ABSOLUTE UNIQUENESS OF PHASE RETRIEVAL WITH RANDOM ILLUMINATION

ALBERT FANNJIANG

ABSTRACT. Random phase or amplitude illumination is proposed to remove at once all types of ambiguity, trivial or nontrivial, at once from phase retrieval and enforce absolute uniqueness. Almost sure irreducibility is proved for *any* complex-valued object of sufficiently high sparsity or of convex support whose dimensional is greater than one. While the new irreducibility result can be viewed as a probabilistic version of the classical result by Bruck, Sodin and Hayes, it provides a novel perspective and an effective method for phase retrieval. In particular, almost sure uniqueness, up to a global phase, is proved for complex-valued objects under general two-point conditions. Under a tight sector constraint absolute uniqueness is proved to hold with probability exponentially close to unity as the object sparsity increases. Under a magnitude constraint with random amplitude illumination, uniqueness modulo global phase is proved to hold with probability exponentially close to unity as object sparsity increases. For general complex-valued objects without any constraint, almost sure uniqueness up to global phase is established for the Fourier magnitude measurement with *two* independent illuminations. Numerical examples show that phasing with random illumination drastically reduces the number of data, iterations and the error in reconstruction.

1. INTRODUCTION

Phase retrieval is a fundamental problem in many areas of physical sciences such as X-ray crystallography, astronomy, electron microscopy, coherent light microscopy, quantum state tomography and remote sensing. Because of loss of the phase information a central question of phase retrieval is the uniqueness of solution which is the focus of the present work.

Researchers in phase retrieval, however, have long settled with the notion of *relative uniqueness* (i.e. irreducibility) for *almost all* objects, without a practical means for deciding the reducibility of the underlying object, and searched for various ad hoc strategies to circumvent problems with stagnation and error in reconstruction. The stagnation problem may be due to the possibility of the iterative process to approach the object and its twin or shifted image, the support not tight enough or the boundary not sharp enough [11, 12, 16]. Besides the uniqueness issue, phase retrieval is also inherently nonconvex and consequently many have believed the lack of convexity in the Fourier magnitude constraint to be a main, if not the dominant, source of numerical problems with the standard phasing algorithms [3, 17, 25]. While there have been dazzling advances in applications of phase retrieval in the past decades [18], we still do not know just how much of the error and stagnation problems is attributable to to the lack of uniqueness or convexity.

We propose here to refocus on the issue of uniqueness as uniqueness is undoubtedly the first foundational issue of any inverse problem, including phase retrieval. Specifically we

The research is partially supported by the NSF grant DMS - 0908535.

(a) (b)

FIGURE 1. Illumination of a transparent object (the blue oval) with a deterministic (a) or random field λ created by a diffuser (b) followed by an intensity measurement of the diffraction pattern. In the case of wave front reconstruction, the random modulator is placed at the exit pupil instead of the entrance pupil as in (b).

will first establish uniqueness in the absolute sense with random illumination under general, physically reasonable constraints (Figure 1) and secondly demonstrate that even though the convexity issue remains unresolved, phasing with random illumination can drastically improve the quality of reconstruction and reduce the numbers of Fourier magnitude data and numerical iterations.

To fix the idea, consider the discrete version of the phase retrieval problem: Let $\mathbf{n} = (n_1, \cdots, n_d) \in \mathbb{Z}^d$ and $\mathbf{z} = (z_1, \cdots, z_d) \in \mathbb{C}^d$. Define the multi-index notation $\mathbf{z}^{\mathbf{n}} = z_1^{n_1} z_2^{n_2} \cdots z_d^{n_d}$. Let $f(\mathbf{n})$ be a finite complex-valued function defined on $\mathbb{Z}^d$ vanishing outside the finite lattice

$$\mathcal{N} = \left\{ \mathbf{0} \leq \mathbf{n} \leq \mathbf{N} \right\}$$

for $\mathbf{N} = (N_1, \cdots, N_d) \in \mathbb{N}^d$. We use the notation $\mathbf{m} \leq \mathbf{n}$ for $m_j \leq n_j, \forall j$. The z-transform of a finite sequence $f(\mathbf{n})$ is given by

$$F(\mathbf{z}) = \sum_{\mathbf{n}} f(\mathbf{n}) \mathbf{z}^{-\mathbf{n}}.$$

The Fourier transform can be obtained from the z-transform as

$$F(\mathbf{w}) = F(e^{\mathrm{i}2\pi w_1}, \cdots, e^{\mathrm{i}2\pi w_d}) = \sum_{\mathbf{n}} f(\mathbf{n}) e^{-\mathrm{i}2\pi \mathbf{n}\cdot\mathbf{w}}, \quad \mathbf{w} = (w_1, \cdots, w_d) \in [0,1]^d$$

by some abuse of notation. The discrete phase retrieval problem is to determine $f(\mathbf{n})$ from the knowledge of the Fourier magnitude $|F(\mathbf{w})|, \forall \mathbf{w} \in [0,1]^d$.

The question of uniqueness was partially answered in [4, 14, 15] which says that in dimension two or higher and with the exception of a measure zero set of finite sequences phase retrieval has a unique solution up to the equivalence class of "trivial associates" (i.e. relative uniqueness). These trivial, but omnipresent, ambiguities include constant global phase,

$$f(\mathbf{n}) \longrightarrow e^{\mathrm{i}\theta} f(\mathbf{n}), \quad \text{for some } \theta \in [0, 2\pi],$$

spatial translation

$$f(\mathbf{n}) \longrightarrow f(\mathbf{n} \oplus \mathbf{m}), \quad \text{for some } \mathbf{m} \in \mathbb{Z}^d,$$

where $\mathbf{n} \oplus \mathbf{m} = \mathbf{n} + \mathbf{m}(mod(N_1 + 1, \cdots, N_d + 1))$, and conjugate inversion

$$f(\mathbf{n}) \longrightarrow f^*(\mathbf{N} - \mathbf{n}).$$

Conjugate inversion produces the so-called twin image.

This landmark uniqueness result, however, has two caveats. First, many sequences with hidden symmetries belong to this unknown set of ambiguous sequences which challenges the validity of the widely held assumption that relative uniqueness holds true in most of the practical problems. Furthermore, there is no way of knowing *a priori* whether the underlying object is uniquely determined even in the relative sense from the Fourier magnitude measurement. Secondly, although the trivial associates share the same object information, they nevertheless can seriously stagnate and impede the iterative reconstruction process [11, 12, 20, 25].

In this paper, we study the notation of *absolute uniqueness*: if two finite objects f and g give rise to the same Fourier magnitude data, then $f = g$ unequivocally. More importantly, we present the approach of random (phase or amplitude) illumination to the absolute uniqueness of phase retrieval. The idea of random illumination is related to coded-aperture imaging whose utility in other imaging contexts than phase retrieval has been established experimentally [1, 13, 26, 27, 28] as well as mathematically [7, 23].

Our basic tool is a probabilistic version (Theorem 2 and 3) of the irreducibility result of [14, 15] with, however, a different perspective and important practical implications. The advantage of our probabilistic approach lies in that the measure is endowed in the ensemble of random illumination, thus avoiding the ambiguity with the measure zero set of exceptional objects.

