UNIVERSITY OF CALIFORNIA, SAN DIEGO

General Phase Retrieval with Locally Supported Measurements

A dissertation submitted in partial satisfaction of the requirements for the degree

Doctorate of Philosophy

in

Mathematics with Specialization in Computational Science

by

Brian P. Preskitt

Committee in charge:

Professor Rayan Saab, Chair
Professor Kamalika Chaudhuri
Professor Todd Kemp
Professor Jiawang Nie
Professor Yoav Freund

2018

The dissertation of Brian P. Preskitt is approved:

Chair

University of California, San Diego

2018

DEDICATION

This dissertation is lovingly dedicated to my brother, Charles Preskitt.

EPIGRAPH

For in much wisdom is much vexation, and he who increases knowledge increases sorrow. – Ecclesiastes 1:18

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGEMENTS

First and foremost, I would like to thank my advisor Rayan Saab for all of his involvement in my academic career. In my first year of graduate school, it was his class on compressed sensing that convinced me to switch into the computational math track, which in turn is where I found the material and the problems that motivated me to continue in academic research. Since then, his support – in our many hours of teamwork at the whiteboard; his connections to problems, authors, conferences, and collaborators; and the simple things such as critiques of my writing and talks – was uniquely indispensable in shaping the environment in which I found my place as a researcher. I am immensely thankful for the inspiration of his talent and energetic leadership.

I would also like to thank Mark Iwen and Aditya Viswanathan, our two co-authors and collaborators on the subjects covered in this thesis. The ground that they broke on this new strain of phase retrieval proved to be incredibly fruitful, and I am thankful for being welcomed as a contributor to their ongoing research efforts. This partnership was foundational to my beginnings in research and much of my subsequent progress, and I am deeply indebted to their generous spirit of academic camaraderie. Chapter **??** section **??**, in full, is a reprint of material published with Iwen and Viswanathan as submitted to Applied and Computational Harmonic Analysis 2018. Chapter **??** section **??**, in part, is a reprint of material published with these authors in the Proceedings of SPIE vol. 10394, 2017.

VITA

2013	Bachelor of Science, Texas Christian University
2013-2018	Teaching Assistant, University of California, San Diego
2015	Master of Science, University of California, San Diego
2016-2017	Associate Instructor, University of California, San Diego
2018	Doctor of Philosophy, University of California, San Diego

PUBLICATIONS

M. Iwen, B. Preskitt, R. Saab, and A. Viswanathan. *An Eigenvector-Based Angular Synchronization Method for Phase Retrieval from Local Correlation Measurements*. arXiv:1612.01182. Submitted for publication Aug. 2017.

M. Iwen, B. Preskitt, R. Saab, and A. Viswanathan. *Phase retrieval from local measurements in two dimensions*. Proceedings of SPIE 10394, Wavelets and Sparsity XVII, San Diego, CA, 2017.

FIELDS OF STUDY

Major Field: Mathematics with Specialization in Computational Sciences
Studies in Signal Processing
Professor Rayan Saab

ABSTRACT

General Phase Retrieval with Locally Supported Measurements

by

Brian P. Preskitt

Doctorate of Philosophy in Mathematics with Specialization in Computational Science

University of California, San Diego, 2018

Professor Rayan Saab, Chair

In this dissertation, we study a new approach to the problem of phase retrieval, which is the task of reconstructing a complex-valued signal from magnitude-only measurements. This problem occurs naturally in several specialized imaging applications such as electron microscopy and X-ray crystallography. Although solutions were first proposed for this problem as early as the 1970s, these algorithms have lacked theoretical guarantees of success, and phase retrieval has suffered from a considerable gap between practice and theory for almost the entire history of its study.

A common technique in fields that use phase retrieval is that of *ptychography*, where

measurements are collected by only illuminating small sections of the sample at any time. We refer to measurements designed in this way as *local measurements*, and in this dissertation, we develop and expand the theory for solving phase retrieval in measurement regimes of this kind. Our first contribution is a basic model for this setup in the case of a one-dimensional signal, along with an algorithm that robustly solves phase retrieval under this model. This work is unique in many ways that represent substantial improvements over previously existing solutions: perhaps most significantly, our model uses a deterministic measurement scheme, and our recovery algorithm is the first to have a solution that may be stated in exact arithmetic. These advantages constitute major progress towards producing theoretical results for phase retrieval that are directly usable in laboratory settings.

Chapter 1 conducts a survey of the history of phase retrieval and its applications. Chapter 2 reviews the mathematical literature on the subject, including the first solutions and the theoretical work of the last decade. Chapter 3 presents co-authored results defining and establishing the setting and solution of the base model explored in this dissertation. Chapter 4 expands the theory on what measurement schemes are admissible in our model, including an analysis of conditioning and runtime. Chapter 5 explores results that bring our model nearer to the actual practice of ptychography. Chapter 6 includes a few relevant results that may be used for future expansion on this topic.

Chapter 1

History of Phase Retrieval

1.1 Notation

- Indices of matrices in $\mathbb{C}^{d\times d}$ and vectors in $\mathbb{C}^d$ are always taken modulo d.
- For $k \in \mathbb{N}, n \in \mathbb{Z}, [k]_n = \{n, n+1, \dots, n+k-1\}$ and $[k] = [k]_1$.
- $S_d \in \mathbb{R}^{d\times d}$ is the $d \times d$ shift operator, such that $(S_d x)_i = x_{i-1}$. Typically we imply the subscript by context, writing S.
- $R \in \mathbb{R}^{d\times d}$ is the operator that reverses a vector's entries, leaving the first entry fixed. Namely, $(Rx)_i = x_{2-i}$.
- Given $x \in \mathbb{C}^d$ and $k \in [d], \mathrm{circ}_k(x) \in \mathbb{C}^{d\times k}$ denotes the first k columns of the circulant matrix whose first column is x. In particular, $\mathrm{circ}_k(x)e_i = S^{i-1}x$ for $i \in [k]$. When the subscript is omitted, $\mathrm{circ}(x) = \mathrm{circ}_d(x)$.
- $\omega_d := \mathrm{e}^{\frac{2\pi\mathrm{i}}{d}}$ is the d^{th} root of unity. When context permits, d is implied and we use just ω.

