# Phase Retrieval by Linear Algebra 

Pengwen Chen * Albert Fannjiang ${ }^{\dagger}$ Gi-Ren Liu ${ }^{\ddagger}$

October 8, 2018


#### Abstract

The null vector method, based on a simple linear algebraic concept, is proposed as a solution to the phase retrieval problem. In the case with complex Gaussian random measurement matrices, a non-asymptotic error bound is derived, yielding an asymptotic regime of accurate approximation comparable to that for the spectral vector method.


## 1 Introduction

We consider the following phase retrieval problem: Let $A=\left[a_{i}\right]$ be a $n \times N$ random matrix with independently and identically distributed entries in $N(0,1)+i N(0,1)$, i.e. circularly symmetric complex Gaussian random variables. Let $x_{0} \in \mathbb{C}^{n}$ and $y=A^{*} x_{0}$. Suppose we are given $A$ and $b:=|y|$ where $|y|$ denote the vector such that $|y|(j)=|y(j)|, \forall j$. The aim of phase retrieval is to find $x_{0}$.

Clearly this is a nonlinear inversion problem. Simple dimension count shows that, for the solution to be unique in general, the number of (nonnegative) data $N$ needs to be at least twice the number $n$ of unknown (complex) components. There are many approaches to phase retrieval, the most efficient and effective, especially when the problem size is large, being fixed point algorithms (see [3, 4, 6, 7] and references therein) and non-convex optimization methods [1,2]. Phase retrieval has a wide range of applications, see [8] for a recent survey.

The following observation motivates our current approach: Let $I$ be a subset of $\{1, \cdots, N\}$ and $I_{c}$ its complement such that $b(i) \leq b(j)$ for all $i \in I, j \in I_{c}$. In other words, $\{b(i): i \in I\}$ are the "weaker" signals and $\left\{b(j): j \in I_{c}\right\}$ the "stronger" signals. Let $|I|$ be the cardinality of the set $I$. Since $b(i)=\left|a_{i}^{*} x_{0}\right|, i \in I$, are small, $\left\{a_{i}\right\}_{i \in I}$ is a set of sensing vectors nearly orthogonal to $x_{0}$. Denote the sub-column matrices consisting of $\left\{a_{i}\right\}_{i \in I}$ and $\left\{a_{j}\right\}_{j \in I_{c}}$ by $A_{I}$

[^0]and $A_{I_{c}}$, respectively. Define the null vector by the singular vector for the least singular value of $A_{I}$ :
$$
x_{\text {null }}:=\arg \min \left\{\left\|A_{I}^{*} x\right\|^{2}: x \in \mathbb{C}^{n},\|x\|=\left\|x_{0}\right\|\right\}
$$
which can be computed by purely linear algebraic methods.
The goal of the paper is to establish a regime where $x_{\text {null }}$ is an accurate approximation to $x_{0}$.

## 2 Approximation theorem

Note that both $x_{\text {null }}$ and the phase retrieval solution is at best uniquely defined up to a global phase factor. So we use the following error metric

$$
\begin{equation*}
\left\|x_{0} x_{0}^{*}-x_{\text {null }} x_{\text {null }}^{*}\right\|^{2}=2\left\|x_{0}\right\|^{4}-2\left|x_{0}^{*} x_{\text {null }}\right|^{2} \tag{1}
\end{equation*}
$$

which has the advantage of being independent of the global phase factor.
The following theorem is our main result.
Theorem 2.1. Suppose

$$
\begin{equation*}
\sigma:=\frac{|I|}{N}<1, \quad \nu=\frac{n}{|I|}<1 . \tag{2}
\end{equation*}
$$

