AN ALGEBRAIC CHARACTERIZATION OF INJECTIVITY IN PHASE RETRIEVAL

ALDO CONCA, DAN EDIDIN, MILENA HERING, AND CYNTHIA VINZANT

Abstract. A complex frame is a collection of vectors that span $\mathbb{C}^M$ and define measurements, called intensity measurements, on vectors in $\mathbb{C}^M$. In purely mathematical terms, the problem of phase retrieval is to recover a complex vector from its intensity measurements, namely the modulus of its inner product with these frame vectors. We show that any vector is uniquely determined (up to a global phase factor) from $4M-4$ generic measurements. To prove this, we identify the set of frames defining non-injective measurements with the projection of a real variety and bound its dimension.

1. Introduction

In signal processing, a signal $x \in \mathbb{C}^M$ often cannot be measured directly. Instead, one can only measure the absolute values of its inner product with a fixed set of vectors $\Phi = \{\phi_1, \ldots, \phi_N\} \in \mathbb{C}^M$. Here we take $\mathbb{C}^M$ with the inner product $\langle x, y\rangle = \sum_{m=1}^M x_m \overline{y_m}$.

An N-element complex *frame* Φ is a collection of vectors $\phi_1, \ldots, \phi_N$ which span $\mathbb{C}^M$. A complex frame $\Phi = \{\phi_n\}_{n=1}^N \subset \mathbb{C}^M$ defines N *intensity measurements* of a vector $x \in \mathbb{C}^M$,

$$|\langle \phi_n, x\rangle|^2 \;=\; \phi_n^* x x^* \phi_n \quad \text{for} \quad n = 1, \ldots, N, \tag{1}$$

where we use v^* to denote the conjugate transpose of a vector (or matrix) v.

The problem of *phase retrieval* is to reconstruct a vector $x \in \mathbb{C}^M$ from its intensity measurements. Note that multiplying x by a scalar of unit modulus does not change the measurements (1), so we can only reconstruct x up to a global phase factor. For phase retrieval to be possible, any two vectors x and y with the same intensity measurements must differ by a scalar multiple of norm one, namely $x = e^{i\theta}y$. In other words, the non-linear map

$$\mathcal{A}_\Phi \colon (\mathbb{C}^M/S^1) \to (\mathbb{R}_{\geq 0})^N \quad \text{given by} \quad x \mapsto \left(|\langle x, \phi_n\rangle|^2\right)_{n=1,\ldots,N} \tag{2}$$

is injective, where $(\mathbb{C}^M/S^1)$ is obtained by identifying $x \in \mathbb{C}^M$ with $e^{i\theta}x$ for every $\theta \in [0, 2\pi]$.

Our main result states that $4M-4$ generic intensity measurements suffice to determine a vector in $\mathbb{C}^M$. This proves part (b) of the "$4M-4$ Conjecture" made in [2].

Theorem 1.1. *If $N \geq 4M-4$, then for a generic frame Φ the map $\mathcal{A}_\Phi$ is injective.*

By generic we mean that Φ corresponds to a point in a non-empty Zariski open subset of $\mathbb{C}^{M\times N} \cong (\mathbb{R}^{M\times N})^2$ (see Section 2.2). In particular, this theorem implies that when $N \geq 4M-4$, there is an open dense set of frames Φ (in the Euclidean topology on $\mathbb{C}^{M\times N}$) for which $\mathcal{A}_\Phi$ is injective. Part (a) of the conjecture in [2] says that this result is tight, i.e. that for $N < 4M-4$ the map $\mathcal{A}_\Phi$ is never injective. This part is still open.

The history of this problem in the context of finite frames will be discussed in Section 2. There, we also define some necessary concepts from algebraic geometry, such as generic points and the dimension of algebraic sets. In Section 3 (specifically on page 5) we prove Theorem 1.1. A polynomial vanishing on the set of frames giving non-injective measurements is found and discussed in Section 4. Finally, in Section 5 we discuss what our algebraic approach can say about injectivity with fewer measurements. We end by rephrasing the open part of conjecture of [2] in the language of real algebraic geometry and operator theory.

2. Background

Here we give a short review of the history of phase retrieval in the context of finite frames and review some needed terminology from algebraic geometry.

2.1. **The phase retrieval problem.** Phase retrieval is an old problem in signal processing, and the literature on this subject is vast. However, in the context of finite frame theory it was first considered Balan, Casazza, and Edidin [1]. In [1, Theorem 3.3], the authors show that the map $\mathcal{A}_\Phi$ (2) is injective for a generic frame Φ when $N \geq 4M-2$. However, Bodmann and Hammen exhibit an explicit family of frames with $4M-4$ vectors for which injectivity holds, which suggests the possibility of a better bound [3]. On the other hand Heinosaari, Mazzarella and Wolf [10] used embedding theorems in homotopy theory to show that $N \geq (4+o(1))M$ is necessary for the injectivity of $\mathcal{A}_\Phi$. Recently, Bandeira, Cahill, Mixon, and Nelson [2] conjectured the following.

The $\mathbf{4M-4}$ Conjecture [2]**.** *Consider a frame $\Phi = \{\phi_n\}_{n=1}^N \subseteq \mathbb{C}^M$ and the mapping $\mathcal{A}_\Phi : (\mathbb{C}^M/S^1) \to (\mathbb{R}_{\geq 0})^N$ taking a vector x to its intensity measurements $(|\langle x, \phi_n\rangle|^2)_{n=1,\ldots,N}$. If $M \geq 2$ then the following hold.*

(a) If $N < 4M-4$, then $\mathcal{A}_\Phi$ is not injective.
(b) If $N \geq 4M-4$, then $\mathcal{A}_\Phi$ is injective for generic Φ.

In [2], this conjecture was proved for $M = 2, 3$. Our Theorem 1.1 establishes part (b).

Injectivity of the map $\mathcal{A}_\Phi$ implies that phase retrieval is possible, but the problem of effectively reconstructing a vector from its intensity measurements is quite difficult. There have been many papers devoted to determining efficient reconstruction algorithms. For references we direct the reader to [2].