On the basis of almost sure irreducibility, the mere assumption that the phases or magnitudes of the object at two arbitrary points lie in a countable set enforces uniqueness, up to a global phase, in phase retrieval with a single random illumination (Theorem 4). The absolute uniqueness can be enforced then by imposing the positivity constraint (Corollary 1). For objects satisfying a tight sector condition, absolute uniqueness is valid with high probability depending on the object sparsity for either phase or amplitude illumination (Theorem 5). For complex-valued objects under a magnitude constraint, uniqueness up to a global phase is valid with high probability (Theorem 6). For general complex-valued objects, almost sure uniqueness, up to global phase, is proved for phasing with two independent illuminations (Theorem 7).

The paper is organized as follows. In Section 2 we discuss various sources of ambiguity. In Section 3 we prove the almost sure irreducibility (Theorem 2 and 3). In Section 4 we derive the uniqueness results (Theorem 4, 5, 6, 7 and Corollary 1). We demonstrate numerical phasing with random illumination in Section 5. We conclude in Section 6.

2. Sources of ambiguity

As commented before the phase retrieval problem does not have a unique solution. Nevertheless, the possible solutions are constrained as stated in the following theorem [14, 22].

Theorem 1. *Let the z-transform $F(\mathbf{z})$ of a finite complex-valued sequence $\{f(\mathbf{n})\}$ be given by*

$$F(\mathbf{z}) = \alpha \mathbf{z}^{-\mathbf{m}} \prod_{k=1}^{p} F_k(\mathbf{z}), \quad \mathbf{m} \in \mathbb{N}^d, \alpha \in \mathbb{C} \tag{1}$$

where $F_k, k = 1, ..., p$ are nontrivial irreducible polynomials. Let $G(\mathbf{z})$ be the $\mathbf{z}$*-transform of another finite sequence $g(\mathbf{n})$. Suppose $|F(\mathbf{w})| = |G(\mathbf{w})|, \forall \mathbf{w} \in [0,1]^d$. Then $G(\mathbf{z})$ must have the form*

$$G(\mathbf{z}) = |\alpha| e^{\mathrm{i}\theta} \mathbf{z}^{-\mathbf{p}} \left(\prod_{k \in I} F_k(\mathbf{z}) \right) \left(\prod_{k \in I^c} F_k^*(1/\mathbf{z}^*) \right), \quad \mathbf{p} \in \mathbb{N}^d, \theta \in \mathbb{R}$$

where I is a subset of $\{1, 2, ..., p\}$.

To prove the theorem, it is convenient to write

$$\begin{aligned} |F(\mathbf{w})|^2 &= \sum_{\mathbf{n}=-\mathbf{N}}^{\mathbf{N}} \sum_{\mathbf{m}+\mathbf{n} \in \mathcal{N}} f(\mathbf{m}+\mathbf{n}) f^*(\mathbf{m}) e^{-\mathrm{i}2\pi \mathbf{n}\cdot\mathbf{w}} \\ &= \sum_{\mathbf{n}=-\mathbf{N}}^{\mathbf{N}} \mathcal{C}_f(\mathbf{n}) e^{-\mathrm{i}2\pi \mathbf{n}\cdot\mathbf{w}} \end{aligned} \tag{2}$$

where

$$\mathcal{C}_f(\mathbf{n}) = \sum_{\mathbf{m} \in \mathcal{N}} f(\mathbf{m}+\mathbf{n}) f^*(\mathbf{m}) \tag{3}$$

is the autocorrelation function of f. Note the symmetry $\mathcal{C}_f^*(\mathbf{n}) = \mathcal{C}_f(-\mathbf{n})$.

The theorem then follows straightforwardly from the equality between the autocorrelation functions of f and g, because $F(\mathbf{w})F^*(\mathbf{w}) = G(\mathbf{w})G^*(\mathbf{w})$, and the unique factorization of polynomials (see [22] for more details).

Remark 1. *If the finite array $f(\mathbf{n})$ is known* a priori *to vanish outside the lattice $\mathcal{N}$, then by Shannon's sampling theorem for band-limited functions the sampling domain for* $\mathbf{w}$ *can be limited to the finite regular grid*

$$\mathcal{M} = \left\{ (k_1, \cdots, k_d) : \forall j = 1, \cdots, d \ \&\ k_j = 0, \frac{1}{2N_j+1}, \frac{2}{2N_j+1}, \cdots, \frac{2N_j}{2N_j+1}. \right\} \tag{4}$$

since $|F(\mathbf{w})|^2$ is band-limited to the set $-\mathbf{N} \le \mathbf{n} \le \mathbf{N}$.

There are three sources of ambiguity. First, the linear phase term $\mathbf{z}^{-\mathbf{m}}$ in (1) remain undetermined because the autocorrelation operation destroys information about spatial shift. The unspecified constant phase θ is another source of ambiguity.

To understand the physical meaning of the operation

$$F(\mathbf{z}) \longrightarrow \mathbf{z}^{-\mathbf{N}} F^*(1/\mathbf{z}^*)$$

consider the case $d = 1$

$$z^{-N} F^*(1/z^*) = f^*(0) z^{-N} + f^*(1) z^{1-N} + \cdots + f^*(N)$$

which is the z-transform of the conjugate space-inversed array $\{f^*(N), f^*(N-1), \cdots, f^*(0)\}$. The same is true in multi-dimensions.

The subtlest form of ambiguity is caused by *partial* conjugate inversion on some, but not all, factors of a factorable object, with reducible z-transform, without which the conjugate inversion, like spatial shift and global phase, is global in nature and considered "trivial" in the literature (even though the twin image may have an opposite orientation). In numerical reconstruction, the trivial ambiguities have to be eliminated by assuming favorable *a priori* knowledge such as support constraints and positivity.

In this paper, we consider both types, trivial and nontrivial, of ambiguity, as they both can degrade the performance of phasing schemes. Our main purpose is to show by rigorous analysis that with random illumination it is possible to eliminate all ambiguities at once.

3. Irreducibility

Nearly independent random illumination can be produced by a diffuser placed near the object [1, 13], cf. Figure 1. Random illumination amounts to replacing the original object $f(\mathbf{n})$ by

$$\tilde{f}(\mathbf{n}) = f(\mathbf{n})\lambda(\mathbf{n}) \tag{5}$$

where $\lambda(\mathbf{n})$, representing the incident field, is a *known* array of samples of random variables. The idea is to first modify the object by the encoding array $\lambda(\mathbf{n})$ so that phase retrieval has unique solution and then use the knowledge of λ to recover f.

Let $\lambda(\mathbf{n})$ be *continuous* random variables with respect to the Lebesgue measure on $\mathbb{S}^1$ (the unit circle), $\mathbb{R}$ or $\mathbb{C}$. The case of $\mathbb{S}^1$ can be facilitated by a random phase modulator (phase diffuser) with

$$\lambda(\mathbf{n}) = e^{\mathrm{i}\phi(\mathbf{n})} \tag{6}$$

where $\phi(\mathbf{n})$ are continuous random variables on $[0, 2\pi]$ while the case of $\mathbb{R}$ can be facilitated by a random amplitude modulator. The case of $\mathbb{C}$ involves simultaneously both phase and amplitude modulations.

For simplicity of notation, we shall consider the case of $d = 2$ for the following result. The argument can be extended to higher dimensions with more complicated lower bound for the sparsity.