Then for any $\epsilon \in(0,1), \delta>0$ and $t \in\left(0, \nu^{-1 / 2}-1\right)$ the following error bound

$$
\begin{equation*}
\left\|x_{0} x_{0}^{*}-x_{\text {null }} x_{\text {null }}^{*}\right\|^{2} \leq\left(\left(\frac{2+t}{1-\epsilon}\right) \sigma+\epsilon(-2 \ln (1-\sigma)+\delta)\right) \frac{2\left\|x_{0}\right\|^{4}}{(1-(1+t) \sqrt{\nu})^{2}} \tag{3}
\end{equation*}
$$

holds with probability at least

$$
\begin{equation*}
1-2 \exp \left(-N \delta^{2} e^{-\delta}|1-\sigma|^{2} / 2\right)-\exp \left(-2\lfloor|I| \epsilon\rfloor^{2} / N\right)-Q \tag{4}
\end{equation*}
$$

where $Q$ has the asymptotic upper bound

$$
\begin{equation*}
2 \exp \left\{-c \min \left[\frac{e^{2} t^{2}}{16}\left(\ln \sigma^{-1}\right)^{2}|I|^{2} / N, \frac{e t}{4}|I| \ln \sigma^{-1}\right]\right\}, \quad \sigma \ll 1 \tag{5}
\end{equation*}
$$

with an absolute constant $c$.
Remark 2.2. To unpack the implications of Theorem 2.1, consider the following asymptotic:
With $\epsilon$ and $t$ fixed, let

$$
n \gg 1, \quad \sigma=\frac{|I|}{N} \ll 1, \quad \frac{|I|^{2}}{N} \gg 1, \quad \nu=\frac{n}{|I|}<1
$$

We have

$$
\begin{equation*}
\left\|x_{0} x_{0}^{*}-x_{\text {null }} x_{\text {null }}^{*}\right\|^{2} \leq c_{0} \sigma\left\|x_{0}\right\|^{4} \tag{6}
\end{equation*}
$$

with probability at least

$$
1-c_{1} e^{-c_{2} n}-c_{3} \exp \left\{-c_{4}\left(\ln \sigma^{-1}\right)^{2}|I|^{2} / N\right\}
$$

for moderate constants $c_{0}, c_{1}, c_{2}, c_{3}, c_{4}$.
The proof of Theorem [2.1] is given in the next section.
The spectral vector method [1,2,7 is another linear algebraic method and uses the leading singular vector $x_{\text {spec }}$ of $B^{*}=\operatorname{diag}[b] A^{*}$ to approximate $x_{0}$ where

$$
x_{\text {spec }}:=\arg \max \left\{\left\|B^{*} x\right\|^{2}: x \in \mathrm{C}^{n},\|x\|=\left\|x_{0}\right\|\right\} .
$$

The spectral vector method has a comparable performance guarantee to (6) which vanishes as $\sigma \rightarrow 0$, with probability close to 1 exponentially in $n$.

In practice, however, the null vector method significantly outperforms the spectral vector method in terms of accuracy and noise stability when $b$ is contaminated with noise [4].

The drawback with both approaches is that the error metric vanishes only with infinitely many data, $N \rightarrow \infty$. For a finite data set, the null vector is best to be deployed in conjunction with a fast (locally) convergent fixed point algorithm such as alternating projection [4] or the Douglas-Rachford algorithm [3].

## 3 Proof of Theorem 2.1

The proof is based on the following two propositions.
Proposition 3.1. There exists $x_{\perp} \in \mathrm{C}^{n}$ with $x_{\perp}^{*} x_{0}=0$ and $\left\|x_{\perp}\right\|=\left\|x_{0}\right\|=1$ such that

$$
\begin{equation*}
\frac{1}{4}\left\|x_{0} x_{0}^{*}-x_{\text {null }} x_{\text {null }}^{*}\right\|^{2} \leq \frac{\left\|b_{I}\right\|^{2}}{\left\|A_{I}^{*} x_{\perp}\right\|^{2}} \tag{7}
\end{equation*}
$$

