal{H} \to \mathcal{H}$ such that $Uu_j = v_j$ for $j = 1, ..., M$. □

COROLLARY 3.0.2 $S(M, N) \leq \binom{M+1}{2}$

Proof. Let $u, v \in (\mathbb{R}^N)^M$ be given. Consider the ensemble $\mathscr{A}$ consisting of M-tuples $E_j = (0, ...0, I, 0, ..., 0), j = 1, ..., M$ and M-tuples $F_{i,j} = (0, ..., I, 0, ..., 0, I, 0, ..., 0)$ where I occupies the ith and jth entry, with all other entries zero in the list of operators.

Combining the operators of type E and F into ensemble $\mathscr{A}$ give the size of $\mathscr{A}$ as $S = |\mathscr{A}| = \binom{M+1}{2}$. Suppose $||\sum_{k=1}^{M} A_{j,k}u_k||^2 = ||\sum_{k=1}^{M} A_{j,k}v_k||^2$ for $j = 1, ..., S$. Then $\langle u_j, u_k\rangle = \langle v_j, v_k\rangle\ \forall j, k$. Applying the previous proposition and noting that the members of $\mathscr{A}$ commute with all linear operators $\mathbb{R}^N \to \mathbb{R}^N$, there exists an $\mathscr{A}$-admissable isometry, S, such that $Su_k = v_k$ for $k = 1, ..., M$. □

A lower bound for $S(M, N)$ follows, derived using embedding theorems. Let $O(N)$ denote the Lie group $O(N) = \{T : \mathbb{R}^N \to \mathbb{R}^N \mid T^T T = I\}$, the Orthogonal group on Euclidean space. Let $O(N, \mathscr{A})$ denote the subgroup of $O(N)$ given by, $O(N, \mathscr{A}) = \{T \in O(N) \mid TA_{n,k} = A_{n,k}T, A_{n,k} \in \mathscr{A}\}$

PROPOSITION 5 $S(M, N) \geq MN - \binom{N}{2}$

Proof. Consider the mapping $\psi : (\mathbb{R}^N)^M / O(N, \mathscr{A}) \to \mathbb{R}^S$

$$[(u_1, ..., u_M)] \mapsto (||\sum_{k=1}^{M} A_{1,k}u_k||^2, ..., ||\sum_{k=1}^{M} A_{S,k}u_k||^2)$$

$S(M,N)$	$M=1$	$M=2$	$M=3$	$M=4$	$M=5$
$N=1$	1	3	5	7	9
$N=2$	1	3	$5 \leq S \leq 6$	$7 \leq S \leq 10$	$9 \leq S \leq 15$
$N=3$	1	3	6	$9 \leq S \leq 10$	$12 \leq S \leq 15$
$N=4$	1	3	6	10	$14 \leq S \leq 15$
$N=5$	1	3	6	10	15

where $[u] = [(u_1, ..., u_M)] = [(v_1, ..., v_M)] = [v]$ if and only if there exists an $\mathscr{A}$-admissable isometry T for which $Tu_j = v_j$ for $j = 1, ..., M$. (It should be checked that ψ is well-defined. This step is essentially just handled by checking the fact T commutes with the members of $\mathscr{A}$)

Letting $H = O(N, \mathscr{A})$, H is a closed subgroup of $G = O(N)$. The Closed Subgroup Theorem for Lie groups (see Chapter 15 of Lee's book, [12]) gives that H is an embedded sub-manifold of G. As such, its dimension is bounded by the dimension of $O(N)$, calculated in [12] (Example 5.26, see Chapter 4 of this thesis for a similar proof) as $\binom{N}{2}$. Hence $\dim(H) \leq \dim(G) = \binom{N}{2}$.

Let H act on the manifold $\mathcal{M} = (\mathbb{R}^N)^M$. By Chapter 4, Theorem 3.8 in Bredon, [5], the dimension of the quotient space $\mathcal{M}/H$ is given by the highest dimension of an element of the orbit space. That is the quotient space has dimension equal to the dimension of the principal orbits. So $\dim(\mathcal{M}/H) = \dim(\mathcal{M}) - \dim(H) \geq MN - \binom{N}{2}$.

Note that ψ is continuous. If ψ is an injective map, we may use the Invariance of Domain theorem (see Kulpa, [11], for an elementary proof) in what follows, which states a continuous injective mapping from $\mathbb{R}^k \to \mathbb{R}^m$ must have $k \leq m$. The dimension of the image of ψ must then at least be that of the pre-image. Hence $S \geq MN - \binom{N}{2}$ and so $S(M,N) \geq MN - \binom{N}{2}$. □

Setting $M = N$ in the previous proposition and using the upper bound derived in Corollary 3.0.1, we obtain the following result:

COROLLARY 3.0.3 $S(M,M) = \binom{M+1}{2}$

As a final note, any collection of M vectors in $\mathbb{R}^N$ for M less than N may be embedded into $\mathbb{R}^M$, and so our corollary gives one last result.

