Appl. Comput. Harmon. Anal. 66 (2023) 151–160

Contents lists available at ScienceDirect

Applied and Computational Harmonic Analysis

journal homepage: www.elsevier.com/locate/acha

Letter to the Editor

Finite alphabet phase retrieval

Tamir Bendory, Dan Edidin *, Ivan Gonzalez

ARTICLE INFO

Article history:
Received 25 January 2023
Received in revised form 31 March 2023
Accepted 20 April 2023
Available online 9 May 2023
Communicated by Radu Balan

Keywords:
Phase retrieval
Homometric sets
Sparse signals

ABSTRACT

We consider the finite alphabet phase retrieval problem: recovering a signal whose entries lie in a small alphabet of possible values from its Fourier magnitudes. This problem arises in the celebrated technology of X-ray crystallography to determine the atomic structure of biological molecules. Our main result states that for generic values of the alphabet, two signals have the same Fourier magnitudes if and only if several partitions have the same difference sets. Thus, the finite alphabet phase retrieval problem reduces to the combinatorial problem of determining a signal from those difference sets. Notably, this result holds true when one of the letters of the alphabet is zero, namely, for sparse signals with finite alphabet, which is the situation in X-ray crystallography.

1. Introduction

X-ray crystallography is a leading technology for determining the 3-D atomic structure of biological molecules, such as proteins. Indeed, thousands of new crystal structures are resolved each year, and more than a dozen Nobel Prizes have been awarded for work involving X-ray crystallography. In X-ray crystallography, the crystal—a periodic arrangement of a repeating unit—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. The signal to be estimated (the electron density function of the crystal) is supported only at the sparsely-spread positions of atoms [13]. Therefore, the *crystallographic phase retrieval problem* entails recovering a sparse signal from its Fourier magnitudes. The crystallographic phase retrieval is a special case of the *phase retrieval* problem, which refers to all problems that involve recovering a signal from its Fourier magnitudes, see [22,1,9,3] and reference therein. A detailed mathematical model of X-ray crystallography is introduced in [7].

A recent paper by a subset of the authors provides the first rigorous attempt to establish a mathematical theory for the crystallographic phase retrieval problem [2]. In particular, it was conjectured that a generic sparse signal $x \in \mathbb{R}^N$ whose support has size at most K is uniquely determined, up to un-

* Corresponding author.
E-mail address: edidind@missouri.edu (D. Edidin).

https://doi.org/10.1016/j.acha.2023.04.005

avoidable ambiguities, as long as $K \leq N/2$. The conjecture was verified for a small set of parameters; see also [8,17].

In practice, however, a more accurate model of the crystallographic phase retrieval problem should account for sparse signals whose non-zero 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. In this paper, we make a first step towards this direction. Specifically, we study the problem of recovering a discrete one-dimensional periodic signal, whose entries are taken from a finite alphabet, from its Fourier magnitudes. We refer to this problem as the *finite alphabet phase retrieval problem*. We note that recovering problems of finite alphabet signals were studied before, but mostly under linear models [12,11,21,20].

In particular, we show that for generic choice of entries in the alphabet, the finite alphabet phase retrieval problem can be reduced to a combinatorial problem involving difference sets. This is similar to the situation for binary phase retrieval (a problem studied before [6]) but new combinatorial subtleties can occur. More specifically, we show that two signals with entries taken from a finite alphabet have the same Fourier magnitudes if and only if the associated partitions have the same difference sets; see Proposition 4.2. Notably, this result remains true when one of the letters of the alphabet is zero, namely, for sparse signals with finite alphabet; see Theorem 4.3. This is the situation in X-ray crystallography where crystals are typically very sparse; the non-zero values occupy only $\sim 1/100$ of the signal's support [6]. Unfortunately, the problem of analyzing if specific difference sets determine a set uniquely (up to unavoidable symmetries) is an extremely difficult combinatorial problem [19, p. 350], [18, Section 3]. Therefore, we cannot provide a complete characterization when a finite-alphabet signal can be recovered uniquely, up to unavoidable symmetries, from its Fourier magnitudes.

Remark 1.1. In this paper we follow a long tradition in the crystallography literature and restrict our discussion to the one-dimensional phase retrieval problem for periodic signals. This corresponds to viewing our signals as functions on the cyclic group $\mathbb{Z}_N$. As was the case in [2], much of our theory can be readily adapted to study functions on any abelian group such as $\mathbb{Z}_N \times \mathbb{Z}_N$; see Section 6.1.

The rest of the paper is organized as follows. Section 2 provides a necessary background on difference sets, homometric sets, and autocorrelations. Section 3 begins our analysis by studying signals whose entries are taken from two-letters alphabet. Section 4 presents and proves our main results about phase retrieval of signals whose entries are taken from a finite alphabet. Section 5 provides a few examples and introduces the intriguing notion of pseudo-equivalent partitions. Section 6 introduces a few possible directions for future research on this problem.

