Determination of all pure quantum states from a minimal number of observables

Damien Mondragon and Vladislav Voroninski

Department of Mathematics, University of California, Berkeley, CA 94720

May 7, 2014

Abstract

Ron Wright conjectured circa 1978 that there exist three observables A_1, A_2, A_3 which uniquely determine any pure state $x \in \mathbb{C}P^{n-1}$. It is now known that Wright's conjecture is false due to general obstructions to embedding $\mathbb{C}P^n$ into Euclidean space and it is natural to consider the minimal number of observables required for informational completeness. We prove in this paper that for any positive integer n, the map $x \in \mathbb{C}^n/\mathbb{S}^1 \mapsto \{|\langle x, z_i\rangle|^2\}_{i=1}^{4n} \in \mathbb{R}^{4n}$, where z_i are the rows of four generic $n \times n$ unitary matrices, is injective, yielding a family of quadratic embeddings of $\mathbb{C}P^{n-1}$ into $\mathbb{R}^{4(n-1)}$. In particular, this implies that four generic observables determine any pure state. This result is sharp for $n \geq 6$.

Keywords. Quantum tomography, Differential geometry, Phase retrieval, Real algebraic geometry, Nash stratification, Informationally complete measurements, Wright's conjecture.

1 Introduction

Consider the standard finite dimensional setting of Quantum Mechanics. Each state $x \in \mathbb{C}^n$ is unit norm and defined up to a global phase factor: $x \sim e^{i\theta}x$ for any $\theta \in \mathbb{R}$. An observable is a Hermitian operator A on $\mathbb{C}^n$ with eigenvalues λ_i and eigenspaces E_i. Taking a measurement of a state x with an observable yields λ_i with probability $\|\mathcal{P}_{E_i}(x)\|_2^2$, where $\mathcal{P}_{E_i}$ is the projection on eigenspace E_i. Generically, A has n distinct real eigenvalues $\lambda_1, \dots \lambda_n$ and in this case, the measurements are λ_i with probability $\|u_i u_i^*(x)\|_2^2 = |\langle u_i, x\rangle|^2$, where u_i are the eigenvectors of A. From now on, we identify an observable A with distinct eigenvalues, with a unitary matrix U that diagonalizes it.

The field of quantum tomography concerns itself with reconstructing a state x from knowledge of the probability distributions that arise from measuring it. Due to the exponential growth in the state space dimension of many-body systems, work in this field aims to recover low-rank mixed states from few measurements [17, 18, 23] [12]. A natural question is: what is the minimal number of observables needed to determine any state x?

Indeed, a conjecture was attributed to Ron Wright in 1978 that there exist 3 unitary $n \times n$ matrices U_1, U_2, U_3, such that for $x \in \mathbb{C}^n$, the measurements $\{|U_i(x)|\}_{i=1}^3$, where the modulus is taken

component-wise, determine any state x uniquely [26]. It is now known that Wright's conjecture is false since at least $4n - 2\alpha(n-1) - 4$, where $\alpha(n-1)$ is the number of 1's in the binary expansion of $n-1$, quadratic measurements of any kind are needed to determine every state [2, 20, 25], which essentially follows from general obstructions to embedding $\mathbb{C}P^n$ into $\mathbb{R}^m$ [19, 21, 22]. We shall refer to a set of observables $\{A_i\}_{i=1}^m$ as informationally complete, if they together determine any pure state $x \in \mathbb{C}P^{n-1}$. A slightly different convention is used in the field of phase retrieval, in which a set of quadratic measurements $|\langle z_i, x\rangle|^2, i = 1, 2, \dots m$, corresponding to m observables $z_i z_i^*, i = 1, 2, \dots, m$, is said to be injective modulo phase if it determines any $x \in \mathbb{C}^n/\mathbb{S}^1$, that is, modulo multiplication by a global phase factor.

There have been some recent breakthroughs in the study of informational completeness of quantum measurements. For instance, the authors of [4–7] showed that measurements with 4n-2 generic rank-1 observables are injective modulo phase and the authors of [8] gave an example of $4n-4$ specific rank 1 observables with the same property. It is conjectured in [20] that $4n-4$ is the minimal number of rank-1 observables required for injectivity modulo phase.

Note that a rank n observable corresponds to a collection of n rank-1 observables $\iff$ the n rank-1 observables form an orthonormal set. Thus, the setting of the papers referenced above is different than ours and to the best of our knowledge, our result is the first of its kind. In this paper we establish that 4 observables are generically sufficient to determine any pure state $x \in \mathbb{C}P^{n-1}$ and since by results of [20, 25], at least 4 observables are necessary to do so when $n \geq 6$, this result is sharp. Our work in particular provides a large family of collections of $4n-3$ rank-1 observables which are injective modulo phase, with each element of this family corresponding to a quadratic embedding of $\mathbb{C}P^{n-1}$ into $\mathbb{R}^{4(n-1)}$.

The study of phase retrieval, which in essence is quantum tomography of pure states, has been a topic of much recent activity. The authors of [9, 10, 24] formulated phase retrieval as a matrix recovery problem. In [24], this framework, called PhaseLift, is analyzed and the authors prove that PhaseLift recovers a fixed state with high probability from $O(n \log n)$ observables $z_i z_i^*$, provided the z_i are iid gaussian on the unit sphere. Moreover, they proved that PhaseLift is stable with respect to measurement noise. A further improvement by [11] showed that PhaseLift recovers all states with $O(n)$ gaussian observables and moreover the authors of [15], show that trace minimization is unnecessary since PhaseLift is actually a feasibility problem with high probability. In direct relevance to the setting of this paper, the author of [28] proved that there is some integer r, such that for n large enough, PhaseLift succeeds in recovering a fixed quantum state from the observables $A_1, \dots, A_r$ with high probability, with respect to Haar measure on $\mathbb{U}_n^r$. These results may also be extended to show stability of PhaseLift in this setting, as well as universality (recovery from all states, as opposed to a fixed state). There have also been other recent algorithmic advances in phase retrieval with recovery and stability guarantees. For instance, the authors of [1, 3] propose an approach that exploits a polarization identity and expander graphs to yield a computationally efficient approach to recovering states from specifically structured rank-1 observables. The authors of [13] formulate phase retrieval as class of instances of MAXCUT, and along with [27], show that PhaseLift is equivalent to the Goemans-Williamson relaxation on the corresponding instance of MAXCUT.