Remark 2.1. In [1], Balan, Casazza, and Edidin characterized frames giving injective measurements in the *real* case. Precisely, [1, Theorem 2.8] says that a real frame Φ defines injective measurements (on $\mathbb{R}^M/\{\pm 1\}$) if and only if Φ satisfies the *finite complement property*, which means that for every subset $\mathbf{S} \subset \{1, \ldots, N\}$ either $\{\phi_n\}_{n\in\mathbf{S}}$ or its complement $\{\phi_n\}_{n\in\mathbf{S}^c}$ spans $\mathbb{R}^M$. In particular, if $N < 2M-1$ then the corresponding map $\mathcal{A}_\Phi$ cannot be injective, and if $N \geq 2M-1$ then for a generic frame Φ, $\mathcal{A}_\Phi$ is injective.

It would be very interesting to have an analogous characterization for complex frames. As a first step in this direction, in Section 4 we describe some polynomials that vanish on the set of frames Φ for which $\mathcal{A}_\Phi$ is non-injective.

Remark 2.2. A frame Φ determines an M-dimensional subspace of $\mathbb{C}^N$ by taking the row span of the $M \times N$ matrix whose columns are the vectors ϕ_n, $1 \leq n \leq N$. It was observed in [1, Proposition 2.1], that if Φ and Φ' determine the same subspace in $\mathbb{C}^N$, then $\mathcal{A}_\Phi$ is injective if and only if $\mathcal{A}_{\Phi'}$ is injective. In other words, injectivity of $\mathcal{A}_\Phi$ only depends on subspace determined by Φ. This subspace corresponds to a point in the Grassmannian $G(M, N)$ of M-dimensional subspaces of $\mathbb{C}^N$. Thus there is a subset of $G(M, N)$ parameterizing frames for which $\mathcal{A}_\Phi$ is injective. This approach was applied in [1].

2.2. **Terminology from algebraic geometry.** Let $\mathbb{F}$ be a field (specifically $\mathbb{F} = \mathbb{R}$ or $\mathbb{F} = \mathbb{C}$). A subset of $\mathbb{F}^d$ defined by the vanishing of finitely many polynomials in $\mathbb{F}[x_1, \ldots, x_d]$ is called an *affine variety.* If these polynomials are homogeneous, then their vanishing defines a subset of projective space $\mathbb{P}(\mathbb{F}^d)$, which is called a *projective variety.*

The *Zariski topology* on $\mathbb{F}^d$ (or $\mathbb{P}(\mathbb{F}^d)$) is defined by declaring affine (resp. projective) varieties to be closed subsets. Note that a Zariski closed set is also closed in the Euclidean topology. The complement of a variety is a *Zariski open* set. A non-empty Zariski open set is open and dense in the Euclidean topology. We say that a *generic point* of $\mathbb{F}^d$ (or $\mathbb{P}(\mathbb{F}^d)$) has a certain property if there is a non-empty Zariski open set of points having this property.

The space of complex frames $\mathcal{F}(M, N)$ can be identified with $M \times N$ matrices of full rank, so it is a Zariski-open set in $\mathbb{C}^{M\times N}$. For the statement of Theorem 1.1 we identify $\mathbb{C}^{M\times N}$ with $(\mathbb{R}^{M\times N})^2$ and view $\mathcal{F}(M, N)$ as an open subset of $(\mathbb{R}^{M\times N})^2$. Theorem 1.1 then states that for $N \geq 4M - 4$, there is a Zariski open subset $\mathcal{U}$ of $\mathcal{F}(M, N)$ such that for every frame Φ corresponding to a point of $\mathcal{U}$, the map $\mathcal{A}_\Phi$ is injective.

In our main proof, we also rely heavily on the notion of the dimension of a variety defined over $\mathbb{C}$. For an introduction and many equivalent definitions of the dimension of a variety, see [9, §11] or [4, Chapter 9]. In particular, the *dimension* of an irreducible variety (meaning that it is not the union of two proper subvarieties) X equals the dimension of its tangent space at a generic point of X.

We will also make use of the interplay between real and complex varieties. Given a complex variety X defined by equations with real coefficients we denote its set of real points by $X_\mathbb{R}$.

3. Proof of Theorem 1.1

We prove Theorem 1.1 by showing that the subset of $\mathbb{C}^{M\times N} \cong (\mathbb{R}^{M\times N})^2$ corresponding to frames Φ for which $\mathcal{A}_\Phi$ is not injective is contained in a proper real algebraic subset. The complement of this algebraic set is an open dense set corresponding to frames Φ for which $\mathcal{A}_\Phi$ is injective. A key ingredient of this proof is a reformulation, due to Bandeira, Cahill, Mixon, and Nelson [2], of the injectivity of the map $\mathcal{A}_\Phi\colon (\mathbb{C}^M/S^1) \to \mathbb{R}^N$ defined in (2).

Proposition 3.1 (Lemma 9 [2]). *The map $\mathcal{A}_\Phi$ is not injective if and only if there is a nonzero Hermitian matrix $Q \in \mathbb{C}^{M\times M}$ for which*

$$\operatorname{rank}(Q) \leq 2 \quad \textit{and} \quad \phi_n^* Q \phi_n = 0 \quad \textit{for each } 1 \leq n \leq N. \tag{3}$$

We use this condition to translate injectivity of the map $\mathcal{A}_\Phi$ into a question in algebraic geometry. Let $\mathbb{C}^{M\times M}_{\text{sym}}$ denote the set of symmetric complex $M \times M$ matrices, and $\mathbb{C}^{M\times M}_{\text{skew}}$ the set of skew-symmetric complex $M \times M$ matrices.

Definition 3.2. Let $\mathcal{B}_{M,N}$ denote the subset of $\mathbb{P}(\mathbb{C}^{M\times N} \times \mathbb{C}^{M\times N}) \times \mathbb{P}(\mathbb{C}^{M\times M}_{\text{sym}} \times \mathbb{C}^{M\times M}_{\text{skew}})$ consisting of quadruples of matrices $([U, V], [X, Y])$ for which

$$\operatorname{rank}(X + \mathrm{i}Y) \leq 2 \quad \text{and} \quad u_n^T X u_n + v_n^T X v_n - 2u_n^T Y v_n = 0 \quad \text{for all} \quad 1 \leq n \leq N, \tag{4}$$

where u_n and v_n are the nth columns of U and V, respectively.