- For $i, n \in \mathbb{N}, e_i^n \in \mathbb{R}^n$ is the i^{th} column of the $n \times n$ identity matrix. When context permits, n is implied and we write e_i. In particular, whenever e_i is used in a matrix multiplication, n is taken to be appropriate so that the multiplication is legal.

- For $k \in \mathbb{Z}, F_k \in \mathbb{C}^{k \times k}$ is the $k \times k$ unitary Fourier matrix with $(F_k)_{ij} = \frac{1}{\sqrt{k}} \omega_k^{(i-1)(j-1)}$.

- For $m, n \in \mathbb{N}, f_n^m = F_m e_n$ is the n^{th} column of the $m \times m$ unitary Fourier matrix, where $e_n \in \mathbb{R}^m$ has its index taken modulo m.

- Given $x, y \in \mathbb{C}^d, x \circ y$ denotes the Hadamard/elementwise product of x and y; specifically $(x \circ y)_i = x_i y_i$.

- Given $A \in \mathbb{C}^{d \times d}, \operatorname{diag}(A, m) \in \mathbb{C}^d$ denotes the m^{th} circulant off-diagonal of A. That is, $\operatorname{diag}(A, m)_i = A_{i,i+m}$.

- Given $x \in \mathbb{C}^d, \operatorname{diag}(x) \in \mathbb{C}^{d \times d}$ is the diagonal matrix whose diagonal entries are the entries of x. Namely, $\operatorname{diag}(x) e_i = x_i e_i$. When the intention is clear from context, we may write $D_x := \operatorname{diag}(x)$.

- $\mathcal{H}^d$ is the set of Hermitian matrices in $\mathbb{C}^{d \times d}$, to be viewed as a d^2-dimensional vector space over $\mathbb{R}$.

- $\mathcal{R}_d : \bigcup_{k=1}^{\infty} \mathbb{C}^k \to \mathbb{C}^d$ is a resize mapping, where for $v \in \mathbb{C}^k$ and $i \in [d]$,

$$\mathcal{R}_d(v)_i = \begin{cases} v_i, & i \leq k \\ 0, & \text{otherwise} \end{cases} \quad \text{for } i \in [d].$$

  Similarly, $\mathcal{R}_{m \times n} : \bigcup_{k_1, k_2}^{\infty} \mathbb{C}^{k_1 \times k_2} \to \mathbb{C}^{m \times n}$ truncates or zero-pads matrices to size $m \times n$.

- Given $k, d \in \mathbb{N}$, we define the operator $T_k : \mathbb{C}^{d\times d} \to \mathbb{C}^{d\times d}$ by

$$T_k(A)_{ij} = \begin{cases} A_{ij}, & |i-j| \mod d < k \\ 0, & \text{otherwise.} \end{cases}$$

  Note that T_k is simply the orthogonal projection operator onto its range $T_k(\mathbb{C}^{d\times d})$. We use T_k interchangeably to refer to both the operator and its range.

1.2 Introduction

Phase retrieval is the problem of solving a system of equations of the form

$$y = |Ax_0|^2 + \eta, \tag{1.1}$$

where $x_0 \in \mathbb{C}^d$ is the objective signal, $A \in \mathbb{C}^{D\times d}$ is a known measurement matrix, $\eta \in \mathbb{R}^D$ is an unknown perturbation vector, and $y \in \mathbb{R}^D$ is the vector of measurement data. $|\cdot|^2$ represents the component-wise magnitude squared operation; i.e. for any $n \in \mathbb{N}$ we have $|\mathbf{v}|_j^2 = |\mathbf{v}_j|^2$ for all $\mathbf{v} \in \mathbb{C}^n$. In phase retrieval, the goal is to recover an estimate of x_0 from knowledge of y and A. We sometimes rephrase the system (1.1) as

$$y_j = |\langle a_j, x_0\rangle|^2 + \eta_j, \tag{1.2}$$

where a_j^* stand for the rows of A and are referred to as the measurement vectors. The name *phase retrieval* comes from viewing the $|\cdot|^2$ operation as erasing the phases of the complex-valued measurements $\langle a_j, x_0\rangle$ and leaving only their magnitudes; solving for x_0 may be considered as a way of retrieving this phase information. We immediately note that this problem contains an unavoidable phase ambiguity, in the sense that, for any solution x and any $\theta \in [0, 2\pi)$, we will have that $\mathrm{e}^{\mathrm{i}\theta}$ is also a solution.

The phase retrieval's problem earliest, and arguably most famous, application is that of x-ray crystallography.

Much of the literature devoted to the phase problem

multiple wavelength anomalous diffraction Jerome Karle

Chapter 2

Applications

One common technique used to generate redundancy in phase retrieval-type measurements is to design a system that illuminates only a small part of the sample at a time. These "partial snapshots" are then positioned along an overlapping grid, which produces the redundancy. The overlap is necessary since, even if you could solve phase retrieval perfectly on each patch, each of these patches would have their own phase ambiguities; these would need to be synchronized to achieve a single, coherent image of the original sample. Usually, ptychography is performed by taking a single *mask* or *illumination function* with small supprt, say $\mathbf{m} \in \mathbb{C}^d$ with $\operatorname{supp}(m) \subseteq [\delta]$ where $\delta \ll d$ and shifting this mask to different positions relative to the sample. These measurements may then be modelled as

$$\mathbf{y}_{\ell,j} = |\mathcal{F}(S^{\ell}\mathbf{m} \circ \mathbf{x})_j|^2 + \eta_{\ell,j} = |\langle f_j \circ \mathbf{m}, \mathbf{x} \rangle|^2 + \eta_{\ell,j}. \tag{2.1}$$

This technique is the inspiration for our model, where we do not require our measurements to take this exact form.