2 Main result

Consider $\mathbb{U}_n^4$, where $\mathbb{U}_n \in \mathbb{C}^{n\times n}$ is the group of unitary $n \times n$ matrices. Letting $\mathbb{H}_n$ be the set of Hermitian $n \times n$ matrices, we will identify $\mathbb{U}_n^4$ with a set of linear maps

$$\mathcal{A} : \mathbb{H}_n \to \mathbb{R}^{4n}$$

by defining, for any $A \in \mathbb{C}^{m\times n}$,

$$\mathcal{A}_A(X) = \{\mathrm{Tr}(z_i z_i^* X)\}_{i=1}^m$$

where z_i are the rows of A. The restriction of $\mathcal{A}$ to the set of rank-1 Hermitian non-negative definite matrices may be considered as a map from $\mathbb{C}^n/\mathbb{S}^1$ to $\mathbb{R}^m$:

$$x \in \mathbb{C}^n/\mathbb{S}^1 \mapsto xx^* \in \mathbb{H}_n \mapsto \mathcal{A}_A(xx^*) = \{|\langle x, z_i\rangle|^2\}_{i=1}^m \in \mathbb{R}^m$$

Similarly, a quadratic map from $\mathbb{C}P^{n-1} \mapsto \mathbb{R}^m$ factors through the restriction of $\mathcal{A}$ to unit norm rank-1 Hermitian positive definite matrices:

$$x \in \mathbb{C}P^{n-1} \mapsto \mathcal{A}\left(\frac{xx^*}{\|x\|_2^2}\right) \in \mathbb{R}^m$$

We call $A \in \mathbb{U}_n^4$ injective modulo phase if for any $x, y \in \mathbb{C}^n$,

$$\mathcal{A}_A(xx^*) = \mathcal{A}_A(yy^*) \implies xx^* = yy^*$$

Note that $\mathbb{U}_n^4$ is a redundant representation of maps $\mathcal{A}$ in the sense that for any $A \in \mathbb{U}_n^4$, only the range of $\bar{A}$ determines whether A is injective mod phase [6]. That is, if $A \in \mathbb{U}_n^4$, then A is injective mod phase $\iff$ every element of $A\mathbb{U}_n$ is injective mod phase. We can now state the main theorem:

Theorem 2.1 *Consider $\mathbb{U}_n$, for $n \geq 1$, acting on $\mathbb{U}_n^4$ by right multiplication and let π_1 be the quotient map of this action. Let*

$$\mathcal{F} = \{A \in \mathbb{U}_n^4; \exists x, y \in \mathbb{C}^n, xx^* \neq yy^*, \mathcal{A}_A(xx^*) = \mathcal{A}_A(yy^*)\}$$

That is, $\mathcal{F}$ is the set of non-injective mod phase elements of $\mathbb{U}_n^4 \subseteq \mathbb{C}^{4n\times n}$. Then, $\pi_1(\mathcal{F})$ is a set of measure zero in $\pi_1(\mathbb{U}_n^4) = \mathbb{U}_n^4/\mathbb{U}_n \cong \mathbb{U}_n^3$, with respect to Haar measure on $\mathbb{U}_n^3$. Thus, almost every quadruple of observables determines any pure state. Moreover, this result is sharp in that for $n \geq 6$, at least 4 observables are required to form an informationally complete set.

Corollary 2.2 *When $n \geq 1$, for almost every element $A \in \mathbb{U}_n^4$, the map*

$$x \in \mathbb{C}P^{n-1} \mapsto \{\frac{1}{\|x\|_2^2}\left(\left|\langle u_i^1, x\rangle\right|^2, \left|\langle u_i^2, x\rangle\right|^2, \left|\langle u_i^3, x\rangle\right|^2, \left|\langle u_i^4, x\rangle\right|^2\right)\}_{i=1}^{n-1} \in \mathbb{R}^{4(n-1)}$$

is an embedding of $\mathbb{C}P^{n-1}$ into $\mathbb{R}^{4(n-1)}$, where u_i^j are the rows of A.

The corollary follows by results in [20,25], in which it is shown that each A of $\mathbb{C}^{m\times n}$ gives a smooth map from $\mathbb{C}P^{n-1}$ into $\mathbb{R}^m$:

$$x \in \mathbb{C}P^{n-1} \mapsto \frac{xx^*}{\|x\|_2^2} \in \mathbb{H}_n \mapsto \frac{1}{\|x\|_2^2}\mathcal{A}_A(xx^*) \in \mathbb{R}^m$$

and that this map is an embedding $\iff$ $\mathcal{A}_A$ is injective on rank-1 Hermitian matrices. Since we are factoring through rank-1 matrices of unit norm, it is enough to keep all but the last measurement from each unitary matrix to retain injectivity over rank-1 matrices (and thus the embedding property of the resulting map into $\mathbb{R}^{4(n-1)}$), because when when the norm of x is known, we may determine $|\langle u_n, x\rangle|^2$ as $1 - \sum_{i=1}^{n-1} |\langle u_i, x\rangle|^2$, where u_i are the rows of any unitary matrix U.

The sharpness of the main result for $n \geq 6$ follows from results of [25]. The rest of theorem 2.1 is proven in the next section.

In reference to an open problem in phase retrieval [20], note that by keeping all measurements from U_1 and throwing away the last from U_2, U_3, U_4, we get that $4n-3$ observables which come from 4 generic unitary matrices, determine any $x \in \mathbb{C}^n/\mathbb{S}^1$.