2. Background

We begin by introducing basic definitions about difference sets. For any $i, j \in [0, N-1]$, we define the *cyclic distance* between i and j by

$$d(i,j) = \min\{N - |i-j|, |i-j|\}. \tag{2.1}$$

We note that $d(i,j) \in [0, \lfloor N/2 \rfloor]$ as illustrated in Fig. 1.

Definition 2.1 *(Difference sets).* Let A, B be two subsets of $[0, N-1]$. We define the cyclic difference multi-set by

$$A - B = \{d(i,j) \mid i \in A, j \in B\}. \tag{2.2}$$

In particular, the self difference multi-set is given by $A - A = \{d(i,j) \mid i \leq j \in A\}$.

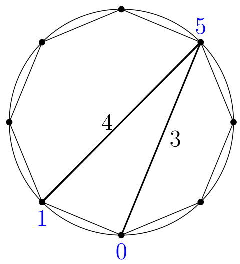

Fig. 1. Illustration of the cyclic distances between the points 0 and 5 and 1 and 5 in $[0, 7]$.

Definition 2.2 *(The dihedral group).* The dihedral group D_{2N} is the group of symmetries of the regular N-gon. It is a group of order $2N$, which is generated by two elements r (rotation) and s (reflection). The elements r, s satisfy the relations $r^N = s^2 = e$ and $rs = sr^{N-1}$, where e is the identity. The group D_{2N} acts on the set $[0, N-1]$ as follows. The element $r \in D_{2N}$ acts by cyclic shift; i.e., $r(i) = (i+1) \bmod N$ and the element s acts by the reflection $s(i) = N - i$.

Next, we define equivalence classes. Since the Fourier magnitude is invariant under cyclic shifts and reflection (i.e., under the dihedral group), we can only hope to determine the support of a signal from the signal's Fourier magnitudes up to an action of the dihedral group D_{2N}.

Definition 2.3. Two subsets $A, B \subset [0, N-1]$ are *equivalent* if there exists an element $\sigma \in D_{2N}$ such that $B = \sigma A$.

Another fundamental definition is that of homometric sets: subsets with the same difference set.

Definition 2.4. Two subsets A, B are *homometric* if $A - A = B - B$.

Lemma 2.5. *If A, B are equivalent then they are homometric.*

Proof. The lemma is an immediate consequence of the fact that the cyclic distance $d(i, j)$ is invariant under cyclic shifts and reflection. $\square$

A key fact we use about homometric subsets of $[0, N-1]$ is the following result, originally stated by Patterson [16]. For a modern proof, see [10, Corollary 1] or [5].

Theorem 2.6 *(Patterson). Two sets $A, B \subset [0, N-1]$ are homometric if and only if their complements are homometric as well.*

We now consider the case of partitions. Let $A_1, \ldots, A_K$ and $B_1, \ldots, B_K$ be two ordered partitions of $[0, N-1]$.

Definition 2.7. Two ordered partitions $A_1, \ldots, A_K$ and $B_1, \ldots, B_K$ are *homometric* if $A_i - A_j = B_i - B_j$ for all pairs $i, j \in \{1, \ldots, K\}$. Two ordered partitions $A_1, \ldots, A_K$ and $B_1, \ldots, B_K$ are *equivalent* if there exists $\sigma \in D_{2N}$ such that $B_i = \sigma A_i$ for all $i \in \{1, \ldots, K\}$.

Lemma 2.5 can be directly extended to ordered partitions.

Lemma 2.8. *Equivalent partitions are homometric.*

Before moving to the next section, we remind the reader of a couple of definitions from signal processing.

Definition 2.9 *(Power spectrum and periodic autocorrelation).* The power spectrum of a signal $x \in \mathbb{C}^N$ is the vector $|\hat{x}|^2 \in \mathbb{R}^N_{\geq 0}$, where $\hat{x}$ is the discrete Fourier transform (DFT) of x and the absolute value is taken componentwise. The periodic auto-correlation of x is defined by

$$a_x[\ell] = \sum_{n=0}^{N-1} x[n]\overline{x[\ell+n]}, \tag{2.3}$$

where all indices are taken modulo N.

A key fact, first observed by Patterson [14,15], is that the DFT of a_x is the power spectrum. The phase retrieval problem is thus equivalent to the problem of recovering a signal from its periodic auto-correlation. In the sequel, we use the terms Fourier magnitudes, power spectrum and autocorrelation interchangeably.