Proof. Since $x_{\text {null }}$ is optimally phase-adjusted, we have

$$
\begin{equation*}
\beta:=x_{0}^{*} x_{\text {null }} \geq 0 \tag{8}
\end{equation*}
$$

and

$$
\begin{equation*}
x_{0}=\beta x_{\mathrm{null}}+\sqrt{1-\beta^{2}} z \tag{9}
\end{equation*}
$$

for some unit vector $z^{*} x_{\text {null }}=0$. Then

$$
\begin{equation*}
x_{\perp}:=-\left(1-\beta^{2}\right)^{1 / 2} x_{\mathrm{null}}+\beta z \tag{10}
\end{equation*}
$$

is a unit vector satisfying $x_{0}^{*} x_{\perp}=0$. Since $x_{\text {null }}$ is a singular vector and $z$ belongs in another singular subspace, we have

$$
\begin{aligned}
\left\|A_{I}^{*} x_{0}\right\|^{2} & =\beta^{2}\left\|A_{I}^{*} x_{\text {null }}\right\|^{2}+\left(1-\beta^{2}\right)\left\|A_{I}^{*} z\right\|^{2}, \\
\left\|A_{I}^{*} x_{\perp}\right\|^{2} & =\left(1-\beta^{2}\right)\left\|A_{I}^{*} x_{\text {null }}\right\|^{2}+\beta^{2}\left\|A_{I}^{*} z\right\|^{2}
\end{aligned}
$$

from which it follows that

$$
\begin{align*}
& \left(2-\beta^{2}\right)\left\|A_{I}^{*} x_{0}\right\|^{2}-\left(1-\beta^{2}\right)\left\|A_{I}^{*} x_{\perp}\right\|^{2}  \tag{11}\\
= & \left\|A_{I}^{*} x_{\mathrm{null}}\right\|^{2}+2\left(1-\beta^{2}\right)^{2}\left(\left\|A_{I}^{*} z\right\|^{2}-\left\|A_{I}^{*} x_{\mathrm{null}}\right\|^{2}\right) \geq 0 .
\end{align*}
$$

By (11), (11) and $\left\|b_{I}\right\|=\left\|A_{I}^{*} x_{0}\right\|$, we also have

$$
\begin{equation*}
\frac{\left\|b_{I}\right\|^{2}}{\left\|A_{I}^{*} x_{\perp}\right\|^{2}} \geq \frac{1-\beta^{2}}{2-\beta^{2}} \geq \frac{1}{2}\left(1-\beta^{2}\right)=\frac{1}{4}\left\|x_{0} x_{0}^{*}-x_{\mathrm{null}} x_{\mathrm{null}}^{*}\right\|^{2} . \tag{12}
\end{equation*}
$$

Proposition 3.2. Let $A \in C^{n \times N}$ be an i.i.d. complex standard Gaussian random matrix. Then for any $\epsilon>0, \delta>0, t>0$

$$
\left\|b_{I}\right\|^{2} \leq|I|\left(\left(\frac{2+t}{1-\epsilon}\right) \frac{|I|}{N}+\epsilon\left(-2 \ln \left(1-\frac{|I|}{N}\right)+\delta\right)\right)
$$

with probability at least

$$
1-2 \exp \left(-N \delta^{2} e^{-\delta}|1-\sigma|^{2} / 2\right)-2 \exp \left(-2 \epsilon^{2}|1-\sigma|^{2} \sigma^{2} N\right)-Q
$$

where $Q$ has the asymptotic upper bound

$$
2 \exp \left\{-c \min \left[\frac{e^{2} t^{2}}{16} \frac{|I|^{2}}{N}\left(\ln \sigma^{-1}\right)^{2}, \frac{e t}{4}|I| \ln \sigma^{-1}\right]\right\}, \quad \sigma:=\frac{|I|}{N} \ll 1
$$

The proof of Proposition 3.2 is given in the next section.

