Quantum tomography from few full-rank observables.

Vladislav Voroninski

Department of Mathematics, Massachusetts Institute of Technology.

September 2013

1 Introduction

It was proven in [8] that the PhaseLift algorithm recovers signals $x \in \mathbb{C}^n$ exactly from $m = O(n \log n)$ measurements $\{|\langle x, z_i \rangle|^2\}_{i=1}^m$ with high probability when the measurement vectors $z_i \in \mathbb{C}^n$ are iid gaussian and that this procedure is provably stable with respect to measurement noise under the same assumptions. To be precise, this means that in the noiseless case, for a fixed $x \in \mathbb{C}^n$ and defining the linear operator $A : X \in \mathbb{C}^{n \times n} \mapsto \{\text{Tr}(X z_i z_i^*)\}_{i=1}^m$, the program

$$
\begin{align*}
\text{minimize} & \quad \text{Tr}(X) \\
\text{subject to} & \quad A(X) = A(xx^*) \\
& \quad X \succeq 0;
\end{align*}
$$

recovered $xx^*$ with high probability. The stability result uses a modified, noise-aware convex program. These guarantees were subsequently improved to hold uniformly over all signals for $m = O(n)$ with sharp stability guarantees in [3] and it was shown in [4] that in the noiseless case, this program has only one point in its feasible set, namely $xx^*$.

However, the gaussian measurement model is not known to be physically realizable. Therefore it is of interest to prove exactness results for PhaseLift under more structured measurement assumptions, which require more technical proofs due to the lack of probabilistic independence between sensing vectors in structured random measurement ensembles.

A step in this direction is to consider the $z_i$ as rows of iid Haar distributed unitary matrices, a situation that occurs in quantum tomography from measurements with full-rank observables. In this paper, we prove that PhaseLift succeeds with high probability under this measurement model as long as the number of observables is $O(1)$ (which corresponds to $m = O(n)$ in the above setting) and point out a corollary of the result which relates to Wright’s conjecture. This conjecture, that there exist 3 observables which determine any pure state, has been recently disproven in [5, 6] and a close variant of it, that 4 generic observables suffice to determine any pure state, was recently settled in [2]. This brings us to the main theorem:

**Theorem 1.1** Take $x \in \mathbb{C}^n$ and assume that measurements of the form $\{|U_k x|^2\}_{k=1}^r$ are available, where the $U_i$ are sampled independently according to the Haar measure on $\mathbb{U}(n)$, the unitary group
or $O(n)$, the orthogonal group, so that the total number of measurements is $m = rn$. Then the PhaseLift algorithm succeeds in recovering $x$ up to global phase with very high probability with $m = O(n)$.

Here we assume that measurements of the form $\{|U_kx|^2\}_{k=1}^r$ are available, where the $U_i$ are sampled independently according to the Haar measure on $U(n)$, the unitary group or $O(n)$, the orthogonal group, and the total number of measurements is $m = rn$. Below, we will label the transpose of the row vectors of $U_k$ as $u_i^{(k)}$ or enumerate them as $\{u_i\}_{i=1}^m$. As in the gaussian case, we may assume wlog that $x = e_1$, in this case by the unitary/orthogonal invariance of the Haar measure.

We proceed by showing that the measurement operator $A$ in this setting obeys some nice properties with high probability. Namely, we need to verify that $A$ satisfies the condition of the following lemma, which is a very slight modification of Lemma 3.6.4 in [8] achieved by noting that if $Y_T^\perp \prec 0$, then $\langle H_T^\perp, Y_T^\perp \rangle \leq 0$.

**Lemma 1.2** Suppose that the mapping $A$ obeys the following two properties: for some $\delta \leq 3/13$:

1) for all positive semidefinite matrices $X$,
\[ m^{-1}\|A(X)\|_1 \leq (1 + \delta)\|X\|_1; \quad (1.2) \]

2) for all matrices $X \in T$
\[ m^{-1}\|A(X)\|_1 \geq 2(\sqrt{2} - 1)(1 - \delta)\|X\| \geq 0.828(1 - \delta)\|X\|. \quad (1.3) \]

Suppose further that there exists $Y$ in the range of $A^*$ obeying
\[ \|Y_T - e_1e_1^*\|_2 \leq 1/5 \quad \text{and} \quad Y_T^\perp \prec 0. \quad (1.4) \]

Then $e_1e_1^*$ is the unique minimizer of PhaseLift.

In particular, the RIP-1 property in this unitary case has implications related to Wright’s conjecture. Furthermore, we adapt a trick in the construction of the dual certificate, used by [3] in the gaussian case, to reduce the number of necessary measurements from $O(n \log n)$ to $O(n)$. Establishing the above yields the main result.

## 2 Restricted Isometry Property of type 1 for Unitary Matrices

In the sequel we will label the transpose of the row vectors of $U_k$ as $u_i^{(k)}$ or enumerate them as $\{u_i\}_{i=1}^m$. As in the gaussian case, we may assume wlog that $x = e_1$, in this case by the unitary/orthogonal invariance of the Haar measure.

First, we aim to establish a RIP-1 property on rank-2 matrices for this class of measurements. Let $A(X) = \{\sqrt{n(n+1)} \operatorname{Tr}(u_iu_i^* X)\}_{i=1}^m$, where $A$ is a linear map from the Hermitian matrices. Let
$X = x_1x_1^* - \lambda x_2x_2^*$ be a rank-2 hermitian matrix in SVD form with $0 \leq \lambda \leq 1$. Then

$$\frac{1}{\sqrt{n(n+1)}} A(x_1x_1^* - \lambda x_2x_2^*) = \{ |\langle u_i, x_1 \rangle |^2 - \lambda |\langle u_i, x_2 \rangle |^2 \}_{i=1}^m$$

$$= d \{ |\langle u_i, e_1 \rangle |^2 - \lambda |\langle u_i, e_2 \rangle |^2 \}_{i=1}^m$$

$$= \{|u_{i1}|^2 - \lambda |u_{i2}|^2 \}_{i=1}^m$$

where we used rotational invariance of Haar measure and the fact that there exist orthogonal or unitary transformations taking any real/complex orthonormal basis to another orthonormal basis and $u_{ij}$ denotes the $j$th entry of the vector $u_i$.

