Discrete phase retrieval in musical structures

John Mandereau, Daniele Ghisi, Emmanuel Amiot, Moreno Andreatta, Carlos Agon

Discrete Phase Retrieval in Musical Structures

John Mandereau[a,d]**, Daniele Ghisi[b], Emmanuel Amiot[c], Moreno Andreatta[d] and Carlos Agon[d]

[a] *Dipartimento di Matematica, Università di Pisa, Italy*; [b] *Cursus de composition, IRCAM, Paris, France*; [c] *CPGE, Perpignan, France*; [d] *UMR 9912, CNRS/IRCAM/UPMC, Paris, France*

This is a preprint of an article whose final and definitive form has been published in the Journal of Mathematics and Music (JMM) © 2011 Taylor & Francis.
The published article is available online at
`http://www.tandfonline.com/doi/abs/10.1080/17459737.2011.608820`

Abstract

This paper describes phase retrieval approaches in music by focusing on the particular case of the cyclic groups (beltway problem). After presenting some old and new results on phase retrieval, we introduce the extended phase retrieval for generalized musical Z-relation. This concept is accompanied by mathematical definitions and motivations from computer-aided composition. We assume from the reader basic knowledge of groups, topological groups, group algebras, group actions, Lebesgue integration, convolution products, and Fourier transform.

Keywords: GIS (Generalized Interval Systems); interval vector; Patterson function; Z-relation; homometry; phase retrieval; spectral units; k-deck.

MCS/CCS/AMS Classification/CR Category numbers: AMS MSC 05E15, 20H15, 43A20.

1 Introduction

One class of combinatorial problems deals with the problems of reconstruction. Especially, a problem that arises in very different contexts is the reconstruction of a set from the collection of its k-subsets up to isomorphism. The same thing may be done with the reconstruction of graphs from a collection of subgraphs (see [7], [6]). One can come across this type of problem in computer graphics, in physics, in genetics, in crystallography and also in musical composition. In Section 2, we define the phase retrieval problem, introduce alternative formulations of it, stressing the role of spectral units in the case of discrete abelian groups, trying to characterize homometric sets in a constructive way. In Section 3 we extend the definitions of our previous paper, *Z-Relation and Homometry in Musical*

**Corresponding author. Email: mandereau@mail.dm.unipi.it

Distributions [17, Sec. 4], by introducing the k-deck, the k-deck up to reflection, the k-vector, and higher-order generalizations of Z-relation and homometry associated to them. Finally, in Section 4, we define the extended phase retrieval problem and the reconstruction index of a cyclic group. The study of k-decks has been widely developed lately, while the k-deck up to reflection has been pretty much left aside. After providing some properties of the Z^k-relation, we end up with the first example of 4-Homometric sets.

2 The phase retrieval problem

We have seen in our paper that immediately precedes this one [17] many properties of the Patterson function of a distribution and the interval contents of a measurable subset of finite measure. In this section, we will focus on the reconstruction problem.

This problem consists in determining whether a given integrable distribution over a locally-compact topological group fitted with its Haar measure, can be uniquely reconstructed – up to translation and inversion, or up to translation – from its Patterson function, and in case it cannot, which distributions are non-trivially homometric with the given one.[1].

2.1 Definition of the problem

Let G be a locally compact group with a right-Haar measure μ.

We recall the notation $\mathcal{D}(G)$ for the image in $\mathrm{Aut}(\Sigma_{\mathsf{C}}(G))$ of $D(G)$, the generalized dihedral group on G. Let H be the largest subgroup of $\mathcal{D}(G)$ such that the Patterson function is constant on the orbits of the action of H on $\Sigma_{\mathsf{C}}(G)$, that is for every P in H, every E in $\Sigma_{\mathsf{C}}(G)$, $d^2(P(E)) = d^2(E)$. According to [17, Prop. 3.5], when G is unimodular, H is the group of left transposition operators[2] $\{T_g, g \in G\}$, and when G is abelian, $H = \mathcal{D}(G)$.

Definition 2.1. The **phase retrieval problem** consists in:

1. determining for every $E \in \Sigma_{\mathsf{C}}(G)$, whether there is some $F \in \Sigma_{\mathsf{C}}(G)$ non-trivially Z-related to E; if there is no such F, one says that E can be **uniquely retrieved** from its Patterson function up to H;

2. determining, for every $E \in \Sigma_{\mathsf{C}}(G)$ that cannot be uniquely retrieved, a family $F = (F_i)_{i \in I}$ of $\Sigma_{\mathsf{C}}(G)$ such $F \cup (E)$ is a maximal family of non-trivially Z-related distributions.

In this definition, H is instrumental in pruning out all trivial Z-relatives.

