GENERALIZED PHASE RETRIEVAL: MEASUREMENT NUMBER, MATRIX RECOVERY AND BEYOND

YANG WANG AND ZHIQIANG XU

Abstract. In this paper, we develop a framework of generalized phase retrieval in which one aims to reconstruct a vector $\mathbf{x}$ in $\mathbb{R}^d$ or $\mathbb{C}^d$ through quadratic samples $\mathbf{x}^*A_1\mathbf{x}, \dots, \mathbf{x}^*A_N\mathbf{x}$. The generalized phase retrieval includes as special cases the standard phase retrieval as well as the phase retrieval by orthogonal projections. We first explore the connections among generalized phase retrieval, low-rank matrix recovery and nonsingular bilinear form. Motivated by the connections, we present results on the minimal measurement number needed for recovering a matrix that lies in a set $W \in \mathbb{C}^{d\times d}$. Applying the results to phase retrieval, we show that generic $d \times d$ matrices $A_1, \dots, A_N$ have the phase retrieval property if $N \geq 2d-1$ in the real case and $N \geq 4d-4$ in the complex case for very general classes of $A_1, \dots, A_N$, e.g. matrices with prescribed ranks or orthogonal projections. We also give lower bounds on the minimal measurement number required for generalized phase retrieval. For several classes of dimensions d we obtain the precise values of the minimal measurement number. Our work unifies and enhances results from the standard phase retrieval, phase retrieval by projections and low-rank matrix recovery.

1. Introduction

1.1. **Problem Setup.** The *phase retrieval* problem is to recover signals from the magnitude of the observations. It has important applications in imaging, optics, quantum tomography, communication, audio signal processing and more, and it has grown into one of the major areas of research in recent years (see e.g. [3, 7, 11, 12, 17, 19, 22] and the references therein). First we state the phase retrieval problem. In the finite dimensional Hilbert space $\mathbb{F}^d$, where $\mathbb{F} = \mathbb{R}$ or $\mathbb{F} = \mathbb{C}$, a set of elements $\{\mathbf{f}_1, \dots, \mathbf{f}_N\}$ in $\mathbb{F}^d$ is called a *frame* if it spans $\mathbb{F}^d$. Given this frame any vector $\mathbf{x} \in \mathbb{F}^d$ can be reconstructed from the inner products $\{\langle \mathbf{x}, \mathbf{f}_1\rangle, \dots, \langle \mathbf{x}, \mathbf{f}_N\rangle\}$. The *standard version* of the phase retrieval problem in $\mathbb{F}^d$ is: Let $\{\mathbf{f}_1, \dots, \mathbf{f}_N\}$ be a subset in the finite dimensional Hilbert space $\mathbb{F}^d$. Is it possible to reconstruct a vector $\mathbf{x} \in \mathbb{F}^d$ from $\{|\langle \mathbf{x}, \mathbf{f}_1\rangle|, \dots, |\langle \mathbf{x}, \mathbf{f}_N\rangle|\}$, i.e. from only the magnitude of the inner products? To do that, the set $\{\mathbf{f}_1, \dots, \mathbf{f}_N\}$ must be a frame because otherwise one can find a nonzero $\mathbf{x}$ such that it is orthogonal to all $\mathbf{f}_j, j = 1, \dots, N$. Furthermore if

2010 *Mathematics Subject Classification.* Primary 42C15, Secondary 94A12, 15A63, 15A83 .

Key words and phrases. Phase Retrieval, Frames, Fusion Frames, Fourier Transform, Measurement Number, Low Rank Matrix Recovery, Bilinear Form, Embedding .

Yang Wang was supported in part by the Hong Kong Research Grant Council grant 16306415. Zhiqiang Xu was supported by NSFC grant (11422113,91630203, 11331012) and by National Basic Research Program of China (973 Program 2015CB856000).

$\mathbf{x}' = b\mathbf{x}$ where $|b| = 1$ then $|\langle \mathbf{x}, \mathbf{f}_j\rangle| = |\langle \mathbf{x}', \mathbf{f}_j\rangle|$ for all $j = 1, \dots, N$, and hence $\mathbf{x}$ and $\mathbf{x}'$ cannot be distinguished from the magnitude of the inner products. Thus all reconstructions from magnitudes, if it is possible, should only be up to a unimodular constant.

1.1.1. *Generalized Phase Retrieval.* There have been significant advances in the study of this standard version of the phase retrieval problem. On the one hand, many theoretical results are presented. Particularly, the problem of finding the minimal measurement number for phase retrieval has attracted a lot of attention [4, 3, 22, 12, 37, 38]. On the other hand, efficient and numerically stable algorithms have been developed to solve for phase retrieval (see [11, 10]).

In this paper, we focus on the more theoretical side of a *generalized version* of the phase retrieval problem. The standard phase retrieval problem is to reconstruct a $\mathbf{x} \in \mathbb{F}^d$ up to a unimodular constant from the measurements $\{\mathbf{x}^*\mathbf{f}_j\mathbf{f}_j^*\mathbf{x} = |\langle \mathbf{x}, \mathbf{f}_j\rangle|^2\}_{j=1}^N$. Set $A_j = \mathbf{f}_j\mathbf{f}_j^*$. Then the problem is to reconstruct $\mathbf{x}$ from the measurements $\{\mathbf{x}^*A_j\mathbf{x}\}_{j=1}^N$, where A_j are positive semidefinite and $\operatorname{rank}(A_j) = 1$. In the generalized phase retrieval problem, the restrictions on A_j are relaxed and replaced, and one aims to reconstruct $\mathbf{x}$ up to a unimodular constant from more general *quadratic measurements* $\{\mathbf{x}^*A_j\mathbf{x}\}_{j=1}^N$.

Let $\mathbf{H}_d(\mathbb{F})$ denote the set of $d \times d$ Hermitian matrices over $\mathbb{F}$ (if $\mathbb{F} = \mathbb{R}$ then Hermitian matrices are symmetric matrices). As with the standard phase retrieval problem we consider the equivalence relation $\sim$ on $\mathbb{F}^d$: $\mathbf{x}_1 \sim \mathbf{x}_2$ if there is a constant $b \in \mathbb{F}$ with $|b| = 1$ such that $\mathbf{x}_1 = b\mathbf{x}_2$. Let $\underline{\mathbb{F}^d} := \mathbb{F}^d/\sim$. We shall use $\underline{\mathbf{x}}$ to denote the equivalent class containing $\mathbf{x}$. For any given $\mathcal{A} = (A_j)_{j=1}^N \subset \mathbf{H}_d(\mathbb{F})$ define the map $\mathbf{M}_\mathcal{A} : \underline{\mathbb{F}^d} \longrightarrow \mathbb{R}^N$ by

$$\mathbf{M}_\mathcal{A}(\underline{\mathbf{x}}) = (\mathbf{x}^*A_1\mathbf{x}, \dots, \mathbf{x}^*A_N\mathbf{x}). \tag{1.1}$$

Thus the *generalized phase retrieval problem* asks whether we can reconstruct $\underline{\mathbf{x}} \in \underline{\mathbb{F}^d}$ from $\mathbf{M}_\mathcal{A}(\underline{\mathbf{x}})$. We should observe that $\mathbf{M}_\mathcal{A}$ can also be viewed as a map from $\mathbb{F}^d$ to $\mathbb{R}^N$, and we shall often do this when there is no confusion.

Definition 1.1. Let $\mathcal{A} = (A_j)_{j=1}^N \subset \mathbf{H}_d^N(\mathbb{F})$. We say $\mathcal{A}$ has the *phase retrieval property* or is *phase retrievable (PR)* if $\mathbf{M}_\mathcal{A}$ is injective on $\underline{\mathbb{F}^d}$.

Note that the generalized phase retrieval problem includes the standard phase retrieval problem as a special case, with the additional restrictions $A_j \succeq 0$ and $\operatorname{rank}(A_j) = 1$. It also includes the so-called *fusion frame (or projection) phase retrieval* as a special case where each A_j is an orthogonal projection matrix, namely $A_j^2 = A_j$ [17, 8, 1]. Moreover, it is very closely related to and a generalization of the problem of information completeness

of positive operator valued measures (POVMs) with respect to pure states in quantum tomography [22], where the norm of the vector we try to recover $\mathbf{x} \in \mathbb{C}^d$ is assumed to be 1. So in essence information completeness of POVMs with respect to pure states is a special case of generalized phase retrieval in $\mathbb{C}^d$ in which one of the measurement matrix A_j is the identity matrix I_d. The generalized phase retrieval problem, just like the standard phase retrieval problem, has in fact several flavors involving different subtleties, some of which will be discussed later in the paper. One of the most fascinating aspect of generalized phase retrieval is its close connections to other areas in mathematics, which include matrix recovery, nonsingular bilinear form, composition of quadratic forms and the embedding problem in topology.

This paper attempts to lay down a foundation for generalized phase retrieval by establishing several fundamental properties. Of particular interest is the various minimality problems for generalized phase retrieval, and its connections to matrix recovery and nonsingular bilinear form. We list some of them below:

Minimality Questions for Generalized Phase Retrieval: *Let $\mathcal{A} = (A_j)_{j=1}^N \subset \mathbf{H}_d^N(\mathbb{F})$. What is the smallest N so that a generic $\mathcal{A} = (A_j)_{j=1}^N$ has the phase retrieval property in $\mathbb{F}^d$?*

There can also be numerous variants of those aforementioned questions. For example, what if we require that all $A_j \succeq 0$? What if we prescribe the ranks for all A_j? We can obviously impose various special restrictions on A_j, and any such restrictions may alter the answer to each of the above questions.

1.1.2. *Generalized Matrix Recovery.* Note that $\mathbf{x}^* A_j \mathbf{x} = \mathrm{Tr}(A_j \mathbf{x}\mathbf{x}^*)$. The generalized phase retrieval problem is equivalent to the recovery of the rank one Hermitian matrix $\mathbf{x}\mathbf{x}^*$ from $(\mathrm{Tr}(A_1\mathbf{x}\mathbf{x}^*), \ldots, \mathrm{Tr}(A_N\mathbf{x}\mathbf{x}^*))$, which establishes a natural connection between generalized phase retrieval and low-rank matrix recovery. The connection is observed in [11] and Candès, Strohmer and Voroninski use it to study the standard phase retrieval. This method is called *PhaseLift*.

The *low-rank matrix recovery* problem is an active research area in recent years and has arisen in many important applications such as image processing, recommender systems and Euclidean embedding and more. The goal of low-rank matrix recovery is to recover $Q \in \mathbb{C}^{d\times d}$ with $\mathrm{rank}(Q) \leq r$ from linear observation $(\mathrm{Tr}(A_1Q), \ldots, \mathrm{Tr}(A_NQ)) \in \mathbb{F}^N$ for some given $A_1, \ldots, A_N$. Depending on the problem and application, one imposes various special restrictions on A_j and Q, e.g. all matrices $A_1, \ldots, A_N$ have rank one [9, 39], and/or

some of entries of Q are 0 etc. The generalized phase retrieval leads us naturally to the following generalized matrix recovery problem:

Generalized Matrix Recovery Problem: *Let $L : \mathbb{F}^{d\times d}\times\mathbb{F}^{d\times d} \to \mathbb{F}$ be a bilinear function. Let $W \subset \mathbb{F}^{d\times d}$ and $V_j \subset \mathbb{F}^{d\times d}$ for $j = 1, \dots, N$. Assume that $\mathcal{A} = (A_j)_{j=1}^N$ with $A_j \in V_j$. Can we reconstruct any $Q \in W$ from $\mathbf{M}_{\mathcal{A}}(Q) := (L(A_1, Q), \dots, L(A_N, Q)) \in \mathbb{F}^N$?*

In this paper, the sets V_j and W above will be taken to be algebraic varieties in $\mathbb{F}^{d\times d}$. We also require that $W - W \subset \mathbb{F}^{d\times d}$ is an algebraic variety, where

$$W - W \ := \ \{\mathbf{x} - \mathbf{y} : \text{ for all } \mathbf{x}, \mathbf{y} \in W\}.$$

Low-rank matrix recovery under different conditions usually becomes a special cases of the generalized matrix recovery problem in this setting. We list some examples here:

- Let
$$\mathcal{M}_{d,r}(\mathbb{F}) := \Big\{Q \in \mathbb{F}^{d\times d} : \operatorname{rank}(Q) \le r\Big\}, \qquad \mathbb{F} = \mathbb{C} \text{ or } \mathbb{R}.$$
Note that $\operatorname{rank}(Q) \le r$ is equivalent to the vanishing of all $(r+1)\times(r+1)$ minors of Q and that these $(r+1)\times(r+1)$ minors are homogeneous polynomials in the entries of Q. Hence, $\mathcal{M}_{d,r}(\mathbb{F})$ is an algebraic variety in $\mathbb{F}^{d\times d}$, which is an *affine determinantal variety* (See Section 3.2 for detail). If we take $W = \mathcal{M}_{d,r}(\mathbb{F})$, then the generalized matrix recovery problem is the rank r matrix recovery problem.
- If V_j is the algebraic variety containing matrices of rank ≤ 1 then matrix recovery problem becomes the problem of matrix recovery by rank one projections [9].
- An interesting and important problem is the recovery of low-rank sparse matrices. Set
$$\Sigma_{d,k}(\mathbb{F}) := \Big\{Q \in \mathbb{F}^{d\times d} : \|Q\|_0 \le k\Big\}, \qquad \mathbb{F} = \mathbb{C} \text{ or } \mathbb{R},$$
where $\|Q\|_0$ denotes the nonzero entries of Q. Then $Q \in \Sigma_{d,k}$ if and only if the product of any $k+1$ entries in Q vanishes which implies $\Sigma_{d,k}$ is an algebraic variety. Thus the recovery of sparse matrices is a special case of generalized matrix recovery by taking $W = \Sigma_{d,k}(\mathbb{F})$ or $W = \Sigma_{d,k}(\mathbb{F}) \cap \mathcal{M}_{d,r}(\mathbb{F})$.
- We often meet the case where the measurement matrix is a Hermitian matrix. The Hermitian matrix set $\mathbf{H}_d(\mathbb{C})$ is *not* an algebraic variety but we can transform it to the setting with $V_j = \mathbb{R}^{d\times d}$ by choosing an appropriate bilinear function L. Define a linear map $\tau : \mathbb{C}^{d\times d} \longrightarrow \mathbb{C}^{d\times d}$ by

$$\tau(A) = \frac{1}{2}(A + A^T) + \frac{i}{2}(A - A^T). \tag{1.2}$$

It is easy to see that τ restricted on $\mathbb{R}^{d\times d}$ is an isomorphism from $\mathbb{R}^{d\times d}$ to $\mathbf{H}_d(\mathbb{C})$. Set $L(A_j, Q) := \mathrm{Tr}(\tau(A_j)Q)$. Then we can take $V_j = \mathbb{R}^{d\times d}$ which is a real algebraic variety.

Minimality Question for Generalized Matrix Recovery: *Let $L : \mathbb{F}^{d\times d} \times \mathbb{F}^{d\times d} \to \mathbb{F}$ be a bilinear form. Let $V_j \subset \mathbb{F}^{d\times d}$ for $j = 1, \dots, N$ and $W \subset \mathbb{F}^{d\times d}$ be algebraic varieties. Assume that $\mathcal{A} = (A_j)_{j=1}^N$ with $A_j \in V_j$. Under what conditions can we reconstruct any $Q \in W$ from $\mathbf{M}_{\mathcal{A}}(Q) := (L(A_1, Q), \dots, L(A_N, Q)) \in \mathbb{F}^N$? In particular, what is the smallest N so that $\mathbf{M}_{\mathcal{A}}$ is injective on W for a generic $\mathcal{A} = (A_j)_{j=1}^N \in V_1 \times \cdots \times V_N$?*

Note that $\mathbf{M}_{\mathcal{A}}$ is injective on W if and only if, for $Q \in W - W$, $\mathbf{M}_{\mathcal{A}}(Q) = 0$ implies that $Q = 0$. Throughout the rest of this paper, to state conveniently, we abuse the notations and still use W to denote $W - W$. We will employ algebraic method to investigate the smallest N so that $\{Q \in W : \mathbf{M}_{\mathcal{A}}(Q) = 0\}$ only contains the zero point which implies the answer for the question above. The results will play an important role in generalized phase retrieval.