PROPOSITION 6 $S(M,N) = \binom{M+1}{2}$ for $N \geq M$

Chapter 4

Phase Retrieval and Quaternions

Recall that the real quaternions, $\mathbb{H}$, consist of elements of the form $x = a + bi + cj + dk$, with $a, b, c, d \in \mathbb{R}$. The following algebraic relations hold in $\mathbb{H}$, $i \times j = k$, $j \times k = i$, $k \times i = j$, $j \times i = -k$, $k \times j = -i$, $i \times k = -j$, and $i^2 = j^2 = k^2 = -1$.

The conjugate of a quaternion x, is denoted $\overline{x} = a - bi - cj - dk$, and the norm-squared is $|x|^2 = x\overline{x}$. The quaternions are a division ring, and the fact that an inner product with elements $x, y \in \mathbb{H}^M$ may be defined: $\langle x, y\rangle = \overline{x}^T y = \sum_{k=1}^{M} \overline{x_k} y_k$, will be useful.

A few preliminary considerations precede our main results and help pave the way to a notion of phase retrieval in the context of quaternions.

Following the authors in [10], we introduce the *symplectic representation* of a matrix $Q \in \mathbb{H}^{M\times M}$ or vector $\xi \in \mathbb{H}^M$ over quaternions. For $\xi = \xi_1 + \xi_2 j$ where $\xi_1, \xi_2 \in \mathbb{C}^M$, this representation is given by $\rho(\xi) = \begin{pmatrix} \xi_1 \\ -\overline{\xi_2} \end{pmatrix}$ and for $Q = \Gamma_1 + \Gamma_2 j$, with $\Gamma_1, \Gamma_2 \in \mathbb{C}^{M\times M}$, this symplectic representation is $\Theta(Q) = \begin{pmatrix} \Gamma_1 & \Gamma_2 \\ -\overline{\Gamma_2} & \overline{\Gamma_1} \end{pmatrix}$. The next lemma proves a fact about this symplectic representation.

LEMMA 4.1 *The correspondences $\rho(\xi)$ and $\Theta(Q)$, for $\xi \in \mathbb{H}^M$ and*
$Q \in \mathbb{H}_*^{M\times M} = \{A \in \mathbb{H}^{M\times M} \mid \overline{A}^T = A\}$ preserve intensity measurements.
Equivalently, that is, $\overline{\rho(\xi)}^T \Theta(Q)\rho(\xi) = \overline{\xi}^T Q\xi$.

Proof. The verification of the identity is an elementary computation in quaternions. First note that since Q is taken to be self-adjoint, the quantity $\overline{\xi}^T Q\xi = \langle \xi, Q\xi\rangle$ is real valued. Now,

$$\overline{\rho(\xi)}^T \Theta(Q)\rho(\xi) = \begin{pmatrix} \overline{\xi_1} & -\xi_2 \end{pmatrix} \begin{pmatrix} \Gamma_1 & \Gamma_2 \\ -\overline{\Gamma_2} & \overline{\Gamma_1} \end{pmatrix} \begin{pmatrix} \xi_1 \\ -\overline{\xi_2} \end{pmatrix} = \overline{\xi_1}^T \Gamma_1 \xi_1 - \overline{\xi_1}^T \Gamma_2 \overline{\xi_2} + \xi_2^T \overline{\Gamma_2} \xi_1 + \xi_2^T \overline{\Gamma_1 \xi_2}$$

while in computing $\overline{\xi}^T Q\xi$, which is known to be real, we may ignore terms involving a single multiple of j.

$$\overline{\xi}^T Q\xi = (\overline{\xi_1}^T - \xi_2^T j)(\Gamma_1 + \Gamma_2 j)(\xi_1 + \xi_2 j) = \overline{\xi_1}^T \Gamma_1 \xi_1 - \overline{\xi_1}^T \Gamma_2 \overline{\xi_2} + \xi_2^T \overline{\Gamma_2} \xi_1 + \xi_2^T \overline{\Gamma_1 \xi_2}$$

Hence the two agree, and the lemma is proven. $\square$

LEMMA 4.2 *If $Q \in \mathbb{H}^{M\times M}$ has rank n over $\mathbb{H}$, then $\phi(Q)$ has rank $2n$ over $\mathbb{C}$.*

Proof. Let $\alpha_1, ..., \alpha_l \in \mathbb{H}^M$ be right-linearly independent over $\mathbb{H}$, that is:

$$\alpha_1 q_1 + \alpha_2 q_2 + ... + \alpha_l q_l = 0 \text{ implies } q_1 = q_2 = ... = q_l = 0$$

