SIAM J. MATH. DATA SCI.
Vol. 2, No. 3, pp. 809–839

Toward a Mathematical Theory of the Crystallographic Phase Retrieval Problem[*]

Tamir Bendory[†] and Dan Edidin[‡]

Abstract. Motivated by the X-ray crystallography technology to determine the atomic structure of biological molecules, we study the crystallographic phase retrieval problem, arguably the leading and hardest phase retrieval setup. This problem entails recovering a K-sparse signal of length N from its Fourier magnitude or, equivalently, from its periodic autocorrelation. Specifically, this work focuses on the fundamental question of uniqueness: what is the maximal sparsity level K/N that allows unique mapping between a signal and its Fourier magnitude, up to intrinsic symmetries. We design a systemic computational technique to affirm uniqueness for any specific pair (K, N), and establish the following conjecture: the Fourier magnitude determines a generic signal uniquely, up to intrinsic symmetries, as long as $K/N \leq 1/2$. Based on group-theoretic considerations and an additional computational technique, we formulate a second conjecture: if $K/N < 1/2$, then for any signal the set of solutions to the crystallographic phase retrieval problem has measure zero in the set of all signals with a given Fourier magnitude. Together, these conjectures constitute the first attempt to establish a mathematical theory for the crystallographic phase retrieval problem.

Key words. phase retrieval, X-ray crystallography, sparsity, symmetry group

AMS subject classifications. 94A12, 15A29, 15A63, 13P25

DOI. 10.1137/20M132136X

1. Introduction.

1.1. Problem formulation.

The *crystallographic phase retrieval problem* entails recovering a K-sparse signal $x_0 \in \mathbb{R}^N$ from its Fourier magnitude

$$y_0 = |Fx_0|, \tag{1.1}$$

where $F \in \mathbb{C}^{N\times N}$ is the discrete-time Fourier (DFT) matrix, and the absolute value is taken entrywise. The problem can be equivalently formulated as recovering x_0 from its *periodic autocorrelation*:

$$a_{x_0}[\ell] = \sum_{i=0}^{N-1} x_0[i]x_0[(i+\ell) \bmod N], \tag{1.2}$$

since $Fa_{x_0} = |Fx_0|^2$.

[*] Received by the editors February 24, 2020; accepted for publication (in revised form) July 14, 2020; published electronically September 15, 2020.
https://doi.org/10.1137/20M132136X
Funding: The first author was partially supported by the NSF-BSF award 2019752, and the Zimin Institute for Engineering Solutions Advancing Better Lives. The second author was partially supported by Simons Collaboration Grant 315460.

[†] School of Electrical Engineering, Tel Aviv University, Tel Aviv, Israel (bendory@tauex.tau.ac.il).
[‡] Department of Mathematics, University of Missouri, Columbia, MO 65211 USA (edidind@missouri.edu).

A useful interpretation of the crystallographic phase retrieval problem is as a feasibility problem of finding the intersection of two nonconvex sets

$$x_0 \in \mathcal{B} \cap \mathcal{S}. \tag{1.3}$$

Here, the set $\mathcal{B}$ describes all signals with the given Fourier magnitude

$$\mathcal{B} := \{x : y_0 = |Fx|\} \tag{1.4}$$

or, equivalently, with the same periodic autocorrelation

$$\mathcal{B} := \{x : a_x[\ell] = a_{x_0}[\ell] \quad \text{for all} \quad \ell = 0, \dots, N-1\}.$$

The set $\mathcal{S}$ consists of all signals with at most K nonzero value entries, that is, all signals for which the support set

$$S = \{n : x[n] \neq 0\} \subseteq [0, N-1], \tag{1.5}$$

obey $|S| \leq K$. Importantly, since the Fourier magnitude and the sparsity level of the signal remain unchanged under sign change, circular shift, and reflection, the signal can be recovered only up to these three *intrinsic symmetries*. A rigorous definition of the group of intrinsic symmetries—occasionally referred to as trivial ambiguities in the phase retrieval literature—is provided in section 4.1.1.

The main objective of this paper is to characterize the sparsity level K/N that allows unique mapping, up to intrinsic symmetries, between a signal and its periodic autocorrelation. In other words, the sparsity level, under which the periodic autocorrelation mapping $x \mapsto a_x$, is injective. For general signals, it is not difficult to bound K/N from above. To this end, we note that the periodic autocorrelation is invariant under reflection, namely, $a_x[i] = a_x[N-i]$. The set of vectors with support set contained in S is a K-dimensional linear subspace L_S and thus the periodic autocorrelation is a quadratic function $L_S \to \mathbb{R}^{\lfloor N/2 \rfloor + 1}$. Therefore, by counting dimensions, we do not expect to be able to obtain unique recovery unless $K \leq \lfloor N/2 \rfloor + 1$, even if the support S is known. This simple argument establishes a necessary condition on K; Conjecture 2.1, formulated in section 2, states that this is also a sufficient condition for uniqueness if the signal is generic.

1.2. X-ray crystallography.

This work is motivated by X-ray crystallography—a prevalent technology for determining the 3-dimensional atomic structure of molecules [49]: nearly 50,000 new crystal structures are added each year to the Cambridge Structural Database, the world's repository for crystal structures [1]. While the crystallographic problem is the leading (and arguably the hardest) phase retrieval problem, its mathematical characterizations have not been analyzed thoroughly so far.

The mathematical model of X-ray crystallography is introduced and discussed at length in [26]. For completeness, we provide a concise summary. In X-ray crystallography, the signal is the electron density function of the crystal—a periodic arrangement of a repeating, compactly supported unit

$$x_c(t) = \sum_{s \in S} x(t-s), \tag{1.6}$$

where x is the repeated motif and S is a large, but finite, subset of a lattice $\Lambda \subset \mathbb{R}^D$; the dimension D is usually two or three. The crystal is illuminated with a beam of X-rays producing a diffraction pattern, which is equivalent to the magnitude of the Fourier transform of the crystal:

$$\begin{aligned}|\hat{x}_c(k)|^2 &= \left|\int_{\mathbb{R}^D} x_c(t)e^{-\iota\langle t,k\rangle}dt\right|^2\\ &= \left|\int_{\mathbb{R}^D}\sum_{s\in S} x(t-s)e^{-\iota\langle t,k\rangle}dt\right|^2\\ &= \left|\sum_{s\in S} e^{-\iota\langle s,k\rangle}\int_{\mathbb{R}^D} x(t)e^{-\iota\langle t,k\rangle}dt\right|^2\\ &= |\hat{s}(k)|^2\,|\hat{x}(k)|^2,\end{aligned} \tag{1.7}$$

where $\hat{x}$ and $\hat{s}$ are, respectively, the Fourier transforms of the signal x and a Dirac ensemble defined on S. As the size of the set S grows (the size of the crystal), the support of the function $\hat{s}$ is more concentrated in the dual lattice Λ^*.[1] Thus, the diffraction pattern is approximately equal to a discrete set of samples of $|\hat{x}|^2$ on Λ^*, called *Bragg peaks*. This implies that the acquired data are the Fourier magnitudes of a Λ-periodic signal on $\mathbb{R}^D$ (or, equivalently, a signal on $\mathbb{R}^D/\Lambda$), defined by its Fourier series

$$x(t) = \frac{1}{\mathrm{Vol}(\Lambda)}\sum_{k\in\Lambda^*}\hat{x}(k)e^{\iota\langle k,t\rangle}. \tag{1.8}$$

This signal is supported only at the sparsely spread positions of atoms. Elser estimated the typical number of strong scatters in a protein crystal (e.g., nitrogen, carbon, oxygen atoms) to be $K/N \sim 0.01$ [24]. In practice, the data also follow a Poisson distribution (namely, noise), whose mean is the signal.

The gaps between the idealized mathematical model (1.1), the phase retrieval crystallographic problem as it appears in X-ray experiments, are discussed in section 2.

1.3. Notation.

Throughout the work, all indices should be considered as modulo N. For instance, $x[-i] = x[N-i]$. The Fourier transform and the conjugate of a signal x are denoted, respectively, by $\hat{x}$ (namely, $Fx = \hat{x}$) and $\bar{x}$. An entrywise product between two vectors u and v is denoted by $u \odot v$ so that $(u\odot v)[n] = u[n]v[n]$; the absolute value of a vector $|u|$ refers to an entrywise operation, that is, $|u|[n] = |u[n]|$. For a set $S \subseteq [0, N-1]$, we let L_S be the subspace of signals with support contained in S (1.5), and denote its cardinality by $|S|$ or K. While most of this work is focused on real signals, some of the results hold for complex signals as well. We use the notation $\mathbb{K}^N$ to denote either the vector space $\mathbb{R}^N$ or $\mathbb{C}^N$, and define the periodic autocorrelation by

$$a_x[\ell] = \sum_{i=0}^{N-1} x[i]\overline{x[(i+\ell) \bmod N]}.$$

It satisfies the conjugation-reflection symmetry $a_x[\ell] = \overline{a[N-\ell]}$.

[1] The dual Λ^* of a lattice $\Lambda \subset \mathbb{R}^D$ is the lattice of all vectors $x \in \mathrm{span}(\Lambda) \subset \mathbb{R}^D$ such that $\langle x, y\rangle$ is an integer for all $y \in \Lambda$. For example, if $\Lambda = 2\mathbb{Z} \subset \mathbb{R}$, then $\Lambda^* = \frac{1}{2}\mathbb{Z} \subset \mathbb{R}$.

To ease notation, we make two assumptions that do not affect the generality of the results. First, we consider one-dimensional (1-D) signals; the extension to a high dimensional setting is straightforward, and is discussed in section 6. Second, hereafter we assume that N is even; all the results hold for odd N, where the only change is that $N/2$ should be replaced by $\lfloor N/2 \rfloor$.

2. Contribution and perspective.

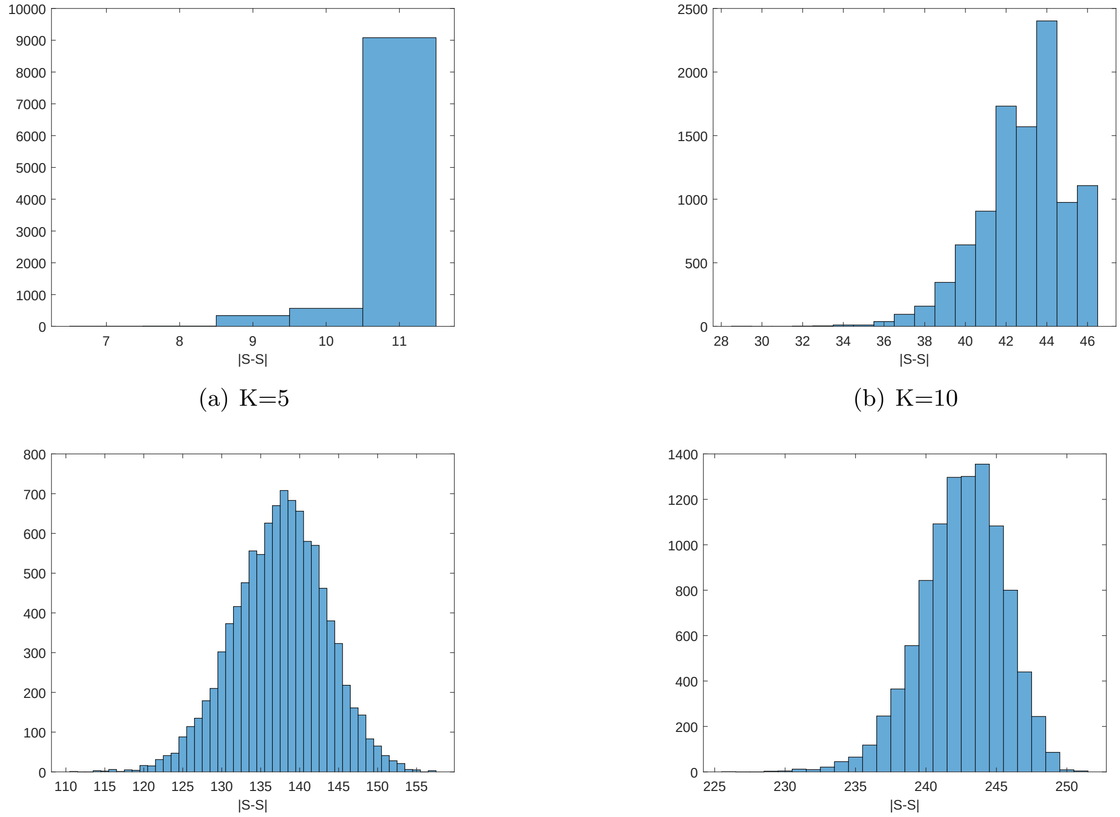
To our best knowledge, this is the first work to rigorously study the mathematics of the crystallographic phase retrieval problem. While general uniqueness results are currently beyond reach, the main contribution of this paper is conjecturing that the Fourier magnitude determines uniquely, up to intrinsic symmetries, almost all K-sparse signals as long as $K \leq N/2$. This number is significantly larger than the typical number of strong scatters in a protein crystal which was estimated to be $K/N \sim 0.01$ [24]. In this sense, our conjecture suggests that (under the stated conditions) crystallographers should not worry too much about uniqueness: the data (i.e., Fourier magnitude) usually determine the sought signal (e.g., the atomic structure of a molecule) uniquely. More formally, the main conjecture of this paper states the following.

Conjecture 2.1. *Suppose that x is a K-sparse generic signal with $K \leq N/2$, whose periodic autocorrelation a_x has more than K nonzero entries. Then, $a_x = a_{x'}$ implies that x' is obtained from x through an intrinsic symmetry. In other words, under the stated conditions, the periodic autocorrelation mapping $x \mapsto a_x$ is injective, up to intrinsic symmetries, for almost all signals.*

In section 4, we state the conjecture more precisely and establish a systematic computational technique to verify it for any particular pair (K, N).