One defines likewise a "restricted" phase retrieval on $\widetilde{\mathcal{A}}$, wherein H is defined as the largest subgroup of $D(G)$ such that for all $A \in \widetilde{\mathcal{A}}, P \in H$, $\mathbf{iv}(P(A)) = \mathbf{iv}(A)$. This restricted phase retrieval problem is identical to the approach used by Forte for classifying pitch class sets in his musical set theory, whereas the definition with distributions comes from crystallography.

2.2 Alternative formulations

We have defined the most general notion of homometry in terms of Patterson functions. But in a number of practical situations, the computations – and indeed the comprehension of the process –

[1] This paper will make use of the notations introduced in [17].

[2] H does not contain I because I does not preserve intervals, that is I does not preserve the interval content of pairs.

are made easier by using the appropriate algebraic tools. A summary of these formulations is shown in Figure 1 at the end of this section.

2.2.1 Polynomials

In the case of distributions on the group $\mathbb{Z}_n$, i.e. maps from $\mathbb{Z}_n$ to some field K, we deal with the algebra $(K^{\mathbb{Z}_n}, +, ., *)$, of which the product law $*$ is essential in defining the Patterson function. It is possible to replace this algebra by the algebra of polynomials.

Definition 2.2. The characteristic polynomial of a subset $A \subset \mathbb{Z}_n$ is $A(x) = \sum_{k\in A} x^k \in K[x] = K[X]/(X^n - 1)$, where we note $x = X \mod X^n - 1$. More generally, for any distribution $E : \mathbb{Z}_n \to K, E = \sum e_k \delta_k$, we define $E(x) = \sum_{k\in\mathbb{Z}_n} e_k x^k$.

Proposition 2.3. *The above transformation is an algebra isomorphism between* $(K^{\mathbb{Z}_n}, +, ., *)$ *and* $(K[x]/(x^n - 1), +, ., \times)$*, namely* $(E * F)(x) = E(x) \times F(x)$*.*

Essentially, the translation operator on subsets turns into multiplication by x: $T(A)(x) = x \times A(x)$. This transformation was introduced by Redei *et al.* around 1950 in the study of tilings by translation. For us, the spotlight is on the Patterson function. Transposing the definitions already given yields the following.

Definition 2.4. The reciprocal polynomial of $E(x) = \sum_{k\in\mathbb{Z}_n} a_k x^k$ is $I(E)(x) = x^{n-1}\overline{E}(1/x) = \sum_{k\in\mathbb{Z}_n} \overline{a}_k x^{n-k}$. The Patterson polynomial function associated with the distribution E is $d^2(E)(x) = E(x)I(E)(x) = \sum_{k\in\mathbb{Z}_n} e_k x^k \quad \text{with} \quad e_k = \sum_{p\in\mathbb{Z}_n} a_p \overline{a}_{p-k}$ where the indices are computed modulo n.

Notice that for any root ξ of $E(x)$, both ξ and $1/\xi$ are roots of $d^2(E)(x)$. Also, for $\xi \in S^1$ (the unit circle), one gets $d^2(E)(\xi) = E(\xi)\overline{E(\xi)} = |E(\xi)|^2 \in \mathbb{R}_+$.

This approach can be further extended to any finite abelian group, or even any finitely generated abelian group, with polynomials in several variables – one for each element of a generator set of the group. Such constructions are essential in Polya's theory of combinatorics.

Any such polynomial, with degree $d < n$, can be determined uniquely with the values it takes in n different points. A judicious choice is to evaluate $E(x)$ in the n^{th} roots of unity, since $E(e^{-2i\,j\pi/n}) = \sum_{k=0}^{n-1} a_k e^{-2i\,j\,k\pi/n}$ is exactly the Fourier transform of the map E.

2.2.2 Fourier transform

Historically, the idea of using the Fourier transform in the theory of intervals goes back to David Lewin's first paper [14]. It was refurbished in recent years, mainly starting from Quinn's PhD [21].

As we have mentioned before, in the case of characteristic functions of subsets of $\mathbb{Z}_n$, the Patterson functions reduces to the simpler case of discrete Fourier transforms (DFT for short):

$$\widehat{\mathbf{1}_A}(t) = \sum_{k\in A} e^{-2i\pi kt/n}$$

This is indeed closer to the crystallographic origin of the Patterson function: as we mentioned in the introduction, the Fourier transform of the interval content is exactly the module of the DFT of the subset: since $\mathbf{iv}(A) = \mathbf{1}_A * \mathbf{1}_{-A}$, applying the Fourier transform yields $\widehat{\mathbf{iv}(A)} = \widehat{\mathbf{1}_A} \times \widehat{\mathbf{1}_{-A}} = \widehat{\mathbf{1}_A} \times \overline{\widehat{\mathbf{1}_A}} = |\widehat{\mathbf{1}_A}|^2$

It is perhaps interesting to mention the slightly more complicated equation used by Lewin: he aimed to retrieve a pc-set A, knowing pc-set B and the interval function between the two: $\mathbf{ifunc}(A,B)(t) = \#\{(a,b) \in A \times B, a+t=b\} = \mathbf{1}_B * \mathbf{1}_{-A}(t)$.