Now we turn to the proof of Theorem 2.1.
Without loss of the generality we may assume $\left\|x_{0}\right\|=1$. Otherwise, we replace $x_{0}, x_{\text {null }}$ by $x_{0} /\left\|x_{0}\right\|$ and $x_{\text {null }} /\left\|x_{0}\right\|$, respectively. Let $Q=\left[\begin{array}{llll}Q_{1} & Q_{2} & \cdots & Q_{n}\end{array}\right]$ be a unitary transformation where $Q_{1}=x_{0}$ or equivalently $x_{0}=Q e_{1}$ where $e_{1}$ is the canonical vector with 1 as the first entry and zero elsewhere. Since unitary transformations do not affect the covariance structure of Gaussian random vectors, the matrix $A^{*} Q$ is an i.i.d. complex standard Gaussian matrix.
Proposition 3.3. Let $I$ be any set such that $b(i) \leq b(j)$ for all $i \in I$ and $j \in I_{\mathrm{c}}=$ $\{1,2, \ldots, N\} \backslash I$. For any unitary matrix $Q$, let $A^{\prime} \in \mathbb{C}^{|I| \times(n-1)}$ be the sub-column matrix of $A_{I}^{*} Q$ with its first column vector deleted. Then $A^{\prime}$ is an i.i.d. complex standard Gaussian random matrix.

Proof. First note that $A_{I}^{*} Q=\left(A^{*} Q\right)_{I}$, the row submatrix of $A^{*} Q$ indexed by $I$. As noted already, $A^{*} Q$ is an i.i.d. complex Gaussian matrix.

Since $x_{0}=Q e_{1}$ and $b=\left|A^{*} Q e_{1}\right|, I$ and $I_{c}$ are entirely determined by the first column of $A^{*} Q$ which is independent of the other columns of $A^{*} Q$. Consequently, the probability law of $A^{\prime}$ conditioned on the choice of $I$ equals the probability law of $A^{\prime}$ for a fixed $I$. Therefore, $A^{\prime}$ is an i.i.d. complex standard Gaussian matrix.

Let $\left\{\nu_{i}\right\}_{i=1}^{n-1}$ be the singular values of $A^{\prime}$ in the ascending order. For ant $z \in \mathrm{C}^{n-1}$,

$$
B^{\prime}:=A^{\prime} \operatorname{diag}(z /|z|)
$$

has the same set of singular values as $A^{\prime}$. Again, we adopt the convention that $z(j) /|z(j)|=1$ when $z(j)=0$. We have

$$
\left\|A^{\prime} z\right\|=\left\|B^{\prime}|z|\right\|
$$

and hence

$$
\left\|A^{\prime} z\right\|=\left(\left\|\Re\left(B^{\prime}\right)|z|\right\|^{2}+\left\|\Im\left(B^{\prime}\right)|z|\right\|^{2}\right)^{1 / 2} \geq \sqrt{2}\left(\left\|\Re\left(B^{\prime}\right)|z|\right\| \wedge\left\|\Im\left(B^{\prime}\right)|z|\right\|\right)
$$

By the theory of Wishart matrices [5], the singular values $\left\{\nu_{j}^{R}\right\}_{j=1}^{n-1},\left\{\nu_{j}^{I}\right\}_{j=1}^{n-1}$ (in the ascending order) of $\Re\left(B^{\prime}\right), \Im\left(B^{\prime}\right)$ satisfy the probability bounds that for every $t>0$ and $j=1, \cdots, n-$ 1

$$
\begin{align*}
& \mathrm{P}\left(\sqrt{|I|}-(1+t) \sqrt{n} \leq \nu_{j}^{R} \leq \sqrt{|I|}+(1+t) \sqrt{n}\right) \geq 1-2 e^{-n t^{2} / 2}  \tag{13}\\
& \mathrm{P}\left(\sqrt{|I|}-(1+t) \sqrt{n} \leq \nu_{j}^{I} \leq \sqrt{|I|}+(1+t) \sqrt{n}\right) \geq 1-2 e^{-n t^{2} / 2} \tag{14}
\end{align*}
$$

By Proposition 3.1 and (13)-(14), we have

$$
\begin{aligned}
\left\|x_{0} x_{0}^{*}-x_{\text {null }} x_{\text {null }}^{*}\right\| & \leq \frac{\sqrt{2}\left\|b_{I}\right\|}{\left\|\Re\left(B^{\prime}\right)|y|\right\| \wedge\left\|\Im\left(B^{\prime}\right)|y|\right\|} \\
& \leq \sqrt{2}\left\|b_{I}\right\|\left(\nu_{n-1}^{R} \wedge \nu_{n-1}^{I}\right)^{-1} \\
& \leq \sqrt{2}\left\|b_{I}\right\|(\sqrt{|I|}-(1+t) \sqrt{n})^{-1}
\end{aligned}
$$

By Proposition 3.2, we obtain the desired bound (3). The success probability is at least the expression (13) minus $4 e^{-n t^{2} / 2}$ which equals the expression (4).