2.1 Proof of the main result, Theorem 2.1.

We begin with some simplifying lemmas. Lemma 9 in [2] is similar in spirit, but we can say something stronger in our more specific setting:

Lemma 2.3 *Let $A \in \mathbb{U}_n^4$ and call $\mathcal{A} = \mathcal{A}_A$. Then A is not injective mod phase $\iff$ there is a rank-2 Hermitian matrix with eigenvalues $1, -1$ in the nullspace of $\mathcal{A}$.*

Proof First, take any rank-2 indefinite matrix X. It can clearly be written as $X = xx^* - yy^*$ for some non-zero $x, y \in \mathbb{C}^n$. If $\mathcal{A}(X) = 0$, then $\mathcal{A}(xx^*) = \mathcal{A}(yy^*)$ and thus A is not injective modulo phase.

Now, assume that A is not injective modulo phase. Thus $\mathcal{A}(xx^*) = \mathcal{A}(yy^*)$ for some $x, y \in \mathbb{C}^n$ such that $xx^* \neq yy^*$. Defining $X = xx^* - yy^*$, this gives $\mathcal{A}(X) = 0$. We have that necessarily $xx^* \neq 0$ and $yy^* \neq 0$ because if, say wlog $xx^* = 0$, then $\mathcal{A}(xx^*) = 0 \implies \mathcal{A}(yy^*) = 0$, but since

$$0 = \|\mathcal{A}(yy^*)\|_1 = \sum_{i=1}^m \mathrm{Tr}(yy^* z_i z_i^*) = \sum_{i=1}^m |\langle z_i, y\rangle|^2 = r\|y\|_2^2$$

, this implies that $y = 0$, which contradicts $xx^* \neq yy^*$. Thus X is an indefinite Hermitian matrix. By linearity, we can assume that $\|X\|_F = \sqrt{2}$, where $\|.\|_F$ is the Frobenius norm. Now, consider the eigenvalue decomposition of $X = xx^* - yy^*$:

$$X = \lambda_1 uu^* + \lambda_2 vv^*$$

with eigenvalues $\lambda_1 > 0, \lambda_2 < 0$. where $\langle u, v\rangle = 0$ and $\|u\|_2 = \|v\|_2 = 1$. Then since $\mathcal{A}(X) = 0$, we have $\lambda_1 \mathcal{A}(uu^*) = -\lambda_2 \mathcal{A}(vv^*)$ and since $\mathcal{A}(uu^*) \geq 0$, we have

$$\lambda_1 \|\mathcal{A}(uu^*)\|_1 = -\lambda_2 \|\mathcal{A}(vv^*)\|_1 \implies \lambda_1 = -\lambda_2$$

because $\|\mathcal{A}(uu^*)\|_1 = \|\mathcal{A}(vv^*)\|_1 = r$. By $\|X\|_F^2 = 2 = \lambda_1^2 + \lambda_2^2$, we have $\lambda_1 = 1, \lambda_2 = -1$. Thus, if $\mathcal{A}$ is not injective modulo phase, there exists a rank 2 indefinite Hermitian matrix in the nullspace of $\mathcal{A}$, with eigenvalues 1, -1. ■

Letting $e_i \in \mathbb{C}^n$ denote the standard basis vectors, define the set

$$N_{e_1,e_2} = \{A \in \mathbb{U}_n^4; \mathcal{A}_A(e_1e_1^* - e_2e_2^*) = 0\}$$

Lemma 2.4 *Let π_1 denote the quotient map associated to the action of $\mathbb{U}_n$ by right multiplication on $\mathbb{U}_n^4$. Then $\pi_1(\mathcal{F}) = \pi_1(N_{e_1,e_2})$.*

Proof Note that $N_{e_1,e_2} \subseteq \mathcal{F}$. Assume that some $\mathcal{A}_A$, corresponding to $A \in \mathbb{U}_n^4$, is not injective mod phase. By above, we must have $\mathcal{A}_A(xx^* - yy^*) = 0$ for some unit normed and orthogonal $x, y \in \mathbb{C}^n$. Now, take some $U \in \mathbb{U}_n$ such that $Ue_1 = \bar{x}, Ue_2 = \bar{y}$. Then, $\mathcal{A}_{AU}$ satisfies

$$\mathcal{A}_{AU}(e_1e_1^* - e_2e_2^*) = \mathcal{A}(xx^* - yy^*) = 0.$$

Since $\pi_1(AU) = \pi_1(A)$, we have that

$$A \in \mathcal{F} \implies N_{e_1,e_1} \bigcap A\mathbb{U}_n \neq \emptyset.$$

This, coupled with $N_{e_1,e_2} \subseteq \mathcal{F}$, implies that $\pi_1(\mathcal{F}) = \pi_1(N_{e_1,e_2})$. ■

The point of this lemma is that since $\pi_1(\mathcal{F}) = \pi_1(N_{e_1,e_2})$, it suffices to show that $\pi_1(N_{e_1,e_2})$ has measure zero in $\mathbb{U}_n^4/\mathbb{U}_n$ to establish the main theorem.

Lemma 2.5 *Let M be a smooth manifold and let G, G' be compact Lie groups which act smoothly, freely and properly on M, such that $G' \leq G$. Assume that (M, B, π, F) is a fiber bundle with projection map π, base space B and fiber F, such that $\pi(pG') = \pi(p)$ for any $p \in M$. Now, let N' be a submanifold of B. Then, $N = \pi^{-1}(N')$ is a G'-stable submanifold of M, with*

$$\dim(N) = \dim(N') + \dim(F),$$

and if

$$\dim(N/G') < \dim(M/G),$$

we have that N/G has measure zero in any chart on M/G. In particular, if M/G is a Lie group, N/G has measure zero with respect to the Haar measure on M/G.

