# PhaseLift: Exact and Stable Signal Recovery from Magnitude Measurements via Convex Programming

EMMANUEL J. CANDÈS

*Departments of Mathematics and of Statistics, Stanford University, Stanford CA 94305*

THOMAS STROHMER

*University of California at Davis, Davis CA 95616*

AND

VLADISLAV VORONINSKI

*University of California at Berkeley, Berkeley CA 94720*

### Abstract

Suppose we wish to recover a signal $x \in \mathbb{C}^n$ from $m$ intensity measurements of the form $|\langle x, z_i \rangle|^2$, $i = 1, 2, \ldots, m$; that is, from data in which phase information is missing. We prove that if the vectors $z_i$ are sampled independently and uniformly at random on the unit sphere, then the signal $x$ can be recovered exactly (up to a global phase factor) by solving a convenient semidefinite program—a trace-norm minimization problem; this holds with large probability provided that $m$ is on the order of $n \log n$, and without any assumption about the signal whatsoever. This novel result demonstrates that in some instances, the combinatorial phase retrieval problem can be solved by convex programming techniques. Finally, we also prove that our methodology is robust vis a vis additive noise. © 2000 Wiley Periodicals, Inc.

## 1 Introduction

In many applications, one would like to acquire information about an object but it is impossible or very difficult to measure and record the phase of the signal. The problem is then to reconstruct the object from intensity measurements only. A problem of this kind that has attracted a considerable amount of attention over the last hundred years or so, is of course that of recovering a signal or image from the intensity measurements of its Fourier transform [15, 16] as in X-ray crystallography. As is well-known, such phase retrieval problems are notoriously difficult to solve numerically.

Formally, suppose $x \in \mathbb{C}^n$ is a discrete signal and that we are given information about the squared modulus of the inner product between the signal and some vectors $z_i$, namely,

$$(1.1) \qquad b_i = |\langle x, z_i \rangle|^2, \quad i = 1, \ldots, m.$$

In truth, we would like to know $\langle x, z_i \rangle$ and record both phase and magnitude information but can only record the magnitude; in other words, phase information is lost. In the classical example discussed above, the $z_i$'s are complex exponentials at frequency $\omega_i$ so that one collects the squared modulus of the Fourier transform of $x$. Of course, many other choices for the measurement vectors $z_i$ are frequently discussed in the literature, see [2, 12] for instance.

We wish to recover $x$ from the data vector $b$, and suppose first that $x$ is known to be real valued a priori. Then assuming that $x$ is uniquely determined by $b$ up to a global sign, the recovery may be cast as a combinatorial optimization problem: find a set of signs $\sigma_i$ such that the solution to the linear equations $\langle x, z_i \rangle = \sigma_i \sqrt{b_i}$, call it $\hat{x}$, obeys $|\langle \hat{x}, z_i \rangle|^2 = b_i$. Clearly, there are $2^m$ choices for $\sigma_i$ and only two choices of these signs yield $x$ up to global phase. The complex case is harder yet, since resolving the phase ambiguities now consists of finding a collection $\sigma_i$ of complex numbers, each being on the unit circle. Formalizing matters, it has been shown that at least one version of the phase retrieval problem is NP-hard [20]. Thus, one of the major challenges in the field is to find conditions on $m$ and $z_i$ which guarantee efficient numerical recovery.

A frame-theoretic approach to signal recovery from magnitude measurements has been proposed in [1–3], where the authors derive various necessary and sufficient conditions for the uniqueness of the solution, as well as various polynomial-time numerical algorithms for very specific choices of $z_i$. While theoretically quite appealing, the drawbacks are that the methods are (1) either algebraic in nature, thus severely limiting their stability in the presence of noise or slightly inexact data, or (2) the number $m$ of measurements is on the order of $n^2$, which is much too large compared to the number of unknowns.

This paper follows a very different route and establishes that if the vectors $z_i$ are independently and uniformly sampled on the unit sphere, then our signal can be recovered exactly from the magnitude measurements (1.1) by solving a simple convex program we introduce below; this holds with high probability with the proviso that the number of measurements is on the order of $n \log n$. Since there are $n$ complex unknowns, we see that the number of samples is nearly minimal. To the best of our knowledge, this is the first result establishing that under appropriate conditions, the computationally challenging nonconvex problem of reconstructing a signal from magnitude measurements is formally equivalent to a convex program in the sense that they are guaranteed to have the same unique solution.

Finally, our methodology is robust with respect to noise in the measurements. To be sure, when the data are corrupted by a small amount of noise, we also prove that the recovery error is small.

## 1.1 Methodology

We introduce some notation that shall be used throughout to explain our methodology. Letting $\mathscr{A}$ be the linear transformation

$$(1.2) \qquad \begin{array}{ccc} \mathscr{H}^{n \times n} & \to & \mathbb{R}^m \\ \boldsymbol{X} & \mapsto & \{\boldsymbol{z}_i^* \boldsymbol{X} \boldsymbol{z}_i\}_{1 \leq i \leq m} \end{array}$$

which maps Hermitian matrices into real-valued vectors, one can express the data collection $b_i = |\langle \boldsymbol{x}, \boldsymbol{z}_i \rangle|^2$ as

$$(1.3) \qquad \boldsymbol{b} = \mathscr{A}(\boldsymbol{x}\boldsymbol{x}^*).$$

For reference, the adjoint operator $\mathscr{A}^*$ maps real-valued inputs into Hermitian matrices, and is given by

$$\begin{array}{ccc} \mathbb{R}^m & \to & \mathscr{H}^{n \times n} \\ \boldsymbol{y} & \mapsto & \sum_i y_i \boldsymbol{z}_i \boldsymbol{z}_i^*. \end{array}$$

As observed in [7, 10] (see also [17]), the phase retrieval problem can be cast as the matrix recovery problem

$$(1.4) \qquad \begin{array}{ll} \text{minimize} & \text{rank}(\boldsymbol{X}) \\ \text{subject to} & \mathscr{A}(\boldsymbol{X}) = \boldsymbol{b} \\ & \boldsymbol{X} \succeq 0. \end{array}$$

Indeed, we know that a rank-one solution exists so the optimal $\boldsymbol{X}$ has rank at most one. We then factorize the solution as $\boldsymbol{x}\boldsymbol{x}^*$ in order to obtain solutions to the phase-retrieval problem. This gives $\boldsymbol{x}$ up to multiplication by a unit-normed scalar. This is all we can hope for since if $\boldsymbol{x}$ is a solution to the phase retrieval problem, then $c\boldsymbol{x}$ for any scalar $c \in \mathbb{C}$ obeying $|c| = 1$ is also solution.[1]

Rank minimization is in general NP hard, and we propose, instead, solving a trace-norm relaxation. Although this is a fairly standard relaxation in control [4, 18], the idea of casting the phase retrieval problem as a trace-minimization problem over an affine slice of the positive semidefinite cone is very recent [7, 10]. Formally, we suggest solving

$$(1.5) \qquad \begin{array}{ll} \text{minimize} & \text{Tr}(\boldsymbol{X}) \\ \text{subject to} & \mathscr{A}(\boldsymbol{X}) = \boldsymbol{b} \\ & \boldsymbol{X} \succeq 0. \end{array}$$

If the solution has rank one, we factorize it as above to recover our signal. This method which lifts up the problem of vector recovery from quadratic constraints

---

[1] When the solution is unique up to multiplication by such a scalar, we shall say that unicity holds up to global phase.

into that of recovering a rank-one matrix from affine constraints via semidefinite programming is known under the name of *PhaseLift* [7].

The program (1.5) is a semidefinite program (SDP) in standard form, and there is a rapidly growing list of algorithms for solving problems of this kind as efficiently as possible. The crucial question is whether and under which conditions the combinatorially hard problem (1.4) and the convex problem (1.5) are formally equivalent.

## 1.2 Main result

In this paper, we consider the simplest and perhaps most natural model of measurement vectors. In this statistical model, we simply assume that the vectors $z_i$ are independently and uniformly distributed on the unit sphere of $\mathbb{C}^n$ or $\mathbb{R}^n$. To be concrete, we distinguish two models.

- *The real-valued model.* Here, the unknown signal $x$ is real valued and the $z_i$'s are independently sampled on the unit sphere of $\mathbb{R}^n$.
- *The complex-valued model.* The signal $x$ is now complex valued and the $z_i$'s are independently sampled on the unit sphere of $\mathbb{C}^n$.

Our main result is that the convex program recovers $x$ exactly (up to global phase) provided the number $m$ of magnitude measurements is on the order of $n \log n$.

**Theorem 1.1.** *Consider an arbitrary signal $x$ in $\mathbb{R}^n$ or $\mathbb{C}^n$ and suppose that the number of measurements obeys $m \geq c_0 n \log n$, where $c_0$ is a sufficiently large constant. Then in both the real and complex cases, the solution to the trace-minimization program is exact with high probability in the sense that* (1.5) *has a unique solution obeying*

$$(1.6) \qquad\qquad \hat{X} = xx^*.$$

*This holds with probability at least $1 - 3e^{-\gamma \frac{m}{n}}$, where $\gamma$ is a positive absolute constant.*

Expressed differently, Theorem 1.1 establishes a rigorous equivalence between a class of phase retrieval problems and a class of semidefinite programs. Clearly, any phase retrieval algorithm, no matter how complicated or intractable, would need at least $2n$ quadratic measurements to recover a complex valued object $x \in \mathbb{C}^n$. In fact recent results, compare Theorem II in [12], show that for complex-valued signals, one needs at least $3n - 2$ intensity measurements to guarantee uniqueness of the solution to (1.4). Further, Balan, Casazza and Edidin have shown that with probability 1, $4n - 2$ generic measurement vectors (which includes the case of random uniform vectors) suffice for uniqueness in the complex case [3]. Hence, Theorem 1.1 shows that the oversampling factor for perfect recovery via convex optimization is rather minimal.

To be absolutely complete, we would like to emphasize that our discrete signals $x$ may represent 1D, 2D, 3D and higher dimensional objects. For instance, in 2D the vector $x \in \mathbb{C}^n$ might be a family of samples of the form $x[t_1,t_2]$, $1 \leq t_1 \leq n_1$, $1 \leq t_2 \leq n_2$, and with $n = n_1 n_2$, so that $x$ is a discrete 2D image. In this case, we would record the squared magnitudes of the dot product

$$\langle x, z_i \rangle = \sum_{t_1,t_2} \bar{x}[t_1,t_2] z_i[t_1,t_2].$$

Hence, our framework and theory apply to one- or multi-dimensional signals.

## 1.3 Geometry

We find it rather remarkable that the only solution to (1.5) is $\hat{X} = xx^*$. To see why this is perhaps unexpected, suppose for simplicity that the trace of the solution were known (we might be given some side information or just have additional measurements giving us this information) and equal to 1, say. In this case, the objective functional is of course constant over the feasible set, and our problem reduces to solving the feasibility problem

(1.7)
$$\begin{array}{ll} \text{find} & X \\ \text{such that} & \mathscr{A}(X) = b, \ X \succeq 0 \end{array}$$

with again the proviso that knowledge of $\mathscr{A}(X)$ determines $\text{Tr}(X)$ (equal to $\text{Tr}(xx^*) = \|x\|_2 = 1$). In this context, our main theorem states that $xx^*$ is the unique feasible point. In other words, there is no other positive semidefinite matrix $X$ in the affine space $\mathscr{A}(X) = b$. Naively, we would not expect this affine space of enormous dimension—it is of co-dimension about $n \log n$ and thus of dimension $n^2 - O(n \log n)$ in the complex case—to intersect the positive semidefinite cone in only one point. Indeed, counting degrees of freedom suggests that there are infinitely many candidates in the intersection. The reason why this is not the case, however, is precisely because there is a feasible solution with low rank. Indeed, the slice of the positive semidefinite cone $\{X : X \succeq 0\} \cap \{\text{Tr}(X) = 1\}$ is quite 'pointy' at $xx^*$ and it is, therefore, possible for the affine space $\{\mathscr{A}(X) = b\}$ to be tangent even though it is of very small codimension.

Figure 1.1 represents this geometry. In this example,

$$x = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} \implies xx^* = \frac{1}{2} \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}$$

and the affine space $\mathscr{A}(X) = b$ is tangent to the positive semidefinite cone at the point $xx^*$.