Since $\widehat{\mathbf{ifunc}(A,B)} = \widehat{\mathbf{1}}_B \times \widehat{\widehat{\mathbf{1}_A}}$, the retrieval of A is always possible *provided that* $\widehat{\mathbf{1}}_B$ *does not vanish.* As we will see below, this condition arises again in the discussion of k-decks. It is also instrumental in numerous problems, for instance rhythmic tilings. For practical retrieval, see the following section.

This approach can of course be extended to distributions on $\mathbb{Z}_n$, enlarging the codomain from $\{0,1\}$ to $\mathbb{C}$; but also to any commutative group instead of $\mathbb{Z}_n$, with the Fourier transform defined in terms of characters. This will be useful again below: in the study of k-decks we will introduce multi-dimensional Fourier transform.

An interesting alternative, introduced by Thomas Noll, is the case $\mathbb{Z}_n \to \mathbb{T}^n \subset \mathbb{C}^n$, modelizing ordered sequences of n notes, e.g. musical scales. On these topics, see [2, 3].

2.2.3 Circulating matrices

Circulating matrices of order n are defined as $\mathcal{C}_n(K)$ or $\mathcal{C}_n$ for short, the (commutative) algebra of matrices of the form $\begin{pmatrix} a_0 & a_{n-1} & \cdots & a_1 \\ a_1 & a_0 & \cdots & a_{n-1} \\ \vdots & \ddots & \ddots & \vdots \\ a_{n-1} & \cdots & a_1 & a_0 \end{pmatrix}$, with coefficients in any field K.

This algebra is actually the algebra of polynomials in the matrix $J = \begin{pmatrix} 0 & \cdots & & 0 & 1 \\ 1 & 0 & \cdots & & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix}$. J can be seen as the matrix for the elementary translation operator $T_1 : k \mapsto k+1$.

There is a natural mapping from distributions on $\mathbb{Z}_n$ onto $\mathcal{C}_n$, setting for any map $E \in K^{\mathbb{Z}_n}$ $a_k = E(k)$. For instance if $E = \mathbf{1}_A$, one gets $a_k = 1 \iff k \in A$ and $a_k = 0$ if $k \notin A$. What makes this bijection interesting is the following:

Proposition 2.5. *The above mapping is an isomorphism of algebras between* $(K^{\mathbb{Z}_n}, +, ., *)$ *and* $(\mathcal{C}_n, +, ., \times)$.

In other words, this matricial representation turns the cumbersome convolution product into the (slightly less cumbersome) matricial product.[3] This is easily checked by a direct computation, left to the reader. But the deep reason for this apparent miracle is linked to simultaneous diagonalization of these matrices:

Theorem 2.6. *Let* $\Omega = \frac{1}{\sqrt{n}}\left[e^{2i\pi j\, k/n}\right]_{j,k=0\ldots n-1}$ *be the* ***Fourier matrix***.[4] *Then for any circulating matrix* S *associated with* $E : k \mapsto a_k$,

$$\Omega^{-1} S\, \Omega = \begin{pmatrix} \psi_0 & 0 & \cdots & 0 \\ 0 & \psi_1 & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & \psi_{n-1} \end{pmatrix}.$$

where the $\psi_k = \widehat{E}(k)$ *are the Fourier coefficients of map* E.

[3] Actually one of the authors first introduced this algebra as the natural representation of $K^{\mathbb{Z}_n}$ acting on itself by way of the adjunction operator $E \mapsto (F \mapsto E * F)$.

[4] Notice that ${}^t\overline{\Omega} = \Omega^{-1}$.