Let $c_k, b_k \in \mathbb{C}$, $c_1\rho(\alpha_1) + \cdots + c_l\rho(\alpha_l) + b_1\rho(\alpha_1 j) + \cdots + b_l\rho(\alpha_l j) = 0$, Then,

$$\rho(\alpha_1 c_1 + \cdots + \alpha_l c_l + \alpha_1 j b_1 + \cdots + \alpha_l j b_l) = 0$$

$\alpha_1(c_1 + jb_1) + \alpha_2(c_2 + jb_2) + \cdots + \alpha_l(c_l + jb_l) = 0$, as $\rho(\xi) = 0$ implies $\xi = 0$.

$$\text{Hence, } c_1 + jb_1 = \cdots = c_l + jb_l = 0 \text{ and so } c_1 = \cdots = c_l = b_1 = \cdots = b_l = 0$$

So $\rho(\alpha_1), \cdots \rho(\alpha_l), \rho(\alpha_1 j), \cdots, \rho(\alpha_l j)$ are linearly independent over $\mathbb{C}$.

Now if $Q \in \mathbb{H}^{M\times M}$ has rank n, there are $M - n$ right-linearly independent over $\mathbb{H}$ vectors in the null space of Q. So to $\Phi(Q)$ there corresponds $2(M - n)$ linearly independent vectors over $\mathbb{C}$ in the null space given by the symplectic representation. So the rank of $\Phi(Q)$ is $2n$. $\square$

Noting that for two vectors $x, \varphi \in \mathbb{H}^M$, $|\langle x, \varphi\rangle|^2 = \langle x, \varphi\rangle\overline{\langle x, \varphi\rangle} = \langle x, \varphi\rangle\langle \varphi, x\rangle = \langle \varphi, x\rangle\langle x, \varphi\rangle = \overline{\varphi}^T x\overline{x}^T\varphi$, the condition $|\langle x, \varphi\rangle|^2 = |\langle y, \varphi\rangle|^2$ can be translated to the condition that $\overline{\varphi}^T(x\overline{x}^T - y\overline{y}^T)\varphi = 0$. Another lemma becomes relevant in the case $x\overline{x}^T = y\overline{y}^T$.

LEMMA 4.3 *For two vectors $x, y \in \mathbb{H}^M$, if $x\overline{x}^T = y\overline{y}^T$, then there exists $\omega \in \mathbb{H}$, $|\omega|^2 = 1$ such that $x = y\omega$.*

Proof. Let $x = (x_1, x_2, ..., x_M)$, $y = (y_1, y_2, ..., y_M)$. Consider the matrix representation of the equality $x\overline{x}^T = y\overline{y}^T$:

$$\begin{pmatrix} |x_1|^2 & x_1\overline{x_2} & \cdots & x_1\overline{x_M} \\ x_2\overline{x_1} & |x_2|^2 & \cdots & x_2\overline{x_M} \\ \vdots & \vdots & \ddots & \vdots \\ x_M\overline{x_1} & x_M\overline{x_2} & \cdots & |x_M|^2 \end{pmatrix} = \begin{pmatrix} |y_1|^2 & y_1\overline{y_2} & \cdots & y_1\overline{y_M} \\ y_2\overline{y_1} & |y_2|^2 & \cdots & y_2\overline{y_M} \\ \vdots & \vdots & \ddots & \vdots \\ y_M\overline{y_1} & y_M\overline{y_2} & \cdots & |y_M|^2 \end{pmatrix}$$

The matrix equality gives the following equalities: $|x_i|^2 = |y_i|^2$ for all $i = 1, ..., M$ and more generally $x_i\overline{x_j} = y_i\overline{y_j}$ for all $i, j = 1, ..., M$. For $x \neq 0$, then $|x_j| = |y_j| > 0$ for some j. Without loss of generality, let $j = 1$. Then $x_i\overline{x_1} = y_i\overline{y_1}$ for all $i = 1, ..., M$ so that $x_i = y_i\overline{y_1}\frac{1}{\overline{x_1}}$ for all $i = 1, ..., M$. Letting $\omega = \overline{y_1}\frac{1}{\overline{x_1}}$ gives the desired conclusion. □

It now is appropriate to introduce the mappings $\mathcal{C}, \mathscr{C}$, along with the equivalence relation , $x \sim_R y$, defined on members $x, y \in \mathbb{H}^M$. $x \sim_R y$ means that x is a right unit-modular constant multiple of y, that is $x = y\omega$ for some $\omega \in \mathbb{H}$ such that $|\omega|^2 = 1$. For $\Phi = \{\varphi_k\}_{k=1}^N$, with $\varphi_k \in \mathbb{H}^M$, the two mappings are defined as follows:

$$\begin{array}{cc} \mathcal{C} : \mathbb{H}_*^{M\times M} \to \mathbb{R}^N & \mathscr{C} : \mathbb{H}^M/\sim_R \to \mathbb{R}^N \\ \mathcal{C}(Q) = \{\overline{\varphi_k}^T Q \varphi_k\}_{k=1}^N & \mathscr{C}([x]) = \{|\langle x, \varphi_k\rangle|^2\}_{k=1}^N \end{array}$$