Theorem 2. *Let $N_1, N_2 \geq 1$. Let $\{f(\mathbf{n})\}$ be a finite complex-valued array of sparsity*

$$S > |\mathcal{N}| - \min\{N_1, N_2\}. \tag{7}$$

Let $\{\lambda(\mathbf{n})\}$ be continuous random variables on $\mathbb{S}^1, \mathbb{R}$ or $\mathbb{C}$ with an absolutely continuous *joint distribution with respect to the product measure. Then, up to a power of $\mathbf{z}$, the z-transform of $\tilde{f}(\mathbf{n}) = f(\mathbf{n})\lambda(\mathbf{n})$ is irreducible with probability one.*

Proof. The proof relies on counting of dimensions.

Suppose that $\{f(\mathbf{n})\}$ vanishes outside $\mathcal{N}$ and has exactly S nonzero elements. Then $\{\tilde{f}(\mathbf{n}) = f(\mathbf{n})\lambda(\mathbf{n})\}$ are continuous random variables on a manifold of S real (the case of $\mathbb{S}^1$ or $\mathbb{R}$) or complex (the case of $\mathbb{C}$) dimensions. Let $\widetilde{F}$ be the polynomial associated with the array $\tilde{f}$ and let $\mathbb{M}_{\widetilde{F}}$ be the manifold of the polynomials associated with the z-transforms of $\tilde{f}$. Clearly, $\mathbb{M}_{\widetilde{F}}$ has a dimension S.

Let $\mathbf{p} = (p_1, p_2) \in \mathbb{N}^2, \mathbf{q} = (q_1, q_2) \in \mathbb{N}^2$ be two integer-valued vectors with $p_1 + q_1 \leq N_1, p_2 + q_2 \leq N_2$. Let $g(\mathbf{n})$ and $h(\mathbf{n})$ be the finite arrays vanishing outside $\mathcal{N}$ and let their associated polynomials $G(\mathbf{z})$ and $H(\mathbf{z})$ have degrees $\mathbf{p}$ and $\mathbf{q}$, respectively, such that GH has a degree at most $\mathbf{N}$ and exactly S nonzero coefficients. Let $\mathbb{M}_{GH}$ be the submanifold in $\mathbb{C}^{2(N_1+1)(N_2+1)}$ of the product polynomials GH of degree at most $\mathbf{N}$ having exactly S nonzero coefficients where G and H have a degree $\mathbf{p}$ and $\mathbf{q}$ respectively.

The manifold $\mathbb{M}_{GH}$ is contained in the affine space $\mathbb{A}$ defined by the coordinate constraints

$$g(\mathbf{n}) = 0, \quad \mathbf{n} \notin \{\mathbf{0} \leq \mathbf{m} \leq \mathbf{p}\}, \quad \mathbf{0} \leq \mathbf{n} \leq \mathbf{N} \tag{8}$$

$$h(\mathbf{n}) = 0, \quad \mathbf{n} \notin \{\mathbf{0} \leq \mathbf{m} \leq \mathbf{q}\}, \quad \mathbf{0} \leq \mathbf{n} \leq \mathbf{N} \tag{9}$$

$$h(0,0) = \text{const.} \neq 0. \tag{10}$$

Equations (8) and (9) are due to the fact that $\deg(G) = \mathbf{p}$ and $\deg(H) = \mathbf{q}$. Equation (10) is to eliminate the redundant degree of freedom due to expressing a polynomial as product of two polynomials and can be substituted by $g(0,0) = \text{const.} \neq 0$.

The dimension of $\mathbb{A}$ is

$$(p_1 + 1)(p_2 + 1) + (q_1 + 1)(q_2 + 1) - 1 = |\mathcal{N}| - p_1 q_2 - p_2 q_1.$$

$p_1 q_2 - p_2 q_1$ is positive unless $p_1 = q_1 = 0$ or $p_2 = q_2 = 0$ or $\mathbf{p} = 0$ or $\mathbf{q} = 0$. The last two cases are ruled out by the factorability assumption. The first two cases correspond to 1-dimensional images with $\tilde{f} = \tilde{f}(n_2)$ or $\tilde{f}(n_1)$ which has zero probability because $\{\tilde{f}(\mathbf{n})\}$ has an absolutely continuous joint distribution with respect to the product measure.

Now if

$$\begin{aligned} S &> \max_{\substack{\mathbf{p}+\mathbf{q} \leq \mathbf{N} \\ \mathbf{p},\mathbf{q} \neq 0}} (p_1 + 1)(p_2 + 1) + (q_1 + 1)(q_2 + 1) - 1 \\ &= \max_{\substack{\mathbf{p}+\mathbf{q} = \mathbf{N} \\ \mathbf{p},\mathbf{q} \neq 0}} (p_1 + 1)(p_2 + 1) + (q_1 + 1)(q_2 + 1) - 1 \\ &= |\mathcal{N}| - \min_{\substack{\mathbf{p}+\mathbf{q} = \mathbf{N} \\ \mathbf{p},\mathbf{q} \neq 0}} (p_1 q_2 + p_2 q_1) \\ &= |\mathcal{N}| - \min\{N_1, N_2\} \end{aligned}$$

then $S = \dim(\mathbb{M}_{\tilde{F}}) > \dim(\mathbb{M}_{GH})$.

For a given array $\tilde{f}$ with exactly S nonzero elements, $\mathbb{M}_{\tilde{F}} \simeq (\mathbb{S}^1)^S, \mathbb{R}^S$ or $\mathbb{C}^S$ with a probability distribution absolutely continuous with respect to the Lebesgue measure on the respective space. Since the manifold of degree $\mathbf{N}$ reducible polynomials with exactly S nonzero coefficients has a dimension less than S, it has a probability measure zero. The proof is complete.

$\square$

This theorem has the same flavor as the results in [14, 15] which says that the set of the reducible polynomials has measure zero in the space of polynomials of two complex variables with real-valued coefficients. While the transition from real-valued to complex-valued coefficients is minor, it is of both theoretical and practical importance that Theorem 2 places the probability measure on the ensemble of random illumination, which we can control, instead of the space of finite objects, which we can not control.

The theorem, however, does not hold for low S. For example, let $p(\mathbf{z})$ be any monomial and consider

$$F(\mathbf{z}) = \sum_j c_j p^j(\mathbf{z}) \tag{11}$$

which is reducible for any $c_j \in \mathbb{C}$, except when F is a monomial, by the fundamental theorem of algebra (of one variable). Another example is the *homogeneous* polynomials of a sum degree $N \leq \min\{N_1, N_2\}$, i.e.

$$F(\mathbf{z}) = \sum_{i+j=N} c_{ij} z_1^i z_2^j \tag{12}$$

which is factorable by the fundamental theorem of algebra. The highest possible sparsity for both examples is $1 + \min\{N_1, N_2\}$.

Almost sure irreducibility can be extended in another direction to avoid the examples such as (11) and (12) by imposing convexity and full dimensionality on the object.

First let us define some notation and definitions. The support of a polynomial $F(\mathbf{z})$, denoted by $\mathrm{supp}(F)$, is the set of exponent vectors in $\mathbb{N}^d$ with nonzero coefficients. The Newton polytope of F, denoted by $\mathrm{Newt}(F)$, is the convex hull of its support in $\mathbb{R}^d$, denoted by $\mathrm{conv}(\mathrm{supp}(F))$.