Conjecture 2.1 puts a structural requirement on the signal's support S: the cardinality of the periodic autocorrelation's support should be larger than K. However, this condition seems to constitute only a minor restriction as it is almost always met. To comprehend the last statement, we need the notion of *cyclic difference set*, denoted by $S - S$, which includes all the differences of a set S, that is, $\{j - i | i, j \in S\}$. In the set $S - S$ we consider only the first $N/2+1$ entries because of the reflection symmetry; see a formal definition in section 4.1.2. For example, if $S = \{0, 1, 2, 5\} \subset [0, 8]$, then $S - S = \{0, 1, 2, 3, 4\}$. The notion of cyclic difference set is useful since it defines the support of the periodic autocorrelation (1.2). Specifically, Conjecture 2.1 assumes $|S - S| > K$. Generally, proving tight bounds on the probability to obtain $|S - S| > K$ (as a function of N and K) is a very challenging combinatorial problem. Nevertheless, empirical examination is easy: Figure 1 shows the empirical distribution of $|S - S|$ for different values of K. As can be seen, in *all trials* we obtained $|S - S| > K$, as desired, even for the rather small value of $K = 5$. In Proposition B.2 we also prove that if N is a prime number, then $|S - S| > K$ with probability one as $N \to \infty$; see a detailed discussion in Appendix B. The empirical affirmation of the condition $|S - S| > K$ implies that we expect Conjecture 2.1 to hold for almost all K-sparse signals provided that $K/N \leq 1/2$.

Our second conjecture states that even if there exist additional solutions (i.e., lack of uniqueness), the set of all solutions is of measure zero. Therefore, in the worst case, there are only a few K-sparse signals that agree with the observed Fourier magnitude. Importantly, the conjecture applies to *all signals* and does not impose any structural condition on the support.



(a) K=5

(b) K=10

(c) K=20

(d) K=40

Figure 1. *The empirical distributions (histograms) of the autocorrelation's support $|S - S|$ for $N = 500$ and randomly sampled subsets of size $|S| = K = \{5, 10, 20, 40\}$. Each histogram is composed of 10^4 trials. In all trials, we obtained $|S - S| > K$, as Conjecture 2.1 requires.*

Conjecture 2.2. *Suppose that x is a K-sparse signal with $K/N < 1/2$. Then, the set of K-sparse signals with periodic autocorrelation a_x is of measure zero.*

Based on group-theoretic considerations, section 5 introduces Conjecture 2.2 in technical terms, and develops a computational confirmation technique for any particular pair of (K, N). In section 6 we discuss the extension of Conjectures 2.1 and 2.2 to higher dimensions, which is straightforward.

Before moving on to surveying related literature, we wish to list the gaps between the model considered in this paper (1.1) and the crystallographic phase retrieval problem in practice. A full mathematical theory of the crystallographic phase retrieval problem should account for the following aspects, which are beyond the scope of this work.

- *Rigorous uniqueness results:* This work formulates conjectures and provides computational means to check unique mapping between a generic signal and its Fourier magnitude for any particular pair (N, K). A complete theory should provide a rigorously proven bound on K (as a function of N) that allows unique mapping for a certain class of signals.

- *Class of signals:* This work puts a special focus on generic signals (e.g., the nonzeros entries are drawn from a continuous distribution) and also discusses binary signals (i.e., the nonzeros entries are all ones). In practice, however, the model should account for sparse signals whose nonzero entries are taken from a finite (small) alphabet; this alphabet models the relevant type of atoms, such as hydrogen, oxygen, carbon, nitrogen, and so on. This model is more involved and requires intricate combinatorial calculations.
- *Noisy data:* In an X-ray crystallography experiment, the data are contaminated with noise, which is characterized by Poisson statistics. In this case, the intersection $\mathcal{B} \cap \mathcal{S}$ is empty, and the goal is to find a point close (in some metric) to the intersection.
- *Provable algorithms:* As discussed in Appendix A, the state-of-the-art algorithms for phase retrieval are based on (nonconvex) variations of the Douglas–Rachford splitting method. While Douglas–Rachford is fairly well understood for convex setups, the analysis of its nonconvex analogues for phase retrieval is lacking. We refer the readers for several recent works on the topic [35, 44, 52, 24, 45, 43], and to Appendix A for a discussion on the computational complexity of the problem.
- *Sampling:* In this work, we consider a discrete setup. In practice, however, the signal is continuous and its Fourier magnitude is measured on a Cartesian grid. Thus, sampling effects should be taken into account.
- *Additional information:* In many setups, the scientists possess some additional information about the underlying signal; this information may significantly alleviate the reconstruction process. For example, some X-ray crystallography algorithms incorporate knowledge of the minimum atom-atom distance, the presence of a known number of heavy atoms, or even the expected histogram of the signal values [26]. Such information may allow recovering a nonsparse signal even in the regime $K > N/2$. We note that a similar analysis has been conducted for the problem of retrieving a 1-D signal from its aperiodic autocorrelation [7].

3. Prior art.

As far as we know, the first to study an instance of the crystallographic phase retrieval problem (from the mathematical and algorithmic perspectives) was Elser in [24]. This paper discusses the hardness of the crystallographic phase retrieval problem for binary signals and linked it to other domains of research, such as cryptography. The subject was further investigated in [61]. In particular, it was shown that the solution of the "box relaxation" optimization problem,

$$\text{find } x \in [0,1]^N \quad \text{subject to} \quad |Fx| = y_0, \tag{3.1}$$

is the underlying binary signal $x_0 \in \{0,1\}^N$. In other words, under the measurement constraint, the solution of (3.1) cannot lie within the box $[0,1]^N$ but only on the vertices. In addition, uniqueness results were derived for the cases of $K = 1, 2, 3, N-3, N-2, N-1$. The general crystallographic phase retrieval problem (1.3) has not been previously studied.

The crystallographic phase retrieval problem is an instance of a broader class problem. The (noiseless) phase retrieval problem is any problem of the form

$$\text{find } x \in \mathcal{C} \quad \text{subject to} \quad |Ax| = y_0, \tag{3.2}$$

where y_0 is the observation, A is a Fourier-type matrix (e.g., DFT, oversampled DFT, short-time Fourier transform) and the set $\mathcal{C}$ corresponds to the constraints dictated by the particular application. For example, in the crystallographic phase retrieval problem, A is the DFT matrix, and $\mathcal{C}$ is the set of all K-sparse signals, denoted by $\mathcal{S}$ in (1.1).

An important example of a phase retrieval problem arises in coherent diffraction imaging. Here, an object is illuminated with a coherent wave and the diffraction intensity pattern (equivalent to the Fourier magnitude of the signal) is measured. As an additional constraint, usually the support of the signal is assumed to be known (i.e., the signal is known to be zero outside of some region) [56, 9]. This condition is equivalent to requiring that the signal lies in the column space of an oversampled DFT matrix. If the oversampling ratio is at least two (namely, the number of rows is at least twice the number of columns), the problem is equivalent to recovering a signal from its *aperiodic autocorrelation*:

$$b_x[\ell] = \sum_{i=0}^{N-\ell-1} x[i]\overline{x[i+\ell]}, \qquad \ell = 0, \dots, N-1. \tag{3.3}$$

Generally, it is known that there are 2^{N-2} nonequivalent 1-D signals that are mapped to the same aperiodic autocorrelation (rather than infinitely many signals that are mapped to the same periodic autocorrelation (1.2)), and the geometry of the problem has been investigated meticulously [6, 21]. It is further known that the number of solutions can be reduced when additional information is available [7, 36]. In more than one dimension, almost any signal can be determined uniquely from its aperiodic autocorrelation [34]. Nevertheless, in practice it might be notoriously difficult to recover the signal due to severe conditioning issues [5]. When the signal is sparse, the recovery problem is significantly easier [53]. In particular, a polynomial-time algorithm was devised to provably recover almost all signals when $K = O(N^{1/2-\varepsilon})$ under some constraints on the distribution of the support entries [40].

Another noteworthy phase retrieval application is ptychography. Here, a moving probe is used to sense multiple diffraction measurements [55, 47]. If the shape of the probe is known precisely,[2] then the problem is equivalent to measuring the short-time Fourier transform (STFT) magnitude of the signal, so that the matrix A in (3.2) represents an STFT matrix [48, 38, 12, 37, 51]. Additional settings that were analyzed mathematically include holography [29, 4], vectorial phase retrieval [54], and ultrashort laser characterization [59, 13, 11].

In addition to the aforementioned phase retrieval setups, we mention a distinct line of work which studies a toy model where—to facilitate the mathematical and algorithmic analysis—the Fourier-type matrix in (3.2) is replaced by a "sensing matrix" $A \in \mathbb{C}^{M\times N}$. In particular, many papers consider the case where the entries of A are drawn independent and identically distributed (i.i.d.) from a normal distribution with $M \geq 2N$. For instance, it was shown that for generic A only $M = 2N-1$ (for real) and $M = 4N-4$ (for complex) observations are required to characterize all signals uniquely [2, 17]. Moreover, based on convex and nonconvex optimization techniques, provable efficient algorithms were devised that estimate the signals stably with merely $M = O(N)$ observations; see [15, 60, 15, 16, 58, 30] to name a few. Later on, the

[2] In practice, the probe shape is unknown precisely, and thus the goal is to recover the signal and the shape of the probe simultaneously; for a theoretical analysis, see [10].

analysis was extended to more intricate models, such as randomized Fourier matrices [15, 32]. In addition, some papers considered similar randomized setups, when $N < M$ and the signal is sparse [14, 50, 57]. This research thread led to new theoretical, statistical, and computational results in a variety of fields, such as algebraic geometry, statistics, and convex and non-convex optimization. Nevertheless, its contribution to the crystallographic phase retrieval problem is disputable: none of the algorithms that were developed for randomized sensing matrices have been successfully implemented to X-ray crystallography [26]. In contrast, the algorithms that are used routinely by practitioners are based on variations of the Douglas–Rachford splitting scheme. The behavior of these algorithms differs significantly from optimization-based algorithms and is far from being understood; see an elaborated discussion in Appendix A.

4. Uniqueness for generic signals.

In this section, we introduce our main conjecture on the uniqueness of generic signals and describe a set of computational tests to verify it for any specific pair of (N, K).

4.1. Preliminaries.

We begin by formally introducing the intrinsic symmetries (i.e., trivial ambiguities) of the crystallographic phase retrieval problem, and discussing difference sets, multisets, and their connection with the uniqueness of binary signals.

4.1.1. Intrinsic symmetries and orbit recovery.

Unique mapping between a K-sparse signal and its Fourier magnitude is possible only up to three types of symmetries: circular shift, reflection through the origin, and global phase change. These symmetries are frequently referred to as trivial ambiguities in the phase retrieval literature [56, 9].

Proposition 4.1. *Let $x \in \mathbb{K}^N$ (either $\mathbb{K} = \mathbb{C}$ or $\mathbb{K} = \mathbb{R}$) be a K-sparse signal. Then, the following are also K-sparse signals with the same Fourier magnitude:*

- *the signal $xe^{\iota\phi}$ for some $\phi \in \mathbb{R}$ (if $\mathbb{K} = \mathbb{R}$, then it reduces to $\pm x$);*
- *the rotated signal $x^{\ell}[n] := x[(n - \ell) \bmod N]$ for some $\ell \in \mathbb{Z}$;*
- *the conjugate-reflected signal $\tilde{x}$, obeying $\tilde{x}[n] = \overline{x[-n \ mod\ N]}$.*

These three types of symmetries form a symmetry group which we call the *group of intrinsic symmetries*. For $\mathbb{K} = \mathbb{C}$, a signal is invariant under the action of the group $D = (S^1 \times \mathbb{Z}_N) \ltimes \mathbb{Z}_2$, where $\ltimes$ denotes a semidirect product. The first S^1 corresponds to the phase symmetry, $\mathbb{Z}_N$ corresponds to the group of N cyclic shifts, and the last $\mathbb{Z}_2$ corresponds to the reflection symmetry; the last two symmetries generate the dihedral group D_{2N} of symmetries of the regular N-gon. For $\mathbb{K} = \mathbb{R}$, the phase symmetry is replaced by a sign ambiguity $\mathbb{Z}_2 = \pm 1$, and the group of intrinsic symmetries reduces to $D = \mathbb{Z}_2 \times D_{2N}$. Interestingly, an analog intrinsic symmetry group is formed when the crystallographic phase retrieval problem is generalized to any abelian finite group; see Appendix E.

Proposition 4.1 implies that the intersection $\mathcal{B} \cap \mathcal{S}$ is invariant under the action of the group of intrinsic symmetries D. In particular, if $x \in \mathcal{B} \cap \mathcal{S}$, then so is $g \cdot x$ for any element g in D. In group theory terminology, the set of signals $\{g \cdot x : g \in D\}$ is called the *orbit of x under D*. Therefore, our goal in this work to identify the regime in which the intersection of $\mathcal{S}$ and $\mathcal{B}$ consists of a single orbit. This interpretation builds a connection between the crystallographic phase retrieval problem (as well as other phase retrieval problems) and other classes of *orbit recovery problems*, such as single-particle reconstruction using cryoelectron microscopy, and multireference alignment; see, for instance, [3, 8]. Throughout this paper we say that two signals are *equivalent* if they lie in the same orbit under D. Otherwise, we say that the signals are nonequivalent.

We note that the two groups S^1 ($\mathbb{Z}_2$ for $\mathbb{K} = \mathbb{R}$) and the dihedral group D_{2N} play a different role in the analysis. The dihedral group acts on the set S—the support of the signal—by permuting its indices (recall that it is a subgroup of the permutation group). In particular, we say that S and S' are equivalent if $g \cdot S = S'$ for some element $g \in D_{2N}$. The phase (or sign in the real case) symmetry affects only the values of the nonzero entries, and thus plays a lesser role for generic signals.

4.1.2. Difference sets, multisets, collisions, and uniqueness for binary signals. The support recovery analysis is tightly related to the notion of cyclic difference sets. Let us identify $[0, N-1]$ with the group $\mathbb{Z}_N$. Then, there is an action of the group $\mathbb{Z}_2 = \pm 1$ on $\mathbb{Z}_N$ by $n \mapsto -n \bmod N$; this action corresponds to the reflection symmetry of the periodic autocorrelation. The set of orbits under this action can be identified with the set $[0, N/2]$. Given a subset $S \subset [0, N-1]$, we define the cyclic difference set $S - S \subset [0, N/2]$ as the set of equivalence classes of $\{j - i \bmod \pm 1 | i, j \in S\}$. For example, if $S = \{0, 1, 2, 5\} \subset [0, 8]$, then $S - S = \{0, 1, 2, 3, 4\}$.