1.2. **Related Results.**

1.2.1. *Phase Retrieval and Matrix Recovery.* For the standard phase retrieval with $\mathbb{F} = \mathbb{R}$ the minimality question is relatively straightforward. Let $\mathcal{A} = (A_j)_{j=1}^N \subset \mathbf{H}_d(\mathbb{R})$ such that $A_j = \mathbf{f}_j\mathbf{f}_j^*$ for some $\mathbf{f}_j \in \mathbb{R}^d$. Then it is easy to prove that the smallest N for which $\mathcal{A}$ can have the phase retrieval property is $N = 2d - 1$, which is also the smallest number that a generic such $\mathcal{A}$ with N elements has the phase retrieval property [3]. However, once we remove the $\mathrm{rank}(A_j) = 1$ condition the answers are already different. For example for fusion frame phase retrieval in $\mathbb{R}^d$, it is known that a generic choice of $N = 2d - 1$ orthogonal projections $\mathcal{A} = (P_j)_{j=1}^N$ with $0 < \mathrm{rank}(P_j) < d$ has the phase retrieval property [8, 17], but the smallest such N remains unknown in general. For $d = 4$, it is known that there exists a fusion frame $\mathcal{A} = (P_j)_{j=1}^N$ with $N = 6 = 2d - 2$ [40] having the phase retrieval property. In this paper, we shall show the number $N = 6$ is tight for $d = 4$.

In the complex case $\mathbb{F} = \mathbb{C}$, the same question remains open for the standard phase retrieval. It is known that in the standard phase retrieval setting, $N \geq 4d - 4$ generic matrices $\mathcal{A} = (A_j)_{j=1}^N \subset \mathbf{H}_d(\mathbb{C})$ where $A_j = \mathbf{f}_j\mathbf{f}_j^*$ have the phase retrieval property [4, 12]. Moreover, the $N = 4d - 4$ is also minimal if $d = 2^k + 1$ where $k \geq 1$ [12]. Vinzant in [37] has constructed an example in $d = 4$ with $N = 11 = 4d - 5 < 4d - 4$ matrices $A_j = \mathbf{f}_j\mathbf{f}_j^*$ such that $\mathcal{A} = (A_j)_{j=1}^{11}$ is phase retrievable in $\mathbb{C}^4$. The construction is done through the use of computational algebra tools and packages. This result implies that $N = 4d - 4$ is not

minimal for some d for the standard phase retrieval. So far, the smallest N is not known even for $d = 4$. In the other direction, a lower bound $N \geq 4d - 3 - 2\alpha$ for the minimal N is given in [22], where α denotes the number of 1's in the binary expansion of $d - 1$. This was the best known lower bound for standard phase retrieval.

Recall that we use $\mathcal{M}_{d,r}(\mathbb{F})$ to denote the set of $d \times d$ matrices in $\mathbb{F}^{d\times d}$ with rank $\leq r$. For low-rank matrix recovery, any $Q \in \mathcal{M}_{d,r}(\mathbb{F})$ can be recovered from $(\mathrm{Tr}(A_jQ))_{j=1}^N$ with probability 1 if $N \geq 4dr - 4r^2$, where the matrices $A_1, \ldots, A_N$ are i.i.d. Gaussian random matrices, provided $r \leq d/2$. It was also conjectured in [18] that $N = 4dr - 4r^2$ is the minimal N for which there exists $\mathcal{A} = (A_j)_{j=1}^N$ so that $\mathbf{M}_{\mathcal{A}}$ is injective on $\mathcal{M}_{d,r}(\mathbb{F})$. In [40], the author proved the conjecture for $\mathbb{F} = \mathbb{C}$ and disproved it for $\mathbb{F} = \mathbb{R}$, showing the existence of $\mathcal{A} = (A_j)_{j=1}^{11}$ for which $\mathbf{M}_{\mathcal{A}}$ is injective on $\mathcal{M}_{4,1}(\mathbb{R})$.

1.2.2. *Nonsingular Bilinear Form.* As we will show in Theorem 2.1, $\mathcal{A} = (A_j)_{j=1}^N \subset \mathbf{H}_d^N(\mathbb{R})$ having the phase retrieval property is equivalent to the corresponding bilinear form $(\mathbf{x}^T A_j \mathbf{y})_{j=1}^N$ being nonsingular. This connection has led us to also study nonsingular bilinear form, an area with deep historical roots. Consider the bilinear form $\mathbf{L} : \mathbb{R}^p \times \mathbb{R}^q \to \mathbb{R}^N$ given by $\mathbf{L}(\mathbf{x}, \mathbf{y}) = (\mathbf{x}^T B_1 \mathbf{y}, \ldots, \mathbf{x}^T B_N \mathbf{y}) \in \mathbb{R}^N$ where $\mathbf{x} \in \mathbb{R}^p, \mathbf{y} \in \mathbb{R}^q$ and $B_j \in \mathbb{R}^{p\times q}$. We shall call (p, q, N) the *size* of $\mathbf{L}$. The bilinear form is *nonsingular* if $\mathbf{L}(\mathbf{x}, \mathbf{y}) = 0$ implies $\mathbf{x} = 0$ or $\mathbf{y} = 0$; it is *normed* if $|\mathbf{L}(\mathbf{x}, \mathbf{y})| = |\mathbf{x}| \cdot |\mathbf{y}|$. A simple observation is that if $\mathbf{L}$ is normed then it is nonsingular. We use $p\#q$ to denote the minimal N for which there exist $B_1, \ldots, B_N$ such that the corresponding bilinear form is nonsingular. The function $p\#q$ appears in the study of the composition of quadratic forms and the immersion problem [35, 34]. It is well-known that $2\#2 = 2$. In 1748, Euler found a normed bilinear form with size $(4, 4, 4)$ in his attempt to prove Fermat's Last Theorem [34], which implies $4\#4 = 4$. Degen proved $8\#8 = 8$ in 1818. The exact values of $p\#q$ for some small $p, q \leq 32$ are known and can be found in [34]. However, finding the exact value for $p\#q$ in general is a very hard problem. A well-known necessary condition for the existence of a nonsingular bilinear form of size (p, q, N) is the Stiefel-Hopf condition, proved by Hopf and Stiefel independently in 1941 (see also [15, 28]).

Theorem 1.1. *(Stiefel-Hopf) If there exists a nonsingular bilinear form of size (p, q, N) then the binomial coefficient $\binom{N}{k}$ is even whenever $N - q + 1 \leq k \leq p - 1$.*

In the generalized phase retrieval setting we always require $p = q = d$ together with the additional requirement that matrices $B_j, j = 1, \ldots, N$, are symmetric. Thus for our study we are interested in the minimal N for which there exists a nonsingular symmetric bilinear

form of size (d, d, N). This is a stronger requirement so $N \geq d\#d$ and (d, d, N) should satisfy the Stiefel-Hopf condition.

1.3. **Our Contribution.** Our study focuses on the number of measurements needed to achieve generalized phase retrieval and other related questions. For these purposes we use the notation $\mathfrak{m}_{\mathbb{F}}(d)$ to denote minimal N for which phase retrieval property is possible:

$$\mathfrak{m}_{\mathbb{F}}(d) := \min\Big\{N : \quad \text{there exists a phase retrievable } \mathcal{A} = (A_j)_{j=1}^N \subset \mathbf{H}_d^N(\mathbb{F}) \text{ in } \mathbb{F}^d\Big\}.$$

We use algebraic methods to study the measurement number N for which a generic $\mathcal{A} = (A_j)_{j=1}^N$ has the phase retrieval property. We also present an upper bound for $\mathfrak{m}_{\mathbb{F}}(d)$. Meanwhile a lower bound for $\mathfrak{m}_{\mathbb{F}}(d)$ is obtained using results on the embedding of projective spaces into real spaces. These results also show a direct link among phase retrieval, matrix recovery and nonsingular bilinear form. In Section 2, we give several equivalent formulations for generalized phase retrieval, where we establish its close connection to nonsingular bilinear form and matrix recovery. In Section 3, we investigate the number of measurements needed for generalized matrix recovery, by showing that $N = \dim(W)$ measurements are necessary, and moreover sufficient for generic measurements in the case $\mathbb{F} = \mathbb{C}$ provided the algebraic varieties $V_j, j = 1, \ldots, N$ and W satisfy some mild conditions. The tools from algebraic geometry play an important role in our investigation. Using these tools we also provide an alternative proof for the Stiefel-Hopf condition (Theorem 1.1), which may be independently interesting in itself. In Section 4 we show that $N = 2d - 1$ (resp. $N = 4d - 4$) generic matrices with prescribed ranks have the phase retrieval property in $\mathbb{R}^d$ (resp. $\mathbb{C}^d$). Similar technique also allows us to establish the $N = 4d-4$ result for generic fusion frames, namely $N = 4d - 4$ generic orthogonal projections have the phase retrieval property in $\mathbb{C}^d$. Finally, in Section 5, we study the minimal measurement number $\mathfrak{m}_{\mathbb{F}}(d)$ by employing the results on the embedding of projective spaces in Euclidean spaces. In the real case $\mathbb{F} = \mathbb{R}$, we prove that $2d - O(\log_2 d) \leq \mathfrak{m}_{\mathbb{R}}(d) \leq 2d - 1$. When d is of the form $d = 2^k + \delta$ where $\delta = 1$ or 2, we obtain the exact value $\mathfrak{m}_{\mathbb{R}}(d) = 2d - \delta$. In the complex case $\mathbb{F} = \mathbb{C}$, let α denotes the number of 1's in the binary expansion of $d - 1$. Then the lower bound $4d - 2 - 2\alpha$ was obtained for information completeness of POVMs with respect to pure states [22], which leads to the lower bound $4d - 3 - 2\alpha$ for the phase retrieval. In this paper we improves the results to $\mathfrak{m}_{\mathbb{C}}(d) \geq 4d - 2 - 2\alpha$. As a result, combining with known upper bounds we are able to obtain the exact value of $\mathfrak{m}_{\mathbb{C}}(d)$ for several classes of dimensions d, including particularly the special case $d = 2^k + 1 > 4$, for which $\mathfrak{m}_{\mathbb{C}}(d) = 4d - 4$. This sharp lower bound in the standard phase retrieval setting was first shown in [12].

2. Equivalent Formulations for Generalized Phase Retrieval

We state an equivalent formulation for the generalized phase retrieval problem here, which allows us to prove some basic but important properties for generalized phase retrieval.

For any $c \in \mathbb{C}$ let $\Re(c)$ and $\Im(c)$ denote the real and imaginary part of c, respectively. A useful formula is that for a Hermitian $A \in \mathbf{H}_d(\mathbb{F})$ and any $\mathbf{x}, \mathbf{y} \in \mathbb{F}^d$ we must have

$$\mathbf{x}^* A\mathbf{x} - \mathbf{y}^* A\mathbf{y} = 4\Re(\mathbf{v}^* A\mathbf{u}) \tag{2.1}$$

where $\mathbf{v} = \frac{1}{2}(\mathbf{x}+\mathbf{y})$ and $\mathbf{u} = \frac{1}{2}(\mathbf{x}-\mathbf{y})$. This is straightforward to check. In the real case $\mathbb{F} = \mathbb{R}$ it means that $\mathbf{x}^* A\mathbf{x} - \mathbf{y}^* A\mathbf{y} = \mathbf{v}^* A\mathbf{u} = \mathbf{v}^T A\mathbf{u}$.

Theorem 2.1. *Let $\mathcal{A} = (A_j)_{j=1}^N \subset \mathbf{H}_d(\mathbb{R})$. The following are equivalent:*

1. *$\mathcal{A}$ has the phase retrieval property.*
2. *There exist no nonzero $\mathbf{v}, \mathbf{u} \in \mathbb{R}^d$ such that $\mathbf{v}^T A_j \mathbf{u} = 0$ for all $1 \le j \le N$.*
3. *$\operatorname{span}\{A_j\mathbf{u}\}_{j=1}^N = \mathbb{R}^d$ for any nonzero $\mathbf{u} \in \mathbb{R}^d$.*
4. *If $Q \in \mathcal{M}_{d,1}(\mathbb{R})$ and $\operatorname{Tr}(A_j Q) = 0$ for all $1 \le j \le N$, then $Q = 0$.*
5. *For any nonzero $Q \in \mathcal{M}_{d,2}(\mathbb{R}) \cap \mathbf{H}_d(\mathbb{R})$ such that $\operatorname{Tr}(A_j Q) = 0$ for all $1 \le j \le N$, Q has two nonzero eigenvalues having the same sign.*
6. *The bilinear form $\mathbf{L} : \mathbb{R}^d \times \mathbb{R}^d \longrightarrow \mathbb{R}^N$ given by $\mathbf{L}(\mathbf{x}, \mathbf{y}) := (\mathbf{x}^T A_j \mathbf{y})_{j=1}^N$ is nonsingular.*
7. *The Jacobian of $\mathbf{M}_{\mathcal{A}}$ has rank d everywhere on $\mathbb{R}^d \setminus \{0\}$.*

Proof. (1) $\Leftrightarrow$ (2). This is rather clear. If there exist $\mathbf{x} \neq \pm\mathbf{y}$ in $\mathbb{R}^d$ such that $\mathbf{M}_{\mathcal{A}}(\mathbf{x}) = \mathbf{M}_{\mathcal{A}}(\mathbf{y}) = 0$ then $\mathbf{x}^T A_j \mathbf{x} - \mathbf{y}^T A_j \mathbf{y} = (\mathbf{v}+\mathbf{u})^T A_j (\mathbf{v}+\mathbf{u}) - (\mathbf{v}-\mathbf{u})^T A_j (\mathbf{v}-\mathbf{u}) = 0$ which implies $\mathbf{v}^T A_j \mathbf{u} = 0$ for all j, where $\mathbf{v} = \frac{1}{2}(\mathbf{x}+\mathbf{y})$ and $\mathbf{u} = \frac{1}{2}(\mathbf{x}-\mathbf{y})$. Clearly, both $\mathbf{u}, \mathbf{v}$ are nonzero. This is a contradiction. The converse also follows from the same argument.

(1) $\Leftrightarrow$ (5). We first show (1) $\Rightarrow$ (5) by contradiction. Assume there is a $Q \in \mathcal{M}_{d,2}(\mathbb{R}) \cap \mathbf{H}_d(\mathbb{R})$ such that $\operatorname{Tr}(A_j Q) = 0$ for all j and Q has two nonzero eigenvalues $\lambda_1 > 0$ and $\lambda_2 < 0$. By spectral decomposition we can write Q as

$$Q = \lambda_1 \mathbf{u}\mathbf{u}^T - |\lambda_2| \mathbf{v}\mathbf{v}^T$$

where $\langle \mathbf{u}, \mathbf{v} \rangle = 0$. Thus

$$\operatorname{Tr}(A_j(\lambda_1 \mathbf{u}\mathbf{u}^T - |\lambda_2|\mathbf{v}\mathbf{v}^T)) = \operatorname{Tr}(A_j \mathbf{x}\mathbf{x}^T) - \operatorname{Tr}(A_j \mathbf{y}\mathbf{y}^T) = 0$$

where $\mathbf{x} = \sqrt{\lambda_1}\mathbf{u}, \mathbf{y} = \sqrt{|\lambda_2|}\mathbf{v}$. Since $\mathbf{x}^T A_j \mathbf{x} = \operatorname{Tr}(A_j \mathbf{x}\mathbf{x}^T)$ and $\mathbf{y}^T A_j \mathbf{y} = \operatorname{Tr}(A_j \mathbf{y}\mathbf{y}^T)$, it follows that $\mathbf{M}_{\mathcal{A}}(\mathbf{x}) = \mathbf{M}_{\mathcal{A}}(\mathbf{y})$. But $\mathbf{x} \neq \pm\mathbf{y}$, this contradicts with (1).

We next show (5) $\Rightarrow$ (1). Assume there exist $\mathbf{x}, \mathbf{y} \in \mathbb{R}^d$ so that $\mathbf{x}^T A_j \mathbf{x} = \mathbf{y}^T A_j \mathbf{y}$ for all j and $\mathbf{x} \neq \pm \mathbf{y}$. Then

$$\mathrm{Tr}(A_j(\mathbf{x}\mathbf{x}^T - \mathbf{y}\mathbf{y}^T)) = \mathbf{x}^T A_j \mathbf{x} - \mathbf{y}^T A_j \mathbf{y} = 0.$$

Set $Q := \mathbf{x}\mathbf{x}^T - \mathbf{y}\mathbf{y}^T \neq 0$. Then $Q \in \mathcal{M}_{d,2}(\mathbb{R}) \cap \mathbf{H}_d(\mathbb{R})$ such that $\mathrm{Tr}(A_j Q) = 0$ for all j. Hence Q has two nonzero eigenvalues of the same sign. This implies that $\mathbf{x}$ and $\mathbf{y}$ are linearly independent, and therefore Q has two nonzero eigenvalues with opposite signs, contradicting (5).