Chapter 3

Our Model

Here we consider the phase retrieval problem as modelled in (2.1).

Chapter 4

Spanning Masks

In this chapter, we consider when a local measurement system $\{m_j\}_{j=1}^K$ composes a *spanning family* of masks.

Definition 1. We say that $\{m_j\}_{j=1}^K \subseteq \mathbb{C}^d$ is a *local measurement system* or *family of masks* of support δ if $1 \in \operatorname{supp}(m_j)$ and $\operatorname{supp}(m_j) \subseteq [\delta]$ for each j.

Definition 2. We say that a family of masks $\{m_j\}_{j=1}^K \subseteq \mathbb{C}^d$ of support δ is a *spanning family* if $\operatorname{span}\{S^\ell m_j m_j^* S^{-\ell}\}_{(\ell,j)\in[d]_0\times[K]} = T_\delta(\mathcal{H}^d)$.

4.1 Conditions for a spanning family

Proposition 1. *Suppose that $\gamma \in \mathbb{R}^d$ has $1 \in \operatorname{supp}(\gamma) = [\delta]$. Set $D = \min\{2\delta - 1, d\}$, take $K \geq 2\delta - 1$ and let*

$$\begin{aligned} v_j &= \sqrt{K}\mathcal{R}_d(F_K e_j) \\ v_j^D &= \sqrt{K}\mathcal{R}_D(F_K e_j) \end{aligned} \quad, \quad j \in [D],\ 2\delta - 1 \leq K.$$

Define a local measurement system $\{m_j\}_{j\in[D]}$ by setting $m_j = \gamma \circ v_j$. Then $\{m_j\}_{j\in[D]}$ is a spanning family if and only if all the sets $J_k := \{m \in [\delta]_0 :$

$(F_d(\gamma \circ S^{-m}\gamma))_k \neq 0\}$, *for all* $k \in [d]$ *satisfy*

$$\begin{cases} 2|J_k| - 1 \geq D, & 0 \in J_k \\ 2|J_k| \geq D, & \text{otherwise} \end{cases}.$$

The proof will make use of the following lemmas.

Lemma 1. *Define* $w_j = \mathcal{R}_{N_1}(f_j^{N_2}), j \in [N_2]$ *and set*

$$\rho_j = \mathfrak{Re}(w_j) \quad \text{and} \quad \mu_j = \mathfrak{Im}(w_j)$$

to be vectors containing the real and imaginary components of w_j. *Then for* $1 \leq \ell_1 < \cdots < \ell_k \leq \frac{N_2+1}{2}$ *with* $k \leq N_1$, *we have*

$$\begin{aligned} \dim \operatorname{span}\{w_{\ell_i}, w_{2-\ell_i}\}_{i=1}^k &= \dim \operatorname{span}\{\rho_{\ell_i}, \mu_{\ell_i}\}_{i=1}^k \\ &= \begin{cases} 2k-1, & \ell_1 = 1 \\ 2k, & \text{otherwise} \end{cases}, \end{aligned}$$

where the indices are taken modulo N_2.

Proof of lemma 1. The first equality is clear by considering that $w_{2-i} = \overline{w_i}$, so $\rho_k = \frac{1}{2}(w_i + w_{2-i})$ and $\mu_i = -\frac{i}{2}(w_i - w_{2-i})$. We set $M = \dim \operatorname{span}\{w_{\ell_i}, w_{2-\ell_i}\}_{i=1}^k$ to be the common dimension of the two spaces under consideration.

We now divide into two cases: if $N_1 < N_2$, then $\{w_j\}_{j \in [N_2]}$ is full spark, as any $N_1 \times N_1$ submatrix of $\begin{bmatrix} w_1 & \cdots & w_{N_2} \end{bmatrix}$ will be a Vandermonde matrix of the form

$$V = \frac{1}{\sqrt{N_2}} \begin{bmatrix} w_{\ell_1} & \cdots & w_{\ell_{N_1}} \end{bmatrix}$$

with determinant

$$N_2^{-N_1/2} \prod_{1 \leq i < j \leq N_1} (\omega_{N_2}^{\ell_i - 1} - \omega_{N_2}^{\ell_j - 1}),$$

which is immediately non-zero since $\omega_{N_2}^{\ell_i - 1} - \omega_{N_2}^{\ell_j - 1} = 0$ only when $\ell_i - \ell_j = 0 \mod N_2$, which cannot happen when $N_1 < N_2$.

When $N_1 \geq N_2, \{w_j\}_{j\in[N_2]}$ is linearly independent, since its members form the matrix $\begin{bmatrix} F_{N_2} \\ 0_{N_1-N_2\times N_2} \end{bmatrix}$.

In either case, M is equal to the cardinality of $\{\ell_i, 2-\ell_i\}_{i=1}^k$, which has $2k-1$ elements if and only if $\ell_1 = 1$; otherwise it has $2k$. We remark that a collision where $\ell_i = (2-\ell_i \mod N_2) = N_2/2+1$ is precluded since we have asserted $\ell_i \leq \frac{N_2+1}{2}$.