We may also view $S - S$ as a multiset, where we count the multiplicities of the differences. For the example above, $S - S = \{0^4, 1^2, 2^1, 3^1, 4^2\}$. The cardinality of $|S - S|$ as a multiset equals $\binom{K+1}{2}$ and thus depends only on K, but the cardinality of $|S - S|$ as a set depends on the particular subset. Note that $S - S$ (either as a set or as a multiset) is invariant under the action of D_{2N} on the set of subsets. Thus, equivalent subsets have the same difference set.

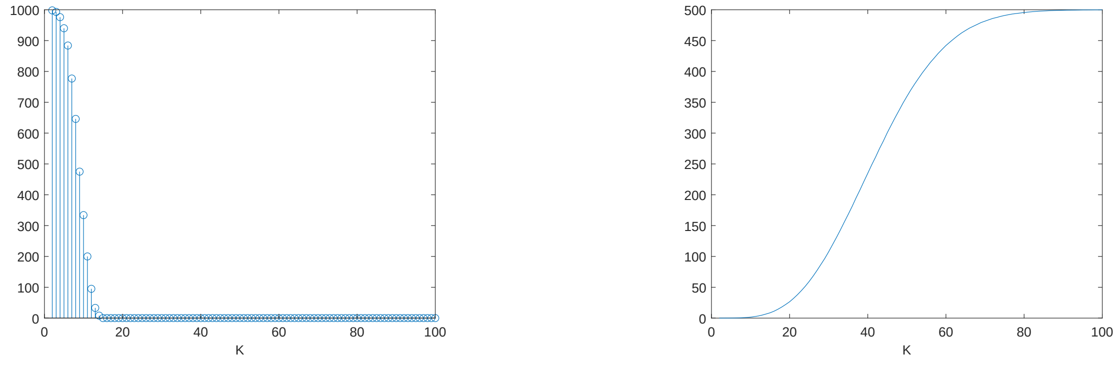
Multiplicities greater than one are occasionally referred to as *collisions*; a collision-free subset is a subset whose corresponding multiset has no multiplicity larger than one. From a phase retrieval standpoint, collisions are challenging since it is difficult to determine a priori how many pairs of the support's entries are mapped into one autocorrelation entry. Unfortunately, the following proposition shows that for any fixed value of K/N, collision-free sets do not exist if N is sufficiently large.

Proposition 4.2. *For any $R \in (0, 1]$, for N sufficiently large (as a function of R), there does not exist a collision-free subset of size $K \geq RN$.*

Proposition 4.2 is proven in Appendix C. Note that the proposition holds true even for an arbitrarily low sparsity level $K/N(R)$. Figure 2 shows empirically that for a fixed N, collision-free subsets are rare unless K is very small compared to N. Figure 3 exemplifies that if we keep the ratio K/N fixed, in this case $K/N = 0.01$—the expected density in proteins—collision-free subsets are uncommon as N grows.

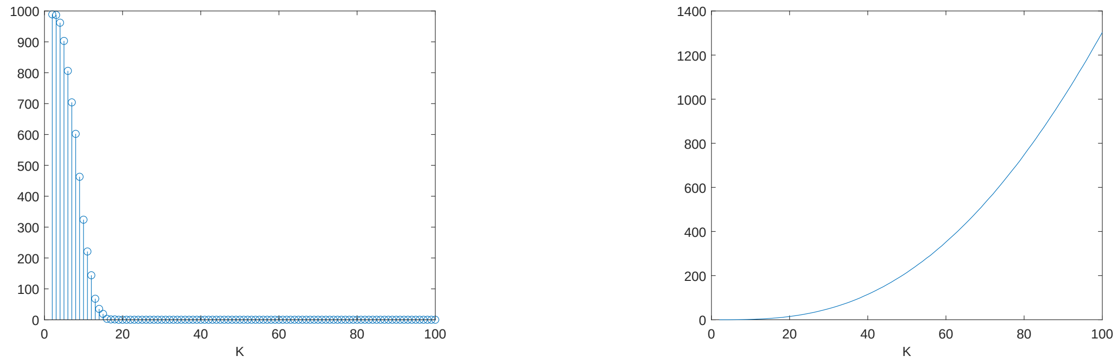
The crystallographic phase retrieval problem for binary signals depends solely on difference multisets: two binary signals with sparsity K have the same periodic autocorrelation if and only if they have the same difference multisets. Thus, the failure to distinguish nonequivalent binary signals from their autocorrelation is equivalent to the existence of two nonequivalent K-element subsets of $[0, N-1]$ with the same difference multiset. For example, the subsets of $[0, 7]$, $\{0, 1, 3, 4\}$, and $\{0, 1, 2, 5\}$ both have cyclic difference multisets $\{0^4, 1^2, 2^1, 3^2, 4^1\}$ but are not equivalent. Yet, these cases seem to be rare, suggesting that uniqueness for the binary case is ubiquitous.

4.2. Impossibility results. We continue our investigation with some impossibility results. We start with a simple parameter counting argument.



(a) Number of collision-free events (b) Average number of collisions

Figure 2. *For a fixed K, we generated* 1000 *K-sparse signals of length $N = 1000$ and counted collisions (namely, entries of $|S - S|$ with multiplicity greater than one; see section* 4.1.2*). The left panel shows the number of collision-free events. The right panel presents the average number of collisions per trial. Clearly, unless K/N is very small, collision-free events are rare.*



(a) Number of collision-free events (b) Average number of collisions

Figure 3. *For a fixed K, we generated* 1000 *K-sparse signals while keeping a fixed ratio $K/N = 0.01$, and counted collisions. The left panel shows the number of collision-free events. The right panel presents the average number of collisions per trial. Clearly, even for fixed K/N collision-free events are rare as N grows.*

Proposition 4.3. *A necessary condition for solving the crystallographic phase retrieval problem* (1.3) *for generic signals is that $K = |S| \leq N/2 + 1$.*

Proof. Since $|S - S|$ is the cardinality of the autocorrelation's support, then a parameter count implies that signal reconstruction is impossible if $|S - S| < |S|$. Since $|S - S| \leq N/2 + 1$, a necessary condition for solving the sparse phase retrieval problem is that $|S| \leq N/2 + 1$. ■

We say that a subset $S \subset [0, N - 1]$ is an *arithmetic progression with difference* d if there exists $d \in [0, N - 1]$ such that $S = \{c_0 + \ell d \,|\, \ell = 0, \ldots, |S| - 1\}$ mod N.[3] Note that because the indices are taken modulo N, we can always assume that $d \leq N/2 + 1$. For example, if $N = 9$,

[3] The term *periodic* has been used in [40], but *arithmetic progression* is more consistent with arithmetic combinatorics literature [41], where the term periodic is used only when d divides N.

then the subsets $\{0,2,4,6\}$ and $\{0,3,5,7\}$ are both arithmetic progressions with $d=2$, where $c_0=0$ and $c_0=3$, respectively. The property of being an arithmetic progression is preserved by the action of the dihedral group: if S is an arithmetic progression with difference d and $s \in D_{2N}$ is a reflection, then $s \cdot S$ is also an arithmetic progression with difference d.

If S is an arithmetic progression, then $S-S=\{0,\overline{d},\dots,\overline{(K-1)d}\}$, where $\overline{m}$ denotes the equivalence class of n in $[0,N/2]$ under the equivalence $n \sim -n$. If all of $\{0,\overline{d},\dots,\overline{(K-1)d}\}$ are distinct, then $|S-S|=K$, but it is possible for $|S-S|<K$. For example, if $S=\{0,2,4,6\} \subset [0,7]$, then $S-S=\{0,2,4\}$ because $6=(-2) \bmod 8$.

Proposition 4.4. *Let S be an arithmetic progression, and let L_S be the vector space of signals whose support is S. Then, for a generic vector $x \in L_S$ there is no unique solution to the crystallographic phase retrieval problem.*

Proof. Applying a shift we can assume $0 \in S$ so $S=\{0,d,2d,\dots,d(K-1)\}$ and $S-S$ is the set $\{0,\overline{d},\overline{2d},\dots,\overline{(K-1)d}\}$. To simplify notation we assume that all of the $\overline{d\ell}$ are distinct so that $|S-S|=K$. In this case, if $x \in L_S$, then the nonzero entries of the periodic autocorrelation of

$$x=(x[0],0,\dots,x[d],0,\dots,x[2d],0\dots,0,x[d(K-1)],0\dots,0),$$

are the same as the entries of the aperiodic autocorrelation of the vector

$$x'=(x[0],x[d],\dots,x[d(K-1)]) \in \mathbb{K}^K.$$

Precisely, we have

$$a_x[\overline{\ell d}]=x[0]\overline{x[\ell d]}+x[d]\overline{x[(\ell+1)d]}+x[K-1-\ell d]\overline{x[(K-1)d]}, \tag{4.1}$$

where the $\overline{x[md]}$ on the right-hand side indicates the complex conjugate, and the notation $a_x[\overline{\ell d}]$ indicates the entry indexd by the integer $\overline{\ell d} \in [0,N/2]$. The right-hand side of (4.1) is exactly the ℓth entry in the aperiodic autocorrelation of the vector $x'=(x[0],x[d],\dots,x[(K-1)d]) \in \mathbb{K}^K$, which does not determines a generic signal uniquely [9]. ■

Remark 4.5. In our model the basic signal x is periodically repeated to represent the crystal structure. If the support S of x is an arithmetic progression, then the basic signal is itself periodic. In this case, Proposition 4.4 says that we cannot solve the phase retrieval problem for x. The reason is that if we replace x by the signal x_p representing one period of x in S, then x and x_p have the same periodic repetition. However, the support of x_p may no longer be sparse as occurs in Example 4.6 below. For this reason we cannot expect to be able to recover x_p or, equivalently x, from its Fourier magnitude without further information. In practice we do not expect this situation to occur.

Example 4.6. Suppose that $S=\{0,2,4,6\} \subset [0,8]$, so S is an arithmetic progression with $d=2$. The difference set is $\{\overline{0},\overline{2},\overline{4},\overline{6}\}=\{0,2,4,3\}$ since $6=-3 \in \mathbb{Z}_9$. Then, the nonzero entries of the periodic autocorrelation a_x are

$$\begin{aligned}
a_x[0] &= |x[0]|^2 + |x[2]|^2 + |x[4]|^2 + |x[6]|^2,\\
a_x[2] &= x[0]\overline{x[2]} + x[2]\overline{x[4]} + x[4]\overline{x[6]},\\
a_x[3] &= x[6]\overline{x[0]},\\
a_x[4] &= x[0]\overline{x[4]} + x[2]\overline{x[6]}.
\end{aligned}$$

If we let $x' = (x[0], x[2], x[4], x[6]) \in \mathbb{K}^4$ and denote by $b_{x'}$ the aperiodic autocorrelation (3.3), then $b_{x'}[0] = a_x[0]$, $b_{x'}[1] = a_x[2]$, $b_{x'}[2] = a_x[4]$, $b_{x'}[3] = a_x[3 = \overline{6}]$.

4.3. The main conjecture.

4.3.1. Terminology from algebraic geometry.

We recall some terminology from algebraic geometry; for more detail see [17, 20] and the references therein.

Let $\mathbb{K}$ denote either $\mathbb{R}$ or $\mathbb{C}$. Given polynomials $f_1, \dots, f_r \in \mathbb{K}[x_0, \dots, x_{N-1}]$, let us define the set

$$Z(f_1, \dots, f_r) = \{(a_0, \dots a_{N-1}) \,|\, f_i(a_0, \dots, a_{N-1}) = 0 \quad \text{for all} \quad i = 1, \dots r\}.$$

A set of the form $Z(f_1, \dots, f_r)$ is called an *algebraic set.* The *Zariski topology* on $\mathbb{K}^N$ is the topology formed by defining open sets to be the complements of algebraic sets. Note that a Zariski closed set is also closed in the Euclidean topology. The complement of an algebraic set is called a *Zariski open* set. Every proper algebraic set in $\mathbb{K}^N$ has dimension strictly smaller than N and every nonempty Zariski open set U is dense in both the Zariski topology and the Euclidean topology. If U is a nonempty Zariski open set, then $\mathbb{K}^N \setminus U$ has dimension strictly less than N and therefore has Lesbegue measure 0.

4.3.2. Statement of the main conjecture.

Recall that we denote by L_S the subspace of $\mathbb{K}^N$ consisting of vectors whose support is contained in $S \subset [0, N-1]$. The following formulates Conjecture 2.1—the main conjecture of this work—in more technical terms. Specifically, it states that if the condition $|S - S| > |S|$ is met, then the D-orbit of a generic signal with support contained in S is determined from its Fourier magnitude.

Conjecture 4.7. *Let S be a subset of $[0, N-1]$ such that $|S - S| > |S|$, and let $x \in L_S$ be a generic signal. Then:*

- *if $a_x = a_{x'}$, then x' is obtained from x by an action of the group D of intrinsic symmetries described in Proposition 4.1 or, equivalently,*
- *the Fourier magnitude mapping $x \mapsto |\hat{x}|$ is injective, modulo intrinsic symmetries.*

By generic signals, we mean that there is a nonempty Zariski open set $U_S \subset L_S = \mathbb{K}^{|S|}$ such that Fourier magnitude mapping $x \mapsto |\hat{x}|$ is injective modulo intrinsic symmetries at all points $x \in U_S$.

Although we cannot prove Conjecture 4.7, we provide a computational method to check the results for any given K and N. There are two aspects to verifying the conjecture: recovering the support of the signal, and signal recovery for a given support. Each of these aspects requires a different computational verification test. Consequently, we treat them separately and formulate independent conjectures. We now elaborate about both.

4.3.3. Support recovery. The support of the periodic autocorrelation is the set $S - S$. If S' is another K-element subset such that $S' - S' \neq S - S$, then the autocorrelation of a generic vector x' in $L_{S'}$ has a different support than the autocorrelation of a generic vector x in L_S. Thus, in order to investigate recovery of generic K-sparse signals in L_S, we only need to consider K-sparse subsets S' with the same difference sets $S' - S' = S - S$ as subsets of $[0, N/2]$.

We denote by $a(L_S)$ the image of the subspace L_S under the autocorrelation map $\mathbb{K}^N \to \mathbb{K}^{N/2+1}$ for either $\mathbb{K} = \mathbb{R}$ or $\mathbb{K} = \mathbb{C}$. The following conjecture states that if $|S - S| > |S|$, then for generic signals the support set S is determined, up to dihedral equivalence, from the Fourier magnitude.