(2) $\Leftrightarrow$ (3). If for some nonzero $\mathbf{u}_0 \in \mathbb{R}^d$ so that $\mathrm{span}\{A_j \mathbf{u}_0\}_{j=1}^N \neq \mathbb{R}^d$. Then we can find $\mathbf{v}_0 \neq 0$ so that $\mathbf{v}_0 \perp \mathrm{span}\{A_j \mathbf{u}_0\}_{j=1}^N$. This implies $\mathbf{v}_0^T A_j \mathbf{u}_0 = 0$ for all j. The converse is clearly also true from the same argument.

(2) $\Leftrightarrow$ (6). The bilinear form $\mathbf{L}$ is nonsingular if and only if $\mathbf{L}(\mathbf{x}, \mathbf{y}) \neq 0$ for all nonzero $\mathbf{x}, \mathbf{y}$. This is precisely the condition in (2).

(4) $\Leftrightarrow$ (6). First we observe that $Q \in \mathcal{M}_{d,1}(\mathbb{R})$ if and only if $Q = \mathbf{x}\mathbf{y}^T$, and $Q \neq 0$ if and only if both $\mathbf{x}, \mathbf{y} \neq 0$. The equivalence follows immediately from the fact $\mathbf{L}(\mathbf{x}, \mathbf{y}) = (\mathrm{Tr}(A_j Q)_{j=1}^N$ where $Q = \mathbf{x}\mathbf{y}^T$.

(3) $\Leftrightarrow$ (7). The Jacobian of $\mathbf{M}_{\mathcal{A}}$ at $\mathbf{x}$ is exactly $J_{\mathcal{A}}(\mathbf{x}) = 2[A_1\mathbf{x}, A_2\mathbf{x}, \ldots, A_N\mathbf{x}]$, i.e. the columns of $J_{\mathcal{A}}(\mathbf{x})$ are precisely $\{A_j\mathbf{x}\}_{j=1}^N$. Thus (3) is equivalent to for any $\mathbf{x} \neq 0$ the rank of $J(\mathbf{x})$ is d. ∎

We remark that the equivalence of some of these conditions are known for the standard phase retrieval. The equivalence of (3) and (1) was also established for real orthogonal projections matrices in [17].

Theorem 2.2. *Let $\mathcal{A} = (A_j)_{j=1}^N \subset \mathbf{H}_d(\mathbb{C})$. The following are equivalent:*

1. *$\mathcal{A}$ has the phase retrieval property.*
2. *There exist no $\mathbf{v}, \mathbf{u} \neq 0$ in $\mathbb{C}^d$ with $\mathbf{u} \neq ic\mathbf{v}$ for any $c \in \mathbb{R}$ such that $\Re(\mathbf{v}^* A_j \mathbf{u}) = 0$ for all $1 \leq j \leq N$.*
3. *The (real) Jacobian of $\mathbf{M}_{\mathcal{A}}$ has (real) rank $2d-1$ everywhere on $\mathbb{C}^d \setminus \{0\}$.*
4. *For any nonzero $Q \in \mathcal{M}_{d,2}(\mathbb{C}) \cap \mathbf{H}_d(\mathbb{C})$ such that $\mathrm{Tr}(A_j Q) = 0$ for all $1 \leq j \leq N$, Q has two nonzero eigenvalues having the same sign.*

Proof. (1) $\Leftrightarrow$ (2). Assume that there exist $\mathbf{v}, \mathbf{u} \neq 0$ in $\mathbb{C}^d$, $\mathbf{u} \neq ic\mathbf{v}$ for some $c \in \mathbb{R}$ such that $\Re(\mathbf{v}^* A_j \mathbf{u}) = 0$ for all $1 \leq j \leq N$. Set $\mathbf{x} = \mathbf{u} + \mathbf{v}$ and $\mathbf{y} = \mathbf{u} - \mathbf{v}$. We have $\mathbf{M}_{\mathcal{A}}(\mathbf{x}) = \mathbf{M}_{\mathcal{A}}(\mathbf{y})$ by (2.1). We show $\mathbf{x} \neq a\mathbf{y}$ whenever $|a| = 1$. If otherwise, note that $a \neq \pm 1$ because $\mathbf{u}, \mathbf{v} \neq 0$. Hence we must have $\mathbf{u} = \frac{a+1}{a-1}\mathbf{v}$. But $\frac{a+1}{a-1}$ is pure imaginary, which is a contradiction. Thus $\mathbf{M}_{\mathcal{A}}$ is not injective on $\underline{\mathbb{F}^d} = \mathbb{C}^d / \sim$ and $\mathcal{A}$ is not phase retrievable.

Conversely assume that $\mathbf{M}_{\mathcal{A}}$ is not injective and $\mathbf{M}_{\mathcal{A}}(\mathbf{x}) = \mathbf{M}_{\mathcal{A}}(\mathbf{y})$ where $\mathbf{x} \neq a\mathbf{y}$ for $|a| = 1$. Set $\mathbf{u} = \mathbf{x} + \mathbf{y}$ and $\mathbf{v} = \mathbf{x} - \mathbf{y}$. Then $\mathbf{u} \neq ic\mathbf{v}$ for any $c \in \mathbb{R}$. Furthermore, $\Re(\mathbf{v}^* A_j \mathbf{u}) = 0$ for all $1 \leq j \leq N$.

(1) $\Leftrightarrow$ (4). The proof is almost identical to the proof of the equivalence of (1) and (5) in Theorem 2.1. We omit the detail here.

(2) $\Leftrightarrow$ (3). Write $A_j = B_j + iC_j$ where B_j, C_j are real. Then $B_j^T = B_j$ and $C_j^T = -C_j$. Let

$$F_j = \begin{bmatrix} B_j & -C_j \\ C_j & B_j \end{bmatrix}. \tag{2.2}$$

Then for any $\mathbf{u} = \mathbf{u}_R + i\mathbf{u}_I \in \mathbb{C}^d$ we have $\mathbf{u}^* A_j \mathbf{u} = \mathbf{x}^T F_j \mathbf{x}$, where $\mathbf{x}^T = [\mathbf{u}_R^T, \mathbf{u}_I^T]$. Thus the real Jacobian of $\mathbf{M}_{\mathcal{A}}(\mathbf{u})$ is precisely

$$J_{\mathcal{A}}(\mathbf{u}) = 2[F_1\mathbf{x}, F_2\mathbf{x}, \ldots, F_N\mathbf{x}].$$

Note that

$$[-\mathbf{u}_I^T, \mathbf{u}_R^T] F_j \mathbf{u} = -\mathbf{u}_I^T B_j \mathbf{u}_R + \mathbf{u}_R^T C_j \mathbf{u}_R + \mathbf{u}_I C_j \mathbf{u}_I + \mathbf{u}_R^T B_j \mathbf{u}_I = 0.$$

Thus the rank of $J_{\mathcal{A}}(\mathbf{u})$ is at most $2d - 1$. Moreover, for any $\mathbf{v} = \mathbf{v}_R + i\mathbf{v}_I \in \mathbb{C}^d$ we have

$$2[\Re(\mathbf{v}^* A_j \mathbf{u})] = [\mathbf{v}_R^T, \mathbf{v}_I^T] J_{\mathcal{A}}(\mathbf{u}).$$

To prove (2) implies (3), assume there exist nonzero $\mathbf{u}, \mathbf{v} \in \mathbb{C}^d$ with $\mathbf{u} \neq ic\mathbf{v}$ for any $c \in \mathbb{R}$ such that $\Re(\mathbf{v}^* A_j \mathbf{u}) = 0$ for all $1 \leq j \leq N$. Denote $\mathbf{x}^T = [\mathbf{u}_R^T, \mathbf{u}_I^T]$ and $\mathbf{y}^T = [\mathbf{v}_R^T, \mathbf{v}_I^T]$. Then $\mathbf{y}^T F_j \mathbf{x} = 0$ for all j. But $\mathbf{u} \neq ic\mathbf{v}$ implies $\mathbf{y}^T \neq c[-\mathbf{u}_I^T, \mathbf{u}_R^T]$ for any real c. Hence the rank of $J_{\mathcal{A}}(\mathbf{u})$ is at most $2d - 2$.

Conversely, to prove (3) implies (2), assume there exists a nonzero $\mathbf{u} \in \mathbb{C}^d$ such that the rank of $J_{\mathcal{A}}(\mathbf{u})$ is at most $2d - 2$ then we can find a $\mathbf{y} \in \mathbb{R}^{2d}$ such that $\mathbf{y}^T J_{\mathcal{A}}(\mathbf{u}) = 0$ and $\mathbf{y}^T$ is not co-linear with $[-\mathbf{u}_I^T, \mathbf{u}_R^T]$. Write $\mathbf{y}^T = [\mathbf{v}_R^T, \mathbf{v}_I^T]$ and $\mathbf{v} = \mathbf{v}_R + i\mathbf{v}_I$. Then $\mathbf{v} \neq ic\mathbf{u}$, and moreover $\Re(\mathbf{v}^* A_j \mathbf{u}) = 0$ for all j. ∎

In the standard phase retrieval, the set of the frames $(\mathbf{f}_1, \ldots, \mathbf{f}_N) \in \mathbb{C}^{d \times N}$ having the phase retrieval property in $\mathbb{C}^d$ is an open set [2, 12]. The conclusion also holds for generalized phase retrieval.

Theorem 2.3. *Let $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$. For any given N, the set of $\mathcal{A} := (A_j)_{j=1}^N \subset \mathbf{H}_d^N(\mathbb{F})$ having the phase retrieval property is an open set in $\mathbf{H}_d^N(\mathbb{F})$.*

Proof. We only need to prove that the set of $\mathcal{A}$'s not having the phase retrieval property is closed. First we consider the real case $\mathbb{F} = \mathbb{R}$. Let $\{\mathcal{A}_n\} \subset \mathbf{H}_d^N(\mathbb{F})$ be a sequence of N-tuples of real symmetric matrices that do not have the phase retrieval property and $\lim_n \mathcal{A}_n = \mathcal{A}$.

By Theorem 2.1 there exists a $\mathbf{x}_n \in \mathbb{R}^d \setminus \{0\}$ such that the Jacobian has rank$J_{\mathcal{A}_n}(\mathbf{x}_n) < d$ for any n. Without loss of generality we may assume $\|\mathbf{x}_n\| = 1$. Thus there is a subsequence $\mathbf{x}_{n_k}$ with $\lim_k \mathbf{x}_{n_k} = \mathbf{x}$. Clearly $\|\mathbf{x}\| = 1$. Furthermore, $J_{\mathcal{A}_{n_k}}(\mathbf{x}_{n_k}) \longrightarrow J_{\mathcal{A}}(\mathbf{x})$ and therefore rank$J_{\mathcal{A}}(\mathbf{x}) < d$. Thus $\mathcal{A}$ does not have the phase retrieval property, which proves that the set of all non-phase retrieval $\mathcal{A}$'s is closed. This yields the theorem for $\mathbb{F} = \mathbb{R}$.

For the complex case $\mathbb{F} = \mathbb{C}$ the proof is essentially identical. Let $\mathcal{A}_n$ be a sequence of N-tuples of Hermitian matrices that do not have the phase retrieval property and $\lim_n \mathcal{A}_n = \mathcal{A}$. By Theorem 2.2 there exists a nonzero $\mathbf{u}_n \in \mathbb{C}^d$ such that the real Jacobian $J_{\mathcal{A}_n}(\mathbf{u}_n)$ has rank at most $2d-2$. Without loss of generality we may assume $\|\mathbf{u}_n\| = 1$. Thus there is a subsequence $\mathbf{u}_{n_k}$ with $\lim_k \mathbf{u}_{n_k} = \mathbf{u}$. Clearly $\|\mathbf{u}\| = 1$. Furthermore, $J_{\mathcal{A}_{n_k}}(\mathbf{u}_{n_k}) \longrightarrow J_{\mathcal{A}}(\mathbf{u})$ and hence rank$J_{\mathcal{A}}(\mathbf{u}) \leq 2d-2$. Thus $\mathcal{A}$ does not have the phase retrieval property, which proves that the set of all non-PR $\mathcal{A}$'s is closed. This yields the theorem for $\mathbb{F} = \mathbb{C}$. ∎

Theorem 2.3 implies the following Corollary:

Corollary 2.4. *The phase retrieval property over $\mathbb{F}$ for $\mathcal{A} \in \mathbf{H}_d^N(\mathbb{F})$ is preserved under small perturbation.*

3. The Generalized Matrix Recovery and Nonsingular Bilinear Form

In this section we present results on the recovery of matrices. We establish its connection to phase retrieval, and use it to investigate nonsingular bilinear form. The main result here serves as the foundation of our results on generalized phase retrieval.

3.1. Background from Algebraic Geometry.

We first introduce some basic notations and results from algebraic geometry that are useful for this paper. Let $V \subseteq \mathbb{C}^d$ be an algebraic variety (affine variety), i.e. V is the locus of a collection of polynomials in $\mathbb{C}[\mathbf{x}]$. We shall use $\mathbf{I}(V)$ to denote the ideal of V, i.e.,

$$\mathbf{I}(V) := \Big\{ f \in \mathbb{C}[\mathbf{x}] : \ f \equiv 0 \text{ on } V \Big\}.$$

The ideal $\mathbf{I}(V)$ is always a finitely generate radical ideal. We write $\mathbf{I}(V) = \langle g_1, \ldots, g_m \rangle$ to denote that $\mathbf{I}(V)$ is generated by the polynomials $g_1, \ldots, g_m \in \mathbb{C}[\mathbf{x}]$. It is well known that there is a one-to-one correspondence between radical ideals of $\mathbb{C}[\mathbf{x}]$ where $\mathbf{x} = (x_1, \ldots, x_d)^T$ and algebraic varieties in $\mathbb{C}^d$.

For a finite set of polynomials $\{f_j\}_{j=1}^m \subset \mathbb{C}[\mathbf{x}]$, the Jacobian of $\{f_j\}_{j=1}^m$ is the $m \times d$ matrix given by

$$J(\mathbf{x}) := \begin{pmatrix} \partial f_1/\partial x_1 & \cdots & \partial f_1/\partial x_d \\ \vdots & \vdots & \vdots \\ \partial f_m/\partial x_1 & \cdots & \partial f_m/\partial x_d \end{pmatrix}. \tag{3.1}$$

Let V be an algebraic variety in $\mathbb{C}^d$ and $\mathbf{x} \in V$. Assume that $\mathbf{I}(V) = \langle f_1, \ldots, f_m \rangle$ and the Jacobian of $\{f_j\}_{j=1}^m$ is $J(\mathbf{x})$. Several results are well known. First the local dimension of V around $\mathbf{x}$ is $d - \min_{\mathbf{y}} \operatorname{rank}(J(\mathbf{y}))$ where $\mathbf{y}$ ranges over the local analytic manifold points of V arbitrarily near $\mathbf{x}$. The dimension of V, denoted by $\dim(V)$, is the maximum of the local dimensions (see Definition 2.3 in [27]). Furthermore, if V is irreducible then the local dimension of V is a constant, which is of course just $\dim(V)$. An equivalent definition of dimension of V is defined as the Krull dimension of $\mathbf{I}(V)$.

Note that a complex algebraic variety V may contain real points. We use $V_{\mathbb{R}}$ to denote the real points of V. Assume that $\mathbf{I}(V) = \langle f_1, \ldots, f_m \rangle$. Each f_j can be written uniquely as $f_j(\mathbf{x}) = g_j(\mathbf{x}) + ih_j(\mathbf{x})$ where both g_j, h_j are polynomials with real coefficients. It is easy to see that $V_{\mathbb{R}}$ is the real zero locus of the real polynomials $g_1, \ldots, g_m, h_1, \ldots, h_m$. According to Theorem 2.3.6 in [6], any real semi-algebraic subset of $\mathbb{R}^d$ is homeomorphic as a semi-algebraic set to a finite disjoint union of hypercubes. Thus one can define the real dimension of $V_{\mathbb{R}}$, denoted by $\dim_{\mathbb{R}}(V_{\mathbb{R}})$ as the maximal dimension of a hypercube in this decomposition. An important fact is:

Lemma 3.1. *Let V be an algebraic variety in $\mathbb{C}^d$. Then $\dim_{\mathbb{R}}(V_{\mathbb{R}}) \leq \dim(V)$.*

Proof. This is already shown in Section 2.1.3 in [17] under the assumption that V is defined by the locus of a collection of polynomials with real coefficients. So we only need to consider the case in which $\mathbf{I}(V) = \langle f_1, \ldots, f_m \rangle$ and not all f_j are real polynomials. Write $f_j(\mathbf{x}) = g_j(\mathbf{x}) + ih_j(\mathbf{x})$ where $g_j(\mathbf{x})$ and $h_j(\mathbf{x})$ are the unique polynomials with real coefficients. Then $V_{\mathbb{R}}$ is the real zero locus of the real polynomials $\{g_j(\mathbf{x}), h_j(\mathbf{x})\}_{j=1}^m$. Let W be the complex zero locus of $\{g_j(\mathbf{x}), h_j(\mathbf{x})\}_{j=1}^m$. Then $\dim(W) \geq \dim_{\mathbb{R}}(V_{\mathbb{R}})$. However, $W \subseteq V$ and hence $\dim(W) \leq \dim(V)$. The lemma follows. ∎

In this paper we shall primarily consider *projective varieties*. Let $\sigma : \mathbb{C}^d \setminus \{0\} \longrightarrow \mathbb{P}(\mathbb{C}^d)$ be the canonical map $\sigma(\mathbf{x}) = [\mathbf{x}]$, where $\mathbb{P}(\mathbb{C}^d)$ is the projective space and $[\mathbf{x}] \in \mathbb{P}(\mathbb{C}^d)$ denotes the line through $\mathbf{x}$. We shall also often consider the *projectivization* of a set $S \subset \mathbb{C}^d \setminus \{0\}$, to be $[S] = \sigma(S)$. A projective variety is the projectivization of an affine variety defined by homogeneous polynomials, which lies in $\mathbb{P}(\mathbb{C}^d)$. But for simplicity, in this paper we adopt a looser terminology. Whenever there is no confusion, the phrase *a projective variety in*

$\mathbb{C}^d$ means an affine variety in $\mathbb{C}^d$ defined by homogeneous polynomials. We shall use a *projective variety in* $\mathbb{P}(\mathbb{C}^d)$ to describe a true projective variety. Throughout the paper, by a *generic* point $\mathbf{x}$ in an algebraic variety V we mean $\mathbf{x} \in V \setminus Z$ where $Z \subset V$ is a subvariety with $\dim(Z) < \dim(V)$.