Ostrowski's theorem [21] says that if $F(\mathbf{z}) = G(\mathbf{z})H(\mathbf{z})$ where G and H are two polynomials, then

$$\mathrm{Newt}(F) = \mathrm{Newt}(G) + \mathrm{Newt}(H)$$

where the right hand side is the Minkowski sum. The Minkowski sum of $\mathcal{A} \subseteq \mathbb{R}^d$ and $\mathcal{B} \subseteq \mathbb{R}^d$ is the set whose elements are the sums of the elements of the two sets:

$$\mathcal{A} + \mathcal{B} = \{\mathbf{a} + \mathbf{b} : \mathbf{a} \in \mathcal{A}, \mathbf{b} \in \mathcal{B}\}.$$

The dimension of a finite subset $\mathcal{A} \subseteq \mathbb{Z}^d$, denoted by $\dim(\mathcal{A})$, is the lowest dimension of the hyperspace containing $\mathcal{A}$ in $\mathbb{R}^d$. A finite subset $\mathcal{A} \subseteq \mathbb{Z}^d$ is said to be *convex* if

$$\mathcal{A} = \mathbb{Z}^d \cap \mathrm{conv}(\mathcal{A}).$$

The above examples (11) and (12) correspond to one-dimensional supports.

Recall the cardinality inequality for the Minkowski sum of two finite sets $\mathcal{A}, \mathcal{B}$ [24]

$$|\mathcal{A} + \mathcal{B}| \geq |\mathcal{A}| + |\mathcal{B}| - 1 \tag{13}$$

where the equality holds if and only if $\mathcal{A}$ and $\mathcal{B}$ are arithmetic progressions of the same difference vector, i.e. $\mathrm{conv}(\mathcal{A})$ and $\mathrm{conv}(\mathcal{B})$ are parallel line segments.

Theorem 3. *Let $\{f(\mathbf{n})\}$ be a finite complex-valued array whose support is convex and has dimension greater than one. Let $\{\lambda(\mathbf{n})\}$ be continuous random variables on $\mathbb{S}^1, \mathbb{R}$ or $\mathbb{C}$ with an* absolutely continuous *joint distribution with respect to the product measure. Then, up to a power of $\mathbf{z}$, the z-transform of $\tilde{f}(\mathbf{n}) = f(\mathbf{n})\lambda(\mathbf{n})$ is irreducible with probability one.*

Proof. We shall adopt the notation of Theorem 2 and its proof.

With probability one, $\mathrm{supp}(\widetilde{F}) = \mathrm{supp}(f)$ and $|\mathrm{supp}(\widetilde{F})|$ equals the dimension of $\mathbb{M}_{\widetilde{F}}$. On the other hand, the dimension of $\mathbb{M}_{GH}$ is at most

$$|\mathrm{supp}(G)| + |\mathrm{supp}(H)| - 1$$

where -1 is due to the normalization (10).

By Ostrowski's theorem,

$$\mathrm{Newt}(\widetilde{F}) = \mathrm{Newt}(G) + \mathrm{Newt}(H)$$

which is equivalent to

$$\mathbb{Z}^d \cap \mathrm{Newt}(\widetilde{F}) = (\mathbb{Z}^d \cap \mathrm{Newt}(G)) + (\mathbb{Z}^d \cap \mathrm{Newt}(H)).$$

Since the object support has dimension greater than one, $\mathrm{Newt}(\widetilde{F})$ has dimension greater than one and thus $\mathrm{Newt}(G)$ and $\mathrm{Newt}(H)$ can not be two parallel line segments. By the strict inequality of (13) we have

$$|\mathbb{Z}^d \cap \mathrm{Newt}(\widetilde{F})| \geq |\mathbb{Z}^d \cap \mathrm{Newt}(G)| + |\mathbb{Z}^d \cap \mathrm{Newt}(H)|$$

and therefore

$$|\mathrm{supp}(\widetilde{F})| = |\mathbb{Z}^d \cap \mathrm{Newt}(\widetilde{F})| > |\mathrm{supp}(G)| + |\mathrm{supp}(H)| - 1$$

i.e. the dimension of $\mathbb{M}_{\widetilde{F}}$ is strictly greater than that of $\mathbb{M}_{GH}$.

The desired conclusion follows from the rest of the argument in the proof of Theorem 1. □

4. Uniqueness

Without additional *a priori* knowledge on the object Theorem 2, however, does not preclude the trivial ambiguities such as global phase, spatial shift and conjugate inversion. For example, we can produce another finite array $\{g(\mathbf{n})\}$ vanishing outside $\mathbf{0} \leq \mathbf{n} \leq \mathbf{N}$ that would yield the same measurement data by setting

$$g(\mathbf{n}) \quad = \quad e^{\mathrm{i}\theta} f(\mathbf{n} \oplus \mathbf{m}) \lambda(\mathbf{n} \oplus \mathbf{m}) / \lambda(\mathbf{n}) \tag{14}$$

or

$$g(\mathbf{n}) \quad = \quad e^{\mathrm{i}\theta} f^*(\mathbf{N} - \mathbf{n} \oplus \mathbf{m}) \lambda^*(\mathbf{N} - \mathbf{n} \oplus \mathbf{m}) / \lambda(\mathbf{n}) \tag{15}$$

for $\theta \in [0, 2\pi]$ and $\mathbf{m} \in \mathbb{Z}^2$ where $\mathbf{n} \oplus \mathbf{m} = \mathbf{n} + \mathbf{m}$ $(\mathrm{mod}(N_1 + 1, N_2 + 1))$. Expression (14) and (15) consist the remaining ambiguities to be addressed.

4.1. **Two-point constraint.** One important exception is the case of *real-valued* objects when the illumination is complex-valued (the case of $\mathbb{S}^1$ or $\mathbb{C}$). In this case, on the one hand (14) produces a complex-valued array with probability one unless $\mathbf{m} = 0, \theta = 0, \pi$ and, on the other hand, (15) is complex-valued with probability one regardless of $\mathbf{m}$. In this case, none of the trivial ambiguities can arise. Indeed, a stronger result is true depending on the nature of random illumination.

Theorem 4. *Suppose either of the following cases holds:*

(i) The phases of the object $\{f(\mathbf{n})\}$ at two points, where f does not vanish, belong to a known countable subset of $[0, 2\pi]$, $\{\lambda(\mathbf{n})\}$ are independent continuous random variables on $\mathbb{S}^1$ or $\mathbb{C}$;

(ii) The amplitudes of the object $\{f(\mathbf{n})\}$ at two points, where f does not vanish, belong to a known measure zero subset of $\mathbb{R}$ and that $\{\lambda(\mathbf{n})\}$ are independent continuous random

variables on $\mathbb{R}$ or $\mathbb{C}$.

If the resulting z-transform is almost surely irreducible then, with probability one, f is determined uniquely, up to a global phase, by the Fourier magnitude measurement on the lattice $\mathcal{M}$.

Remark 2. *For the two-point constraint in case (i) to be convex, it is necessary for the constraint set to be a singleton, namely the phases of the object at two nonzero points must take on a single known value. On the other hand, the amplitude constraint in case (ii) can never be convex.*

Proof. We prove the theorem case by case.

Case (i): Suppose the phases of $f(\mathbf{n}_1)$ and $f(\mathbf{n}_2)$ belong to the coutable set $\Theta \subset [0, 2\pi]$. Let us show the probability that the phase of $g(\mathbf{n})$ as given by (14) with $\mathbf{m} \neq 0$ takes on a value in Θ for any point $\mathbf{n}$ is zero.