Conjecture 4.8. *Suppose that S and S' are two nonequivalent K-element subsets of $[0, N-1]$ (i.e., S' is not in the orbit of S under the action of the dihedral group) with $|S-S| = |S'-S'| > K$. Then, for generic $x \in L_S$, $a(x)$ is not in $a(L_{S'})$. Namely, the support of x is determined, up to dihedral equivalence, by the periodic autocorrelation of x.*

Verifying Conjecture 4.8 computationally. For a specific pair S, S', there is a method to verify Conjecture 4.8 as follows. Consider the incidence subvariety $I_{S,S'}$ of $L_S \times L_{S'}$ consisting of pairs

$$\{(x, x') \,|\, a(x) = a(x'), x \in L_S, x' \in L_{S'}\}.$$

The projection $\pi_S \colon I_{S,S'} \to L_S$ is the set of $x \in L_S$ such that there exists $x' \in L_{S'}$ with $a(x) = a(x')$. To prove the conjecture, it suffices to prove that $\pi_S(I_{S,S'})$ is not dense; this in turn implies that for a generic signal, if $a(x) = a(x')$, then $S = S'$. For this statement, it is sufficient to show that $\dim I_{S,S'} < |S|$. The reason this is sufficient is that if $\dim I_{S,S'} < |S| = \dim L_S$, then $\dim \pi_S(I_{S,S'}) < \dim L_S$ as well, which means that the complement $L_S \setminus \pi_S(I_{S,S'})$ is dense in the Zariski topology. Now, if $x \in L_S \setminus \pi_S(I_{S,S'})$, then by definition there is no $x' \in L_{S'}$ such that $a_x = a_{x'}$. Since a finite intersection of Zariski dense subsets is Zariski dense, we see that if x is in the Zarski dense set $L_S \setminus \bigcup_{\{S' | S'-S'=S-S\}} \pi_S(I_{S,S'})$ (namely, we consider all possible, finitely many, relevant cyclic difference sets), then there is no nonequivalent subset S' and vector $x' \in L_{S'}$ such that $a_x = a_{x'}$. In other words, for generic x in L_S the equivalence class of the subset S is determined by the autocorrelation a_x.

As mentioned above, it suffices to check whether $\dim I_{S,S'} < |S|$. When $\mathbb{K} = \mathbb{R}$ (the main interest of this paper) and K is small, the dimension of the variety $I_{S,S'}$ can be computed relatively quickly using a computer algebra system to compute the Hilbert polynomial of the ideal[4] defining $I_{S,S'}$ in the polynomial ring $\mathbb{K}[\{x_i\}_{i \in S}, \{x'_j\}_{j \in S'}]$. (See section 4.3.5 for a discussion on the computational complexity of computing Hilbert polynomials.) The degree of the Hilbert polynomial is the dimension of the variety, so a sufficient condition for the conjecture to hold is if the degree of the Hilbert polynomial is less than $|S|$. More technical details are provided in Appendix D.

Example 4.9. We give an explicit example to illustrate the methods used to generate the data presented in Example 4.10 below. Let $S = \{0, 1, 2, 4\}$ and $S' = \{0, 1, 2, 5\}$ be subsets of

[4] Recall that the ideal generated by a set of polynomials is all polynomial combinations of its generators $f_1, \ldots, f_n$,: $I = \{\sum_{i=1}^n c_i f_i \text{ for } c_i \in \mathbb{K}[x_1, \ldots, x_n]\}$.

Table 1
Verification of Conjecture 4.8 for $N=8, K=4$.

S	$S-S$	$\lvert S-S\rvert$
{0,1,2,3}	{0,1,2,3}	4
{0,1,2,4}	{0,1,2,3,4}	5
{0,1,2,5}	{0,1,2,3,4}	5
{0,1,3,4}	{0,1,2,3,4}	5
{0,1,3,5}	{0,1,2,3,4}	5
{0,1,3,6}	{0,1,2,3}	4
{0,1,4,5}	{0,1,3,4}	4
{0,2,4,6}	{0,2,4}	3

$[0,7]$. If $x=(x_0,x_1,x_2,0,x_4,0,0,0)\in L_S$ and $y=(y_0,y_1,y_2,0,0,y_5,0,0)\in L_{S'}$, then

$$a_x=(x_0^2+x_1^2+x_2^2+x_4^2, x_0x_1+x_1x_2, x_0x_2+x_2x_4, x_1x_4, x_4x_0)$$

and

$$a_y=(y_0^2+y_1^2+y_2^2+y_5^2, y_0y_1+y_1y_2, y_0y_2, y_2y_5+y_5y_0, y_1y_5).$$

Hence $a_x=a_y$ if and only if the following five equations are satisfied:

$$\begin{aligned} x_0^2+x_1^2+x_2^2+x_4^2-y_0^2-y_1^2-y_2^2-y_5^2&=0,\\ x_0x_1+x_1x_2-y_0y_1-y_1y_2&=0,\\ x_0x_2+x_2x_4-y_0y_2&=0,\\ x_1x_4-y_2y_5-y_5y_0&=0,\\ x_0x_4-y_1y_5&=0. \end{aligned} \tag{4.2}$$

Thus, the incidence $I_{S,S'}=\{(x,y)\,|\,a_x=a_y\}\subset L_S\times L_{S'}$ is the algebraic subset of $\mathbb{K}^4\times\mathbb{K}^4$ defined by the set of equations (4.2). Therefore, the generators of the ideal of $I_{S,S'}$ are the five polynomials in the left-hand side of (4.2) included in $\mathbb{R}[x_0,x_1,x_2,x_4,y_0,y_1,y_2,y_5]$. Using Macaulay2 [31], we calculated the Hilbert polynomial of this ideal to be $32P_2-80P_1+80P_0$, which means that $I_{S,S'}$ is a 3-dimensional algebraic subset of $\mathbb{K}^4\times\mathbb{K}^4$ and therefore its image under π_S to $\mathbb{K}^4$ has dimension at most 3.

Example 4.10. We consider the case where $K=4$ and $N=8,9$. As presented in Table 1, when $K=4, N=8$, there are 8 equivalence classes of 4-sparse subsets of which only 4 satisfy $|S-S|>4$. For the 6 pairs of subsets S,S' with $S-S=S'-S'=\{0,1,2,3,4\}$, we have verified using Macaulay2 [31] that $\dim I_{S,S'}=3$; this is the desired result since $|S-S|=5$ means that we expect to impose 5 constraints on the 8-dimensional space $L_S\times L_{S'}$. Hence, the support of a generic vector $x\in L_S$ can be recovered from its periodic autocorrelation. However, this is not the case if $|S-S|=4$. For example, if $S=\{0,1,2,3\}$ and $S'=\{0,1,3,6\}$, then $\dim I_{S,S'}=4$.

Recall that when $S-S$ and $S'-S'$ differ as multisets, we can recover the support of a binary signal from its periodic autocorrelation (and thus, obviously, also the binary signal itself). Interestingly, the nonequivalent subsets $\{0,1,3,4\}$ and $\{0,1,2,5\}$ have the same difference multisets so we cannot distinguish their supports from binary signals but we can from generic signals.

Table 2
Verification of Conjecture 4.8 for $N = 9, K = 4$.

S	$S - S$	$\lvert S - S\rvert$
{0,1,2,3}	{0,1,2,3}	4
{0,1,2,4}	{0,1,2,3,4}	5
{0,1,2,5}	{0,1,2,3,4}	5
{0,1,3,4}	{0,1,2,3,4}	5
{0,1,3,5}	{0,1,2,3,4}	5
{0,1,3,6}	{0,1,2,3,4}	5
{0,1,3,7}	{0,1,2,3,4}	5
{0,1,4,5}	{0,1,3,4}	4
{0,1,4,6}	{0,1,2,3,4}	5
{0,2,4,6}	{0,2,3,4}	4

When $N = 9$ and $K = 4$, there are 10 equivalence classes of subsets, which are presented in Table 2. In this case, all incidences $I_{S,S'}$ are 3-dimensional, so the support of a generic vector can be determined from its autocorrelation even if $|S - S| = 4$ because for each distinct pair S, S' $|(S - S) \cup (S' - S')| \geq 5$ which means that we obtain at least five constraints on the entries of a pair $(x, y) \in I_{S,S'}$. For example if $S = \{0, 1, 2, 3, \}$ and $S' = \{0, 2, 4, 6\}$ and $x = (x_0, x_1, x_2, x_3, 0, 0, 0, 0, 0) \in L_S$ and $y = (y_0, 0, y_2, 0, y_4, 0, y_6, 0, 0) \in L_{S'}$, then $a_x = a_y$ if and only if the following 5 equations are satisfied:

$$\begin{aligned} x_0^2 + x_1^2 + x_2^2 + x_3^2 - y_0^2 - y_2^2 - y_4^2 - y_6^2 &= 0, \\ x_0x_1 + x_1x_2 + x_2x_3 &= 0, \\ x_0x_2 + x_1x_3 - y_0y_2 - y_2y_4 - y_4y_6 &= 0, \\ x_0x_3 - y_6y_0 &= 0, \\ y_0y_4 + y_2y_6 &= 0. \end{aligned} \tag{4.3}$$

Namely, in this specific example we do not demand $|S - S| > K$.

4.3.4. Generic signal recovery given knowledge of the support. The difficulty of reconstructing a signal given its support depends on the structure of $S - S$. We first consider two simple cases, and then move forward to the general case.

The easiest case is the collision-free case. This means that no nonzero entry in the cyclic difference set $S - S$ appears with multiplicity greater than one. In this case there is a relatively easy eigenvalue argument to determine the entries of x from its autocorrelation [53]. Note, however, that collision-free subsets appear to be quite rare unless K is very small compared to N, as demonstrated in Figure 2. Even if we keep the ratio K/N fixed, then collision-free events are rare as N grows. Figure 3 exemplifies it for $K/N = 0.01$, which is the expected sparsity level in proteins.

The other easy case is when the difference set S can be concentrated in the interval $[0, N/2]$ after applying reflection and translation (i.e., an element of the dihedral group). In this case, the periodic autocorrelation of $x \in L_S$ is the same as the nonperiodic autocorrelation of x viewed as a vector in $\mathbb{R}^{N/2+1}$. For example, if $N = 8$ then the support set $\{0, 5, 7\}$ can be moved to $\{0, 1, 3\}$ by reflection and this set is concentrated. For concentrated sets uniqueness of recovery depends on whether the support forms an arithmetic progression as discussed in [39].

Next, we consider the general case. Given a subset $S \subset [0, N-1]$, we let D_S be the subgroup of the group of intrinsic symmetries D that leaves L_S invariant. We refer to this group as the group of intrinsic symmetries of S. For a typical S, $D_S = \pm 1$ if $\mathbb{K} = \mathbb{R}$ and $D_S = S^1$ if $\mathbb{K} = \mathbb{C}$ (recall that these subgroups do not affect the support). However, there are subsets S for which D_S is a bigger group. For example, the subset $\{0, 1, 3, 4\}$ of $[0, 7]$ is preserved by the subgroup of D_{16} consists of two elements: the identity and reflection followed by four shifts. Thus, $D_S = \pm 1 \times \mathbb{Z}_2$ or $D_S = S^1 \times \mathbb{Z}_2$, depending on whether $\mathbb{K}$ is real or complex.

The following conjecture states that if the support of the signal is known, the Fourier magnitude determines a generic signal uniquely, up to an element of D_S.

Conjecture 4.11. *Suppose that $|S - S| > |S|$. If $x \in L_S$ is a generic vector and $x' \in L_S$ is another vector (in the same subspace) such that $a(x) = a(x')$, then $x' = g \cdot x$ for some $g \in D_S$.*

Conjecture 4.8 states that if $|S - S| > |S|$, then we can recover the support S of a generic vector in L_S. Conjecture 4.11 argues that once we know that $x \in L_S$, then we recover x itself. These two conjectures combined imply Conjecture 4.7.

Verifying Conjecture 4.11 computationally. To verify the conjecture we consider the incidence

$$I_S = \{(x, x') \,|\, a(x) = a(x')\} \subset L_S \times L_S. \tag{4.4}$$

By construction, I_S contains the K-dimensional linear subspaces $L_g = \{(x, g{\cdot}x) \,|\, g \in D_S\}$. The goal is to show that $I_S \setminus \cup_{g \in D_S} L_g$ (namely, the incidence without the subspaces corresponding to the intrinsic symmetries of S) has dimension strictly less than K. To verify the conjecture we can show that the K-dimensional components of I_S correspond to pairs (x, x'), where x' is obtained from x by a trivial ambiguity, and that all other components have strictly smaller dimension.

This can be done by computing the Hilbert polynomial P_I of the ideal I which defines the algebraic subset $I_S \subset L_S \times L_S$. As discussed in Appendix D, the Hilbert polynomial P_I can expressed in the following form:

$$P_I = a_\ell P_\ell + a_{\ell-1} P_{\ell-1} + \cdots + a_0 P_0,$$

where $\ell = \dim I_S - 1$ and a_ℓ is the degree of I_S as an algebraic subset of $L_S \times L_S$. Since a linear subspace has degree one, to show that $I_S \setminus \cup_{g \in D_S} L_g$ has dimension smaller than K, it suffices to show that $\ell \leq |S| - 1$ and $a_\ell = |D_S|$ whenever $|S - S| > K$.

Example 4.12. We give an example to illustrate the methods used to generate the data presented in Example 4.13 below. Let $S = \{0, 1, 2, 5\} \subset [0, 7]$ and let L_S be a subspace of $\mathbb{R}^N$ with support in S. The set S is preserved by the element of order two $\sigma \in D_{16}$ which is the reflection composed with a shift by 2. Thus, the group D_S that stabilizes L_S consists of four elements which we denote by $(1, -1, \sigma, -\sigma)$. Specifically, if $(a, b, c, 0, 0, d, 0, 0) \in L_S$, then

$$\begin{aligned}
1 \cdot (a, b, c, 0, 0, d, 0, 0) \cdot &= (a, b, c, 0, 0, d, 0, 0), \\
-1 \cdot (a, b, c, 0, 0, d, 0, 0) &= (-a, -b, -c, 0, 0, -d, 0, 0), \\
\sigma \cdot (a, b, c, 0, 0, d, 0, 0) &= (c, b, a, 0, 0, d, 0, 0), \\
-\sigma \cdot (a, b, c, 0, 0, d, 0, 0) &= (-c, -b, -a, 0, 0, -d, 0, 0).
\end{aligned}$$

Table 3

Verification of Conjecture 4.11 for $N = 8, K = 4$.