### 3.1 Proof of Proposition 3.2

By the Gaussian assumption, $b(i)^{2}=\left|a_{i}^{*} x_{0}\right|^{2}$ has a chi-squared distribution with the probability density $e^{-z / 2} / 2$ on $z \in[0, \infty)$ and the cumulative distribution

$$
F(\tau):=\int_{0}^{\tau} 2^{-1} \exp (-z / 2) d z=1-\exp (-\tau / 2)
$$

Let

$$
\begin{equation*}
\tau_{*}=-2 \ln (1-|I| / N) \tag{15}
\end{equation*}
$$

for which $F\left(\tau_{*}\right)=|I| / N$.
Define

$$
\hat{I}:=\left\{i: b(i)^{2} \leq \tau_{*}\right\}=\left\{i: F\left(b^{2}(i)\right) \leq|I| / N\right\},
$$

and

$$
\|\hat{b}\|^{2}:=\sum_{i \in \hat{I}} b(i)^{2} .
$$

Let

$$
\left\{\tau_{1} \leq \tau_{2} \leq \ldots \leq \tau_{N}\right\}
$$

be the sorted sequence of $\left\{b(1)^{2}, \ldots, b(N)^{2}\right\}$ in magnitude.
Proposition 3.4. (i) For any $\delta>0$, we have

$$
\begin{equation*}
\tau_{|I|} \leq \tau_{*}+\delta \tag{16}
\end{equation*}
$$

with probability at least

$$
\begin{equation*}
1-\exp \left(-\frac{N}{2} \delta^{2} e^{-\delta}|1-|I| / N|^{2}\right) \tag{17}
\end{equation*}
$$

(ii) For each $\epsilon>0$, we have

$$
\begin{equation*}
|\hat{I}| \geq|I|(1-\epsilon) \tag{18}
\end{equation*}
$$

or equivalently,

$$
\begin{equation*}
\tau_{\lfloor|I|(1-\epsilon)\rfloor} \leq \tau_{*} \tag{19}
\end{equation*}
$$

with probability at least

$$
\begin{equation*}
1-2 \exp \left(-4 \epsilon^{2}|1-|I| / N|^{2}|I|^{2} / N\right) \tag{20}
\end{equation*}
$$

Proof. (i) Since $F^{\prime}(\tau)=\exp (-\tau / 2) / 2$,

$$
\begin{equation*}
|F(\tau+\epsilon)-F(\tau)| \geq \epsilon / 2 \exp (-(\tau+\epsilon) / 2) \tag{21}
\end{equation*}
$$

For $\delta>0$, let

$$
\zeta:=F\left(\tau_{*}+\delta\right)-F\left(\tau_{*}\right)
$$

which by (21) satisfies

$$
\begin{equation*}
\zeta \geq \frac{\delta}{2} \exp \left(-\frac{1}{2}\left(\tau_{*}+\delta\right)\right) \tag{22}
\end{equation*}
$$

Let $\left\{w_{i}: i=1, \ldots, N\right\}$ be the i.i.d. indicator random variables

$$
w_{i}=\chi_{\left\{b(i)^{2}>\tau_{*}+\delta\right\}}
$$

whose expectation is given by

$$
\mathrm{E}\left[w_{i}\right]=1-F\left(\tau_{*}+\delta\right) .
$$

The Hoeffding inequality yields

$$
\begin{align*}
\mathrm{P}\left(\tau_{|I|}>\tau_{*}+\delta\right) & =\mathrm{P}\left(\sum_{i=1}^{N} w_{i}>N-|I|\right)  \tag{23}\\
& =\mathrm{P}\left(N^{-1} \sum_{i=1}^{N} w_{i}-\mathrm{E}\left[w_{i}\right]>1-|I| / N-\mathrm{E}\left[w_{i}\right]\right) \\
& =\mathrm{P}\left(N^{-1} \sum_{i=1}^{N} w_{i}-\mathrm{E}\left[w_{i}\right]>\zeta\right) \\
& \leq \exp \left(-2 N \zeta^{2}\right)
\end{align*}
$$