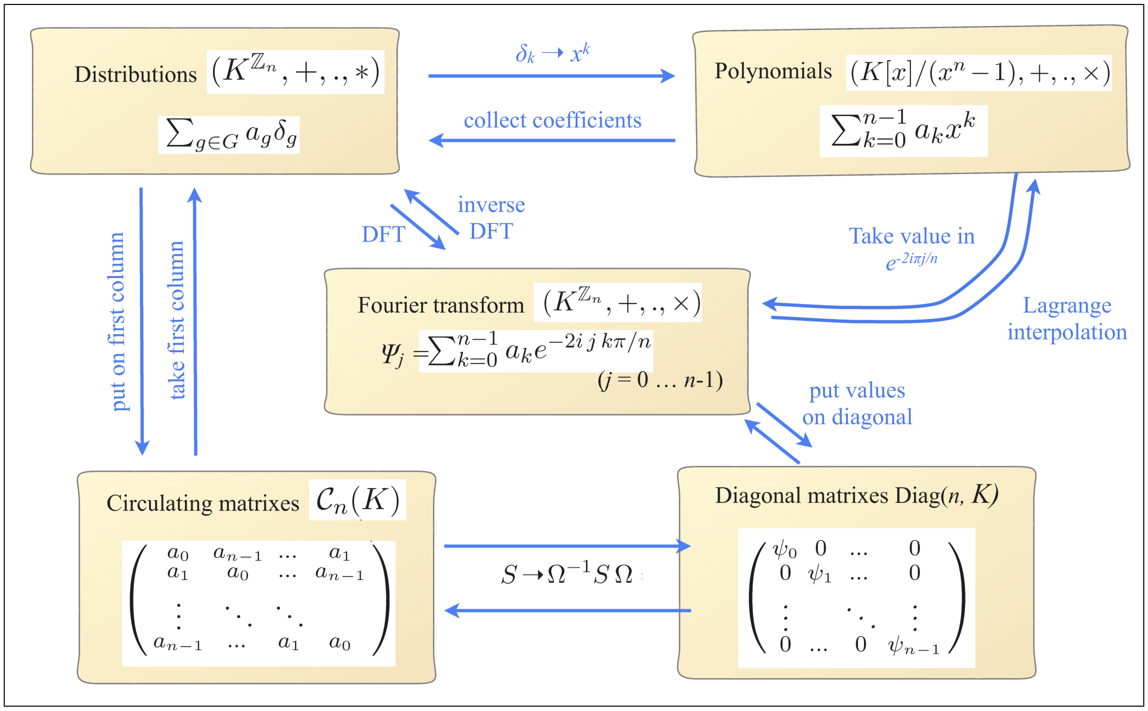

Figure 1: Isomorphisms between different algebras.

Proof. It is straightforward to check that the colums of Ω are eigenvectors of the matrix J, with eigenvalue equal to the first element of the column. Hence $\Omega^{-1} J\,\Omega = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & e^{-2i\pi/n} & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & e^{-2i\pi(n-1)/n} \end{pmatrix}$ and for $S = a_0 I + a_1 J + \cdots a_{n-1} J^{n-1}$, $\Omega^{-1} S\,\Omega = \begin{pmatrix} \psi_0 & 0 & \cdots & 0 \\ 0 & \psi_1 & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & \psi_{n-1} \end{pmatrix}$ where $\psi_k = \sum_{j=0}^{n} a_j e^{-2i\pi j\,k/n}$. $\square$

So the miracle of the algebra morphism is just the fact that convolution $*$ is turned into ordinary product by the Fourier transform. Here the Fourier transform is read as a diagonal matrix, whose algebra is clearly isomorph to K^n with term-to-term product.

This matrix representation is still close enough to the musical material (the distribution can be read *verbatim* in the first column) and introduces the whole, powerful machinery of linear algebra. For some fascinating applications, see [5]. We will sample here a few results or techniques related to our topic:

- The Fourier transform is non-vanishing iff the determinant of the matrix is different from 0. This is a straightforward criteria for all of Lewin's 'special cases', which was hitherto a messy catalogue of obscure conditions.
- The matrix associated with **ifunc**(A, B) (resp. **iv**(A)) is ${}^tS_A S_B$ (resp. ${}^tS_A S_A$) where S_A, S_B

are the matrices associated with $\mathbf{1}_A, \mathbf{1}_B$. For more general distributions (complex valued instead of 0,1) the conjugate must be used, e.g. if S is associated with map E, then its **iv** is associated with ${}^t\overline{S}S$.

- Hence "Lewin retrieval" (finding A from $\mathbf{ifunc}(A, B)$) is accomplished by inverting S_B (notice the condition on non-vanishing Fourier coefficients again here).
- S_A and S_B are homometric iff ${}^tS_AS_A = {}^tS_BS_B$. Diagonalizing, this in turn is equivalent to the existence of some matrix U such that
  1. U is a circulating matrix [it diagonalizes with the same eigenvectors as all others] and
  2. U is unitary: its eigenvalues lie on the unit circle (or equivalently: ${}^t\overline{U}U = I_n$, the identity matrix).
  3. $S_B = US_A$.

We will elaborate below on these so-called spectral units, see 2.3. A straightforward example is J, the equation $S_B = JS_A$ expressing that $B = T_1(A)$. It is, however, much less easy to characterize the inversion operator I in terms of spectral units.

In this paragraph, we have restricted ourselves to (distributions on) the cyclic group; nonetheless we look forward to further research making use of group representation theory, of which this is but one of the most elementary examples. It might be the best access to the non-commutative case.