Mathematically speaking, phase retrieval is a problem in algebraic geometry since we are trying to find a solution to a set of polynomial equations. The originality in our approach is that we do not use tools from this field. For instance, we prove that there is no other positive semidefinite matrix $X$ in the affine space $\mathscr{A}(X) = b$,
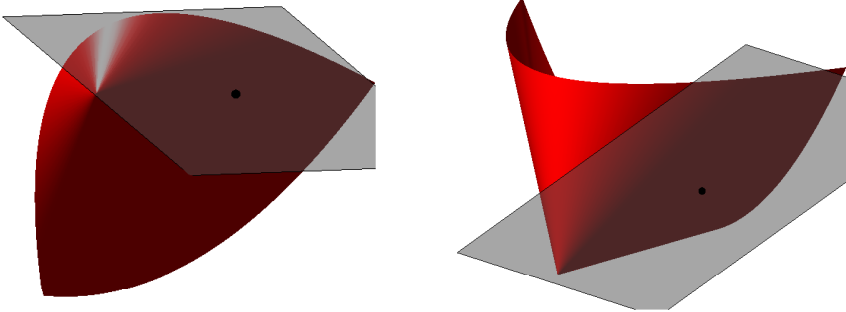
**FIGURE 1.1.** Representation of the affine space $\mathscr{A}(X) = b$ (gray) and of the semidefinite cone $\begin{bmatrix} x & y \\ y & z \end{bmatrix} \succeq 0$ (red) which is a subset of $\mathbb{R}^3$. These two sets are drawn so that they are tangent to each other at the rank 1 matrix $\frac{1}{2} \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}$ (black dot). Two views of the same 3D figure are provided for convenience.

or equivalently, that a certain system of polynomial equations (a symmetric matrix is positive semidefinite if and only if the determinants of all the leading principal minors are nonnegative) only has one solution; this is a fact that general techniques from algebraic geometry appear to not detect.

## 1.4 Stability

In the real world, measurements are contaminated by noise. Using the frameworks developed in [8] and [14], it is possible to extend Theorem 1.1 to accommodate noisy measurements. One could consider a variety of noise models as discussed in [7] but we work here with a simple generic model in which we observe

$$(1.8) \qquad b_i = |\langle x, z_i \rangle|^2 + v_i,$$

where $v_i$ is a noise term with bounded $\ell_2$ norm, $\|v\|_2 \leq \varepsilon$. This model is non-standard since the usual statistical linear model posits a relationship of the form $b_i = \langle x, z_i \rangle + v_i$ in which the mean response is a linear function of the unknown signal, not a quadratic function. Furthermore, we prefer studying (1.8) rather than the related model $b_i = |\langle x, z_i \rangle| + v_i$ (the modulus is not squared) because in many applications of interest in optics and other areas of physics, one can measure squared magnitudes or intensities—not magnitudes.

We now consider the solution to

$$
\begin{aligned}
\text{minimize} \quad & \text{Tr}(\boldsymbol{X}) \\
\text{subject to} \quad & \|\mathscr{A}(\boldsymbol{X}) - \boldsymbol{b}\|_2 \leq \varepsilon \\
& \boldsymbol{X} \succeq 0.
\end{aligned}
$$

(1.9)

We do not claim that $\hat{\boldsymbol{X}}$ has low rank so we suggest estimating $\boldsymbol{x}$ by extracting the largest rank-1 component. Write $\hat{\boldsymbol{X}}$ as

$$
\hat{\boldsymbol{X}} = \sum_{k=1}^{n} \hat{\lambda}_k \hat{\boldsymbol{u}}_k \hat{\boldsymbol{u}}_k^*, \quad \hat{\lambda}_1 \geq \ldots \geq \hat{\lambda}_n \geq 0,
$$

where $\hat{\boldsymbol{u}}_1, \ldots, \hat{\boldsymbol{u}}_n$ are mutually orthogonal, and set

$$
\hat{\boldsymbol{x}} = \sqrt{\hat{\lambda}_1}\, \hat{\boldsymbol{u}}_1.
$$

We prove the following estimate.

**Theorem 1.2.** *Fix $\boldsymbol{x} \in \mathbb{C}^n$ or $\mathbb{R}^n$ and assume the $\boldsymbol{z}_i$'s are uniformly sampled on the sphere of radius $\sqrt{n}$. Under the hypotheses of Theorem 1.1, the solution to (1.9) obeys ($\|\boldsymbol{X}\|_2$ is the Frobenius norm of $\boldsymbol{X}$)*

(1.10)
$$
\|\hat{\boldsymbol{X}} - \boldsymbol{x}\boldsymbol{x}^*\|_2 \leq C_0\,\varepsilon
$$

*for some positive numerical constant $C_0$. We also have*

(1.11)
$$
\|\hat{\boldsymbol{x}} - e^{i\phi}\boldsymbol{x}\|_2 \leq C_0 \min(\|\boldsymbol{x}\|_2, \varepsilon/\|\boldsymbol{x}\|_2)
$$

*for some $\phi \in [0, 2\pi]$. Both these estimates hold with nearly the same probability as in the noiseless case.*

Thus our approach also provides stable recovery in presence of noise. This important property is not shared by other reconstruction methods, which are of a more algebraic nature and rely on particular properties of the measurement vectors, such as the methods in [2, 3, 12], as well as the methods that appear implicitly in Theorem 3.1 and Theorem 3.3 of [7].

We note that one can further improve the accuracy of the solution $\hat{\boldsymbol{x}}$ by "debiasing" it. We replace $\hat{\boldsymbol{x}}$ by its rescaled version $s\hat{\boldsymbol{x}}$ where $s = \sqrt{\sum_{k=1}^{n} \hat{\lambda}_k}/\|\hat{\boldsymbol{x}}\|_2$. This corrects for the energy leakage occurring when $\hat{\boldsymbol{X}}$ is not exactly a rank-1 solution, which could cause the norm of $\hat{\boldsymbol{x}}$ to be smaller than that of the actual solution. Other corrections are of course possible.

## 1.5 Organization of the paper

The remainder of the paper is organized as follows. Subsection 1.6 introduces some notation used throughout the paper. In Section 2 we present the main architecture of the proof of Theorem 1.1, which comprises two key ingredients: approximate $\ell_1$ isometries and approximate dual certificates. Section 3 is devoted to establishing

approximate $\ell_1$ isometries. In Section 4, we construct approximate dual certificates and complete the proof of Theorem 1.1 in the real-valued case. Section 5 shows how the proof for the real-valued case can be adapted to the complex-valued case. Section 6 is concerned with the proof of Theorem 1.2. Numerical simulations, illustrating our theoretical results, are presented in Section 7. We conclude the paper with a short discussion in Section 8.

## 1.6 Notations

It is useful to introduce notations that shall be used throughout the paper. Matrices and vectors are denoted in boldface (such as $X$ or $x$), while individual entries of a vector or matrix are denoted in normal font; e.g. the $i$th entry of $x$ is $x_i$. For matrices, we define

$$\|X\|_p = \left[ \sum_i \sigma_i^p(X) \right]^{1/p},$$

(where $\sigma_i(X)$ denotes the $i$th singular value of $X$), so that $\|X\|_1$ is the nuclear norm, $\|X\|_2$ is the Frobenius norm and $\|X\|_\infty$ is the operator norm also denoted by $\|X\|$. For vectors, $\|x\|_p$ is the usual $\ell_p$ norm. We denote the $n-1$ dimensional sphere by $S^{n-1}$, i.e. the set $\{x \in \mathbb{R}^n : \|x\|_2 = 1\}$.

Next, we define $T_x$ to be the set of symmetric matrices of the form

(1.12) $$T_x = \{X = xy^* + yx^* : y \in \mathbb{R}^n\}$$

and denote $T_x^\perp$ by its orthogonal complement. Note that $X \in T_x^\perp$ if and only if both the column and row spaces of $X$ are perpendicular to $x$. Further, the operator $\mathscr{P}_{T_x}$ is the orthogonal projector onto $T_x$ and similarly for $\mathscr{P}_{T_x^\perp}$. We shall almost always use $X_{T_x}$ as a shorthand for $\mathscr{P}_{T_x}(X)$.

Finally, we will abuse language and say that a symmetric matrix $H$ is feasible if and only if $xx^* + H$ is feasible for our problem (1.5). This means that $H$ obeys

(1.13) $$xx^* + H \succeq 0 \quad \text{and} \quad \mathscr{A}(H) = 0.$$

## 2 Architecture of the Proof

In this section, we introduce the main architecture of the argument and defer the proofs of crucial intermediate results to later sections. We shall prove Theorem 1.1 in the real case first for ease of exposition. Then in Section 5, we shall explain how to modify the argument to the complex and more general case.

Suppose then that $x \in \mathbb{R}^n$ and that the $z_i$'s are sampled on the unit sphere. It is clear that we may assume without loss of generality that $x$ is unit-normed. Further, since the uniform distribution on the unit sphere is rotationally invariant, it suffices

to prove the theorem in the case where $x = e_1$. Indeed, we can write any unit vector $x$ as $x = Ue_1$ where $U$ is orthogonal. Since

$$|\langle x, z_i \rangle|^2 = |\langle Ue_1, z_i \rangle|^2 = |\langle e_1, U^* z_i \rangle|^2 =^d |\langle e_1, z_i \rangle|^2,$$

the problem is the same as that of finding $e_1$. We henceforth assume that $x = e_1$.

Finally, the theorem can be equivalently stated in the case where the $z_i$'s are i.i.d. copies of a white noise vector $z \sim \mathcal{N}(0, I)$ with independent standard normals as components. Indeed, if $z_i \sim \mathcal{N}(0, I)$,

$$|\langle x, z_i \rangle|^2 = b_i \quad \Longleftrightarrow \quad |\langle x, u_i \rangle|^2 = b_i / \|z_i\|_2^2,$$

where $u_i = z_i / \|z_i\|_2$ is uniformly sampled on the unit sphere. Since $\|z_i\|_2$ does not vanish with probability one, establishing the theorem for Gaussian vectors establishes it for uniformly sampled vectors and vice versa. From now on, we assume $z_i$ i.i.d. $\mathcal{N}(0, I)$.

## 2.1 Key lemma

The set $T := T_{e_1}$ defined in (1.12) may be interpreted as the tangent space at $e_1 e_1^*$ to the manifold of symmetric matrices of rank 1. Now standard duality arguments in semidefinite programming show that a sufficient (and nearly necessary) condition for $xx^*$ to be the unique solution to (1.5) is this:

- the restriction of $\mathscr{A}$ to $T$ is injective ($X \in T$ and $\mathscr{A}(X) = 0 \Rightarrow X = 0$),
- and there exists a *dual certificate* $Y$ in the range of $\mathscr{A}^*$ obeying[2]

(2.1) $$Y_T = e_1 e_1^* \quad \text{and} \quad Y_{T^\perp} \prec I_{T^\perp}.$$

The proof is straightforward and omitted. Our strategy to prove Theorem 1.1 hinges on the fact that a strengthening of the injectivity property allows to relax the properties of the dual certificate, as in the approach pioneered in [13] for matrix completion. We establish the crucial lemma below.

**Lemma 2.1.** *Suppose that the mapping $\mathscr{A}$ obeys the following two properties: for all positive semidefinite matrices $X$,*

(2.2) $$m^{-1}\|\mathscr{A}(X)\|_1 < (1 + 1/9)\|X\|_1;$$

*and for all matrices $X \in T$*

(2.3) $$m^{-1}\|\mathscr{A}(X)\|_1 > 0.94(1 - 1/9)\|X\|.$$

*Suppose further that there exists $Y$ in the range of $\mathscr{A}^*$ obeying*

(2.4) $$\|Y_T - e_1 e_1^*\|_2 \leq 1/3 \quad \text{and} \quad \|Y_{T^\perp}\| \leq 1/2.$$

*Then $e_1 e_1^*$ is the unique minimizer to (1.5).*

---

[2] The notation $A \prec B$ means that $B - A$ is positive definite.

The first property (2.2) is reminiscent of the (one-sided) Restricted Isometry Property (RIP) in the area of compressed sensing [9]. The difference is that it is expressed in the 1-norm rather than the 2-norm. Having said this, we note that RIP-1 properties have also been used in the compressed sensing literature, see [6] for example. We use this property instead of a property about $\|\mathscr{A}(X)\|_2$, because a RIP property in the 2-norm does not hold here (essentially because $\|\mathscr{A}(X)\|_2^2$ involves fourth moments of Gaussian variables), as we demonstrate in the Appendix. The second property (2.3) is a form of local RIP-1 since it holds only for matrices in $T$.

We would like to emphasize that the bound for the dual certificate in (2.4) is loose in the sense that $Y_T$ and $e_1 e_1^*$ may not be that close, a fact which will play a crucial role in our proof. This is in stark contrast with the work of David Gross [13], which requires a very tight approximation.

## 2.2 Proof of Lemma 2.1

We need to show that there is no feasible $xx^* + H \neq xx^*$ with $\mathrm{Tr}(xx^* + H) \leq \mathrm{Tr}(xx^*)$. Consider then a feasible $H \neq 0$ obeying $\mathrm{Tr}(H) \leq 0$, write

$$H = H_T + H_{T^\perp},$$

and observe that

$$(2.5) \qquad 0 = \|\mathscr{A}(H)\|_1 = \|\mathscr{A}(H_T)\|_1 - \|\mathscr{A}(H_{T^\perp})\|_1.$$

Now it is clear that $xx^* + H \succeq 0 \Rightarrow H_{T^\perp} \succeq 0$ and, therefore, (2.2) gives

$$m^{-1}\|\mathscr{A}(H_{T^\perp})\|_1 \leq (1+\delta)\mathrm{Tr}(H_{T^\perp})$$

for some $\delta < 1/9$. Also, $\mathrm{Tr}(H_T) \leq -\mathrm{Tr}(H_{T^\perp}) \leq 0$, which implies that $|\mathrm{Tr}(H_T)| \geq \mathrm{Tr}(H_{T^\perp})$. We then show that the operator and Frobenius norms of $H_T$ must nearly be the same.

