On the 2D Phase Retrieval Problem

Dani Kogan, Yonina C. Eldar, *Fellow, IEEE*, and Dan Oron

Abstract—The recovery of a signal from the magnitude of its Fourier transform, also known as phase retrieval, is of fundamental importance in many scientific fields. It is well known that due to the loss of Fourier phase the problem in one-dimensional (1D) is ill-posed. Without further constraints, there is no unique solution to the problem. In contrast, uniqueness up to trivial ambiguities very often exists in higher dimensions, with mild constraints on the input. In this paper, we focus on the 2D phase retrieval problem and provide insight into this uniqueness property by exploring the connection between the 2D and 1D formulations. In particular, we show that 2D phase retrieval can be cast as a 1D problem with additional constraints, which limit the solution space. We then prove that only one additional constraint is sufficient to reduce the many feasible solutions in the 1D setting to a unique solution for almost all signals. These results allow to obtain an analytical approach (with combinatorial complexity) to solve the 2D phase retrieval problem when it is unique.

Index Terms—Phase retrieval, 2D autocorrelation, uniqueness.

I. INTRODUCTION

RECOVERY of a signal from the modulus of its Fourier transform, also known as phase retrieval [1], [2], is of paramount importance in many scientific fields such as optics [3], X-ray crystallography [4], astronomy [5], computational biology [6], speech recognition [7] and more [8], [9]. Generally, the phase retrieval problem has no unique solution since any choice of the Fourier phase will generate a valid solution which can be far from the original signal [10], [11]. If the unknown input is compactly supported and the frequency domain is oversampled by a factor of two, then the phase retrieval problem can be equivalently stated as that of retrieving a vector from its autocorrelation function.

To study uniqueness in the 1D discrete case, Bruck and Sodin [12] considered the z-transform of the autocorrelation sequence. The fact that 1D polynomials can always be factored, leads to the conclusion that in general there is no uniqueness in 1D phase retrieval. This is true even when we ignore trivial ambiguities which include a global phase shift, conjugate inversion

and spatial shift. Furthermore, there are generally as many as 2^{N-2} vectors of length N that share the same autocorrelation sequence [13]. An exception is when prior knowledge on the signal is available. One example is when the signal is minimum phase so that all the zeros of its z-transform are known to lie within the unit circle [14]. For higher dimensions, and especially in 2D, Bruck and Sodin argued that since multivariate polynomials cannot in general be factored, phase retrieval has a unique solution for almost all signals.

Despite the uniqueness guarantees in 2D, there is no general solution method available to find the unknown signal from its Fourier magnitude [15]. Over the years, several approaches have been suggested for solving the phase retrieval problem algorithmically. The most popular techniques are based on alternating projections, pioneered by Gerchberg and Saxton [16] and extended by Fienup [17]–[19]. More recent approaches include semi-definite programming (SDP) algorithms [20]–[22], gradient techniques with appropriate initialization such as Wirtinger flow [23], or truncated amplitude flow [24], and greedy methods with a sparsity prior [25], [26].

In this work we study the 2D discrete phase retrieval problem with the goal of obtaining further insight into its uniqueness properties, and understanding the intrinsic differences and relationships between the 1D and 2D formulations. In particular, it is natural to attempt to describe the 2D autocorrelation matrix $\mathbf{R}$ of an $N \times N$ matrix $\mathbf{X}$ in terms of the 1D autocorrelation $\mathbf{r}$ of its vectorized version $\mathbf{x}$ with length N^2. We will see that we can indeed compute $\mathbf{r}$ from $\mathbf{R}$, but the reverse computation is not possible. Namely, the 2D autocorrelation $\mathbf{R}$ provides more knowledge on $\mathbf{X}$ than the 1D autocorrelation of its vectorized version. Nonetheless, we can formulate the 2D phase retrieval problem in terms of the 1D autocorrelation $\mathbf{r}$ and $(N-1)^2$ additional constraints which correspond to knowledge of certain autocorrelation values of $\mathbf{X}$. Next we show that to ensure uniqueness for almost all signals, it is sufficient to remove most of these constraints, and add a *single* constraint beyond knowing the autocorrelation sequence $\mathbf{r}$. More specifically, for almost all matrices $\mathbf{X}$, knowing the 1D autocorrelation $\mathbf{r}$ of its vectorized version together with the additional constraint $R(N-1, -(N-1)) = x[N-1]x[N^2-N]$ is sufficient to reduce the many non-trivial solutions of the 1D problem and guarantee uniqueness. Finally, we illustrate how to use these results to construct the unique recovery when it exists.

This paper is organized as follows. In Section II, we mathematically set up the phase retrieval problem and discuss uniqueness in one and two dimensions. We then show how 2D phase retrieval can be recast as a 1D phase retrieval problem with additional constraints in Section III. In Section IV we prove that only one additional constraint from the reformulated problem is sufficient to guarantee uniqueness for almost all signals. We provide several examples to demonstrate the results.

II. PHASE RETRIEVAL IN ONE AND TWO DIMENSIONS

We begin by formulating the 1D and 2D phase retrieval problems, and discussing their basic uniqueness properties.

A. 1D Phase Retrieval

The 1D phase retrieval problem is to recover a vector $\mathbf{x}$ from the magnitude of its Fourier transform. To set up the problem mathematically, let $\mathbf{x} \in \mathbb{R}^N$ be a real length-N vector. Its discrete Fourier transform (DFT) of length $M \geq N$ is defined as

$$\widehat{x}[k] = \sum_{n=0}^{N-1} x[n] e^{-j \frac{2\pi k}{M}}, \quad 0 \leq k \leq M - 1. \tag{1}$$

Since the DFT is a linear transformation it can be represented by a matrix-vector multiplication $\mathbf{F}_{M,N}\mathbf{x}$, where $\mathbf{F}_{M,N}$ is the $M \times N$ matrix consisting of the first N columns of the M-point DFT matrix

$$\mathbf{F}_{M,N} = \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & \phi & \phi^2 & \ldots & \phi^{N-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \phi^{M-1} & \phi^{2(M-1)} & \ldots & \phi^{(N-1)(M-1)} \end{pmatrix}, \tag{2}$$

and $\phi = e^{-j2\pi/M}$. With these definitions we can state the 1D phase retrieval problem as

$$\begin{aligned} &\text{find} && \mathbf{x} \\ &\text{subject to} && \mathbf{y} = |\mathbf{F}_{M,N}\mathbf{x}|^2 \end{aligned} \tag{3}$$

where $\mathbf{y}$ are the given measurements and the absolute value operation is taken element-wise.

Assuming $M \geq 2N - 1$, phase retrieval can equivalently be formulated as the problem of reconstructing a signal from its autocorrelation measurements

$$r[\ell] = \sum_{i=0}^{N-1-\ell} x[i]x[i+\ell], \quad 0 \leq \ell \leq N - 1, \tag{4}$$

with $r[\ell] = r[-\ell]$. For shorthand notation, we denote by $\mathbf{r} = \mathbf{x} \star \mathbf{x}$ the autocorrelation operator. We can then write problem (3) as

$$\begin{aligned} &\text{find} && \mathbf{x} \\ &\text{subject to} && \mathbf{r} = \mathbf{x} \star \mathbf{x}. \end{aligned} \tag{5}$$

Due to the loss of phase, problem (3) is ill posed and generally there are many possible solutions. First, there are trivial ambiguities that result from the fact that the following three operations conserve the Fourier magnitude:
1. Global phase shift $x[n] \rightarrow \pm x[n]$
2. Inversion $x[n] \rightarrow x[-n]$
3. Spatial shift $x[n] \rightarrow x[n + n_0]$.

Even up to trivial ambiguities, the 1D problem is not unique. In particular, any two sequences of length N that lead to the same autocorrelation sequence will have the same Fourier magnitude. In [27] the authors show that there are as many as 2^{N-2} signals

that share the same autocorrelation and are not trivially related. To see this, we analyze the roots of $\widehat{r}[k]$, the DFT of $r[\ell]$.