3.2. **Generalized Matrix Recovery.** The aim of this subsection is to investigate the generalized matrix recovery problem introduced earlier, through the study of related algebraic varieties. Let $L_j : \mathbb{F}^n \times \mathbb{F}^m \longrightarrow \mathbb{F}$ be a bilinear function where $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$. Suppose that $V_j \subset \mathbb{F}^n, j = 1, \ldots, N$, and $W \subset \mathbb{F}^m$ are algebraic varieties. Our objective is to show that under certain conditions an element $\mathbf{w} \in W$ can be uniquely determined by a series of "observations" in the form of $L_j(\mathbf{x}_j, \mathbf{w})$ where $\mathbf{x}_j \in V_j$. As said before, it is enough to consider whether $\{\mathbf{w} \in W : L_j(\mathbf{x}_j, \mathbf{w}) = 0, \mathbf{x}_j \in V_j, j = 1, \ldots, N\}$ only contains zero point. For matrix recovery, we usually assume V_j and W are varieties in the space of matrices. The bilinear functions L_j is usually in the form $L_j(A, Q) = \mathrm{Tr}(AQ)$ or more generally $L_j(A, Q) = \mathrm{Tr}(\tau(A)Q)$ where $A, Q \in \mathbb{F}^{d\times d}$ and $\tau : \mathbb{F}^{d\times d} \longrightarrow \mathbb{F}^{d\times d}$ is a linear map.

Definition 3.1. Let V be projective variety in $\mathbb{C}^d$ with $\dim(V) > 0$ and let $\ell_\alpha : \mathbb{C}^d \longrightarrow \mathbb{C}$, $\alpha \in I$, be a family of (homogeneous) linear functions where I is an index set. We say V is *admissible* with respect to $\{\ell_\alpha : \alpha \in I\}$ if $\dim(V \cap \{\mathbf{x} \in \mathbb{C}^d : \ell_\alpha(\mathbf{x}) = 0\}) < \dim(V)$ for all $\alpha \in I$.

It is well known in algebraic geometry that if a projective variety V is irreducible in $\mathbb{C}^d$ then $\dim(V \cap Y) = \dim(V) - 1$ for any hyperplane Y that does not contain V (see Corollary 4 in [13]). Thus the above admissible condition is equivalent to the property that no irreducible component of V of dimension $\dim(V)$ is contained in any hyperplane $\ell_\alpha(\mathbf{x}) = 0$. In general a variety V is admissible if for a *generic point* $\mathbf{x} \in V$ and any small neighborhood U of $\mathbf{x}$, $U \cap V$ is not completely contained in any hyperplane $\ell_\alpha(\mathbf{x}) = 0$.

We now prove the following theorem, which is one of the key theorems of this paper. It will be applied to matrix recovery and used to establish results for phase retrieval.

Theorem 3.2. *For $j = 1, \ldots, N$ let $L_j : \mathbb{C}^n \times \mathbb{C}^m \to \mathbb{C}$ be bilinear functions and V_j be projective varieties in $\mathbb{C}^n$. Set $V := V_1 \times \cdots \times V_N \subseteq (\mathbb{C}^n)^N$. Let W be a projective variety in $\mathbb{C}^m$. For each fixed j, assume that V_j is admissible with respect to the linear functions $\{f^{\mathbf{w}}(\cdot) = L_j(\cdot, \mathbf{w}) : \ \mathbf{w} \in W \setminus \{0\}\}$.*

(1) *Assume that $N \geq \dim(W)$ and let $\delta := N - \dim(W) + 1 \geq 1$. Then there exists an algebraic subvariety $Z \subset V$ with $\dim(Z) \leq \dim(V) - \delta$ such that, for any $X = (\mathbf{x}_j)_{j=1}^N \in V \setminus Z$ and $\mathbf{w} \in W$, $L_j(\mathbf{x}_j, \mathbf{w}) = 0$ for all $1 \leq j \leq N$ implies $\mathbf{w} = 0$.*

(2) *If* $N < \dim(W)$, *for any* $X = (\mathbf{x}_j)_{j=1}^N \in V$, *there exists a nonzero* $\mathbf{w} \in W$ *such that* $L_j(\mathbf{x}_j, \mathbf{w}) = 0$ *for all* $1 \le j \le N$.

Proof. We first prove (1). For any $X = (\mathbf{x}_j)_{j=1}^N \in V$, define $\Phi_X : W \to \mathbb{C}^N$ by $\Phi_X(\mathbf{w}) = (L_j(\mathbf{x}_j, \mathbf{w}))_{j=1}^N$. We show that if $X \in V \setminus Z$, then $\Phi_X(\mathbf{w}) = 0$ if and only if $\mathbf{w} = 0$. Let $\mathcal{G}$ be the subset of $[V] \times [W] \subset \mathbb{P}((\mathbb{C}^n)^N) \times \mathbb{P}(\mathbb{C}^m)$ such that $([X], [\mathbf{w}]) \in \mathcal{G}$ if and only if $\Phi_X(\mathbf{w}) = 0$, i.e. $L_j(\mathbf{x}_j, \mathbf{w}) = 0$ for all j. Note that $\mathcal{G} \subset \mathbb{P}((\mathbb{C}^n)^N) \times \mathbb{P}(\mathbb{C}^m)$ is the zero locus of homogeneous polynomials $L_j(\mathbf{x}_j, \mathbf{w}) = 0$ in the entries $X = (\mathbf{x}_j)_{j=1}^N$ and $\mathbf{w}$. Thus we can view $\mathcal{G}$ as a projective variety via Segre embedding [21, Page 27]. We examine its dimension. Let π_1 and π_2 be projections from $\mathbb{P}((\mathbb{C}^n)^N) \times \mathbb{P}(\mathbb{C}^m)$ onto the first and the second coordinates, respectively, namely

$$\pi_1([X], [\mathbf{w}]) = [\mathbf{x}_1, \ldots, \mathbf{x}_N], \quad \pi_2([X], [\mathbf{w}]) = [\mathbf{w}].$$

We claim that $\pi_2(\mathcal{G}) = [W]$, the projectivization of W. Indeed, for any fixed nonzero $\mathbf{w}_0 \in W$ we consider the set $\{\mathbf{x}_j \in \mathbb{C}^n : L_j(\mathbf{x}_j, \mathbf{w}_0) = 0\}$. If $L_j(\cdot, \mathbf{w}_0) \equiv 0$, then $\{\mathbf{x}_j \in \mathbb{C}^n : L_j(\mathbf{x}_j, \mathbf{w}_0) = 0\} = \mathbb{C}^n$. For the case where $L_j(\cdot, \mathbf{w}_0) \not\equiv 0$, $\{\mathbf{x}_j \in \mathbb{C}^n : L_j(\mathbf{x}_j, \mathbf{w}_0) = 0\}$ is a hyperplane in $\mathbb{C}^n$ since $L_j(\mathbf{x}_j, \mathbf{w}_0) = 0$ is a linear equation about $\mathbf{x}_j$. It follows that the set $\{\mathbf{x} \in \mathbb{C}^n : L_j(\mathbf{x}, \mathbf{w}_0) = 0\}$ must intersect $V_j \setminus \{0\}$ (see [21, Prop.11.4]). Let $\mathbf{y}_j \neq 0$ be in the intersection. Set $X_0 := (\mathbf{y}_1, \ldots, \mathbf{y}_N)$. Then we have $([X_0], [\mathbf{w}_0]) \in \mathcal{G}$ and thus $\pi_2([X_0], [\mathbf{w}_0]) = [\mathbf{w}_0]$. Consequently we have $\pi_2(\mathcal{G}) = [W]$. Now $[W] \subset \mathbb{P}(\mathbb{C}^m)$ is a projective variety because it is the zero locus of homogeneous polynomials. Thus

$$\dim(\pi_2(\mathcal{G})) \;=\; \dim(W) - 1. \tag{3.2}$$

We next consider the dimension of the preimage $\pi_2^{-1}([\mathbf{w}_0]) \subset \mathbb{P}((\mathbb{C}^n)^N))$ for a fixed $[\mathbf{w}_0] \in \mathbb{P}(\mathbb{C}^m)$. Let $V_j' := V_j \cap H_j$ where $H_j := \{\mathbf{x} \in \mathbb{C}^n : L_j(\mathbf{x}, \mathbf{w}_0) = 0\}$ is a hyperplane. The admissibility property of V_j implies that $\dim(V_j') = \dim(V_j) - 1$ (see [21]). Hence after projectivization the preimage $\pi_2^{-1}([\mathbf{w}_0])$ has dimension

$$\dim(\pi_2^{-1}([\mathbf{w}_0])) = \sum_{j=1}^{N} (\dim(V_j) - 1) - 1 = \dim(V) - N - 1. \tag{3.3}$$

By [21, Cor.11.13], we have

$$\begin{aligned} \dim(\mathcal{G}) &= \dim(\pi_2(\mathcal{G})) + \dim(\pi_2^{-1}([\mathbf{w}_0])) \\ &= (\dim(W) - 1) + (\dim(V) - N - 1) \\ &= \dim(V) + \dim(W) - N - 2 \end{aligned}$$

where for the second equality we use (3.2) and (3.3). If $N \geq \dim(W)$ then

$$\dim(\pi_1(\mathcal{G})) \leq \dim(\mathcal{G}) = \dim(V) + \dim(W) - N - 2 = \dim(V) - \delta - 1. \tag{3.4}$$

Here, we use the result that the dimension of the projection is less than or equal to the dimension of the original variety, see [21, Theorem 11.12 and Cor.11.13]. Note that $\pi_1(\mathcal{G})$ is itself a projective variety. Let Z be the lift of $\pi_1(\mathcal{G})$ into the vector space $(\mathbb{C}^n)^N$. Then

$$\dim(Z) \leq \dim(V) - \delta.$$

For any $X = (\mathbf{x}_j)_{j=1}^n \in V \setminus Z$, by the definition of $\mathcal{G}$, $\Phi_X(\mathbf{w}) = 0$ for $\mathbf{w} \in W$ implies $\mathbf{w} = 0$.

We now prove (2), namely Φ_X cannot be injective if $N < \dim(W)$. Set

$$Z_X := \Big\{[\mathbf{w}] \in \mathbb{P}(\mathbb{C}^m) : \ \mathbf{w} \in \mathbb{C}^m, \Phi_X(\mathbf{w}) = 0\Big\}.$$

Then Z_X is a linear subspace in $\mathbb{P}(\mathbb{C}^m)$ with $\dim(Z_X) \geq m - 1 - N$. The projective variety $[W] \subseteq \mathbb{P}(\mathbb{C}^m)$ has dimension $\dim(W) - 1$. If $N \leq \dim(W) - 1$ then

$$\dim(Z_X) \dim([W]) \geq m - 1,$$

which implies that (see [21, Prop.11.4])

$$Z_X \cap [W] \neq \emptyset.$$

Thus for $N \leq \dim(W) - 1$ there exists a non-zero $\mathbf{w}_0 \in \mathbb{C}^m$ with $[\mathbf{w}_0] \in Z_X \cap [W]$ satisfying $\Phi_X(Q_0) = 0$. It follows that Φ_X is not injective on W. ∎

Corollary 3.3. *Under the hypotheses of Theorem 3.2, let $V_{\mathbb{R}}$ be the real points of V. Assume that $\dim_{\mathbb{R}}(V_{\mathbb{R}}) = \dim(V)$. Then there exists a real algebraic subvariety $\tilde{Z} \subset V_{\mathbb{R}}$ with $\dim_{\mathbb{R}}(\tilde{Z}) < \dim_{\mathbb{R}}(V_{\mathbb{R}})$ such that, for any $X = (\mathbf{x}_j)_{j=1}^N \in V_{\mathbb{R}} \setminus \tilde{Z}$ and $\mathbf{w} \in W$, $L_j(\mathbf{x}_j, \mathbf{w}) = 0$ for all $1 \leq j \leq N$ implies $\mathbf{w} = 0$.*

Proof. Let $\tilde{Z} := Z_{\mathbb{R}}$ be the real points of Z where the definition of Z is given in Theorem 3.2. Note that

$$\dim_{\mathbb{R}}(\tilde{Z}) \leq \dim(Z) \leq \dim(V) - \delta = \dim_{\mathbb{R}}(V_{\mathbb{R}}) - \delta$$

where $\delta = N - \dim(W) + 1$ as in Theorem 3.2. The Corollary now follows immediately. ∎

We now apply Theorem 3.2 to study matrix recovery. In this setting we consider bilinear functions $L_j(A, Q) = \mathrm{Tr}(AQ)$ where $A, Q \in \mathbb{C}^{d \times d}$. We shall let $W = \mathcal{M}_{d,r}(\mathbb{C})$ where as before

$$\mathcal{M}_{d,r}(\mathbb{F}) := \Big\{Q \in \mathbb{F}^{d \times d} : \mathrm{rank}(Q) \leq r\Big\}, \qquad \mathbb{F} = \mathbb{C} \text{ or } \mathbb{R}.$$

Note that $\mathrm{rank}(Q) \leq r$ is equivalent to the vanishing of all $(r+1) \times (r+1)$ minors of Q and that these $(r+1) \times (r+1)$ minors are homogeneous polynomials in the entries of Q.

Hence, $\mathcal{M}_{d,r}(\mathbb{F})$ is a projective variety in $\mathbb{F}^{d^2}$. For $\mathbb{F}=\mathbb{C}$ it has dimension $2dr-r^2$ [21, Prop. 12.2] and degree $\prod_{i=0}^{d-r-1}\frac{(d+i)!\cdot i!}{(r+i)!\cdot(d-r+i)!}$ [21, Example 19.10]. The projectivization of $\mathcal{M}_{d,r}(\mathbb{F})$ is a projective variety in $\mathbb{P}(\mathbb{F}^{d^2})$ and is called a *determinantal variety*. It is also well known that a determinantal variety is irreducible (see [32]). Theorem 3.2 implies the following theorem:

Corollary 3.4. *For $j=1,\dots,N$ let $L_j:\mathbb{C}^{d\times d}\times\mathbb{C}^{d\times d}\to\mathbb{C}$ be bilinear functions and V_j be projective varieties in $\mathbb{C}^{d\times d}$. Set $V:=V_1\times\cdots\times V_N\subseteq(\mathbb{C}^{d\times d})^N$. For each fixed j, assume that V_j is admissible with respect to the linear functions $\{f^Q(\cdot)=L_j(\cdot,Q):\ Q\in\mathcal{M}_{d,r}(\mathbb{C})\setminus\{0\}\}$.*

1. *Assume that $N\geq 2rd-r^2$, $Q\in\mathcal{M}_{d,r}(\mathbb{C})$ and set $\delta:=N-2rd-r^2+1\geq 1$. Then there exists an algebraic subvariety $Z\subset V$ with $\dim(Z)\leq\dim(V)-\delta$ such that for any $\mathcal{A}=(A_j)_{j=1}^N\in V\setminus Z$, $L_j(A_j,Q)=0$ for all $1\leq j\leq N$ implies $Q=0$.*
2. *If $N<2rd-r^2$ then for any $\mathcal{A}=(A_j)_{j=1}^N\in V$ there exists a nonzero $Q\in\mathcal{M}_{d,r}(\mathbb{C})$ such that $L_j(A_j,Q)=0$ for all $1\leq j\leq N$.*

Proof. This follows immediately from Theorem 3.2 by taking $\mathbb{C}^n=\mathbb{C}^m=\mathbb{C}^{d\times d}$ and $W=\mathcal{M}_{d,r}(\mathbb{C})$. Here, we use $\dim(W)=2rd-r^2$ [21, Prop. 12.2]. ∎

For $W=\mathcal{M}_{d,r}(\mathbb{C})$ and $L_j(A_j,Q)=\mathrm{Tr}(A_jQ)$, the hypothesis in Corollary 3.4 that V_j is admissible with respect to the linear functions $\{f^Q(\cdot)=L_j(\cdot,Q):\ Q\in\mathcal{M}_{d,r}(\mathbb{C})\setminus\{0\}\}$ is satisfied under many circumstances, e.g. if $V_j=\mathcal{M}_{d,r_j}(\mathbb{C})$ where $r_j\geq 1$ (see the proof of Theorem 3.6). In the next section more examples will be given.