3. Binary and two-alphabet phase retrieval

The binary phase retrieval problem is the problem of recovering a binary signal $x \in \mathbb{R}^N$ from its periodic auto-correlation $a_x \in \mathbb{R}^N$ [6,4]. Let $S(x)$ denote the support of a signal x. A well known result for binary signals states that $a_x = a_{x'}$ if and only if $S(x) - S(x) = S(x') - S(x')$; i.e., the two supports are homometric (e.g., [2]).

Let us expand upon this result and replace the zeros and ones in the traditional binary phase retrieval with arbitrary scalars α and β. We refer to this problem as the *two-alphabet phase retrieval problem*. When either α or β is zero, then this problem reduces to the binary phase retrieval problem. Otherwise, we do not have a well-defined notion of a support set since neither one of the two letters is assumed to be zero. Instead, we consider the sets

$$S_\alpha(x) = \{i \mid x[i] = \alpha\} \qquad \text{and} \qquad S_\beta(x) = \{j \mid x[j] = \beta\}.$$

We prove the following result.

Theorem 3.1. *For a generic choice of values of α, β, the following are equivalent for signals $x, x' \in \{\alpha, \beta\}^N$.*

(i) $a_x = a_{x'}$
(ii) *$S_\alpha(x)$ and $S_\alpha(x')$ are homometric*
(iii) *$S_\beta(x)$ and $S_\beta(x')$ are homometric*
(iv) *The ordered partitions $(S_\alpha(x), S_\beta(x))$ and $(S_\alpha(x'), S_\beta(x'))$ are homometric.*

Remark 3.2. By generic choice of α, β, we mean that the set of α, β for which the conclusion of the theorem does not hold is contained in the zero set of a collection of non-zero polynomials in $\mathbb{R}[\alpha, \beta]$. In particular, the pairs $(\alpha, \beta) \in \mathbb{R}^2$ for which the theorem holds has full Lesbegue measure.

Proof. Clearly (iv) implies (ii) and (iii). If we show that (ii) implies (iv) then by symmetry we can also conclude that (iii) implies (iv). To see that (ii) implies (iv) we use Patterson's Theorem, Theorem 2.6. Note that $S_\beta(x) = S_\alpha(x)^c$, so by Patterson's Theorem $S_\alpha(x)$ and $S_\alpha(x')$ are homometric if and only if $S_\beta(x)$ and $S_\beta(x')$ are also homometric. To show that the partitions $(S_\alpha(x), S_\beta(x))$ and $(S_\alpha(x'), S_\beta(x'))$ are homometric we must show that $S_\alpha(x) - S_\beta(x) = S_\alpha(x') - S_\beta(x')$. This follows from the fact that the difference sets $S_\alpha(x) - S_\alpha(x), S_\alpha(x) - S_\beta(x), S_\beta(x) - S_\beta(x)$ (respectively $S_\alpha(x') - S_\alpha(x'), S_\alpha(x') - S_\beta(x'), S_\beta(x') - S_\beta(x')$) form a partition of the multi-set $[0, N-1] - [0, N-1]$.

Let $a_x[\ell]$ and $a_{x'}[\ell]$ be the ℓ-th entry of a_x and $a_{x'}$, respectively. Then, $a_x[\ell] = m_\ell \alpha^2 + n_\ell \beta^2 + p_\ell \alpha\beta$, and $a_{x'}[\ell] = m'_\ell \alpha^2 + n'_\ell \beta^2 + p'_\ell \alpha\beta$, where m_ℓ (resp. m'_ℓ) is the multiplicity of ℓ in $S_\alpha(x) - S_\alpha(x)$ (resp.

$S_\alpha(x') - S_\alpha(x')$), n_ℓ (resp. n'_ℓ) is the multiplicity of ℓ in $S_\beta(x) - S_\beta(x)$ (resp. $S_\beta(x') - S_\beta(x')$), and p_ℓ (resp. p'_ℓ) is the multiplicity of ℓ in $S_\alpha(x) - S_\beta(x)$ (resp. $S_\alpha(x') - S_\beta(x')$). Hence, if $(S_\alpha(x), S_\beta(x))$ and $(S_\alpha(x'), S_\beta(x'))$ are homometric then $a_x[\ell] = a_{x'}[\ell]$. Thus $(iv) \implies (i)$.

Conversely, suppose that $a_x = a_{x'}$. This means that for each ℓ we have that

$$m_\ell \alpha^2 + n_\ell \beta^2 + p_\ell \alpha\beta = m'_\ell \alpha^2 + n'_\ell \beta^2 + p'_\ell \alpha\beta.$$