Let $P_{\mathbf{r}}(z)$ be the *associated polynomial* to $\widehat{r}[k]$:

$$P_{\mathbf{r}}(z) := \sum_{n=0}^{2N-2} r[n - N + 1]z^n. \tag{6}$$

Since $r[\ell]$ is symmetric, the zeros of $P_{\mathbf{r}}(z)$ appear in reflected pairs $(\gamma_i, \bar{\gamma}_i^{-1})$ with respect to the unit circle and there are $N - 1$ such zero pairs. The associated polynomial can therefore be factored as

$$P_{\mathbf{r}}(z) = r[N-1] \prod_{i=1}^{N-1} (z - \gamma_i)\left(z - \bar{\gamma}_i^{-1}\right). \tag{7}$$

On the unit circle we have

$$\widehat{r}[k] = r[N-1] \prod_{i=1}^{N-1} \left(e^{-j2\pi k/M} - \gamma_i\right)\left(e^{-j2\pi k/M} - \bar{\gamma}_i^{-1}\right). \tag{8}$$

Recalling that $\widehat{r}[k] = |\widehat{x}[k]|^2$, it follows that given $\widehat{r}[k]$, we cannot determine whether a zero γ_i or its conjugate reciprocal $\bar{\gamma}_i^{-1}$ is a root of $\widehat{x}[k]$ which leads to the non-uniqueness in phase retrieval.

More specifically, each vector $\mathbf{x} \in \mathbb{R}^N$ with autocorrelation sequence $\mathbf{r}$ and with $x[0], x[N-1] \neq 0$ has an associated polynomial of the form (up to a phase factor):

$$\begin{aligned} P_{\mathbf{x}}(z) &= \sum_{i=0}^{N-1} x[i]z^i \\ &= \left[|r[N-1]| \prod_{j=1}^{N-1} |\beta_j|^{-1}\right]^{\frac{1}{2}} \prod_{j=1}^{N-1} (z - \beta_j) \end{aligned} \tag{9}$$

where the parameters β_j in (9) can be chosen as $\beta_j \in \{\gamma_j, \bar{\gamma}_j^{-1}\}$. Aside from trivial ambiguities each solution is characterized by a different *zero set* $B : \{\beta_1, \ldots, \beta_{N-1}\}$. Obviously as β_j is allowed to either be γ_j or $\bar{\gamma}_j^{-1}$ we can construct up to 2^{N-1} different zero sets. It can be shown (see [27, corollary 3.3]) that if a signal $\mathbf{x}$ of the form (9) has a zero set $\{\beta_1, \ldots, \beta_{N-1}\}$ then the conjugate reflected signal of $\mathbf{x}$ has a zero set $\{\bar{\beta}_1^{-1}, \ldots, \bar{\beta}_{N-1}^{-1}\}$. Thus we conclude that there are up to 2^{N-2} non-trivially different vectors $\mathbf{x}$ with the same autocorrelation $\mathbf{r}$.

B. 2D Phase Retrieval

We now turn to discuss the 2D phase retrieval problem. In this case our unknown is an $N \times N$ real matrix $\mathbf{X}$. We assume we are given the magnitude-square of the 2D Fourier transform $\mathbf{Y} = |\mathbf{F}_{M,N}\mathbf{X}\mathbf{F}_{M,N}^T|^2$. Our problem can then be written as

$$\begin{aligned} &\text{find} && \mathbf{X} \\ &\text{subject to} && \text{vec}(\mathbf{Y}) = |(\mathbf{F}_{M,N} \otimes \mathbf{F}_{M,N})\text{vec}(\mathbf{X})|^2, \end{aligned} \tag{10}$$

where $\otimes$ denotes the Kronecker product and vec is the vectorization of a matrix. Assuming once again that $M \geq 2N - 1$, we can reformulate this problem in terms of the 2D autocorrelation

of the matrix $\mathbf{X}$, where the 2D autocorrelation is defined by

$$R(i,j) = \sum_{m=0}^{N-1-|i|}\sum_{n=0}^{N-1-|j|} X(m,n)X(m+i,n+j),$$
$$0 \le i,j \le N-1,$$

$$R(i,j) = \sum_{m=0}^{N-1-i}\sum_{n=-j}^{N-1} X(m,n)X(m+i,n+j),$$
$$i > 0, -(N-1) \le j \le -1, \quad (11)$$

and $R(-i,-j) = R(i,j)$. As in the 1D case, we use the notation $\mathbf{R} = \mathbf{X} \star \mathbf{X}$ to describe (11). We can then write (10) as

$$\text{find} \qquad \mathbf{X}$$
$$\text{subject to} \qquad \mathbf{R} = \mathbf{X} \star \mathbf{X}. \qquad (12)$$

Similarly to the 1D setting, the ambiguities of the 2D phase retrieval problem depend on the factorization of a multivariate algebraic polynomial into irreducible polynomials [10]. Since almost all 2D polynomials are irreducible, namely the reducible polynomials form a set of measure zero in the space of all polynomials [28], almost every 2D signal can be uniquely recovered from its 2D Fourier magnitude. Therefore, the uniqueness properties in 1D and 2D Fourier phase retrieval are markedly different. Our goal in this paper is to obtain further insight into this difference from the point of view of the autocorrelation sequences rather than the traditional algebraic viewpoint.

III. REFORMULATING THE 2D PROBLEM

In order to understand the essential differences between the 2D and 1D phase retrieval problems, it is intuitive to try and write the 2D problem in terms of a vector $\mathbf{x}$ representing the matrix $\mathbf{X}$. A natural approach is to vectorize $\mathbf{X}$ and then attempt to express the correlations in (12) in terms of the vector $\mathbf{x}$. To be explicit, we will focus on the choice $\mathbf{x} = \text{vec}(\mathbf{X}^T)$ which vectorizes $\mathbf{X}$ row-wise. Two immediate questions arise in this context:

1) Can we express the 2D autocorrelation $\mathbf{R} = \mathbf{X} \star \mathbf{X}$ in terms of the 1D autocorrelation $\mathbf{r} = \mathbf{x} \star \mathbf{x}$?
2) Is the 1D autocorrelation $\mathbf{r}$ together with a small number of constraints sufficient to obtain uniqueness for almost all matrices $\mathbf{X}$?

In this section we focus on the first question and show that $\mathbf{R}$ contains more information than $\mathbf{r}$. In other words, knowing $\mathbf{r}$ is not enough to recover $\mathbf{R}$. Beyond $\mathbf{r}$ we will need an additional $(N-1)^2$ constraints to fully characterize $\mathbf{R}$. The second question will be discussed in Section IV where we show that knowledge of $\mathbf{r}$ together with only one additional constraint that involves a specific value of $\mathbf{R}$ is sufficient to ensure uniqueness for almost all 2D signals.

A. From 2D to 1D

A first step towards reformulating the 2D problem into a 1D counterpart is to vectorize the matrix $\mathbf{X}$ so we effectively retrieve the same object as one would in a 1D setting. As noted above we will do that via $\mathbf{x} = \text{vec}(\mathbf{X}^T)$ which implies that

$$x[mN+n] = X(m,n), \quad 0 \le m,n \le N-1. \qquad (13)$$

The next step is to understand the relationship between the 2D autocorrelation $\mathbf{R}$ of $\mathbf{X}$ and the 1D autocorrelation $\mathbf{r}$ of $\mathbf{x}$. This relationship is expressed in the following proposition.

Proposition 1: Let $\mathbf{X}$ be a real valued $N \times N$ matrix and let $\mathbf{x} = \text{vec}(\mathbf{X}^T)$ be its row vectorized representation of length N^2. Let $\mathbf{R} = \mathbf{X} \star \mathbf{X}$ be the 2D autocorrelation matrix of $\mathbf{X}$ and let $\mathbf{r} = \mathbf{x} \star \mathbf{x}$ be the 1D autocorrelation sequence of $\mathbf{x}$. Then for values $0 \le \ell \le N^2 - 1$ we have

$$r(\ell)$$
$$= \begin{cases} R(i,0) & \ell = iN, \\ R(N-1,j) & N(N-1) < \ell \le N^2 - 1 \\ R(i,j) + R(i+1,j-N) & \text{otherwise}, \end{cases} \qquad (14)$$

where $0 \le i,j \le N-1$ are the unique values satisfying $\ell = iN+j$, namely, $i = \lfloor \ell/N \rfloor$ and $j = \ell \mod N$.