Hence, for any fixed $\delta>0$,

$$
\begin{equation*}
\tau_{|I|} \leq \tau_{*}+\delta \tag{24}
\end{equation*}
$$

holds with probability at least

$$
\begin{aligned}
1-\exp \left(-2 N \zeta^{2}\right) & \geq 1-\exp \left(-\frac{N \delta^{2}}{2} e^{-\tau_{*}-\delta}\right) \\
& =1-\exp \left(-\frac{N \delta^{2}}{2} e^{-\delta}|1-|I| / N|^{2}\right)
\end{aligned}
$$

by (221).
(ii) Consider the following replacement
(a) $|I| \longrightarrow\lceil|I|(1-\epsilon)\rceil$
(b) $\tau_{*} \longrightarrow F^{-1}(\lceil|I|(1-\epsilon)\rceil / N)$
(c) $\delta \longrightarrow F^{-1}(|I| / N)-F^{-1}(\lceil|I|(1-\epsilon)\rceil / N)$
(d) $\zeta \longrightarrow F^{-1}\left(\tau_{*}+\delta\right)-F^{-1}\left(\tau_{*}\right)=|I| / N-\lceil|I|(1-\epsilon)\rceil / N=\frac{\lfloor|I| \epsilon\rfloor}{N}$
in the preceding argument. Then (23) becomes

$$
\mathrm{P}\left(\tau_{\lceil|I|(1-\epsilon)\rceil}>F^{-1}(|I| / N)\right) \leq \exp \left(-2 N \zeta^{2}\right)=\exp \left(-\frac{2\lfloor|I| \epsilon\rfloor^{2}}{N}\right)
$$

That is,

$$
\tau_{\lceil|I|(1-\epsilon)\rceil} \leq \tau_{*}
$$

holds with probability at least

$$
1-\exp \left(-2\lfloor|I| \epsilon\rfloor^{2} / N\right)
$$

Proposition 3.5. For each $\epsilon>0$ and $\delta>0$,

$$
\begin{equation*}
\frac{\left\|b_{I}\right\|^{2}}{|I|} \leq \frac{\|\hat{b}\|^{2}}{|\hat{I}|}+\epsilon\left(\tau_{*}+\delta\right) \tag{25}
\end{equation*}
$$

with probability at least

$$
\begin{equation*}
1-2 \exp \left(-\frac{1}{2} \delta^{2} e^{-\delta}|1-|I| / N|^{2} N\right)-2 \exp \left(-2 \epsilon^{2}|1-|I| / N|^{2} \frac{|I|^{2}}{N}\right) . \tag{26}
\end{equation*}
$$

Proof. Since $\left\{\tau_{j}\right\}$ is an increasing sequence, the function $T(m)=m^{-1} \sum_{i=1}^{m} \tau_{i}$ is also increasing. Consider the two alternatives either $|I| \geq|\hat{I}|$ or $|\hat{I}| \geq|I|$. For the latter,

$$
\left\|b_{I}\right\|^{2} /|I| \leq\|\hat{b}\|^{2} /|\hat{I}|
$$

due to the monotonicity of $T$.
For the former case $|I| \geq|\hat{I}|$, we have

$$
\begin{aligned}
T(|I|) & =|I|^{-1} \sum_{i=1}^{|\hat{I}|} \tau_{i}+|I|^{-1} \sum_{i=|\hat{\mid}|+1}^{|I|} \tau_{i} \\
& \leq T(|\hat{I}|)+|I|^{-1}(|I|-|\hat{I}|) \tau_{|I|} .
\end{aligned}
$$