To establish $\frac{1}{m} \|A(X)\|_1 \leq (1 + \delta) \|X\|_1$ for all psd matrices, it is enough to consider $X$ to be rank 1 psd. Taking any unit vector $x \in \mathbb{C}^n$, we have

$$\frac{1}{r} \frac{1}{\sqrt{n(n+1)}} \|A(xx^*)\|_1 = \frac{1}{r} \sum_{i=1}^m |\langle u_m, x \rangle |^2 = 1$$

This implies that

$$\frac{1}{r} \frac{1}{\sqrt{n(n+1)}} \|A(X)\|_1 \leq (1 + \delta) \|X\|_1$$

for any $\delta > 0$ and for any psd $X$. Now since $\frac{m}{r \sqrt{n(n+1)}} = \frac{\sqrt{n}}{n+1}$, we can get the desired property with $\delta = \frac{3}{r^2}$.

To get the other part of RIP-1, we need to examine the quantity

$$\frac{1}{r} \frac{1}{\sqrt{n(n+1)}} \|A(x_1x_1^* - \lambda x_2x_2^*)\|_1 = d \frac{1}{r} \sum_{i=1}^m |u_{i1}|^2 - \lambda |u_{i2}|^2 | = \frac{1}{r} \sum_{k=1}^r \sum_{i=1}^n |u_{i1}^{(k)}|^2 - \lambda |u_{i2}^{(k)}|^2$$

and show that it is lower bounded by a multiple of the operator norm of $X = x_1x_1^* - \lambda x_2x_2^*$ whp. This sum may be expressed as a function of $2rn$ iid gaussian rvs. This function is not Lipschitz, so we will use a surrogate function that is Lipschitz in order to apply Talagrand’s inequality [3] and then show that this introduces only a very small error.

We will treat the real and complex cases simultaneously. To be specific, one way to obtain the Haar measure on $O(n)$ or $U(n)$ is to perform Gram-Schmidt on the columns of a gaussian or complex gaussian matrix. Thus, we will consider the columns $u_1$ and $u_2$ of a Haar-distributed orthogonal matrix as the result of the Gram-Schmidt procedure on a pair of iid gaussian vectors $\zeta$ and $z$. Introduce the functions $v(x) = \frac{x}{\|x\|_2}$ and $t(x,y) = x - y \langle y, x \rangle$. Then if $\zeta, z$ are iid $\mathcal{N}(0, I)$ or $\mathcal{CN}(0, I, 0)$, it can be verified that

$$(u_1, u_2) = d (v(z), v(t(v(\zeta), v(z))))$$

We can now express the distribution of the quantity above as

$$\frac{1}{r} \sum_{i=1}^m |u_{i1}|^2 - \lambda |u_{i2}|^2 | = \frac{1}{r} \sum_{k=1}^r F(\zeta^{(k)}, z^{(k)})$$

$$= \frac{1}{r} \sum_{k=1}^r \sum_{i=1}^n |v(z^{(k)})_i|^2 - \lambda |v(t(v(\zeta^{(k)}), v(z^{(k)})))_i|^2$$
Now take

\[ \frac{1}{r} \sum_{k=1}^{r} \tilde{F}(\zeta^{(k)}, z^{(k)}) = \frac{1}{r} \sum_{k=1}^{r} \sum_{i=1}^{n} |\tilde{v}_1(z^{(k)}_i)|^2 - \lambda |\tilde{v}_2(t(\tilde{v}_1(\zeta^{(k)}), \tilde{v}_1(z^{(k)})))_i|^2 \]

is equal to the original with probability at least

\[ 1 - 2r \mathbb{P}\{\|\zeta\|_2^2 < \frac{n}{c_1}\} - r \mathbb{P}\{\left\langle \frac{\zeta}{\|\zeta\|_2}, \frac{z}{\|z\|_2} \right\rangle \geq 1 - c_2 \} \geq 1 - O(\gamma n) \]

where \( \gamma \) can be made arbitrarily large by taking \( c_1 \) large enough and \( c_2 \) small enough. It now remains to verify that the surrogate function is Lipschitz with a good enough constant and that it introduces only a small error.

Consider the function \( g(x, y) = \sum_{i=1}^{n} |x_i|^2 - \lambda |y_i|^2 \), with \( x, y \in \mathbb{R}^n \) or \( \mathbb{C}^n \) and assume \( \|x_i\|_2 \leq 1, \|y_i\|_2 \leq 1 \). We have

\[
|g(x_1, y_1) - g(x_2, y_2)| \leq \sum_{i=1}^{n} \left| |x_{1i}|^2 - \lambda |y_{1i}|^2 - |x_{2i}|^2 - \lambda |y_{2i}|^2 \right|
\leq \sum_{i=1}^{n} \left| (|x_{1i}|^2 - |x_{2i}|^2) - \lambda (|y_{1i}|^2 - |y_{2i}|^2) \right|
\leq \sum_{i=1}^{n} \left| (|x_{1i}| + |x_{2i}|)(|x_{1i}| - |x_{2i}|) + \lambda (|y_{1i}| + |y_{2i}|)(|y_{1i}| - |y_{2i}|) \right|
\leq \|x_1 - x_2\|_2 \|x_1 - x_2\|_2 + \lambda \|y_1\|_2 \|y_1 - y_2\|_2
\leq 2\|x_1 - x_2\|_2 + 2\|y_1 - y_2\|_2
\]