Proof: Substituting (13) into (11) the 2D autocorrelation takes the form

$$R(i,j) = \sum_{m=0}^{N-1-|i|}\sum_{n=0}^{N-1-|j|} x[mN+n]x[(m+i)N+n+j]$$
$$= \sum_{m=0}^{N-1-|i|}\sum_{n=0}^{N-1-|j|} x[mN+n]x[mN+n+\ell], \qquad (15)$$

for $0 \le i,j \le N-1$ where $\ell = iN+j$. Similarly, for $i > 0, -(N-1) \le j \le -1$ we have

$$R(i,j) = \sum_{m=0}^{N-1-|i|}\sum_{n=-j}^{N-1} x[mN+n]x[mN+n+\ell]. \qquad (16)$$

Since the summand in $R(i,j)$ depends only on ℓ, any valid choice of i,j that leads to the same value of $\ell = iN+j$ will have the same summand. In particular, the pairs (i,j) and $(i+1, j-N)$ result in the same ℓ. Therefore, for every $0 < i \le N-2$ and $0 < j \le N-1$ there is a corresponding value $j' = j - N$ in the range $-(N-1) \le j \le -1$ with the same ℓ. For this choice of i,j' we have

$$R(i+1,j-N) = \sum_{m=0}^{N-2-i}\sum_{n=N-j}^{N-1} x[mN+n]x[mN+n+\ell]. \qquad (17)$$

Adding (15) and (17) for $0 < i \le N-2, 0 < j \le N-1$ gives

$$R(i,j) + R(i+1,j-N)$$

$$= \left(\sum_{m=0}^{N-2-i} \sum_{n=N-j}^{N-1} + \sum_{m=0}^{N-1-i} \sum_{n=0}^{N-1-j} \right) x[mN+n]x[mN+n+\ell]$$

$$= \sum_{m=0}^{N-2-i} \sum_{n=0}^{N-1} x[mN+n]x[mN+n+\ell]$$

$$+ \sum_{n=0}^{N-1-j} x[(N-1-i)N+n]x[(N-1-i)N+n+\ell]. \tag{18}$$

We next substitute $k = mN + n$ in the first term of (18) and $s = (N-i-1)N+n$ in the second term which results in

$$R(i,j) + R(i+1,j-N)$$

$$= \sum_{k=0}^{(N-i-1)N-1} x[k]x[k+\ell] + \sum_{s=(N-i-1)N}^{(N-i-1)N+N-1-j} x[s]x[s+\ell]$$

$$= \sum_{k=0}^{N^2-1-(iN+j)} x[k]x[k+\ell]$$

$$= \sum_{k=0}^{N^2-1-\ell} x[k]x[k+\ell]. \tag{19}$$

The expression in (19) is precisely the autocorrelation sequence of $\mathbf{x}$ for values of $\ell = iN + j$ with $0 < i \le N-2, 0 < j \le N-1$. This corresponds to all values $0 \le \ell \le N(N-1)-1$ excluding $\ell = Ni$.

It remains to determine $r(\ell)$ for $\ell = Ni$ and $N(N-1) < \ell \le N^2-1$. We begin with $\ell = Ni$ which corresponds to $j = 0$. Substituting these values into (15) results in

$$R(i,0) = \sum_{m=0}^{N-1-|i|} \sum_{n=0}^{N-1} x[mN+n]x[mN+n+\ell]$$

$$= \sum_{k=0}^{(N-1-|i|)N+N-1} x[k]x[k+\ell]$$

$$= \sum_{k=0}^{N^2-1-\ell} x[k]x[k+\ell] = r[\ell], \tag{20}$$

where we defined $k = mN + n$. Next, the values $N(N-1) < \ell \le N^2-1$ correspond to $i = N-1$ and $0 \le j \le N-1$. Plugging into (15) leads to

$$R(N-1,j) = \sum_{n=0}^{N-1-j} x[n]x[n+\ell]$$

$$= \sum_{k=0}^{N^2-1-\ell} x[k]x[k+\ell] = r[\ell], \tag{21}$$

since $\ell = (N-1)N + j$. ∎

Proposition 1 establishes that the 1D autocorrelation provides less knowledge on $\mathbf{X}$ than the 2D autocorrelation. Indeed, knowing $\mathbf{r}$ provides information on $R(i,j)$ for $-(N-1) \le j \le -1$ only through the sum of these values with matching autocorrelation values. Therefore, in order to be able to recover $\mathbf{R}$ from $\mathbf{r}$ we must obtain these values separately, namely we require an additional $(N-1)^2$ constraints on $\mathbf{R}$. This observation combined with Proposition 1 leads to the following theorem, which establishes that the 2D phase retrieval problem can be cast as a 1D problem with additional constraints.

Theorem 2: Let $\mathbf{X}$ be a real valued $N \times N$ matrix and let $\mathbf{x} = \text{vec}(\mathbf{X}^T)$ be its row vectorized representation. Let $\mathbf{R} = \mathbf{X} \star \mathbf{X}$ be the 2D autocorrelation matrix of $\mathbf{X}$ and let $\mathbf{r} = \mathbf{x} \star \mathbf{x}$ be the 1D autocorrelation sequence of $\mathbf{x}$. Then the 2D phase retrieval problem

$$\text{find} \qquad \mathbf{X}$$

$$\text{subject to} \qquad \mathbf{R} = \mathbf{X} \star \mathbf{X}$$

is equivalent to the 1D problem with $(N-1)^2$ additional constraints:

$$\text{find} \qquad \mathbf{x}$$

$$\text{subject to } \mathbf{r} = \mathbf{x} \star \mathbf{x}$$

$$R(i,j) = \sum_{m=0}^{N-1-i} \sum_{n=-j}^{N-1} \tag{22}$$

$$x[mN+n]x[mN+n+\ell]$$

for $i > 0, -(N-1) \le j \le -1$ where $\ell = iN + j$ and $0 \le \ell \le N^2-1$. The values of $r(\ell)$ are determined from $R(i,j)$ via (14).

To summarize, the general procedure for reformulating a 2D problem as a 1D problem is as follows:
1) Define the vector $\mathbf{x}$ that is generated by vectorizing the matrix $\mathbf{X}^T$, i.e $\mathbf{x} = \text{vec}(\mathbf{X}^T)$.
2) Extract the 1D autocorrelation sequence of $\mathbf{x}$ from the 2D autocorrelation matrix of $\mathbf{X}$ via Proposition 1.
3) Using the extracted 1D autocorrelation, recast the 2D phase retrieval problem on $\mathbf{X}$ as a 1D phase retrieval problem on $\mathbf{x}$ with additional $(N-1)^2$ constraints as stated in Theorem 2.

B. An Example

We now provide an example demonstrating the steps above in order to reformulate a simple 2D problem.