Since $\lambda(\mathbf{n}+\mathbf{m}), \mathbf{m} \neq 0$, and $\lambda(\mathbf{n})$ are independent and continuously distributed w.r.t. to the Lebesgue measure on $\mathbb{S}^1$ or $\mathbb{C}$, the phase of $g(\mathbf{n}), \forall \mathbf{n}$, is continuously distributed on $[0, 2\pi]$ for all θ.

Now suppose the phase of $g(\mathbf{n}_0)$ for some $\mathbf{n}_0$ lies in the set Θ. This implies that θ must belong to the countable set Θ' which is Θ shifted by the negative phase of $f(\mathbf{n}_0+\mathbf{m})\lambda(\mathbf{n}_0 \oplus \mathbf{m})/\lambda(\mathbf{n}_0)$. The phase of $g(\mathbf{n})$ at a different location $\mathbf{n} \neq \mathbf{n}_0$, however, almost surely does not take on any value in the set Θ for any fixed $\theta \in \Theta'$ unless $\mathbf{m} = 0$. Since a countable union of measure-zero sets has zero measure, the probability that the phases of g at two points lie in Θ is zero if $\mathbf{m} \neq 0$.

Likewise, $\lambda^*(\mathbf{N} - \mathbf{n} \oplus \mathbf{m})/\lambda(\mathbf{n}), \forall \mathbf{m}$, has a random phase that is continuously distributed on $[0, 2\pi]$ and by the same argument the probability that the phases of g as given by (15) at two points lie in Θ is zero.

Case (ii): Suppose the amplitudes of $f(\mathbf{n}_1)$ and $f(\mathbf{n}_2)$ belong to the measure zero set $\mathcal{A}$. Since $\lambda(\mathbf{n}+\mathbf{m}), \mathbf{m} \neq 0$, and $\lambda(\mathbf{n})$ are independent and continuously distributed on $\mathbb{R}$ or $\mathbb{C}$, the amplitude of $g(\mathbf{n})$ as given by (14) is continuously distributed on $\mathbb{R}$ and hence the probability that the amplitude of $g(\mathbf{n})$ as given by (14) belongs to $\mathcal{A}$ at any $\mathbf{n}$ is zero.

Now consider $g(\mathbf{n})$ given by (15). Suppose that the amplitude of $g(\mathbf{n}_0)$ belongs to $\mathcal{A}$ at some $\mathbf{n}_0$. This is possible only for $\mathbf{n}_0 = (\mathbf{N}+\mathbf{m})/2$ in which case $g(\mathbf{n}_0) = e^{\mathrm{i}\theta} f^*(\mathbf{n}_0)$. The amplitude of $g(\mathbf{n}), \mathbf{n} \neq \mathbf{n}_0$, has a continuous distribution on $\mathbb{R}$ and zero probability to lie in $\mathcal{A}$.

The global phase θ, however, can not be determined uniquely in either case.

□

The global phase factor can be determined uniquely by additional constraint on the values of the object. For example, the following result follows immediately from Theorem 4 (i).

Corollary 1. *Suppose that $\{f(\mathbf{n})\}$ is real and nonnegative and that $\{\lambda(\mathbf{n})\}$ are independent continuous random variables on $\mathbb{S}^1$ or $\mathbb{C}$. If the resulting z-transform is almost surely irreducible, then $\{f(\mathbf{n})\}$ can be determined absolutely uniquely.*

Proof. With a real, positive object, the countable set for phase is the singleton $\{0\}$ and the global phase is uniquely fixed. $\square$

4.2. **Sector constraint.** More generally, we consider the *sector* constraint that the phases of $\{f(\mathbf{n})\}$ belong to $[a, b] \subset [0, 2\pi]$. For example, the class of complex-valued objects relevant to X-ray diffraction typically have nonnegative real and imaginary parts where the real part is the effective number of electrons coherently diffracting photons, and the imaginary part represents the attenuation [20]. For such objects, $[a, b] = [0, \pi/2]$.

Generalizing the argument for Theorem 4 we can prove the following.

Theorem 5. *Let the finite object $\{f(\mathbf{n})\}$ satisfy the* sector *constraint that the phases of $\{f(\mathbf{n})\}$ belong to $[a, b] \subset [0, 2\pi]$. Let S be the sparsity (the number of nonzero elements) of the object.*

(i) Consider the random phase illumination (6) and suppose that the phases $\phi(\mathbf{n})$ are i.i.d. uniform random variables on $[0, 2\pi]$. Assume that the resulting z-transform is almost surely irreducible. Then with probability at least $1 - |\mathcal{N}||b-a|^{[S/2]}(2\pi)^{-[S/2]}$ the object f is uniquely determined, up to a global phase, by the Fourier magnitude measurement. Here $[S/2]$ is the greatest integer at most $S/2$.

(ii) Consider the random amplitude illumination with i.i.d. random variables $\{\lambda(\mathbf{n})\} \subset \mathbb{R}$ that are equally likely negative or positive, i.e. $\mathbb{P}\{\lambda(\mathbf{n}) > 0\} = \mathbb{P}\{\lambda(\mathbf{n}) < 0\} = 1/2, \forall \mathbf{n}$. Assume that the resulting z-transform is almost surely irreducible. Then with probability at least

$$1 - |\mathcal{N}| 2^{-[(S-1)/2]} \left(1 - \max\left\{0, \frac{b-a}{\pi} - 1\right\}\right)^{[(S-1)/2]}$$

the object f is uniquely determined, up to a global phase, by the Fourier magnitude measurement.

The global phase is uniquely determined if the sector $[a, b]$ is tight in the sense that no proper subset of $[a, b]$ contains all the phases of the object.

Proof. Case (i): Consider first the expression (14) with any $\mathbf{m} \neq 0$ and the $[S/2]$ independently distributed random variables of $g(\mathbf{n})$ corresponding to $[S/2]$ nonoverlapping pairs of points $\{\mathbf{n}, \mathbf{n} \oplus \mathbf{m}\}$. The probability for every such the phase of $g(\mathbf{n})$ to lie in the sector $[a, b]$ is $|b-a|/(2\pi)$ for any θ and hence the probability for all $g(\mathbf{n})$ with $\mathbf{m} \neq 0, \theta \neq 0$, to lie in the sector is at most $|b-a|^{[S/2]}(2\pi)^{-[S/2]}$. The union over $\mathbf{m} \neq 0$ of these events has probability at most $|\mathcal{N}||b-a|^{[S/2]}(2\pi)^{-[S/2]}$.

Likewise the probability for all $g(\mathbf{n})$ given by (15) to lie in the first quadrant for any $\mathbf{m}$ is at most $|\mathcal{N}||b-a|^{[S/2]}(2\pi)^{-[S/2]}$.