□

Lemma 2. *For $v \in \mathbb{R}^d$, we have*

$$\operatorname{circ}(v)\rho_k^d = \frac{1}{2}\mathfrak{Re}((Fv)_k f_k^d) \tag{4.1}$$

$$\operatorname{circ}(v)\mu_k^d = \frac{1}{2}\mathfrak{Im}((Fv)_k f_k^d). \tag{4.2}$$

In particular, if $(Fv)_k \neq 0$ and $k \notin \{1, \frac{d}{2}+1\}$, then $\rho_k^d, \mu_k^d \notin \operatorname{Nul}(\operatorname{circ}(v))$; if $k \in \{1, \frac{d}{2}+1\}$, then $\rho_k^d \notin \operatorname{Nul}(\operatorname{circ}(v))$ and $\mu_k^d = 0$. On the other hand, if $(Fv)_k = 0$, then $\rho_k^d, \mu_k^d \in \operatorname{Nul}(\operatorname{circ}(v))$.

Proof of lemma 2. We set $\lambda_k^d = (Fv)_k$, and recalling that $\operatorname{circ}(v) = F\operatorname{diag}(Fv)F^*$, we observe that

$$\begin{aligned}\operatorname{circ}(v)\mu_k^d = \operatorname{circ}(v)\frac{1}{2}(f_k^d + f_{2-k}^d) &= \frac{1}{2}(\operatorname{circ}(v)f_k^d + \operatorname{circ}(v)f_{2-k}^d) \\ &= \frac{1}{2}(\lambda_k^d f_k^d + \lambda_{2-k}^d f_{2-k}^d).\end{aligned}$$

(4.1) follows immediately since $\lambda_k^d = \overline{\lambda_{2-k}^d}$ when $v \in \mathbb{R}^D$. (4.2) follows from an analogous calculation.

If $\lambda_k^d \neq 0$ and $k \notin \{1, \frac{d}{2}+1\}$, then ω_d^{k-1} is a non-real root of unity and there exists some j such that $\mathfrak{Re}(\omega_d^{(j-1)(k-1)}\lambda_k^d) \neq 0$, and similarly for $\mathfrak{Im}(\omega_d^{(j-1)(k-1)}\lambda_k^d) \neq 0$. When $k \in \{1, \frac{d}{2}+1\}, \omega_d^{(k-1)} \in \mathbb{R}$ so $\mu_k^d = 0$, but $\lambda_k^d \in \mathbb{R}$ in this case (because $v \in \mathbb{R}^d$), so $\operatorname{circ}(v)\rho_k^d = \lambda_k^d\rho_k^d \neq 0$. The claim concerning the case of $\lambda_k^d = 0$ is immediate from (4.1) and (4.2). □

Proof of proposition 1. For this proof, we set

$$
\begin{aligned}
(\rho_k^d, \mu_k^d) &= (\mathfrak{Re}(f_k^d), \mathfrak{Im}(f_k^d)) \\
(\rho_k, \mu_k) &= (\mathfrak{Re}(v_k), \mathfrak{Im}(v_k)) \\
(\rho_k^D, \mu_k^D) &= (\mathfrak{Re}(v_k^D), \mathfrak{Im}(v_k^D))
\end{aligned}
$$

We consider the conditions under which a linear combination of the matrices

$$B_\gamma := \{S^\ell m_j m_j^* S^{-\ell}\}_{(\ell,j)\in[d]\times[D]}$$

can be equal to zero; by a basic dimension count, $\{m_j\}_{j\in[D]}$ is a spanning family if and only if B_γ is linearly independent. To this end, we define the operator $\mathcal{A}^* : \mathbb{R}^{d\times D} \to \mathbb{C}^{d\times d}$ by

$$\mathcal{A}^*(C) = \sum_{\ell\in[d],j\in[D]} C_{\ell,j} S^\ell m_j m_j^* S^{-\ell} \tag{4.3}$$

and begin with the observation that, for any $A \in \mathbb{C}^{d\times d}$ we have

$$\operatorname{diag}(S^\ell A S^{-\ell}, m) = S^\ell \operatorname{diag}(A, m).$$

We then have

$$
\begin{aligned}
& \sum_{j\in[D],\ell\in[d]} C_{\ell,j} S^\ell m_j m_j^* S^{-\ell} = 0 \\
\iff & \operatorname{diag}\left(\sum_{j\in[D],\ell\in[d]} C_{\ell,j} S^\ell m_j m_j^* S^{-\ell}, m\right) = 0 \quad \text{for all } m \in [\delta]_0 \\
\iff & \sum_{j\in[D],\ell\in[d]} C_{\ell,j} \operatorname{diag}(S^\ell m_j m_j^* S^{-\ell}, m) = 0 \quad \text{for all } m \in [\delta]_0 \\
\iff & \sum_{j\in[D],\ell\in[d]} C_{\ell,j} S^\ell \operatorname{diag}(m_j m_j^*, m) = 0 \quad \text{for all } m \in [\delta]_0
\end{aligned}
$$

At this point, we consider that

$$\operatorname{diag}(m_j m_j^*, m) = \operatorname{diag}((\gamma \circ v_j)(\gamma \circ v_j)^*, m) = \operatorname{diag}(D_{v_j} \gamma\gamma^* D_{\overline{v_j}}, m) \tag{4.4}$$

$$= \omega_K^{m(j-1)} \operatorname{diag}(\gamma\gamma^*, m). \tag{4.5}$$

We now set $g_m := \operatorname{diag}(\gamma\gamma^*, m) = \gamma \circ S^{-m}\gamma$ and proceed with the previous chain of implications:

$$\begin{aligned}
& \sum_{j\in[D],\ell\in[d]} C_{\ell,j} S^\ell \operatorname{diag}(m_j m_j^*, m) = 0 \quad \text{for all } m \in [\delta]_0 \\
\iff \quad & \sum_{j\in[D],\ell\in[d]} C_{\ell,j} S^\ell (\omega_K^{m(j-1)} g_m) = 0 \quad \text{for all } m \in [\delta]_0 \\
\iff \quad & \sum_{j\in[D],\ell\in[d]} C_{\ell,j} \omega_K^{m(j-1)} S^\ell g_m = 0 \quad \text{for all } m \in [\delta]_0 \\
\iff \quad & \operatorname{circ}(g_m) C\, v_{m+1}^D = 0 \quad \text{for all } m \in [\delta]_0
\end{aligned}$$