PROPOSITION 7 Let $\Phi = \{\varphi_k\}_{k=1}^N$ be given such that the mapping $\mathcal{C}$ has no rank 1 or 2 matrices $Q \in \mathbb{H}_*^{M\times M}$ in its kernel. Then the mapping $\mathscr{C}$ is injective, that is, $|\langle x, \varphi_k\rangle|^2 = |\langle y, \varphi_k\rangle|^2$ for $k = 1, ..., N$ gives $x = y\omega$ for some $\omega \in \mathbb{H}$ such that $|\omega|^2 = 1$

Proof. Consider the mapping $\mathcal{C}$'s action on matrices $x\overline{x}^T$, $y\overline{y}^T \in \mathbb{H}_*^{M\times M}$.
By the previous observation, for $x, \varphi_k \in \mathbb{H}^M$

$$|\langle x, \varphi_k\rangle|^2 = \overline{\varphi_k}^T x\overline{x}^T \varphi_k$$

One can translate the statement, for $x, y \in \mathbb{H}^M$,

$$|\langle x, \varphi_k\rangle|^2 = |\langle y, \varphi_k\rangle|^2 \text{ for all } k = 1, ..., N$$

into a statement about mapping $\mathcal{C}$, namely,

$$\mathcal{C}(x\overline{x}^T) = \mathcal{C}(y\overline{y}^T)$$

Equivalently, by linearity of $\mathcal{C}$,

$$\mathcal{C}(x\overline{x}^T - y\overline{y}^T) = 0$$

Now, either $x\overline{x}^T - y\overline{y}^T$ is an element of $\mathbb{H}_*^{M\times M}$ of rank 1 or 2, or $x\overline{x}^T - y\overline{y}^T = 0$. So if Φ is taken such that $\mathcal{C}$ has no rank 1 or 2 members of $\mathbb{H}_*^{M\times M}$ in its null space, and $\mathcal{C}(x\overline{x}^T - y\overline{y}^T) = 0$, it must be that $x\overline{x}^T = y\overline{y}^T$. By the lemma, this gives $x = y\omega$ for some $\omega \in \mathbb{H}$ such that $|\omega|^2 = 1$. That is $x \sim_R y$, and so $\mathscr{C}$ is injective. □

The mapping $\mathcal{C}$, an analog to the "super-analysis operator" as termed by the authors of [3], readily allows the introduction of tools from algebraic geometry. Following the arguments in [7], we see how results in complex phase retrieval can be lifted to ones for phase retrieval over quaternions.

Let $\mathbb{C}^{M\times M}_{skew}$, $\mathbb{C}^{M\times M}_{sym}$, and $\mathbb{C}^{M\times M}_{Herm}$ donte the set of $M \times M$ skew symmetric, symmetric, and Hermitian matrices respectively. Let $\mathcal{B}_{2M,N} = \{([U,V],[X,Y]) \in \mathbb{P}(\mathbb{C}^{2M\times N} \times \mathbb{C}^{2M\times N}) \times \mathbb{P}(\mathbb{C}^{2M\times 2M}_{sym} \times \mathbb{C}^{2M\times 2M}_{skew}) \mid$
$(U - iV)^T(X + iY)(U + iV) = 0$ and $rank(X + iY) \leq 4\}$.
Let $\pi_1 : \mathbb{P}(\mathbb{C}^{2M\times N} \times \mathbb{C}^{2M\times N}) \times \mathbb{P}(\mathbb{C}^{2M\times 2M}_{sym} \times \mathbb{C}^{2M\times 2M}_{skew}) \to \mathbb{P}(\mathbb{C}^{2M\times N} \times \mathbb{C}^{2M\times N})$ be the projection of $\mathcal{B}_{2M,N}$ onto its first coordinate. For a complex variety X, let $X_{\mathbb{R}}$ denote the real points of X.

PROPOSITION 8 Let frame $\Phi = \{\varphi_k\}_{k=1}^N$, $\varphi_k \in \mathbb{H}^M$, have corresponding complex frame $\Lambda = \{\lambda_k\}_{k=1}^N$ where $\lambda_k = \rho(\varphi_k) \in \mathbb{C}^{2M}$. Let $\lambda_k = u_k + iv_k$ and U (respectively V) be the real matrix with columns u_k (respectively v_k). Then the map $\mathscr{C}$ is injective if and only if $[U, V]$ does not belong to the projection $\pi_1((\mathcal{B}_{2M,N})_{\mathbb{R}})$.