Corollary 3.5. *Under the hypotheses of Corollary 3.4, suppose that $\dim_{\mathbb{R}}(V_{\mathbb{R}})=\dim(V)$ and $Q\in\mathcal{M}_{d,r}(\mathbb{C})$. Then there exists a real algebraic subvariety $\tilde{Z}\subset V_{\mathbb{R}}$ with $\dim_{\mathbb{R}}(\tilde{Z})\leq\dim_{\mathbb{R}}(V_{\mathbb{R}})-\delta$ where $\delta=N-(2rd-r^2)+1\geq 1$, such that for any $\mathcal{A}=(A_j)_{j=1}^N\in V_{\mathbb{R}}\setminus\tilde{Z}$, $L_j(A_j,Q)=0$ for all $1\leq j\leq N$ implies $Q=0$.*

Proof. Let $\tilde{Z}:=Z_{\mathbb{R}}$ be the real points of Z, where Z is the algebraic variety in Corollary 3.4. Note that

$$\dim_{\mathbb{R}}(\tilde{Z})\leq\dim(Z)\leq\dim(V)-\delta=\dim_{\mathbb{R}}(V_{\mathbb{R}})-\delta.$$

The Corollary now follows immediately from Corollaries 3.3 and 3.4. ∎

3.3. **Nonsingular Bilinear Form.** For $\mathbb{F}=\mathbb{R}$, Theorem 2.1 shows the equivalence between the generalized phase retrieval property and the existence of nonsingular symmetric bilinear form. Inspired by this result, we take a detour from phase retrieval to consider nonsingular bilinear form in this subsection. First we recall some notations concerning bilinear form. Let $\mathbf{L}:\mathbb{F}^p\times\mathbb{F}^q\to\mathbb{F}^N$ be a bilinear form of size (p,q,N) given by

$\mathbf{L}(\mathbf{x},\mathbf{y}) = (\mathbf{x}^T B_1 \mathbf{y}, \ldots, \mathbf{x}^T B_N \mathbf{y}) \in \mathbb{F}^N$ where $\mathbf{x} \in \mathbb{F}^p, \mathbf{y} \in \mathbb{F}^q$ and $B_j \in \mathbb{F}^{p\times q}$. We call the bilinear form $\mathbf{L}$ the *bilinear form corresponding to* $B_1, \ldots, B_N$. $\mathbf{L}$ is said to be *nonsingular* if $\mathbf{L}(\mathbf{x},\mathbf{y}) = 0$ implies $\mathbf{x} = 0$ or $\mathbf{y} = 0$. We shall call $\mathbf{L}$ a *real* bilinear form if $\mathbb{F} = \mathbb{R}$.

Theorem 3.6. *Let $p, q \geq 1$, $N \geq p+q-1$ and $1 \leq r_1, \ldots, r_N \leq \min\{p, q\}$. For $j = 1, \ldots, N$ let $B_1, \ldots, B_N \in \mathbb{F}^{p\times q}$ be N generic matrices with $\operatorname{rank}(B_j) = r_j$, where $\mathbb{F} = \mathbb{C}$ or $\mathbb{R}$. Then the bilinear form $\mathbf{L}$ corresponding to $B_1, \ldots, B_N$ is nonsingular.*

Proof. We apply Theorem 3.2 to prove this result. Define

$$\mathcal{M}_{(q\times p),r}(\mathbb{F}) := \Big\{ Q \in \mathbb{F}^{q\times p} : \ \operatorname{rank}(Q) \leq r \Big\}.$$

Then $\mathcal{M}_{(q\times p),r}(\mathbb{F})$ is an algebraic variety and its dimension is known to be $(p+q)r - r^2$. Now

$$\mathbf{L}(\mathbf{x},\mathbf{y}) = \left(\operatorname{Tr}(B_1 \mathbf{y}\mathbf{x}^T), \ldots, \operatorname{Tr}(B_N \mathbf{y}\mathbf{x}^T)\right).$$

Hence the bilinear form $\mathbf{L}$ is nonsingular if and only if

$$\Big\{ Q \in \mathbb{F}^{q\times p} : \ \operatorname{Tr}(B_j Q) = 0, j = 1, \ldots, N \Big\} \cap \mathcal{M}_{(q\times p),1}(\mathbb{F}) = \{0\}. \tag{3.5}$$

We prove the theorem first for $\mathbb{F} = \mathbb{C}$. In Theorem 3.2 we take $\mathbb{C}^n = \mathbb{C}^{p\times q}$ and $V_j = \mathcal{M}_{(p\times q),r_j}(\mathbb{C})$. Let $W = \mathcal{M}_{(q\times p),1}(\mathbb{C})$. Note that $N \geq \dim(W) = p + q - 1$. We show that the bilinear functions $L_j(A, Q) = \operatorname{Tr}(AQ)$ satisfies the admissibility hypothesis of Theorem 3.2. Since each V_j is irreducible, we only need to show that for any nonzero $Q_0 \in W$ not all $A \in V_j$ are in the hyperplane defined by $\operatorname{Tr}(AQ_0) = 0$. To see this, let $Q_0 = \mathbf{y}_0 \mathbf{x}_0^T$ where $\mathbf{y}_0 \in \mathbb{C}^q$ and $\mathbf{x}_0 \in \mathbb{C}^q$ are nonzero. Set $A_0 = \bar{\mathbf{x}}_0 \mathbf{y}_0^* \in V_j$. Then $\operatorname{Tr}(A_0 Q_0) = \|\mathbf{x}_0\|^2 \|\mathbf{y}_0\|^2 > 0$. Thus the admissibility hypothesis is met by each V_j. It follows from Theorem 3.2 that there exists a variety $Z \subset V := V_1 \times \cdots \times V_N$ with $\dim(Z) < \dim(V)$ such that for any $(B_j)_{j=1}^N \in V \setminus Z$, (3.5) holds, and thus $\mathbf{L}$ corresponding to $B_1, \ldots, B_N$ is nonsingular. This proves the theorem for $\mathbb{F} = \mathbb{C}$.

For $\mathbb{F} = \mathbb{R}$ we notice that $\mathcal{M}_{(p\times q),r_j}(\mathbb{R})$ is the real points of $\mathcal{M}_{(p\times q),r_j}(\mathbb{C})$, and furthermore its real dimension is $r(p+q) - r^2$, the same as $\dim \mathcal{M}_{(p\times q),r_j}(\mathbb{C})$. Thus $\dim(V_{\mathbb{R}}) = \dim(V)$. The theorem now follows directly from Corollary 3.3. ∎

Remark. In the complex $\mathbb{F} = \mathbb{C}$ setting part (ii) of Theorem 3.2 also shows that no complex bilinear form with $N \leq p+q-2$ can be nonsingular. For the real setting $\mathbb{F} = \mathbb{R}$ the situation is quite different. We know through the above theorem that $p\#q \leq p+q-1$. But $p+q-1$ is in general not sharp. For example, as mentioned in the Introduction, for $p = q = 1, 2, 4, 8$ we have $p\#q = p$. The problems of finding $p\#q$ and constructing nonsingular bilinear forms are difficult in general. Theorem 3.6 shows that generic $\{B_j\}_{j=1}^{p+q-1}$ with prescribed ranks

$\operatorname{rank}(B_j) = r_j$ will yield a nonsingular bilinear form $\mathbf{L}$ of size $(p, q, p+q-1)$. To our knowledge, the result is new.

We next consider the case where $N \leq p+q-2$. It is possible that a nonsingular real bilinear form of size (p, q, N) still exists. A necessary condition for its existence is the Stiefel-Hopf condition (see Theorem 1.1). Below we provide another necessary condition, which is a rediscovery of the work by Felix Behrend [5]. Though later we show that this condition is equivalent to the Stiefel-Hopf condition, still we decide to include it here because the proof is purely algebraic and is different from many other known proofs. We also hope the method can be helpful for finding something new.

Theorem 3.7. *Suppose a nonsingular real bilinear form of size (p, q, N) with $N \leq p+q-2$ exists. Then the following binomial coefficients must be even:*

$$\binom{n}{p-1}, \quad N \leq n \leq p+q-2.$$

Proof. Clearly if there is a nonsingular real bilinear of size (p, q, N) exists then so does a nonsingular real bilinear of size (p, q, n) for any $n \geq N$. Hence, we only need to show that $\binom{N}{p-1}$ is even.

To this end, we only need to show that if $\binom{N}{p-1}$ is odd then any real bilinear form of size (p, q, N) must be singular. Assume that $\mathbf{L}$ is a real bilinear form corresponding to $B_1, \ldots, B_N \in \mathbb{R}^{p\times q}$. For any $\mathbf{y} \in \mathbb{C}^q$ we let

$$Q_{\mathbf{y}} := (B_1\mathbf{y}, B_2\mathbf{y}, \ldots, B_N\mathbf{y})$$

where the columns of $Q_{\mathbf{y}}$ are $B_1\mathbf{y}, \ldots, B_N\mathbf{y}$. Thus $\mathbf{L}$ is singular if and only if there exits a nonzero $\mathbf{y}_0 \in \mathbb{R}^q$ such that $\operatorname{rank}(Q_{\mathbf{y}_0}) \leq p-1$.

We now consider elements $(A, \mathbf{y}) \in \mathbb{C}^{p\times N} \times \mathbb{C}^q$. Define the projective subvariety

$$V_{p,N,q} := \Big\{[(A, \mathbf{y})] \in \mathbb{P}(\mathbb{C}^{p\times N} \times \mathbb{C}^q) : \ \operatorname{rank}(A) \leq p-1\Big\}$$

In other words, $V_{p,N,q}$ is the projectivization of the variety $\mathcal{M}_{(p\times N),p-1}(\mathbb{C}) \times \mathbb{C}^q$. Hence it has dimension

$$\dim(V_{p,N,q}) = (p-1)(p+N) - (p-1)^2 + q - 1 = N(p-1) + p + q - 2.$$

Furthermore, by [21, Example 19.10] it has degree $\binom{N}{p-1}$.

Finally we observe that the existence of $\mathbf{y}_0 \in \mathbb{R}^q \setminus \{0\}$ such that $\operatorname{rank}(Q_{\mathbf{y}_0}) \leq p-1$ if and only if there exists a $[(A, \mathbf{y})] \in V_{p,N,q}$ such that $\mathbf{y} \in \mathbb{R}^q$ and the j-th column of A, say $\mathbf{a}_j$, is exactly $B_j\mathbf{y}$ for each j. Set

$$\mathcal{H} := \Big\{[(A, \mathbf{y})] \in \mathbb{P}(\mathbb{C}^{p\times N} \times \mathbb{C}^q) : \ \mathbf{a}_j - B_j\mathbf{y} = 0, j = 1, \ldots, N\Big\}.$$

Then $\mathcal{H}$ is a linear subspace in $\mathbb{P}(\mathbb{C}^{p\times N}\times\mathbb{C}^q)$ with $\dim(\mathcal{H})\geq q-1$. Since $N\leq p+q-2$, we have

$$\dim(\mathcal{H})+\dim(V_{p,N,q})\geq Np+q-1=\dim(\mathbb{P}(\mathbb{C}^{p\times N}\times\mathbb{C}^q))$$

which implies $V_{p,N,q}\cap\mathcal{H}\neq\emptyset$, see [21, Proposition 11.4]. Now all B_j are real so $V_{p,N,q}$ is defined by polynomials of real coefficients. If the degree of $V_{p,N,q}=\binom{N}{p-1}$ is odd, then the intersection $V_{p,N,q}\cap\mathcal{H}$ must contain real points. Hence $\mathbf{L}$ is singular. The theorem is proved. ∎

Remark. Because of symmetry, we also know that a necessary condition for the existence of nonsingular real bilinear from of size (p,q,N) is that $\binom{n}{q-1}$ is even for all $N\leq n\leq p+q-2$. It turns out that our condition in Theorem 3.7 is equivalent to the Stiefel-Hopf condition stated in Theorem 1.1. To see this, we note the identity $\binom{N+t}{k}=\binom{N+t-1}{k-1}+\binom{N+t-1}{k}$. Hence by induction we have

$$\binom{N+t}{k}=\sum_{j=0}^{t}a_j\binom{N}{k-j}$$

for some positive integers $a_j\in\mathbb{N}$. If $\binom{N}{p-1},\binom{N}{p-2},\ldots,\binom{N}{N-q+1}$ are even then

$$\binom{N+t}{p-1}=\sum_{j=0}^{t}a_j\binom{N}{p-1-j}$$

must be even for all $t=0,\ldots,p+q-2-N$. The converse is proved by the same way.

It is worth noting that $\binom{n}{m}$ is odd if and only if the sum of m and $n-m$ has no carry in base 2, i.e. the base expansion of m and $n-m$ have no overlapping 1's. This fact leads to finer results on $p\#q$, which we omit here. Theses results can be found in [34], which were obtained using different methods.

4. Generalized Phase Retrieval With Generic Measurements

In this section we establish several results on the phase retrieval property of $\mathcal{A}=(A_j)_{j=1}^N$ where A_j are chosen to be generic from some classes of matrices. The corresponding results are mostly known in the standard phase retrieval setting where all $A_j=\mathbf{f}_j\mathbf{f}_j^*$ with $\mathbf{f}_j\in\mathbb{F}^d$. However, even for the standard phase retrieval the complex case is highly nontrivial. Of particular note, we show that a generic choice of $N\geq 4d-4$ subspaces (fusion frames) $\{X_j\}_{j=1}^N$ in $\mathbb{C}^d$ with $1\leq\dim(X_j)\leq d-1$ have the phase retrieval property.

Theorem 4.1. *Let $N\geq 2d-1$ and $1\leq r_1,\ldots,r_N\leq d$. Then a generic $\mathcal{A}=(A_j)_{j=1}^N\in\mathbf{H}_d^N(\mathbb{R})$ with $\operatorname{rank}(A_j)=r_j$ has the phase retrieval property in $\mathbb{R}^d$.*

Proof. By Theorem 2.1, we only need show that if $Q \in \mathcal{M}_{d,1}(\mathbb{R})$ and $\mathrm{Tr}(A_j Q) = 0$ for all $1 \leq j \leq N$ then $Q = 0$. To prove this we apply Corollaries 3.4 and 3.5. Set in Corollary 3.4 $V = V_{r_1} \times \cdots \times V_{r_N}$, where V_{r_j} denotes the symmetric determinantal variety of the set of complex symmetric matrices in $\mathbb{C}^{d\times d}$ with rank at most r_j. The V_{r_j} is an algebraic variety which is defined by the zero locus of a set of homogeneous polynomials. It is well known that $\dim(V_{r_j}) = dr_j - \frac{r_j(r_j-1)}{2}$ and $\dim_{\mathbb{R}}((V_{r_j})_{\mathbb{R}}) = dr_j - \frac{r_j(r_j-1)}{2}$. Thus $\dim(V) = \dim_{\mathbb{R}}(V_{\mathbb{R}})$.

Set $W = \mathcal{M}_{d,1}(\mathbb{C})$ and let $L_j(A, Q) = \mathrm{Tr}(AQ)$. Assume we know that V_{r_j} is admissible with respect to $\{f^Q(\cdot) = L_j(\cdot, Q) : \ Q \in \mathcal{M}_{d,1}(\mathbb{C}) \setminus \{0\}\}$ for all j then our theorem follows immediately from Corollary 3.5.