Subset	$\lvert D_S\rvert$	Degree	Dimension	Phase retrieval
{0,1,2,4}	2	2	4	Yes
{0,1,2,5}	4	4	4	Yes
{0,1,3,4}	4	4	4	Yes
{0,1,3,5}	2	2	4	Yes

If $x = (x_0, x_1, x_2, 0, 0, x_5, 0, 0)$ and $y = (y_0, y_1, y_2, 0, 0, y_5, 0, 0)$, then $a_x = a_y$ if and only if the following equations are satisfied:

$$\begin{aligned} x_0^2 + x_1^2 + x_2^2 + x_5^2 - y_0^2 - y_1^2 - y_2^2 - y_5^2 &= 0,\\ x_0x_1 + x_1x_2 - y_0y_1 - y_1y_2 &= 0,\\ x_0x_2 - y_0y_2 &= 0,\\ x_2x_5 + x_5x_0 - y_2y_5 - y_5y_0 &= 0,\\ x_1x_5 - y_1y_5 &= 0. \end{aligned} \tag{4.5}$$

Let I be the ideal in $\mathbb{K}[x_0, x_1, x_2, x_5, y_0, y_1, y_2, y_5]$ generated by the five polynomials in the left-hand side of (4.5). Equations (4.5) are clearly satisfied if $x = y$ of $x = -y$. Thus, the 4-dimensional linear subspaces $L_1 = \{(x, x) \mid x \in L_S\}$ and $L_{-1} = \{(x, -x) \mid x \in L_S\}$ are in $Z(I)$, where $Z(I)$ denotes the algebraic subset of $L_S \times L_S$ defined by the ideal I. In addition for any 4 real numbers (a, b, c, d) the vectors $x = (a, b, c, 0, 0, d, 0, 0)$ and $y = \pm(c, b, a, 0, 0, d, 0, 0)$ are solutions of (4.5). Hence, there are two additional 4-dimensional linear subspaces $L_\sigma = \{(x, \sigma x) \mid x \in L_S\}$ and $L_{-\sigma} = \{(x, -\sigma x) \mid x \in L_S\}$ in $Z(I)$.

Using Macaulay2 we calculated the Hilbert polynomial of the ideal I to be $P_I = 4P_3 + 10P_2 - 30P_1 + 20P_0$. Since $I_S = Z(I)$ contains four linear subspaces $L_1, L_{-1}, L_\sigma, L_{-\sigma}$, then Proposition D.1 implies that

$$I_S \setminus (L_0 \cup L_{-1} \cup L_\sigma \cup L_{-\sigma}) = \{(x, x') \mid a_x = a_{x'} \text{ and } x' \neq g \cdot x \text{ for some } g \in D_S\}, \tag{4.6}$$

has dimension at most 3. Hence, for generic $x \in L_S$ if $a_x = a_{x'}$, then $x' = g \cdot x$ for some $g \in D_S$.

Example 4.13. For each of the equivalence classes of 4-element subsets S with $|S - S| > 4$ and $N = 8, 9$, we used Macaulay2 [31] to compute the Hilbert polynomial of I_S and verify that generic $x \in L_S$ can determined from its periodic autocorrelation. Tables 3 and 4 present the degree and dimension of I_S. In each case, the degree of I_S equals $|D_S|$ and dimension equals K.

The hypothesis is that $|S - S| > K$ in Conjecture 4.11 is necessary. To demonstrate it, the following example gives two different signals with the same support and the same autocorrelation when $|S| = |S - S| = 4$.

Example 4.14. Consider the subset $S = \{0, 1, 4, 5\}$ of $[0, 7]$ so that $|S - S| = |S| = 4$. Then, the vectors

$$[x[0], x[1], 0, 0, x[4], x[5], 0, 0],$$

Table 4
Verification of Conjecture 4.11 for $N = 9, K = 4$.

Subset	$\|D_S\|$	Degree	Dimension	Phase retrieval
{0,1,2,4}	2	2	4	Yes
{0,1,2,5}	2	2	4	Yes
{0,1,3,4}	4	4	4	Yes
{0,1,3,5}	2	2	4	Yes
{0,1,3,6}	6	6	4	Yes
{0,1,3,7}	4	4	4	Yes
{0,1,4,6}	4	4	4	Yes

and

$$1/2[(x[0]+x[1]-x[4]+x[5]),(x[0]+x[1]+x[4]-x[5]),\\ 0,0,(-x[0]+x[1]+x[4]+x[5]),(x[0]-x[1]+x[4]+x[5]),0,0)],$$

have the same autocorrelation but are not related by an intrinsic symmetry.

4.3.5. The computational complexity of verifying Conjecture 4.8 and Conjecture 4.11.

There is no expectation that the computational complexity of verifying Conjectures 4.8 and 4.11 is polynomial in N or in K. There are two significant issues. The first is that verification of Conjecture 4.8 requires enumerating over all $\binom{N}{K}$ element subsets of $[1, N]$. If $K \sim N$, then Stirling's formula implies that this number asymptotic to at least $a^N/\sqrt{2\pi N}$ for some $a > e$.

In addition there are no good bounds on the computational complexity of computing the Hilbert polynomial of an ideal in a polynomial ring. The reason is that implemented algorithms for computing Hilbert polynomials first compute Gröbner bases. The computational complexity of computing Gröbner bases is not known, but for the ideals we consider which are generated by degree two elements in $2K$ variables, the best theoretical bound on the complexity is doubly exponential, namely $O(a^{2^K})$ [19].[5] To illustrate this, we tabulate below (Table 5) the run times of the `hilbertPolynomial` function in Macaulay2 [31] to compute the Hilbert polynomial of the ideal of the incidence I_S defined by (4.4), where S is a random K element subset of $[0, 99]$, and $K = 5, \ldots, 12$. For these reasons numerical verification is only feasible for small-scale problems and cannot be applied directly to X-ray crystallography.

5. Group-theoretic considerations.

In Fourier domain, signals x and x' have the same Fourier magnitude if and only if $\hat{x}'[i] = e^{\iota\theta_i}\hat{x}[i]$ for some set of rotations $(\theta_0, \ldots, \theta_{N-1})$. It follows that if $\mathbb{K} = \mathbb{C}$, then the group $G = (S^1)^N$ preserves $|\hat{x}|$. The group G acts on signals in the time domain via the Fourier transform. In other words, if $x \in \mathbb{C}^N$ and $g = (e^{\iota\theta_0}, \ldots, e^{\iota\theta_{N-1}})$, then $g \cdot x = F^{-1}gFx$, where F is the $N \times N$ DFT matrix.

We call G the group of *nontrivial symmetries* for the phase retrieval problem. The action of G is related to the action of D, the group of intrinsic symmetries (see Proposition 4.1), as follows. The subgroup S^1 of D corresponds to the diagonal subgroup of $G = (S^1)^N$ since $\widehat{e^{\iota\theta}x} = e^{\iota\theta}\hat{x}$. The circular shift of D forms the subgroup $\mathbb{Z}_N \subset G$, generated by the element

[5] The doubly exponential bound of [19] is a bound on the maximum degree of an element in a Gröbner basis.

Table 5

Run times to compute the Hilbert polynomial of the ideal of I_S for S, a random subset of $[0, 99]$.

K	Run time in seconds
5	0.394786
6	0.300032
7	0.48212
8	1.02593
9	2.79231
10	38.6528
11	67.4881
12	191.163

$(1, \omega, \omega^2, \dots, \omega^{N-1})$, where $\omega = e^{2\pi\iota/N}$. If $\tilde{x}$ is the reflected signal, then in the Fourier domain $\hat{\tilde{x}} = \overline{\hat{x}}$. Thus, the action of the reflection in D_{2N} does not correspond to the action of an element of $(S^1)^N$. However, by letting $\hat{x} = (e^{\iota\theta_0}, \dots, e^{\iota\theta_{N-1}}) \odot |\hat{x}|$ we see that $\hat{\tilde{x}} = \overline{\hat{x}} = g_x \hat{x}$, where $g_x = (e^{-2\iota\theta_0}, \dots, e^{-2\iota\theta_{N-1}})$. It follows that $\tilde{x}$ is in the G-orbit of x. Hence the orbit $G \cdot x$ contains the orbit $D \cdot x$ even though the nonabelian group D is not a subgroup of the abelian G.

A similar analysis holds in the real case (as in crystallographic phase retrieval) but the group G of nontrivial symmetries is smaller. The reason is that if g is an arbitrary element of $(S^1)^N$, then $g \cdot \hat{x}$ is not the Fourier transform of a real vector, because x is real if and only $\hat{x}$ is invariant under reflection and conjugation; i.e., $\hat{x}[N-i] = \overline{\hat{x}[i]}$. In particular, $\hat{x}[0]$ is real and if N is even, then $\hat{x}[N/2]$ is real as well. Thus, if $\mathbb{K} = \mathbb{R}$ we let G be the subgroup of $(S^1)^N$ that preserves the Fourier transforms of real vectors: $G = \{(e^{\iota\theta_0}, \dots, e^{\iota\theta_{N-1}}) \,|\, \theta_n + \theta_{N-n} \equiv 0 \bmod 2\pi\}$. If N is odd, then G is isomorphic to $\pm 1 \times (S^1)^{\lfloor N/2 \rfloor}$ and if N is even G is isomorphic to $\pm 1 \times (S^1)^{N/2-1} \times \pm 1$. Again, if $x \in \mathbb{R}^N$, then the orbit $D \cdot x$ is contained in the orbit $G \cdot x$.

5.1. Group-theoretic formulation of Conjecture 4.7.

Given a K-dimensional subspace L (not necessarily sparse), we denote by $G \cdot L$ the orbit of L under the group G. By definition, $G \cdot L = \{g \cdot x \,|\, g \in G, x \in L\} \subset \mathbb{K}^N$ and consists of all vectors $x' \in \mathbb{K}^N$ with the property that $a_{x'} = a_x$ for some fixed $x \in L$. If S' is equivalent to S, then $G \cdot L_S = G \cdot L_{S'}$ because $L_{S'} = d \cdot L_S$ for some $d \in D$, where D is the group of intrinsic symmetries. We can now reformulate our conjectures in group-theoretic terms.

The group-theoretic version of Conjecture 4.7 can be stated as follows.

Conjecture 5.1. *Suppose that $x \in L_S$ is a K-sparse generic signal such that $|S - S| > K$. Then, the orbit $G \cdot x$ contains a single D orbit, which corresponds to the intrinsic symmetries of a K-sparse signal.*

Similarly, Conjectures 4.8 and 4.11 are restated as follows.

Conjecture 5.2 (support recovery). *Suppose that $x \in L_S$ is a K-sparse generic signal such that $|S - S| > K$. Then, $D \cdot L_S$ is the only D orbit of a linear subspace of dimension K contained in $G \cdot L_S$.*

Conjecture 5.3 (generic signal recovery). *Suppose that $x \in L_S$ is a K-sparse generic signal such that $|S - S| > K$. Then, $G \cdot x \cap L_S = D_S \cdot x$, where D_S is the group of intrinsic symmetries of S.*

5.2. Conjecture: Sparse signals are rare among signals with the same autocorrelation.

Given the group-theoretic formulation of the crystallographic phase retrieval problem, we pose an additional conjecture, stating that the set of K-sparse signals among all signals with the same periodic autocorrelation is of measure zero. More precisely, if x is any K-sparse signal with $K \leq N/2+1$, then for a generic element g in the group G of nontrivial symmetries, $g \cdot x$ is not K-sparse. The conjecture implies that even if there exist additional solutions to the crystallographic phase retrieval problem, they are of measure zero. Importantly, this conjecture refers to all signals, not necessarily generic, without imposing any structure on the signal's support.

Conjecture 5.4 (generic transversality). *Let L_S be a K-sparse subspace of $\mathbb{K}^N$ (either $\mathbb{K}=\mathbb{R}$ or $\mathbb{K}=\mathbb{C}$). For generic g in the group G of nontrivial symmetries the following hold:*

1. *If $\mathbb{K}=\mathbb{R}$ and $K < N/2$, then for all K-sparse subspaces $L_{S'}$ (including $S'=S$) the translated subspace $g \cdot L_S$ has 0-intersection with $L_{S'}$ (i.e., $g \cdot L_S \cap L_{S'} = \{0\}$).*
2. *If $\mathbb{K}=\mathbb{C}$ and $K \leq N/2$, then for all K-sparse subspaces $L_{S'}$ (including $S'=S$) the translated subspace $g \cdot L_S$ has 0-intersection with $L_{S'}$.*

In particular, if $K < N/2$, then a generic translate of a sparse subspace contains no sparse vectors.

Verifying Conjecture 5.4 computationally. Given a K-element subset $S \subset [0, N-1]$, we can verify Conjecture 5.4 as follows. If $S = \{i_1, \ldots, i_K\}$ we let $e_{i_1}, \ldots, e_{i_K}$ be the standard basis for L_S, namely, e_{i_j} denotes the vector $(0,0,\ldots 0,1,0\ldots 0)$, where the 1 is in the i_jth place. Then, $g \cdot e_{i_1}, \ldots, g \cdot e_{i_K}$ form a basis for $g \cdot L_S$. Let $S' = \{j_1, \ldots, j_k\}$ be any other K-element subset. Then, $e_{j_1}, \ldots, e_{j_k}$ form a basis for $L_{S'}$, and the $2K$ vectors $\{g \cdot e_{i_1}, \ldots, g \cdot e_{i_K}, e_{j_1}, \ldots, e_{j_K}\}$ span the subspace $g \cdot L_S + L_{S'}$ of $\mathbb{K}^N$. By the standard linear algebra formula

$$\dim(g \cdot L_S + L_{S'}) = \dim g \cdot L_S + \dim L_{S'} - \dim(g \cdot L_S \cap L_{S'}),$$

and thus we have $g \cdot L_S \cap L_{S'} = \{0\}$ if and only if $\dim(g \cdot L_S + L_{S'}) = 2K$. This is equivalent to requiring that the $2K$ vectors $\{g \cdot e_{i_1}, \ldots, g \cdot e_{i_K}, e_{j_1}, \ldots, e_{j_K}\}$ be linearly independent. Therefore, $g \cdot L_S \cap L_{S'} \neq \{0\}$ if and only if the $2K \times N$ matrix,

$$A_{S,S'}(g) = \left[e_{j_1}, e_{j_2}, \ldots, e_{j_K}, g \cdot e_{i_1}, \ldots, g \cdot e_{i_K}\right]^T,$$

spanned by the $2K$ vectors $e_{i_1}, \ldots, e_{i_K}, g \cdot e_{i_1}, \ldots, g \cdot e_{i_K}$ (where we treat the vectors as row vectors) has rank strictly less than $2K$.