Proof. Let $\Lambda = U + iV$, $\lambda_k = u_k + iv_k$, $u_k, v_k \in \mathbb{R}^M$ and $Q = X + iY$, with X symmetric and Y skew symmetric, $X, Y \in \mathbb{R}^{M\times M}$.

Let $\mathcal{I} = \{(\Lambda, Q) \in \mathbb{C}^{2M\times N} \times \mathbb{C}^{2M\times 2M}_{Herm} \mid Q \neq 0, rank(Q) \leq 4$ and $\overline{\lambda_k}^T Q\lambda_k = 0$ for $k = 1, ..., N\}$.
$\mathcal{I}$ is linearly isomorphic over $\mathbb{R}$ to $\mathcal{J}$, a subset of real vector space $\mathbb{R}^{2M\times N} \times \mathbb{R}^{2M\times N} \times \mathbb{R}^{2M\times 2M}_{sym} \times \mathbb{R}^{2M\times 2M}_{skew}$, given below:
$\mathcal{J} = \{(U, V, X, Y) \mid X + iY \neq 0, rank(X + iY) \leq 4$ and $\overline{\lambda_k}^T (X + iY)\lambda_k = 0\}$.
$\mathscr{C}$ is injective by the preceding proposition if (U, V) is not contained in the projection of $\mathcal{J}$ onto the first two coordinates. $(\mathcal{B}_{2M,N})_{\mathbb{R}}$ is the projectivization of $\mathcal{J}$, hence (U, V) is not contained in this projectivization if and only if $[U, V] \notin \pi_1((\mathcal{B}_{2M,N})_{\mathbb{R}})$ □

THEOREM 4.1 *The projective complex variety $\mathcal{B}_{2M,N}$ has dimension*
$4MN - N + 16M - 18$.

Proof. Let $\mathcal{B}'_{2M,N}$ be the subvariety of $\mathbb{P}(\mathbb{C}^{2M\times N} \times \mathbb{C}^{2M\times N}) \times \mathbb{P}(\mathbb{C}^{2M\times 2M})$ consisting of triples $([U, V], [Q])$ such that

$$rank(Q) \leq 4 \text{ and } (u_k - iv_k)^T Q(u_k + iv_k) = 0 \text{ for all } k = 1, ..., N$$

where u_k and v_k are the kth columns of U and V respectively.

$\mathcal{B}_{2M,N}$ and $\mathcal{B}'_{2M,N}$ are linearly isomorphic by the mapping

$\mathcal{F} : \mathbb{C}^{2M\times 2M}_{sym} \times \mathbb{C}^{2M\times 2M}_{skew} \to \mathbb{C}^{2M\times 2M}$, $(X,Y) \to X + iY = Q$. $\mathcal{F}^{-1}(Q) = \frac{Q+Q^T}{2} + i\frac{Q-Q^T}{2i}$.

Hence $\dim(\mathcal{B}_{2M,N}) = \dim(\mathcal{B}'_{2M,N})$.

Let π_1 and π_2 be the projections onto the first and second coordinate of $\mathcal{B}'_{2M,N}$.

Using the following formula from Harris, the dimension of $\mathcal{B}'_{2M,N}$ may be calculated from $\dim(\pi_2(\mathcal{B}'_{2M,N}))$ and $\dim(\pi_2^{-1}(Q))$ for $Q \in \mathbb{C}^{2M\times 2M}$.

$$\dim(\mathcal{B}'_{2M,N}) = \dim(\pi_2(\mathcal{B}'_{2M,N})) + \min_{Q\in\pi_2(\mathcal{B}'_{2M,N})} \dim(\pi_2^{-1}(Q))$$

The image of $\mathcal{B}'_{2M,N}$ under π_2 is the set of $rank \leq 4$ matrices in $\mathbb{P}(\mathbb{C}^{2M\times 2M})$. To see this, take u, v such that $(u - iv)^T Q(u + iv) = 0$ (Q has $rank \leq 4$ hence take $u + iv$ such that it is in the kernel of Q for instance). Let U and V be built by repeating column vectors $u_k = u$, $v_k = v$. Then, $([U, V], [Q])$ belongs to $\mathcal{B}'_{2M,N}$ and hence, every $rank \leq 4$, $Q \in \mathbb{C}^{2M\times 2M}$, is in the image of π_2.