Thus all it remains is to show the admissibility of V_{r_j}. To do so it suffices to show that at a generic point $A_0 \in V_{r_j}$ and any nonzero $Q_0 \in \mathcal{M}_{d,1}(\mathbb{C})$ we must have $\mathrm{Tr}(AQ_0) \not\equiv 0$ in any small neighborhood of A_0 in V_{r_j}. If $\mathrm{Tr}(A_0Q_0) \neq 0$ we are done. Assume that $\mathrm{Tr}(A_0Q_0) = 0$. According to SVD, we can write $Q_0 = \mathbf{x}_0\mathbf{y}_0^T$. Applying the Tagaki factorization to A_0 we get

$$A_0 = \sum_{j=1}^{s} \mathbf{z}_j \mathbf{z}_j^T.$$

Now set $\hat{\mathbf{z}}_1 = \mathbf{z}_1 + t\mathbf{u}$ where $\mathbf{u} \in \mathbb{C}^d$ and let $A = \hat{\mathbf{z}}_1\hat{\mathbf{z}}_1^T + \sum_{j=2}^{s} \mathbf{z}_j\mathbf{z}_j^T$. Then

$$\mathrm{Tr}(AQ) = t^2(\mathbf{y}_0^T\mathbf{u})(\mathbf{u}^T\mathbf{x}_0) + t(\mathbf{y}_0^T\mathbf{u} + \mathbf{u}^T\mathbf{x}_0) + \mathrm{Tr}(A_0Q) = t^2(\mathbf{y}_0^T\mathbf{u})(\mathbf{u}^T\mathbf{x}_0) + t(\mathbf{y}_0^T\mathbf{u} + \mathbf{u}^T\mathbf{x}_0).$$

Clearly, since $\mathbf{u}$ can be arbitrary, we can pick a $\mathbf{u}$ such that $(\mathbf{y}_0^T\mathbf{u})(\mathbf{u}^T\mathbf{x}_0) \neq 0$. By taking t to be very small we must have $\mathrm{Tr}(AQ_0) \not\equiv 0$ in any small neighborhood of A_0 in V_{r_j}. This completes the proof of the Theorem. ∎

Remark. Since the set of positive semidefinite matrices of rank r in $\mathbb{R}^{d\times d}$ is an open set in V_r, where V_r denotes the symmetric determinantal variety of the set of complex symmetric matrices in $\mathbb{C}^{d\times d}$ with rank at most r, Theorem 4.1 also holds if we require the matrices A_j are positive semi-definite.

It is shown in Edidin [17] that $N \geq 2d-1$ generic fusion frames have the phase retrieval property. Below we show an alternative proof using our method.

Theorem 4.2 (Edidin [17])**.** *Let $N \geq 2d-1$ and $1 \leq r_1, \ldots, r_N \leq d-1$. Then a generic set of N orthogonal projection matrices $\mathcal{A} = (A_j)_{j=1}^N \in \mathbf{H}_d^N(\mathbb{R})$ where $A_j^2 = A_j$ and $\mathrm{rank}(A_j) = r_j$ has the phase retrieval property in $\mathbb{R}^d$.*

Proof. For any integer let V_s denote the set of complex symmetric matrices A in $\mathbb{C}^{d\times d}$ with the property

$$A^2 = \frac{1}{s}\mathrm{Tr}(A)A. \tag{4.1}$$

Clearly (4.1) gives a set of homogeneous polynomial equations in the entries of A. Hence, V_s is an algebraic variety. We next consider the dimension of V_s. We claim that $\mathrm{rank}(A) = s$ for any nonzero $A \in V_s$. To see this, $A^2 = \lambda A$ where $\lambda = \frac{1}{s}\mathrm{Tr}(A)$. Thus the eigenvalues of A are λ with multiplicity $k := \mathrm{rank}(A)$ and 0 with multiplicity $d-k$. Hence $\mathrm{Tr}(A) = \lambda k$ and $A^2 = \frac{k}{s}\lambda A$ which implies $s = k = \mathrm{rank}(A)$. Note also that by Jordan canonical form we easily see that $A^2 = \lambda A$ can only happen if the Jordan canonical form of A is diagonal. So A must be diagonalizable. It follows from [24, Theorem 4.4.13] that there exists a complex orthogonal matrix P (i.e. $PP^T = I$) such that

$$A = P\begin{pmatrix} \lambda I_s & 0 \\ 0 & 0 \end{pmatrix} P^T = \lambda \sum_{j=1}^{s} \mathbf{v}_j \mathbf{v}_j^T \tag{4.2}$$

where $\mathbf{v}_j$ is the j-th column of P so $\{\mathbf{v}_j\}_{j=1}^s$ are complex orthonormal in the sense that $\mathbf{v}_i^T\mathbf{v}_j = \delta_{ij}$. Conversely, it is clear that any matrix A having the form (4.2) must be in V_s.

Define the map $\varphi : V_s \setminus \{0\} \longrightarrow G(s, \mathbb{C}^d)$ by $\varphi(A) = A(\mathbb{C}^d)$, where we use $A(\mathbb{C}^d)$ to denote the subspace $\{A\mathbf{x} : \mathbf{x} \in \mathbb{C}^d\}$ and $G(s, \mathbb{C}^d)$ to denote the Grassmannian of s-dimensional subspaces of $\mathbb{C}^d$. The map φ is onto because any s-dimensional subspaces X in $\mathbb{C}^d$ has a complex orthonormal basis $\{\mathbf{v}_1, \ldots, \mathbf{v}_s\}$ (see [24]), and hence $X = PP^T(\mathbb{C}^d) = \varphi(PP^T)$ with $P = (\mathbf{v}_1 \ldots \mathbf{v}_s) \in \mathbb{C}^{d\times s}$. Moreover we claim φ is injective on $V_s \cap \{A \in \mathbb{C}^{d\times d} : A^2 = A\}$. To see this, if $A_1(\mathbb{C}^d) = A_2(\mathbb{C}^d)$ then we must have $A_1 = A_2R$ for some nonsingular $R \in \mathbb{C}^{d\times d}$. Hence $A_2A_1 = A_2^2R = A_2R = A_1$. By symmetry we also have $A_1A_2 = A_2$, which yields $A_2 = A_2^T = A_2^TA_1^T = A_2A_1 = A_1$. Thus $A_1 = A_2$. As a consequence, $\dim(V_s \cap \{A^2 = A\}) = s(d-s)$, which is the dimension of the Grassmannian. Hence $\dim(V_s) = s(d-s)+1$. Recall that $(V_s)_{\mathbb{R}} = V_s \cap \mathbb{R}^{d\times d}$. Then $(V_s)_{\mathbb{R}} \cap \{A \in \mathbb{R}^{d\times d} : A^2 = A\}$ corresponds to the real Grassmannian $G(s, \mathbb{R}^d)$, which has the real dimension $s(d-s)$. Thus $\dim_{\mathbb{R}}((V_s)_{\mathbb{R}}) = \dim(V_s)$.

Assume we know that V_s is admissible with respect to $\{f^Q(\cdot) = \mathrm{Tr}(\cdot\, Q) :\ Q \in \mathcal{M}_{d,1}(\mathbb{C}) \setminus \{0\}\}$ for all $1 \le s \le d-1$. We prove the theorem in exactly the same way as we have proved Theorem 4.1, namely by setting $V = V_{r_1} \times \cdots \times V_{r_N}$, $W = \mathcal{M}_{d,1}(\mathbb{C})$ and let $L_j(A, Q) = \mathrm{Tr}(AQ)$ in Corollary 3.4. Here, V_{r_j} is defined by taking $s = r_j$ in V_s. Since each V_s is just a scale multiple of a complex orthogonal projection, the theorem is equivalent to that

a generic $\mathcal{A} = (A_j)_{j=1}^N \in V_{\mathbb{R}}$ has the phase retrieval property. The theorem thus follows immediately from Corollary 3.5.

Now all we need is to show the admissibility of V_s. The map φ induces an isomorphism from $[V_s]$, the projectivization of V_s, to the Grassmannian. Since the Grassmannian is an irreducible projective variety, it follows that V_s is irreducible. To show it is admissible we now only have to show that it is not contained in any hyperplane $\{A : \mathrm{Tr}(AQ_0) = 0\}$ where $Q_0 \in \mathcal{M}_{d,1}(\mathbb{C})$. Write $Q_0 = \mathbf{x}\mathbf{y}^T$. Then $\mathrm{Tr}(AQ_0) = \mathbf{y}^T A\mathbf{x}$. Without loss of generality we assume $y_1 \neq 0$. Taking A that maps $\mathbf{x}$ to $\lambda\mathbf{e}_1$ for some $\lambda \neq 0$ will yield $\mathbf{y}^T A\mathbf{x} = \lambda y_1 \neq 0$. This completes the proof of the Theorem. ∎

Theorem 4.3. *Let $N \geq 4d - 4$ and $1 \leq r_1, \ldots, r_N \leq d$. Then a generic $\mathcal{A} = (A_j)_{j=1}^N \in \mathbf{H}_d^N(\mathbb{C})$ with $\mathrm{rank}(A_j) = r_j$ has the phase retrieval property in $\mathbb{C}^d$.*

Proof. Define a linear map $\tau : \mathbb{C}^{d\times d} \longrightarrow \mathbb{C}^{d\times d}$ by

$$\tau(A) = \frac{1}{2}(A + A^T) + \frac{i}{2}(A - A^T).$$

It is easy to see that τ is an isomorphism on $\mathbb{C}^{d\times d}$ and furthermore τ restricted on $\mathbb{R}^{d\times d}$ is an isomorphism from $\mathbb{R}^{d\times d}$ to $\mathbf{H}_d(\mathbb{C})$. Set $L(A, Q) = \mathrm{Tr}(\tau(A)Q)$. By Theorem 2.2, it suffices to show that for a generic $\mathcal{A} = (A_j)_{j=1}^N \subset \mathbb{R}^{d\times d}$ with $\mathrm{rank}(\tau(A_j)) = r_j$, if $Q \in \mathcal{M}_{d,2}(\mathbb{C})$ and $L(A_j, Q) = 0$ then $Q = 0$.

For any $s \geq 1$ let V_s denote the set of matrices A in $\mathbb{C}^{d\times d}$ such that $\mathrm{rank}(\tau(A)) \leq s$. The V_s is clearly an algebraic variety defined by the zero locus of a set of homogeneous polynomials. Since τ is an isomorphism on $\mathbb{C}^{d\times d}$, we have $\dim(V_s) = \dim \mathcal{M}_{d,s}(\mathbb{C}) = 2ds - s^2$. Moreover, $\dim_{\mathbb{R}}((V_s)_{\mathbb{R}}) = \dim_{\mathbb{R}}(V_s \cap \mathbb{R}^{d\times d})$ is exactly the (real) dimension of the set of Hermitian matrices of rank $\leq s$, which is also $2ds - s^2$ (see also [26, Lemma II.1]).

We now prove the theorem in exactly the same way as before through the application of Corollaries 3.4 and 3.5. Set $r = 2$, $V = V_{r_1} \times \cdots \times V_{r_N}$, $W = \mathcal{M}_{d,2}(\mathbb{C})$ and let $L_j(A, Q) = L(A, Q) = \mathrm{Tr}(\tau(A)Q)$ in Corollary 3.4. Here, V_{r_j} is defined by taking $s = r_j$ in V_s. Assume that we know each V_{r_j} is admissible with respect to $\{f^Q(\cdot) := \mathrm{Tr}(\tau(\cdot)Q)\}_{Q\in W\setminus\{0\}}$. Then the theorem follows immediately from Corollary 3.5, as $N \geq 4d - 4 = 2rd - r^2$.

Thus all it remains is to prove the admissibility of V_s for all $1 \leq s < d$. The argument is similar with the one in the proof of Theorem 4.1. To do so it suffices to show that at a generic point $A_0 \in V_s$ and any nonzero $Q_0 \in \mathcal{M}_{d,2}(\mathbb{C})$ we must have $\mathrm{Tr}(\tau(A)Q_0) \not\equiv 0$ in any small neighborhood of A_0 in V_s. Note that $\{\tau(A) : A \in V_s\} = \mathcal{M}_{d,s}(\mathbb{C})$. Thus we only need to show that for any $B_0 \in \mathcal{M}_{d,s}(\mathbb{C})$ we have $\mathrm{Tr}(BQ_0) \not\equiv 0$ in any small neighborhood of B_0

in $\mathcal{M}_{d,s}(\mathbb{C})$. Write

$$Q_0 = \mathbf{x}_1\mathbf{y}_1^T + \mathbf{x}_2\mathbf{y}_2^T \quad \text{where } \mathbf{x}_1, \mathbf{y}_1 \neq 0, \text{ and } \quad B_0 = \sum_{j=1}^{s} \mathbf{v}_j\mathbf{u}_j^T.$$

Let $\hat{\mathbf{v}}_1 = \mathbf{v}_1 + t\mathbf{z}$ and $\hat{\mathbf{u}}_1 = \mathbf{u}_1 + t\mathbf{w}$ where $\mathbf{z}, \mathbf{w} \in \mathbb{C}^{d\times d}$ and let $B = \hat{\mathbf{v}}_1\hat{\mathbf{u}}_1^T + \sum_{j=2}^{s} \mathbf{v}_j\mathbf{u}_j^T$. Then

$$\mathrm{Tr}(BQ_0) - \mathrm{Tr}(B_0Q_0) = t^2\Big((\mathbf{y}_1^T\mathbf{z})(\mathbf{x}_1^T\mathbf{w}) + (\mathbf{y}_2^T\mathbf{z})(\mathbf{x}_2^T\mathbf{w})\Big) + C_0t = t^2\mathbf{w}^TQ_0\mathbf{z} + C_0t$$

where $C_0 \in \mathbb{C}$ does not depend on t. If $\mathrm{Tr}(B_0Q_0) \neq 0$ we are done. Otherwise we can always find $\mathbf{z}, \mathbf{w} \in \mathbb{C}^d$ such that $\mathbf{w}^TQ_0\mathbf{z} \neq 0$ because $Q_0 \neq 0$. Thus $\mathrm{Tr}(BQ_0) - \mathrm{Tr}(B_0Q_0) = \mathrm{Tr}(BQ_0) \neq 0$ for sufficiently small t. This proves the admissibility of V_s. ∎

Remark. For any positive semidefinite Hermitian matrix A of rank s in $\mathbb{C}^{d\times d}$, a sufficiently small neighborhood of A in the set of all Hermitian matrices of rank at most s consists of only positive semidefinite Hermitian matrices of rank s. Thus the set of all positive semidefinite Hermitain matrices of rank s is an open subset of the set of all Hermitian matrices of rank at most s. It follows that Theorem 4.3 also holds if we require the matrices A_j to be positive semi-definite.

We now turn to the case of complex fusion frames (projection) phase retrieval by the proving the following new result.

Theorem 4.4. *Let $N \geq 4d-4$ and $1 \leq r_1, \ldots, r_N \leq d-1$. Then a generic set of N orthogonal projection matrices $\mathcal{A} = (A_j)_{j=1}^N \in \mathbf{H}_d^N(\mathbb{C})$ with $A_j^2 = A_j$ and $\mathrm{rank}(A_j) = r_j$ has the phase retrieval property in $\mathbb{C}^d$.*

Proof. Let $\tau : \mathbb{C}^{d\times d} \longrightarrow \mathbb{C}^{d\times d}$ be

$$\tau(A) = \frac{1}{2}(A + A^T) + \frac{i}{2}(A - A^T).$$

We have already shown it is an isomorphism on $\mathbb{C}^{d\times d}$ and furthermore τ restricted on $\mathbb{R}^{d\times d}$ is an isomorphism from $\mathbb{R}^{d\times d}$ to $\mathbf{H}_d(\mathbb{C})$.

For any integer $s \geq 1$ let V_s denote the set of matrices A in $\mathbb{C}^{d\times d}$ with the property

$$(\tau(A))^2 = \frac{1}{s}\mathrm{Tr}(\tau(A))\tau(A). \tag{4.3}$$

Note that V_s is a variety in $\mathbb{C}^{d\times d}$. Moreover, the same arguments in the proof of Theorem 4.2 shows $\mathrm{rank}(\tau(A)) = s$ for any nonzero $A \in V_s$, and through the Jordan Canonical Form, $\tau(A)$ is diagonalizable which means there exists a nonsingular P such that

$$\tau(A) = P\begin{pmatrix} \lambda I_s & 0 \\ 0 & 0 \end{pmatrix}P^{-1}. \tag{4.4}$$

Let $\tilde{V}_s = (V_s)_{\mathbb{R}}$ be the real points of V_s. For any $A \in \tilde{V}_s$, $\tau(A) \in \mathbf{H}_d(\mathbb{C})$ which implies that $\tau(A)$ is an orthogonal projection matrix. Then τ is a one-to-one map from $\tilde{V}_s$ to the set of all scalar multiples of orthogonal projection matrices in $\mathbb{C}^{d\times d}$. To this end, it suffices to prove $(\tau(A_j))_{j=1}^N$ has the phase retrieval property for a generic $(A_j)_{j=1}^N \in \tilde{V}_{r_1} \times \cdots \times \tilde{V}_{r_N}$.