**Lemma 2.2.** *Any feasible matrix $H$ such that $\mathrm{Tr}(H) \leq 0$ must obey*

$$\|H_T\|_2 \leq \sqrt{\frac{17}{16}}\,\|H_T\|.$$

*Proof.* Since the matrix $H_T$ has rank at most 2 and cannot be negative definite, it is of the form

$$-\lambda(u_1 u_1^* - t u_2 u_2^*),$$

where $u_1$ and $u_2$ are orthonormal eigenvectors, $\lambda \geq 0$ and $t \in [0,1]$. We claim that we cannot have $t \geq 1/4$.[3] Suppose the contrary and fix $t \geq 1/4$. By (2.3), we know that

$$m^{-1}\|\mathscr{A}(H_T)\|_1 \geq 0.94(1-\delta)\|H_T\|.$$

------

[3] The choice of $1/4$ is somewhat arbitrary here.

Further, since
$$\|\boldsymbol{H}_T\| = \frac{|\mathrm{Tr}(\boldsymbol{H}_T)|}{1-t} \geq \frac{4}{3}|\mathrm{Tr}(\boldsymbol{H}_T)|$$
for $t \geq 1/4$, it holds that
$$0 \geq \frac{5}{4}(1-\delta)|\mathrm{Tr}(\boldsymbol{H}_T)| - (1+\delta)\mathrm{Tr}(\boldsymbol{H}_{T^\perp}).$$
The right-hand side above is positive if $\mathrm{Tr}(\boldsymbol{H}_{T^\perp}) < \frac{5}{4}\frac{(1-\delta)}{(1+\delta)}|\mathrm{Tr}(\boldsymbol{H}_T)|$, so that we may assume that
$$\mathrm{Tr}(\boldsymbol{H}_{T^\perp}) \geq \frac{5}{4}\frac{(1-\delta)}{(1+\delta)}|\mathrm{Tr}(\boldsymbol{H}_T)|.$$
Since $|\mathrm{Tr}(\boldsymbol{H}_T)| \geq \mathrm{Tr}(\boldsymbol{H}_{T^\perp})$, this gives
$$0 \geq \left[\frac{5}{4}(1-\delta) - (1+\delta)\right]\mathrm{Tr}(\boldsymbol{H}_{T^\perp}).$$
If $\delta < 1/9$, the only way this can happen is if $\mathrm{Tr}(\boldsymbol{H}_{T^\perp}) = 0 \Rightarrow \boldsymbol{H}_{T^\perp} = 0$. So we would have $\boldsymbol{H} = \boldsymbol{H}_T$ of rank 2 and $\mathscr{A}(\boldsymbol{H}_T) = 0$. Clearly, (2.3) implies that $\boldsymbol{H} = 0$.

Now that it is established that $t \leq 1/4$, the chain of inequalities follow from the relation between the eigenvalues of $\boldsymbol{H}_T$. $\qquad\square$

To conclude the proof of Lemma 2.1, we show that the existence of an inexact dual certificate rules out the existence of matrices obeying the conditions of Lemma 2.2. From
$$0.94(1-\delta)\|\boldsymbol{H}_T\| \leq m^{-1}\|\mathscr{A}(\boldsymbol{H}_T)\|_1 = m^{-1}\|\mathscr{A}(\boldsymbol{H}_{T^\perp})\|_1 \leq (1+\delta)\mathrm{Tr}(\boldsymbol{H}_{T^\perp}),$$
we conclude that
$$(2.6) \qquad \mathrm{Tr}(\boldsymbol{H}_{T^\perp}) \geq 0.94\frac{1-\delta}{1+\delta}\|\boldsymbol{H}_T\| \geq 0.94\frac{1-\delta}{1+\delta}\sqrt{\frac{16}{17}}\|\boldsymbol{H}_T\|_2,$$
where we used Lemma 2.2. Next,
$$\begin{aligned}
0 \geq \mathrm{Tr}(\boldsymbol{H}_T) + \mathrm{Tr}(\boldsymbol{H}_{T^\perp}) &= \langle \boldsymbol{H}, e_1 e_1^* \rangle + \mathrm{Tr}(\boldsymbol{H}_{T^\perp}) \\
&= \langle \boldsymbol{H}, e_1 e_1^* - \boldsymbol{Y} \rangle + \langle \boldsymbol{H}, \boldsymbol{Y} \rangle + \mathrm{Tr}(\boldsymbol{H}_{T^\perp}) \\
&= \langle \boldsymbol{H}_T, e_1 e_1^* - \boldsymbol{Y}_T \rangle - \langle \boldsymbol{H}_{T^\perp}, \boldsymbol{Y}_{T^\perp} \rangle + \mathrm{Tr}(\boldsymbol{H}_{T^\perp}) \\
&\geq \frac{1}{2}\mathrm{Tr}(\boldsymbol{H}_{T^\perp}) - \frac{1}{3}\|\boldsymbol{H}_T\|_2.
\end{aligned}$$
The third line above follows from $\langle \boldsymbol{H}, \boldsymbol{Y} \rangle = 0$ and the fourth from Cauchy-Schwarz together with $|\langle \boldsymbol{H}_{T^\perp}, \boldsymbol{Y}_{T^\perp} \rangle| \leq \frac{1}{2}\mathrm{Tr}(\boldsymbol{H}_{T^\perp})$. Hence, it follows from (2.6) that
$$0 \geq \frac{1}{2}\left(0.94\frac{1-\delta}{1+\delta}\sqrt{\frac{16}{17}} - \frac{2}{3}\right)\|\boldsymbol{H}_T\|_2.$$
Since the numerical factor is positive for $\delta < 0.155$, the only way this can happen is if $\boldsymbol{H}_T = 0$. In turn, $\|\mathscr{A}(\boldsymbol{H}_{T^\perp})\|_1 = 0 \geq (1-\delta)\mathrm{Tr}(\boldsymbol{H}_{T^\perp})$ which gives $\boldsymbol{H}_{T^\perp} = 0$. This concludes the proof.

# 3 Approximate $\ell_1$ Isometries

We have seen that in order to prove our main result, it suffices to show 1) that the measurement operator $\mathscr{A}$ enjoys approximate isometry properties (in an $\ell_1$ sense) when acting on low-rank matrices and 2) that an inexact dual certificate exists. This section focuses on the former and establishes that both (2.2) and (2.3) hold with high probability. In fact, we shall prove stronger results than what is strictly required.

**Lemma 3.1.** *Fix any $\delta$ in $(0, 1/2)$ and assume $m \geq 20\delta^{-2}n$. Then for all unit vectors $\boldsymbol{u}$,*

$$(3.1) \qquad (1 - \delta) \leq \frac{1}{m}\|\mathscr{A}(\boldsymbol{u}\boldsymbol{u}^*)\|_1 \leq (1 + \delta)$$

*on an event $E_\delta$ of probability at least $1 - 2e^{-m\varepsilon^2/2}$, where $\delta/4 = \varepsilon^2 + \varepsilon$. On the same event,*

$$(1 - \delta)\|\boldsymbol{X}\|_1 \leq \frac{1}{m}\|\mathscr{A}(\boldsymbol{X})\|_1 \leq (1 + \delta)\|\boldsymbol{X}\|_1$$

*for all positive semidefinite matrices. The right inequality holds for all Hermitian matrices.*

*Proof.* This lemma has an easy proof. Let $\boldsymbol{Z}$ be the $m \times n$ matrix with $\boldsymbol{z}_i$'s as rows. Then

$$\|\mathscr{A}(\boldsymbol{u}\boldsymbol{u}^*)\|_1 = \sum_i |\langle \boldsymbol{z}_i, \boldsymbol{u}\rangle|^2 = \|\boldsymbol{Z}\boldsymbol{u}\|^2$$

so that

$$\sigma_{\min}^2(\boldsymbol{Z}) \leq \|\mathscr{A}(\boldsymbol{u}\boldsymbol{u}^*)\|_1 \leq \sigma_{\max}^2(\boldsymbol{Z}).$$

The claim is a consequence of well-known deviations bounds concerning the singular values of Gaussian random matrices [21], namely,

$$(3.2) \qquad \mathbb{P}\left(\sigma_{\max}(\boldsymbol{Z}) > \sqrt{m} + \sqrt{n} + t\right) \leq e^{-t^2/2}$$

$$(3.3) \qquad \mathbb{P}\left(\sigma_{\min}(\boldsymbol{Z}) < \sqrt{m} - \sqrt{n} - t\right) \leq e^{-t^2/2}.$$

The conclusion follows from taking $m \geq \varepsilon^{-2}n$ and $t = \sqrt{m}\varepsilon$ (and from $\varepsilon^2 \geq \delta^2/20$ for $0 < \delta \leq 1/2$). For the second part of the lemma, observe that $\boldsymbol{X} = \sum_j \lambda_j \boldsymbol{u}_j \boldsymbol{u}_j^*$ with nonnegative eigenvalues $\lambda_j$ so that

$$\|\mathscr{A}(\boldsymbol{X})\|_1 = \sum_j \sum_i \lambda_j |\langle \boldsymbol{u}_j, \boldsymbol{z}_i\rangle|^2 = \sum_j \lambda_j \|\mathscr{A}(\boldsymbol{u}_j \boldsymbol{u}_j^*)\|_1.$$

The claim follows from (3.1). The last claim is a consequence of $\|\mathscr{A}(\boldsymbol{X})\|_1 \leq \sum_j \sum_i |\lambda_j||\langle \boldsymbol{u}_j, \boldsymbol{z}_i\rangle|^2$ together with $\sum_j |\lambda_j| = \|\boldsymbol{X}\|_1$. $\qquad\square$

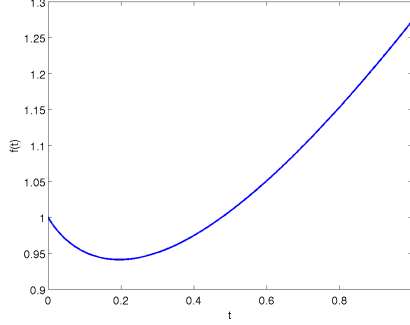Our next result is concerned with the mapping of rank-2 matrices.

**FIGURE 3.1.** $f(t) = \mathbb{E}\,|Z_1^2 - tZ_2^2|$ as a function of $t$.

**Lemma 3.2.** *Fix $\delta > 0$. Then there are positive numerical constants $c_0$ and $\gamma_0$ such that if $m \geq c_0\,[\delta^{-2}\log\delta^{-1}]\,n$, $\mathscr{A}$ obeys the following property with probability at least $1 - 3e^{-\gamma_0 m\delta^2}$: for any symmetric rank-2 matrix $X$,*

$$(3.4) \qquad \frac{1}{m}\|\mathscr{A}(X)\|_1 \geq 0.94(1-\delta)\|X\|.$$

*Proof.* By homogeneity, it suffices to consider the case where $\|X\| = 1$. Consider then a rank-2 matrix $X$ with eigenvalue decomposition $X = u_1 u_1^* - t u_2 u_2^*$ with $t \in [-1, 1]$ and orthonormal $u_i$'s. Note that for $t \leq 0$, Lemma 3.1 already claims a tighter lower bound so it only suffices to consider $t \in [0, 1]$. We have

$$\frac{1}{m}\|\mathscr{A}(X)\|_1 = \frac{1}{m}\sum_{i=1}^{m}\Big|\,|\langle u_1, z_i\rangle|^2 - t|\langle u_2, z_i\rangle|^2\,\Big| = \frac{1}{m}\sum_i \xi_i,$$

where the $\xi_i$'s are independent copies of the random variable

$$\xi = |Z_1^2 - tZ_2^2|$$

in which $Z_1$ and $Z_2$ are independent standard normal variables. This comes from the fact that $\langle u_1, z_i\rangle$ and $\langle u_2, z_i\rangle$ are independent standard normal. We calculate below that

$$(3.5) \qquad \mathbb{E}\,\xi = f(t) = \frac{2}{\pi}\Big(2\sqrt{t} + (1-t)(\pi/2 - 2\arctan(\sqrt{t}))\Big).$$

The graph of this function is shown in Figure 3.1; we check that $f(t) \geq 0.94$ for all $t \in [0, 1]$.

We now need a deviation bound concerning the fluctuation of $m^{-1}\sum_i \xi_i$ around its mean and this is achieved by classical Chernoff bounds. Note that $\xi \leq Z_1^2 + |t|Z_2^2$ is a sub-exponential variable and thus, $\|\xi\|_{\psi_1} := \sup_{p \geq 1}[\mathbb{E}\,|\xi|^p]^{1/p}$ is finite.[4]

---

[4] It would be possible to compute a bound on this quantity but we will not pursue this at the moment.