The set $\mathcal{B}_{M,N}$ is defined by the vanishing of polynomials in the entries of U, V, X, and Y, namely the 3×3 minors of $X + \mathrm{i}Y$ and the polynomials $u_n^T X u_n + v_n^T X v_n - 2u_n^T Y v_n = 0$. Note that these polynomials are homogeneous in the entries of U, V and X, Y. In other words, they are invariant under scaling U and V by a non-zero scalar, and also X and Y by a non-zero scalar. Thus $\mathcal{B}_{M,N}$ is a well-defined subvariety of the given product of projective spaces. Let π_1 be the projection onto the first coordinate,

$$\pi_1 \,:\, \mathbb{P}\big(\mathbb{C}^{M\times N}\times\mathbb{C}^{M\times N}\big)\times\mathbb{P}\big(\mathbb{C}^{M\times M}_{\text{sym}}\times\mathbb{C}^{M\times M}_{\text{skew}}\big) \;\to\; \mathbb{P}\big(\mathbb{C}^{M\times N}\times\mathbb{C}^{M\times N}\big).$$

Recall that we use $X_{\mathbb{R}}$ to denote the set of real points of a complex variety X.

Proposition 3.3. *Let $\Phi = \{\phi_n\}_{n=1}^N \subset \mathbb{C}^M$ be a complex frame. Write $\phi_n = u_n + \mathrm{i}v_n$ and let U (resp. V) be the real matrix with columns u_n (resp. v_n). Then the map $\mathcal{A}_\Phi$ is injective if and only if $[U,V]$ does not belong to the projection $\pi_1((\mathcal{B}_{M,N})_{\mathbb{R}})$.*

Proof. Consider the incidence correspondence $\mathcal{I}$ of frames and Hermitian matrices given by

$$\mathcal{I} = \big\{(\Phi,Q)\in\mathbb{C}^{M\times N}\times\mathbb{C}^{M\times M}_{\text{Herm}} \;:\; Q\neq 0,\ \operatorname{rank}(Q)\le 2,\ \text{and } \phi_n^*Q\phi_n = 0 \text{ for } n=1,\dots,N\big\}.$$

Note that the conditions for $\mathcal{I}$ involve complex conjugation, an inherently real operation. Thus we cannot view $\mathcal{I}$ as a complex algebraic variety. However, complex conjugation is a polynomial on the real parts. So we decompose Φ and Q into their real and imaginary parts, i.e., $\Phi = U + \mathrm{i}V$, $\phi_n = u_n + \mathrm{i}v_n$ with $u_n, v_n \in \mathbb{R}^M$ and $Q = X + \mathrm{i}Y$, with X symmetric and Y skew symmetric. Then $\mathcal{I}$ is linearly isomorphic over $\mathbb{R}$ to the subset $\mathcal{J}$,

$$\mathcal{J} = \{(U,V,X,Y) \;:\; X+\mathrm{i}Y\neq 0,\ \operatorname{rank}(X+\mathrm{i}Y)\le 2,\ \text{and } u_n^TXu_n + v_n^TXv_n - 2u_n^TYv_n = 0\},$$

of the real vector space $\mathbb{R}^{M\times N}\times\mathbb{R}^{M\times N}\times\mathbb{R}^{M\times M}_{\text{sym}}\times\mathbb{R}^{M\times M}_{\text{skew}}$.

By Proposition 3.1, $\mathcal{A}_\Phi$ is injective if and only if (U,V) is not contained in the projection of $\mathcal{J}$ onto the first two coordinates. Since $(\mathcal{B}_{M,N})_{\mathbb{R}}$ is the projectivization of $\mathcal{J}$, (U,V) is not contained in this projection if and only if $[U,V]\notin\pi_1((\mathcal{B}_{M,N})_{\mathbb{R}})$. □

To bound the dimension of the projection $\pi_1(\mathcal{B}_{M,N})$ we find the dimension of $\mathcal{B}_{M,N}$ itself.

Theorem 3.4. *The projective complex variety $\mathcal{B}_{M,N}$ has dimension $2MN - N + 4M - 6$.*

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

$$\operatorname{rank}(Q)\le 2 \quad\text{and}\quad (u_n - \mathrm{i}v_n)^TQ(u_n+\mathrm{i}v_n) = 0 \ \text{ for all } \ 1\le n\le N,$$

where u_n and v_n are the nth columns of U and V, respectively. This is a well defined subvariety of the product of projective spaces because the defining equations are homogeneous in each set of variables.

Note that $\mathcal{B}_{M,N}$ and $\mathcal{B}'_{M,N}$ are linearly isomorphic. We can identify $\mathbb{C}^{M\times M}_{\text{sym}}\times\mathbb{C}^{M\times M}_{\text{skew}}$ with $\mathbb{C}^{M\times M}$ by the map $(X,Y)\mapsto X+\mathrm{i}Y = Q$. Indeed any complex matrix Q can be uniquely written as $Q = X+\mathrm{i}Y$ where $X = (Q+Q^T)/2$ is a complex symmetric matrix and $Y = (Q-Q^T)/(2\mathrm{i})$ is a complex skew symmetric matrix. Hence it suffices to prove that $\mathcal{B}'_{M,N}$ has the desired dimension.

We define π_1 and π_2 to be projections onto the first and second coordinates, namely

$$\pi_1\big([U,V],[Q]\big) = \ [U,V] \quad\text{and}\quad \pi_2\big([U,V],[Q]\big) = \ [Q].$$

We will determine the dimension of $\mathcal{B}'_{M,N}$ by finding the dimension of its second projection $\pi_2(\mathcal{B}'_{M,N})$ and the dimension of the preimages $\pi_2^{-1}(Q)$ for $Q\in\mathbb{C}^{M\times M}$.