2.3 Spectral units

As the Patterson function of a bounded distribution with compact support is defined using a convolution product, it is natural to ask whether there exist distributions U such that the convolution with U does not change the value of the Patterson function, i.e. such that for every $E \in \Sigma_{\mathsf{C}}(G)$ $E * U * I(E * U) = E * I(E)$, which is equivalent – if $d^2(U)$ is well defined and G abelian – to $d^2(E) * d^2(U) = d^2(E)$, i.e. E and $E * U$ are homometric.

When the algebra $(L^1(\mu), +, ., *)$ does not have a unit, which is equivalent to G having a non-discrete topology [24, Chap. 3, 5.6], in order to formulate the Z-relation and phase retrieval problem, it is necessary to enlarge the algebra to the space of distributions, which has been done in depth for $G = \mathbb{R}$ in [25].

When G is discrete and abelian, which we will assume henceforth, such distributions U are easily characterized as distributions homometric to the unit of $L^1(\mu)$, which is the Dirac distribution in e, the neutral element of G.

Definition 2.7. A distribution $U \in \Sigma_{\mathsf{C}}(G)$ is called a spectral unit of G if $I(U) * U = \delta_e$.

Proposition 2.8. *The set of spectral units of G is a subgroup of the group of invertible elements of the algebra $L^1(G)$.*

Rosenblatt has proven that any pair of homometric distributions is connected by a spectral unit.[5] Hence, in a way, enumerating all spectral units would solve the phase-retrieval problem. In practice it is not so, because we do not want $E * U$ to be just any distribution; for instance for pc-sets, we would want its codomain to be $\{0, 1\}$. As we will see below, even in the simplest case of distributions in $\mathbb{Z}_n$, this is far from obvious.

[5] There are some technical conditions about the field wherein the computations are made.

2.4 Phase retrieval in the case of cyclic groups: the beltway problem

2.4.1 Spectral units of $\mathbb{Z}_n$

Putting together circular matrices and spectral units, we are looking for unitary circulating matrices: ${}^t\overline{U^{-1}} = U \in \mathcal{C}_n$. Then any pair of circulating matrices S, T such that $S = UT$ provides homometric distributions. For convenience, let us generally denote by shortcase $s \in K^n$ the first column of uppercase $S \in \mathcal{C}_n$.

For instance, let the first column of S be $s = {}^t(1,0,0,1,0,0,0,1,0,0,0,0)$ (the C minor triad) and T defined by the first column $t = {}^t(1,0,0,0,1,0,0,1,0,0,0,0)$ (the C major triad). Then transposition is achieved by multiplication with $j = {}^t(0,1,0,0,0,0,0,0,0,0,0,0)$ and its powers, e.g. E-flat minor triad is obtained with the matrix product J^3S, or equivalently $j^3 * s = {}^t(0,0,0,1,0,0,1,0,0,0,1,0)$. It is, however, much less straightforward to achieve inversion by way of a spectral unit: from C major to C minor we must have $U = S^{-1}T$, which yields $u = \frac{1}{15}(7,4,-2,1,7,4,-2,1,-8,4,-2,1)$. Contrary to transposition, the spectral unit achieving inversion depends on the inversed subset (or distribution), and even more strangely, in general, such units are of infinite order in the group of units, like u in the example above.

Still, we managed to completely characterize rational[6] spectral units with finite order:

Theorem 2.9. *Any spectral unit with finite order is completely determined by the values of the subset $\{\xi_j, j \mid n\}$ of its eigenvalues. The possibilities are listed* infra*:*

- $\xi_0 = \pm 1$*;*
- *When n is odd, for all $j \mid n$, ξ_j OR $-\xi_j$ is any power of $e^{2ij\pi/n}$.*
- *When n is even, ξ_j is any power of $e^{2ij\pi/n}$ if n/j is even, or any power of $e^{ij\pi/n}$ if n/j is odd.*

Then for any k coprime with n, $\xi_{kj} = \xi_j^k$ (or $-\xi_j^k$ in a specific case, cf. [4]).

For instance, for $n = 12$ the structure of this group is $\mathbb{Z}_{12} \times (\mathbb{Z}_6)^2 \times \mathbb{Z}_4 \times (\mathbb{Z}_2)^2$, with 6,912 elements. In general, the group of rational spectral units with finite order is isomorphic with $\prod_{d|n} \mathbb{Z}/(\mathrm{lcm}(2,d)\mathbb{Z})$.

Notice the similarity with 4.1.2 below. Proofs and details can be found in [4].