The set of $rank \leq 4$ matrices in $\mathbb{C}^{2M\times 2M}$ is an irreducible variety of dimension $16M - 16$, [8]. So the projectivization of this variety in $\mathbb{P}(\mathbb{C}^{2M\times 2M})$ has dimension $16M - 17$, so that

$$\dim(\pi_2(\mathcal{B}'_{2M,N})) = 16M - 17$$

Fix $Q \in \pi_2(\mathcal{B}'_{2M,N})$. Then the polynomial equation holds for Q

$$(u_k - iv_k)^T Q(u_k + iv_k) = 0$$

For each pair of columns (u_k, v_k), this equation defines a hypersurface of dimension $4M - 1$ in $(\mathbb{C}^{2M})^2$. So the pre-image of Q, $\pi_2^{-1}(Q)$ consists of N hypersurfaces of dimension $4M - 1$ in $((\mathbb{C}^{2M})^2)^N$.

After projectivization, $\pi_2^{-1}(Q)$ has dimension $(4M - 1)N - 1$.

Using the formula, one obtains

$$\begin{aligned}\dim(\mathcal{B}'_{2M,N}) &= \dim(\pi_2(\mathcal{B}'_{2M,N})) + \min_{Q\in\pi_2(\mathcal{B}'_{2M,N})} \dim(\pi_2^{-1}(Q)) \\ &= 16M - 17 + 4MN - N - 1\end{aligned}$$

□

Our main result for this section follows.

THEOREM 4.2 *There exists* $\Phi = \{\varphi_k\}_{k=1}^N, \varphi_k \in \mathbb{H}^M$ *of size* $|\Phi| = N \leq 16M - 16$ *for which corresponding mapping* $\mathscr{C}$ *is injective.*

Proof. By the preceding proposition, $\Lambda = U + iV$ gives $[U, V]$ in $\pi_1((\mathcal{B}_{2M,N})_{\mathbb{R}}) \subset (\pi_1(\mathcal{B}_{2M,N}))_{\mathbb{R}}$. The dimension of the projectivization is bounded by the original dimension, so,

$$\dim(\pi_1(\mathcal{B}_{2M,N})) \leq \dim(\mathcal{B}_{2M,N}) = 4MN + 16M - N - 18$$

when N is $16M - 16$ or higher the dimension of this projection is strictly less than $4MN - 1$, the dimension of $\mathbb{P}(\mathbb{C}^{2M\times N} \times \mathbb{C}^{2M\times N})$.

Hence, for $N \geq 16M - 16$ there exists $[U, V] \in \mathbb{P}(\mathbb{C}^{2M\times N} \times \mathbb{C}^{2M\times N})$ such that $(U - iV)^T Q(U + iV) \neq 0$ for all $rank \leq 4$, $Q \in \mathbb{C}^{2M\times 2M}$. Hence, by letting the inverse to mapping ρ be denoted $e : \mathbb{C}^{2M} \to \mathbb{H}^M$ and the inverse to mapping Θ, $\theta : \mathbb{C}^{2M\times 2M} \to \mathbb{H}^{M\times M}$, there exist Λ with corresponding $\Phi = \{e(\lambda_k)\}_{k=1}^N = \{\varphi_k\}_{k=1}^N$ such that for $\theta(Q) = W$,

$$\overline{\varphi_k}^T W\varphi_k \neq 0 \text{ for some } k, \text{ for all } rank \leq 2, W \in \mathbb{H}_*^{M\times M}.$$

Hence, the mapping $\mathscr{C}$:$\mathbb{H}^M/\sim_R \to \mathbb{R}^N$ is injective for Φ. □

Regarding multiplication on the right by a unit-modular quaternion as an isometry, phase retrieval over quaternions can be related to the problem of calculating $S(M, 4)$. The previous theorem gives

If $|\langle x, \varphi_k\rangle|^2$=$|\langle y, \varphi_k\rangle|^2$ for $k = 1, ..., N$, then
there exists $\omega \in \mathbb{H}$, $|\omega|^2 = 1$, such that $x\omega = y$.

Using this equality, $|\langle x, \varphi_k\rangle|^2 = |\sum_{j=1}^M \overline{\varphi_{k,j}} x_j|^2 = |\sum_{j=1}^M \overline{\varphi_{k,j}} y_j|^2 = |\langle y, \varphi_k\rangle|^2$. By splitting $\overline{\varphi_k}$ into its components and considering their action on each component of x, we may further consider the matrix representation of the components $\overline{\varphi_k}$, $A_{k,j}$. Then

$$|\sum_{j=1}^M \overline{\varphi_{k,j}} x_j|^2 = ||\sum_{j=1}^M A_{k,j} x'_j||^2 = ||\sum_{j=1}^M A_{k,j} y'_j||^2 = |\sum_{j=1}^M \overline{\varphi_{k,j}} y_j|^2.$$

Where for instance if $\overline{\varphi_{k,j}} = \alpha - i\beta - j\gamma - k\delta$, and $x_j = a + ib + jc + kd$

$$A_{k,j} x'_j = \begin{pmatrix} \alpha & \beta & \gamma & \delta \\ -\beta & \alpha & \delta & -\gamma \\ -\gamma & -\delta & \alpha & \beta \\ -\delta & \gamma & -\beta & \alpha \end{pmatrix} \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}$$