Proof By properties assumed of G and M, M/G is a smooth manifold and the quotient map

$$\pi_1 : M \mapsto M/G$$

is smooth. Moreover,

$$\dim(M/G) = \dim(M) - \dim(G).$$

Since M is a fiber bundle, we have that for any point $p \in M$, there is a chart

$$\Big(U \times Y \subseteq M, \phi : p \in U \times Y \mapsto (u_1, u_2, \dots u_l, x_1, \dots x_n) \in U' \times Y' \subseteq \mathbb{R}^{\dim(B)} \times \mathbb{R}^{\dim(F)})\Big)$$

where $l = \dim(B)$, U is an open neighborhood of $\pi(p)$ and U' and Y' are open subsets of $\mathbb{R}^{\dim(B)}$ and $\mathbb{R}^{\dim(F)}$. Now, since N' is a submanifold of the base space B, and $(U, u_1, \dots u_l)$ is a chart for $\pi(p) \in B$, we can refine the coordinates $u_1, \dots, u_l$ such that the submanifold N' can be expressed locally as $(u_1 = 0, \dots u_r = 0, u_{r+1}, \dots u_l)$, where $r = \dim(B) - \dim(N')$. Therefore,

$$(u_1 = 0, \dots u_r = 0, u_{r+1}, \dots u_l, x_1, \dots x_n)$$

gives coordinates for N as a submanifold of M. Note that N is G'-stable. The action of G' on M restricts to a smooth and free action on N, which is furthermore proper since G' is compact. We then have that the associated quotient map

$$\pi_2 : N \mapsto N/G'$$

is a surjective submersion and N/G' is a smooth manifold, with $\dim(N/G') = \dim(N) - \dim(G')$. Since N is a submanifold, π_1 restricts to a smooth map on N and thus, since $\pi_1|_N = g \circ \pi_2$, where

$$g : N/G' \mapsto M/G$$

sends an element of N/G' to its G-orbit in M/G, we have that g is smooth by Proposition 5.19 in [16]. By construction,

$$N/G = \pi_1(N) = g \circ \pi_2(N) = g(N/G') \subseteq M/G.$$

Thus, N/G is the image of a smooth map, in a manifold of dimension $\dim(M) - \dim(G)$, from a manifold of dimension $\dim(N) - \dim(G') < \dim(M) - \dim(G)$. By Sard's theorem, we have therefore that N/G has measure zero in M/G.

■

Using the notation of Lemma 2.5, let $M = \mathbb{U}_n^4$, $G = \mathbb{U}_n$ and

$$G' = \{U \in \mathbb{U}_n; |e_i^* U e_i| = 1, i = 1, 2\} \cong \mathbb{S}^1 \times \mathbb{S}^1 \times \mathbb{U}_{n-2}.$$

Consider G, G' acting by right multiplication on M. We will show that the set N_{e_1,e_2} can be expressed as a union of manifolds which satisfy the properties of N in Lemma 2.5.

First note that G and G' both act smoothly, freely and properly by right multiplication on M, the last property due to each being a compact Lie group. Define

$$G'' = \{\{U_i\}_{i=1}^4 \in \mathbb{U}_n^4; |e_1^* U_i e_1| = |e_2^* U_i e_2| = 1, i = 1, \dots, 4, e_j^* U_l e_j = e_j^* U_k e_j, j = 1, 2. \quad 1 \leq l < k \leq 4\}$$

as a subgroup of the product Lie group $\mathbb{U}_n^4$ and let G'' act on $\mathbb{U}_n^4$ by right multiplication in each component. Since G'' is a closed Lie subgroup of $\mathbb{U}_n^4$, we have that

$$(M = \mathbb{U}_n^4, B = \mathbb{V}_2(\mathbb{C}^n)^4/(\mathbb{S}^1 \times \mathbb{S}^1), \pi, F = \mathbb{S}^1 \times \mathbb{S}^1 \times \mathbb{U}_{n-2}^4 \cong G'')$$

is a fiber bundle, with base space

$$B = \mathbb{U}_n^4/G'' \cong \mathbb{V}_2(\mathbb{C}^n)^4/(\mathbb{S}^1 \times \mathbb{S}^1),$$

where $\mathbb{V}_2(\mathbb{C}^n)$ is the Stiefel manifold of complex orthonormal 2-frames, the projection map π is the quotient map associated to the action of G'' and the fiber F is diffeomorphic to $G'' \cong \mathbb{S}^1 \times \mathbb{S}^1 \times \mathbb{U}_{n-2}^4$. The quotient by $\mathbb{S}^1 \times \mathbb{S}^1$ is to be interpreted as given by the equivalence relation

$$(u_1^1, \dots u_1^4, u_2^1, \dots u_2^4) \equiv (e^{i\theta_1}u_1^1, \dots e^{i\theta_1}u_1^4, e^{i\theta_2}u_2^1, \dots e^{i\theta_2}u_2^4)$$

for any $\theta_i \in \mathbb{R}$.

It is clear that for any $p \in \mathbb{U}_n^4$, we have $\pi(pG') = \pi(p)$, since G' can be thought of as a subgroup of G'' in the product Lie group $\mathbb{U}_n^4$. Moreover, $M/G \cong \mathbb{U}_n^3$ is a compact Lie group. Thus, G, G' and (M, B, π, F) satisfy the conditions of Lemma 2.5.

Consider $P = \pi(N_{e_1,e_2}) = N_{e_1,e_2}/G''$ as a subset of the base space. We state here an intermediary theorem which we prove in the next section:

Theorem 2.6 *P may be expressed as*

$$P = \bigcup_{\alpha=1}^{k} P'_\alpha \subseteq \mathbb{V}_2(\mathbb{C}^n)^4/(\mathbb{S}^1 \times \mathbb{S}^1),$$

for some integer k, where each P'_α is a submanifold of $\mathbb{V}_2(\mathbb{C}^n)^4/(\mathbb{S}^1 \times \mathbb{S}^1)$ and $\dim(P'_\alpha) \leq 4(3n-3)-2$.