Let $\mathbf{X}$ be the 2×2 matrix given by

$$\mathbf{X} = \begin{pmatrix} -24 & 26 \\ -9 & 1 \end{pmatrix}. \tag{23}$$

In a phase retrieval experiment we measure the 2D autocorrelation of the matrix $\mathbf{X}$:

$$\mathbf{R} = \begin{pmatrix} R(-1,-1) & R(-1,0) & R(-1,1) \\ R(0,-1) & R(0,0) & R(0,1) \\ R(1,-1) & R(1,0) & R(1,1) \end{pmatrix}. \tag{24}$$

The autocorrelation matrix $\mathbf{R}$ has 5 unique values corresponding to the 5 constraints

$$X(0,0)^2 + X(0,1)^2 + X(1,0)^2 + X(1,1)^2 = R(0,0)$$

$$X(0,0)X(0,1) + X(1,0)X(1,1) = R(0,1)$$

$$X(0,0)X(1,0) + X(0,1)X(1,1) = R(1,0)$$

$$X(0,0)X(1,1) = R(1,1)$$

$$X(0,1)X(1,0) = R(1,-1). \tag{25}$$

Computing these values results in

$$\mathbf{R} = \begin{pmatrix} -24 & 242 & -234 \\ -633 & 1334 & -633 \\ -234 & 242 & -24 \end{pmatrix}. \tag{26}$$

Therefore, the 2D phase retrieval problem can be stated as:

$$\text{find } \mathbf{X} = \begin{pmatrix} X(0,0) & X(0,1) \\ X(1,0) & X(1,1) \end{pmatrix}$$

subject to

$$X(0,0)^2 + X(0,1)^2 + X(1,0)^2 + X(1,1)^2 = 1334$$

$$X(0,0)X(0,1) + X(1,0)X(1,1) = -633$$

$$X(0,0)X(1,0) + X(0,1)X(1,1) = 242$$

$$X(0,0)X(1,1) = -24$$

$$X(0,1)X(1,0) = -234. \tag{27}$$

Next we show how to reformulate (27) as a 1D problem with one additional constraint using the steps described at the end of the previous section:

1) Define the vector $\mathbf{x} = \text{vec}(\mathbf{X}^T) = [X(0,0), X(0,1), X(1,0), X(1,1)]$ by vectorizing the matrix $\mathbf{X}^T$.
2) Using Proposition 1 extract the 1D autocorrelation $\mathbf{r}$ of $\mathbf{x}$ which results in

$$\mathbf{r} = [R(0,0), R(0,1) + R(1,-1), R(1,0), R(1,1)]$$

$$= [1334, -867, 242, -24]$$

for the nonnegative part of $\mathbf{r}$.

3) From Theorem 2 we can now recast the 2D phase retrieval problem as a 1D phase retrieval problem with $(N-1)^2 = 1$ additional constraints:

find $\mathbf{x}$

subject to

$$\mathbf{x} \star \mathbf{x} = [-24, 242, -867, 1334, -867, 242, -24]$$

$$x[1]x[2] = -234. \tag{28}$$

IV. AMBIGUITY REDUCTION

In Section III we established how to recast 2D phase retrieval as a 1D problem with $(N-1)^2$ additional constraints. We now show that, for almost all signals, a single constraint is sufficient to reduce the many feasible solutions of the 1D formulation to

one solution (up to trivial ambiguities). In particular, we prove the following theorem.

Theorem 3: Let $\mathbf{X}$ be a real valued $N \times N$ matrix and let $\mathbf{x} = \text{vec}(\mathbf{X}^T)$ be its row vectorized representation. Let $\mathbf{R} = \mathbf{X} \star \mathbf{X}$ be the 2D autocorrelation matrix of $\mathbf{X}$ and let $\mathbf{r} = \mathbf{x} \star \mathbf{x}$ be the 1D autocorrelation sequence of $\mathbf{x}$ defined by (14). Then the constraint $R(N-1, -(N-1)) = x[N-1]x[N^2-N]$ alone is sufficient to reduce the non-trivial ambiguities of the 1D phase retrieval problem on $\mathbf{x}$. Specifically, the solution to

find $\quad \mathbf{x}$

subject to $\mathbf{r} = \mathbf{x} \star \mathbf{x}$

$$R(N-1, -(N-1)) = x[N-1]x[N^2-N]$$

is unique for almost all vectors $\mathbf{x}$.

Theorem 2 implies that the problem of recovering a matrix $\mathbf{X}$ from the magnitude of its 2D Fourier transform can be recast as a 1D phase retrieval problem on the vector $\text{vec}(\mathbf{X}^T)$ with additional constraints. Theorem 3 proves that it is sufficient to choose the constraint $R(N-1, 1-N)$ to resolve the non-trivial ambiguities in the 1D problem on $\text{vec}(\mathbf{X}^T)$. These insights can be used to retrieve a 2D signal from its Fourier magnitude using the following four steps:

1) Extract the 1D autocorrelation $\mathbf{r} = \mathbf{x} \star \mathbf{x}$ of $\mathbf{x} = \text{vec}(\mathbf{X}^T)$ from the 2D autocorrelation $\mathbf{R}$ of the matrix $\mathbf{X}$ using (14).
2) Construct the associated polynomial (6) of $\mathbf{r}$. Using the factorization (7) and (9) find all non-trivially different vectors with autocorrelation $\mathbf{r}$.
3) Search for the vector that fulfills the constraint $R(N-1, 1-N) = x[N-1]x[N^2-n]$. Theorem 3 suggests that almost always there will be exactly one such vector.
4) Reshape the vector back into a matrix. This matrix is the unique solution to the 2D phase retrieval problem considered.

Note that the steps above have combinatorial complexity and therefore are practical primarily for small system sizes. However, they provide an analytic approach to solving 2D phase retrieval which can be of interest.

A. Proof of Theorem 3

Our derivations below rely on the results of [27] and [29].

In Theorem 2 we showed that the 2D phase retrieval problem with respect to $\mathbf{X}$ is equivalent to 1D phase retrieval of $\mathbf{x}$ with $(N-1)^2$ additional constraints. One of these constraints is on the value of $x[N-1]x[N^2-N]$ which must be equal to $R(N-1, 1-N)$. This constraint follows from substituting $i = N-1, j = 1-N$ and $\ell = (N-1)^2$ into the expression for $R(i,j)$ in the theorem. For this choice, $m = 0$ and $n = N-1$ so that the sum reduces to the single element $x[N-1]x[N^2-N]$. We now show that, for almost all signals, there is only one trivially non-different vector that fulfills this constraint.

We begin by considering the 1D problem $\mathbf{r} = \mathbf{x} \star \mathbf{x}$ where $\mathbf{x}$ has length N^2. We define the *autocorrelation vector* of $\mathbf{r}$ as the vector of zeros $\boldsymbol{\gamma} = [\gamma_1, \ldots, \gamma_{N^2-1}]$. Any autocorrelation

sequence can be uniquely defined by one of its autocorrelation vectors up to scale. In Section II-A we have seen that knowing $\mathbf{r}$ is equivalent to knowing the polynomial $P_{\mathbf{r}}(z)$ of (7) where now there are $N^2 - 1$ pairs of zeros $(\gamma_j, \overline{\gamma}_j^{-1})$. In addition, we assume that there are at most 2^{N^2-2} distinct possible ways to factor this polynomial as in (9) such that the corresponding vectors are not trivially related. Denote by $A = \{\mathbf{y}_1, \ldots, \mathbf{y}_L\}$ with $L \leq 2^{N^2-2}$ the set of all real vectors $\mathbf{y}_i \in \mathbb{R}^{N^2}$ with autocorrelation $\mathbf{r} = \mathbf{x} \star \mathbf{x}$ that are non-trivially different, and let $\mathbf{y} \in A$ be a vector with zero set $B = \{\beta_1, \ldots, \beta_{N^2-1}\}$ and associated polynomial

$$P_{\mathbf{y}}(z) = y[0] + y[1]z + \ldots + y[N^2 - 1]z^{N^2-1}$$
$$= \left[|r[N^2 - 1]| \prod_{j=1}^{N^2-1} |\beta_j|^{-1} \right]^{\frac{1}{2}} \prod_{j=1}^{N^2-1} (z - \beta_j). \quad (29)$$

We next rely on Vieta's formula [30] which relates a polynomial's coefficients to sums and products of its roots. Vieta's result then implies that

$$\frac{y[N^2 - 1 - k]}{y[N^2 - 1]} = \left(\sum_{1 \leq i_1 \leq i_2 \leq \ldots \leq i_k \leq N^2-1} \beta_{i_1} \beta_{i_2} \ldots \beta_{i_k} \right). \quad (30)$$

Choosing $k = N - 1$ leads to

$$y[N^2 - N] = y[N^2 - 1] \left(\sum_{\tilde{N}^2} \beta_{i_1} \beta_{i_2} \ldots \beta_{i_{N-1}} \right), \quad (31)$$

where $\sum_{\tilde{N}^2} = \sum_{1 \leq i_1 < i_2 < \ldots < i_{N-1} \leq N^2-1}$. Let $\mathbf{y}^{(I)}$ be the vector with associated polynomial

$$P_{\mathbf{y}^{(I)}}(z) = \left[|r[N^2 - 1]| \prod_{j=1}^{N^2-1} |\beta_j| \right]^{\frac{1}{2}} \prod_{j=1}^{N^2-1} (z - \overline{\beta}_j^{-1})$$
$$= \prod_{j=1}^{N^2-1} (-e^{i \arg \beta_j}) \left(y[N^2 - 1] + \ldots + y[0]z^{N^2-1} \right)$$
$$= (-1)^{N^2-1} \left(y[N^2 - 1] + \ldots + y[0]z^{N^2-1} \right). \quad (32)$$

In the last transition we used the fact that the coefficients of the polynomial are real and hence the roots of (32) come in conjugate pairs. The vector $\mathbf{y}^{(I)}$ is the flipped version of the vector $\mathbf{y}$ where $y^{(I)}[i] = y[N^2 - 1 - i]$.