**Lemma 3.3** (Bernstein-type inequality [21]). *Let $X_1, \ldots, X_m$ be i.i.d. sub-exponential random variables. Then*

$$\mathbb{P}\left(\left|\frac{1}{m}\sum_{i=1}^{m}X_i - \mathbb{E}X_1\right| \geq \varepsilon\right) \leq 2\exp\left[-c_0 m \min\left(\frac{\varepsilon^2}{\|X\|_{\psi_1}^2}, \frac{\varepsilon}{\|X\|_{\psi_1}}\right)\right]$$

*in which $c_0$ is a positive numerical constant.*

We have thus established that for a fixed $X$,

$$m^{-1}\|\mathscr{A}(X)\|_1 \geq (0.94 - \varepsilon_0)\|X\|$$

with probability at least $1 - 2e^{-\gamma_0 m \varepsilon_0^2}$ (provided $\varepsilon_0 \leq \|\xi\|_{\psi_1}$, which we assume).

To complete the argument, let $\mathscr{S}_\varepsilon$ be an $\varepsilon$ net of the unit sphere, $\mathscr{T}_\varepsilon$ be an $\varepsilon$ net of $[0,1]$, and set

$$\mathscr{N}_\varepsilon = \{X = u_1 u_1^* - t u_2 u_2^* : (u_1, u_2, t) \in \mathscr{S}_\varepsilon \times \mathscr{S}_\varepsilon \times \mathscr{T}_\varepsilon\}.$$

Since $|\mathscr{S}_\varepsilon| \leq (3/\varepsilon)^n$, we have

$$|\mathscr{N}_\varepsilon| \leq (3/\varepsilon)^{2n+1}.$$

Now for any $X = uu^* - tvv^*$, consider the approximation $X_0 = u_0 u_0^* - t_0 v_0 v_0^* \in \mathscr{N}_\varepsilon$, where $\|u_0 - u\|_2$, $\|v - v_0\|_2$ and $|t - t_0|$ are each at most $\varepsilon$. We claim that

(3.6)
$$\|X - X_0\|_1 \leq 9\varepsilon,$$

and postpone the short proof. On the intersection of $E_1 = \{m^{-1}\|\mathscr{A}(X)\|_1 \leq (1+\delta_1)\|X\|_1, \text{ for all } X\}$ with $E_2 := \{m^{-1}\|\mathscr{A}(X_0)\|_1 \geq (0.94 - \varepsilon)\|X_0\|, \text{ for all } X_0 \in \mathscr{N}_\varepsilon\}$,

$$\begin{aligned}
m^{-1}\|\mathscr{A}(X)\|_1 &\geq \|\mathscr{A}(X_0)\|_1 - \|\mathscr{A}(X - X_0)\|_1 \\
&\geq (0.94 - \varepsilon)\|X_0\| - 9(1 + \delta_1)\varepsilon \\
&\geq (0.94 - \varepsilon)(\|X\| - \|X_0 - X\|) - 9(1 + \delta_1)\varepsilon \\
&\geq (0.94 - \varepsilon)(1 - 5\varepsilon) - 9(1 + \delta_1)\varepsilon \\
&\geq 0.94 - (15 + 9\delta_1)\varepsilon,
\end{aligned}$$

which is the desired bound by setting $0.94\delta = (15 + 9\delta_1)\varepsilon$. In conclusion, set $\delta_1 = 1/2$ and take $\varepsilon = 0.94\delta/20$. Then $E_1$ holds with probability at least $1 - O(e^{-\gamma_1 m \varepsilon^2})$ provided $m$ obeys the condition of the theorem. Further, Lemma 3.2 states that $E_2$ holds with probability at least $1 - 2e^{-\gamma_2 m}$. This concludes the proof provided we check (3.6).

We begin with

$$\|X - X_0\|_1 \leq \|uu^* - u_0 u_0^*\|_1 + |t - t_0|\|vv^*\|_1 + |t_0|\|vv^* - v_0 v_0^*\|_1.$$

Now

$$\|uu^* - u_0 u_0^*\|_1 \leq 2\|uu^* - u_0 u_0^*\| \leq 4\|u - u_0\|_2,$$

where the first inequality follows from the fact that $uu^* - u_0u_0^*$ is of rank at most 2, and the second follows from

$$\|uu^* - u_0u_0^*\| = \sup_{\|x\|_2=1} \left|\langle u_0, x\rangle^2 - \langle u, x\rangle^2\right|$$

$$= \sup_{\|x\|_2=1} \left|\langle u - u_0, x\rangle\langle u + u_0, x\rangle\right| \le \|u - u_0\|_2\|u + u_0\|_2 \le 2\|u - u_0\|_2.$$

Similarly, $\|vv^* - v_0v_0^*\|_1 \le 4\varepsilon$ and this concludes the proof.[5] $\qquad\square$

**Lemma 3.4.** *Let $Z_1$ and $Z_2$ be independent $\mathcal{N}(0,1)$ variables and $t \in [0,1]$. We have*

$$E|Z_1^2 - tZ_2^2| = f(t),$$

*where $f(t)$ is given by (3.5).*

*Proof.* Set

$$\rho = \frac{1-t}{1+t} \text{ and } \cos\theta = \rho$$

in which $\theta \in [0, \pi/2]$. By using polar coordinates, we have

$$\mathbb{E}|Z_1^2 - tZ_2^2| = \frac{1}{2\pi}\int_0^\infty r^3 e^{-r^2/2}\,dr \int_0^{2\pi} |\cos^2\phi - t\sin^2\phi|\,d\phi$$

$$= \frac{1}{\pi}\int_0^{2\pi} |\cos^2\phi - t\sin^2\phi|\,d\phi$$

$$= \frac{2}{\pi}\int_0^{\pi} |\cos^2\phi - t\sin^2\phi|\,d\phi$$

Now using the identities $\cos^2\phi = (1+\cos 2\phi)/2$ and $\sin^2\phi = (1-\cos 2\phi)/2$, we have

$$\mathbb{E}|Z_1^2 - tZ_2^2| = \frac{1+t}{\pi}\int_0^\pi |\cos 2\phi + \rho|\,d\phi$$

$$= \frac{1+t}{2\pi}\int_0^{2\pi} |\cos\phi + \rho|\,d\phi$$

$$= \frac{1+t}{\pi}\int_0^\pi |\cos\phi + \rho|\,d\phi$$

$$= \frac{1+t}{\pi}\int_0^\pi |\rho - \cos\phi|\,d\phi$$

$$= \frac{1+t}{\pi}\left[\int_0^\theta \cos\phi - \rho\,d\phi + \int_\theta^\pi \rho - \cos\phi\,d\phi\right]$$

$$= \frac{2}{\pi}(1+t)[\sin\theta + \rho(\pi/2 - \theta)].$$

We recognize (3.5). $\qquad\square$

---

[5] The careful reader will remark that we have also used $\|X - X_0\| \le 5\varepsilon$, which also follows from our calculations.

# 4 Dual Certificates

To prove our main theorem, it remains to show that one can construct an inexact dual certificate $\boldsymbol{Y}$ obeying the conditions of Lemma 2.1.

## 4.1 Preliminaries

The linear mapping $\mathscr{A}^*\mathscr{A}$ is of the form[6]

$$\mathscr{A}^*\mathscr{A} = \sum_{i=1}^{m} \boldsymbol{z}_i\boldsymbol{z}_i^* \otimes \boldsymbol{z}_i\boldsymbol{z}_i^*,$$

which is another way to express that $\mathscr{A}^*\mathscr{A}(\boldsymbol{X}) = \sum_i \langle \boldsymbol{z}_i\boldsymbol{z}_i^*, \boldsymbol{X}\rangle \boldsymbol{z}_i\boldsymbol{z}_i^*$. Now observe the simple identity:

$$(4.1) \qquad \mathbb{E}[\boldsymbol{z}_i\boldsymbol{z}_i^* \otimes \boldsymbol{z}_i\boldsymbol{z}_i^*] = 2\mathscr{I} + \boldsymbol{I}_n \otimes \boldsymbol{I}_n := \mathscr{S},$$

where $\mathscr{I}$ is the identity operator and $\boldsymbol{I}_n$ the $n$-dimensional identity matrix. Put differently, this means that for all $\boldsymbol{X}$,

$$\mathscr{S}(\boldsymbol{X}) = 2\boldsymbol{X} + \mathrm{Tr}(\boldsymbol{X})\boldsymbol{I}.$$

The proof is a simple calculation and omitted. It is also not hard to see that the mapping $\mathscr{S}$ is invertible and its inverse is given by

$$\mathscr{S}^{-1} = \frac{1}{2}\left(\mathscr{I} - \frac{1}{n+2}\boldsymbol{I}_n \otimes \boldsymbol{I}_n\right) \quad \Leftrightarrow \quad \mathscr{S}^{-1}(\boldsymbol{X}) = \frac{1}{2}\left(\boldsymbol{X} - \frac{1}{n+2}\mathrm{Tr}(\boldsymbol{X})\boldsymbol{I}_n\right).$$

We will use this object in the definition of our dual certificate.

## 4.2 Construction

For pedagogical reasons, we first introduce a possible candidate certificate defined by

$$(4.2) \qquad \bar{\boldsymbol{Y}} := \frac{1}{m}\mathscr{A}^*\mathscr{A}\mathscr{S}^{-1}(\boldsymbol{e}_1\boldsymbol{e}_1^*).$$

Clearly, $\bar{\boldsymbol{Y}}$ is in the range of $\mathscr{A}^*$ as required. To justify this choice, the law of large numbers gives that in the limit of infinitely many samples,

$$\lim_{m\to\infty} \frac{1}{m}\sum_i (\boldsymbol{z}_i\boldsymbol{z}_i^* \otimes \boldsymbol{z}_i\boldsymbol{z}_i^*)\mathscr{S}^{-1}(\boldsymbol{e}_1\boldsymbol{e}_1^*) = \mathbb{E}(\boldsymbol{z}_i\boldsymbol{z}_i^* \otimes \boldsymbol{z}_i\boldsymbol{z}_i^*)\mathscr{S}^{-1}(\boldsymbol{e}_1\boldsymbol{e}_1^*) = \boldsymbol{e}_1\boldsymbol{e}_1^*.$$

In other words, in the limit of large samples, we have a perfect certificate since $\bar{\boldsymbol{Y}}_T = \boldsymbol{e}_1\boldsymbol{e}_1^*$ and $\bar{\boldsymbol{Y}}_{T^\perp} = 0$. Our hope is that the sample average is sufficiently close to the population average so that one can check (2.4). In order to show that this is the case, it will be useful to think of $\bar{\boldsymbol{Y}}$ (4.2) as the random sum

$$\bar{\boldsymbol{Y}} = \frac{1}{m}\sum_i \boldsymbol{Y}_i,$$

---

[6] For symmetric matrices, $\boldsymbol{A} \otimes \boldsymbol{B}$ is the linear mapping $\boldsymbol{H} \mapsto \langle \boldsymbol{A}, \boldsymbol{H}\rangle \boldsymbol{B}$.

where each matrix $Y_i$ is an independent copy of the random matrix

$$\frac{1}{2}\left[z_1^2 - \frac{1}{n+2}\|z\|_2^2\right]zz^*$$

in which $z = (z_1, \ldots, z_n) \sim \mathcal{N}(0, I)$.

We would like to make an important point before continuing. We have seen that all we need from $\bar{Y}$ is

$$\|\bar{Y}_T - e_1 e_1^*\|_2 \leq 1/3$$

(and $\|\bar{Y}_{T^\perp}\| \leq 1/2$). This is in stark contrast with David Gross' approach [13] which requires a very small misfit, i.e. an error of at most $1/n^2$. In turn, this loose bound has an enormous implication: it eliminates the need for the golfing scheme and allows for the simple certificate candidate (4.2). In fact, our certificate can be seen as the first iteration of Gross' golfing scheme.

## 4.3 Truncation

For technical reasons, it is easier to work with a truncated version of $\bar{Y}$ and our dual certificate is taken to be

(4.3) $$Y = \frac{1}{m}\sum_i Y_i 1_{E_i},$$

where the $Y_i$'s are as before and $1_{E_i}$ are independent copies of $1_E$ ($1_E$ denotes the indicator function for the event $E$) with

$$E = \{|z_1| \leq \sqrt{2\beta \log n}\} \cap \{\|z\|_2 \leq \sqrt{3n}\}.$$

We shall work with $\beta = 3$ so that $|z_1| \leq \sqrt{6 \log n}$.