The image of $\mathcal{B}'_{M,N}$ under the projection π_2 is precisely the set of rank ≤ 2 matrices in $\mathbb{P}(\mathbb{C}^{M\times M})$. To see that any rank ≤ 2 matrix Q belongs to this image, take any non-zero vector $(u,v)\in\mathbb{C}^M\times\mathbb{C}^M$ satisfying the equation $(u-\mathrm{i}v)^TQ(u+\mathrm{i}v)^T = 0$. (Such a vector exists because the zero set of this polynomial is a hypersurface in $\mathbb{C}^M\times\mathbb{C}^M$.) Now let U and

V be the matrices with N repeated columns $u_n = u$ and $v_n = v$. Then $([U,V],[Q])$ belongs to $\mathcal{B}'_{M,N}$ and $[Q]$ is its image under π_2.

The set of matrices of rank ≤ 2 in $\mathbb{C}^{M\times M}$ is an irreducible (affine) variety of dimension $4M-4$ [9, Prop. 12.2]. So its projectivization in $\mathbb{P}(\mathbb{C}^{M\times M})$ has dimension $4M-5$, meaning

$$\dim(\pi_2(\mathcal{B}'_{M,N})) \;\;=\;\; 4M-5.$$

Now fix $Q \in \pi_2(\mathcal{B}'_{M,N})$. We will show that the preimage, $\pi_2^{-1}(Q)$ in $\mathbb{P}(\mathbb{C}^{M\times N}\times\mathbb{C}^{M\times N})$ has dimension $2MN-N-1$. By Lemma 3.5 below, Q defines a nonzero polynomial equation

$$(u_n - \mathrm{i}v_n)^T Q(u_n + \mathrm{i}v_n) = 0$$

on the n-th columns of U and V. For each pair of columns (u_n, v_n), this polynomial defines a hypersurface of dimension $2M-1$ in $(\mathbb{C}^M)^2$. Thus the preimage of Q in $\mathcal{B}'_{M,N}$ is a product of N copies of this hypersurface in $((\mathbb{C}^M)^2)^N \cong (\mathbb{C}^{M\times N})^2$, one for each pair of columns (u_n, v_n) for $1 \leq n \leq N$. Therefore after projectivization, this preimage $\pi_2^{-1}(Q)$ has dimension $N(2M-1)-1 = 2MN-N-1$. We put these together using the following theorem about dimensions of projections and their fibers [9, Cor. 11.13]. It states that the dimension of the projective variety $\mathcal{B}'_{M,N}$ is the sum of the dimension of the image of the projection $\pi_2(\mathcal{B}'_{M,N})$ and the minimum dimension of a preimage $\pi_2^{-1}(Q)$. Since the dimension of the preimages is constant, we conclude that

$$\dim(\mathcal{B}'_{M,N}) \;\;=\;\; \dim(\pi_2(\mathcal{B}'_{M,N})) + \dim(\pi_2^{-1}(Q)) \;\;=\;\; (4M-5)+(2MN-N-1). \qquad \square$$

Above we used that any non-zero matrix Q imposes a nontrivial condition on each pair (u,v) of columns of U and V. We now verify this statement.

Lemma 3.5. *For a nonzero matrix $Q = (q_{\ell m}) \in \mathbb{C}^{M\times M}$, the polynomial*

$$q(u,v) \;\;=\;\; (u-\mathrm{i}v)^T Q(u+\mathrm{i}v) \;\;\in\;\; \mathbb{C}[u_1,\ldots,u_M,v_1,\ldots,v_M],$$

where $u = (u_1,\ldots,u_M)^T$ and $v = (v_1,\ldots,v_M)^T$, is not identically zero.

Proof. Computing explicitly the expression of $q(u,v)$, one has:

$$q(u,v) = \sum_{1\leq m\leq M} q_{mm}(u_m^2+v_m^2) + \sum_{1\leq \ell<m\leq M} (q_{\ell m}+q_{m\ell})(u_\ell u_m + v_\ell v_m) + \mathrm{i}(q_{\ell m}-q_{m\ell})(u_\ell v_m - v_\ell u_m).$$

If the polynomial $q(u,v)$ is identically zero, then so are its coefficients, meaning

$$\begin{aligned} q_{mm} &= 0 \quad \text{for all } 1\leq m\leq M, \\ q_{\ell m}+q_{m\ell} &= 0 \quad \text{for all } 1\leq \ell<m\leq M, \text{ and} \\ q_{\ell m}-q_{m\ell} &= 0 \quad \text{for all } 1\leq \ell<m\leq M. \end{aligned}$$

It follows that Q is the zero-matrix. $\square$

By bounding the dimension of $\mathcal{B}_{M,N}$, we can bound the dimension of its projection, which contains the frames Φ for which $\mathcal{A}_\Phi$ is not injective, and thus prove our main theorem.

Proof of Theorem 1.1. By Proposition 3.3, a pair of real $M\times N$ matrices (U,V) for which $\mathcal{A}_{U+\mathrm{i}V}$ is not injective gives a point $[U,V]$ in $\pi_1((\mathcal{B}_{M,N})_\mathbb{R}) \subset (\pi_1(\mathcal{B}_{M,N}))_\mathbb{R}$. The dimension of the projection is at most the dimension of the original variety [9, Cor. 11.13]. Thus the dimension of $\pi_1(\mathcal{B}_{M,N})$ can be bounded using Theorem 3.4:

$$\dim\big(\pi_1(\mathcal{B}_{M,N})\big) \;\leq\; \dim(\mathcal{B}_{M,N}) \;\;=\;\; 2MN+4M-6-N.$$

When N is $4M-4$ or higher, the dimension of this projection is *strictly less* than $2MN-1$, which is the dimension of $\mathbb{P}((\mathbb{C}^{M\times N})^2)$, the target of the projection π_1. Thus the image of this projection is contained in a hypersurface defined by the vanishing of some polynomial.