For simplicity of notation, we assume that N is odd so that the phase factor $(-1)^{N^2-1}$ is equal $+1$. If N is even, then the treatment below is identical up to a minus sign and the conclusions remain the same. Using Vieta's formula we have for $y^{(I)}[N^2 - N] = y[N - 1]$,

$$y^{(I)}[N^2 - N] = y^{(I)}[N^2 - 1] \sum_{\tilde{N}^2} \overline{\beta}_{i_1}^{-1} \ldots \overline{\beta}_{i_{N-1}}^{-1}. \quad (33)$$

The product of (31) and (33) is given by:

$$y[N^2 - N]y[N - 1] = y[N^2 - N]y^{(I)}[N^2 - N]$$
$$= |[r[N^2 - 1]| \left(\sum_{\tilde{N}^2} \beta_{i_1} \ldots \beta_{i_{N-1}} \right) \left(\sum_{\tilde{N}^2} \overline{\beta}_{i_1}^{-1} \ldots \overline{\beta}_{i_{N-1}}^{-1} \right),$$
$$\quad (34)$$

where we used the fact that from (29) and (32),

$$y[N^2 - 1]y^{(I)}[N^2 - 1]$$
$$= \left[|r[N^2 - 1]| \prod_{j=1}^{N^2-1} |\beta_j| \right]^{\frac{1}{2}} \left[|r[N^2 - 1]| \prod_{j=1}^{N^2-1} |\beta_j|^{-1} \right]^{\frac{1}{2}}$$
$$= |r[N^2 - 1]|. \quad (35)$$

Since $\beta_i \in \{\gamma_i, \overline{\gamma}_i^{-1}\}$, the value $y[N^2 - N]y[N - 1]$ defines a function $f_{\mathbf{y}}(\gamma) = y[N - 1]y[N^2 - N]$ in the autocorrelation vector γ. Assuming $\mathbf{y}$ is real, any complex roots come in conjugate pairs. Suppose, without loss of generality, that $\mathbf{y}_1 = \mathbf{x}$ and that the zero set of $\mathbf{y}_1$ is given by $B = \{\gamma_1, \ldots, \gamma_{N^2-1}\}$. The function $f_{\mathbf{y}_1}(\gamma)$ then becomes

$$f_{\mathbf{y}_1}(\gamma) = y_1[N - 1]y_1[N^2 - N]$$
$$= |[r[N^2 - 1]| \left(\sum_{\tilde{N}^2} \gamma_{i_1} \ldots \gamma_{i_{N-1}} \right) \left(\sum_{\tilde{N}^2} \overline{\gamma}_{i_1}^{-1} \ldots \overline{\gamma}_{i_{N-1}}^{-1} \right). \quad (36)$$

Suppose that we are given a specific autocorrelation sequence γ_0 for which the signal $\mathbf{x}$ cannot be uniquely recovered up to trivial ambiguities with the additional constraint $R(N - 1, -(N - 1))$ alone. Then there exists a second solution of the form $\mathbf{y} \in A \backslash \{\mathbf{y}_1\}$ with a zero set defined by $B^{(\Gamma)}$, where

$$B^{(\Gamma)} = \begin{cases} \overline{\gamma}_j^{-1}, & \text{for } j \in \Gamma, \\ \gamma_j, & \text{otherwise} \end{cases} \quad (37)$$

and Γ is a nonzero subset of the index set $S = \{1, \ldots, N^2 - 1\}$. For this choice,

$$F_{\mathbf{y}_1, \mathbf{y}}(\gamma_0) = f_{\mathbf{y}_1}(\gamma_0) - f_{\mathbf{y}}(\gamma_0) = 0. \quad (38)$$

This implies that the number of functions $F_{\mathbf{y}_1, \mathbf{y}_i}(\gamma_0), 1 < i \leq L$ that are zero for this given autocorrelation corresponds to the number of non-trivially different solutions with the same value $R(N - 1, 1 - N)$.

Let us now define Λ as the set of all autocorrelations for which the function $F_{\mathbf{y}_1, \mathbf{y}}(\gamma)$ is zero, i.e,

$$\Lambda = \left\{ \gamma \in D \,\middle|\, F_{\mathbf{y}_1, \mathbf{y}}(\gamma) = 0 \right\}, \quad (39)$$

where D is the domain on which the function is defined (see the Appendix for more details). The following theorem, whose proof is provided in the Appendix, shows that for almost all autocorrelations the function is not zero.

Theorem 4: The zero set Λ of $F_{\mathbf{y}_1, \mathbf{y}}(\gamma)$ has measure zero.

From Theorem 4 we conclude that the probability that for a given autocorrelation (a given $\gamma \in D$) there is at least one function $F_{\mathbf{y}_1, \mathbf{y}_i}(\gamma) = 0$, $1 < i \leq L$ is zero. This shows that for almost all signals the constraint $R(N-1, -(N-1))$ alone is sufficient to guarantee uniqueness.

B. An Example

In the example in Section III we considered a simple 2×2 matrix and showed how to recast the corresponding 2D phase retrieval problem into 1D phase retrieval. The reformulated 1D problem we obtained was:

find $\mathbf{x}$

subject to

$$\mathbf{x} \star \mathbf{x} = [-24, 242, -867, 1334, -867, 242, -24]$$

$$x[1]x[2] = -234. \tag{40}$$

The solution to this problem without the additional constraint $x[1]x[2] = -234$ can be found by considering the associated polynomial of the autocorrelation sequence (6) and its factorization (7):

$$P_{\mathbf{r}}(z) = \sum_{n=0}^{6} r[n - N^2 + 1]z^n$$

$$= -24 + 242z - 633z^2 + 1334z^3 - 633z^4 + 242z^5 - 24z^6$$

$$= -24(z-2)(z-3)(z-4)(z-1/2)(z-1/3)(z-1/4). \tag{41}$$

The autocorrelation vector of $\mathbf{r}$ is given by $\gamma_0 = [2, 3, 4]$.

There are $2^{4-1} = 8$ different vectors with autocorrelation $\mathbf{r}$ (up to global phase and a shift) which can be found by considering all associated polynomials with zero sets $B = \{\beta_1, \beta_2, \beta_3\}$ where $\beta_1 \in \{2, 1/2\}$, $\beta_2 \in \{3, 1/3\}$, $\beta_3 \in \{4, 1/4\}$. Using (9), the associated polynomials are given by:

$$P_{\mathbf{y}_1}(z) = -24 + 26z^2 - 9z + z^3$$

$$P_{\mathbf{y}_2}(z) = -6 + 29z - 21z^2 + 4z^3$$

$$P_{\mathbf{y}_3}(z) = -8 + 30z - 19z^2 + 3z^3$$

$$P_{\mathbf{y}_4}(z) = -2 + 15z - 31z^2 + 12z^3$$

$$P_{\mathbf{y}_5}(z) = -12 + 31z - 15z^2 + 2z^3$$

$$P_{\mathbf{y}_6}(z) = -3 + 19z - 30z^2 + 8z^3$$

$$P_{\mathbf{y}_7}(z) = -4 + 21z - 29z^2 + 6z^3$$

$$P_{\mathbf{y}_8}(z) = -1 + 9z - 26z^2 + 24z^3. \tag{42}$$

Solutions $\mathbf{y}_{8,\ldots,5}$ are just a flipped version of $\mathbf{y}_{1,\ldots,4}$ (times-1) and are therefore trivially different. We conclude that the phase retrieval problem has $2^{4-2} = 4$ non-trivially different solutions

(a) The vector $\mathbf{v}_1$.   (b) The vector $\mathbf{v}_2$.