By Proposition 3.4 (ii) $|\hat{I}| \geq(1-\epsilon)|I|$ and hence

$$
T(|I|) \leq T(|\hat{I}|)+|I|^{-1}(|I|-|I|(1-\epsilon)) \tau_{|I|}=T(|\hat{I}|)+\epsilon \tau_{|I|}
$$

with probability at least given by (20).
By Proposition $3.4(\mathrm{i}), \tau_{|I|} \leq \tau_{*}+\delta$ with probability at least given by (17).
Continuing the proof of Proposition 3.2, let us consider the i.i.d. centered, bounded random variables

$$
\begin{equation*}
Z_{i}:=\frac{N^{2}}{|I|^{2}}\left[b(i)^{2} \chi_{\tau_{*}}-\mathrm{E}\left[b(i)^{2} \chi_{\tau_{*}}\right]\right] \tag{27}
\end{equation*}
$$

where $\chi_{\tau_{*}}$ is the characteristic function of the set $\left\{b(i)^{2} \leq \tau_{*}\right\}$. Note that

$$
\begin{equation*}
\mathrm{E}\left(b(j)^{2} \chi_{\tau_{*}}\right)=\int_{0}^{\tau_{*}} 2^{-1} z \exp (-z / 2) d z=2-\left(\tau_{*}+2\right) \exp \left(-\tau_{*} / 2\right) \leq 2|I|^{2} / N^{2} \tag{28}
\end{equation*}
$$

and hence

$$
\begin{equation*}
-2 \leq Z_{i} \leq \sup \left\{\frac{N^{2}}{|I|^{2}} b(i)^{2} \chi_{\tau_{*}}\right\}=\frac{N^{2}}{|I|^{2}} \tau_{*} \tag{29}
\end{equation*}
$$

Next recall the Bernstein-inequality.
Proposition 3.6. [9] Let $Z_{1}, \ldots, Z_{N}$ be i.i.d. centered sub-exponential random variables. Then for every $t \geq 0$, we have

$$
\begin{equation*}
\mathrm{P}\left\{N^{-1}\left|\sum_{i=1}^{N} Z_{i}\right| \geq t\right\} \leq 2 \exp \left\{-c \min \left(N t^{2} / K^{2}, N t / K\right)\right\} \tag{30}
\end{equation*}
$$

where $c$ is an absolute constant and

$$
K=\sup _{p \geq 1} p^{-1}\left(\mathrm{E}\left|Z_{j}\right|^{p}\right)^{1 / p}
$$

Remark 3.7. For $K$ we have the following estimates

$$
\begin{align*}
K & \leq \frac{2 N^{2}}{|I|^{2}} \sup _{p \geq 1} p^{-1}\left(\mathrm{E}\left|b(i)^{2} \chi_{\tau_{*}}\right|^{p}\right)^{1 / p}  \tag{31}\\
& \leq \frac{2 N^{2}}{|I|^{2}} \tau_{*} \sup _{p \geq 1} p^{-1}\left(\mathrm{E} \chi_{\tau_{*}}\right)^{1 / p} \\
& \leq \frac{2 N^{2}}{|I|^{2}} \tau_{*} \sup _{p \geq 1} p^{-1}\left(1-e^{-\tau_{*} / 2}\right)^{1 / p}
\end{align*}
$$

The maximum of the right hand side of (31) occurs at

$$
p_{*}=-\ln \left(1-e^{-\tau_{*} / 2}\right)
$$

and hence

$$
K \leq \frac{2 N^{2}}{|I|^{2}} \frac{\tau_{*}}{p_{*}}\left(1-e^{-\tau_{*} / 2}\right)^{1 / p_{*}}
$$

We are interested in the regime

$$
\tau_{*} \asymp 2|I| / N \ll 1
$$

which implies

$$
p_{*} \asymp-\ln \frac{\tau_{*}}{2} \asymp \ln \frac{N}{|I|}
$$

and consequently

$$
\begin{equation*}
K \leq \frac{4 N}{e|I|}\left(\ln \frac{N}{|I|}\right)^{-1}, \quad \sigma=|I| / N \ll 1 \tag{32}
\end{equation*}
$$