Proposition 5.5. *If for each K-elements subset S' there exists a single $g_{S'}$ in each connected component*[6] *of G such that $A_{S,S'}(g_{S'})$ has maximal rank, then for generic $g \in G$ and all K-element subsets S', $g \cdot L_S \cap L_{S'} = \{0\}$.*

Proof. The first K rows of the matrix $A(g_{S'})$ are fixed, while the last K rows depend linearly on the coordinates of $g_{S'} \in G$. The matrix $A_{S,S'}(g)$ fails to have rank $2K$ if and only if all

[6] When $\mathbb{K}=\mathbb{C}$ the group G of nontrivial symmetries is $(S^1)^N$, which is connected. However, if $\mathbb{K}=\mathbb{R}$ and N is odd, then $G = \mathbb{Z}_2 \times (S^1)^{\lfloor N/2 \rfloor}$ and if N is even, then $G = \mathbb{Z}_2 \times (S^1)^{N/2-1} \times \mathbb{Z}_2$. Thus, if $\mathbb{K}=\mathbb{R}$ the group of nontrivial symmetries has either 2 or 4 connected components.

$2K \times 2K$ minors vanish. Each minor is polynomial in the entries of $A_{S,S'}(g_{S'})$ and thus a polynomial in the coordinates of $g_{S'}$. Hence, the set $Z_{S,S'} = \{g \in G \mid \text{rank } A_{S,S'}(g) \text{ is not maximal}\}$ of matrices which do not have maximal rank is an algebraic subset of the real algebraic group G. The set $U = G \setminus \bigcup_{S'} Z_{S,S'}$ is Zariski open and consists of the $g \in G$ such that $g \cdot L_S$ is transverse to all $L_{S'}$. Thus, to verify Conjecture 5.4 for a specific L_S it suffices to prove that the intersection of U with each connected component is nonempty, implying it is dense. In other words, it suffices to find for each subset $L_{S'}$ a single $g_{S'}$ in each connected component of G such that $g_{S'} \cdot L_S$ is transverse to $L_{S'}$. ■

Example 5.6. Using the technique above we verified Conjecture 5.4 for every K-sparse subspace of $\mathbb{C}^{2K}$ with $2 \leq K \leq 7$. We chose for each K a random element $g_K \in G$ and showed that for each pair of K-element subsets of $[0, 2K-1]$ the appropriate matrix had maximal rank. Likewise, we verified the conjecture for every K-sparse subspace of $\mathbb{R}^{2K+1}$ for $2 \leq K \leq 7$. In this case we choose for each K a random element in each connected component of G.

The next example illustrates the technique in detail for a given pair of subspaces and illustrates the differences between the real and complex cases.

Example 5.7. Let $S = \{0,1,2,3\}$ and let $S' = \{0,1,2,7\}$ be subsets $[0,7]$. When $\mathbb{K} = \mathbb{C}$ a random element of G can be taken to have the form $g = (e^{\iota\theta_0}, \ldots, e^{\iota\theta_7})$, where the θ_i are drawn randomly from the interval $[0, 2\pi)$. We used the Mathematica command $G =$ DiagonalMatrix$[e^{i\text{RandomReal}[\{0,2\pi\},8]}]$ to obtain the element:[7]

$$g = [-0.26 + 0.96\iota, -0.87 - 0.47\iota, -0.47 - 0.88\iota, -0.33 + 0.94\iota, 0.70 \\ + 0.71\iota, -0.81 + 0.58\iota, -0.59 - 0.80\iota, -0.09 + 0.99\iota].$$

The matrix $A_{S,S'}$ is the 8×8 matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ -0.34+0.25\iota & -0.06\iota & 0.41+0.26\iota & -0.04+0.07\iota & 0.18-0.25\iota & -0.22+0.16\iota & -0.04+0.57\iota & -0.21-0.04\iota \\ -0.21-0.04\iota & -0.34+0.25\iota & -0.07\iota & 0.41+0.26\iota & -0.05+0.08\iota & 0.18-0.25\iota & -0.22+0.16\iota & -0.04+0.57\iota \\ -0.04+0.57\iota & -0.21-0.04\iota & -0.34+0.25\iota & -0.07\iota & 0.41+0.26\iota & -0.04+0.07\iota & 0.18-0.25\iota & -0.22+0.16\iota \\ -0.07\iota & 0.41+0.26\iota & -0.04+0.07\iota & 0.18-0.25\iota & -0.22+0.16\iota & -0.04+0.57\iota & -0.21-0.04\iota & -0.34+0.25\iota \end{pmatrix}$$

which has nonzero determinant and thus maximal rank. It follows that when $\mathbb{K} = \mathbb{C}$ the general translate of L_S does not intersect $L_{S'}$.

If $\mathbb{K} = \mathbb{R}$ a random element of G has the form $(\pm 1, e^{\iota\theta_1}, e^{\iota\theta_2}, e^{\iota\theta_3}, \pm 1, e^{-\iota\theta 3}, e^{-\iota\theta 2}, e^{-\iota\theta 1})$. We take the element

$$g = [1, 0.44 + 0.9\iota, 0.22 + 0.97\iota, -0.39 + 0.92\iota, 1, -0.39 - 0.92\iota, 0.22 - 0.97\iota, 0.44 - 0.9\iota],$$

[7] We present only the first two significant digits for clear presentation.

and obtain the matrix

$$\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0.31 & -0.41 & 0.2 & -0.22 & 0.29 & -0.07 & 0.18 & 0.71 \\
0.71 & 0.31 & -0.41 & 0.2 & -0.22 & 0.29 & -0.07 & 0.18 \\
0.18 & 0.71 & 0.31 & -0.41 & 0.2 & -0.22 & 0.29 & -0.07 \\
-0.41 & 0.2 & -0.22 & 0.29 & -0.07 & 0.18 & 0.71 & 0.31
\end{pmatrix}$$

which has rank 7, that is rank deficient. It follows that $g \cdot L_S \cap L_{S'} \neq \{0\}$ and thus we expect that every translate of L_S in the identity component of G contains sparse vectors. A similar calculation can be made using a random element of the other components.

6. Higher dimensional autocorrelations.

Our analysis can also be carried out for higher dimensional periodic autocorrelations. Here, a signal is the function $x\colon [0, N-1]^M \to \mathbb{K}$. We denote by $x[\ell_0, \ell_2, \dots \ell_{M-1}]$ the value of x at $(\ell_0, \dots, \ell_{M-1}) \in [0, N-1]^M$. The periodic autocorrelation function $a_x\colon [0, N-1]^M \to \mathbb{K}$ is given by

$$a_x[n_0, \dots, n_{M-1}] = \sum_{(\ell_0, \dots, \ell_{M-1}) \in [0, N-1]^M} x[\ell_0, \dots, \ell_{N-1}] \overline{x[\ell_0 + n_0, \dots, \ell_{M-1} + n_{M-1}]},$$

where all indices are considered modulo N. By definition, the periodic autocorrelation obeys a conjugation-reflection $\mathbb{Z}_2$ symmetry $a_x[n_0, \dots, n_{M-1}] = \overline{a_x[N - n_0, \dots, N - n_{M-1}]}$.

If $K = \mathbb{C}$, then the group $D = (S^1 \times (\mathbb{Z}_N)^M) \ltimes \mathbb{Z}_2$ preserves the autocorrelation. Here, $e^{\iota\phi} \in S^1$ acts by global phase change, $h = (n_0, \dots, n_{M-1}) \in \mathbb{Z}_N^M$ acts by cyclic shift, i.e.,

$$(hx)[\ell_0, \dots, \ell_{M-1}] = x[\ell_0 + n_0, \dots, \ell_{M-1} + n_{M-1}],$$

and $(-1) \in \mathbb{Z}_2$ acts by reflection and conjugation; i.e.,

$$(-1) \cdot x[\ell_0, \dots, \ell_{M-1}] = \overline{x[N - \ell_0, \dots, N - \ell_{M-1}]}.$$

Similarly, if $\mathbb{K} = \mathbb{R}$, then the group $D = (\pm 1 \times (\mathbb{Z}^N)^M) \ltimes \mathbb{Z}_2$ preserves the periodic autocorrelation. In either case we refer to D as the (M-dimensional) group of intrinsic symmetries. Two signals $x\colon [0, N-1]^M \to \mathbb{K}$ are equivalent if they are in the same orbit of the group D of intrinsic symmetries.

Given a subset $S \subset [0, N-1]^M$, we let L_S be the subspace of signals $[0, N-1]^M \to \mathbb{K}$ whose support is contained in S. Let C be the set of equivalence classes of $[0, N-1]^M$ modulo the equivalence relation $(n_0, \dots, n_{M-1}) \sim (N - n_0, \dots, N - n_{M-1})$ and let $S - S$ be the cyclic difference set $\{(n_0 - m_0, \dots, n_{M-1} - m_{M-1}) \,|\, (n_0, \dots, n_{M-1}), (m_0, \dots m_{M-1})\} \subset C$. For a generic $x \in L_S$, the autocorrelation a_x has $|S - S|$ distinct entries up to reflection and conjugation. Again for dimensional reasons we cannot recover a generic signal if $|S - S| < |S|$ since the autocorrelation function, restricted to the subspace L_S, can be viewed as a polynomial function from $\mathbb{K}^{|S|} \to \mathbb{K}^{|S-S|}$.

As in the 1-D case, we expect to be able to recover a generic vector in L_S (up to an action of the group D of intrinsic symmetries) from its higher dimensional autocorrelation a_x provided $|S - S| > |S|$. In other words, we expect that the analogue of Conjectures 4.7, 4.8, and 4.11 when S is a subset of $[0, N-1]^M$ with the property that $|S - S| > |S|$ to hold true. For any specific $S \subset [0, N-1]^M$, this can be verified in a manner similar to the 1-D computational tests, by computing the Hilbert polynomial of an appropriate incidence variety as in sections 4.3.3, 4.3.4.

The problem of recovering a signal from its periodic autocorrelation can be extended to signals defined on any finite abelian group A as discussed in section E. Under this more general framework, the setups considered in this paper are just special cases: in the one 1-D case $A = \mathbb{Z}_N$ and in the multidimensional case $A = \mathbb{Z}_N^M$.

Appendix A. Phase retrieval algorithms and computational complexity.

While this work focuses on the question of uniqueness, we would like to briefly discuss phase retrieval algorithms and the computational complexity of the crystallographic phase retrieval problem; we refer the reader to [27, 24, 26, 43] for further insights.

A.1. Phase retrieval algorithms.

Recall that our goal is to find a signal in the intersection of two nonconvex sets $x_0 \in \mathcal{S} \cap \mathcal{B}$ (1.3). We thus define projectors onto these sets; these projectors are simple and can be computed efficiently. The projection onto $\mathcal{B}$ (1.4) of a general signal $x \in \mathbb{C}^N$ combines the observed Fourier magnitude y_0 from (1.1) with the current estimate of the Fourier phase. Formally, the projector onto $\mathcal{B}$ is defined by

$$P_{\mathcal{B}}(x) = F^{-1}(y_0 \odot \operatorname{sign}(Fx)), \tag{A.1}$$

where "$\odot$" denotes an elementwise product and $\operatorname{sign}(x)[n] = \frac{x[n]}{|x[n]|}$ for any $x[n] \neq 0$ and $\operatorname{sign}(x)[n] = 0$ otherwise. The projector onto $\mathcal{S}$ leaves the K entries with the largest absolute values intact, and zeros out all other entries. Therefore, $P_{\mathcal{S}}(x)$ is a K-sparse signal by definition.

A naive approach to solve the X-ray crystallography phase retrieval problem, and phase retrieval in general, is to apply the two projectors iteratively, i.e.,

$$x \mapsto P_{\mathcal{S}} P_{\mathcal{B}}(x). \tag{A.2}$$

This scheme is called alternating projection in the mathematics literature, and Gerchberg–Saxton in the phase retrieval literature. Unfortunately, for hard problems such as crystallographic phase retrieval, this scheme tends to stagnate quickly in points far away from a solution.

Alternatively, algorithmic schemes which are close relatives of the Douglas–Rachford splitting algorithm [18, 45, 44] and the alternating direction method of multipliers have been proven to be highly effective. These algorithms are based on the reflection operators, defined as $R_{\mathcal{B}} = 2P_{\mathcal{B}} - I$ and $R_{\mathcal{S}} = 2P_{\mathcal{S}} - I$, where I is the identity operator. One representative, simple yet effective, algorithm is called *relaxed reflect reflect* (RRR). For a fixed parameter $\beta \in (0, 2)$, the RRR iterations read

$$x \mapsto x + \frac{1}{2}(I + \beta R_{\mathcal{B}} R_{\mathcal{S}})(x) \tag{A.3}$$

or, more explicitly,

$$x \mapsto x + \beta(P_{\mathcal{B}}(2P_{\mathcal{S}}(x) - x) - P_{\mathcal{S}}(x)). \tag{A.4}$$

For $\beta = 1$ this algorithm coincides with Douglas–Rachford. Other variations of Douglas–Rachford that are used in practice include Fienup's hybrid input-output algorithm [28], the difference map algorithm [23], and the relaxed averaged alternating reflections algorithm [46]. In addition to phase retrieval, these algorithms seem to be surprisingly effective for a variety of challenging feasibility problems, such as the Diophantine equations, sudoku, and protein conformation determination [27]; recently, it was even applied to deep learning [25]. One specific interesting property of RRR (and most of its relatives) is that—in contrast to optimization-based algorithms—it stagnates only when it finds a point from which the intersection $\mathcal{S} \cap \mathcal{B}$ can be found trivially by projection. Note that this property does not guarantee finding a solution in a finite number of steps.

A.2. Computational complexity.

Strong empirical evidence suggests that the computational complexity of RRR for the crystallographic phase retrieval problem increases exponentially fast with K [26]; however, rigorous theoretical analysis is lacking.