**Lemma 4.1.** *Let $Y$ be as in (4.3). Then*

(4.4) $$\mathbb{P}\left(\|Y_T - e_1 e_1^*\|_2 \geq \frac{1}{3}\right) \leq 2\exp\left(-\gamma\frac{m}{n}\right),$$

*where $\gamma > 0$ is an absolute constant. This holds with the proviso that $m \geq c_1 n$ for some numerical constant $c_1 > 0$, and that $n$ is sufficiently large.*

**Lemma 4.2.** *Let $Y$ be as in (4.3). Then*

(4.5) $$\mathbb{P}\left(\|Y_{T^\perp}\| \geq \frac{1}{2}\right) \leq 4\exp\left(-\gamma\frac{m}{\log n}\right).$$

*where $\gamma > 0$ is an absolute constant. This holds with the proviso that $m \geq c_1 n \log n$ for some numerical constant $c_1 > 0$, and that $n$ is sufficiently large.*

### 4.4 $Y$ on $T$ and proof of Lemma 4.1

It is obvious that for any symmetric matrix $X \in T$,

$$\|X\|_2 \leq \sqrt{2}\|Xe_1\|_2$$

since only the first row and column are nonzero. We have

(4.6) $$Y_T e_1 - e_1 = \frac{1}{m}\sum_{i=1}^{m} y_i 1_{E_i} - \frac{1}{m}\sum_{i=1}^{m} e_1 1_{E_i^c},$$

where the $y_i$'s are independent copies of the random vector

(4.7) $$y = \frac{1}{2}\left[z_1^2 - \frac{1}{n+2}\|z\|_2^2\right]z_1 z - e_1 := (\xi z_1) z - e_1.$$

We claim that

$$\left\|\frac{1}{m}\sum_{i=1}^{m} e_1 1_{E_i^c}\right\|_2 \leq 1/9,$$

with probability at least $1 - 2e^{-\gamma m}$ for some $\gamma > 0$. This is a simple application of Bernstein's inequality. Set $\pi(\beta) = \mathbb{P}(E_i^c)$ and observe that

(4.8) $$\pi(\beta) = \mathbb{P}(|z_1| \geq \sqrt{2\beta \log n}) + \mathbb{P}(\|z\|_2^2 \geq 3n) \leq n^{-\beta} + e^{-\frac{n}{3}}.$$

The right-hand side follows from $\mathbb{P}(|z_1| \geq t) \leq e^{-t^2/2}$ which holds for $t \geq 1$ and from $\mathbb{P}(\|z\|_2^2 \geq 3n) \leq e^{-n/3}$. In turn, this last bound follows from

$$\mathbb{P}(\|z\|_2^2 - n \geq \sqrt{2nt} + t^2) \leq e^{-t^2/2}.$$

Returning to Bernstein, this gives

$$\mathbb{P}\left(\left|\frac{1}{m}\sum_{i=1}^{m} 1_{E_i^c} - \pi(\beta)\right| \geq t\right) \leq 2\exp\left(-\frac{mt^2}{2\pi(\beta) + 2t/3}\right).$$

Setting $t = 1/18$, $\beta = 3$ and taking $n$ large enough so that $\pi(3) \leq 1/18$ proves the claim.

The main task is to bound the 2-norm of the sum $\sum_{i=1}^{m} y_i 1_{E_i}$ and a convenient way to do this is via the vector Bernstein inequality, cf. [13, Theorem 12].

**Theorem 4.3** (Vector Bernstein inequality). *Let $x_i$ be a sequence of independent random vectors and set $V \geq \sum_i \mathbb{E}\|x_i\|_2^2$. Then for all $t \leq V/\max\|x_i\|_2$, we have*

$$\mathbb{P}(\|\sum_i (x_i - \mathbb{E}x_i)\|_2 \geq \sqrt{V} + t) \leq e^{-t^2/4V}.$$

It is because this inequality requires bounded random vectors that we work with the truncation $\sum_{i=1}^{m} y_i 1_{E_i}$.

Put $\bar{y} = y 1_E$. Since $\|\bar{y}\|_2^2 \leq \|y\|_2^2$, we first compute $\mathbb{E}\|y\|_2^2$. We have

$$\|y\|_2^2 = \|z\|_2^2 z_1^2 \xi^2 - 2z_1^2 \xi + 1, \qquad \xi = \frac{1}{2}\left[z_1^2 - \frac{1}{n+2}\|z\|_2^2\right],$$

and a little bit of algebra yields

$$\|\boldsymbol{y}\|_2^2 = \frac{1}{4}z_1^6\|\boldsymbol{z}\|_2^2 - \frac{1}{2(n+2)}z_1^4\|\boldsymbol{z}\|_2^4 + \frac{1}{4(n+2)^2}z_1^2\|\boldsymbol{z}\|_2^6 - z_1^4 + \frac{1}{n+2}z_1^2\|\boldsymbol{z}\|_2^2 + 1.$$

Thus,

$$\mathbb{E}\left[\|\boldsymbol{y}\|_2^2\right] = \frac{1}{4}(15n+90) - \frac{1}{2(n+2)}(3n^2+30n+72) + \frac{1}{4(n+2)}(n+4)(n+6) - 1$$

$$(4.9) \qquad \leq 4(n+4),$$

where we have used the following identities

$$\mathbb{E}\left[z_1^2\|\boldsymbol{z}\|_2^2\right] = n+2,$$
$$\mathbb{E}\left[z_1^2\|\boldsymbol{z}\|_2^6\right] = (n+2)(n+4)(n+6),$$
$$\mathbb{E}\left[z_1^4\|\boldsymbol{z}\|_2^4\right] = 3n^2+30n+72,$$
$$\mathbb{E}\left[z_1^6\|\boldsymbol{z}\|_2^2\right] = 15n+90.$$

Second, on the event of interest we have $|\xi| \leq \beta \log n$ (assuming $2\beta \log n \geq 3$), $|z_1| \leq \sqrt{2\beta \log n}$ and $\|\boldsymbol{z}\|_2 \leq \sqrt{3n}$ and, therefore,

$$\|\bar{\boldsymbol{y}}\|_2 \leq \sqrt{6n}(\beta \log n)^{3/2} + 1 \leq \sqrt{7n}(\beta \log n)^{3/2}$$

provided $n$ is large enough.

Third, observe that by symmetry, all the entries of $\bar{\boldsymbol{y}}$ but the first have mean zero. Hence,

$$\|\mathbb{E}\,\bar{\boldsymbol{y}}\|_2 = |\mathbb{E}\,y_1 - \bar{y}_1| = |\mathbb{E}\,1_{E^c}y_1| \leq \sqrt{\mathbb{P}(E^c)}\sqrt{\mathbb{E}\,y_1^2}.$$

We have

$$y_1^2 = (\xi z_1^2 - 1)^2 = \frac{1}{4}z_1^8 - z_1^4 + \frac{1}{n+2}\|z\|_2^2 z_1^4 - \frac{1}{2(n+2)}\|z\|_2^2 z_1^6 + \frac{1}{4(n+2)^2}\|z\|_2^4 z_1^4 + 1$$

and using the identities above

$$\mathbb{E}\,y_1^2 = \frac{101}{4} - \frac{27n^2 + 210n + 288}{4(n+2)^2} \leq 22,$$

which gives

$$\|\mathbb{E}\,\bar{\boldsymbol{y}}\|_2 \leq \sqrt{22(n^{-\beta} + e^{-\frac{n}{3}})}.$$

Finally, with $V = 4m(n+4)$, Bernstein's inequality gives that for each $t \leq 4(n+4)/[\sqrt{7n}(\beta \log n)^{3/2}]$,

$$\|m^{-1}\sum_i(\bar{\boldsymbol{y}}_i - \mathbb{E}\,\bar{\boldsymbol{y}}_i)\|_2 \geq 2\sqrt{\frac{n+4}{m}} + t$$

with probability at most $\exp\left(-\frac{mt^2}{16(n+4)}\right)$. It follows that

$$\|m^{-1}\sum_i \bar{y}_i\|_2 \geq \sqrt{22(n^{-\beta} + e^{-\frac{n}{3}})} + 2\sqrt{\frac{n+4}{m}} + t$$

with at most the same probability. Our result follows by taking $t = 1/6$, $\beta = 3$, $m \geq c_1 n$ where $n$ and $c_1$ are sufficiently large such that

$$\sqrt{22(n^{-\beta} + e^{-\frac{n}{3}})} + 2\sqrt{\frac{n+4}{m}} + \frac{1}{6} \leq \frac{2}{9}.$$

## 4.5 $Y$ on $T^\perp$ and proof of Lemma 4.2

We have

$$Y_{T^\perp} = \frac{1}{m}\sum_i X_i 1_{E_i},$$

where the $X_i$'s are independent copies of the random matrix

(4.10)
$$X = \frac{1}{2}\left[z_1^2 - \frac{1}{n+2}\|z\|_2^2\right]\mathscr{P}_{T^\perp}(zz^T).$$

One natural way to bound the norm of this random sum is via the operator Bernstein's inequality. We develop a more customized approach, which gives sharper results.

Decompose $X$ as

$$X = \frac{1}{2}\left[z_1^2 - 1\right]\mathscr{P}_{T^\perp}(zz^T) + \frac{1}{2}\left[1 - \frac{1}{n+2}\|z\|_2^2\right]\mathscr{P}_{T^\perp}(zz^T) := X^{(0)} + X^{(1)}.$$

Note that since $z_1$ and $\mathscr{P}_{T^\perp}(zz^T)$ are independent, we have $\mathbb{E}\,X^{(0)} = 0$ and thus, $\mathbb{E}\,X^{(1)} = 0$ since $\mathbb{E}\,X = 0$. With $\bar{X}_i^{(0)} = X_i^{(0)}1_{E_i}$ and similarly for $\bar{X}_i^{(1)}$, it then suffices to show that

(4.11)
$$\left\|\sum_i \bar{X}_i^{(0)}\right\| \leq m/4 \quad \text{and} \quad \left\|\sum_i \bar{X}_i^{(1)}\right\| \leq m/4$$

with large probability. Write the norm as

$$\left\|\sum_i \bar{X}_i^{(0)}\right\| = \sup_u \left|\sum_i \langle u, \bar{X}_i^{(0)} u\rangle\right|,$$

where the supremum is over all unit vectors $u$ that are orthogonal to $e_1$. The strategy is now to find a bound on the right-hand side for each fixed $u$ and apply a covering argument to control the supremum over the whole unit sphere. In order to do this, we shall make use of a classical large deviation result.

**Theorem 4.4** (Bernstein inequality). *Let $\{X_i\}$ be a finite sequence of independent random variables. Suppose that there exist $V_i$ and $c$ such that for all $X_i$ and all $k \geq 3$,*

$$\mathbb{E}\,|X_i|^k \leq \frac{1}{2}k!V_i c_0^{k-2}.$$

*Then for all $t \geq 0$,*

(4.12) $$\mathbb{P}\left(\left|\sum_i X_i - \mathbb{E}X_i\right| \geq t\right) \leq 2\exp\left(-\frac{t^2}{2\sum_i V_i + 2c_0 t}\right).$$

For the first sum in (4.11), we write

$$\sum_i \langle u, \bar{X}_i^{(0)} u\rangle = \sum_i \eta_i \, 1_{E_i},$$

where the $\eta_i$'s are independent copies of

$$\eta = \frac{1}{2}\left[z_1^2 - 1\right]\langle z, u\rangle^2.$$

The point of the decomposition $X^{(0)} + X^{(1)}$ is that $z_1$ and $\langle z, u\rangle$ are independent since $u$ is orthogonal to $e_1$. We have $\mathbb{E}\,\eta = 0$ and for $k \geq 2$,

$$\mathbb{E}\,|\eta \, 1_E|^k \leq 2^{-k}\,\mathbb{E}\,|(z_1^2 - 1)\,1_{\{z_1^2 \leq 2\beta \log n\}}|^k \, \mathbb{E}\,|\langle z, u\rangle|^{2k}.$$

First,

$$\mathbb{E}\,|(z_1^2 - 1)\,1_{\{z_1^2 \leq 2\beta \log n\}}|^k \leq (2\beta \log n)^{k-2}\,\mathbb{E}(z_1^2 - 1)^2 = 2(2\beta \log n)^{k-2}.$$

Second, the moments of a chi-square variable with one degree of freedom are well known:

$$\mathbb{E}\,|\langle z, u\rangle|^{2k} = 1 \times 3 \times \ldots \times (2k - 1) \leq 2^k k!$$

Hence we can apply Bernstein inequality with $V_i = 4, i = 1, \ldots, m$, and $c_0 = 2\beta \log n$ and, obtain

$$\mathbb{P}\left(\left|\sum_i \eta_i \, 1_{E_i} - \mathbb{E}[\eta_i \, 1_{E_i}]\right| \geq mt\right) \leq 2\exp\left(-\frac{m}{4}\frac{t^2}{2 + \beta t \log n}\right).$$

We now note that

$$|\mathbb{E}\,\eta_i 1_{E_i}| = |\mathbb{E}\,\eta_i 1_{E_i^c}| \leq \sqrt{\mathbb{P}(E_i^c)}\sqrt{\mathbb{E}\,\eta_i^2} = \sqrt{\frac{3\pi(\beta)}{2}}$$

which gives

$$\mathbb{P}\left(m^{-1}\left|\sum_i \eta_i \, 1_{E_i}\right| \geq t + \sqrt{\frac{3\pi(\beta)}{2}}\right) \leq 2\exp\left(-\frac{m}{4}\frac{t^2}{2 + \beta t \log n}\right).$$

For instance, take $t = 1/12$, $\beta = 3$, $m \geq c_1 n$ and $n$ large enough to get

$$\mathbb{P}\left(m^{-1}\left|\sum_i \eta_i \, 1_{E_i}\right| \geq 1/8\right) \leq 2\exp\left(-\gamma\frac{m}{\log n}\right).$$

To derive a bound about $\|\bar{X}^{(0)}\|$, we use (see Lemma 4 in [21])

$$\sup_u \left|\langle u, \bar{X}^{(0)} u\rangle\right| \leq 2 \sup_{u \in \mathcal{N}_{1/4}} \left|\langle u, \bar{X}^{(0)} u\rangle\right|,$$

where $\mathcal{N}_{1/4}$ is a 1/4-net of the unit sphere $\{u : \|u\|_2 = 1, u \perp e_1\}$. Since $|\mathcal{N}_{1/4}| \leq 9^n$,

$$\mathbb{P}(m^{-1}\|\bar{X}^{(0)}\| > 1/4) \leq \mathbb{P}\Big(m^{-1} \sup_{u \in \mathcal{N}_{1/4}} \big|\langle u, \bar{X}^{(0)}u\rangle\big| > 1/8\Big) \leq 9^n \times 2\exp\Big(-\gamma\frac{m}{\log n}\Big).$$

Choosing $m \geq cn\log n$, where $c > 0$ is a sufficiently large numerical constant, ensures that the expression $9^n \times 2\exp\big(-\gamma\frac{m}{\log n}\big)$ will be sufficiently small.