(c) The vector $\mathbf{v}_3$.   (d) The vector $\mathbf{v}_4$.
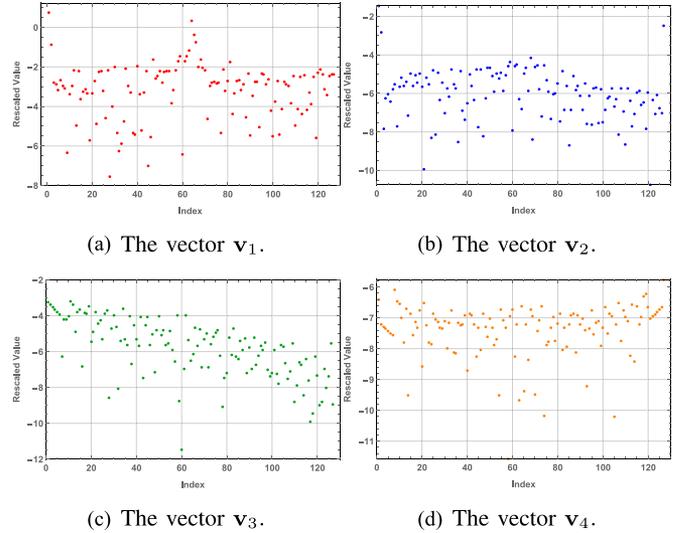
Fig. 1. The vectors $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_4$. Since all values are finite each one of the additional constraints guarantees uniqueness.

given by

$$\begin{pmatrix} \mathbf{y}_1 \\ \mathbf{y}_2 \\ \mathbf{y}_3 \\ \mathbf{y}_4 \end{pmatrix} = \begin{pmatrix} -24 & 26 & -9 & 1 \\ -6 & 29 & -21 & 4 \\ -8 & 30 & -19 & 3 \\ -2 & 15 & -31 & 12 \end{pmatrix}. \tag{43}$$

The additional constraint in (40) states that $x[1]x[2] = -234$. It is easy to see that only the vector $\mathbf{y}_1$ satisfies this constraint. Therefore, this vector uniquely solves (40). By reshaping $\mathbf{y}_1$ into its matrix form we conclude that the unique solution to (40) is

$$\mathbf{X} = \begin{pmatrix} -24 & 26 \\ -9 & 1 \end{pmatrix}. \tag{44}$$

C. Extensions

In our derivation of Theorem 3 we considered the specific constraint $R(N-1, -(N-1))$. We chose this constraint since it involves only two elements of the vector $\mathbf{x}$ and is therefore simple to work with. However, in random simulations, the conclusions appear to hold true for any of the other $(N-1)^2$ constraints, as we now demonstrate. We randomly generated 100 valid autocorrelation vectors (specifically, we randomly generated 100 1D vectors $\mathbf{r}$) of lengths 17, 31 and 49. We achieve this by first generating 100 random vectors with corresponding lengths of 9, 16 and 25, and then computing their corresponding autocorrelation sequences. We check the values of the additional constraints in (22) for each of the non-trivially different vectors that share the same autocorrelation sequence. For all the autocorrelation sequences we tested, the constraints of each non-trivially different vector had a unique value.

In Fig. 1 we consider the case in which $N = 3$. The equivalent 1D problem has dimension $N^2 = 9$. We consider one of the randomly generated autocorrelation sequences we tested. There are

$2^{N^2-2} = 128$ non-trivially different vectors $\mathbf{y}_i$, $0 \leq i \leq 127$ that share this autocorrelation sequence. For $N = 3$ the additional constraints in Theorem 2 are given by:

$$R_i(1, -2) = y_i[2]y_i[3] + y_i[5]y_i[6]$$

$$R_i(1, -1) = y_i[1]y_i[3] + y_i[2]y_i[4] + y_i[4]y_i[6] + y_i[5]y_i[7]$$

$$R_i(2, -2) = y_i[2]y_i[6]$$

$$R_i(2, -1) = y_i[1]y_i[6] + y_i[2]y_i[7]. \tag{45}$$

We define the vectors d_1, d_2, d_3, d_4 with elements $d_1[i] = c_1 R_{\ell_1(i)}(1, -2)$, $d_2[i] = c_2 R_{\ell_2(i)}(1, -1)$, $d_3[i] = c_3 R_{\ell_3(i)}(2, -2)$ and $d_4[i] = c_4 R_{\ell_4(i)}(2, -1)$ for $0 \leq i \leq 127$, so that the $\ell_j(i)$ $(1 \leq j \leq 4)$ are injective mappings from the index set $0 \leq i \leq 127$ to the same index set. The mappings are defined in such a way, that the vectors $\mathbf{d}_j$ are ordered in ascending order (i.e $d_j[i] < d_j[i+1]$ for all relevant i, j). The constants c_j are defined such that $d_j[127] = 1$ for $1 \leq j \leq 4$. In Fig. 1 we plot the vector $\mathbf{v}_j$ where $v_j[i] = \log(d_j[i+1] - d_j[i])$ for $0 \leq i \leq 126$ and for $1 \leq j \leq 4$. Clearly the entries of $\mathbf{d}_j$ have distinct values. Therefore, prior knowledge on the value of one of the additional constraints in (45) guarantees uniqueness in these examples.

V. CONCLUSION

In this work we considered 2D phase retrieval and showed that it can be restated as a 1D phase retrieval problem with additional constraints. We then proved that one additional constraint is sufficient to reduce the many feasible solutions of the complementary 1D phase retrieval problem to a single solution for almost all 2D cases. This approach can be used to obtain an explicit solution for almost all 2D phase retrieval problems.

APPENDIX

In this appendix we prove Theorem 4. In particular, we show that the zero set of $F_{\mathbf{y}_1, \mathbf{y}}(\boldsymbol{\gamma})$ has measure zero.

As a first step, we prove the following proposition.

Proposition 5: The function $F_{\mathbf{y}_1, \mathbf{y}}(\boldsymbol{\gamma}) = f_{\mathbf{y}_1}(\boldsymbol{\gamma}) - f_{\mathbf{y}}(\boldsymbol{\gamma})$ is not the zero function.

Proof: Let $\mathbf{y}$ be the vector set $B^{(\Gamma)}$ defined in (37) and $S = \{1, \ldots, N^2 - 1\}$. To show that $F_{\mathbf{y}_1, \mathbf{y}}(\boldsymbol{\gamma})$ is not the zero function it is enough to show that it is not zero at a single point. Select one index $i_1 \in S \backslash \Gamma$ and one index $i_2 \in \Gamma$, and consider the autocorrelation defined by $\tilde{\gamma}_{i_1} = \alpha$, $\tilde{\gamma}_{i_2}^{-1} = \alpha$ and $\tilde{\gamma}_i = 1$ for $i \in S \backslash \{i_1, i_2\}$ where we choose $\alpha \gg 1$. Using simple combinatorics it can be shown that up to a phase factor

$$f_{\mathbf{y}_1}(\tilde{\gamma}) = \alpha^2 \left[\binom{N^2 - 3}{N - 2}^2 + \mathcal{O}(\alpha^{-1}) \right], \tag{46}$$

and

$$f_{\mathbf{y}}(\tilde{\gamma}) = \alpha^2 \left[\binom{N^2 - 3}{N - 3} \binom{N^2 - 3}{N - 1} + \mathcal{O}(\alpha^{-1}) \right]. \tag{47}$$