Now take

\[
\tilde{F}(\zeta_1, z_1) - \tilde{F}(\zeta_2, z_2)
= |g(\tilde{v}_1(\zeta_1), \tilde{v}_2(t(\tilde{v}_1(\zeta_1), \tilde{v}_1(z_1)))) - g(\tilde{v}_1(\zeta_2), \tilde{v}_2(t(\tilde{v}_1(\zeta_2), \tilde{v}_1(z_2))))|
\leq 2\|\tilde{v}_1(z_1) - \tilde{v}_1(z_2)\|_2 + 2\lambda \|\tilde{v}_2(t(\tilde{v}_1(\zeta_1), \tilde{v}_1(z_1))) - \tilde{v}_2(t(\tilde{v}_1(\zeta_2), \tilde{v}_1(z_2)))\|_2
\leq 2\text{Lip}(\tilde{v}_1)\|z_1 - z_2\|_2 + 2\lambda \text{Lip}(\tilde{v}_2)\|t(\tilde{v}_1(\zeta_1), \tilde{v}_1(z_1)) - t(\tilde{v}_1(\zeta_2), \tilde{v}_1(z_2))\|_2
\leq 2\text{Lip}(\tilde{v}_1)\|z_1 - z_2\|_2 + 2\lambda \text{Lip}(\tilde{v}_2)\text{Lip}(t)\|\tilde{v}_1(\zeta_1) - (\zeta_2, z_2)\|_2
\leq 2\text{Lip}(\tilde{v}_1)\|z_1 - z_2\|_2 + 2\lambda \text{Lip}(\tilde{v}_2)\text{Lip}(t)\|\tilde{v}_1(\zeta_1) - (\zeta_2, z_2)\|_2
\]

One can verify that in either the real or complex case, when \( \|x_i\|_2, \|y_i\|_2 \leq 1 \), the function \( t \) satisfies

\[
\|t(x_1, y_1) - t(x_2, y_2)\|_2 \leq 2\|(x_1, y_1) - (x_2, y_2)\|_2
\]
For $x \in \mathbb{R}^n$, let $\hat{v}(x) = \frac{x}{\|x\|_2 v(x)}$ for some positive constant $c$. Now, we have that $D(\frac{x}{\|x\|_2}) = \frac{1}{\|x\|_2^2}(\|x\|_2^2 I - xx^*)$ and hence $\|D(\frac{x}{\|x\|_2})\| \leq \frac{2}{\|x\|_2^2}$. Thus, $\|D(\hat{v})\| \leq \frac{2}{c}$ on $B(0, c)$ so that $\text{Lip}(\hat{v}) \leq \frac{2}{c}$ for any open convex set $U \in B(0, c)^c$. Furthermore, we have $D(\hat{v}) = \frac{1}{c}I$ on $B(0, c)$ and thus $\|D(\hat{v})\| \leq \frac{1}{c}$ on $B(0, c)$ so that $\text{Lip}(\hat{v}|_{B(0, c)}) \leq \frac{1}{c}$.

Take $x_i \in B(0, c)^c$, $i = 1, 2$ such that the line connecting these two points intersects $B(0, c)$. Assume that the point(s) of intersection are $z_1$ and $z_2$ (with the line from $x_1$ to $x_2$ first hitting $z_1$ and then $z_2$). Then we have

$$\|\hat{v}(x_1) - \hat{v}(x_2)\|_2 \leq \|\hat{v}(x_1) - \hat{v}(z_1)\|_2 + \|\hat{v}(z_1) - \hat{v}(z_2)\|_2 + \|\hat{v}(z_2) - \hat{v}(x_2)\|_2$$

$$\leq \frac{2}{c} \|x_1 - z_1\|_2 + \frac{1}{c} \|z_1 - z_2\|_2 + \frac{2}{c} \|z_2 - x_2\|_2$$

$$\leq \frac{2}{c} \|x_1 - x_2\|_2$$

where for the sets $U_i$ we take $B(x_i, \|z_i - x_i\|_2)$. The other cases of arrangements of $x_i$ are similarly proven. We conclude that $\text{Lip}(\hat{v}) \leq \frac{2}{c}$. Note that this implies that in the complex case, we also have $\text{Lip}(\hat{v}) \leq \frac{2}{c}$ with $\hat{v}$ defined analogously. We have thus established that $\text{Lip}(\hat{v}_1) \leq \frac{\sqrt{c_1}}{\sqrt{n}}$ and $\text{Lip}(\hat{v}_2) \leq \frac{2}{\sqrt{c_1}}$. Using this information,

$$|\tilde{F}(\zeta_1, z_1) - \tilde{F}(\zeta_2, z_2)| \leq \frac{16 \sqrt{c_1}}{\sqrt{n}} \|\zeta_1 - (\zeta_2, z_2)\|_2$$

Finally, this implies

$$\text{Lip}(\frac{1}{r} \sum_{k=1}^{r} \tilde{F}(\zeta(k), z(k))) \leq \frac{16 \sqrt{c_1}}{\sqrt{n} \sqrt{r}}$$

By Talagrand’s inequality, we have

$$\mathbb{P}\left\{ \frac{1}{r} \sum_{k=1}^{r} \tilde{F}(\zeta(k), z(k)) - \mathbb{E} \left[ \frac{1}{r} \sum_{k=1}^{r} \tilde{F}(\zeta(k), z(k)) \right] \geq t \right\} \leq e^{-c(rn)t^2}$$

for a constant $c$ which depends on $c_1$. Let

$$\tilde{G} = \frac{1}{r} \sum_{k=1}^{r} \tilde{F}(\zeta(k), z(k)), \quad G = \frac{1}{r} \sum_{k=1}^{r} F(\zeta(k), z(k)).$$

$G$ and $\tilde{G}$ are both bounded by 2 and disagree on a set of probability $O (re^{-cn})$, thus

$$\lim_{n \to \infty} \left| \mathbb{E}[\tilde{G}] - \mathbb{E}[G] \right| = 0.$$
Therefore, we have established

\[ \mathbb{P}\{ |G - \mathbb{E}[G]| \geq t \} \]
\[ \leq \mathbb{P}\{ |\tilde{G} - \mathbb{E}[\tilde{G}]| \geq t - |\tilde{G} - G| - |\mathbb{E}[\tilde{G}] - \mathbb{E}[G]| \} \]
\[ \leq \mathbb{P}\{ G \neq \tilde{G} \} + \mathbb{P}\{ |\tilde{G} - \mathbb{E}[\tilde{G}]| \geq t - |\mathbb{E}[\tilde{G}] - \mathbb{E}[G]| \} \]
\[ \leq O(re^{-\gamma n}) + e^{-c(rn)(t/2)^2} \]

Therefore, we have established

\[ \mathbb{P}\left\{ \left| \frac{1}{r} \sum_{i=1}^{m} |u_{i1}|^2 - \lambda |u_{i2}|^2 \right| - \mathbb{E}\left[ \left| \frac{1}{r} \sum_{i=1}^{m} |u_{i1}|^2 - \lambda |u_{i2}|^2 \right| \right] \geq t \} \leq e^{-c(rn)(t/2)^2} + O(re^{-\gamma n}) \]

for constants \( c \) and \( \gamma \) which depend on \( c_i \). To achieve an arbitrarily fast exponential rate, first select \( c \) so that \( \gamma \) is as large as needed, then fix \( r \) large enough.