Let us define $m = m_\ell - m'_\ell$, $n = n_\ell - n'_\ell$, $p = p_\ell - p'_\ell$. If the integers m, n, p are not all zero, then α, β must be contained in the zero set of a quadratic polynomial with integer coefficients m, n, p, each of absolute value at most N. This means that for a generic choice of α, β we must have that $m = n = p = 0$; i.e., $m_\ell = m'_\ell$, $n_\ell = n'_\ell$, and $p_\ell = p'_\ell$, meaning that the multiplicities of ℓ in $S_\alpha(x) - S_\alpha(x), S_\beta(x) - S_\beta(x), S_\alpha(x) - S_\beta(x)$ are equal to the multiplicities of ℓ in $S_\alpha(x') - S_\alpha(x'), S_\beta(x') - S_\beta(x'), S_\alpha(x') - S_\beta(x')$, respectively. Since for generic α, β this is true for every $\ell = 0, \ldots, N-1$ we conclude that the partitions $(S_\alpha(x), S_\beta(x))$ and $(S_\alpha(x'), S_\beta(x'))$ are homometric. Thus, $(i) \implies (iv)$ for generic choice of α, β. □

4. Signals with entries taken from a finite alphabet

We now extend our analysis to account for signals whose entries are taken from a finite alphabet. Let $S = \{\alpha_1, \ldots, \alpha_K\}$ be a set K real numbers and let $\mathbb{R}_S$ be the set of all vectors in $\mathbb{R}^N$ whose entries are taken from S. A vector $x \in \mathbb{R}_S$ determines a length K partition $A_1(x), \ldots A_K(x)$ of $[0, N-1]$, where $A_k(x) = \{n \in [0, N-1] \,|\, x[n] = \alpha_k\}$.

Remark 4.1. In this paper we assume that the alphabet is taken from the reals, but the theory is unchanged if we consider complex alphabet entries.

Proposition 4.2. *For a generic choice of $\alpha_1, \ldots, \alpha_K$, two vectors $x, x' \in \mathbb{R}_S$ have the same auto-correlation if and only if the associated partitions $\{A_k(x)\}$ and $\{A_k(x')\}$ are homometric.*

Proof. The proof is similar to the proof of the equivalence $(i) \iff (iv)$ in Theorem 3.1.

Since the entries $\alpha_1, \ldots \alpha_K$ are generic we can treat them as indeterminates. By definition, $a_x[\ell] = \sum_{n=0}^{N-1} x[n]x[n+\ell]$ and $a_{x'}[\ell] = \sum_{n=0}^{N-1} x'[n]x'[n+\ell]$, where all indices are taken modulo N. Since the entries of x, x' are taken from the set S, $a_x[\ell]$ and $a_{x'}[\ell]$ are quadratic polynomials in $\alpha_1, \ldots, \alpha_K$. The coefficient of $\alpha_i\alpha_j$ in $a_x[\ell]$ is the multiplicity of ℓ in the difference multi-set $A_i(x) - A_j(x)$. Likewise, the coefficient of $\alpha_i\alpha_j$ in $a_{x'}[\ell]$ is the multiplicity of ℓ in the difference multi-set $A_i(x') - A_j(x')$. Hence, $a_x = a_{x'}$ if and only if $A_i(x) - A_j(x) = A_i(x') - A_j(x')$ for all i, j. In other words, $a_x = a_{x'}$ if and only if the corresponding partitions are homometric. □

We are now ready to present our main result, which is motivated by the crystallographic phase retrieval problem of recovering a sparse signal, whose non-zero values are taken from a finite alphabet, from its autocorrelation.

Theorem 4.3 *(Sparse signals). Consider two signals x, x' with entries taken from an alphabet $0, \alpha_2, \ldots, \alpha_K$ with $\alpha_2, \ldots, \alpha_K$ generic. Then, $a_x = a_{x'}$ if and only if the partitions $A(x)$ and $A(x')$ are homometric.*

Remark 4.4. The significance of this result is that we no longer assume that α_1 is arbitrary. Equivalently, our result states that if we view $a_x, a_{x'}$ as polynomials in the variables $\alpha_1, \ldots, \alpha_K$, then $a_x(\alpha_1, \ldots, \alpha_K) = a_{x'}(\alpha_1, \ldots, \alpha_K)$ if and only if $a_x(0, \alpha_2, \ldots, \alpha_k) = a_{x'}(0, \alpha_2, \ldots, \alpha_K)$.

Proof. If the partitions $A(x)$ and $A(x')$ are homometric then clearly $a_x = a_{x'}$.

Conversely, if $a_x = a_{x'}$, then for every ℓ the coefficients of $\alpha_i\alpha_j$ in $a_x[\ell]$ and $a_{x'}[\ell]$ are equal for $i, j \geq 2$. As before, this coefficient is just the multiplicity of ℓ in the difference multi-sets $A_i(x) - A_j(x)$ and $A_i(x') - A_j(x')$ respectively. Using the same reasoning as in the proof of Theorem 3.1 we see that if $\alpha_2, \ldots, \alpha_k$ are generic then $A_i(x) - A_j(x) = A_i(x') - A_j(x')$ for $i, j > 1$.

We begin with the following lemma.