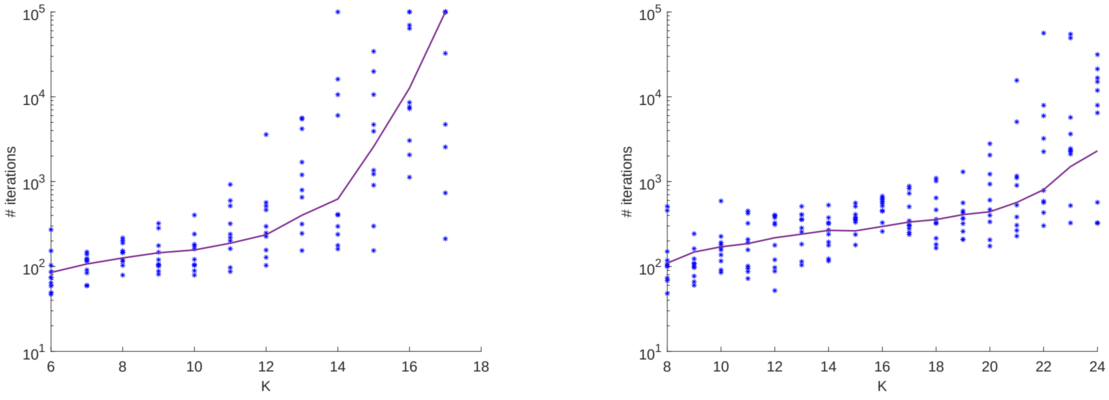
To illustrate the computational complexity, we ran RRR with step size parameter $\beta = 1/2$ (chosen empirically), $N = 50$, and varying K, and counted how many iterations are required to reach a solution from a random initialization.[8] To measure the error while taking symmetries into account, we define

$$\text{error} = \min_{g \in D} \frac{\|g \cdot x_{\text{est}} - x_0\|_2^2}{\|x_0\|_2^2}, \tag{A.5}$$

where x_{est} is the estimated signal and $D = \mathbb{Z}_2 \times D_{2N}$—the group of intrinsic symmetries. A solution was declared when the error dropped below 10^{-8}. Plainly, this measure cannot be used in practice since it requires knowing the sought signal, but it suffices for the purposes of this work. In practice, a natural error measure is $\eta = \frac{\|P_{\mathcal{S}}(x)\|_2^2}{\|x\|_2}$: this index measures the portion of the signal's energy concentrated in the dominant K entries of the current estimate [26]. To generate the underlying signal, we drew a random set of K indices from $[0, N-1]$ to form the support set S. Then, each entry $x[i]$ for $i \in S$ was drawn i.i.d. from a uniform distribution over $[0, 1]$. The rest of the entries were set to zero. Figure 4 shows that the median number of iterations required to reach a solution grows exponentially fast. We believe that this is not a flaw of RRR, but an indication for the computational hardness of the crystallographic phase retrieval problem, regardless of any specific algorithm. In particular, as far as we know, there are no polynomial-time algorithms for this problem. The iteration counts also display a considerable variability.

The exponential computational complexity of RRR restricts our ability to empirically verify the conjectured uniqueness limit $K \approx N/2$ for large values of N. Unfortunately, for small N, there are few subsets S that satisfy the necessary condition $|S - S| > K$. As a compromise, we conducted an experiment with $N = 8$ and $K = 3, 4$. For each K, we ran 1000

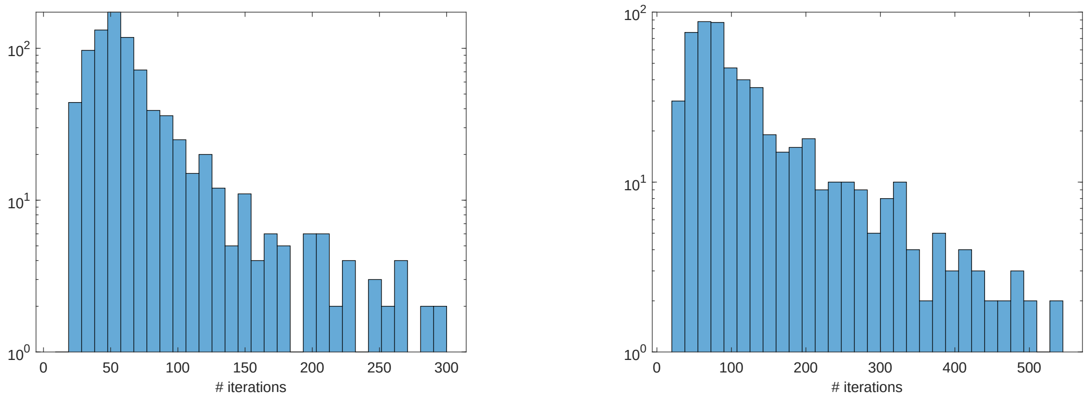
[8] The code to reproduce this experiment, as well as to regenerate all other figures in the paper, is publicly available at https://github.com/TamirBendory/crystallographicPR.



(a) N = 50

(b) N = 100

Figure 4. *The median number of RRR iteration counts (running time) over* 500 *trials per* K *for* $N = 50$ *(left) and* $N = 100$ *(right). As can be seen, the iteration counts grow exponentially fast with* K*. The blue asterisks present the specific iteration count of* 10 *individual trials per* K*, and are used only to illustrate the high variability of the results.*



(a) K=3

(b) K=4

Figure 5. *Iteration counts (running time) histograms over* 1000 *trials for* $N = 8$ *and* $K = 3, 4$*. The iteration counts decay at an exponential rate. Only the left ends of the histograms (that include almost all trials) are presented for clear visualization.*

trials with random support sets that satisfy $|S - S| > K$. The maximum number of iterations was set to 10^7. For $K = 3$, 77 trials out of 1000 reached the maximal number of iterations. In other words, 85% of the trials were declared successful. For $K = 4$, only 60% of the trials were successful. Figure 5 shows the empirical distribution of the iteration counts, which decays at an exponential rate.

Appendix B. Density of sets with small difference sets.

For a given value of K and N, an important mathematical question is to estimate the number of K-element subsets S with the property that $|S - S| \leq K$. This question is quite subtle and relates to some deep problems in additive number theory. It is beyond the scope of this paper to obtain this analysis, but classic results of Kemperman [41] (see also [42]) give a technique for enumerating the sets S with this property. This classification is somewhat involved and depends on the prime factorization of N. However, if N is prime, then Kemperman's results imply the following.

Proposition B.1. *If N is prime, then $|S - S| \leq |S|$ if and only if S is an arithmetic progression.*

Proof. Denote by $S -^{\mathbb{Z}_N} S \subset \mathbb{Z}_N$ the set of differences $\{i - j | i, j \in S\} \subset \mathbb{Z}_N$. (Here we do not identify an element and its negative in $\mathbb{Z}_N$.) Because $0 \in S -^{\mathbb{Z}_N} S$ is its own negative, it follows that $|S -^{\mathbb{Z}_N} S| \leq 2|S - S| - 1$. Hence, if $|S - S| \leq |S|$, then $|S -^{\mathbb{Z}_N} S| < 2|S| = |S| + |-S|$, where $-S = \{-i | i \in S\}$. In this case [41, Corollary, p. 74] implies that S is an arithmetic progression.

Conversely, if $S = \{a_0, a_0 + d, \ldots, a_0 + (d-1)K\}$, then $S - S = \{0, \overline{d}, \ldots, \overline{(d-1)K}\}$, where $\overline{m}$ indicates the element of $[0, N/2]$ corresponding to the equivalence class of m under the equivalence relation $m \sim -m$. ■

Let $\mathcal{S}_K$ be the set of K-element subsets of $[0, N-1]$ and let $\mathcal{T}_K$ be the set of K-element subsets of $[0, N-1]$ such that $|S - S| < |S|$. The following corollary says that, at least when N is prime, the probability of picking a subset with $|S - S| < |S|$ drops quickly to 0 as $N \to \infty$.

Proposition B.2. *For prime N and $K/N \leq 1/2$, the ratio $|\mathcal{T}_K|/|\mathcal{S}_K|$ tends to 0 as $N \to \infty$.*

Proof. By Proposition B.1, when N is prime, $S \in \mathcal{T}_K$ if and only if S is an arithmetic progression of length K. The equivalence class of an arithmetic progression is determined by its difference $d \in \mathbb{Z}_N$. Moreover, any progression with difference d is equivalent under the action of the dihedral group to a progression with difference $N - d$. Thus, the number of equivalence classes of arithmetic progressions equals $N/2$. Since the dihedral group D_{2N} has $2N$ elements we see that that the total number of arithmetic progressions is $\sim N^2$. On the other hand, the total number of K-element subsets is $\binom{N}{K}$. Thus, the ratio $|\mathcal{T}_K|/|\mathcal{S}_K| \sim \frac{N^2}{\binom{N}{K}}$ which goes quickly to 0 as $N \to \infty$. ■

We expect that a more refined analysis using Kemperman's classification will show that the number of equivalence classes of S such that $|S - S| \leq K$ is asymptotic to 0 even for composite N; see Figures 1 for supporting empirical evidences. However, deriving such a results analytically is beyond the scope of the current work.

Appendix C. Proof of Proposition 4.2.

In order for S to be collision free we need that every nonzero element of the multiset $S - S$ appears with multiplicity exactly one so that $|S - S|$ is maximized. If $|S| = K$, then the number of nonzero differences (counted with multiplicity) in $S - S$ is $\binom{K}{2}$. Thus, S is collision free if and only if $|S - S| = \binom{K}{2} + 1$. (We add one because $0 \in |S - S|$). Thus, a necessary condition for $[0, N-1]$ to contain any collision-free subset is that $\binom{K}{2} + 1 \leq N$. For any fixed value of R, the function $\binom{RN}{2} + 1$ grows quadratically in N. Therefore, for N sufficiently large, $\binom{K}{2} + 1 > N$ so there can be no collision-free subsets.

Appendix D. Hilbert polynomial, dimensions and degrees of varieties. Consider the polynomial ring $R = \mathbb{K}[x_0, \dots, x_n]$, where $\mathbb{K}$ is a field. For each d, the set R_d consisting of homogeneous polynomials of degree d is a finite dimensional $\mathbb{K}$-vector subspace with basis consisting of the monomials of degree d in $x_0, \dots, x_n$. A well-known combinatorial formula for the number of monomials implies that $\dim_{\mathbb{K}} R_d = \binom{n+d}{d}$. For example, if $n = 1$, then $\dim R_d$ is the number of binary forms of degree 2 in $(n+1)$-variables which is $d + 1 = \binom{d+1}{d}$. Note that function $d \mapsto \dim R_d$ is a polynomial in d of degree n.

Given a set of homogenous polynomials $f_1, \dots, f_r$, let $I = (f_1, \dots, f_r)$ be the ideal they generate. The *Hilbert function* H_I is defined as the function $d \mapsto \dim(R/I)_d$, where $(R/I)_d$ denotes the subspace of R/I, consisting of homogeneous elements of degree d. The *Hilbert–Serre theorem* [33, Theorem I.7.5] states that there exists an integer valued polynomial P_I such that for $d \gg 0$, $H_I(d) = P_I(d)$. The polynomial P_I is called the *Hilbert polynomial* of I. If we set P_k to be the polynomial $P_k(d) = \binom{k+d}{d}$, then we can write

$$P_I = a_\ell P_l + a_{\ell-1} P_{l-1} + \cdots + a_0 P_0$$

with $a_0, \dots, a_\ell$ integers and $a_\ell > 0$.

In addition, the Hilbert–Serre theorem implies that $\deg P_I$ equals the dimension of the subvariety of the projective space $\mathbb{P}^n$ defined by the homogeneous polynomials $f_1, \dots, f_r$. Equivalently if we consider $Z(f_1, \dots, f_r)$ as a subset of $\mathbb{K}^n$, then $\deg P_I = \dim Z(I) - 1$. Moreover, the coefficient a_ℓ is positive and equal to the degree of $Z(I)$ as a projective variety, where the degree of a projective variety $Z(I)$ of dimension ℓ is defined as the number of points in the intersection $Z(I) \cap L_{n-\ell}$, where $L_{n-\ell}$ is a general linear subspace of dimension $n - \ell$ [33, Theorem 7.7].

Using the Hilbert function we can obtain the following proposition which we use in section 4.3.4.

Proposition D.1. *Suppose that* $\dim Z(I) = \ell$ *and has degreee* a. *If* $Z(I)$ *contains* ℓ*-dimensional linear subspaces* $L_1, \dots, L_a$, *then* $\dim Z(I) \setminus (L_1 \cup \cdots \cup L_a) < \ell$.

Proof. Let I_L be the ideal generated by the linear forms defining the subspaces $L_1, \dots, L_a$. By [33, Proposition 7.6], $Z(I_L)$ has dimension ℓ and degree a_ℓ. Thus, $P_{I_L} = a_\ell P_\ell + \tilde{P}$ for some lower degree terms $\tilde{P}$. Hence, $Z(I)$ and $L_1 \cup \cdots \cup L_a$ have the same degree and dimension. Let Y be the closure of $Z(I) \smallsetminus (L_1 \cup \cdots \cup L_a)$ in $\mathbb{P}^n$. Then $Z(I) = Y \cup (L_1 \cup \cdots \cup L_a)$. Since $Y \subset Z(I)$ we know that $\dim Y \leq \dim Z(I)$. Suppose that $\dim Y = \dim Z(I)$. Then by [33, Proposition 7.6b], $\deg Z(I) = \deg Y + \deg(L_1 \cup \cdots \cup L_a)$. But since $\deg Z(I) = a$ this a contradiction. Hence, $\dim Y < \dim Z(I)$. ■

The Hilbert function of an ideal generated by polynomials $f_1, \dots, f_r$ with rational coefficients can be computed exactly using a computer algebra system. This is automated in two steps, which are executed by the command `hilbertPolynomial` in Macaulay2 [31]. The first step is to replace the generators $f_1, \dots, f_r$ of the ideal I with new generators $g_1, \dots, g_t$ called a Gröbner basis; see [22, Chapter 15] for the definition of a Gröbner basis. Given a Gröbner basis, the problem of computing the Hilbert polynomial of an ideal is combinatorial. Both steps can be computed to infinite precision using a computer algebra system. Although neither step can be performed in polynomial time, implemented algorithms are efficient when the number of variables is relatively small.

Appendix E. Sparse periodic phase retrieval in finite abelian groups.