Case (ii): For (14) with any $\mathbf{m} \neq 0$ the $[S/2]$ independently distributed random variables $g(\mathbf{n})$ corresponding to $[S/2]$ nonoverlapping pairs of points $\{\mathbf{n}, \mathbf{n} \oplus \mathbf{m}\}$, satisfy the sector constraint with probability at most $2^{-[S/2]}$ if $|b-a| \leq \pi$ or $(1-(b-a)/(2\pi))^{[S/2]}$ if $|b-a| > \pi$ for any θ. Hence the probability that all $g(\mathbf{n})$ with $\mathbf{m} \neq 0$ satisfy the sector constraint is at most

$$|\mathcal{N}|2^{-[S/2]}\left(1-\max\left\{0,\frac{b-a}{\pi}-1\right\}\right)^{[S/2]}.$$

For (15) with $\theta=0$ and any $\mathbf{m}$, $g(\mathbf{n}_0)=f(\mathbf{n}_0)$ at $\mathbf{n}_0=(\mathbf{N}+\mathbf{m})/2$ and hence $g(\mathbf{n}_0)$ lies in the first quadrant with probability one. For $\mathbf{n}\neq\mathbf{n}_0$, $g(\mathbf{n})$ satisfies the sector constraint with probability $1/2$ if $|b-a|\leq\pi$ or with probability $1-(b-a)/(2\pi)$ if $|b-a|>\pi$. Now the $[(S-1)/2]$ independently distributed random variables $g(\mathbf{n})$ corresponding to nonoverlapping pairs of points $\{\mathbf{n},\mathbf{n}\oplus\mathbf{m}\},\mathbf{n}\neq\mathbf{n}_0$, satisfy the sector constraint with probability at most $2^{-[(S-1)/2]}$ if $|b-a|\leq\pi$ or $(1-(b-a)/(2\pi))^{[(S-1)/2]}$ if $|b-a|>\pi$. Hence the probability that all $g(\mathbf{n})$ given by (15) with arbitrary $\mathbf{m}$ satisfy the sector constraint is at most

$$|\mathcal{N}|2^{-[(S-1)/2]}\left(1-\max\left\{0,\frac{b-a}{\pi}-1\right\}\right)^{[(S-1)/2]}.$$

□

4.3. **Magnitude constraint.** Likewise if the object satisfies a magnitude constraint then we can use random *amplitude* illumination to enforce uniqueness (up to a global phase).

Theorem 6. *Suppose that K pixels of the complex-valued object f satisfy the magnitude constraint $0<a\leq|f(\mathbf{n})|\leq b$ and that $\{\lambda(\mathbf{n})\}$ are i.i.d. continuous random variables on $\mathbb{R}$ or $\mathbb{C}$ with $\mathbb{P}\{|\lambda(\mathbf{n})/\lambda(\mathbf{n}')|>b/a \text{ or } |\lambda(\mathbf{n})/\lambda(\mathbf{n}')|<a/b\}=1-p>0$ for $\mathbf{n}\neq\mathbf{n}'$. If the resulting z-transform is almost surely irreducible then the object f is determined uniquely, up to a global phase, by the Fourier magnitude data on $\mathcal{M}$, with probability at least $1-|\mathcal{N}|p^{-[K/2]}$.*

Proof. The proof is similar to that for Theorem 5(ii).

For (14) with any $\mathbf{m}\neq 0$ the $[K/2]$ independently distributed random variables $g(\mathbf{n})$ corresponding to $[K/2]$ nonoverlapping pairs of points $\{\mathbf{n},\mathbf{n}\oplus\mathbf{m}\}$ satisfy $0<a\leq|g(\mathbf{n})|\leq b$ with probability less than $p^{-[K/2]}$ for any θ. Hence the probability that $g(\mathbf{n})$ with $\mathbf{m}\neq 0$ satisfy the magnitude constraint at K or more points is at most $|\mathcal{N}|p^{-[K/2]}$.

For (15) with any $\mathbf{m}$, $|g(\mathbf{n}_0)|=|f(\mathbf{n}_0)|$ at $\mathbf{n}_0=(\mathbf{N}+\mathbf{m})/2$ and hence $g(\mathbf{n}_0)$ satisfies the magnitude constraint with probability one. For $\mathbf{n}\neq\mathbf{n}_0$, there is at most probability p for $g(\mathbf{n})$ to satisfy the magnitude constraint. By independence, the $[(K-1)/2]$ independently distributed random variables $g(\mathbf{n})$ corresponding to nonoverlapping pairs of points $\{\mathbf{n},\mathbf{n}\oplus\mathbf{m}\},\mathbf{n}\neq\mathbf{n}_0$, satisfy the magnitude constraint with probability at most $p^{-[(K-1)/2]}$. Hence the probability that $g(\mathbf{n})$ given by (15) with arbitrary $\mathbf{m}$ satisfy the magnitude constraint at K or more points is at most $|\mathcal{N}|p^{-[(K-1)/2]}$.

The global phase factor is clearly undetermined. □

As in Theorem 4 case (ii) the magnitude constraint here, however, is not convex.

4.4. **Complex objects without constraint.** For general complex-valued objects without any constraint, we consider two sets of Fourier magnitude data produced with two independent random illuminations and obtain almost sure uniqueness modulo global phase.

Theorem 7. *Let $\{f(\mathbf{n})\}$ be a finite complex-valued array. Let $\{\lambda_1(\mathbf{n})\}$ and $\{\lambda_2(\mathbf{n})\}$ be two independent arrays of* continuous *random variables on $\mathbb{S}^1$, $\mathbb{R}$ or $\mathbb{C}$ with an absolutely* *continuous joint distribution with respect to the product measure. Suppose that the resulting z-transform from random illumination is almost surely irreducible.*

Then with probability one $f(\mathbf{n})$ is uniquely determined, up to a global phase, by the Fourier magnitude measurements on $\mathcal{M}$ with two illuminations λ_1 and λ_2.

If the second illumination $\{\lambda_2(\mathbf{n})\}$ is deterministic while $\{\lambda_1(\mathbf{n})\}$ is random as above, then the same conclusion holds.

Proof. Let $g(\mathbf{n})$ be another array that vanishes outside $\mathcal{N}$ and produces the same data. By Theorem 1, 2 and Remark 1

$$g(\mathbf{n}) = \begin{cases} e^{\mathrm{i}\theta_i} f(\mathbf{n}\oplus\mathbf{m}_i)\lambda_i(\mathbf{n}\oplus\mathbf{m}_i)/\lambda_i(\mathbf{n}) \\ e^{\mathrm{i}\theta_i} f^*(\mathbf{N}-\mathbf{n}\oplus\mathbf{m}_i)\lambda_i^*(\mathbf{N}-\mathbf{n}\oplus\mathbf{m}_i)/\lambda_i(\mathbf{n}), \end{cases} \tag{16}$$

for some $\mathbf{m}_i \in \mathbb{Z}^2, \theta_i \in \mathbb{R}, i = 1, 2$.

Four scenarios of ambiguity exist but because of the independence of $\lambda_1(\mathbf{n}), \lambda_2(\mathbf{n})$ none can arise.

First of all, if

$$g(\mathbf{n}) = e^{\mathrm{i}\theta_i} f(\mathbf{n}\oplus\mathbf{m}_i)\lambda_i(\mathbf{n}\oplus\mathbf{m}_i)/\lambda_i(\mathbf{n}), \quad i = 1, 2$$

then

$$e^{\mathrm{i}\theta_1} f(\mathbf{n}\oplus\mathbf{m}_1)\lambda_1(\mathbf{n}\oplus\mathbf{m}_1)/\lambda_1(\mathbf{n}) = e^{\mathrm{i}\theta_2} f(\mathbf{n}\oplus\mathbf{m}_2)\lambda_2(\mathbf{n}\oplus\mathbf{m}_2)/\lambda_2(\mathbf{n}).$$

This almost surely can not occur unless $\mathbf{m}_1 = \mathbf{m}_2 = \mathbf{0}, \theta_1 = \theta_2$ in which case g equals f up to a global phase factor.