On the other hand, upon substituting the asymptotic bound (32) in the probability bound

$$
Q=2 \exp \left\{-c \min \left(N t^{2} / K^{2}, N t / K\right)\right\}
$$

of (30), we have

$$
K \leq 2 \exp \left\{-c \min \left[\frac{e^{2} t^{2}}{16}\left(\ln \sigma^{-1}\right)^{2}|I|^{2} / N, \frac{e t}{4}|I| \ln \sigma^{-1}\right]\right\}, \quad \sigma \ll 1
$$

The Bernstein inequality ensures that with high probability

$$
\left|\frac{\|\hat{b}\|^{2}}{N}-\mathrm{E}\left(b^{2}(i) \chi_{\tau_{*}}\right)\right| \leq t \frac{|I|^{2}}{N^{2}} .
$$

By (18) and (28), we also have

$$
\begin{align*}
\frac{\|\hat{b}\|^{2}}{|\hat{I}|} & \leq \mathrm{E}\left(b(i)^{2} \chi_{\tau_{*}}\right) \frac{N}{|\hat{I}|}+t \frac{|I|^{2}}{|\hat{I}| N}  \tag{33}\\
& \leq\left(\mathrm{E}\left(b(i)^{2} \chi_{\tau_{*}}\right) \frac{N^{2}}{|I|^{2}}+t\right) \frac{|I|}{N} \\
& \leq \frac{2+t}{1-\epsilon} \cdot \frac{|I|}{N}
\end{align*}
$$

By Prop. 3.5, we now have

$$
\left\|b_{I}\right\|^{2} \leq|I|\left(\frac{\|\hat{b}\|^{2}}{|\hat{I}|}+\epsilon\left(\tau_{*}+\delta\right)\right)
$$

with probability at least given by (4), which together with (33) and (15) complete the proof of Proposition 3.2.

Acknowledgements. Research of P. Chen is supported in part by the grant 103-2115-M-005-006-MY2 from Ministry of Science and Technology, Taiwan, and US NIH grant U01-HL114494. Research of A. Fannjiang is supported in part by US National Science Foundation grant DMS-1413373 and Simons Foundation grant 275037.

## References

[1] E.J. Candès and Y. Chen, " Solving random quadratic systems of equations is nearly as easy as solving linear systems." arXiv:1505.05114, 2015.
[2] E.J. Candes, X. Li and M. Soltanolkotabi, "Phase retrieval via Wirtinger flow: theory and algorithms," IEEE Trans Inform. Th. 61(4), 1985-2007 (2015).
[3] P. Chen and A. Fannjiang, "Phase retrieval with a single mask by the Douglas-Rachford algorithm," Appl. Comput. Harmon. Anal., in press. arXiv:1509.00888.
[4] P. Chen, A. Fannjiang and G.-R. Liu, "Phase retrieval with one or two coded diffraction patterns by alternating projection with the null initialization," arxiv:1510.07379.
[5] K.R. Davidson and S.J. Szarek. "Local operator theory, random matrices and Banach spaces," in Handbook of the geometry of Banach spaces, Vol. I, pp. 317-366. Amsterdam: North-Holland, 2001.
[6] S. Marchesini, " A unified evaluation of iterative projection algorithms for phase retrieval," Rev. Sci. Instr. 78, 011301 (2007).
[7] P. Netrapalli, P. Jain, S. Sanghavi, "Phase retrieval using alternating minimization," IEEE Trans. Signal Proc. 63 (2015), pp. 4814-4826.
[8] Y. Shechtman, Y.C. Eldar, O. Cohen, H.N. Chapman, M. Jianwei and M. Segev, "Phase retrieval with application to optical imaging: A contemporary overview," IEEE Mag. Signal Proc. 32(3) (2015), 87-109.
[9] R. Vershynin. "Introduction to the non-asymptotic analysis of random matrices." arXiv preprint arXiv:1011.3027.


[^0]:    *Department of Applied Mathematics, National Chung Hsing University, Taichung 402, Taiwan.
    ${ }^{\dagger}$ Department of Mathematics, University of California, Davis, CA 95616, USA. fannjiang@math.ucdavis.edu.
    ${ }^{\ddagger}$ Department of Mathematics, University of California, Davis, CA 95616, USA