We deal with the second term in a similar way, and write

$$\sum_i \langle u, \bar{X}_i^{(1)}u\rangle = \sum_i \eta_i \mathbf{1}_{E_i},$$

where the $\eta_i$'s are now independent copies of

$$\eta = \frac{1}{2}\Big[1 - \frac{\|z\|_2^2}{n+2}\Big]\langle z, u\rangle^2.$$

On $E$, $\|z\|_2^2 \leq 3n$ and, therefore, $\mathbb{E}|\eta\,\mathbf{1}_E|^k \leq 2^k k!$. We can apply Bernstein's inequality with $c_0 = 2$ and $V = 8m$, which gives

$$\mathbb{P}\Big(\Big|\sum_i \eta_i \mathbf{1}_{E_i} - \mathbb{E}[\eta_i \mathbf{1}_{E_i}]\Big| \geq mt\Big) \leq 2\exp\Big(-\frac{m}{4}\frac{t^2}{4+t}\Big).$$

The remainder of the proof is identical to that above and is therefore omitted.

## 4.6 Proof of Theorem 1.1

We now assemble the various intermediate results to establish Theorem 1.1. As pointed out, Theorem 1.1 follows immediately from Lemma 2.1, which in turn hinges on the validity of the conditions stated in (2.2), (2.3), and (2.4).

Lemma 3.1 asserts that condition (2.2) holds with probability of failure at most $p_1$, where $p_1 = 2e^{-\gamma_1 m}$ and here and below, $\gamma_1, \ldots, \gamma_4$ are positive numerical constants. Similarly, Lemma 3.2 shows that condition (2.3) holds with probability of failure at most $p_2$, where $p_2 = 3e^{-\gamma_2 m}$. In both cases we need that $m > cn$ for an absolute constant $c > 0$.

Proceeding to the dual certificate in (2.4), we note that Lemma 4.1 establishes the first part of the dual certificate with a probability of failure at most $p_3$, where $p_3 = 3e^{-\gamma_3 m/n}$. The second part of the dual certificate in (2.4) is shown in Lemma 4.2 to hold with probability of failure at most $p_4$, where $p_4 = 4e^{-\gamma_4 \frac{m}{\log n}}$. In the former case we need $m > cn$ for an absolute constant $c > 0$ and in the latter $m > c'n\log n$.

Finally, the union bound gives that under the hypotheses of Theorem 1.1, exact recovery holds with probability at least $1 - 3e^{-\gamma m/n}$ for some $\gamma > 0$, as claimed.

# 5 The Complex Model

This section proves that Theorem 1.1 holds for the complex model as well. Not surprisingly, the main steps of the proof are the same as in the real case, but there are here and there some noteworthy differences. Instead of deriving the whole proof, we will carefully indicate the nontrivial changes that need to be carried out.

First, we can work with $x = e_1$ because of rotational invariance, and with independent complex valued Gaussian sequences $z_i \sim \mathscr{CN}(0, I, 0)$. This means that the real and imaginary parts of $z_i$ are independent white noise sequences with variance $1/2$.

The key Lemma 2.1 only requires a slight adjustment in the numerical constants. The reason for this is that while Lemma 3.1 does not require any modification, Lemma 3.2 changes slightly; in particular, the numerical constants are somewhat different. Here is the properly adjusted complex version.

**Lemma 5.1.** *Fix* $\delta > 0$. *Then there are positive numerical constants* $c_0$ *and* $\gamma_0$ *such that if* $m \geq c_0 [\delta^{-2} \log \delta^{-1}] n$, $\mathscr{A}$ *has the following property with probability at least* $1 - 3e^{-\gamma_0 m \delta^2}$: *for any Hermitian rank-2 matrix X,*

$$(5.1) \qquad \frac{1}{m} \| \mathscr{A}(X) \|_1 \geq 2(\sqrt{2} - 1)(1 - \delta) \| X \| \geq 0.828(1 - \delta) \| X \|.$$

The proof of this lemma follows essentially the proof of Lemma 3.2. The function $f(t)$ (cf. equation (3.5)) now takes the form

$$(5.2) \qquad \mathbb{E}\,\xi = f(t) = \frac{1 + t^2}{1 + t},$$

where $\xi = \left| |Z_1|^2 - t|Z_2|^2 \right|$, with $Z_1$ and $Z_2$ independent $\mathscr{CN}(0, 1, 0)$, as demonstrated in the following lemma.

**Lemma 5.2.** *Let* $Z_1$ *and* $Z_2$ *be independent* $\mathscr{CN}(0, 1, 0)$ *variables and* $t \in [0, 1]$. *We have*

$$E\left| |Z_1|^2 - t|Z_2|^2 \right| = f(t),$$

*where* $f(t)$ *is given by (5.2).*

*Proof.* Set

$$\rho = \frac{1 - t}{1 + t} \text{ and } \cos\theta = \rho$$

in which $\theta \in [0, \pi/2]$. By using polar coordinates for the variables $(x_1, y_1)$ associated with $Z_1$ and $(x_2, y_2)$, associated with $Z_2$ we have

$$\mathbb{E}\left| |Z_1|^2 - t|Z_2|^2 \right| = \frac{1}{2} \int_0^\infty \int_0^\infty |r_1^2 - t r_2^2| r_1 r_2 e^{-r_1^2/2} e^{-r_2^2/2}\, dr_1 dr_2$$

$$= \frac{1}{8} \int_0^\infty r^5 e^{-r^2/2}\, dr \int_0^{2\pi} |\sin\phi \cos\phi| |\cos^2\phi - t\sin^2\phi|\, d\phi,$$
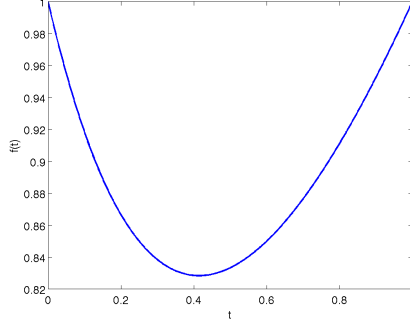
**FIGURE 5.1.** The function $f(t)$ in (5.2) as a function of $t$.

where we used polar coordinates again in variables $(r_1, r_2)$. Now using the identities $\cos^2 \phi = (1 + \cos 2\phi)/2$, $\sin^2 \phi = (1 - \cos 2\phi)/2$ and $2 \sin \phi \cos \phi = \sin 2\phi$ we have

$$
\begin{aligned}
\mathbb{E}\,|Z_1^2 - tZ_2^2| &= \frac{1}{2} \int_0^\pi |\sin 2\phi| |\cos 2\phi + \rho| \, d\phi \\
&= \frac{1}{2} \left[ \int_0^\theta \sin\phi (\cos\phi - \rho) \, d\phi + \int_\theta^\pi \sin\phi (\rho - \cos\phi) \, d\phi \right] \\
&= \frac{1}{2} (1 + t)[-\frac{1}{2} \cos 2\theta + 2\rho \cos\theta + \frac{1}{2}] \\
&= \frac{1}{2} (1 + t)[\rho^2 + 1] \\
&= \frac{1 + t^2}{1 + t}
\end{aligned}
$$

as claimed. □

The graph of $f(t)$ is shown in Figure 5.1. The minimum of this function on $[0, 1]$ is $2(\sqrt{2} - 1) > 0.828$. Furthermore, the covering argument in that proof has to be adapted; for example, unit spheres need to be replaced by complex unit spheres.

A consequence of this change in numerical values is that the numerical factors in Lemma 2.2 need to be adjusted.

**Lemma 5.3.** *Any feasible matrix* $\boldsymbol{H}$ *such that* $\mathrm{Tr}(\boldsymbol{H}) \leq 0$ *must obey*

$$
\|\boldsymbol{H}_T\|_2 \leq \sqrt{\frac{5}{4}} \|\boldsymbol{H}_T\|.
$$

Finally, with all of this in place, Lemma 2.1 becomes this:

**Lemma 5.4.** *Suppose that the mapping $\mathscr{A}$ obeys the following two properties: for some $\delta \leq 3/13$: 1) for all positive semidefinite matrices $X$,*

$$(5.3) \qquad m^{-1}\|\mathscr{A}(X)\|_1 \leq (1+\delta)\|X\|_1;$$

*2) for all matrices $X \in T$*

$$(5.4) \qquad m^{-1}\|\mathscr{A}(X)\|_1 \geq 2(\sqrt{2}-1)(1-\delta)\|X\| \geq 0.828(1-\delta)\|X\|.$$

*Suppose further that there exists $Y$ in the range of $\mathscr{A}^*$ obeying*

$$(5.5) \qquad \|Y_T - e_1 e_1^*\|_2 \leq 1/5 \quad and \quad \|Y_{T^\perp}\| \leq 1/2.$$

*Then $e_1 e_1^*$ is the unique minimizer to (1.5).*

We now turn our attention to the properties of the dual certificate we studied in Section 4. The first difference is that the expectation of $\mathscr{A}^*\mathscr{A}$ in (4.1) is different in the complex case. A simple calculation yields

$$\mathbb{E}\frac{1}{m}\mathscr{A}^*\mathscr{A} = \mathscr{I} + I_n \otimes I_n := \mathscr{S}.$$

This means that for all $X$,

$$(5.6) \qquad \mathscr{S}(X) = X + \text{Tr}(X)I.$$

We note that in this case

$$(5.7) \qquad \mathscr{S}^{-1} = \mathscr{I} - \frac{1}{n+1}I_n \otimes I_n \quad \Leftrightarrow \quad \mathscr{S}^{-1}(X) = X - \frac{1}{n+1}\text{Tr}(X)I_n.$$

We of course use this new $\mathscr{S}^{-1}$ in the complex analog of the candidate certificate (4.3). A consequence is that in the proof of Lemma 4.1, for instance, (4.7) now takes the form

$$(5.8) \qquad X = \left[|z_1|^2 - \frac{1}{n+1}\|z\|_2^2\right]\bar{z}_1 z - e_1 := (\xi \bar{z}_1) z - e_1.$$

To bound the 2-norm of a sum of i.i.d. such random variables (as in Lemma 4.1), we employ the same Bernstein inequality for real vectors, using the fact that $\|z\|_2 = \|(\Re(z), \Im(z))\|_2$ for any complex vector $z$. Similarly (4.10) becomes

$$(5.9) \qquad X = \left[|z_1|^2 - \frac{1}{n+1}\|z\|_2^2\right]\mathscr{P}_{T^\perp}(zz^*).$$

To bound the operator norm of a sum of i.i.d. such random matrices (as in Lemma 4.2), we again use a covering argument, this time working with chi-square variables with two degrees of freedom, since $|\langle z, u \rangle|^2$ is distributed as $\frac{1}{2}\chi^2(2)$. Since $|\langle z, u \rangle|^2$ are real random variables, we use the same version of the Bernstein inequality as in the real-valued case. The only difference is that the moments are now

$$\mathbb{E}|\langle z, u \rangle|^{2k} = 2^{-k} \times (2+0) \times (2+2) \times (2+4) \times \ldots \times (2+2k-2) = k!$$

# 6 Stability

This section proves the stability of our approach, namely, Theorem 1.2. Our proof parallels the argument of Candès and Plan for showing the stability of matrix completion [8] as well as that of Gross et al. in [14].

Just as before, we prove the theorem in the real case since the complex case is essentially the same. Further, we may still take $x = e_1$ without loss of generality. We shall prove stability when the $z_i$'s are i.i.d. $\mathcal{N}(0, I_n)$ and later explain how one can easily transfer a result for Gaussian vectors to a result for vectors sampled on the sphere. Under the assumptions of the theorem, the RIP-1-like properties, namely, Lemmas 3.1 and 3.2 hold with a numerical constant $\delta_1$ we shall specify later. Under the same hypotheses, the dual certificate $Y$ (4.2) obeys

$$\|\mathscr{P}_T(Y - e_1 e_1^*)\|_2 \le \gamma, \qquad \|Y_{T^\perp}\| \le \frac{1}{2},$$

in which $\gamma$ is a numerical constant also specified later.