Lemma 4.5. $A_1[x] - A_1[x] = A_1[x'] - A_1[x']$.

Proof. Let $B[x] = \cup_{i=2}^{K} A_i[x]$ and $B[x'] = \cup_{i=2}^{K} A_i[x']$. Then, $\{A_1[x], B[x]\}$ and $\{A_1[x], B[x']\}$ are length two partitions of $[0, N-1]$. Now, $B[x] - B[x] = \uplus_{i,j\geq 2}(A_i[x] - A_j[x]) = B[x'] - B[x']$. (Here, the notation $\uplus$ refers to the additive union of multi-sets. If $C_1, \ldots, C_r$ are multi-sets, then an element $c \in \uplus C_i$ appears with multiplicity equal to the sum of the multiplicities in each of the sets C_i.) In other words, the subsets $B[x]$ and $B[x']$ are homometric. Since $A_1[x] = B[x]^c$ and $A_1[x'] = B[x']^c$, it follows from Patterson's Theorem that they also have the same difference sets. $\square$

To complete the proof that the partitions are homometric, we need to show that the difference sets $A_1[x] - A_i[x]$ and $A_1[x'] - A_i[x']$ are equal for all $i > 1$. To do this we can argue inductively. Assume by induction that $A_1[x] - A_i[x] = A_1[x'] - A_i[x']$ for $i < k$ with the initial case $k = 1$ established by Lemma 4.5. Let $B_k[x] = \cup_{j>k} A_k[x]$ and $B_k[x'] = \cup_{j>k} A_k[x']$. We know already that $B_k[x] - B_k[x] = B_k[x'] - B_k[x']$. Hence, by Patterson's Theorem we know that $B_k[x]^c - B_k[x]^c = B_k[x']^c - B_k[x']^c$. But these difference sets are just $\uplus_{i,j\leq k} A_i[x] - A_j[x]$ and $\uplus_{i,j\leq k} A_i[x'] - A_j[x']$. We a priori know that if $i, j \geq 2$ then $A_i[x] - A_j[x] = A_i[x'] - A_j[x']$. By induction, we know that $A_1[x] - A_j[x] = A_1[x'] - A_j[x']$ for $j < k$. Hence, by the pigeon-hole principle we conclude that $A_1[x] - A_k[x] = A_1[x] - A_k[x']$ for all k. $\square$

5. Equivalent, homometric and pseudo-equivalent partitions

In the conclusion to his 1944 paper [16], Patterson noted that

> in very few cases are the atoms of a crystal all of one kind and it seems very probable that the presence of a second kind of atom will often resolve the ambiguities which might occur in the location of the first if taken alone.

In the following example we illustrate this phenomenon for 1-D signals.

Example 5.1. Consider $A = \{0, 1, 4, 7\}$ and $A' = \{0, 1, 3, 4\}$ as subsets of $[0, 7]$. These sets are homometric but not equivalent. Let $B = A^c = \{2, 3, 5, 6\}$ and $B' = (A')^c = \{2, 5, 6, 7\}$. Direct inspection or Patterson's Theorem implies that the sets B and B' are also homometric but not equivalent. In particular $B - B = B' - B' = \{0^4, 1^2, 2^2, 3, 4\}$ as multi-sets and any two binary signals supported on B, B' have the same autocorrelation.

Now, we consider the decomposition of B and B' into two subsets of size two B_1, B_2 and B'_1, B'_2, respectively. We can now ask which of the six possible ordered partitions A, B_1, B_2 are homometric with any of the six possible partitions A', B'_1, B'_2. Of the six possible three-set partitions of the form A, B_1, B_2, only the partitions $(\{0, 1, 3, 4\}, \{2, 6\}, \{3, 5\})$ are homometric but not equivalent to the partitions $A', B'_1, B'_2 = (\{0, 1, 4, 7\}, \{2, 6\}, \{5, 7\})$. For example the partitions $(\{2, 3\}, \{5, 6\})$ and $(\{2, 5\}, \{6, 7\})$ are not homometric as illustrated in Fig. 2.

On the other hand, if we consider partitions of B and B' into three subsets, respectively, then no partition of the form A, B_1, B_2, B_3 is homometric with a partition of the form A, B'_1, B'_2, B'_3. This reinforces Patterson's intuition that by considering a second kind of atom we increase the likelihood that the ambiguities of the auto-correlation can be resolved.

Fig. 2. The ordered partition $(B_1, B_2) = (\{2,3\}, \{5,6\})$ is shown on the left circle with points of B_1 in red and B_2 in blue. The ordered partition $(B'_1, B'_2) = (\{2,5\}, \{6,7\})$ is shown on the right circle with the points in B'_1 in red and B'_2 in blue. These partitions are clearly not homometric since the distance between the red points on the left is one but in the circle on the right the distance is three. However, the sets $B_1 \cup B_2 = \{2,3,5,6\}$ and $B'_1 \cup B'_2 = \{2,5,6,7\}$ are homometric; see Example 5.1. (For interpretation of the colors in the figure(s), the reader is referred to the web version of this article.)