Now, let T_ω represent the linear operator whose action corresponds to multiplication of an element $x \in \mathbb{H}^M$ by ω on the right. For $\omega = \omega_1 + \omega_2 i + \omega_3 j + \omega_4 k$

$$x_j\omega = (a\omega_1 - b\omega_2 - c\omega_3 - d\omega_4) + (a\omega_2 + b\omega_1 + c\omega_4 - d\omega_3)i +$$
$$(a\omega_3 - b\omega_4 + c\omega_1 - d\omega_2)j + (a\omega_4 + b\omega_3 + c\omega_2 + d\omega_1)k$$

$$\text{Hence, } T_\omega(x_j) = \begin{pmatrix} \omega_1 & -\omega_2 & -\omega_3 & -\omega_4 \\ \omega_2 & \omega_1 & \omega_4 & -\omega_3 \\ \omega_3 & -\omega_4 & \omega_1 & \omega_2 \\ \omega_4 & \omega_3 & -\omega_2 & \omega_1 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}$$

The equality $|\langle x, \varphi_k \rangle|^2 = |\langle y, \varphi_k \rangle|^2$ may be reinterpreted

$$|\sum_{j=1}^{M} \overline{\varphi_{k,j}} x_j|^2 = |\sum_{j=1}^{M} \overline{\varphi_{k,j}} y_j|^2 = |\sum_{j=1}^{M} \overline{\varphi_{k,j}} x_j \omega|^2 = ||\sum_{j=1}^{M} A_{k,j} T_\omega x_j||^2$$
$$|(\sum_{j=1}^{M} \overline{\varphi_{k,j}} x_j)\omega|^2 = ||\textstyle\sum_{j=1}^{M} T_\omega A_{k,j} x_j||^2 = ||T_\omega \displaystyle\sum_{j=1}^{M} A_{k,j} x_j||^2 = ||\sum_{j=1}^{M} A_{k,j} x_j||^2$$

Above, an implicit argument is given for $A_{k,j}T_\omega = T_\omega A_{k,j}$. By computation each of $A_{k,j}T_\omega$ and $T_\omega A_{k,j}$ are given as:

$$\begin{pmatrix} \alpha\omega_1 + \beta\omega_2 + \delta\omega_4 + \gamma\omega_3 & -\alpha\omega_2 + \beta\omega_1 + \delta\omega_3 - \gamma\omega_4 & -\alpha\omega_3 + \beta\omega_4 - \delta\omega_2 + \gamma\omega_1 & -\alpha\omega_4 - \beta\omega_3 + \delta\omega_1 + \gamma\omega_2 \\ \alpha\omega_2 - \beta\omega_1 + \delta\omega_3 - \gamma\omega_4 & \alpha\omega_1 + \beta\omega_2 - \delta\omega_4 - \gamma\omega_3 & \alpha\omega_4 + \beta\omega_3 + \delta\omega_1 + \gamma\omega_2 & -\alpha\omega_3 + \beta\omega_4 + \delta\omega_2 - \gamma\omega_1 \\ \alpha\omega_3 + \beta\omega_4 - \delta\omega_2 - \gamma\omega_1 & -\alpha\omega_4 + \beta\omega_3 - \delta\omega_1 + \gamma\omega_2 & \alpha\omega_1 - \beta\omega_2 - \delta\omega_4 + \gamma\omega_3 & \alpha\omega_2 + \beta\omega_1 + \delta\omega_3 + \gamma\omega_4 \\ \alpha\omega_4 - \beta\omega_3 - \delta\omega_1 + \gamma\omega_2 & \alpha\omega_3 + \beta\omega_4 + \delta\omega_2 + \gamma\omega_1 & -\alpha\omega_2 - \beta\omega_1 + \delta\omega_3 + \gamma\omega_4 & \alpha\omega_1 - \beta\omega_2 + \delta\omega_4 - \gamma\omega_3 \end{pmatrix}$$

Hence T_ω is an $\mathscr{A}$-admissable isometry with respect to ensembles of operators, $\mathscr{A}$, representing multiplication of a quaternion by a quaternion on the left. Thus, the results in this Chapter imply an upper bound on $S(M, 4)$:

PROPOSITION 9 $S(M, 4) \leq 16M - 16$

Chapter 5
Appendix

Let $F : \mathbb{R}^{n+k} \to \mathbb{R}^k$ be a C^∞ map and $y \in \mathbb{R}^k$.

DEFINITION 5.0.1 y is said to be a regular value for the mapping F should the following hold: the derivative $D_{F,y}(x) : \mathbb{R}^{n+k} \to \mathbb{R}^k$ is surjective, that is $\dim(\ker D_{F,y}(x)) = n$.