Thus, using this theorem, Lemma 2.5, and noting that N_{e_1,e_2} is G''-stable, we have that

$$N_{e_1,e_2} = \pi^{-1}(P) = \pi^{-1}(\bigcup_{\alpha=1}^{k} P'_\alpha) = \bigcup_{\alpha=1}^{k} \pi^{-1}(P'_\alpha)$$

is itself a union of submanifolds: $N_{e_1,e_2} = \bigcup_{\alpha=1}^{k} P_\alpha$, where $P_\alpha = \pi^{-1}(P'_\alpha)$ and furthermore,

$$\dim(P_\alpha) \leq \dim(P'_\alpha) + \dim(F) = \dim(P'_\alpha) + \dim(\mathbb{S}^1 \times \mathbb{S}^1 \times \mathbb{U}_{n-2}^4) \leq 4(3n-3) + 4(n-2)^2$$

Also, each P_α is G'-stable, and modding out by G' we have

$$\dim(P_\alpha/G') = \dim(P_\alpha) - \dim(G') = 3n^2 - 2.$$

Thus, since $\dim(P_\alpha/G') \leq 3n^2 - 2 < 3n^2 = \dim(M/G)$, Lemma 2.5 gives that each P_α/G has measure zero in M/G.

Now, since

$$\pi_1(N_{e_1,e_2}) = \pi_1(\bigcup_{\alpha=1}^{k} P_\alpha) = \bigcup_{\alpha=1}^{k} \pi_1(P_\alpha),$$

we have that $N_{e_1,e_2}/G$ has measure zero in $\mathbb{U}_n^4/G$, because the union is finite. This implies that $\mathcal{F}/\mathbb{U}_n$ has measure zero in $\mathbb{U}_n^4/\mathbb{U}_n$, completing the proof of Theorem 2.1.

2.2 Proof of Theorem 2.6

Define the space $Z = (\mathbb{C}^{2n})^4/\mathbb{S}^1 \times \mathbb{S}^1 = (\mathbb{R}^{4n})^4/\mathbb{S}^1 \times \mathbb{S}^1$ and consider

$$P = N_{e_1,e_2}/(\mathbb{S}^1 \times \mathbb{S}^1 \times \mathbb{U}^r_{n-2}) \subseteq B = \mathbb{V}_2(\mathbb{C}^n)^4/(\mathbb{S}^1 \times \mathbb{S}^1) \subseteq Z.$$

We have $P =$

$$\{\{(u_1^j, u_2^j)\}_{j=1}^4 \in (\mathbb{C}^{2n})^4; \|u_1^j\|_2 = \|u_2^j\|_2 = 1, \left\langle u_1^j, u_2^j \right\rangle = 0, \left|u_{1i}^j\right|^2 = \left|u_{2i}^j\right|^2, i = 1, 2, \dots n, j = 1, 2, 3, 4\}/(\mathbb{S}^1 \times \mathbb{S}^1).$$

For $1 \leq i < j \leq n$, at a point $z \in Z$ for which $u_{1i}^1 \neq 0, u_{2j}^1 \neq 0$, consider the following charts on Z,

$$\left(U_{ij} = \{\{(u_1^j, u_2^j)\}_{j=1}^4 \in Z; u_{1i}^1 \neq 0, u_{2j}^1 \neq 0\}, \phi_{ij}\right)$$

The coordinate maps ϕ_{ij} on these charts send

$$\{(u_1^j, u_2^j)\}_{j=1}^4 \in Z \mapsto (\pi_{/ij}(e^{i\theta_1}u_1^j, e^{i\theta_2}u_2^j), \{(e^{i\theta_1}u_1^j, e^{i\theta_2}u_2^j)\}_{j=2}^4) \in \mathbb{R}^{4n \times 4-2}$$

where $\pi_{/ij}$ takes $(u_1^1, u_2^1) \in \mathbb{C}^{2n}$ to $\mathbb{R}^{4n-2}$ by keeping all but the imaginary parts of u_{1i}^1 and u_{2j}^1 and $e^{i\theta_1}, e^{i\theta_2}$ are chosen such that $im(u_{1i}^1) = 0$ and $im(u_{2j}^1) = 0$.

By orthonormality of vectors in $\mathbb{V}_2(\mathbb{C}^n)$, we have that

$$P = \bigcup_{1 \leq i < j \leq n} P \cap U_{ij}$$

Define

$$W = \{(u_1, u_2) \in \mathbb{V}_2(\mathbb{C}^n); |u_{1i}| = |u_{2i}|, i = 1, 2 \dots n\} \subseteq \mathbb{C}^{2n}$$

where $\mathbb{V}_2(\mathbb{C}^n)$ is the Steifel manifold of two orthonormal complex n-dimensional vectors, and let

$$W_{ij} = \{(u_1, u_2) \in W; u_{1i} \neq 0, u_{2j} \neq 0, im(u_{1i}) = im(u_{2j}) = 0\} \subseteq \mathbb{C}^{2n}$$

In coordinates on the charts U_{ij}, we have

$$\phi_{ij}(P \cap U_{ij}) = \pi_{/ij}(W_{ij}) \times W^3$$

Lemma 2.7 *W and W_{ij} are semialgebraic sets in $\mathbb{R}^{4n}$, with $\dim(W) \leq 3n - 3$ and $\dim(W_{ij}) \leq 3n - 5$.*

By the Nash stratification theorem, Proposition 9.1.8 in [14], any semialgebraic set is a union of Nash submanifolds. Therefore, we can express any $P \cap U_{ij}$ as a union of Nash submanifolds of U_{ij} and therefore P is a union of submanifolds of Z. Now, since B is a submanifold of Z and $P \subseteq B$, P is also a union of submanifolds of B (by submanifold we always mean embedded submanifold). The dimension of any of these submanifolds is clearly upper bounded by

$$\dim(\pi_{/ij}(W_{ij}) \times W^3) \leq 4(3n - 3) - 2$$

Since $\pi_{/ij}$ cannot increase algebraic dimension, this completes the proof of theorem 2.6, once we prove the lemma 2.7 below.