Set $X = xx^* = e_1 e_1^*$ and write $\hat{X} = X + H$. We begin by recording two useful properties. First, since $X$ is feasible for our optimization problem, we have

$$(6.1) \qquad \mathrm{Tr}(X + H) \le \mathrm{Tr}(X) \quad \Longleftrightarrow \quad \mathrm{Tr}(H) \le 0.$$

Second, the triangle inequality gives

$$(6.2) \qquad \|\mathscr{A}(H)\|_2 = \|\mathscr{A}(\hat{X} - X)\|_2 \le \|\mathscr{A}(\hat{X}) - b\|_2 + \|b - \mathscr{A}(X)\|_2 \le 2\varepsilon.$$

In the noiseless case, $\mathscr{A}(H) = 0 \Longrightarrow \langle H, Y \rangle = 0$, by construction. In the noisy case, a third property is that $|\langle H, Y \rangle|$ is at most on the order of $\varepsilon$. Indeed,

$$m|\langle H, Y \rangle| = |\langle \mathscr{A}(H), \mathscr{A}\mathscr{S}^{-1}(X) \rangle| \le \|\mathscr{A}(H)\|_\infty \|\mathscr{A}\mathscr{S}^{-1}(X)\|_1.$$

Since $\|\mathscr{A}(H)\|_\infty \le \|\mathscr{A}(H)\|_2$ and

$$\|\mathscr{A}\mathscr{S}^{-1}(X)\|_1 \le m(1 + \delta_1)\|\mathscr{S}^{-1}(X)\|_1 \le m(1 + \delta_1),$$

we obtain

$$(6.3) \qquad |\langle H, Y \rangle| \le 2\varepsilon(1 + \delta_1).$$

We now reproduce the steps of the proof of Lemma 2.1, and obtain

$$0 \ge \mathrm{Tr}(H_T) + \mathrm{Tr}(H_{T^\perp}) \ge \frac{1}{2}\mathrm{Tr}(H_{T^\perp}) - \gamma\|H_T\|_2 - |\langle H, Y \rangle|,$$

which gives

$$(6.4) \qquad \mathrm{Tr}(H_{T^\perp}) \le 4\varepsilon(1 + \delta_1) + 2\gamma\|H_T\|_2 \le 4\varepsilon(1 + \delta_1) + 2\sqrt{2}\gamma\|H_T\|,$$

where we recall that $H_T$ has rank at most 2. We also have

$$0.94(1-\delta_1)\|H_T\| \leq m^{-1}\|\mathscr{A}(H_T)\|_1 \leq m^{-1}\|\mathscr{A}(H)\|_1 + m^{-1}\|\mathscr{A}(H_{T^\perp})\|_1$$

(6.5)
$$\leq m^{-1/2}\|\mathscr{A}(H)\|_2 + (1+\delta_1)\operatorname{Tr}(H_{T^\perp})$$

(6.6)
$$\leq 2m^{-1/2}\varepsilon + (1+\delta_1)\operatorname{Tr}(H_{T^\perp}),$$

where the second inequality follows from the RIP-1 property together with the Cauchy-Schwarz inequality. Plugging this last bound into (6.4) gives

$$\operatorname{Tr}(H_{T^\perp}) \leq 4\varepsilon(1+\delta_1+\gamma\alpha m^{-1/2}) + \beta\gamma\operatorname{Tr}(H_{T^\perp}),$$

where

$$\alpha = \frac{\sqrt{2}}{0.94(1-\delta_1)}, \quad \beta = 2\alpha(1+\delta_1).$$

Hence, when $\beta\gamma < 1$, we have

$$\operatorname{Tr}(H_{T^\perp}) = \|H_{T^\perp}\|_1 \leq \frac{4(1+\delta_1+\gamma\alpha m^{-1/2})}{1-\beta\gamma}\varepsilon = c_1\varepsilon.$$

In addition, (6.6) then gives

$$\|H_T\| \leq \frac{2m^{-1/2}+(1+\delta_1)c_1}{0.94(1-\delta_1)}\varepsilon = c_2\varepsilon.$$

In conclusion,

$$\|H\|_2 \leq \|H_T\|_2 + \|H_{T^\perp}\|_2 \leq \sqrt{2}\|H_T\| + \|H_{T^\perp}\|_1 \leq (\sqrt{2}c_2+c_1)\varepsilon = c_0\varepsilon,$$

and we also have $\|H\| \leq (c_2+c_1)\varepsilon$.

It remains to show why the fact that $\hat{X}$ is close to $X = xx^*$ in the Frobenius or operator norm produces a good estimate of $x$ (recall that $x = e_1$). Set $\varepsilon_0 := \|\hat{X}-X\| \leq c_0\varepsilon$. Below, $\hat{\lambda}_1 \geq 0$ is the largest eigenvalue of $\hat{X} \succeq 0$, and $\hat{u}_1$ the first eigenvector. Likewise, $\lambda_1 = 1$ is the top eigenvalue of $X = e_1e_1^*$. Since $\operatorname{Tr}(\hat{X}) \leq \operatorname{Tr}(X)$,

$$\hat{\lambda}_1 \leq \lambda_1.$$

In the other direction, we know from perturbation theory that

$$|\lambda_1 - \hat{\lambda}_1| \leq \|\hat{X}-X\| = \varepsilon_0.$$

Assuming that $\varepsilon_0 < 1$, this gives $\hat{\lambda}_1 \in [1-\varepsilon_0, 1]$. The sin-$\theta$-Theorem [11] implies that

$$|\sin\theta| \leq \frac{\|\hat{X}-X\|}{|\hat{\lambda}_1|} \leq \frac{\varepsilon_0}{1-\varepsilon_0},$$

where $0 \leq \theta \leq \pi/2$ is the angle between the spaces spanned by $\hat{u}_1$ and $e_1$. Writing

$$\hat{u}_1 = \cos\theta\, e_1 + \sin\theta\, e_1^\perp$$

in which $e_1^\perp$ is a unit vector orthogonal to $e_1$, Pythagoras' relationship gives

$$\|e_1 - \sqrt{\hat{\lambda}_1}\hat{u}_1\|_2^2 = (1 - \sqrt{\hat{\lambda}_1}\cos\theta)^2 + \hat{\lambda}_1\sin^2\theta.$$

Since $\cos\theta = \sqrt{1 - \sin^2\theta}$, we have

$$1 \geq \sqrt{\hat{\lambda}_1}\cos\theta \geq \sqrt{1 - \varepsilon_0 - \frac{\varepsilon_0^2}{1 - \varepsilon_0}} \geq 1 - \varepsilon_0$$

for $\varepsilon_0 < 1/3$. Hence,

$$\|e_1 - \sqrt{\hat{\lambda}_1}\hat{u}_1\|_2^2 \leq \varepsilon_0^2 + \frac{\varepsilon_0^2}{(1 - \varepsilon_0)^2} \leq \frac{13}{4}\varepsilon_0^2$$

provided $\varepsilon_0 < 1/3$. Since we always have

$$\|e_1 - \sqrt{\hat{\lambda}_1}\hat{u}_1\|_2 \leq \|e_1\|_2 + \sqrt{\hat{\lambda}_1}\|\hat{u}_1\|_2 \leq 2,$$

we have established

$$\|e_1 - \sqrt{\hat{\lambda}_1}\hat{u}_1\|_2 \leq C_0\min(\varepsilon, 1).$$

This holds for all values of $\varepsilon_0$ and proves the claim in the case where $\|x\|_2 = 1$. The general case is obtained via a simple rescaling.

As mentioned above, we proved the theorem for Gaussian $z_i$'s but it is clear that our results hold true for vectors sampled uniformly at random on the sphere of radius $\sqrt{n}$. The reason is that of course, $\|z_i\|_2$ deviates very little from $\sqrt{n}$. Formally, set $\tilde{z}_i = [\sqrt{n}/\|z_i\|_2]z_i$ so that these new vectors are independently and uniformly distributed on the sphere of radius $\sqrt{n}$. Then

$$\langle X, \tilde{z}_i\tilde{z}_i^*\rangle = \frac{n}{\|z_i\|_2^2}\langle X, z_iz_i^*\rangle,$$

and thus $\langle X, z_iz_i^*\rangle$ is between $(1 - \delta_2)\langle X, \tilde{z}_i\tilde{z}_i^*\rangle$ and $(1 + \delta_2)\langle X, \tilde{z}_i\tilde{z}_i^*\rangle$ with very high probability. This holds uniformly over all Hermitian matrices. Thus if $\tilde{\mathscr{A}}(X) = \{\tilde{z}_i^*X\tilde{z}_i\}_{1\leq i\leq m}$,

$$(1 - \delta_2)\|\tilde{\mathscr{A}}(X)\|_q \leq \|\mathscr{A}(X)\|_q \leq (1 + \delta_2)\|\tilde{\mathscr{A}}(X)\|_q$$

for any $1 \leq q \leq \infty$.

Now take $b_i = |\langle x, \tilde{z}_i\rangle|^2 + v_i$ and solve (1.9) to get $\tilde{X} = X + \tilde{H}$. Going through the same steps as above by using the relationships between $\mathscr{A}$ and $\tilde{\mathscr{A}}$ throughout, and by using the dual certificate $Y$ associated with $\mathscr{A}$, we obtain

$$\|\tilde{\mathscr{A}}(\tilde{H})\|_2 \leq 2\varepsilon, \qquad |\langle\tilde{H}, Y\rangle| \leq 2\varepsilon(1 + \delta_1)(1 + \delta_2),$$

and

$$\mathrm{Tr}(\tilde{H}_{T^\perp}) \leq (1 + \delta_2)c_1\varepsilon, \qquad \|\tilde{H}_T\| \leq (1 + \delta_2)c_2\varepsilon.$$

Therefore,

$$\|\tilde{H}\|_2 \leq (1 + \delta_2)(\sqrt{2}c_2 + c_1)\varepsilon.$$

The rest of the proof goes through just the same.

# 7 Numerical Simulations

In this section we illustrate our theoretical results with numerical simulations. In particular, we will demonstrate PhaseLift's robustness vis a vis additive noise.

We consider the setup in Section 1.4, where the measurements are contaminated with additive noise. The solution to (1.9) is computed using the following regularized nuclear-norm minimization problem:

$$(7.1) \qquad \begin{aligned} \text{minimize} \quad & \tfrac{1}{2}\|\mathscr{A}(\boldsymbol{X}) - \boldsymbol{b}\|_2^2 + \lambda \operatorname{Tr}(\boldsymbol{X}) \\ \text{subject to} \quad & \boldsymbol{X} \succeq 0. \end{aligned}$$

It follows from standard optimization theory [19] that (7.1) is equivalent to (1.9) for some value of $\lambda$. Hence, we use (7.1) to compute the solution of (1.9) by determining via a simple and efficient bisection search the largest value $\lambda(\varepsilon)$ such that $\|\mathscr{A}(\boldsymbol{X}) - \boldsymbol{b}\|_2 \leq \varepsilon$. The numerical algorithm to solve (7.1) was implemented in Matlab using TFOCS [5]. We then extract the largest rank-1 component as described in Section 1.4 to obtain an approximation $\hat{\boldsymbol{x}}$.

We will use the relative mean squared error (MSE) and the relative root mean squared error (RMS) to measure performance. However, since a solution is only unique up to global phase, it does not make sense to compute the distance between $\boldsymbol{x}$ and its approximation $\hat{\boldsymbol{x}}$. Instead we compute the distance modulo a global phase term and define the relative MSE between $\boldsymbol{x}$ and $\hat{\boldsymbol{x}}$ as

$$\min_{c:|c|=1} \frac{\|c\boldsymbol{x} - \hat{\boldsymbol{x}}\|_2^2}{\|\boldsymbol{x}\|_2^2}.$$

The (relative) RMS is just the square root of the (relative) MSE.

In the first set of experiments, we investigate how the reconstruction algorithm performs as the noise level increases. The test signal is a complex-valued signal of length $n = 128$ with independent Gaussian complex entries (each entry is of the form $a + ib$ where $a$ and $b$ are independent $\mathcal{N}(0,1)$ variables) so that the real and imaginary parts are independent white noise sequences. Obviously, the signal is arbitrary. We use $m = 6n$ measurement vectors sampled independently on the unit sphere $\mathbb{C}^n$.

We generate noisy data from both a Gaussian model and a Poisson model. In the Gaussian model, $b_i \sim \mathcal{N}(\mu_i, \sigma^2)$ where $\mu_i = |\langle \boldsymbol{x}, \boldsymbol{z}_i \rangle|^2$ and $\sigma$ is adjusted so that the total noise power is bounded by $\varepsilon^2$. In the Poisson model, $b_i \sim \operatorname{Poi}(\mu_i)$ and the noise $b_i - \mu_i$ is rescaled to achieve a desired total power as above (we might do without this rescaling as well but have decided to work with a prescribed signal-to-noise ratio SNR for simplicity of exposition). We do this for five different SNR
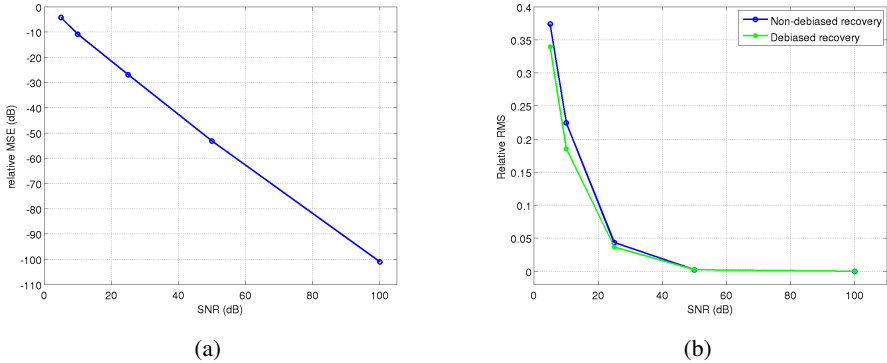
**FIGURE 7.1.** Performance of PhaseLift for Poisson noise. The stability of the algorithm is apparent as its performance degrades gracefully with decreasing SNR. (a) Relative MSE on a log-scale for the non-debiased recovery. (b) Relative RMS for the original and debiased recovery.

levels,[7] ranging from 5dB to 100dB. However, we point out that we do not make use of the noise statistics in our reconstruction algorithm[8], since our purpose is only to assume an upper bound on the total noise power, as in Theorem 1.2.