THEOREM 5.1 If $y \in \mathbb{R}^k$ is a regular value of a C^∞ map $F : \mathbb{R}^{n+k} \to \mathbb{R}^k$, then $F^{-1}(y)$ is a C^∞-manifold of dimension n.

Let A and T denote linear transformations in what follows.

DEFINITION 5.0.2 The Orthogonal group on Euclidean space $\mathbb{R}^n$, denoted by $O(n)$, is $O(n) = \{T : \mathbb{R}^n \to \mathbb{R}^n \mid T^T T = I\}$.

PROPOSITION 10 The Orthogonal group, $O(n) = \{T : \mathbb{R}^n \to \mathbb{R}^n | T^T T = I\}$, is a Lie group of dimension $\dim O(n) = \binom{n}{2}$

Proof. Let $M_n(\mathbb{R}) = \{A : \mathbb{R}^n \to \mathbb{R}^n\}$, and $S_n(\mathbb{R}) = \{A : \mathbb{R}^n \to \mathbb{R}^n | A = A^T\}$. Consider the mapping $F : M_n(\mathbb{R}) \to M_n(\mathbb{R})$ given by $F(A) = A^T A$. Let $M \in S_n(\mathbb{R})$, be a element in the image of F. Then the derivative of F at M is:

$$D_{F,M}(A) = \tfrac{d}{dt}(M + tA)^T(M + tA)|_{t=0} = \tfrac{d}{dt} M^T M + tA^T M + tM^T A + t^2 A^T A|_{t=0} =$$
$$A^T M + M^T A$$

For $B \in S_n(\mathbb{R})$, there is a transformation $H = \frac{1}{2}MB$ such that:

$$D_{F,M}(H) = (\tfrac{1}{2}MB)^T M + M^T(\tfrac{1}{2}MB) = \tfrac{1}{2}(B^T M^T M + M^T M B) = \tfrac{1}{2}(B^T + B) = B$$

Consider $M \in O(n)$, $F(M) = I$, where I denotes the identity map. I is a regular value for the mapping F as the derivative of F, $D_{F,I}(A)$ is surjective. $F^{-1}(I) = O(n)$ by definition, and so $O(n)$ is a C^∞ manifold of dimension:

$$\dim(M_n(\mathbb{R})) - \dim(S_n(\mathbb{R})) = n^2 - \tfrac{n(n+1)}{2} = \tfrac{n(n-1)}{2} = \tbinom{n}{2}$$

To prove that $O(n)$ is a Lie group, one checks that the mappings $m(A, B) = AB$ and $i(A) = A^T$ are continuous on $O(n)$. $\square$

References

[1] B. Alexeev, J. Cahill, and D. G. Mixon, Full spark frames, J. Fourier Anal. Appl., vol. 3, pp. 25, Oct. 2011.

[2] R. Balan, P. Casazza, D. Edidin. On signal reconstruction without phase. Appl. Comp. Harmon. Anal. 20 (2006) 345-346.

[3] A. Bandeira, J. Cahill, D. Mixon, and A. Nelson. Saving phase: Injectivity and stability for phase retrieval. arXiv:1302.4618.

[4] B. G. Bodmann, N. Hammen. Stable phase retrieval with low-redundancy frames. arXiv:1302.5487.

[5] G.E. Bredon. Introduction to compact transformation groups. Academic Press, 1972.

[6] E. J. Candès, T. Strohmer, V. Voroninski. PhaseLift: Exact and stable signal recovery from magnitude measurements via convex programming. Commun. Pure Appl. Math. 66 (2013), 1241-1274.

[7] A. Conca, D. Edidin, M. Hering, and C. Vinzant. An algebraic characterization of injectivity in phase retrieval. Appl. Comp. Harmon. Anal., vol. 38, no. 2, pp.346 - 356, 2015.

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

[9] T. Heinosaari, L. Mazzarella, M. M. Wolf. Quantum tomography under prior information. arxiv:1109.5478.

[10] D.R. Farenick, B.A.F. Pidkowich The spectral theorem in quaternions Linear Algebra Appl., 371 (2003), pp. 75102

[11] W. Kulpa Poincaré and domain invariance theorem. Acta Univ. Carolin. Math. Phys. 39 (1998), 127-136.

[12] J.M. Lee. Introduction to Smooth Manifolds. Springer Verlag, 2003.

[13] Vincent, Ian. Lie Groups. Internet Resource, $\texttt{http}: //\texttt{www2.warwick.ac.uk/fac/sci/maths/people/staff/vincent/lie}_{\texttt{g}}\texttt{roups.pdf}$.

[14] C. Vinzant. A small frame and a certificate of its injectivity. Preprint, arXiv:1502.0465v1.