This still holds when we restrict to real matrices U and V. In the real vector space $(\mathbb{R}^{M\times N})^2$, there is some nonzero polynomial that vanishes on all of the pairs (U,V) for which $\mathcal{A}_{U+\mathrm{i}V}$ is not injective. The complement of the zero-set of this polynomial is a Zariski open subset of $(\mathbb{R}^{M\times N})^2$ and for any pair (U,V) in this open set, $\mathcal{A}_{U+\mathrm{i}V}$ is injective. □

4. A hypersurface containing bad frames

When $N \geq 4M-4$, the proof of our main theorem guarantees a polynomial that is zero on the set of frames Φ for which $\mathcal{A}_\Phi$ is non-injective. Here we discuss how to obtain such a polynomial and compute its degree.

Specifically, here we describe a polynomial in the variables u_{mn}, v_{mn} for $1 \leq m \leq M$ and $1 \leq n \leq N$ vanishing on the projection $\pi_1(\mathcal{B}_{M,N})$. The projection from a product of projective spaces onto one of its coordinates, $\mathbb{P}^r \times \mathbb{P}^s \to \mathbb{P}^r$, is a closed map in the Zariski topology [11, Theorem I.5.3]. Thus $\pi_1(\mathcal{B}_{M,N})$ is indeed a subvariety of $\mathbb{P}((\mathbb{C}^{M\times N})^2)$, i.e., a closed set in the Zariski topology. The equations defining this projection can be in principle computed using symbolic computations involving eliminations, saturations and resultants.

Suppose $F_0, \ldots, F_s$ be $s+1$ are homogeneous polynomials in $s+1$ variables $x_0, \ldots, x_s$ of degrees $d_0, \ldots, d_s$. We have $F_j = \sum_{\alpha\in\mathbb{N}^{s+1}, |\alpha|=d_j} c_{j\alpha}x^\alpha$ and there exists a unique polynomial in the coefficients $c_{j\alpha}$ that vanishes if and only if there exists a nontrivial solution to the equations $F_0 = \cdots = F_s = 0$. This polynomial is called the *resultant*. See Chapter 3 in [5] for an introduction to resultants and Chapters 12 and 13 in [8] for details and proofs. The problem of expressing the resultant in an efficient way, for example as a single determinant, is still a central topic in elimination theory, see for instance [6]. For computing an equation of the image of the projection of a subvariety of $\mathbb{P}^r \times \mathbb{P}^s$ given by $s+1$ bi-homogeneous equations $F_0, \ldots, F_s$ in variables $y_0, \ldots, y_r, x_0, \ldots, x_s$ to $\mathbb{P}^r$, we treat $y_0, \ldots, y_r$ as coefficients and take the resultant with respect to the variables $x_0, \ldots, x_s$.

Proposition 4.1. *There is a nonzero polynomial in* $\mathbb{R}[u_{11}, \ldots, u_{M(4M-4)}, v_{11}, \ldots, v_{M(4M-4)}]$ *vanishing on the projection* $\pi_1(\mathcal{B}_{M,4M-4})$ *which has total degree* $2\cdot(4M-4)\cdot 3^{(M-2)^2}$ *and has degree* $2\cdot 3^{(M-2)^2}$ *in the set of column variables* $\{u_{mn}, v_{mn},\ m = 1, \ldots, M\}$ *for each* n.

Proof. Let $X = (x_{\ell m})$ and $Y = (y_{\ell m})$ be $M\times M$ symmetric and skew-symmetric matrices of variables, and let Z denote this collection of these M^2 variables:

$$Z = \{x_{11}, x_{12}, \ldots, x_{1M}, x_{22}, \ldots, x_{MM}, y_{12}, y_{13}, \ldots, y_{1M}, y_{23}, \ldots, y_{M-1M}\}.$$

We will choose M^2 polynomials that vanish on $\mathcal{B}_{M,4M-4}$, so that they cut out a variety V of codimension M^2, necessarily containing $\mathcal{B}_{M,4M-4}$. By [5, Ch. 3, Theorem 2.3], the resultant of these equations with respect to the variables Z is a non-zero polynomial (since $\mathrm{codim}(V) = M^2$) that vanishes on $\pi_1(V)$. As $\mathcal{B}_{M,4M-4} \subset V$, it follows that this resultant also vanishes on $\pi_1(\mathcal{B}_{M,4M-4}) \subset \pi_1(V)$.

To choose the equations, we start with the $N = 4M-4$ equations

$$g_n \;=\; u_n^T X u_n + v_n^T X v_n - 2u_n^T Y v_n \;=0 \quad \text{ with } n = 1, \ldots, N$$

where u_n and v_n are the vector of variables $(u_{mn})_m$ and $(v_{mn})_m$. Note that g_n has degree 1 in the Z-variables and degree 2 in the u_{mn}, v_{mn} variables. We have already seen in the proof of Theorem 3.4 that each polynomial equation $g_n = 0$ cuts down the dimension by one. To this set we add the vanishing of $E = (M-2)^2$ general linear combinations (with complex coefficients) of the 3×3 minors of the matrix $X + \mathrm{i}Y$, say $G_1, \ldots, G_E$. Note that these polynomials have degree 3 in the Z-variables and degree 0 in the u_{mn}, v_{mn} variables. (For small values of M the collection of polynomials $G_1, \ldots, G_E$ can be taken to be a subset of properly chosen 3×3 minors. However for higher M one needs to take linear combinations to make sure that each equation cuts down the dimension by one.)

By [5, Ch. 3, Theorem 3.1], the resultant of homogeneous polynomials $F_0, \ldots, F_s$ of degrees $d_0, \ldots, d_s$ is homogeneous in the coefficients of F_j of degree $d_0 \cdots d_{j-1} d_{j+1} \cdots d_s$. So for each $1 \leq j \leq N$ the resultant is homogeneous of degree 3^E in the coefficients of g_j. Since the coefficients of g_j are homogeneous of degree 2 in the u_{mj}, v_{mj}, it is homogeneous of degree $2 \cdot 3^E$ in the column variables u_{mj}, v_{mj}. On the other hand, the resultant is homogeneous of degree 3^{E-1} in the coefficients of G_j, but the coefficients are of degree 0 in the u_{mn}, v_{mn} variables. Thus the resultant has total degree $2N3^E$. □

When $N > 4M-4$, for every subset $S \subset \{1, \ldots, N\}$ of size $4M-4$, we can apply the above construction to the corresponding columns of U and V. The result is a nonzero polynomial vanishing on the set of frames Φ for which $\mathcal{A}_\Phi$ is not injective and involving only the variables u_{mn}, v_{mn} where $n \in S$.