For the dimension of V_s we compute $\dim(\tau(V_s)) = \dim(V_s)$. Let $G(s, \mathbb{C}^d)$ denote the Grassmannians of s-dimensional subspaces of $\mathbb{C}^d$. We define the map $\pi : [\tau(V_s)] \longrightarrow G(s, \mathbb{C}^d)\times G(d-s, \mathbb{C}^d)$, where $[\tau(V_s)]$ is the projectivization of $\tau(V_s)$, by $\pi([B]) = (\mathrm{Im}(B), \mathrm{Ker}(B))$ for any $B \in \tau(V_s)$. If $B = \tau(A)$ has the form (4.4) then it is easily checked that

$$\mathrm{Im}(B) = B(\mathbb{C}^d) = P(Y_s), \qquad \mathrm{Ker}(B) = P(Y_s^\perp),$$

where Y_s is the subspace of $\mathbb{C}^s \times \{0\}^{d-s}$ of $\mathbb{C}^d$, i.e. the s-dimensional subspace spanned by the first s coordinates. Alternatively speaking, $\mathrm{Im}(B)$ is the span of the first s columns of P and $\mathrm{Ker}(B)$ is the span of the last $d-s$ columns of P. Since P can be arbitrary, it immediately implies that the map π is onto. We show it is also one-to-one. To see this, if there is a Q such that $Q(Y_s) = P(Y_s)$ and $Q(Y_s^\perp) = P(Y_s^\perp)$, it is rather straightforward to check that we must have $PR = Q$ where R has the block diagonal form $R = \mathrm{diag}(R_1, R_2)$ with $R_1 \in \mathbb{C}^{s\times s}$ and $R_2 \in \mathbb{C}^{(d-s)\times(d-s)}$. But in this case we have

$$Q \begin{pmatrix} \lambda I_s & 0 \\ 0 & 0 \end{pmatrix} Q^{-1} = P \begin{pmatrix} \lambda I_s & 0 \\ 0 & 0 \end{pmatrix} P^{-1}.$$

Thus π is one-to-one. Now it follows that π is an isomorphism and

$$\dim([\tau(V_s)]) = \dim(G(s, \mathbb{C}^d)) + \dim(G(d-s, \mathbb{C}^d)) = 2s(d-s),$$

which yields $\dim(V_s) = \dim(\tau(V_s)) = \dim([\tau(V_s)]) + 1 = 2s(d-s) + 1$. This is exactly the real dimension of all real scalar multiples of projection matrices in $\mathbb{C}^{d\times d}$. Thus $\dim_{\mathbb{R}}(\tilde{V}_s) = \dim(V_s)$.

We now prove the theorem following the exactly same argument as in Theorem 4.3. Let $V = V_{r_1} \times \cdots \times V_{r_N}$, $W = \mathcal{M}_{d,2}(\mathbb{C})$ and $L_j(A, Q) = \mathrm{Tr}(\tau(A)Q)$. Here V_{r_j} is defined by taking $s = r_j$ in V_s. Assume that we know V_s is admissible with respect to $\{f^Q(\cdot) := \mathrm{Tr}(\tau(\cdot)Q)\}_{Q\in W\setminus\{0\}}$ for all $1 \le s \le d$. Then the theorem follows immediately from Corollary 3.5 by taking $r = 2$. Here we use the result $\dim_{\mathbb{R}}(\tilde{V}_s) = \dim(V_s)$.

It remains to prove the admissibility of V_s. To do so it suffices to show that at a generic point $A_0 \in V_s$ and any nonzero $Q_0 \in \mathcal{M}_{d,2}(\mathbb{C})$ we must have $\mathrm{Tr}(\tau(A)Q_0) \not\equiv 0$ in any small neighborhood of A_0 in V_s. Note that $\{\tau(A) : A \in V_s\}$ consists of all projection matrices in $\mathcal{M}_{d,s}(\mathbb{C})$. Thus we only need to show that for any $B_0 \in \mathcal{M}_{d,s}(\mathbb{C})$ with $B_0^2 = B_0$ we have $\mathrm{Tr}(BQ_0) \not\equiv 0$ for projection matrices B in any small neighborhood of B_0 in $\mathcal{M}_{d,s}(\mathbb{C})$. Also,

if $B = PCP^{-1}$ then $C^2 = C$ and moreover $\mathrm{Tr}(BQ_0) = \mathrm{Tr}(C(P^{-1}Q_0P))$. Thus we may consider the canonical case with $B_0 = J_s$ where

$$J_s = \begin{pmatrix} I_s & 0 \\ 0 & 0 \end{pmatrix} \in \mathbb{C}^{d\times d}.$$

Set $B_t = (I+tD)B_0(I+tD)^{-1} = (I+tD)J_s(I+tD)^{-1}$. Then all we need to show is that for some D and arbitrarily small $t \neq 0$ we have $\mathrm{Tr}(B_tQ_0) \not\equiv 0$. Since $(I+tD)^{-1} = \sum_{n=0}^{\infty}(-1)^n t^n D^n$, we have

$$\mathrm{Tr}(B_tQ_0) = \mathrm{Tr}(B_0Q_0) + \sum_{n=1}^{\infty}(-1)^{n-1}t^n\mathrm{Tr}\Big((DJ_s - J_sD)D^{n-1}Q_0\Big).$$

If there exists a $D \in \mathbb{C}^{d\times d}$ such that $\mathrm{Tr}((DJ_s - J_sD)D^{n-1}Q_0) \neq 0$ for some $n \geq 1$ then we are done. For $n = 1$

$$\mathrm{Tr}\Big((DJ_s - J_sD)D^{n-1}Q_0\Big) = \mathrm{Tr}\Big((DJ_s - J_sD)Q_0\Big) = \mathrm{Tr}\Big(D(J_sQ_0 - Q_0J_s)\Big).$$

We fist consider the case where $J_sQ_0 - Q_0J_s \not\equiv 0$. Then we can take $D = (J_sQ_0 - Q_0J_s)^*$ and obtain $\mathrm{Tr}\Big(D(J_sQ_0 - Q_0J_s)\Big) \neq 0$. We are done. We next only consider the case where $J_sQ_0 - Q_0J_s \equiv 0$. If $J_sQ_0 - Q_0J_s \equiv 0$ then Q_0 must have the form

$$Q_0 = \begin{pmatrix} Q_1 & 0 \\ 0 & Q_2 \end{pmatrix}$$

where $Q_1 \in \mathbb{C}^{s\times s}$ and $Q_2 \in \mathbb{C}^{(d-s)\times(d-s)}$. Consider now $n = 2$ and we have

$$\begin{aligned}(DJ_s - J_sD)D^{n-1}Q_0 &= \begin{pmatrix} 0 & -D_{12} \\ D_{21} & 0 \end{pmatrix}\begin{pmatrix} D_{11} & D_{12} \\ D_{21} & D_{22} \end{pmatrix}\begin{pmatrix} Q_1 & 0 \\ 0 & Q_2 \end{pmatrix} \\ &= \begin{pmatrix} -D_{12}D_{21}Q_1 & -D_{12}D_{22}Q_2 \\ D_{21}D_{11}Q_1 & D_{21}D_{12}Q_2 \end{pmatrix},\end{aligned}$$

which yields

$$\mathrm{Tr}\Big((DJ_s - J_sD)DQ_0\Big) = \mathrm{Tr}(-D_{12}D_{21}Q_1 + D_{21}D_{12}Q_2).$$

Assume that $Q_1, Q_2 \neq 0$ then both have rank 1 because $\mathrm{rank}(Q_0) \leq 2$. Write $Q_1 = \mathbf{x}\mathbf{y}^*$ and $Q_2 = \mathbf{z}\mathbf{w}^*$ where $\mathbf{x}, \mathbf{y} \in \mathbb{C}^s$ and $\mathbf{z}, \mathbf{w} \in \mathbb{C}^{d-s}$. Let $\mathbf{u} \neq 0$ be orthogonal to $\mathbf{z}$, i.e., $\mathbf{z}^*\mathbf{u} = 0$. Take $D_{12} := \mathbf{y}\mathbf{u}^*$ and $D_{21} := \mathbf{u}\mathbf{x}^*$. Then

$$\mathrm{Tr}((DJ_s - J_sD)DQ_0) = -\|\mathbf{y}\|^2\|\mathbf{u}\|^2\|\mathbf{x}\|^2 < 0.$$

Assume one of Q_1, Q_2 is 0, say $Q_2 = 0$. Then $Q_1 \neq 0$ and $\mathrm{rank}(Q_1) \leq 2$. Write $Q_1 = \mathbf{x}_1\mathbf{y}_1^* + \mathbf{x}_2\mathbf{y}_2^*$ where $\mathbf{x}_1, \mathbf{x}_2$ are linearly independent and $\mathbf{y}_1 \neq 0$. Let $\mathbf{u} \in \mathbb{C}^s$ such that $\mathbf{u}^*\mathbf{x}_2 = 0$ but $\mathbf{u}^*\mathbf{x}_1 \neq 0$. Set $D_{12} = \mathbf{y}_1\mathbf{z}^*$ and $D_{21} = \mathbf{z}\mathbf{u}^*$, where $\mathbf{z} \in \mathbb{C}^{d-s} \setminus \{0\}$. Then

$$\mathrm{Tr}((DJ_s - J_sD)DQ_0) = -\|\mathbf{y}_1\|^2\|\mathbf{z}\|^2(\mathbf{u}^*\mathbf{x}_1) \neq 0.$$

The theorem is now proved. ∎

5. Minimal Measurements for Generalized Phase Retrievals

In this section, we focus on the question: *What is the minimal N for which there exists an $\mathcal{A} = (A_j)_{j=1}^N \in \mathbf{H}_d^N(\mathbb{F})$ having the phase retrieval property in $\mathbb{F}^d$, where $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$?* Recall that we use $\mathfrak{m}_{\mathbb{F}}(d)$ to denote the minimal measurement number for which such an $\mathcal{A}$ with phase retrieval property in $\mathbb{F}^d$ exists.

It is well known that for $\mathbb{F} = \mathbb{R}$ the standard phase retrieval property always implies $N \geq 2d-1$. Thus $N = 2d-1$ is sharp in this case. However, for generalized phase retrieval the situation differs considerably, and it is no longer straightforward to calculate $\mathfrak{m}_{\mathbb{R}}(d)$. We have

Theorem 5.1. (i) $\mathfrak{m}_{\mathbb{R}}(d) \leq 2d-1$ *for any odd* d *and* $\mathfrak{m}_{\mathbb{R}}(d) \leq 2d-2$ *for any even* d.

(ii) *For any* $k \geq 1$,

$$\mathfrak{m}_{\mathbb{R}}(d) = \begin{cases} 2d-1, & d = 2^k+1 \\ 2d-2, & d = 2^k+2. \end{cases}$$

(iii) *For any* $d \geq 5$,

$$\mathfrak{m}_{\mathbb{R}}(d) \geq \begin{cases} 2d - 6\lfloor \log_2(d-1) \rfloor + 6, & d \text{ odd} \\ 2d - 6\lfloor \log_2(d-2) \rfloor + 4, & d \text{ even}. \end{cases}$$

Proof. The key ingredient in the proof of this theorem is the fact that $\mathcal{A} = (A_j)_{j=1}^N \subset \mathbf{H}_d^N(\mathbb{R})$ has the phase retrieval property if and only if the symmetric bilinear form corresponding to the matrices $\{A_j\}_{j=1}^N$ is nonsingular (Theorem 2.1). Furthermore, if there exists a nonsingular symmetric bilinear form of size (d, d, N) with $N > d$ then there exists an embedding (and hence an immersion) of the projective space $\mathbb{P}(\mathbb{R}^d) = \mathbb{P}^{d-1}$ in $\mathbb{R}^{N-1}$, see [25, Theorem 6.3].

(i) Clearly we have $\mathfrak{m}_{\mathbb{R}}(d) \leq 2d-1$ by Theorem 4.1. For even d it is known that there exists a nonsingular symmetric bilinear form with size $(d, d, 2d-2)$, see [23] or [34, Page 260]. Thus $\mathfrak{m}_{\mathbb{R}}(d) \leq 2d-2$.

(ii) For the case $d = 2^k+1$ we apply the result in [33] that for this d, $\mathbb{P}(\mathbb{R}^d)$ can not be embedded into $\mathbb{R}^{2d-3}$. Thus if $(A_j)_{j=1}^N$ has phase retrieval property, then $N-1 \geq 2d-2$, which implies $\mathfrak{m}_{\mathbb{R}}(d) \geq 2d-1$. Thus $\mathfrak{m}_{\mathbb{R}}(d) = 2d-1$ because we already know $\mathfrak{m}_{\mathbb{R}}(d) \leq 2d-1$.

For the case $d = 2^k+2$, by (i) we have $\mathfrak{m}_{\mathbb{R}}(d) \leq 2d-2$. It was shown in [29] that for this d, $\mathbb{P}(\mathbb{R}^d)$ can not be embedded into $\mathbb{R}^{2(d-1)-2} = \mathbb{R}^{2d-4}$ (see also [25, page 272]). This implies $\mathfrak{m}_{\mathbb{R}}(d) - 1 \geq 2d-3$. Hence $\mathfrak{m}_{\mathbb{R}}(d) = 2d-2$.

(iii) Here we use a non-immersion result of Davis [14] that $\mathbb{P}^{2(n+\alpha(n)-1)} = \mathbb{P}(\mathbb{R}^{2(n+\alpha(n))-1})$ can not be embedded into $\mathbb{R}^{4n-2\alpha(n)}$ for any $n \geq 1$, where $\alpha(n)$ denotes the number of 1's

in the binary expansion of n. It follows that

$$\mathfrak{m}_{\mathbb{R}}(2n+2\alpha(n)-1) \geq 4n-2\alpha(n)+2. \tag{5.1}$$

Let $\mathcal{S} = \{n+\alpha(n) : n \in \mathbb{N}\}$. Unfortunately, $\mathcal{S} \neq \mathbb{N}$. For example, $6 \notin \mathcal{S}$. Nevertheless, observe that $\alpha(n+1) = \alpha(n)+1$ for even n and $\alpha(n+1) = \alpha(n)+1-k \leq \alpha(n)$ for odd n where k is the smallest positive integer such that $n \equiv 2^k - 1 \pmod{2^k}$. Thus $n+1+\alpha(n+1)-(n+\alpha(n)) \leq 2$ which implies that $\mathcal{S}$ cannot miss two consecutive integers. In particular, if $m \notin \mathcal{S}$ then $m-1 = n+\alpha(n) \in \mathcal{S}$ for some even n.

We now derive a lower bound for $\mathfrak{m}_{\mathbb{R}}(d)$. First consider odd $d = 2s-1$ and $s \in \mathcal{S}$ with $s = n+\alpha(n)$ for some n. We have $n \geq 3$ because $d \geq 5$. By (5.1) we have

$$\mathfrak{m}_{\mathbb{R}}(d) = \mathfrak{m}_{\mathbb{R}}(2n+2\alpha(n)-1) \geq 4n-2\alpha(n)+2 = 2d-6\alpha(n)+4.$$

Since $\alpha(n) \leq \lfloor \log_2(n+1) \rfloor$ for all n and $n = s-\alpha(n)$ we have

$$\log_2(n+1) \leq \log_2\Big(s+1-\alpha(n)\Big) = \log_2\Big(\frac{d-1}{2}+2-\alpha(n)\Big). \tag{5.2}$$

If $\alpha(n) \geq 2$ then we have $\log_2(n+1) \leq \log_2(d-1)-1$. Thus $\alpha(n) \leq \lfloor \log_2(d-1) \rfloor - 1$ and hence $\mathfrak{m}_{\mathbb{R}}(d) \geq 2d - 6\lfloor \log_2(d-1) \rfloor + 10$. If $\alpha(n) = 1$ then $n = 2^k$ and $d = 2^{k+1}+1$ with $k \geq 1$, and in this case by (iii) we actually have the stronger estimate $\mathfrak{m}_{\mathbb{R}}(d) = 2d-1 \geq 2d - 6\lfloor \log_2(d-1) \rfloor + 10$.