We now recall that any circulant matrix $\operatorname{circ}(v)$ is diagonalized by the Discrete Fourier Matrix, such that, for $v \in \mathbb{C}^d$,

$$\operatorname{circ}(v) = F_d \operatorname{diag}(\sqrt{d} F_d v) F_d^* = \sqrt{d} \sum_{j=1}^d (F_d v)_j f_j^d (f_j^d)^*.$$

By writing $\lambda_k^m = \sqrt{d}(F g_m)_k$, we get a natural decoupling of the previous equations: for a fixed m, we have that $\operatorname{circ}(g_m) C f_{m+1} = 0$ if and only if

$$\sum_{k=1}^d \lambda_k^m f_k^d (f_k^d)^* C\, f_{m+1} = \sum_{k=1}^d (\lambda_k^m (f_k^d)^* C\, f_{m+1}) f_k^d = 0.$$

Since this last expression is a linear combination of an orthonormal basis, it occurs only when $\lambda_k^m (f_k^d)^* C\, f_{m+1} = 0$ for all $k \in [d]$. We collect these equations over $m \in [\delta]_0$, considering the definition of J_k and that $g_m \in \mathbb{R}^d$ implies $\lambda_k^m = 0 \iff \lambda_{2-k}^m = 0$ to restate this condition as $\begin{bmatrix} f_k^d & f_{2-k}^d \end{bmatrix}^* C v_{m+1}^D = 0$ for all $k \in [d], m \in J_k$. Since $\operatorname{span}\{f_k^d, f_{2-k}^d\} = \operatorname{span}\{\rho_k^d, \mu_k^d\}$, we further restate this as $\begin{bmatrix} \rho_k^d & \mu_k^d \end{bmatrix}^* C v_{m+1}^D = 0$ for all $k \in [d], m \in J_k$; setting $W_k = C^* \begin{bmatrix} \rho_k^d & \mu_k^d \end{bmatrix} \in \mathbb{R}^{D\times 2}$, we now get that $\mathcal{A}^*(C) = 0 \iff \operatorname{Col}(W_k) \subseteq \{v_{m+1}^D\}_{m\in J_k}^\perp \cap \mathbb{R}^D$ for all $k \in [d]$.

We now claim that $\mathcal{A}^*$ is invertible if and only if the subspaces $\{v_{m+1}^D\}_{m\in J_k}^{\perp} \cap \mathbb{R}^D$ are all trivial. Indeed, if we fix a k and have some non-zero $u \in \{v_{m+1}^D\}_{m\in J_k}^{\perp} \cap \mathbb{R}^D$, then we may set $C = \rho_k^d u^*$, such that

$$\mathrm{circ}(g_m) C v_{m+1}^D = (\mathrm{circ}(g_m)\rho_k^d)(u^* v_{m+1}^D).$$

For $m \in J_k, u^* v_{m+1}^D = 0$ by hypothesis on u, and for $m \notin J_k, \mathrm{circ}(g_m)\rho_k^d = 0$ by definition of J_k and lemma 2.

For the other direction, assume $\{v_{m+1}^D\}_{m\in J_k}^{\perp} \cap \mathbb{R}^D = 0$ for each $k \in [d]$. Then $\mathcal{A}^*(C) = 0 \iff \mathrm{Col}(W_k) = \{0\} \iff W_k = 0$ for all k. However, $\{\rho_k^d\}_{k\in[d]} \cup \{\mu_k^d\}_{k\in[d]\setminus\{1,\frac{d}{2}+1\}}$ is an orthogonal basis for $\mathbb{R}^d$, so

$$\begin{aligned} W_k &= 0 \quad \text{for all } k \in [d] \\ \iff \quad C^*\rho_k^d = C^*\mu_k^d &= 0 \quad \text{for all } k \in [d] \\ \iff \quad C &= 0 \end{aligned}$$

We complete the proof by considering that, for $u \in \mathbb{R}^D, \langle v_j^D, u\rangle = 0$ if and only if $\langle \rho_j^D, v\rangle = \langle \mu_j, v\rangle = 0$, so

$$\{v_{m+1}\}_{m\in J_k}^{\perp} \cap \mathbb{R}^D = \{\rho_{m+1}, \mu_{m+1}\}_{m\in J_k}^{\perp}$$

which has dimension $\max\{D - (2|J_k| - \mathbb{1}_{0\in J_k}), 0\}$ by lemma 1. Therefore, $\mathcal{A}^*$ is invertible if and only if $2|J_k| - \mathbb{1}_{0\in J_k} \leq D$ for all $k \in [d]$, as claimed. $\square$

Remark. It turns out that this condition is generic, in the sense that it fails to hold only on a subset of $\mathbb{R}^d$ with Lebesgue measure zero. We consider that the set of $\gamma \in \mathbb{R}^d$ giving at least one zero in $F(\gamma \circ S^{-m}\gamma)$ is a finite union of zero sets of non-trivial quadratic polynomials (except when $2 \mid d, \delta \geq d/2$, and $m = d/2$, discussed below) and hence a set of zero measure; therefore, $J_k = [\delta]_0$ for all γ outside a set of measure zero and B_γ is linearly independent under generic conditions.

To address the case of $m = d/2$, we first remark that this is the only possible exception: indeed, when $m \neq d/2$, we have that

$$F((e_1 + e_{m+1}) \circ S^m(e_1 + e_{m+1}))_k = f_k^* e_{m+1} = \omega^{m(k-1)},$$

so $\gamma \to F(\gamma \circ S^m \gamma)_k$ is a non-zero, homogeneous quadratic polynomial and therefore has a zero locus of measure zero.