The other possibilities can be similarly ruled out:

$$\begin{aligned} g(\mathbf{n}) &= e^{\mathrm{i}\theta_1} f(\mathbf{n}\oplus\mathbf{m}_1)\lambda_1(\mathbf{n}\oplus\mathbf{m}_1)/\lambda_1(\mathbf{n}) \\ &= e^{\mathrm{i}\theta_2} f^*(\mathbf{N}-\mathbf{n}\oplus\mathbf{m}_2)\lambda_2^*(\mathbf{N}-\mathbf{n}\oplus\mathbf{m}_2)/\lambda_2(\mathbf{n}) \end{aligned}$$

and

$$g(\mathbf{n}) = e^{\mathrm{i}\theta_i} f^*(\mathbf{N}-\mathbf{n}\oplus\mathbf{m}_i)\lambda_i^*(\mathbf{N}-\mathbf{n}\oplus\mathbf{m}_i)/\lambda_i(\mathbf{n}), \quad i = 1, 2 \tag{17}$$

for any $\mathbf{m}_i, \theta_i, i = 1, 2$.

Now consider the case that $\{\lambda_2(\mathbf{n})\}$ is deterministic. Let g be given as in (16) with $i = 1$. Then the Fourier magnitude data for the second illumination

$$\widetilde{F}_2(\mathbf{w}) = \sum_{\mathbf{n}} g(\mathbf{n})\lambda_2(\mathbf{n})e^{-\mathrm{i}2\pi\mathbf{n}\cdot\mathbf{w}} \tag{18}$$

are *continuous* random variables unless $g(\mathbf{n}) = e^{\mathrm{i}\theta_1} f(\mathbf{n})$. On the other hand, since $\{\lambda_2(\mathbf{n})\}$ is deterministic, the Fourier magnitude $\widetilde{F}_2(\mathbf{w})$ must be deterministic also. Thus, $g(\mathbf{n}) = e^{\mathrm{i}\theta_1} f(\mathbf{n})$ for some constant θ_1.

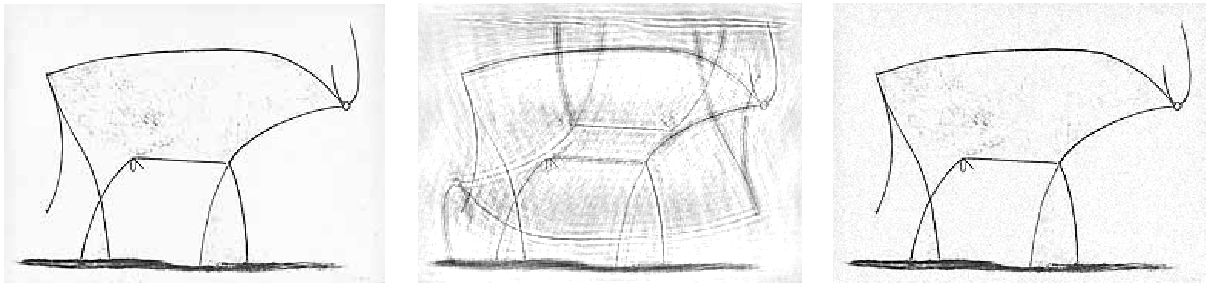
□

5. Numerical examples

The following numerical examples (Figures 3 and 2) give a glimse of how the quality and efficiency of reconstruction can be improved by random *phase* illumination (6).

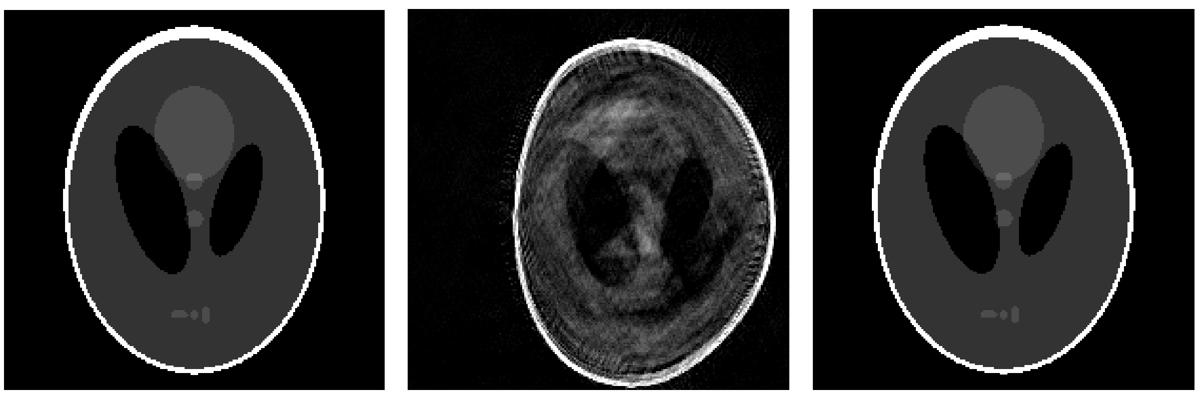
To test how many Fourier magnitude data are needed for phasing, we define the sampling rate

$$\rho = \#\text{ Fourier magnitude data}/\#\text{ image pixels.}$$



(a) (b) (c)

FIGURE 2. (a) The original object and reconstructions with (b) uniform illumination, $\rho = 4$, relative error 13%, relative Fourier magnitude residual 0.74% and (c) random phase illumination, $\rho = 0.55$, relative error 2.97%, relative Fourier magnitude residual 0.37% (adapted from [8]).



(a) (b) (c)

FIGURE 3. (a) The original object and reconstructions with (b) uniform illumination, $\rho = 4$, relative error 115.1%, relative Fourier magnitude residual 4.3% and (c) random phase illumination, $\rho = 1.1$, relative error 0.17%, relative Fourier magnitude residual 0.04% (adapted from [9]).

The uniqueness results above are established for $\rho = 4$ (in two dimensions).

The standard HIO algorithm of various numbers of iterations is implemented in the framework of the oversampling method [19, 20] which converts the Fourier magnitude data with $\rho > 1$ into a support constraint to reduces the ambiguity of spatial shift (but not the twin image).

Consider two real, positive images for which absolute uniqueness holds with random illumination (Corollary 1): Picasso's bull (Figure 2(a)), a tight image (due to the bright pixels surrounding the bull), and the phantom (Figure 3(a)), a loose image (due to the dark pixels surrounding the phantom).

Let $\mathcal{N}$ be the square (in the case of the phantom) or rectangular (in the case of Picasso's bull) frame of image. A tight image has a tightly defined support (i.e. $\mathcal{N}$) while a loose image has a loosely defined support (i.e. a proper subset of $\mathcal{N}$).

With uniform illumination ($\lambda(\mathbf{n}) = 1, \forall \mathbf{n}$), $\rho = 4$ and 3000 HIO iterations, the recovered bull has a poor quality (Figure 2(b)) due to the interference of the twin image while the recovered phantom is shifted and distorted due to the loose support constraint (Figure 3(b)).