Example 4.2 ($M = 2$, $N = 4$)**.** Since all matrices in $\mathbb{C}^{2\times 2}$ have rank ≤ 2, the variety $\mathcal{B}_{2,4}$ is defined by the equations $g_n = 0$ where

$$g_n \;=\; (u_{1n}^2 + v_{1n}^2)x_{11} + 2(u_{1n}u_{2n} + v_{1n}v_{2n})x_{12} + (u_{2n}^2 + v_{2n}^2)x_{22} + 2(u_{2n}v_{1n} - u_{1n}v_{2n})y_{12}$$

for $n = 1, \ldots, 4$. These equations are linear in the variables $z_k \in Z = \{x_{11}, x_{12}, x_{22}, y_{12}\}$. Thus for fixed u_{mn}, v_{mn}, there is a nonzero solution to these equations if and only if the determinant of the Jacobian matrix

$$\left(\frac{\partial g_n}{\partial z_k}\right)_{n,k} \;=\; \begin{pmatrix} u_{11}^2 + v_{11}^2 & 2(u_{11}u_{21} + v_{11}v_{21}) & u_{21}^2 + v_{21}^2 & 2(u_{21}v_{11} - u_{11}v_{21}) \\ u_{12}^2 + v_{12}^2 & 2(u_{12}u_{22} + v_{12}v_{22}) & u_{22}^2 + v_{22}^2 & 2(u_{22}v_{12} - u_{12}v_{22}) \\ u_{13}^2 + v_{13}^2 & 2(u_{13}u_{23} + v_{13}v_{23}) & u_{23}^2 + v_{23}^2 & 2(u_{23}v_{13} - u_{13}v_{23}) \\ u_{14}^2 + v_{14}^2 & 2(u_{14}u_{24} + v_{14}v_{24}) & u_{24}^2 + v_{24}^2 & 2(u_{24}v_{14} - u_{14}v_{24}) \end{pmatrix}$$

is zero. This is the hypersurface defining $\pi_1(\mathcal{B}_{2,4})$, which has total degree 8 and degree 2 in the entries of u_n and v_n. If this determinant is *non-zero*, then the map $\mathcal{A}_{U+\mathrm{i}V}$ is injective.

Example 4.3 ($M = 3$, $N = 8$)**.** For fixed u_{mn}, v_{mn} the polynomials g_n give 8 linear equations in the 9 variables $Z = \{z_k\} = \{x_{11}, x_{12}, x_{13}, x_{22}, x_{23}, x_{33}, y_{12}, y_{13}, y_{23}\}$. We can solve for this solution symbolically. To do this consider the Jacobian matrix:

$$J = \left(\frac{\partial g_n}{\partial z_k}\right)_{n,k} \quad \text{with} \quad 1 \leq n \leq 8, \quad 1 \leq k \leq 9.$$

The solution to the equations $g_1 = \cdots = g_8 = 0$ is then given by the 8×8 sub-determinants

$$z_k \;=\; D_k \;=\; (-1)^k \det(J^{\{k\}})$$

where $J^{\{k\}}$ is obtained by erasing the k-th column of J. Note that D_k has total degree $2 \cdot 8$ and degree 2 the entries of u_n and v_n for each n. This solution gives a 3×3 matrix $X + \mathrm{i}Y$ satisfying the desired equations $g_n = 0$. In order for the pair $([U, V], [X, Y])$ to belong to

$\mathcal{B}_{3,8}$, this matrix $X + \mathrm{i}Y$ must have rank ≤ 2, meaning that its 3×3 determinant,

$$\det \begin{pmatrix} D_1 & D_2 + \mathrm{i}D_7 & D_3 + \mathrm{i}D_8 \\ D_2 - \mathrm{i}D_7 & D_4 & D_5 + \mathrm{i}D_9 \\ D_3 - \mathrm{i}D_8 & D_5 - \mathrm{i}D_9 & D_6 \end{pmatrix},$$

must vanish. The vanishing of this determinant defines $\pi_1(\mathcal{B}_{3,8})$. As promised, it has total degree $2 \cdot 8 \cdot 3 = 48$ and degree $2 \cdot 3 = 6$ in the entries of u_n and v_n for each $1 \leq n \leq 8$.

Remark 4.4. The set of frames Φ such that $\mathcal{A}_\Phi$ is not injective is $\pi_1((\mathcal{B}_{M,N})_{\mathbb{R}})$. Since projective space is compact, π_1 is a closed map with respect to the Euclidean topology. In particular, the locus of frames Φ for which $\mathcal{A}_\Phi$ is non-injective is closed in the Euclidean topology on $\mathbb{P}((\mathbb{R}^{M \times N})^2)$. Note however, that the image of the set of real points of a variety need not be Zariski closed as the example below shows. This means that there may be real points belonging to the projection $\pi_1(\mathcal{B}_{M,N})$ which are not the projection of real points of $\mathcal{B}_{M,N}$. That is, in principle there may be a real point $[U, V]$ in $\pi_1(\mathcal{B}_{M,N})$ whose corresponding frame $\Phi = U + \mathrm{i}V$ is nonetheless injective.

Example 4.5. Let $C \subset \mathbb{C}^2$ be the parabola defined by $x^2 = y$ and let $\pi \colon C \to \mathbb{C}^1$ be the projection onto the second factor. Since every real number has a complex square root, every point in $\mathbb{R}$ is the image of a point of C. However, if $a < 0$ then a is not image of a real point of C. In particular the image of $C_{\mathbb{R}}$ is the closed subset $\{a \geq 0\} \subset \mathbb{R}$. Any polynomial vanishing on $\pi(C_{\mathbb{R}})$ vanishes on all of $\mathbb{R}$, so the Zariski closure of $\pi(C_{\mathbb{R}})$ is all of $\mathbb{R}$.