However, when $d = 2m$, then $\gamma \circ S^m \gamma$ is periodic with period m and $F(\gamma \circ S^m \gamma)_{2i} = 0$ for $i \in [m]_0$. In particular, if $\delta \geq m$, then $D = d$ and $m \notin J_{2i}$ for all $i \in [m]_0$ for any γ. In particular, $|J_2| \leq \delta - 1$ and $2|J_2| - \mathbb{1}_{0 \in J_2} \leq 2\delta - 3$, so if $\delta \in \{d/2, d/2+1\}$, all choices of γ automatically fail to produce a spanning family.

This exception is quite pathological, though: since our intention is to have $\delta \ll d$, this will rarely be an impediment. Nonetheless, in the case that you *do* want to have $\operatorname{span} B_\gamma = \mathcal{H}^d$, then taking $\delta > d/2 + 1$ gives some space for the condition $2|J_k| - \mathbb{1}_{0 \in J_k}$, and we again have that generic γ will produce spanning families.

4.2 Condition number

$$\begin{aligned} \mathcal{A} &: \mathbb{C}^{d \times d} \to \mathbb{R}^{[d] \times [D]} \\ \mathcal{A}(X)_{(\ell, j)} &= \langle S^\ell m_j m_j^* S^{-\ell}, X \rangle \end{aligned} \tag{4.6}$$

Now that we have characterized this collection of spanning families, we are interested in the condition number for solving the linear system $y = \mathcal{A}(T_\delta(xx^*)) + \eta$ to estimate $T_\delta(xx^*)$. We begin by introducing the main result of this section:

Proposition 2. *Accept the hypotheses of proposition 1 and define $\mathcal{A}$ as in* (4.6). *If we additionally assume that $2\delta - 1 \leq d$ and $K = 2\delta - 1$, then the condition* *number of $\mathcal{A}$ is*

$$\kappa(\mathcal{A}) = \frac{\max\limits_{m\in[\delta]_0, j\in[d]} |F_d(\gamma \circ S^{-m}\gamma)_j|}{\min\limits_{m\in[\delta]_0, j\in[d]} |F_d(\gamma \circ S^{-m}\gamma)_j|}. \tag{4.7}$$

Otherwise, we may bound the condition number by

$$\kappa(\mathcal{A}) \leq \frac{\max\limits_{m\in[\delta]_0, j\in[d]} |F_d(\gamma \circ S^{-m}\gamma)_j|}{\min\limits_{m\in[\delta]_0, j\in[d]} |F_d(\gamma \circ S^{-m}\gamma)_j|} \kappa(\overline{F}_K), \tag{4.8}$$

where $\overline{F}_K \in \mathbb{C}^{D\times D}$ is the $D \times D$ principal submatrix of F_K.

To accomplish this, we introduce the operators $P^{(d,N)} : \mathbb{C}^{dN} \to \mathbb{C}^{dN}$, each of which is a permutation defined by

$$(P^{(d,N)}v)_{(i-1)N+j} = v_{(j-1)d+i}.$$

We can view this is beginning with $v \in C^{dN}$ written as N blocks of d entries, and interleaving them into d blocks each of N entries. Additionally, for $k, N_1, N_2 \in \mathbb{N}, v \in \mathbb{C}^{kN_1}$, and $H \in \mathbb{C}^{kN_1\times N_2}$, we define circ^{N_1} by

$$\begin{aligned} \mathrm{circ}^{N_1}(v) &= \begin{bmatrix} v & S_{kN_1}^{N_1} v & \cdots & S_{kN_1}^{(k-1)N_1} v \end{bmatrix} \\ \mathrm{circ}^{N_1}(H) &= \begin{bmatrix} H & S_{kN_1}^{N_1} H & \cdots & S_{kN_1}^{(k-1)N_1} H \end{bmatrix}. \end{aligned}$$

We now proceed with the following lemmas.

Lemma 3. *Suppose $v_i, v_{ij} \in \mathbb{C}^k, w_j \in \mathbb{C}^{kN_1}$ for $i \in [N_1], j \in [N_2]$ and*

$$M_1 = \begin{bmatrix} \mathrm{circ}(v_1) \\ \vdots \\ \mathrm{circ}(v_{N_1}) \end{bmatrix}, \quad M_2 = \begin{bmatrix} \mathrm{circ}^{N_1}(w_1) & \cdots & \mathrm{circ}^{N_1}(w_{N_2}) \end{bmatrix}, \text{ and}$$

$$M_3 = \begin{bmatrix} \mathrm{circ}(v_{11}) & \cdots & \mathrm{circ}(v_{1N_2}) \\ \vdots & \ddots & \vdots \\ \mathrm{circ}(v_{N_11}) & \cdots & \mathrm{circ}(v_{N_1N_2}) \end{bmatrix}.$$

Then

$$P^{(k,N_1)}M_1 = \mathrm{circ}^{N_1}\left(P^{(k,N_1)}\begin{bmatrix} v_1 \\ \vdots \\ v_{N_1}\end{bmatrix}\right) \tag{4.9}$$

$$M_2P^{(k,N_2)*} = \mathrm{circ}^{N_1}\left(\begin{bmatrix} w_1 & \cdots & w_{N_2}\end{bmatrix}\right) \tag{4.10}$$

$$P^{(k,N_1)}M_3P^{(k,N_2)*} = \mathrm{circ}^{N_1}\left(P^{(k,N_1)}\begin{bmatrix} v_{11} & \cdots & v_{1N_2} \\ \vdots & \ddots & \vdots \\ v_{N_11} & \cdots & v_{N_1N_2}\end{bmatrix}\right). \tag{4.11}$$