Table 1
Results of Example 5.4.

N	Partition Sizes	Equivalent Pairs	Pseudo-equivalent pairs	Total homometric pairs
6	2,2,2,	369	0	369
7	3,2,2	1218	0	1218
8	3,3,2	2005	99	2104
9	3,3,3	813	158	971
10	4,3,3	360	12	372
11	4,4,3	148	1	149
12	4,4,4	62	3	70
13	5,4,4	10	0	10

We next consider pseudo-equivalent partitions. As far as we know, this case was not considered before.

Definition 5.2. Two partitions $A_1, \dots, A_K$ and $A'_1, \dots, A'_K$ of $[0, N-1]$ are *pseudo-equivalent* if there exist elements $\sigma_1, \dots, \sigma_K \in D_{2N}$ such that $A'_i = \sigma_i A_i$

When $K = 2$, any pair of pseudo-equivalent partitions are automatically equivalent because in this case if $\sigma_1 A_1 = A'_1$ then $\sigma_1 A_2 = A'_2$ since $A_2 = A_1^c$ and $A'_2 = {A'_1}^c$, respectively. Note that if the partitions $A_1, \dots, A_k$ and $A'_1, \dots, A'_k$ are pseudo-equivalent then $A_i - A_i = A'_i - A'_i$ for each i. However, in general pseudo-equivalent partitions need not be homometric and homometric partitions need not be pseudo-equivalent.

Example 5.3. The ordered partitions $\{0,1,4\}, \{7\}, \{3\}, \{2,5,6\}$ and $\{0,1,4\}, \{3\}, \{7\}, \{2,5,6\}$ are pseudo-equivalent and also homometric but not equivalent.

Although homometric partitions need not be pseudo-equivalent and vice-versa, a numerical experiment seems to indicate that for approximately uniform partitions (i.e., partitions where the sets have approximately the same size) homometric partitions are in fact pseudo-equivalent.

Example 5.4. We conducted the following experiment. For a given N in the range, $N = 6, \dots, 13$, we considered a set $S(N)$ of partitions where $N_1 = \lceil N/3 \rceil$, $N_2 = \lceil N - N_1/2 \rceil$, $N_3 = N - N_2 - N_3$. When $N = 6, 7$ we considered all partitions and when $N \geq 8$ we took a random sample of size 300. (For $N = 6, 7$ there are fewer than 300 partitions.) Each of the $\binom{|S(N)|}{2}$ pairs of partitions in $S(N)$ were tested to see if they were homometric. As indicated in Table 1, except for the case $N = 12$, all homometric pairs found were either equivalent or pseudo-equivalent.

Unfortunately, the problem of analyzing, for a particular partition type, which partitions are homometric but not equivalent seems to be an extremely difficult combinatorial problem. We conclude with the following positive result when each atom in the alphabet appears with multiplicity exactly one. To state our result we introduce the following notation. An ordered partition of $A_1, \dots, A_K$ of $[1, N]$ has *type* $[n_1, \dots, n_K]$, where $n_i = |A_i|$.

Proposition 5.5. *Any two ordered partitions of type* $[N-K, \underbrace{1,\dots,1}_{K\,times}]$ *are homometric if and only if they are equivalent.*

Proof. We use induction on K. For $K=1$, any two partitions of type $[N-1,1]$ are necessarily equivalent because the dihedral group acts transitively on the set $[0, N-1]$. Hence, if $(A, \{\alpha\})$ and $(A', \{\alpha'\})$ are two partitions of this form, then there exists $\sigma \in D_{2N}$ such that $\alpha' = \sigma(\alpha)$.

Assume by induction that the statement holds for partitions of type $[N-K, 1, \dots, 1]$; i.e., if $(A', \{a_1'\}, \dots, \{a_K'\})$ and $(A, \{a_1\}, \dots, \{a_K\})$ are two homometric ordered partitions, then they are equivalent. We will prove that the statement holds for partitions of type $[N-K-1, 1, \dots, 1]$.