Next consider $d = 2s-1$ and $s \notin \mathcal{S}$. Thus $s-1 = n+\alpha(n)$ for some even n, and $d = 2n+2\alpha(n)+1$. Again by (5.1) we have

$$\mathfrak{m}_{\mathbb{R}}(d) \geq \mathfrak{m}_{\mathbb{R}}(2n+2\alpha(n)-1) \geq 4n-2\alpha(n)+2 = 2d-6\alpha(n).$$

But n is even so its last digit is 0 and hence $\alpha(n) = \alpha(n+1)-1$. Now $n+1 = s-\alpha(n)$, and similar to (5.2) we have

$$\log_2(n+1) \leq \log_2\Big(s-\alpha(n)\Big) = \log_2\Big(\frac{d-1}{2}+1-\alpha(n)\Big) \leq \log_2(d-1)-1.$$

Hence $\mathfrak{m}_{\mathbb{R}}(d) \geq 2d - 6\lfloor \log_2(d-1) \rfloor + 6$. This completes the proof of (iv) for odd d.

For even $d = 2s$ we can apply the obvious result $\mathfrak{m}_{\mathbb{R}}(d) \geq \mathfrak{m}_{\mathbb{R}}(d-1)$, and the conclusion follows. ∎

Remark. Part (ii) in Theorem 5.1 implies $\mathfrak{m}_{\mathbb{R}}(4) = 6$, which answers the *Smoothie Problem*. In [16] Edidin offers a smoothie to the first person who answers the question whether there exists a fusion frame with 5 subspaces in $\mathbb{R}^4$ having the phase retrieval property. Our result proves that this is impossible. In [40] the author has constructed a fusion frame with 6 rank 2 subspaces in $\mathbb{R}^4$ having the phase retrieval property.

We next present results for the complex case. These results are again obtained from known results on embedding of projective spaces. The best known lower bound for the standard phase retrieval is $4d-3-2\alpha(d-1)+\epsilon_\alpha$ where $\alpha(d-1)$ is the number of 1's in the binary expansion of $d-1$ and ϵ_α is defined below, which follows from the lower bound $4d-2-2\alpha(d-1)+\epsilon_\alpha$ for information completeness of POVMs with respect to pure states [22]. We prove

Theorem 5.2. *Let $d>4$. Then $4d-2-2\alpha+\epsilon_\alpha \le \mathfrak{m}_{\mathbb{C}}(d) \le 4d-3-\alpha-\delta$, where $\alpha=\alpha(d-1)$ denotes the number of 1's in the binary expansion of $d-1$,*

$$\epsilon_\alpha = \begin{cases} 2 & d \text{ odd, } \alpha \equiv 3 \pmod 4 \\ 1 & d \text{ odd, } \alpha \equiv 2 \pmod 4 \\ 0 & \text{otherwise.} \end{cases} \quad \text{and} \quad \delta = \begin{cases} 0 & d \text{ odd} \\ 1 & d \text{ even.} \end{cases}$$

Proof. The upper bound, proved for information completeness of POVMs with respect to pure states [22, Theorem 3], was obtained via constructions in Milgram [31]. Since information completeness of POVMs with respect to pure states is a special case of generalized phase retrieval in which one of the matrices A_j is set to be the identity matrix, the upper bound also stands as an upper bound of $\mathfrak{m}_{\mathbb{C}}(d)$. We remark that the upper bound actually holds for $d>2$, not just $d>4$.

We next consider the lower bound. Assume that $\mathfrak{m}_{\mathbb{C}}(d) \ge 3d$, and let $\mathcal{A}=(A_j)_{j=1}^N \subset \mathbf{H}_d^N(\mathbb{C})$ have phase retrieval property. Then $N \ge \mathfrak{m}_{\mathbb{C}}(d) \ge 3d$. Define the map $\psi : \mathbb{C}^d \to \mathbb{S}^{N-1}(\mathbb{R})$ by $\psi(\mathbf{x}) = \frac{\mathbf{M}_{\mathcal{A}}(\mathbf{x})}{\|\mathbf{M}_{\mathcal{A}}(\mathbf{x})\|}$, where $\mathbb{S}^{N-1}(\mathbb{R})$ denotes the real $(N-1)$-dimensional unit sphere in $\mathbb{R}^N$. Note that $\mathcal{A}$ has the phase retrieval property. Therefore $\psi(\mathbf{x})=\psi(\mathbf{y})$ if and only if $\mathbf{x}=\lambda\mathbf{y}$ for some $\lambda \in \mathbb{C}$ which implies that ψ is a topological embedding of $\mathbb{P}(\mathbb{C}^d)$ in $\mathbb{S}^{N-1}(\mathbb{R})$. We recall a well-known result which says that, the manifold M can be embedded in $\mathbb{R}^{\dim(M)+k}$ if and only if M can be embedded in $\mathbb{S}^{\dim(M)+k}$ provided $k \ge 1$ (see [25, Page 257]). Now observe that $N-1 \ge 3d-1 > \dim(\mathbb{P}(\mathbb{C}^d))$ which implies that we can construct a topological embedding of $\mathbb{P}(\mathbb{C}^d)$ in $\mathbb{R}^{N-1}$. We now use the following result: if there exists a topological embedding of $\mathbb{P}(\mathbb{C}^d)$ in $\mathbb{R}^{N-1}$ then there exists a smooth embedding provided $N \ge 3d$ ([25, Corollary 1.5] and [20]). Hence, there exists a smooth embedding of $\mathbb{P}(\mathbb{C}^d)$ in $\mathbb{R}^{N-1}$. But the results in [30] shows that $\mathbb{P}(\mathbb{C}^d)$ can not be smoothly embedded in $\mathbb{R}^{4(d-1)-2\alpha+\epsilon_\alpha}$. Consequently $N-1 \ge 4(d-1)-2\alpha+\epsilon_\alpha+1$ and hence $\mathfrak{m}_{\mathbb{C}}(d) \ge 4d-2-2\alpha+\epsilon_\alpha$.

We still need to consider the case $\mathfrak{m}_{\mathbb{C}}(d) \le 3d-1$. If $\mathfrak{m}_{\mathbb{C}}(d) \le 3d-1$ we can then construct an $\mathcal{A}=(A_j)_{j=1}^N \subset \mathbf{H}_d^N(\mathbb{C})$ with $N=3d$ having the phase retrieval property because $N \ge \mathfrak{m}_{\mathbb{C}}(d)$. But now $N \ge 3d$ so the conclusion from the above case holds, namely

$N-1 \geq 4d-2\alpha-3+\epsilon_\alpha$. Now we have $4d-2\alpha-3+\epsilon_\alpha > 3d-1 = N$ for $d \geq 5$. This is a contradiction. ∎

The improvement from the lower bound for the standard phase retrieval in the above theorem is useful in the case $d = 2^k+1$ and $k \geq 2$. Theorem 5.2 allows us to obtain the following Corollary:

Theorem 5.3. *We have the following exact values for* $\mathfrak{m}_{\mathbb{C}}(d)$*:*

$$\mathfrak{m}_{\mathbb{C}}(d) = \begin{cases} 4d-4 & d = 2^k+1,\ k>1 \\ 4d-6 & d = 2^k+2,\ k>1 \\ 4d-5 & d = 2^k+2^j+1,\ k>j>0 \\ 4d-6 & d = 2^k+2^j+2^l+1,\ k>j>l>0. \end{cases}$$

Also, $\mathfrak{m}_{\mathbb{C}}(2) = 3$.

Proof. According to Theorem 5.2, we examine the conditions for the equality

$$4d-2-2\alpha+\epsilon_\alpha = \mathfrak{m}_{\mathbb{C}}(d) = 4d-3-\alpha-\delta \tag{5.3}$$

to hold, where α, ϵ_α and δ are as in Theorem 5.2. It holds if and only if $\alpha = 1+\epsilon_\alpha+\delta$. For even d we have $\epsilon_\alpha = 0$ and $\delta = 1$. So $\alpha = \alpha(d-1) = 2$. This happens if and only if $d = 2^k+2$ where $k>1$. For odd d we have $\delta = 0$. Hence $\alpha = 1+\epsilon_\alpha$. Since $\epsilon_\alpha \leq 2$ we only need to consider three cases: $(\alpha,\epsilon_\alpha) \in \{(1,0),(2,1),(3,2)\}$.

In the first case $(\alpha,\epsilon_\alpha) = (1,0)$, we have $\alpha = \alpha(d-1) = 1$ and hence $d = 2^k+1$. In the second case $(\alpha,\epsilon_\alpha) = (2,1)$, $\alpha = \alpha(d-1) = 2$ and it is clear that $d = 2^k+2^j+1$ where $k>j>1$. In the third case $(\alpha,\epsilon_\alpha) = (3,2)$, $\alpha = \alpha(d-1) = 3$ and $d = 2^k+2^j+2^l+1$ where $k>j>l>1$.

Finally for $\mathfrak{m}_{\mathbb{C}}(2)$, based on Theorem 2.2, $\mathcal{A}$ has the phase retrieval property if and only if the (real) Jacobian of $\mathbf{M}_{\mathcal{A}}$ has (real) rank 3 everywhere on $\mathbb{C}^2 \setminus \{0\}$. This immediately implies $\mathfrak{m}_{\mathbb{C}}(2) \geq 3$. Next we show the following 3 matrices have the phase retrieval property. Set

$$A_1 = \begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix}, \quad A_2 = \begin{pmatrix} -1 & -2-i \\ -2+i & 2 \end{pmatrix}, \quad A_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Then

$$\left\{ Q \in \mathbb{C}^{2\times 2} : \mathrm{Tr}(A_1Q) = 0, \mathrm{Tr}(A_2Q) = 0, \mathrm{Tr}(A_3Q) = 0 \right\} = \left\{ \begin{pmatrix} 2x & xi \\ -xi & 2x \end{pmatrix} : x \in \mathbb{R} \right\}$$

The eigenvalues of the matrix

$$\begin{pmatrix} 2x & xi \\ -xi & 2x \end{pmatrix}$$

are $\lambda_1 = x, \lambda_2 = 3x$ which have the same sign. According to Theorem 2.2, $\mathcal{A} = (A_1, A_2, A_3)$ has the phase retrieval property. Thus $\mathfrak{m}_{\mathbb{C}}(2) = 3$. ∎

We remark that the minimal measurement number for standard phase retrieval for $d = 2$ is known to be $4d - 4 = 4$, see [4]. The above theorem shows that the minimal measurement number can be different for generalized phase retrieval.

References

[1] Saeid Bahmanpour, Jameson Cahill, Peter G Casazza, John Jasper, and Lindsey M Woodland. Phase retrieval and norm retrieval. *arXiv preprint arXiv:1409.8266*, 2014.

[2] Radu Balan. Stability of phase retrievable frames. In *SPIE Optical Engineering+ Applications*, pages 88580H–88580H. International Society for Optics and Photonics, 2013.

[3] Radu Balan, Pete Casazza, and Dan Edidin. On signal reconstruction without phase. *Applied and Computational Harmonic Analysis*, 20(3):345–356, 2006.

[4] Afonso S Bandeira, Jameson Cahill, Dustin G Mixon, and Aaron A Nelson. Saving phase: Injectivity and stability for phase retrieval. *Applied and Computational Harmonic Analysis*, 37(1):106–125, 2014.

[5] Behrend, Felix. Über Systeme reeller algebraischer Gleichungen. *Compositio Mathematica*, 7 : 1-19, 1940.

[6] Jacek Bochnak, Michel Coste, and Marie-Françoise Roy. *Real algebraic geometry*, volume 36. Springer Science & Business Media, 2013.

[7] Bernhard G Bodmann and Nathaniel Hammen. Stable phase retrieval with low-redundancy frames. *Advances in computational mathematics*, 41(2):317–331, 2015.

[8] Jameson Cahill, Peter G Casazza, Jesse Peterson, and Lindsey Woodland. Phase retrieval by projections. *arXiv preprint arXiv:1305.6226*, 2013.

[9] T Tony Cai, Anru Zhang. Rop: Matrix recovery via rank-one projections. *The Annals of Statistics*, 43(1):102–138, 2015.

[10] E.J. Candes, Y. Eldar, T. Strohmer, and V. Voroninski. Phase retrieval via matrix completion. *SIAM Journal on Imaging Sciences*, 6(1):199–225, 2013.

[11] E.J. Candes, T. Strohmer, and V. Voroninski. Phaselift: Exact and stable signal recovery from magnitude measurements via convex programming. *Communications on Pure and Applied Mathematics*, 66(8):1241–1274, 2013.

[12] Aldo Conca, Dan Edidin, Milena Hering, and Cynthia Vinzant. An algebraic characterization of injectivity in phase retrieval. *Applied and Computational Harmonic Analysis*, 38(2):346–356, 2015.

[13] David Cox, John Little, and Donal O'shea. *Ideals, varieties, and algorithms*, volume 3. Springer, 1992.

[14] Donald M Davis. A strong non-immersion theorem for real projective spaces. *Annals of Mathematics*, 120(3):517–528, 1984.

[15] Daniel Dugger and Daniel C Isaksen. The hopf condition for bilinear forms over arbitrary fields. *Annals of mathematics*, pages 943–964, 2007.

[16] Dan Edidin. Fusion frame phase retrieval. *Workshop on Frames and Algebraic & Combinatorial Geometry, Universität Bremen, Bremen, Germany*, 2015.

[17] Dan Edidin. Projections and phase retrieval. *Applied and Computational Harmonic Analysis*, 2015.

[18] Yonina C Eldar, Deanna Needell, and Yaniv Plan. Uniqueness conditions for low-rank matrix recovery. *Applied and Computational Harmonic Analysis*, 33(2):309–314, 2012.

[19] Matthew Fickus, Dustin G Mixon, Aaron A Nelson, and Yang Wang. Phase retrieval from very few measurements. *Linear Algebra and its Applications*, 449:475–499, 2014.

[20] André Haefliger and Arnold Shapiro. Plongements différentiables dans le domaine stable. *Commentarii Mathematici Helvetici*, 37(1):155–176, 1962.

[21] Joe Harris. *Algebraic geometry: a first course*, volume 133. Springer Science & Business Media, 2013.

[22] Teiko Heinosaari, Luca Mazzarella, and Michael M Wolf. Quantum tomography under prior information. *Communications in Mathematical Physics*, 318(2):355–374, 2013.

[23] Heinz Hopf. Systeme symmetrischer bilinearformen und euklidische modelle der projektiven räume. In *Selecta Heinz Hopf*, pages 107–118. Springer, 1964.

[24] Roger A Horn and Charles R Johnson. *Matrix analysis*. Cambridge university press, 2012.

[25] IM James. Euclidean models of projective spaces. *Bulletin of the London Mathematical Society*, 3(3):257–276, 1971.

[26] Michael Kech and Michael Wolf. Quantum tomography of semi-algebraic sets with constrained measurements. *arXiv preprint arXiv:1507.00903*, 2015.
[27] Keith Kendig. *Elementary algebraic geometry*, volume 44. Springer Science & Business Media, 2012.
[28] Kee Yuen Lam. Some new results on composition of quadratic forms. *Inventiones mathematicae*, 79(3):467–474, 1985.
[29] Mark Mahowald. On the embeddability of the real projective spaces. *Proceedings of the American Mathematical Society*, 13(5):763–764, 1962.
[30] Karl Heinz Mayer. Elliptische differentialoperatoren und ganzzahligkeitssätze für charakteristische zahlen. *Topology*, 4(3):295–313, 1965.
[31] R James Milgram. Immersing projective spaces. *Annals of Mathematics*, pages 473–482, 1967.
[32] Himanee Narasimhan. The irreducibility of ladder determinantal varieties. *Journal of Algebra*, 102(1):162–185, 1986.
[33] Franklin P Peterson. Some non-embedding problems. *Bol. Soc. Mat. Mexicana (2)*, 2:9–15, 1957.
[34] Daniel B Shapiro. *Compositions of quadratic forms*, volume 33. Walter de Gruyter, 2000.
[35] DB Shapiro. Products of sums of squares. *Expo. Math*, 2:235–261, 1984.
[36] B Steer. On the embedding of projective spaces in euclidean space. *Proceedings of the London Mathematical Society*, 3(3):489–501, 1970.
[37] Cynthia Vinzant. A small frame and a certificate of its injectivity. *arXiv preprint arXiv:1502.04656*, 2015.
[38] Yang Wang and Zhiqiang Xu. Phase retrieval for sparse signals. *Applied and Computational Harmonic Analysis*, 37(3):531–544, 2014.
[39] Chris D White, Sujay Sanghavi, and Rachel Ward. The local convexity of solving systems of quadratic equations. *arXiv preprint arXiv:1506.07868*, 2015.
[40] Zhiqiang Xu. The minimal measurement number for low-rank matrices recovery. *Applied and Computational Harmonic Analysis* , https://doi.org/10.1016/j.acha.2017.01.005, 2017.

Department of Mathematics, The Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong
E-mail address: yangwang@ust.hk

LSEC, ICMSEC, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, China;
School of Mathematical Sciences, University of Chinese Academy of Sciences, Beijing 100049, China
E-mail address: xuzq@lsec.cc.ac.cn