The sparse phase retrieval problem can be generalized to any finite abelian group. Let A be a finite abelian group. We denote the composition operation by $+$, the identity by 0, and the inverse of an element a as $-a$. Let V be the $\mathbb{K}$-vector space of functions $x\colon A \to \mathbb{K}$. In the case of one-dimensional phase retrieval $A = \mathbb{Z}_N$ is a cyclic group, and in the case of higher dimensional phase retrieval $A = \mathbb{Z}_N^M$ is a product of cyclic groups of the same order. The autocorrelation of $x \in V$ is the function $a_x\colon A \to \mathbb{K}$ defined by the formula

$$a_x[\ell] = \sum_{\ell' \in A} x[\ell']\overline{x[\ell + \ell']}. \tag{E.1}$$

The function $a\colon V \to V, x \mapsto a_x$ is invariant under the group $D_A = (S^1 \times A) \ltimes \mathbb{Z}_2$ if $\mathbb{K} = \mathbb{C}$ or $D_A = (\pm 1 \times A) \ltimes \mathbb{Z}_2$ and $\mathbb{K} = \mathbb{R}$. Here, S^1 (resp., ± 1) acts by a scalar multiplication, A acts by translation, that is,

$$(\ell \cdot x)[\ell'] = x[\ell' + \ell]$$

for some $\ell \in A$, and $\mathbb{Z}_2$ acts by conjugation and reflection, i.e.,

$$(-1 \cdot x)[\ell] = \overline{x[\ell]}.$$

If we let $C = A/\mathbb{Z}_2$, where $\mathbb{Z}_2$ acts on A by $(-1 \cdot \ell) = -\ell$, then we can define the "difference set" $S - S = \{\ell_1 - \ell_2 \,|\, \ell_1, \ell_2 \in A\} \subset C$. With this setup, our main conjecture is as follows.

Conjecture E.1. *Suppose that S is a subset of A such that $|S - S| > |S|$ and $x \in L_S$ is a generic signal. Then, $a_x = a_{x'}$ implies that x' is obtained from x by an action of the group D_A of intrinsic symmetries.*

Similarly, we can formulate general group-theoretic versions of Conjectures 4.8 and 4.11. To establish notation we note that the group $A \ltimes \mathbb{Z}_2$ (the analog of the dihedral group) acts on the set of subsets of A, where $a \in A$ acts by translation, i.e., $a + S = \{a + s | s \in S\}$ and the nontrivial element in $\mathbb{Z}_2$ acts by "reflection," i.e., it maps S to $-S = \{-s | s \in S\}$. We say that two subsets S, S' are equivalent if $S' = g \cdot S$ for some $g \in A \ltimes \mathbb{Z}_2$. Given a subset $S \subset A$, we denote by $D_{S,A}$ the subgroup of D_A that preserves L_S and again refer to it as the group of intrinsic symmetries of the subspace L_S.

Conjecture E.2. *Suppose that S and S' are two nonequivalent K-element subsets of an abelian group A with $|S - S| = |S' - S'| > K$. Then, for generic $x \in L_S$, $a(x)$ is not in $a(L_{S'})$. Namely, the support of x is determined up to equivalence under the action of the group $A \ltimes \mathbb{Z}_2$ by the periodic autocorrelation of x.*

Conjecture E.3. *Suppose that $|S - S| > |S|$. If $x \in L_S$ is a generic vector and $x' \in L_S$ is another vector (in the same subspace) such that $a(x) = a(x')$, then $x' = g \cdot x$ for some $g \in D_{S,A}$.*

Acknowledgments. The authors thank Ti-Yen Lan for his comments on an early draft of this paper, and the anonymous referees for their valuable comments and suggestions.

REFERENCES

[1] *The Cambridge Structural Database (CSD)*. https://www.ccdc.cam.ac.uk/solutions/csd-system/components/csd/.

[2] R. Balan, P. Casazza, and D. Edidin, *On signal reconstruction without phase*, Appl. Comput. Harmon. Anal., 20 (2006), pp. 345–356.

[3] A. S. Bandeira, B. Blum-Smith, J. Kileel, A. Perry, J. Weed, and A. S. Wein, *Estimation under Group Actions: Recovering Orbits from Invariants*, preprint, arXiv:1712.10163.

[4] D. A. Barmherzig, J. Sun, P.-N. Li, T. Lane, and E. J. Candès, *Holographic phase retrieval and reference design*, Inverse Problems, 35 (2019), 094001.

[5] A. Barnett, C. L. Epstein, L. Greengard, and J. Magland, *Geometry of the Phase Retrieval Problem*, Inverse Problems, to appear.

[6] R. Beinert and G. Plonka, *Ambiguities in one-dimensional discrete phase retrieval from Fourier magnitudes*, J. Fourier Anal. Appl., 21 (2015), pp. 1169–1198.

[7] R. Beinert and G. Plonka, *Enforcing uniqueness in one-dimensional phase retrieval by additional signal information in time domain*, Appl. Comput. Harmon. Anal., 45 (2018), pp. 505–525.

[8] T. Bendory, A. Bartesaghi, and A. Singer, *Single-particle cryo-electron microscopy: Mathematical theory, computational challenges, and opportunities*, IEEE Signal Process. Mag., 37 (2020), pp. 58–76.

[9] T. Bendory, R. Beinert, and Y. C. Eldar, *Fourier phase retrieval: Uniqueness and algorithms*, in Compressed Sensing and its Applications, Springer, Cham, Switzerland, 2017, pp. 55–91.

[10] T. Bendory, D. Edidin, and Y. C. Eldar, *Blind phaseless short-time Fourier transform recovery*, IEEE Trans. Inform. Theory, 66 (2020), pp. 3232–3241.

[11] T. Bendory, D. Edidin, and Y. C. Eldar, *On signal reconstruction from FROG measurements*, Appl. Comput. Harmon. Anal., 48 (2020), pp. 1030–1044.

[12] T. Bendory, Y. C. Eldar, and N. Boumal, *Non-convex phase retrieval from STFT measurements*, IEEE Trans. Inform. Theory, 64 (2017), pp. 467–484.

[13] T. Bendory, P. Sidorenko, and Y. C. Eldar, *On the uniqueness of FROG methods*, IEEE Signal Process. Lett., 24 (2017), pp. 722–726.

[14] T. T. Cai, X. Li, and Z. Ma, *Optimal rates of convergence for noisy sparse phase retrieval via thresholded Wirtinger flow*, Ann. Statist., 44 (2016), pp. 2221–2251.

[15] E. J. Candès, Y. C. Eldar, T. Strohmer, and V. Voroninski, *Phase retrieval via matrix completion*, SIAM Rev., 57 (2015), pp. 225–251.

[16] Y. Chen and E. J. Candès, *Solving random quadratic systems of equations is nearly as easy as solving linear systems*, Comm. Pure Appl. Math., 70 (2017), pp. 822–883.

[17] A. Conca, D. Edidin, M. Hering, and C. Vinzant, *An algebraic characterization of injectivity in phase retrieval*, Appl. Comput. Harmon. Anal., 38 (2015), pp. 346–356.

[18] J. Douglas and H. H. Rachford, *On the numerical solution of heat conduction problems in two and three space variables*, Trans. Amer. Math. Soc., 82 (1956), pp. 421–439.

[19] T. W. Dubé, *The structure of polynomial ideals and Gröbner bases*, SIAM J. Comput., 19 (1990), pp. 750–773, https://doi.org/10.1137/0219053.

[20] D. Edidin, *Projections and phase retrieval*, Appl. Comput. Harmon. Anal., 42 (2017), pp. 350–359.

[21] D. Edidin, *The geometry of ambiguity in one-dimensional phase retrieval*, SIAM J. Appl. Algebra Geom., 3 (2019), pp. 644–660.

[22] D. Eisenbud, *Commutative Algebra: With a View Toward Algebraic Geometry*, Grad. Texts in Math. 150, Springer, New York, 2013.

[23] V. Elser, *Phase retrieval by iterated projections*, J. Opt. Soc. Amer. A, 20 (2003), pp. 40–55.

[24] V. Elser, *The complexity of bit retrieval*, IEEE Trans. Inform. Theory, 64 (2017), pp. 412–428.

[25] V. Elser, *Learning Without Loss*, preprint, arXiv:1911.00493, 2019.

[26] V. Elser, T.-Y. Lan, and T. Bendory, *Benchmark problems for phase retrieval*, SIAM J. Imaging Sci., 11 (2018), pp. 2429–2455.

[27] V. Elser, I. Rankenburg, and P. Thibault, *Searching with iterated maps*, Proc. Natl. Acad. Sci. USA, 104 (2007), pp. 418–423.

[28] J. R. Fienup, *Phase retrieval algorithms: A comparison*, Appl. Opt., 21 (1982), pp. 2758–2769.

[29] D. Gabor, *A new microscopic principle*, Nature, 161 (1948), pp. 777–778.

[30] T. Goldstein and C. Studer, *Phasemax: Convex phase retrieval via basis pursuit*, IEEE Trans. Inform. Theory, 64 (2018), pp. 2675–2689.

[31] D. R. Grayson and M. E. Stillman, *Macaulay*2, http://www.math.uiuc.edu/Macaulay2/.

[32] D. Gross, F. Krahmer, and R. Kueng, *Improved recovery guarantees for phase retrieval from coded diffraction patterns*, Appl. Comput. Harmon. Anal., 42 (2017), pp. 37–64.

[33] R. Hartshorne, *Algebraic Geometry*, Vol. 52, Springer, New York, 1997.

[34] M. Hayes, *The reconstruction of a multidimensional sequence from the phase or magnitude of its Fourier transform*, IEEE Trans. Acoust. Speech Signal Process., 30 (1982), pp. 140–154.

[35] R. Hesse and D. R. Luke, *Nonconvex notions of regularity and convergence of fundamental algorithms for feasibility problems*, SIAM J. Optim., 23 (2013), pp. 2397–2419.

[36] K. Huang, Y. C. Eldar, and N. D. Sidiropoulos, *Phase retrieval from* 1*D Fourier measurements: Convexity, uniqueness, and algorithms*, IEEE Trans. Signal Process., 64 (2016), pp. 6105–6117.

[37] M. A. Iwen, A. Viswanathan, and Y. Wang, *Fast phase retrieval from local correlation measurements*, SIAM J. Imaging Sci., 9 (2016), pp. 1655–1688.

[38] K. Jaganathan, Y. C. Eldar, and B. Hassibi, *STFT phase retrieval: Uniqueness guarantees and recovery algorithms*, IEEE J. Sel. Topics Signal Process., 10 (2016), pp. 770–781.

[39] K. Jaganathan, S. Oymak, and B. Hassibi, *Recovery of sparse* 1*-D signals from the magnitudes of their Fourier transform*, in 2012 IEEE International Symposium on Information Theory Proceedings, IEEE, Piscataway, NJ, 2012, pp. 1473–1477.

[40] K. Jaganathan, S. Oymak, and B. Hassibi, *Sparse phase retrieval: Uniqueness guarantees and recovery algorithms*, IEEE Trans. Signal Process., 65 (2017), pp. 2402–2410.

[41] J. H. Kemperman, *On small sumsets in an abelian group*, Acta Math., 103 (1960), pp. 63–88.

[42] V. F. Lev, *On small sumsets in abelian groups*, Astérisque, 258 (1999), pp. 317–321.

[43] E. Levin and T. Bendory, *A Note on Douglas-Rachford, Subgradients, and Phase Retrieval*, preprint, arXiv:1911.13179, 2019.

[44] G. Li and T. K. Pong, *Douglas–Rachford splitting for nonconvex optimization with application to nonconvex feasibility problems*, Math. Program., 159 (2016), pp. 371–401.

[45] S. B. Lindstrom and B. Sims, *Survey: Sixty Years of Douglas–Rachford*, J. Aust. Math. Soc., to appear.

[46] D. R. Luke, *Relaxed averaged alternating reflections for diffraction imaging*, Inverse Problems, 21 (2004), pp. 37–50.

[47] A. M. Maiden, M. J. Humphry, F. Zhang, and J. M. Rodenburg, *Superresolution imaging via ptychography*, J. Opt. Soc. Amer. A, 28 (2011), pp. 604–612.

[48] S. Marchesini, Y.-C. Tu, and H.-T. Wu, *Alternating projection, ptychographic imaging and phase synchronization*, Appl. Comput. Harmon. Anal., 41 (2016), pp. 815–851.

[49] R. P. Millane, *Phase retrieval in crystallography and optics*, J. Opt. Soc. Amer. A, 7 (1990), pp. 394–411.

[50] H. Ohlsson and Y. C. Eldar, *On conditions for uniqueness in sparse phase retrieval*, in 2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), IEEE, Piscataway, NJ, 2014, pp. 1841–1845.

[51] G. E. Pfander and P. Salanevich, *Robust phase retrieval algorithm for time-frequency structured measurements*, SIAM J. Imaging Sci., 12 (2019), pp. 736–761.

[52] H. M. Phan, *Linear convergence of the Douglas–Rachford method for two closed sets*, Optimization, 65 (2016), pp. 369–385.

[53] J. Ranieri, A. Chebira, Y. M. Lu, and M. Vetterli, *Phase Retrieval for Sparse Signals: Uniqueness Conditions*, preprint, arXiv:1308.3058, 2013.

[54] O. Raz, N. Dudovich, and B. Nadler, *Vectorial phase retrieval of* 1*-D signals*, IEEE Trans. Signal Process., 61 (2013), pp. 1632–1643.

[55] J. M. Rodenburg, *Ptychography and related diffractive imaging methods*, Adv. Imag. Elect. Phys., 150 (2008), pp. 87–184.

[56] 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., 32 (2015), pp. 87–109.

[57] M. Soltanolkotabi, *Structured signal recovery from quadratic measurements: Breaking sample complexity barriers via nonconvex optimization*, IEEE Trans. Inform. Theory, 65 (2019), pp. 2374–2400.

[58] J. Sun, Q. Qu, and J. Wright, *A geometric analysis of phase retrieval*, Found. Comput. Math., 18

(2018), pp. 1131–1198.

[59] R. Trebino, *Frequency-Resolved Optical Gating: The Measurement of Ultrashort Laser Pulses*, Kluwer, Boston, 2002.

[60] I. Waldspurger, A. d'Aspremont, and S. Mallat, *Phase recovery, maxcut and complex semidefinite programming*, Math. Program., 149 (2015), pp. 47–81.

[61] W. H. Wong, Y. Lou, and T. Zeng, *Phase Retrieval for Binary Signals: Box Relaxation and Uniqueness*, preprint arXiv:1904.10157, 2019.