For $\alpha \gg 1$ we have

$$f_{\mathbf{y}_1}(\tilde{\gamma}) - f_{\mathbf{y}}(\tilde{\gamma})$$

$$= \binom{N^2 - 3}{N - 2}^2 \left[1 - \left(\frac{N - 2}{N^2 - N} \right) \left(\frac{N^2 - N - 1}{N - 1} \right) \right] \alpha^2. \tag{48}$$

Since $\left(\frac{N-2}{N-1} \right) \left(\frac{N^2-N-1}{N^2-N} \right) \neq 1$ the above expression is not zero and therefore the function $F_{\mathbf{y}_1, \mathbf{y}}(\boldsymbol{\gamma})$ is not identically zero. ∎

We now analyze the function $f_{\mathbf{y}}(\boldsymbol{\gamma})$. The domain and the image of this function are defined such that $f_{\mathbf{y}} : \mathbb{C}^{N^2-1} \backslash G \to \mathbb{C}$ where G is the set for which $\gamma_i = 0$ for at least one $i \in \{1, \ldots, N^2 - 1\}$. If we instead define $\boldsymbol{\gamma} = [\Re\gamma_1, \Im\gamma_1, \ldots, \Re\gamma_{N^2-1}, \Im\gamma_{N^2-1}]$ then $f_{\mathbf{y}} : \mathbb{R}^{2(N^2-1)} \backslash G \to \mathbb{C}$.

We restrict ourselves to real vectors so that any complex roots γ_i appear in conjugate pairs. Thus, we may define a set of functions, that represent the function $f_{\mathbf{y}}(\boldsymbol{\gamma})$, that are defined as $f_{\mathbf{y}, n} : \mathbb{R}^{N^2-1} \backslash G \to \mathbb{R}$ with $0 \leq n \leq \lfloor (N^2 - 1)/2 \rfloor$ where n denotes the number of pairs of the roots that are not real valued. To understand how, we provide a simple example. Consider the case $N = 2$. The function $f_{\mathbf{y}_1}(\boldsymbol{\gamma})$ is then given by (up to a global phase factor):

$$f_{\mathbf{y}_1}(\boldsymbol{\gamma}) = r[3] (\gamma_1 + \gamma_2 + \gamma_3) \left(\bar{\gamma}_1^{-1} + \bar{\gamma}_2^{-1} + \bar{\gamma}_3^{-1} \right). \tag{49}$$

In this case the number of pairs of complex roots can either be $n = 0$ or $n = 1$. If $n = 1$ then we must have $\gamma_2 = \bar{\gamma}_1$. Expressing each root in terms of its real and complex part we have $\gamma_j = a_j + ib_j$, $1 \leq j \leq 3$ and the vector of variables becomes $\mathbf{d} = [a_1, b_1, a_3]$. The function takes the form

$$f_{\mathbf{y}_1, 1}(\mathbf{d}) = r[3] \frac{2a_1 b_1^2 + a_3 b_1^2 + 2a_1^3 + 5a_3 a_1^2 + 2a_3^2 a_1}{a_3 (a_1^2 + b_1^2)}. \tag{50}$$

On the other hand if all the roots are real we have $b_j = 0$, $1 \leq j \leq 3$ and the requirement that $\gamma_2 = \bar{\gamma}_1$ no longer needs to be fulfilled. The vector $\boldsymbol{\gamma}$ becomes $\mathbf{d} = [a_1, a_2, a_3]$ and the function takes the form

$$f_{\mathbf{y}_1, 0}(\mathbf{d}) = r[3] \frac{(a_1 + a_2 + a_3)(a_2 a_3 + a_1 (a_2 + a_3))}{a_1 a_2 a_3}. \tag{51}$$

For this case the function $f_{\mathbf{y}_1}(\boldsymbol{\gamma})$ which is defined on $\mathbb{C}^6 \backslash G$ can be fully represented by the two functions $f_{\mathbf{y}_1, 0}(\mathbf{d})$ and $f_{\mathbf{y}_1, 1}(\mathbf{d})$ that are defined on $\mathbb{R}^3 \backslash G$.

For our problem the function $F_{\mathbf{y}_1, \mathbf{y}}^{(n)}(\mathbf{d}) : f_{\mathbf{y}_1, n}(\mathbf{d}) - f_{\mathbf{y}, n}(\mathbf{d})$ where $\mathbf{d} \in \mathbb{R}^{N^2-1}$ can be written as

$$F_{\mathbf{y}_1, \mathbf{y}}^{(n)}(\mathbf{d}) = \frac{g_1(\mathbf{d})}{g_2(\mathbf{d})} \tag{52}$$

where $g_1(\mathbf{d})$ and $g_2(\mathbf{d})$ are some multivariate polynomials with real coefficients in $\mathbf{d}$. The zero set V_n of $F_{\mathbf{y}_1, \mathbf{y}}^{(n)}(\mathbf{d})$ is defined as

$V_n = \{\mathbf{d} \in \mathbb{R}^{N^2-1} \setminus G \,|\, F_{\mathbf{y}_1,\mathbf{y}}^{(n)}(\mathbf{d}) = 0\}$. The zero set of $g_1(\mathbf{d})$ is given by $W = \{\mathbf{v} \in \mathbb{R}^{N^2-1} \,|\, g_1(\mathbf{v}) = 0\}$. Since $g_1(\mathbf{d})$ is a real analytic function, which is not the zero function (as shown in Proposition 5), and is defined on an open and connected set, the equation $g_1(\mathbf{d}) = 0$ defines a hyperplane on the real space $\mathbb{R}^{N^2-1}$ and its zero set is therefore of measure zero. For a rigorous proof the reader is referred to [31, corollary 10, p.9] for complex valued analytical functions and [32] for real valued analytical functions. The function $F_{\mathbf{y}_1,\mathbf{y}}^{(n)}(\mathbf{d})$ is zero if and only if $g_1(\mathbf{d})$ is zero so that $V_n \subseteq W$. Since W is a set of measure zero, so is V_n. The zero set Λ of the function $F_{\mathbf{y}_1,\mathbf{y}}(\boldsymbol{\gamma})$ is given by the union of all zero sets V_n,

$$\Lambda = \bigcup_{i=1}^{\lfloor (N^2-1)/2 \rfloor} V_i. \tag{53}$$

A countable union of sets of measure zero is still measure zero and thus Λ defines a set of measure zero over the domain of $F_{\mathbf{y}_1,\mathbf{y}}(\boldsymbol{\gamma})$.

References

[1] A. L. Paterson, "A fourier series method for the determination of the components of interatomic distances in crystals," *Phys. Rev.*, vol. 46, no. 5, pp. 372–376, 1934.

[2] A. L. Paterson, "Ambiguities in the X-ray analysis of crystal structures," *Phys. Rev.*, vol. 65, nos. 5/6, 1944, Art. no. 195.

[3] A. Walther, "The question of phase retrieval in optics," *J. Modern Opt.*, vol. 10, no. 1, pp. 41–49, 1963.

[4] R. P. Millane, "Phase retrieval in crystallography and optics," *J. Opt. Soc. Amer. A*, vol. 7, no. 3, pp. 394–411, 1990.

[5] C. Fienup and J. Dainty, "Phase retrieval and image reconstruction for astronomy," in *Image Recovery: Theory and Application*. New York, NY, USA: Academic, 1987, pp. 231–275.

[6] M. Stefik, "Inferring dna structures from segmentation data," *Artif. Intell.*, vol. 11, no. 1, pp. 85–114, 1978.

[7] L. Rabiner and B.-H. Juang, *Fundamentals of Speech Recognition*. Upper Saddle River, NJ, USA: Prentice-Hall, 1993.

[8] K. Jaganathan, Y. C. Eldar, and B. Hassibi, "Phase retrieval: An overview of recent developments," in *Opt. Compressive Sens.*, 2016, arxiv: 1510.07713.

[9] Y. Shechtman, Y. C. Eldar, O. Cohen, H. N. Chapman, J. Miao, and M. Segev, "Phase retrieval with application to optical imaging: A contemporary overview," *IEEE Signal Process. Mag.*, vol. 32, no. 3, pp. 87–109, May 2015.