We claim that \( \mathbb{E}\left[ |u_{i1}|^2 - \lambda |u_{i2}|^2 \right] = \frac{1 + \lambda^2}{n + 1 + x} \), which we compute below. We have from [4] that \((|u_{i1}|^2, \ldots, |u_{n-1}|^2)\) are uniformly distributed on \( \{(x_1, \ldots x_{n-1}); x_i \geq 0, \sum_{i=1}^{n-1} x_i \leq 1\} \). Thus

\[ \mathbb{E}\left[ |u_{i1}|^2 - \lambda |u_{i2}|^2 \right] \frac{1}{(n-1)(n-2)} \]
\[ = (n-3)! \int_{\mathbb{R}^{n-1}} |x_1 - \lambda x_2| \chi_{\{\sum_{i=1}^{n-1} x_i \leq 1, x_i \geq 0\}} \ dx_1 \cdots \ dx_{n-1} \]
\[ = (n-3)! \int_{\mathbb{R}^{2}} |x_1 - \lambda x_2| \chi_{\{x_1+x_2 \leq 1, x_i \geq 0\}} \int_{\mathbb{R}^{n-3}} \chi_{\{x_1+x_2 \leq 1 \}} \ dx_3 \cdots \ dx_{n-1} \]
\[ = (n-3)! \int_{\mathbb{R}^{2}} |x_1 - \lambda x_2| (1 - (x_1 + x_2))^{n-3} \chi_{\{x_1+x_2 \leq 1 \}} \ dx_1 \ dx_2 \]
\[ = \int_{0}^{1} \int_{0}^{\lambda x_2} \chi_{\{x_1 + x_2 \leq 1 \}} (x_2 - x_1) (1 - (x_1 + x_2))^{n-3} \ dx_1 \ dx_2 \]
\[ + \chi_{\{x_1 \geq \lambda x_2 \}} \int_{0}^{1-x_2} (\lambda x_2 - x_1) (1 - (x_1 + x_2))^{n-3} \ dx_1 \]
\[ + \chi_{\{x_1 \leq \lambda x_2 \}} \int_{0}^{1-x_2} (\lambda x_2 - x_1) (1 - (x_1 + x_2))^{n-3} \ dx_1 \]
\[ + \chi_{\{x_1 + x_2 \leq 1 \}} \int_{\lambda x_2}^{1-x_2} (\lambda x_2 - x_1) (1 - (x_1 + x_2))^{n-3} \ dx_1 \ dx_2 \]
\[ + \int_{0}^{x} \int_{0}^{\lambda x_2} (\lambda x_2 - x_1) (1 - (x_1 + x_2))^{n-3} \ dx_1 \ dx_2 \]
\[ + \int_{0}^{1} \int_{0}^{1-x_2} (\lambda x_2 - x_1) (1 - (x_1 + x_2))^{n-3} \ dx_2 \ dx_2 \]

6
\[
\begin{align*}
&= \int_0^{1+x} \lambda x_2 \left( \frac{-1}{n-2} (1 - (x_1 + x_2))^{n-2} \right) \bigg|_0^{\lambda x_2} - \int_0^{\lambda x_2} x_1 (1 - (x_1 + x_2))^{n-3} dx_1 dx_2 \\
&+ \int_0^{1+x} \int_0^{1-x_2} x_1 (1 - (x_1 + x_2))^{n-3} dx_1 - \lambda x_2 \left( \frac{-1}{n-2} (1 - (x_1 + x_2))^{n-2} \right) \bigg|_0^{1-x_2} dx_2 \\
&+ \int_0^1 \lambda x_2 \left( \frac{-1}{n-2} (1 - (x_1 + x_2))^{n-2} \right) \bigg|_0^{1-x_2} - \int_0^{1-x_2} x_1 (1 - (x_1 + x_2))^{n-3} dx_1 dx_2 \\
&= \int_0^{1+x} \lambda x_2 \left( \frac{-1}{n-2} (1 - (1 + \lambda)x_2)^{n-2} + \frac{1}{n-2} (1 - x_2)^{n-2} \right) dx_2 \\
&- \int_0^{\lambda x_2} x_1 (1 - (x_1 + x_2))^{n-3} dx_1 dx_2 \\
&+ \int_0^{1+x} \int_0^{1-x_2} x_1 (1 - (1 + \lambda)x_2)^{n-3} dx_1 - \lambda x_2 \left( \frac{1}{n-2} (1 - (1 + \lambda)x_2)^{n-2} \right) dx_2 \\
&+ \int_0^1 \lambda x_2 \left( \frac{1}{n-2} (1 - x_2)^{n-2} \right) dx_1 - \int_0^{1-x_2} x_1 (1 - (1 + \lambda)x_2)^{n-3} dx_1 dx_2 \\
&= \frac{\lambda}{(1 + \lambda)^2} \frac{-1}{n-2} \int_0^1 x_2 (1 - x_2)^{n-2} dx_2 + \lambda \frac{1}{n-2} \int_0^{1+x} x_2 (1 - x_2)^{n-2} dx_2 \\
&- \int_0^{1+x} \frac{-1}{n-2} x_1 (1 - (x_1 + x_2))^{n-2} \bigg|_0^{\lambda x_2} - \frac{1}{(n-2)(n-1)} (1 - (x_1 + x_2))^{n-1} \bigg|_0^0 dx_2 \\
&+ \int_0^{1+x} \frac{-1}{n-2} x_1 (1 - (x_1 + x_2))^{n-2} \bigg|_0^{1-x_2} - \frac{1}{(n-2)(n-1)} (1 - (x_1 + x_2))^{n-1} \bigg|_0^{1-x_2} dx_2 \\
&- \frac{-\lambda}{(1 + \lambda)^2} \frac{1}{n-2} \int_0^1 x_2 (1 - x_2)^{n-2} dx_2 + \frac{\lambda}{n-2} \int_0^1 x_2 (1 - x_2)^{n-2} dx_2 \\
&- \int_0^{1+x} \frac{-1}{n-2} x_1 (1 - (x_1 + x_2))^{n-2} \bigg|_0^{1-x_2} - \frac{1}{(n-2)(n-1)} (1 - (x_1 + x_2))^{n-1} \bigg|_0^{1-x_2} dx_2
\end{align*}
\]
measurements, this shows that there exists some integer such that the measurements of 2\((\sqrt{2} - 1) > 0.828.