2.4.2 Existence of non-trivially Z-related subsets of $\mathbb{Z}_n$

Theorem 2.10. *Let $n \in \mathbb{N}$ with $n \geqslant 2$. There exist A, B non-trivially Z-related subsets of $\mathbb{Z}_n$ if and only if $n = 8$ or $n = 10$ or $n \geqslant 12$.*

Proof. If $n = 8$, sets A, B that fit are given by $\{0,1,3,4\}_8, \{2,5,6,7\}_8$. If $n = 10$, $A = \{0,1,3,4,8\}_{10}, B = \{2,5,6,7,9\}_{10}$ fit. It is easily seen that these two cases are instances of the (Generalized) Hexachord Theorem [17, Th. 7.2]; the non-triviality of the Z-relation comes from the fact that there is a sequence of three consecutive elements $\{5,6,7\} \subset B$, whereas there is no such sequence in A.

[6] For many musical applications, homometric distributions will be Z-related (multi)sets, and because of the matricial equation between them, a spectral unit connecting them must have rational coefficients. Conversely of course, a rational spectral unit will not necessarily yield integer coefficients when multiplied with the characteristic function of a (multi)set. Finally, the whole group of rational (or real) spectral unit matrices can be described implicitely by the equations $(E_k) : \sum_{j=0}^{n-1} a_j a_{j+k} = 0, k = 1 \dots \lfloor \frac{n-1}{2} \rfloor$, and the condition $\sum a_j^2 = 1$, where indices are taken modulo n. For instance, for $n = 3$ the group of real spectral units is the pair of circles made of the matrices $\begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix}$ with $a^2 + b^2 + c^2 = 1$ and $a + b + c = \pm 1$.

Let us assume now that $n \geqslant 12$; we note $\pi_n : \mathbb{Z} \to \mathbb{Z}_n$ the canonical projection. $A = \{0, 1, 2, 6, 8, 11\}$ and $B = \{0, 1, 6, 7, 9, 11\}$ are Z-related in $\mathbb{Z}$, so using [17, Cor. 6.2], $\pi_n(A)$ and $\pi_n(B)$ are Z-related; moreover, there is a sequence $\{0, 1, 2\}$ of three (four in the case $n = 12$) consecutive integers in $\pi_n(A)$, whereas there is no such sequence in $\pi_n(B)$, so this Z-relation is not trivial.

Conversely, for $n \leqslant 7$, $n = 9$ and $n = 11$, it is easy to check by computer search that there are no non-trivially Z-related subsets in $\mathbb{Z}_n$. $\square$

2.5 Is there a group action representing the Z-relation?

An appealing formulation of the phase retrieval problem is asking whether there is a non-trivial group action on $\Sigma_{\mathsf{C}}(G)$ wherein the orbits are the equivalence classes of the homometry, and whether there is a non-trivial group action on the set of elements of $\mathcal{A}$ of finite measure wherein the orbits are the equivalence classes of the Z-relation.

A "trivial group action" can always be achieved with the direct sum of the permutation groups of the equivalence classes, which is both a huge and uninteresting group. Precluding this is essential in practice if one is to use properties of group actions of which both the group and the set are finite, for instance computing effectively the number of orbits using the equation of Burnside-Frobenius. We prove below that, in essence, there is no reasonable group action whose orbits are the homometric classes.

Theorem 2.11. *Let $n \in \mathbb{N}$ with $n \geqslant 2$. If $n = 8$, $n = 10$ or $n \geqslant 12$, then for every field K and for every subgroup H of the linear group $\mathrm{GL}_n(K)$ such that the natural group action of H on $\mathcal{P}(\mathbb{Z}_n)$ identified with $\{0, 1\}^n$ is well-defined, the orbits of this group action are not identical with the equivalence classes of the Z-relation.*

Proof. We suppose that $n = 8$, $n = 10$ or $n \geqslant 12$. Let K be a field, let H be a subgroup of $\mathrm{GL}_n(K)$ such that the natural group action of H on K^n can be restricted to a group action of H on $\{0_K, 1_K\}^n$; note that this restriction is well-defined if and only if $\{0_K, 1_K\}^n$ is a union of some orbits of the group action of H on K^n.

We note the natural injective group morphism into permutation matrices

$$P\colon\ S(\mathbb{Z}_n) \to \mathrm{GL}_n(K)$$
$$\sigma \mapsto P_\sigma = (\delta_{i,\sigma(j)})_{i,j \in \mathbb{Z}_n}$$

From Theorem 2.10, there exist two non-trivially Z-related subsets A, B of $\mathbb{Z}_n$. If we assume that the orbits of H are the classes of Z-related sets, B is in the orbit $[A]_H$ of A, so there exists $M \in H$ such that $M\mathbf{1}_A = \mathbf{1}_B$, and since the homometry between $\mathbf{1}_A$ and $\mathbf{1}_B$ is not trivial, M is not in $P(D(\mathbb{Z}_n))$.