[10] M. H. Hayes, "The reconstruction of a multidimensional sequence from the phase or magnitude of its fourier transform," *IEEE Trans. Acoust., Speech, Signal Process.*, vol. ASSP-30, no. 2, pp. 140–154, Apr. 1982.

[11] R. Bates, "Fourier phase problems are uniquely solvable in mute than one dimension. I: Underlying theory," *Optik (Stuttgart)*, vol. 61, pp. 247–262, 1982.

[12] Y. M. Bruck and L. Sodin, "On the ambiguity of the image reconstruction problem," *Opt. Commun.*, vol. 30, no. 3, pp. 304–308, 1979.

[13] E. M. Hofstetter, "Construction of time-limited functions with specified autocorrelation functions," *IEEE Trans. Inf. Theory*, vol. IT-10, no. 2, pp. 119–126, Apr. 1964.

[14] K. Huang, Y. C. Eldar, and N. Sidiropoulos, "Phase retrieval from 1D Fourier measurements: Convexity, uniqueness, and algorithms," *IEEE Trans. Signal Process.*, vol. 64, no. 23, pp. 6105–6117, Dec. 2016.

[15] 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. Amer. A*, vol. 19, no. 7, pp. 1334–1345, 2002.

[16] R. W. Gerchberg, "A practical algorithm for the determination of phase from image and diffraction plane pictures," *Optik*, vol. 35, 1972, Art. no. 237.

[17] J. R. Fienup, "Reconstruction of an object from the modulus of its Fourier transform," *Opt. Lett.*, vol. 3, no. 1, pp. 27–29, 1978.

[18] N. Streibl, "Phase imaging by the transport equation of intensity," *Opt. Commun.*, vol. 49, no. 1, pp. 6–10, 1984.

[19] J. R. Fienup, "Phase retrieval algorithms: A comparison," *Appl. Opt.*, vol. 21, no. 15, pp. 2758–2769, 1982.

[20] Y. Shechtman, Y. C. Eldar, A. Szameit, and M. Segev, "Sparsity based sub-wavelength imaging with partially incoherent light via quadratic compressed sensing," *Opt. Express*, vol. 19, no. 16, pp. 14807–14822, 2011.

[21] E. J. Candes, Y. C. Eldar, T. Strohmer, and V. Voroninski, "Phase retrieval via matrix completion," *SIAM Rev.*, vol. 57, no. 2, pp. 225–251, 2015.

[22] I. Waldspurger, A. d'Aspremont, and S. Mallat, "Phase recovery, Max-Cut and complex semidefinite programming," *Math. Program.*, vol. 149, nos. 1/2, pp. 47–81, 2015.

[23] E. J. Candes, X. Li, and M. Soltanolkotabi, "Phase retrieval via Wirtinger flow: Theory and algorithms," *IEEE Trans. Inf. Theory*, vol. 61, no. 4, pp. 1985–2007, Apr. 2015.

[24] G. Wang, G. B. Giannakis, and Y. C. Eldar, "Solving systems of random quadratic equations via truncated amplitude flow," 2016, arXiv:1605.08285.

[25] A. Beck and Y. C. Eldar, "Sparsity constrained nonlinear optimization: Optimality conditions and algorithms," *SIAM Optim.*, vol. 23, no. 3, pp. 1480–1509, Oct. 2013.

[26] Y. Shechtman, A. Beck, and Y. C. Eldar, "GESPAR: Efficient phase retrieval of sparse signals," *IEEE Trans. Signal Process.*, vol. 62, no. 4, pp. 928–938, Feb. 2014.

[27] R. Beinert and G. Plonka, "Ambiguities in one-dimensional discrete phase retrieval from fourier magnitudes," *J. Fourier Anal. Appl.*, vol. 21, no. 6, pp. 1169–1198, 2015.

[28] M. H. Hayes and J. H. McClellan, "Reducible polynomials in more than one variable," *Proc. IEEE*, vol. 70, no. 2, pp. 197–198, Feb. 1982.

[29] R. Beinert and G. Plonka, "Enforcing uniqueness in one-dimensional phase retrieval by additional signal information in time domain," 2016, arXiv:1604.04493.

[30] M. Hazewinkel, "Viète theorem," in *Encyclopedia of Mathematics*. New York, NY, USA: Springer, 2001.

[31] R. C. Gunning and H. Rossi, *Analytic Functions of Several Complex Variables*. Providence, RI, USA: Amer. Math. Soc., 2009, vol. 368.

[32] B. Mityagin, "The zero set of a real analytic function," 2015, arXiv:1512.07276.

Dani Kogan received the B.Sc. degree from Ben-Gurion University, Be'er Sheva, Israel, in 2014, and the M.Sc. degree from the Weizmann Institute of Science, Rehovot, Israel, in 2016, both in physics.

Yonina C. Eldar (S'98–M'02–SM'07–F'12) received the B.Sc. degree in physics and the B.Sc. degree in electrical engineering both from Tel-Aviv University (TAU), Tel-Aviv, Israel, in 1995 and 1996, respectively, and the Ph.D. degree in electrical engineering and computer science from the Massachusetts Institute of Technology (MIT), Cambridge, MA, USA, in 2002. From January 2002 to July 2002, she was a Postdoctoral Fellow at the Digital Signal Processing Group at MIT. She is currently a Professor in the Department of Electrical Engineering at the Technion, Israel Institute of Technology, Haifa, Israel, where she holds the Edwards Chair in Engineering. She is also a Research Affiliate with the Research Laboratory of Electronics at MIT and was a Visiting Professor at Stanford University, Stanford, CA, USA. Her research interests include the broad areas of statistical signal processing, sampling theory and compressed sensing, optimization methods, and their applications to biology and optics. She is author of the book *Sampling Theory: Beyond Bandlimited Systems* (Cambridge University Press) and the co-author of the books *Compressed Sensing* (Cambridge University Press) and *Convex Optimization Methods in Signal Processing and Communications* (Cambridge University Press).

She received many awards for excellence in research and teaching, including the IEEE Signal Processing Society Technical Achievement Award (2013), the IEEE/AESS Fred Nathanson Memorial Radar Award (2014), and the IEEE Kiyo Tomiyasu Award (2016). She was a Horev Fellow of the Leaders in Science and Technology program at the Technion and an Alon Fellow. She received the Michael Bruno Memorial Award from the Rothschild Foundation, the Weizmann Prize for Exact Sciences, the Wolf Foundation Krill Prize for Excellence in Scientific Research, the Henry Taub Prize for Excellence in Research (twice), the Hershel Rich Innovation Award (three times), the Award for Women with Distinguished Contributions, the Andre and Bella Meyer Lectureship, the Career Development Chair at the Technion, the Muriel & David Jacknow Award for Excellence in Teaching, and the Technions Award for Excellence in Teaching (two times). She received several best paper awards and best demo awards together with her research students and colleagues and was selected as one of the 50 most influential women in Israel. She is a member of the Young Israel Academy of Science and Humanities and the Israel Committee for Higher Education. She is the Editor-in-Chief of Foundations and Trends in Signal Processing, serves on several IEEE committees. She served as an Associate Editor of IEEE TRANSACTIONS ON SIGNAL PROCESSING, the *EURASIP Journal of Signal Processing*, the *SIAM Journal on Matrix Analysis and Applications*, and the *SIAM Journal on Imaging Sciences*.

Dan Oron received his B.Sc. in physics and mathematics from the Hebrew University of Jerusalem, Jerusalem, Israel, in 1994, the M.Sc. degree in physics in hydrodynamic instability from Ben-Gurion, Beer sheva, Israel, in 1998, and his Ph.D. in physics from the Weizmann Institute of Science on ultrafast phenomena (2005). Following postdoctoral studies in the Hebrew University of Jerusalem he joined the department of Physics of Complex System at the Weizmann Institute, where he is currently a professor and serves as department head. His research focuses on the development of novel imaging modalities and on the optical properties of colloidal nanocrystals.