5. The case of fewer measurements

Here we use our algebraic reformulation to discuss some cases of part (a) of the $4M - 4$ Conjecture. We show that when $N \leq 4M - 5$ the projection $\pi_1(\mathcal{B}_{M,N})$ fills the entire space and show that the projection of the real points $(\mathcal{B}_{M,N})_{\mathbb{R}}$ does this in the case $M = 2^k + 1$.

Proposition 5.1. *If $N \leq 4M - 5$, then for every $[U, V] \in \mathbb{P}(\mathbb{C}^{M \times N})^2$, the preimage under the first projection $\pi_1^{-1}([U, V])$ is a non-empty variety of degree*

$$d_{M,2} \;=\; \prod_{i=0}^{M-3} \frac{\binom{M+i}{2}}{\binom{2+i}{2}}. \tag{5}$$

In particular, the projection $\pi_1(\mathcal{B}_{M,N})$ is all of $\mathbb{P}((\mathbb{C}^{M \times N})^2)$.

Proof. Fix U and V in $\mathbb{C}^{M \times N}$. Each pair of columns u_n and v_n define (at most) one linear condition on an $M \times M$ matrix Q, namely that $(u_n - \mathrm{i}v_n)^T Q (u_n + \mathrm{i}v_n) = 0$. Thus in total U and V define (at most) N linear conditions. The subvariety of $\mathbb{P}(\mathbb{C}^{M \times M})$ of matrices satisfying these linear conditions is a linear subspace

$$L_\Phi \;=\; \{Q \in \mathbb{P}(\mathbb{C}^{M \times M}) \;:\; (u_n - \mathrm{i}v_n)^T Q (u_n + \mathrm{i}v_n) = 0 \quad \text{for each} \quad 1 \leq n \leq N\}$$

of dimension at least $M^2 - 1 - N$.

On the other hand, the projective variety $H_2 \subset \mathbb{P}(\mathbb{C}^{M \times M})$ of matrices of rank ≤ 2 has dimension $4M - 5$ [9, Prop. 12.2]. When $N \leq 4M - 5$,

$$\dim L_\Phi \;+\; \dim H_2 \;\geq\; M^2 - 1.$$

Thus by [9, Prop. 11.4], there is a point in the intersection $L_\Phi \cap H_2$. Since the degree of H_2 is $d_{M,2}$ (see for example [9, Ex. 19.10]), it follows that the degree of $L_\Phi \cap H_2$ is also $d_{M,2}$. Note that $L_\Phi \cap H_2$ is the preimage of the first projection of the variety $\mathcal{B}'_{M,N}$ introduced in the beginning of the proof of Theorem 3.4. As noted in the same proof, $\mathcal{B}'_{M,N}$ is linearly isomorphic to $\mathcal{B}_{M,N}$. This isomorphism preserves the fibers under the first projection. Thus the claims follow. □

Recall from Proposition 3.3 that Part (a) of the $4M-4$ Conjecture is equivalent to saying that when $N \leq 4M-5$, we have $\pi_1((\mathcal{B}_{M,N})_{\mathbb{R}}) = \mathbb{P}((\mathbb{R}^{M\times N})^2)$. In other words, for $[U,V]$ real, $\pi_1^{-1}([U,V])$ contains a real point, or equivalently the variety $L_\Phi \cap H_2$ introduced in the proof of Proposition 5.1 contains a Hermitian matrix. In particular, if we could show that for $N \leq 4M-5$ we have $(\pi_1(\mathcal{B}_{M,N}))_{\mathbb{R}} \subset \pi_1((\mathcal{B}_{M,N})_{\mathbb{R}})$ Proposition 5.1 would imply part (a) of the $4M-4$ conjecture. Unfortunately, as noted in Example 4.5 in general the image of the set of real points of a variety need not equal the set of real points of the image. Despite this subtlety, there is one case where we can use algebro-geometric methods to prove part (a) of the $4M-4$ Conjecture.

Proposition 5.2. *If $M = 2^k+1$ and $N \leq 4M-5$, then $\mathcal{A}_\Phi$ is not injective.*

Proof. By the discussion in the preceeding paragraph, we have to show that for every $[U,V]$ in $\mathbb{P}(\mathbb{R}^{M\times N} \times \mathbb{R}^{M\times N})$ the preimage $\pi_1^{-1}([U,V])$ contains a real point. By Proposition 5.1 the degree of this preimage is $d_{M,2}$, and by Lemma 5.3 below, $d_{M,2}$ is odd when $M = 2^k+1$. Hence the claim follows from the fact that any projective variety defined over $\mathbb{R}$ and having odd degree has real point.[1] □

Lemma 5.3. *When $M = 2^k+1$, the degree $d_{M,2}$ of the variety of $M \times M$ matrices of rank ≤ 2 is odd.*

Proof. Recall the definition of $d_{M,2}$ in (5). Let $s_p(n)$ denote the sum of the digits in the base p expansion of n. Legendre's formula says that the highest power of a prime dividing $n!$ is given by $(n - s_p(n))/(p-1)$. Thus $(s_p(n-2)+s_p(2)-s_p(n))/(p-1)$ is the highest power of p dividing $\binom{n}{2}$. Using this formula we see that the highest power of 2 dividing $d_{M,2}$ is

$$\left(\sum_{i=0}^{M-3} s_2(M+i-2) - s_2(M+i)\right) - \left(\sum_{i=0}^{M-3} s_2(i) - s_2(i+2)\right). \tag{6}$$

Since $M = 2^k+1$ we know that for $0 \leq n \leq M-2$ we have that $s_2(M-1+n) = s_2(n)+1$. Thus the expression (6) simplifies to

$$\begin{aligned} s_2(M-2) - s_2(M) + \left(\sum_{i=1}^{M-3} s_2(i-1) - s_2(i+1)\right) - \left(\sum_{i=0}^{M-3} s_2(i) - s_2(i+2)\right) \\ = s_2(M-2) - s_2(M) - s_2(M-3) + s_2(M-1). \end{aligned} \tag{7}$$