2.1 Implications related to Wright’s conjecture

Using the same covering argument over rank-2 indefinite matrices as in Lemma 3.4.2 in [S], we obtain the RIP-1 property for unitary matrices. Since RIP-1 is stronger than injectivity of the measurements, this shows that there exists some integer \(r\) such that the measurements \(|U_i x|_{i=1}^r\),
where $U_i$ are iid Haar distributed unitary matrices, are injective up to global phase with very high probability. It would be interesting to see how small of an integer $r$ can be achieved by probabilistic arguments, say by using more sophisticated concentration arguments, but there seems to be a bottleneck in the large constants that appear in concentration inequalities. On the other hand, algebraic and differential geometry techniques are successful in establishing that an RIP-1 property with some nonzero, possibly very small constant holds for 4 unitary matrices [2].

3 Dual certification

We start with a useful property:

3.1 Moments of entries of a unitary matrix

Wlog, we shall further treat below the complex case only. We record some useful identities from [7]. Let $u_{ij}$ be an entry of a $n \times n$ Haar distributed unitary matrix. Then

$$\mathbb{E}[|u_{ij}|^{2d}] = \frac{d!}{n(n+1) \ldots (n+d-1)}$$

Which implies that $\mathbb{E}[|u_{ia}|^4] = \frac{2}{n(n+1)}$. Using the identity

$$\frac{1}{n} = \mathbb{E}[|u_{ia}|^2] = \mathbb{E}[|u_{ia}|^2(\sum_{b=1}^{n} |u_{ib}|^2)] = \mathbb{E}[|u_{ia}|^4] + (n-1) \mathbb{E}[|u_{ib}|^2|u_{ia}|^2]$$

we obtain, for $a \neq b$

$$\mathbb{E}[|u_{ia}|^2|u_{ib}|^2] = \frac{1}{n(n+1)}$$

3.2 Dual Certificates

With $A$ as above, it can be verified that

$$\frac{1}{m} \mathbb{E}[A^*A] = I - \frac{1}{n+1} I \otimes I = S$$

and we have $S^{-1}(X) = X - \frac{1}{n+1} \text{Tr}(X) I_n$. Thus, the regular construction of the dual certificate would be

$$\frac{1}{m} A^* S^{-1} (e_1 e_1^*) = \frac{1}{m} \sum_{i=1}^{m} n(n+1) u_i u_i^* \otimes u_i u_i^* (e_1 e_1^* - \frac{1}{n+1} I_n)$$

$$= \frac{n(n+1)}{m} \sum_{i=1}^{m} (|u_{i1}|^2 - \frac{1}{n+1}) u_i u_i^*$$

$$= \frac{n}{m} \sum_{i=1}^{m} ((n+1)|u_{i1}|^2 - 1) u_i u_i^*$$
Let $\psi_n = \mathbb{E} \left[ (n)(n + 1)(|u_{i1}| \wedge \frac{3}{\sqrt{n+1}})^4 \right]$. $\psi_n$ is slightly less than 2. Using a construction similar to that found in [5], we could then take the enhanced certificate to be

$$Y = \frac{1}{m} \sum_{i=1}^{m} (2n(n + 1)(|u_{i1}| \wedge \frac{3}{\sqrt{n+1}})^2 - n(2\psi_n - 1))u_iu_i^*$$

We have then the expected value of this sum is 1 in the upper left corner, near to -1 on the rest of the diagonal and zero elsewhere. Furthermore, the contribution of the $|u_{i1}|$ term is capped to not be too large. We thus hope to acquire the same properties of the enhanced dual certificate as in the gaussian case.

### 3.3 Behavior of $Y_T$

Here we control the quantity $\|Y_T - e_1e_1^*\|_F$. We can re-write the certificate as

$$Y = \frac{1}{r} \sum_{k=1}^r \sum_{i=1}^n (2(n + 1)(|u_{i1}^{(k)}| \wedge \frac{3}{\sqrt{n+1}})^2 - (2\psi_n - 1))u_i^{(k)}u_i^{(k)*}$$

where $\{u_i^{(k)}\}_{i=1}^n$ are (indexed by k) iid Haar distributed on $U_n$. To show that $\|Y_T - e_1e_1^*\|_F$ is small, it is enough to show that

$$\left\| \frac{1}{r} \sum_{k=1}^r x_k - e_1 \right\|_2$$

is small, where

$$x_k = \sum_{i=1}^n (2(n + 1)(|u_{i1}| \wedge \frac{3}{\sqrt{n+1}})^2 - (2\psi_n - 1))\bar{u}_{i1}u_i$$
We have

\[ \mathbb{E} \left[ \|x_k\|^2 \right] = \mathbb{E} \left[ \sum_{i=1}^{n} \left( (2(n+1)(|u_{i1}| \wedge \frac{3}{\sqrt{n+1}})^2 - (2\psi_n - 1)) |u_{i1}|^2 \right) \right] \]

\[ = n \mathbb{E} \left[ \left( 4(n+1)^2 \left( |u_{i1}| \wedge \frac{3}{\sqrt{n+1}} \right)^4 \right) |u_{i1}|^2 \right] + \]

\[ n \mathbb{E} \left[ \left( (2\psi_n - 1)^2 - 4(n+1)(2\psi_n - 1) \left( |u_{i1}| \wedge \frac{3}{\sqrt{n+1}} \right)^2 \right) |u_{i1}|^2 \right] \]

\[ = 4n(n+1)^2 \mathbb{E} \left[ \left( |u_{i1}| \wedge \frac{3}{\sqrt{n+1}} \right)^4 |u_{i1}|^2 \right] + (2\psi_n - 1)^2 \]

\[ - 4n(n+1)(2\psi_n - 1) \mathbb{E} \left[ \left( |u_{i1}| \wedge \frac{3}{\sqrt{n+1}} \right)^2 |u_{i1}|^2 \right] \]

\[ \leq 4n(n+1)^2 \mathbb{E} \left[ |u_{i11}|^6 \right] + (2\psi_n - 1)^2 - 4n(n+1)(2\psi_n - 1) \mathbb{E} \left[ \left( |u_{i1}| \wedge \frac{3}{\sqrt{n+1}} \right)^4 \right] \]

\[ = 4n(n+1)^2 \frac{3!}{n(n+1)(n+2)} + 4\psi_n^2 - 4\psi_n + 1 - 4(2\psi_n - 1)\psi_n \]

\[ = 24 \frac{n+1}{n+2} + 1 - 4\psi_n^2 \leq 24 \]