The induction hypothesis implies that if $(\alpha_1', \dots, \alpha_K')$ and $(a_1, \dots, a_K)$ are any sequences of distinct integers in $[0, N-1]$ such that $d(a_i', a_j') = d(a_i, a_j)$ for all $1 \le i < j \le K$ then there exists $\sigma \in D_{2N}$ such that $\alpha_i' = \sigma\alpha_i$ for $i = 1, \dots, K$. To establish the induction step we must prove that if $(\alpha_1, \dots, \alpha_K, \alpha_{K+1})$ and $(\alpha_1', \dots, \alpha_K', \alpha_{K+1}')$ are two sequences such that $d(a_i', a_j') = d(a_i, a_j)$ for $1 \le i, j \le K+1$, then there exists $\sigma \in D_{2N}$ such that $\alpha_i' = \sigma\alpha_i$ for $i = 1, \dots K+1$. By induction, there exists $\sigma_1 \in D_{2N}$ such that $\sigma_1(\alpha_1, \dots, \alpha_K) = (\alpha_1', \dots, \alpha_K')$. In particular, we may assume that $(\alpha_1', \dots, \alpha_K', \alpha_{K+1}')$ is equivalent to a sequence of the form $(\alpha_1, \dots, \alpha_K, \alpha_{K+1}')$. Applying a suitable element of D_{2N} we may also assume that $\alpha_1 = 0$. Hence, $d(\alpha_{K+1}, 0) = d(\alpha_{K+1}', 0)$ which implies that $\alpha_{K+1}' = N - \alpha_{K+1}$ or $\alpha_{K+1}' = \alpha_{K+1}$. In the latter case we are done since the sequences would be equal. If $\alpha_{K+1}' = N - \alpha_K$ then for $i = 2, \dots, K$ we have that $d(N - \alpha_{K+1}, \alpha_i) = d(\alpha_{K+1}, \alpha_i)$ This implies that either $2\alpha_{K+1} \equiv 0 \bmod N$ or $2\alpha_i \equiv 0 \bmod N$. Since neither α_{K+1} nor α_i can be zero, we see that in either case N must be even and in the former case we have that $\alpha_{K+1} = N/2$ so $\alpha_{K+1}' = \alpha_{K+1}$. On the other hand, the integers $\alpha_2, \dots, \alpha_K$ are distinct so we cannot have that $\alpha_i = N/2$ for $2 \le i \le K$ unless $K = 2$. In the case of $K = 2$, then we see that our sequences would necessarily be of the form $(0, N/2, \alpha_3)$ and $(0, N/2, N - \alpha_3)$. However, these sequences are also dihedrally equivalent since they are related by the reflection $\alpha \mapsto N - \alpha$. □

Remark 5.6. When $N - K > N/2$ we expect that analogous results hold for partitions of type $[N - K, a_1, \dots, a_L]$ where $L \ll K$ and the a_ℓ are approximately equal. Unfortunately, investigating this problem is currently beyond reach from both a computational and theoretical perspective.

6. Extensions

6.1. Finite alphabet phase retrieval in finite abelian groups

The finite alphabet phase retrieval problem can be generalized to any finite abelian group. Let G be a finite abelian group and let V be the vector space of functions $x\colon A \to \mathbb{K}$, where $\mathbb{K} = \mathbb{R}$ or $\mathbb{K} = \mathbb{C}$. In the case of one-dimensional phase retrieval, $G = \mathbb{Z}_N$, and for higher-dimensional phase retrieval $G = \mathbb{Z}_N^M$ is a product of cyclic groups. In this case, the auto-correlation is defined as a function $A \to \mathbb{K}$ defined by the formula

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

Given a subset $A \subset G$, we can again define the G-difference set $A - A$ [2, Appendix E], and define the notion of homometric sets. The G-difference set is invariant under the action of a group $D_G = G \ltimes \mathbb{Z}_2$, and we say that two subsets A, A' are equivalent if there is an element $\sigma \in D_G$ such that $A' = \sigma A$. The proof of Lemma 2.5 easily generalizes to show that two equivalent subsets of G are homometric. Likewise, Theorem 3.1 and Proposition 4.2 generalize to partitions of finite abelian groups. However, the existing proofs Patterson's theorem make use of the fact that the signals are one-dimensional; i.e., that the group is $\mathbb{Z}_N$. A natural question for future work is to prove the analogue of Patterson's theorem for any abelian group G. If such a theorem held, then Theorem 4.3 could be generalized to the case where G is an arbitrary finite abelian group.

6.2. Other questions

1. In our model we assume that each atom is represented by a single letter. An interesting alternative model to investigate is to assume that the atoms are represented by a few letters placed consecutively in $[0, N-1]$. While this model is combinatorially more complicated, it may also be more likely to resolve the ambiguities of the auto-correlation.
2. Another model worth further investigation, particularly in higher dimensions, is to assume that the separate atoms are placed within the basic crystal structure in a regular way. For example, if $G = \mathbb{Z}_N^2$ and our alphabet is $\{a, b\}$ we might assume that the sets $S_a(x)$ and $S_b(x)$ are the orbits of different cyclic subgroups of G. (Note that $G = \mathbb{Z}_N^2$ has many distinct cyclic subgroups.)
3. In an X-ray crystallography experiment, the measurement is contaminated with noise, which is characterized by Poisson statistics. In this case, we are not searching for a signal which is precisely consistent with the power spectrum (as in this paper), but only approximately consistent. Understanding the information-theoretic limits of this problem, namely, what is the optimal expected error regardless of any specific algorithm, is an important research question.