Proof of lemma 3. We index the matrices to check the equalities. For (4.9), we have

$$\begin{aligned}(P^{(k,N_1)}M_1)_{(a-1)N_1+b,j} &= (M_1)_{(b-1)k+a,j} \\ &= \begin{bmatrix} S^{j-1}v_1 \\ \vdots \\ S^{j-1}v_{N_1}\end{bmatrix}_{(b-1)k+a} \\ &= (S^{j-1}v_b)_a = (v_b)_{a+j-1}\end{aligned}$$

and

$$\begin{aligned}\mathrm{circ}^{N_1}\left(P^{(k,N_1)}\begin{bmatrix} v_1 \\ \vdots \\ v_{N_1}\end{bmatrix}\right)_{(a-1)N_1+b,j} &= \left(P^{(k,N_1)}\begin{bmatrix} v_1 \\ \vdots \\ v_{N_1}\end{bmatrix}\right)_{(a-1)N_1+b+(j-1)N_1} \\ &= (v_b)_{a+j-1}\end{aligned}$$

For (4.10), we have

$$(P^{(k,N_2)}M_2^*)_{(a-1)N_2+b,j} = (M_2)_{j,(b-1)k+a} = (w_b)_{j+(a-1)N_1}$$

and

$$\left(\mathrm{circ}^{N_1}\left(\begin{bmatrix} w_1 & \cdots & w_{N_2}\end{bmatrix}\right)\right)_{j,(a-1)N_2+b} = (S^{N_1(a-1)}w_b)_j = (w_b)_{j+N_1(a-1)}$$

(4.11) follows immediately by combining (4.9) and (4.10). $\square$

Lemma 4. *Suppose* $V \in C^{kN\times m}$*, then* $\mathrm{circ}^N(V)$ *is block diagonalizable by*

$$\mathrm{circ}^N(V) = (F_k \otimes I_N)\,(\mathrm{diag}(M_1, \dots, M_k))\,(F_k \otimes I_m)^*,$$

where

$$\sqrt{k}\,(F_k \otimes I_N)^*\,V = \begin{bmatrix} M_1 \\ \vdots \\ M_k \end{bmatrix}, \quad \text{or} \quad M_j = \sqrt{k}(f_j^k \otimes I_N)^* V$$

Proof of lemma 4. We set V_i to be the $k\times m$ blocks of V such that $V^* = \begin{bmatrix} V_1^* & \cdots & V_k^* \end{bmatrix}$ and begin by observing that, for $u \in \mathbb{C}^k$ and $W \in \mathbb{C}^{m\times p}$, the ℓ^{th} $k \times p$ block of $\mathrm{circ}^N(V)(u \otimes W)$ is given by

$$\left(\mathrm{circ}^N(V)(u \otimes W)\right)_\ell = \sum_{i=1}^k u_i (S^{N(i-1)} V)_\ell W = \sum_{i=1}^k u_i V_{\ell-i+1} W.$$

Taking $u = f_j^k$ and $W = I_m$, this gives

$$\begin{aligned}
\left(\mathrm{circ}^N(V)(f_j^k \otimes I_m)\right)_\ell &= \frac{1}{\sqrt{k}} \sum_{i=1}^k \omega_k^{(j-1)(i-1)} V_{\ell-i+1} I_m \\
&= \frac{1}{\sqrt{k}} \omega_k^{(j-1)(\ell-1)} \sum_{i=1}^k \omega_k^{-(j-1)(i-1)} V_i \\
&= (f_j^k)_\ell \left(\sqrt{k}(f_j^k \otimes I_N)^* V\right) = (f_j^k)_\ell M_j.
\end{aligned}$$

This relation is equivalent to having

$$\mathrm{circ}^N(V)(f_j^k \otimes I_m) = (f_j^k \otimes M_j) = (f_j^k \otimes I_N) M_j,$$

which is the statement of the lemma. $\square$

Lemma 4 immediately gives the following corollary.

Corollary 1. *With notation as in lemma 4, the condition number of* $\operatorname{circ}^N(V)$ *is*

$$\frac{\max_{i\in[k]} \sigma_{\max}(M_i)}{\min_{i\in[k]} \sigma_{\min}(M_i)}.$$

We now consider the rows of the measurement operator $\mathcal{A}$ defined in (4.6). For now, we assume $2\delta-1 \le d$, and we vectorize $X \in T_\delta(\mathbb{C}^{d\times d})$ by its diagonals, taking $\chi_m = \operatorname{diag}(X, m), m \in [2\delta-1]_{1-\delta}$, and for now we set $g_m^j = \operatorname{diag}(m_j m_j^*, m)$, for now omitting the assumption that $m_j = \gamma \circ v_j$ as in proposition 1. Therefore, each measurement looks like

$$\begin{aligned} \mathcal{A}(X)_{(\ell,j)} &= \langle S^\ell m_j m_j^* S^{-\ell}, X\rangle \\ &= \sum_{m=1-\delta}^{\delta-1} \langle S^\ell g_m^j, \chi_m\rangle, \end{aligned}$$

so if we define the matrix $A \in \mathbb{C}^{dD\times(2\delta-1)d}$ such that

$$\left(A \begin{bmatrix} \chi_{1-\delta} \\ \vdots \\ \chi_{\delta-1} \end{bmatrix}\right)_{(j-1)d+\ell} = \mathcal{A}(X)_{(\ell,j)}, \tag{4.12}$$

the $(j-1)d+\ell^{\text{th}}$ row of A is given by

$$\begin{bmatrix} S^\ell g_{1-\delta}^j \\ \vdots \\ S^\ell g_{\delta-1}^j \end{bmatrix}^*,$$

such that A is the block matrix given by

$$A = \begin{bmatrix} \operatorname{circ}(g_{1-\delta}^1)^* & \cdots & \operatorname{circ}(g_{\delta-1}^1)^* \\ \vdots & \ddots & \vdots \\ \operatorname{circ}(g_{1-\delta}^D)^* & \cdots & \operatorname{circ}(g_{\delta-1}^D)^* \end{bmatrix} = \begin{bmatrix} \operatorname{circ}(Rg_{1-\delta}^1) & \cdots & \operatorname{circ}(Rg_{\delta-1}^1) \\ \vdots & \ddots & \vdots \\ \operatorname{circ}(Rg_{1-\delta}^D) & \cdots & \operatorname{circ}(Rg_{\delta-1}^D) \end{bmatrix},$$

which may be transformed, by Lemma 3, to

$$P^{(d,D)} A P^{(d,2\delta-1)*} = \operatorname{circ}^D\left(P^{(d,D)} \begin{bmatrix} Rg_{1-\delta}^1 & \cdots & Rg_{\delta-1}^1 \\ \vdots & \ddots & \vdots \\ Rg_{1-\delta}^D & \cdots & Rg_{\delta-1}^D \end{bmatrix}\right) =: \operatorname{circ}^D(H). \tag{4.13}$$