2.3 Proof of Lemma 2.7

2.4 An Auxiliary Variety

Let I denote the ideal

$$(f_1, \ldots, f_n, g, h_1, h_2) \subset \mathbb{R}[x_1, \ldots, x_n, y_1, \ldots, y_n, v_1, \ldots, v_n, w_1, \ldots, w_n]$$

where

$$f_i = x_i^2 + y_i^2 - 1, \quad g = \sum_{j=1}^{n}(v_j^2 + w_j^2) - 1, \quad h_1 = \sum_{j=1}^{n}(v_j^2 + w_j^2)x_j, \quad h_2 = \sum_{j=1}^{n}(v_j^2 + w_j^2)y_j$$

Lemma 2.8 *Let X be the algebraic set in $\mathbb{R}^{4n}$ defined by the ideal I. Then X is a smooth scheme-theoretic complete intersection of dimension $3n-3$.*

Proof There is a smooth action of $(\mathbb{S}^1)^n$ on $\mathbb{R}^{4n}$, defined by

$$(\mu, (v, w, x, y)) \in (\mathbb{S}^1)^n \times \mathbb{R}^{4n} \mapsto (\mu \circ (v + iw), x + iy)$$

Since for each μ, this map is a diffeomorphism, the Zariski tangent spaces of X will be isomorphic along orbits of this action and thus we need only consider a representative of each orbit. In particular, we consider points where $w_i = 0$ for all i.

The tangent space at a point $p = (\tilde{v}_1, \ldots, \tilde{v}_n, \tilde{w}_1 = 0, \ldots, \tilde{w}_n = 0, \tilde{x}_1, \ldots, \tilde{x}_n, \tilde{y}_1, \ldots, \tilde{y}_n) \in X$ is the orthogonal complement of the subspace spanned by the following differentials:

$$F_i = \tilde{x}_i \frac{\partial}{\partial x_i} + \tilde{y}_i \frac{\partial}{\partial y_i}, \quad i = 1, 2, \ldots, n$$

$$G = \sum_{i=1}^{n} 2\tilde{v}_i \frac{\partial}{\partial v_i}$$

$$H_1 = \sum_{i=1}^{n} 2\tilde{v}_i\tilde{x}_i \frac{\partial}{\partial v_i} + \tilde{v}_i^2 \frac{\partial}{\partial x_i}$$

$$H_2 = \sum_{i=1}^{n} 2\tilde{v}_i\tilde{y}_i \frac{\partial}{\partial v_i} + \tilde{v}_i^2 \frac{\partial}{\partial y_i}$$

We will show that these differentials are linearly independent at every point $p \in X$, thereby establishing that $\dim(T_p(X)) = 4n - (3n+3) = 3n - 3$.

Suppose $(\sum_{i=1}^{n} a_i F_i) + bG + cH_1 + dH_2 = 0$ for some $(a_1, \ldots, a_n, b, c, d) \in \mathbb{R}^{n+3}$. Then, collecting terms we get the following:

$$(\frac{\partial}{\partial x_i}) \quad \alpha_i := a_i\tilde{x}_i + c\tilde{v}_i^2 = 0$$

$$(\frac{\partial}{\partial y_i}) \quad \beta_i := a_i\tilde{y}_i + d\tilde{v}_i^2 = 0$$

$$(\frac{\partial}{\partial v_i}) \quad \gamma_i := \tilde{v}_i(b + c\tilde{x}_i + d\tilde{y}_i) = 0$$

Define

$$\tilde{f}_1 = f_1(p), \ldots, \tilde{f}_n = f_n(p), \quad \tilde{g} = g(p), \quad \tilde{h}_1 = h_1(p), \quad \tilde{h}_2 = h_2(p)$$

Since $p \in X$, $\tilde{f}_i = \tilde{g} = \tilde{h}_1 = \tilde{h}_2 = 0$ and in particular,

$$\begin{aligned} 0 &= b\tilde{g} + c\tilde{h}_1 + d\tilde{h}_2 \\ &= b(\sum_{i=1}^{n} \tilde{v}_i^2 - 1) + c\sum_{i=1}^{n} \tilde{x}_i\tilde{v}_i^2 + d\sum_{i=1}^{n} \tilde{y}_i\tilde{v}_i^2 \\ &= \left(\sum_i \tilde{v}_i(\tilde{v}_i(b + c\tilde{x}_i + d\tilde{y}_i))\right) - b \\ &= \left(\sum_i \tilde{v}_i(\gamma_i)\right) - b = -b \end{aligned}$$

Thus $b = 0$.

Note that since $\tilde{g} = 0$, not all $\tilde{v}_i = 0$. Say, without loss of generality, that $\tilde{v}_1 \neq 0$. Then since $\gamma_1 = 0$,

$$b + c\tilde{x}_1 + d\tilde{y}_1 = c\tilde{x}_1 + d\tilde{y}_1 = 0$$

Continuing,

$$\begin{aligned} 0 &= c\alpha_1 + d\beta_1 \\ &= c(a_1\tilde{x}_1 + c\tilde{v}_1^2) + d(a_1\tilde{y}_1 + d\tilde{v}_1^2) \\ &= a_1(c\tilde{x}_1 + d\tilde{y}_1) + (c^2 + d^2)\tilde{v}_1^2 \\ &= (c^2 + d^2)\tilde{v}_1^2 \end{aligned}$$

Since $\tilde{v}_1^2 \neq 0$, $c^2 + d^2 = 0$ and hence $c = d = 0$ as $c, d \in \mathbb{R}$.