When $M = 2^k+1$, we can see that $s_2(M) = 2$, $s_2(M-1) = 1$, $s_2(M-2) = k$ and $s_2(M-3) = k-1$. Hence the expression in (7) is zero and $d_{M,2}$ is odd. □

Example 5.4 ($M = 2,\ N = 3$)**.** As shown in [2], here part (a) of the $4M-4$ Conjecture holds, meaning that the intersection $L_\Phi \cap H_2$ contains a Hermitian matrix. Every matrix has rank ≤ 2, H_2 is all of $\mathbb{C}^{2\times 2}$, and $d_{2,2} = 1$. The projective linear space L_Φ is nonempty

[1] When the dimension of the variety is zero, this follows from the fact that such a variety is invariant under complex conjugation, so an odd number of points must contain a fixed point under complex conjugation which must be real. In higher dimensions, the result follows from the zero-dimensional case by intersecting with a subspace of complementary dimension that is defined over $\mathbb{R}$.

and invariant under the involution $Q \mapsto Q^*$. So it contains a Hermitian matrix. In this case, we recover the first part of the $4M-4$ conjecture from Proposition 5.1 and Proposition 3.3.

Example 5.5 ($M = 3,\ N = 7$)**.** As shown in [2], here part (a) of the $4M-4$ Conjecture holds. The variety of rank ≤ 2 matrices is defined by the 3×3 determinant, meaning $d_{3,2} = 3$. Thus for generic $U, V \in \mathbb{R}^{3\times 7}$, the intersection $L_\Phi \cap H_2$ contains three complex matrices. Since this intersection is invariant, at least one of these must be fixed under the involution $Q \mapsto Q^*$. So in this case, we also recover the first part of the $4M-4$ conjecture from Proposition 5.1 and Proposition 3.3.

Remark 5.6. Proposition 5.2 is similar to, but does not seem to follow from, previous results [7, 10]. Heinosaari, Mazzarella and Wolf use embedding results from topology to show that when $N \leq 4M - 2s_2(M-1) - 4$, the map $\mathcal{A}_\Phi$ is never injective [10]. In particular, if $M = 2^k+1$ then $s_2(M-1) = 1$, and this bound gives $N \leq 4M-6$, rather than $N \leq 4M-5$.

We end by rephrasing part (a) of the $4M-4$ Conjecture. The first open case is $M = 4$.

Conjecture 5.7. *Let $\phi_1, \ldots, \phi_{4M-5} \in \mathbb{C}^M$ and consider the linear space L_Φ of $\mathbb{C}^{M\times M}_{\text{Herm}}$,*

$$L_\Phi \ = \ \{Q \ : \ \phi_n^* Q \phi_n = 0 \ \ \textit{for } n = 1, \ldots, 4M-5\} \ = \ \operatorname{span}\{\phi_1\phi_1^*, \ldots, \phi_{4M-5}\phi_{4M-5}^*\}^\perp.$$

The $4M-4$ Conjecture states that $L_\Phi \subset \mathbb{C}^{M\times M}_{\text{Herm}}$ always contains a matrix of rank ≤ 2. In other words, if we take $d = (M-2)^2+1$ Hermitian matrices $A_1, \ldots, A_d$ spanning L_Φ, there is some linear combination $x_1A_1 + \ldots + x_dA_d$ with rank two.

Acknowledgements. We are very grateful to the conference held at the AIM conference "Frame theory intersects geometry" held in Summer 2013 and many of the people attending. Among others, we would especially like to thank Bernhard Bodmann, Jameson Cahill, Matthew Fickus, Dustin Mixon, and Vlad Voroninski for helpful discussions. Aldo Conca would like to thank Carlos D'Andrea and Laurent Busé for useful discussions concerning elimination and discriminants. Milena Hering was supported by NSF grant DMS-1001859. Cynthia Vinzant was supported by an NSF postdoc DMS-1204447.

References

[1] Radu Balan, Pete Casazza, and Dan Edidin. On signal reconstruction without phase. *Appl. Comput. Harmon. Anal.*, 20(3):345–356, 2006.

[2] A. Bandeira, J. Cahill, D. Mixon, and A. Nelson. Saving phase: Injectivity and stability for phase retrieval. *arXiv:1302.4618*, 2013.

[3] B. Bodmann and N. Hammen. Stable phase retrieval with low-redundancy frames. *arXiv:1302.5487*, 2013.

[4] David Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer, New York, third edition, 2007. An introduction to computational algebraic geometry and commutative algebra.

[5] David A. Cox, John Little, and Donal O'Shea. *Using algebraic geometry*, volume 185 of *Graduate Texts in Mathematics*. Springer, New York, second edition, 2005.

[6] Carlos D'Andrea and Alicia Dickenstein. Explicit formulas for the multivariate resultant. *J. Pure Appl. Algebra*, 164(1-2):59–86, 2001. Effective methods in algebraic geometry (Bath, 2000).

[7] Donald M. Davis. Some new immersion results for complex projective space. *Proc. Edinb. Math. Soc. (2)*, 51(1):45–56, 2008.

[8] I. M. Gel′fand, M. M. Kapranov, and A. V. Zelevinsky. *Discriminants, resultants, and multidimensional determinants*. Mathematics: Theory & Applications. Birkhäuser Boston Inc., Boston, MA, 1994.

[9] 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.

[10] Teiko Heinosaari, Luca Mazzarella, and Michael M. Wolf. Quantum tomography under prior information. *Comm. Math. Phys.*, 318(2):355–374, 2013.

[11] Igor R. Shafarevich. *Basic algebraic geometry. 1*. Springer-Verlag, Berlin, second edition, 1994. Varieties in projective space, Translated from the 1988 Russian edition and with notes by Miles Reid.

Aldo Conca (conca@dima.unige.it)
Department of Mathematics,
University of Genova,
Via Dodecaneso 35,
I-16146 Genova, Italy

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

Milena Hering (m.hering@ed.ac.uk)
School of Mathematics and Maxwell Institute of Mathematics,
University of Edinburgh,
Edinburgh, EH9 3JZ, UK

Cynthia Vinzant (vinzant@umich.edu)
Department of Mathematics,
University of Michigan,
Ann Arbor, MI 48109, USA