On the other hand, we get from [17, Lemma 4.8] that any distribution with codomain $\{0, 1\}$ homometric to $\mathbf{1}_{\{0\}}$ is a $\mathbf{1}_{\{k\}}$ for some $k \in \mathbb{Z}_n$. In particular, as $M\mathbf{1}_{\{0\}}$ and $\mathbf{1}_{\{0\}}$ are homometric, there is a $k \in \mathbb{Z}_n$ such that $M\mathbf{1}_{\{0\}} = \mathbf{1}_{\{k\}}$. Identifying the distributions with circulating matrices (cf. 2.2.3), we find $MI_n = J^k$, so $M \in P(D(\mathbb{Z}_n))$, which leads to a contradiction. $\square$

A previous version of this theorem, looking for a group of permutations of $\mathbb{Z}_n$, was made in [16].

3 Homometry and Z-relation of higher order

3.1 k-vector, k-deck and k-deck up to reflection

We have seen that the Patterson function does not, in general, provide enough information for the reconstruction of a distribution. So we need to extend these concepts far enough to describe exactly the content of our distribution.

Let G be a discrete abelian group.

Definition 3.1. Let H be a subgroup of $S(G)$. Let us define a H**-copy** of a set $S \subset G$ as any set of the form $h(S)$, with $h \in H$.

Two interesting cases are $H = T(G)$, the group of transpositions; and $H = D(G)$, the generalized dihedral group of transpositions and inversions.

We begin by noticing that the interval vector of a set A is simply counting, for every interval $g \in G$, how many D-copies of the set $\{0, g\}$ are embedded in A, and this correspond exactly to $\#(A \cap (A - g))$. Analogously, the coefficient of δ_g (or x^g in polynomial representation) of the Patterson function of a distribution $\mathbf{1}_A$ tells us how many D-copies of the distributions $\delta_0 + \delta_g$ are embedded in $\mathbf{1}_A$, which still correspond exactly to $\#(A \cap (A-g))$. We may now ask, more generally, how many D-copies of some general k-subsets are contained in A. This has been done on the musical side in [15] and then [8] and [9].

Following these works, we define the concept of k**-vector**; contrary to the definition of the interval content [17, Def. 3.2], but similarly to Forte's interval vector, we define it on the orbits of k-subsets of G for the action of the dihedral group D.

Definition 3.2. Let $A \subset G$; we call k**-vector** of A the map

$$\mathbf{mv}^k(A) : [S]_D, \text{ where } S \subset G \text{ and } \#S = k \mapsto mv^k(A)_S = \#\{S' \in [S]_D, S' \subset A\}$$

which counts for of any k-set S the number of its D-copies embedded in A.

It is obvious from the formula that this definition is correct, i.e. that each value of the k-vector at $[S]_D$ does not depend of the choice of $T \in [S]_D$.

Example 3.3. The set $A = \{0, 1, 3, 4, 7\}_{12}$ has essentially only 6 non-zero entries in its 3-vector, as shown in Figure 2.

$$\begin{array}{ll}
\mathbf{mv}^3(A)_{\{0,1,3\}_{12}} = 2 & \mathbf{mv}^3(A)_{\{0,1,4\}_{12}} = 3 \\
\mathbf{mv}^3(A)_{\{0,1,6\}_{12}} = 1 & \mathbf{mv}^3(A)_{\{0,2,6\}_{12}} = 1 \\
\mathbf{mv}^3(A)_{\{0,3,6\}_{12}} = 1 & \mathbf{mv}^3(A)_{\{0,3,7\}_{12}} = 2
\end{array}$$

Indeed, $\mathbf{mv}^3(A)_{\{0,1,3\}} = 2$ since there are two D-copies of $\{0, 1, 3\}_{12}$ embedded in A (they are $\{0, 1, 3\}_{12}$ and $\{1, 3, 4\}_{12}$); $\mathbf{mv}^3(A)_{\{0,1,4\}} = 3$ since there are three D-copies of $\{0, 1, 4\}_{12}$ embedded in A (they are $\{0, 1, 4\}_{12}$, $\{0, 3, 4\}_{12}$ and $\{3, 4, 7\}_{12}$); and so on.