But then, $\tilde{x}_i\alpha_i + \tilde{y}_i\beta_i = a_i(\tilde{x}_i^2 + \tilde{y}_i^2) = 0$. As $\tilde{f}_i = 0$, we have $a_i(\tilde{x}_i^2 + \tilde{y}_i^2) = a_i$ and thus $a_i = 0$ for all i. We've thereby shown that $(a_i, b, c, d) = 0$ and hence X is smooth of dimension $\dim T_pX = 4n - (n + 3) = 3n - 3$. ■

Note that by pairing real coordinates into complex ones, X may be written set-theoretically as:

$$X = \{(v+iw, x+iy) \in \mathbb{R}^{4n}; (x+iy)\circ(x-iy) = 1, \langle v + iw, v + iw\rangle = 1, \langle v + iw, (v + iw) \circ (x + iy)\rangle = 0\}$$

where $\circ$ denotes the Hadamard product.

For the following two corollaries, we will need the polynomial map:

$$S : (v, w, x, y) \in \mathbb{R}^{4n} \mapsto (v + iw, (v + iw) \circ (x + iy)) \in \mathbb{R}^{4n}$$

The equations defining X in complex coordinates say that S surjects X onto W. Since S is a semialgebraic map, we have $\dim(W) \leq \dim(X) = 3n - 3$. We've shown:

Corollary 2.9 $\dim W \leq 3n - 3$

We will have thus completed the proof of Lemma 2.7 once we show:

Corollary 2.10 $\dim W_{ij} \leq 3n-5$

Proof Consider the linear map ϕ_j defined on $\mathbb{R}^{4n}$ as

$$\begin{aligned}&(u_{11},\ldots,u_{1n},u_{21},\ldots,u_{2n})\\ &\quad\mapsto (u_{11},\ldots,u_{1(j-1)},u_{2j},u_{1(j+1)},\ldots,u_{1n},u_{21},\ldots,u_{2(j-1)},\bar{u}_{1j},u_{2(j+1)},\ldots,u_{2n})\end{aligned}$$

i.e. the identity on all components of $(u_1,u_2)\in\mathbb{C}^{2n}$ except the j-th ones where it sends

$$(re(u_{1j}),im(u_{1j}),re(u_{2j}),im(u_{2j}))\mapsto(re(u_{2j}),im(u_{2j}),re(u_{1j}),-im(u_{1j}))$$

This map is semialgebraic and it is easy to verify that it is a bijection between W_{ij} and

$$W'_{ij}:=\{(u_1,u_2)\in W; u_{1i}\neq 0, u_{1j}\neq 0, im(u_{1i})=im(u_{1j})=0\}.$$

Therefore, it is enough to upper bound the dimension of W'_{ij}. Again, wlog, we take $i=1,j=2$.

Consider the subvariety

$$\begin{aligned}Y&:=\{(v+iw,x+iy)\in X; w_1=w_2=0\}\\ &=\{(v+iw,x+iy)\in\mathbb{R}^{4n}; w_1=w_2=0,|x+iy|=1,\langle v+iw,v+iw\rangle=1,\langle v+iw,(v+iw)\circ(x+iy)\rangle=0\}\\ &\subseteq X\end{aligned}$$

This clearly surjects onto $\{(u_1,u_2)\in W; im(u_{1i})=im(u_{1j})=0\}\supseteq W'_{ij}$ via the map S defined above. Thus, it will be enough to show $\dim Y\leq 3n-5$.

$\mathbb{C}^{2n}$ admits an action of $(\mathbb{S}^1)^{n-2}$ on the final $n-2$ components of the first vector, which is just the restriction of the $(\mathbb{S}^1)^n$ action on $\mathbb{C}^{2n}$ to the subgroup $(\mathbb{S}^1)^{n-2}\hookrightarrow(\mathbb{S}^1)^n$ where $(\mu_3,\ldots,\mu_n)\mapsto(1,1,\mu_3,\ldots,\mu_n)$. Tangent space dimensions are equal along orbits of this action and so, as above, we need only consider representatives where all $w_i=0$. At such a point $p=(\tilde{v}_1,\ldots,\tilde{v}_n,\tilde{w}_1=0,\ldots,\tilde{w}_n=0,\tilde{x}_1,\ldots,\tilde{x}_n,\tilde{y}_1,\ldots,\tilde{y}_n)\in X$, the tangent space is the orthogonal complement (in the vector space spanned by $\frac{\partial}{\partial v_i},\frac{\partial}{\partial w_i},\frac{\partial}{\partial x_i},\frac{\partial}{\partial y_i}, i=1,2\ldots,n$) of the vectors

$$\begin{aligned}&\frac{\partial}{\partial w_1},\quad \frac{\partial}{\partial w_2}\\ &F_i=\tilde{x}_i\frac{\partial}{\partial x_i}+\tilde{y}_i\frac{\partial}{\partial y_i},\quad i=1,2,\ldots,n\\ &G=\sum_{i=1}^n 2\tilde{v}_i\frac{\partial}{\partial v_i}\\ &H_1=\sum_{i=1}^n 2\tilde{v}_i\tilde{x}_i\frac{\partial}{\partial v_i}+\tilde{v}_i^2\frac{\partial}{\partial x_i}\\ &H_2=\sum_{i=1}^n 2\tilde{v}_i\tilde{y}_i\frac{\partial}{\partial v_i}+\tilde{v}_i^2\frac{\partial}{\partial y_i}\end{aligned}$$

That is,

$$T_pY = \mathbb{R}\left\langle \frac{\partial}{\partial w_i}, \frac{\partial}{\partial v_i}, \frac{\partial}{\partial x_i}, \frac{\partial}{\partial y_i} \right\rangle / \mathbb{R}\left\langle \frac{\partial}{\partial w_1}, \frac{\partial}{\partial w_2}, F, G, H_1, H_2 \right\rangle$$
$$\cong \mathbb{R}\left\langle \frac{\partial}{\partial w_3}, \ldots, \frac{\partial}{\partial w_n} \right\rangle \oplus \left(\mathbb{R}\left\langle \frac{\partial}{\partial v_i}, \frac{\partial}{\partial x_i}, \frac{\partial}{\partial y_i} \right\rangle / \mathbb{R}\left\langle F, G, H_1, H_2 \right\rangle\right)$$

the last isomorphism since none of F, G, H_1, H_2 involve w's. Note that in the course of proving Lemma 2.8 we actually showed $\dim \mathbb{R}\left\langle \frac{\partial}{\partial v_i}, \frac{\partial}{\partial x_i}, \frac{\partial}{\partial y_i} \right\rangle / \mathbb{R}\left\langle F, G, H_1, H_2 \right\rangle = 2n-3$ so that the tangent space of Y has dimension $(n-2)+(2n-3) = 3n-5$ everywhere, implying Y is smooth of dimension $3n-5$. ■