Data availability

No data was used for the research described in the article.

Acknowledgments

The authors were supported by the BSF grant no. 2020159. T.B. is also supported in part by the NSF-BSF grant no. 2019752, and the ISF grant no. 1924/21 and D.E. was also supported by NSF-DMS 1906725 and NSF-DMS 2205626. The problems posed in Section 6.2 are based on remarks of the anonymous referee.

References

[1] Tamir Bendory, Robert Beinert, Yonina C. Eldar, Fourier phase retrieval: uniqueness and algorithms, in: Compressed Sensing and Its Applications, Springer, 2017, pp. 55–91.
[2] Tamir Bendory, Dan Edidin, Toward a mathematical theory of the crystallographic phase retrieval problem, SIAM J. Math. Data Sci. 2 (3) (2020) 809–839.
[3] Tamir Bendory, Dan Edidin, Algebraic theory of phase retrieval, Not. Am. Math. Soc. 69 (2022) 3489–3499.
[4] Tamir Bendory, Oscar Mickelin, Amit Singer, Sparse multi-reference alignment: sample complexity and computational hardness, in: ICASSP 2022-2022 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), IEEE, 2022, pp. 8977–8981.
[5] Martin J. Buerger, Proofs and generalizations of Patterson's theorems on homometric complementary sets, Z. Kristallogr. 143 (1–6) (1976) 79–98.
[6] Veit Elser, The complexity of bit retrieval, IEEE Trans. Inf. Theory 64 (1) (2017) 412–428.
[7] Veit Elser, Ti-Yen Lan, Tamir Bendory, Benchmark problems for phase retrieval, SIAM J. Imaging Sci. 11 (4) (2018) 2429–2455.
[8] Subhroshekhar Ghosh, Philippe Rigollet, Sparse multi-reference alignment: phase retrieval, uniform uncertainty principles and the beltway problem, Found. Comput. Math. (2022) 1–48.
[9] Philipp Grohs, Sarah Koppensteiner, Martin Rathmair, Phase retrieval: uniqueness and stability, SIAM Rev. 62 (2) (2020) 301–350.
[10] Juan E. Iglesias, On Patterson's cyclotomic sets and how to count them, Z. Kristallogr. 156 (3–4) (1981) 187–196.
[11] Sandra Keiper, Gitta Kutyniok, Dae Gwan Lee, Götz Pfander, Reconstruction of Finite-Valued Sparse Signals, Wavelets and Sparsity XVII, vol. 10394, SPIE, 2017, pp. 244–252.
[12] Sandra Keiper, Gitta Kutyniok, Dae Gwan Lee, Götz E. Pfander, Compressed sensing for finite-valued signals, Linear Algebra Appl. 532 (2017) 570–613.

[13] Rick P. Millane, Phase retrieval in crystallography and optics, JOSA A 7 (3) (1990) 394–411.
[14] A.L. Patterson, A Fourier series method for the determination of the components of interatomic distances in crystals, Phys. Rev. 46 (Sep 1934) 372–376.
[15] A.L. Patterson, A direct method for the determination of the components of interatomic distances in crystals, Z. Kristallogr. 90 (1–6) (1935) 517–542.
[16] A.L. Patterson, Ambiguities in the X-ray analysis of crystal structures, Phys. Rev. 65 (Mar 1944) 195–201.
[17] Juri Ranieri, Amina Chebira, Yue M. Lu, Martin Vetterli, Phase retrieval for sparse signals: uniqueness conditions, arXiv preprint arXiv:1308.3058, 2013.
[18] Joseph Rosenblatt, Phase retrieval, Commun. Math. Phys. 95 (3) (1984) 317–343.
[19] Joseph Rosenblatt, Paul D. Seymour, The structure of homometric sets, SIAM J. Algebraic Discrete Methods 3 (3) (1982) 343–350.
[20] Pulak Sarangi, Ryoma Hattori, Takaki Komiyama, Piya Pal, Super-resolution with binary priors: theory and algorithms, arXiv preprint arXiv:2301.01724, 2023.
[21] Pulak Sarangi, Piya Pal, No relaxation: guaranteed recovery of finite-valued signals from undersampled measurements, in: ICASSP 2021-2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), IEEE, 2021, pp. 5440–5444.
[22] Yoav Shechtman, Yonina C. Eldar, Oren Cohen, Henry Nicholas Chapman, Jianwei Miao, Mordechai Segev, Phase retrieval with application to optical imaging: a contemporary overview, IEEE Signal Process. Mag. 32 (3) (2015) 87–109.