For each SNR level, we repeat the experiment ten times with different noise terms, different signals, and different random measurement vectors; we then record the average relative RMS over these ten experiments. Figure 7.1(a) shows the average relative MSE in dB (the values of $10\log_{10}(\text{rel. MSE})$ are plotted) versus the SNR for Poisson noise. In each case, the performance degrades very gracefully with decreasing SNR, as predicted by Theorem 1.2. Debiasing as described at the end of Section 1.4 leads to a further improvement in the reconstruction for low SNR, as illustrated in Figure 7.1(b). The results for Gaussian noise are comparable, see Figure 7.2.

In the next experiment, we collect Poisson data about a complex-valued random signal just as above, and work with a fixed SNR set to 15dB. The number of measurements varies so that the oversampling rate $m/n$ is between 5 and 22 ($m$ is thus between $n\log n$ and $4.5n\log n$). We repeat the experiment ten times with different noise terms and different random measurement vectors for each oversampling rate; we then record the average relative RMS. Figure 7.3 shows the average relative RMS of the solution to (1.5) versus the oversampling rate. We observe that the decrease in the RMS is inversely proportional to the number of measurements.

---

[7]The SNR of two signals $\boldsymbol{x}, \hat{\boldsymbol{x}}$ with respect to $\boldsymbol{x}$ is defined as $10\log_{10}\|\boldsymbol{x}\|_2^2/\|\boldsymbol{x} - \hat{\boldsymbol{x}}\|_2^2$. So we say that the SNR is 10dB if $10\log_{10}\|\boldsymbol{x}\|_2^2/\|\boldsymbol{\nu}\|_2^2 = 10$.

[8]We refer to [7] for efficient ways to incorporate statistical noise models into the reconstruction algorithm.

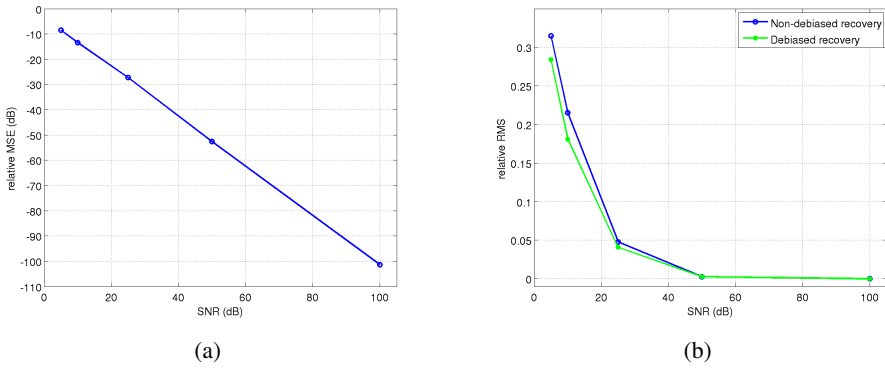(a)                                              (b)

**FIGURE 7.2.** Performance of PhaseLift for Gaussian noise. (a) Relative MSE on a log-scale for the non-debiased recovery. (b) Relative RMS for the original and the debiased recovery.
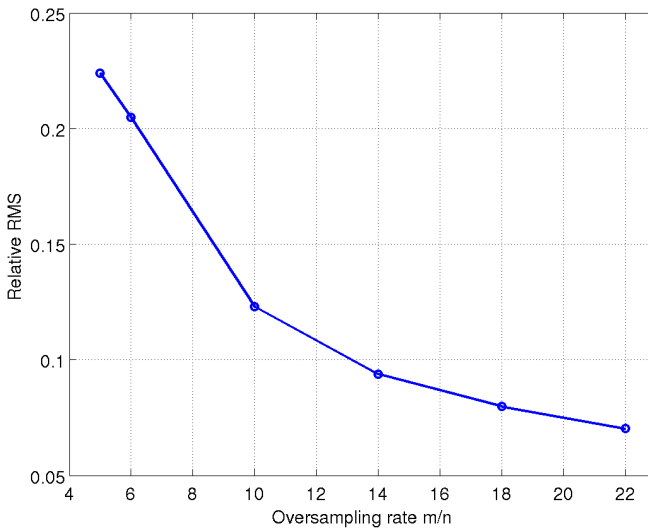


**FIGURE 7.3.** Oversampling rate versus relative RMS.

For instance, the error reduces by a factor of two when we double the number of measurements. If instead we hold the standard deviation of the errors at a constant level, the mean squared error (MSE) reduces by a factor of about two when we double the number of measurements.

# 8 Discussion

In this paper, we have shown that it is possible to recover a signal exactly (up to a global phase factor) from the knowledge of the magnitude of its inner products with a family of sensing vectors $\{z_i\}$. The fact that on the order of $n \log n$ magnitude measurements $|\langle x, z_i \rangle|^2$ uniquely determine $x$ is not surprising. The part we find unexpected, however, is that what appears to be a combinatorial problem is solved exactly by a convex program. Further, we have established the existence of a noise-aware recovery procedure—also based on a tractable convex program—which is robust vis a vis additive noise. To the best of our knowledge, there are no other results—about the recovery of an arbitrary signal from noisy quadratic data—of this kind.

An appealing research direction is to study the recovery of a signal from other types of intensity measurements, and consider other families of sensing vectors. In particular, *structured* random families would be of great interest. It also seems plausible that assuming stochastic errors in Theorem 1.2 would allow to derive sharper error bounds; it would be of interest to know if this is indeed the case. We leave this to future work.

## Appendix

We prove that the RIP in the 2-norm (and in any $p$-norm with $p > 1$) cannot hold for $\mathscr{A}$. We derive the claim for the real-valued setting, but the arguments can be easily extended to the complex-valued setting. Here and below, $|y| = (|y_1|, \ldots, |y_m|)$.

Consider an $m \times n$ matrix $A$ with i.i.d. rows $z_i =^d \mathcal{N}(0, I)$ and set $\mathscr{A}(X) = \{z_i^* X z_i\}_{i=1}^m$. Then for $x \in \mathbb{R}^n$, $\mathscr{A}(xx^*) = |Ax|^2$ and

$$\|\mathscr{A}(xx^*)\|_2 = \Big( \sum_{i=1}^m |\langle z_i, x \rangle|^4 \Big)^{1/2}.$$

Taking $x = z_1 / \|z_1\|_2$, we get

$$\sup_{u \in \mathscr{S}^{n-1}} \|\mathscr{A}(uu^*)\|_2 \geq \|\mathscr{A}(xx^*)\|_2 = \Big( \sum_{i=1}^m \Big| \Big\langle z_i, \frac{z_1}{\|z_1\|_2} \Big\rangle \Big|^4 \Big)^{1/2}$$

$$\geq \Big| \Big\langle z_1, \frac{z_1}{\|z_1\|_2} \Big\rangle \Big|^2 = \|z_1\|_2^2 = \Omega(n),$$

where the last equality holds with high probability.

Now, expand $A$ into its singular value decomposition $A = \sum_{i=1}^n \sigma_i u_i v_i^*$ with $\sigma_1 \geq \sigma_2 \ldots \geq \sigma_n$. As a consequence of (3.2), the inequalities

$$m(1 - \delta) \leq \sigma_n^2 \leq \sigma_1^2 \leq m(1 + \delta)$$

for some $\delta$ with $0 < \delta < 1$ hold with high probability provided that $m \geq Cn\log n$, where $C > 0$ is a suitable constant. All singular values of $A$ are simple with probability 1 and thus $u_n$, the singular vector corresponding to the smallest singular value, is well-defined and we can think of it as being distributed uniformly at random on the unit sphere. Therefore, with high probability

$$\|u_n\|_\infty = \mathcal{O}\left(\frac{\sqrt{\log n}}{\sqrt{m}}\right).$$

This gives

$$\inf_{u \in \mathscr{S}^{n-1}} \|\mathscr{A}(uu^*)\|_2 \leq \|\mathscr{A}(v_n v_n^*)\|_2 = \||Av_n|^2\|_2 = \||\sigma_n u_n|^2\|_2$$

$$= \sigma_n^2 \left(\sum_{i=1}^{m} |u_{ni}|^4\right)^{1/2} = \sigma_n^2 \mathcal{O}\left(\frac{\log n}{\sqrt{m}}\right) = \mathcal{O}(\sqrt{m}\log n)$$

(also with high probability). This implies that

$$\frac{\sup_{u \in \mathscr{S}^{n-1}} \|\mathscr{A}(uu^*)\|_2}{\inf_{u \in \mathscr{S}^{n-1}} \|\mathscr{A}(uu^*)\|_2} = \Omega\left(\frac{n}{\sqrt{m}\log n}\right) \qquad \text{w.h.p.}$$

Therefore, unless we take $m$ to be at least on the order of $n^2/\log^2 n$ (which is much too large to be of interest), the RIP-2 cannot hold. Similar arguments show that

$$\frac{\sup_{u \in \mathscr{S}^{n-1}} \|\mathscr{A}(uu^*)\|_p}{\inf_{u \in \mathscr{S}^{n-1}} \|\mathscr{A}(uu^*)\|_p} = \Omega\left(\frac{n}{m^{\frac{1}{p}}\log n}\right) \qquad \text{w.h.p.,}$$

and thus the RIP-$p$ cannot hold for $p > 1$, unless $m$ is at least on the order of $n^p/(\log n)^p$. Obviously, since the RIP does not hold for rank-1 matrices, it cannot hold for higher ranks.

**Acknowledgment.**

# Bibliography

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

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

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

[4] C. Beck and R. D'Andrea. Computational study and comparisons of LFT reducibility methods. In *Proceedings of the American Control Conference*, pages 1013–1017, 1998.

[5] S. Becker, E. Candès, and M. Grant. Templates for convex cone problems with applications to sparse signal recovery. Technical report, Department of Statistics, Stanford University, 2010. Preprint available at http://tfocs.stanford.edu/tfocs/paper.shtml.

[6] R. Berinde, A. Gilbert, P. Indyk, H. Karloff, and M. Strauss. Combining geometry and combinatorics: A unified approach to sparse signal recovery. *CoRR*, pages –1–1, 2008.

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

[8] E. Candès and Y. Plan. Matrix completion with noise. *Proceedings of the IEEE*, 98(6):925–936, 2010.

[9] E. J. Candès and T. Tao. Decoding by linear programming. *IEEE Trans. on Information Theory*, 51(2):4203–4215, 2005.

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

[11] C. Davis and W. M. Kahan. The rotation of eigenvectors by a perturbation. III. *SIAM J. Numer. Anal.*, 7:1–46, 1970.

[12] J. Finkelstein. Pure-state informationally complete and "really" complete measurements. *Phys. Rev. A*, 70:052107, 2004.

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

[14] D. Gross, Y. Liu, S. T. Flammia, S. Becker, and J. Eisert. Quantum-state tomography via compressed sensing. *Physical Review Letters*, 105(15), 2010.

[15] N. Hurt. *Phase Retrieval and Zero Crossings*. Kluwer Academic Publishers, Norwell, MA, 1989.

[16] M. Klibanov, P. Sacks, and A. Tikhonravov. The phase retrieval problem. *Inverse problems*, 11:1995, 1–28.

[17] Y. Lu and M. Vetterli. Sparse spectral factorization: Unicity and reconstruction algorithms. In *The 36th International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Prague, Czech Republic, 2011.

[18] M. Mesbahi and G. P. Papavassilopoulos. On the rank minimization problem over a positive semidefinite linear matrix inequality. *IEEE Trans. on Automatic Control*, 42(2):239–243, 1997.

[19] R. Rockafellar. *Convex analysis*. Princeton Landmarks in Mathematics and Physics. Princeton University Press, 1970.

[20] H. Sahinoglou and S. Cabrera. On phase retrieval of finite-length sequences using the initial time sample. *IEEE Transactions on Circuits and Systems*, 38(5):954–958, 1991.

[21] R. Vershynin. Introduction to the non-asymptotic analysis of random matrices. In Y. C. Eldar and G. Kutyniok, editors, *Compressed Sensing: Theory and Applications*. Cambridge University Press, 2010. To Appear. Preprint available at http://www-personal.umich.edu/~romanv/papers/papers.html.