3 Acknowledgements

We are thankful to Andre Kornell, Harold Williams, Emmanuel Candes and Richard Schoen for fruitful discussions, to Ben McMillan and Bernd Sturmfels for detailed comments on a near-final version of the manuscript, and to Thomas Strohmer for introducing us to Wright's conjecture. We are particularly grateful to Daniel Cristofaro-Gardiner for some very helpful suggestions. We are also thankful to Dustin Mixon for maintaining his research blog "Short, Fat Matrices", via which we first became aware that Wright's conjecture is false and of the embedding obstructions that give lower bounds on the required number of measurements. A special thanks goes out to Y Combinator, for providing an entirely orthogonal effort, during which the ideas for this paper were conceived as a hedge.

References

[1] Dustin G. Mixon Afonso S. Bandeira, Yutong Chen. Phase retrieval from power spectra of masked signals. *http://arxiv.org/abs/1303.4458*.

[2] Dustin G. Mixon Aaron A. Nelson Afonso S. Bandeira, Jameson Cahill. Saving phase: Injectivity and stability for phase retrieval. *http://arxiv.org/abs/1302.4618*, 2013.

[3] M. Fickus D. G. Mixon B. Alexeev, A. S. Bandeira. Phase retrieval with polarization. *arXiv:1210.7752*, 2012.

[4] R. Balan, B. Bodmann, P.G. Casazza, and D. Edidin. Fast algorithms for signal reconstruction without phase. In *Wavelets XII*, volume 6701 of *Proc. SPIE*, pages 670111920–670111932, 2007.

[5] R. Balan, B. Bodmann, P.G. Casazza, and D. Edidin. Painless reconstruction from magnitudes of frame coefficients. *J. Four. Anal. Appl.*, 15:488–501, 2009.

[6] R. Balan, P.G. Casazza, and D. Edidin. On signal reconstruction without noisy phase. *Appl. Comp. Harm. Anal.*, 20:345–356, 2006.

[7] R. Balan, P.G. Casazza, and D. Edidin. Equivalence of reconstruction from the absolute value of the frame coefficients to a sparse representation problem. *IEEE Sig. Proc. Letters*, 14(5):341–343, 2007.

[8] Nathaniel Hammen Bernhard G. Bodmann. Stable phase retrieval with low-redundancy frames. *arXiv:1302.5487*.

[9] E.J. Candès, Y.C. Eldar, T. Strohmer, and V. Voroninski. Phase retrieval via matrix completion. *Preprint*, 2011.

[10] A. Chai, M. Moscoso, and G. Papanicolaou. Array imaging using intensity-only measurements. Technical report, Stanford University, 2010.

[11] X. Li E.J. Candes. Solving quadratic equations via phaselift when there are about as many equations as unknowns. *arXiv:1208.6247*.

[12] D. Gross. Recovering low-rank matrices from few coefficients in any basis, 2009. Available at http://arvix.org/abs/0910.1879.

[13] S. Mallat I. Waldspurger, A. dAspremont. Phase recovery, maxcut and complex semidefinite program- ming. *arXiv:1206.0102*, 2012.

[14] Marie-Francoise Roy Jacek Bochnak, Michel Coste. *Real Algebraic Geometry*. Springer, 1998.

[15] P. Hand L. Demanet. Stable optimizationless recovery from phaseless linear measurements. *arXiv:1208.180*.

[16] John M. Lee. *Introduction to Smooth Manifolds*. 2000.

[17] Steven T. Flammia David Gross Stephen D. Bartlett Rolando Somma Olivier Landon-Cardinal Yi-Kai Liu David Poulin. Marcus Cramer, Martin B. Plenio. Efficient quantum state tomography. *http://arxiv.org/abs/1101.4366*.

[18] David Gross Yi-Kai Liu Jens Eisert Matthias Ohliger, Vincent Nesme. Continuous-variable quantum compressed sensing. *http://arxiv.org/abs/1111.0853*.

[19] R. J. Milgram. Immersing projective spaces,. *Ann. Math.*, 85:473482, 1967.

[20] Dustin Mixon. Short, fat matrices. *http://dustingmixon.wordpress.com/*.

[21] A. Mukherjee. Embedding complex projective spaces in euclidean space. *Bull. London Math. Soc.*, 13:323–324, 1981.

[22] B. Steer. On the embedding of projective spaces in euclidean space. *Proc. London Math. Soc.*, 21:489–501, 1970.

[23] Yi-Kai Liu Jens Eisert Steven T. Flammia, David Gross. Quantum tomography via compressed sensing: Error bounds, sample complexity, and efficient estimators. *http://arxiv.org/abs/1205.2300*.

[24] E. Candès T. Strohmer and V. Voroninski. Phaselift: Exact and stable signal recovery from magnitude measurements via convex programming. *Communications on Pure and Applied Mathematics*, 2011.

[25] Michael M. Wolf Teiko Heinosaari, Luca Mazzarella. Quantum tomography under prior information. *Arxiv e-print*, 2011.

[26] A. Vogt. Position and momentum distributions do not determine the quantum mechanical state. In A.R. Marlow, editor, *Mathematical Foundations of Quantum Theory*. Academic Press, New York, 1978.

[27] Vladislav Voroninski. A comparison between the phaselift and phasecut algorithms. *http://math.berkeley.edu/ vladv/*.

[28] Vladislav Voroninski. Phase retrieval from unitary quadratic measurements and implications for wright's conjecture. *http://math.berkeley.edu/ vladv/*.