Furthermore, we have

\[ \|x_k\|_2 = \left( \sum_{i=1}^{n} \left( (2(n+1)(|u_{i1}| \wedge \frac{3}{\sqrt{n+1}})^2 - (2\psi_n - 1)) |u_{i1}|^2 \right) \right)^{1/2} \leq \sqrt{24} \]

These facts allow us to apply the vector Bernstein inequality (Theorem 3.5.3) to get that \( \|Y_T - e_1 e_1^*\|_F \) is as small as necessary with probability at least \( 1 - e^{-cr} \) for some constant \( c \).

### 3.4 Behavior of \( Y_{T\perp} \)

We would like to show that \( Y_{T\perp} \prec 0 \) whp. It is enough to consider \( \sup \{ \langle x, Y_{T\perp} x \rangle ; x \in \mathbb{C}S^n, x_1 = 0 \} \) and we aim to control this quantity via a covering argument. Using rotational invariance, we have

\[ \langle x, Y_{T\perp} x \rangle = \mathbb{E} \left[ \langle e_2, Y_{T\perp} e_2 \rangle \right] = \frac{1}{r} \sum_{k=1}^{r} \sum_{i=1}^{n} (2(n+1)(|u_{i1}^{(k)}| \wedge \frac{3}{\sqrt{n+1}})^2 - (2\psi_n - 1)) |u_{i2}^{(k)}|^2 \]

\[ = \frac{1}{r} \sum_{k=1}^{r} \sum_{i=1}^{n} (2(n+1)(|u_{i1}^{(k)}| \wedge \frac{3}{\sqrt{n+1}})^2 |u_{i2}^{(k)}|^2 - (2\psi_n - 1)) \]

A straightforward application of Talagrand’s inequality fails here. Bernstein’s inequality for weakly dependent variables also fails [1], so we will use an approach that involves conditioning and Talagran-
grand’s inequality. It suffices to show that
\[
\frac{1}{r} \sum_{k=1}^{r} \sum_{i=1}^{n} (2(n+1)(|u_{i1}^{(k)}| \wedge \frac{3}{\sqrt{n+1}})^2 - \phi_n)|u_{i2}^{(k)}|^2
\]
concentrates well about 0, where
\[
\phi_n = \mathbb{E} \left[ \frac{1}{r} \sum_{k=1}^{r} \sum_{i=1}^{n} (2(n+1)(|u_{i1}^{(k)}| \wedge \frac{3}{\sqrt{n+1}})^2)|u_{i2}^{(k)}|^2 \right] = \mathbb{E} \left[ 2n(n+1)(|u_{i1}| \wedge \frac{3}{\sqrt{n+1}})^2|u_{i2}|^2 \right] \leq 2
\]
we have,
\[
\frac{1}{r} \sum_{k=1}^{r} \sum_{i=1}^{n} (2(n+1)(|u_{i1}^{(k)}| \wedge \frac{3}{\sqrt{n+1}})^2 - \phi_n)|u_{i2}^{(k)}|^2 = d \frac{1}{r} \sum_{k=1}^{r} G^{(k)}(z^{(k)})
\]
and as before, we consider the surrogate function
\[
\frac{1}{r} \sum_{k=1}^{r} \tilde{G}^{(k)}(z^{(k)}) = \frac{1}{r} \sum_{k=1}^{r} \sum_{i=1}^{n} (2(n+1)(|\tilde{v}_{1}(z^{(k)})| \wedge \frac{3}{\sqrt{n+1}})^2 - \phi_n)|\tilde{v}_{2}(t(\tilde{v}_{1}(z^{(k)}), \tilde{v}_{1}(z^{(k)})))|^2
\]
Now,
\[
\mathbb{P}\left( \frac{1}{r} \sum_{k=1}^{r} \tilde{G}^{(k)}(z^{(k)}) \geq t \right) = \mathbb{E} \left[ \mathbb{E} \left[ \chi_{\left(\frac{1}{r} \sum_{k=1}^{r} \tilde{G}^{(k)}(z^{(k)}) \geq t \right)} \left( z^{(1)}, \ldots, z^{(r)} \right) \right] \right] = \mathbb{E}_z \left[ \mathbb{P}_\xi \left( \frac{1}{r} \sum_{k=1}^{r} \tilde{G}^{(k)}(z^{(k)}) \geq t \right) \right]
\]
\[
\leq \mathbb{E}_z \left[ \mathbb{P}_\xi \left( \frac{1}{r} \sum_{k=1}^{r} \tilde{G}^{(k)}(z^{(k)}) - \mathbb{E}_\xi \left[ \frac{1}{r} \sum_{k=1}^{r} \tilde{G}^{(k)}(z^{(k)}) \right] \geq t - \mathbb{E}_\xi \left[ \frac{1}{r} \sum_{k=1}^{r} \tilde{G}^{(k)}(z^{(k)}) \right] \right) \right]
\]
\[
\leq \mathbb{E}_z \left[ \mathbb{P}_\xi \left( \frac{1}{r} \sum_{k=1}^{r} \tilde{G}^{(k)}(z^{(k)}) - f(\{|z^{(i)}|_{i=1}^{r}\} \geq t - t_1) \chi_{\{|f({z^{(i)}})_{i=1}^{r}| \leq t_1\}} \right) \right] + \mathbb{P}(|f(\{z^{(i)}\}_{i=1}^{r})| > t_1)
\]
where \( f(\{z^{(i)}\}_{i=1}^{r}) = \mathbb{E}_\xi \left[ \frac{1}{r} \sum_{k=1}^{r} \tilde{G}^{(k)}(z^{(k)}) \right] \).
It now suffices to analyze the quantities \( \text{Lip}_\zeta(\tilde{G}(\zeta, z)) \) and \( \mathbb{E}_\zeta \left[ \tilde{G}(\zeta, z) \right] \) as functions of \( z \).