Quoting corollary 1, this establishes the next proposition.

Proposition 3. *Setting $M_j = \sqrt{d}\left(f_j^d \otimes I_D\right)^* H$, the condition number of A is*

$$\kappa(A) = \frac{\max\limits_{i\in[d]} \sigma_{\max}(M_i)}{\min\limits_{i\in[d]} \sigma_{\min}(M_i)}.$$

We are now able to prove proposition 2.

Proof. For the moment, we assert that $D = 2\delta - 1 \leq d$ and set $\overline{F}_K \in \mathbb{C}^{2\delta-1\times 2\delta-1}$, $(\overline{F}_K)_{ij} = \frac{1}{\sqrt{K}}\omega_K^{(i-1)(j-\delta)}$ to be the principal submatrix of $\sqrt{K}\,\mathrm{diag}(f_{1-\delta}^K)F_K$. In this case, $g_m^j = \mathrm{diag}(m_j m_j^*, m) = \omega_K^{m(j-1)} g_m$, as in (4.5). Therefore, we label the $2\delta-1\times 2\delta-1$ blocks of H by $H^* = \begin{bmatrix} H_1^* & \cdots & H_d^* \end{bmatrix}$, so that

$$(H_\ell)_{ij} = (Rg_{j-\delta}^i)_\ell = \omega_K^{(i-1)(j-\delta)}(Rg_{j-\delta})_\ell$$

and $M_\ell = \sum_{k=1}^d \omega_d^{(\ell-1)(k-1)} H_k$, giving

$$\begin{aligned}(M_\ell)_{ij} &= \sum_{k=1}^d \omega_d^{(\ell-1)(k-1)}(H_k)_{ij} = \omega_K^{(i-1)(j-\delta)} \sum_{k=1}^d \omega_d^{(\ell-1)(k-1)}(Rg_{j-\delta})_k \\ &= \omega_K^{(i-1)(j-\delta)}(F_d^* g_{j-\delta})_\ell.\end{aligned}$$

In other words, $M_\ell = \sqrt{K}\,\mathrm{diag}(f_\ell^{d*} g_{1-\delta}, \ldots, f_\ell^{d*} g_{\delta-1})\overline{F}_K$. If $K = 2\delta - 1$, then $\overline{F}_K$ is unitary, and the singular values of M_ℓ are $\{\sqrt{K} f_\ell^{d*} g_j\}_{j=1-\delta}^{\delta-1}$. Recognizing that $S^j g_j = g_{-j}$, then proposition 3 takes us to (4.7).

If $D = 2\delta - 1 < K$, then the argument remains unchanged, except that the singular values of M_ℓ, instead of being known explicitly, are bounded above and below by $\max\limits_{|j|<\delta} |f_\ell^{d*} g_j| \sigma_{\max}(\overline{F}_K)$ and $\min\limits_{|j|<\delta} |f_\ell^{d*} g_j| \sigma_{\min}(\overline{F}_K)$ respectively, which gives the more general result of (4.8).

If $2\delta - 1 > d$, then instead of using diagonals $1 - \delta, \ldots, \delta - 1$, we use diagonals $0, 1, \ldots, d - 1$. This change propagates from (4.12) to (4.13), so that

$$(H_\ell)_{ij} = \omega_K^{(i-1)(j-1)}(Rg_{j-1})_\ell \quad \text{and} \quad (M_\ell)_{ij} = \omega_K^{(i-1)(j-1)}(F_d^* g_{j-1})_\ell,$$

giving $M_\ell = \sqrt{K}\,\mathrm{diag}(f_\ell^{d*} g_0, \ldots, f_\ell^{d*} g_{d-1})\mathcal{R}_{d\times d}(F_K)$, which immediately gives us (4.8). We remark that indexing only over the diagonals $m \in [\delta]_0$ in (4.8) suffices, again because $S^j g_j = g_{-j}$, so having $2\delta - 1 > d$ makes $1-\delta, \ldots, -1$ redundant.

$\square$

Chapter 5

Ptychographic Model

In our model for the ptychographic setup of (2.1), we assume that measurements are taken corresponding to all shifts $\ell \in [d]_0$. Unfortunately, in practice, this is usually an impossibility, since in many cases an illumination of the sample can cause damage to the sample, and applying the illumination beam (which can be highly irradiative) repeatedly at a single point can destory the sample. In usual ptychography, the beam is shifted by a far larger distance than the width of a single pixel – instead of overlapping on $\delta - 1$ of δ pixels, adjacent illumination regions will typically overlap on a percentage of their support on the order of 50% or even less. Considering the risks to the sample and the costs of operating the measurement equipment, there are strong incentives to reduce the number of illuminations applied to any object, and therefore our theory ought to address a model that reflects this concern.

In particular, instead of taking all d shifts in $[d]$, we hope to use only $\ell \in k[d/k]_0$, where k is an integer divisor of d.

Chapter 6

Novelty Results

In this chapter, we produce some fun results.

Appendix A

Sample Appendix

If you seek a pleasant appendix, look no further.