In both cases, the reconstruction error is high (13% for the bull and 115.1% for the phantom) but the residual is low (0.37% for the bull and 0.04% for the phantom) indicating the iterative process has more or less converged. Hence the reconstruction error should be attributed to the lack of uniqueness rather than the lack of convexity of phasing with uniform illumination.

In principle, the stagnation problem (large number of iterations) may be due to the lack of convexity or uniqueness. But consider Figure 2(c) and Figure 3(c): With just a single random phase illumination, both problems with stagnation and error disappear and phasing with *100 HIO iterations and* $\rho = 1.1$ achieves accurate, high-quality recovery. This experiment confirms our belief that once absolute uniqueness is enforced, most of the numerical problems with the phasing algorithms can be alleviated.

6. Conclusions

In conclusion, we have proposed the approach of random illumination to the phase retrieval problem to address at once all phasing ambiguities, including trivial and nontrivial types. For general random illumination we have proved almost sure irreducibility for *any* complex-valued object of sufficiently high sparsity (Theorem 2) or of convex support whose dimension is greater than one (Theorem 3). We have proved the almost sure uniqueness, up to a global phase, under the two-point assumption (Theorem 4). The absolute uniqueness is then enforced by the positivity constraint (Corollary 1). Under the tight sector constraint, we have proved the absolute uniqueness with probability exponentially close to unity as the object sparsity increases (Theorem 5). Under the magnitude constraint, we have proved uniqueness up to a global phase with probability exponentially close to unity (Theorem 6). For general complex-valued objects without any constraint, we have established almost sure uniqueness modulo global phase with two independent random illuminations (Theorem 7).

Numerical examples show that phasing with random illumination drastically reduces the number of Fourier magnitude data, numerical iterations and the error in reconstruction and reveal that much of the previous problems with reconstruction error and stagnation is due to the lack of absolute uniqueness.

Practical implementation of our approach demands precise maneuver of illumination which can be expected to realize with advances of technology. Systematic and thorough numerical study of phasing with random illumination in the presence of noise will be presented in the forthcoming paper [9].

On the issue of convexity on the other hand, there have been recent attempts to formulate phase retrieval as a convex optimization problem [5, 6]. These approaches, however promising, require a lot more Fourier magnitude data and computational resources.

Acknowledgements. I thank Jesus De Loera for helpful discussion and references.

References

[1] P. F. Almoro, G. Pedrini, P. N. Gundu, W. Osten, S. G. Hanson, " Enhanced wavefront reconstruction by random phase modulation with a phase diffuser," *Opt. Laser Eng.* **49** 252-257 (2011).

[2] R.H.T. Bates, "Fourier phase problems are uniquely soluble in more than one dimension. I: underlying theory," *Optik* (Stuttgart) **61**, 247-262 (1982).

[3] H.H. Bauschke, P.L. Combettes, and D.R. Luke, "Phase retrieval, error reduction algorithm, and Fienup variants: a view from convex optimization," *J. Opt. Soc. Am. A* **19**(7), 1334 - 1345 (2002).

[4] Yu. M. Bruck and L. G. Sodin, "On the ambiguity of the image reconstruction problem," *Opt. Commun.***30**, 304-308 (1979).

[5] E. J. Candès, Y. Eldar, T. Strohmer and V. Voroninski, " Phase retrieval via matrix completion," preprint, August 2011.

[6] A. Chai, M. Moscoso, and G. Papanicolaou. "Array imaging using intensity-only measurements," *Inv. Probl.* **27** 015005 (2011)

[7] A. Fannjiang, " Exact localization and superresolution with noisy data and random illumination," *Inverse Problems* **27** 065012 (2011)

[8] A. Fannjiang and W. Liao, "Compressed sensing phase retrieval," Proceedings of IEEE Asilomar Conference on Signals, Systems and Computers, Pacific Grove, CA, Nov 6-9, 2011.

[9] A. Fannjiang and W. Liao, "Phase retrieval with random illumination," to appear.

[10] J.R. Fienup, "Phase retrieval algorithms: a comparison, " *Appl. Opt.* **21** 2758-2769 (1982).

[11] J.R. Fienup, "Reconstruction of a complex-valued object from the modulus of its Fourier transform using a support constraint," *J. Opt. Soc. Am. A* **4**, 118 -123 (1987).

[12] J.R. Fienup and C.C. Wackerman, "Phase-retrieval stagnation problems and solutions," *J. Opt. Soc. Am. A* **3** 1897-1907 (1986).

[13] J. Garcia, Z. Zalevsky, and D. Fixler, "Synthetic aperture superresolution by speckle pattern projection," *Opt. Exp.* **13** 6073-6078 (2005).

[14] M. Hayes, "The reconstruction of a multidimensional sequence from the phase or magnitude of its Fourier transform," *IEEE Trans. Acoust. Speech Sign. Proc.* **30** 140- 154 (1982).

[15] M.H. Hayes and J.H. McClellan. "Reducible Polynomials in More Than One Variable." *Proc. IEEE* **70**(2):197 198, (1982).

[16] H. He, "Simple constraint for phase retrieval with high efficiency," *J. Opt. Soc. Am. A***23** 550 - 556 (2006).

[17] S. Marchesini, " A unified evaluation of iterative projection algorithms for phase retrieval," *Rev. Sci. Instr.* **78**, 011301 (2007).

[18] J. Miao, T. Ishikawa, Q. Shen, and T. Earnest, "Extending X-Ray crystallography to allow the imaging of non- crystalline materials, cells and single protein complexes," *Annu. Rev. Phys. Chem.* **59**, pp. 387410 (2008).

[19] J. Miao and D. Sayre, "On possible extensions of X-ray crystallography through diffraction-pattern oversampling," *Acta Cryst. A* **56** 596-605 (2000).

[20] J. Miao, D. Sayre and H.N. Chapman, "Phase retrieval from the magnitude of the Fourier transforms of nonperiodic objects," *J. Opt. Soc. Am. A* **15** 1662-1669 (1998).

[21] A. M. Ostrowski, On multiplication and factorization of polynomials, I. Lexicographic ordering and extreme aggregates of terms, *Aequationes Math.* **13** (1975), 201228.

[22] T.A. Pitts and J. F. Greenleaf, "Fresnel transform phase retrieval from magnitude," *IEEE Trans. Ultrasonics, Ferroelec. Freq. Contr.* **50** (8) 1035-1045 (2003).

[23] J. Romberg, "Compressive sensing by random convolution," *SIAM J. Imag. Sci.* **2** 1098-1128 (2009).

[24] I. Z. Ruzsa, "Sum of sets in several dimensions," *Combinatorica* **14** 485 - 490 (1994).

[25] H. Stark, *Image Recovery: Theory and Applications.* New York: Academic Press, 1987.

[26] D. Sylman, V. Mico, J. Garcia, and Z. Zalevsky, "Random angular coding for superresolved imaging," *Appl. Opt.* **49** 4874-4882 (2010)

[27] C. Ventalon and J. Mertz, "Dynamic speckle illumination microscopy with translated versus randomized speckle patterns," *Opt. Exp.* **14** 7198-7209 (2006).

[28] Z. Zalevsky, S. Rozental and M. Meller, "Usage of Turbulence for Super Resolved Imaging," *Opt. Lett.* **32** 1072-1074 (2007).

Department of Mathematics, UC Davis, CA 95616-8633. fannjiang@math.ucdavis.edu