For \( x \in \mathbb{R}^n \) or \( \mathbb{C}^n \), \( g(x) = \sum_{i=1}^n a_i |x_i|^2 \) and \( \|x_1\|_2 + \|x_2\|_2 \leq 2 \), we have
\[
|g(x_1) - g(x_2)| \leq 2\|a\|_\infty \|x_1 - x_2\|_2
\]

Letting \( a_i = \left(2(n+1)(|\tilde{v}_1(z)|_i \wedge \frac{3}{\sqrt{n+1}})^2 - \phi_n\) and noting \( a_\infty \leq 20 \)
\[
\left| \tilde{G}(\zeta_1, z) - \tilde{G}(\zeta_2, z) \right| = |g(\tilde{v}_2(t(\tilde{v}_1(\zeta_1), \tilde{v}_1(z)))) - g(\tilde{v}_2(t(\tilde{v}_1(\zeta_2), \tilde{v}_1(z))))| \\
\leq 2\|a\|_\infty \|\tilde{v}_2(t(\tilde{v}_1(\zeta_1), \tilde{v}_1(z))) - \tilde{v}_2(t(\tilde{v}_1(\zeta_2), \tilde{v}_1(z)))\|_2 \\
\leq 40\text{Lip}(\tilde{v}_2)\text{Lip}(t_{S(0,1)^2})\text{Lip}(\tilde{v}_1)\|\zeta_1 - \zeta_2\|_2
\]

In conclusion
\[
\text{Lip}_\zeta(\tilde{G}(\zeta, z)) \leq 8 \times 40 \frac{\sqrt{\epsilon_2}}{\sqrt{n}}
\]

uniformly in \( z \) and thus
\[
\text{Lip}(\frac{1}{r} \sum_{k=1}^r \tilde{G}(\zeta(k), z(k))) \leq \frac{1}{\sqrt{r}} 8 \times 40 \frac{\sqrt{\epsilon_2}}{\sqrt{n}}
\]

uniformly in \((z(1), \ldots, z(r))\). This gives that
\[
\mathbb{P}_\zeta \left( \left| \frac{1}{r} \sum_{k=1}^r \tilde{G}(\zeta(k), z(k)) - f(z(1), \ldots, z(r)) \right| \geq t \right) \leq e^{-crnt^2}
\]

for a constant \( c \) which depends on \( c_i \) but does not depend on \( z \). Now we need to show that \( f(z(1), \ldots, z(r)) \) concentrates well about its mean and that this mean is very small. We have
\[
f(z(1), \ldots, z(r)) = \frac{1}{r} \sum_{k=1}^r \sum_{i=1}^n \mathbb{E}_\zeta \left[ \left| \tilde{v}_2(t(\tilde{v}_1(\zeta(k)), \tilde{v}_1(z(k))))_i \right|^2 \right] \left( 2(n+1)(|\tilde{v}_1(z)|_i \wedge \frac{3}{\sqrt{n+1}})^2 - \phi_n \right)
\]

Let
\[
h(z) = \{ \mathbb{E}_\zeta \left[ \left| \tilde{v}_2(t(\tilde{v}_1(\zeta), \tilde{v}_1(z)))_i \right|^2 \right] \}_{i=1}^n.
\]

and
\[
p(z) = \{ (2(n+1)(|\tilde{v}_1(z)|_i \wedge \frac{3}{\sqrt{n+1}})^2 - \phi_n) \}_{i=1}^n
\]

First, using the following facts,
\[
\mathbb{E} [\tilde{v}_1(\zeta)_i] = 0 \\
\mathbb{E} [\tilde{v}_1(\zeta)_a \tilde{v}_1(\zeta)_b] = 0, a \neq b \\
\mathbb{E} [\left| \tilde{v}_1(\zeta)_i \right|^2] \leq \frac{1}{n} \\
\mathbb{E} [\left| \langle \tilde{v}_1(\zeta), y \rangle \right|^2] \leq \|y\|^2 \frac{1}{n} \\
\mathbb{E} [2\tilde{v}_1(\zeta)_i \tilde{v}_i \langle \tilde{v}_1(\zeta), y \rangle] = 0
\]
for any $y \in \mathbb{C}^n$, we establish
\begin{align*}
\mathbb{E}_\zeta \left[ |\tilde{h}_2(t(\tilde{v}_1(\zeta), \tilde{v}_1(z)))| \right] & \leq \mathbb{E}_\zeta \left[ \frac{1}{c_2} |(t(\tilde{v}_1(\zeta), \tilde{v}_1(z)))| \right] \\
& \leq \frac{1}{c_2} \mathbb{E}_\zeta \left[ |\tilde{v}_1(\zeta)|^2 + |\tilde{v}_1(z)|^2 \right] \\
& \leq \frac{1}{c_2} \mathbb{E}_\zeta \left[ |\tilde{v}_1(\zeta)|^2 + |\tilde{v}_1(z)|^2 \right] - 2\mathbb{R}(\bar{v}_1(\zeta), \tilde{v}_1(z), \bar{v}_1(\zeta), \tilde{v}_1(z)) \\
& \leq \frac{1}{c_2} \left[ \frac{1}{n} + |\tilde{v}_1(z)|^2 \right] \leq \frac{2}{c_2 n}
\end{align*}

Thus, for any $z$, $\|h(z)\|_\infty \leq \frac{2}{c_2 n}$.

Now we shall compute $\text{Lip}(\sum_{i=1}^n h_i(z) p_i(z))$ directly:
\begin{align*}
\left| \sum_{i=1}^n h_i(z_1) p_i(z_1) - \sum_{i=1}^n h_i(z_2) p_i(z_2) \right| & \leq \|h(z_1)\|_\infty \sum_{i=1}^n |p_i(z_1) - p_i(z_2)| + \|p(z_2)\|_\infty \sum_{i=1}^n |h(z_2) - h(z_2)| \\
& \leq 2(n+1)\|h(z_1)\|_\infty \sum_{i=1}^n \left| |\tilde{v}_1(z_1)| - \left(3 \frac{1}{\sqrt{n+1}} \right)^2 - |\tilde{v}_1(z_2)| - \left(3 \frac{1}{\sqrt{n+1}} \right)^2 \right| + \\
& \|p(z_2)\|_\infty \mathbb{E}_\zeta \left[ \sum_{i=1}^n \left| \tilde{v}_2(t(\tilde{v}_1(\zeta), \tilde{v}_1(z_1))) - \tilde{v}_2(t(\tilde{v}_1(\zeta), \tilde{v}_1(z_2))) \right| \right] \\
& \leq 2(n+1)\|h(z_1)\|_\infty 2\text{Lip}(\tilde{v}_1) + \|p(z_2)\|_\infty 2\text{Lip}(\tilde{v}_2)\text{Lip}(t|_{E(0,1)}) \text{Lip}(\tilde{v}_1) \|z_1 - z_2\|_2 \\
& \leq \left( \frac{16 \sqrt{n+1}}{n} \frac{1}{c_2^\epsilon} + 2 \frac{1}{c_2^\epsilon} \right) \|z_1 - z_2\|_2
\end{align*}

Thus,
\begin{align*}
\text{Lip}(f(z^{(1)}, \ldots, z^{(r)})) = O \left( \frac{1}{c_2^\epsilon} \right)
\end{align*}

This will allow us to get the desired concentration of $f(z^{(1)}, \ldots, z^{(r)})$ around its mean via Talagrand’s inequality. Namely, we obtain
\begin{align*}
P \left( \left| f(z^{(1)}, \ldots, z^{(r)}) - \mathbb{E} \left[ f(z^{(1)}, \ldots, z^{(r)}) \right] \right| \geq t \right) \leq e^{-c \epsilon t^2}
\end{align*}

for a constant $c$ which depends on $c_i$.

Let $F = \frac{1}{r} \sum_{k=1}^r G(\zeta^{(k)}, z^{(k)})$ and $\tilde{F} = \frac{1}{r} \sum_{k=1}^r \tilde{G}(\zeta^{(k)}, z^{(k)})$. Then $\mathbb{E} \left[ f(z^{(1)}, \ldots, z^{(r)}) \right] = \mathbb{E} \left[ \tilde{F} \right]$ and note $\mathbb{E} \left[ F \right] = 0$. Since both $F$ and $\tilde{F}$ are bounded and differ on a set of exponentially small
probability, for any valid choice of $c_i$, $\lim_{n \to \infty} E[\tilde{F}] = 0$ and so having fixed $t$ apriori, for $n$ large enough

$$P\left(\left| f(z^{(1)}, \ldots, z^{(r)}) \right| \geq \frac{t}{2}\right) \leq e^{-cn(t/4)^2}$$

Taking $t_1 = \frac{t}{2}$, this implies

$$P\left(\left| \frac{1}{r} \sum_{k=1}^r G(\ell^{(k)}, z^{(k)}) \right| \geq t\right) \leq e^{-cn(t-\frac{t_1}{2})^2} + e^{-cn(t/4)^2}$$

Now using that $F$ and $\tilde{F}$ differ on a set of probability at most $O(re^{-\gamma n})$, we have

$$P(|F| \geq t) \leq P\{|\tilde{F}| \geq t - |\tilde{F} - F|\} \leq P\{F \neq \tilde{F}\} + P\{|\tilde{F}| \geq t\} \leq O(re^{-\gamma n}) + e^{-cn(t/2)^2} + e^{-cn(t/4)^2}$$

Therefore, we have established

$$P\{\langle x, Y_{\perp_{x}} \rangle \geq t + \phi_n - (2\psi_n - 1)\} \leq O(re^{-\gamma n}) + e^{-cn(t/2)^2} + e^{-cn(t/4)^2}$$

To get an arbitrarily fast exponential rate of concentration, fix $\gamma$ to be as large as needed by choosing $c_i$ appropriately, then fix $r$ large enough. Note that $\phi_n \leq 2$ and $\psi_n$ is very close to 2 so that $\phi_n - (2\psi_n - 1) \approx -1$. Choosing an appropriate $t$, we get that $Y_{\perp_{x}}$ is negative definite with high probability via the standard covering argument, which completes the proof of the main theorem.

4 Discussion

We show that pure states can be recovered from few full-rank observables using the PhaseLift algorithm. We note that these results can be extended to show noise stability by using a modified convex program, as well as uniformity over signals $x \in \mathbb{C}^n$. Finally, a very similar proof would yield that rank-$k$ states $X_k = \sum_{i=1}^k \lambda_i x_i x_i^*$ can be recovered from $m = O(kn)$ measurements, by establishing an RIP-1 property for rank $2k$ matrices and a using a dual certificate motivated by $A^*A(X_k)$.

5 Acknowledgements

We acknowledge fruitful discussions with Emmanuel Candes and Xiaodong Li.

References

[1] Bernstein’s inequality. Wikipedia.
[2] V. Voroninski, D. Mondragon. Determination of all pure quantum states from a minimal number of observables. Arxiv, http://arxiv.org/abs/1306.1214, 2013.

[3] X. Li, E. Candes. Solving quadratic equations via phaselift when there are about as many equations as unknowns. Arxiv. http://arxiv.org/abs/1208.6247, August 2012.

[4] L. Demanet, P. Hand. Stable optimizationless recovery from phaseless linear measurements. Arxiv. http://arxiv.org/abs/1208.1803, 2012.

[5] T. Heinosaari, L. Mazzarella, and M.M. Wolf. Quantum tomography under prior information. Preprint, [arXiv:1109.5478], 2011.

[6] D. Mixon. Short, fat matrices. Online Blog, 2012.

[7] J. Novak. Truncations of random unitary matrices and young tableaux. The electronic journal of combinatorics, 14(R21), 2007.

[8] 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.

[9] T. Tao. Talagrand's concentration inequality - blog entry. 2009.