Since $\mathbf{iv}(A)_h = \mathbf{mv}^2(A)_{\{0,h\}}$, this definitions extends the concept of interval vector. Analogously we define the concept of k**-deck**:

Definition 3.4. Let $E = \sum_{g \in G} e_g \delta_g$ be a K-valued distribution on G. We call

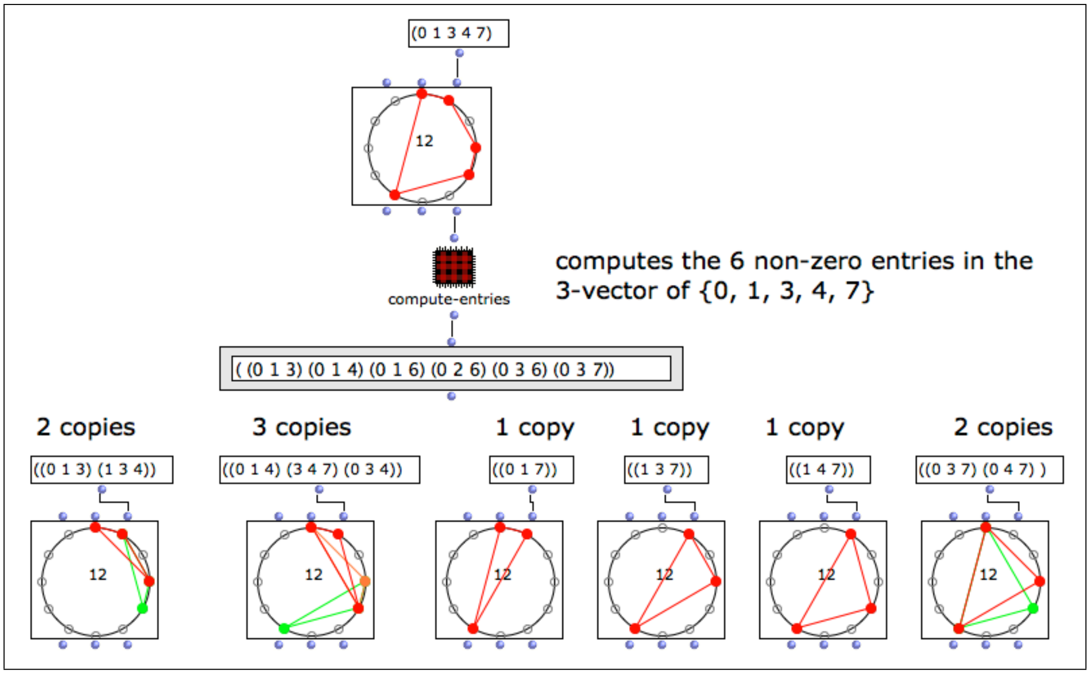

Figure 2: An OpenMusic patch showing the computation of a 3-vector in $\mathbb{Z}_{12}$.

Definition 3.5. k-deck of E the function $d^k(E)\colon G^{k-1} \to K$ defined by

$$d^k(E)(s_1, \dots, s_{k-1}) = \sum_{g \in G} e_g e_{g+s_1} e_{g+s_2} \cdots e_{g+s_{k-1}}. \tag{1}$$

Notice that, since $E * E' = \sum_{g \in G} \sum_{h \in G} e_g e_{-h} \delta_{g-h} = \sum_{t \in G} \left(\sum_{s \in G} e_s e_{t+s} \right) \delta_t$, when $k = 2$, $d^k(E)(s) = \sum_{g \in G} e_g e_{g+s}$ is exactly the value at s of the Patterson function of E, and thus the k-deck extends the Patterson function.

Now, let $G = \mathbb{Z}_n$ and $E = \mathbf{1}_A$; then all the e_g's are either 0 (if $g \in A$) or 1 (otherwise), and thus $d^k(\mathbf{1}_A)(s_1, \dots, s_{k-1}) = \#(A \cap (A - s_1) \cap \dots \cap (A - s_{k-1}))$, which is non zero if and only if there is a T-copy of $\{0, s_1, \dots, s_{k-1}\}$ in A. In other words, the k-deck of $\mathbf{1}_A$ tells us how many T-copies of $\{0, s_1, \dots, s_{k-1}\}$ are contained in A.

These two definitions extend (respectively) the concept of interval vector and the concept of Patterson function. Indeed $\mathbf{iv}(A)_h = \mathbf{mv}^2(A)_{\{0,h\}}$, and $d^2(A)(s) = \#(A \cap (A - s))$ is the coefficient of δ_s in the Patterson function of A.

We see that the k-vector and the k-deck are quite similar objects, with the difference that the first one counts the D-copies, while the last one counts the T-copies. We may solve this discrepancy by introducing the k-deck up to reflection, with a capital D as a symbol, following the terminology of [22]:

Definition 3.6. Let $E = \sum_{g \in \mathbb{Z}_n} e_g \delta_g$ be a real distribution on $\mathbb{Z}_n$. We call **k-deck up to reflection** of E the function $d^k(E)\colon (\mathbb{Z}_n)^{k-1} \to \mathbb{Q}$ defined by $D^k(E) = d^k(E) + d^k(I(E))$.

In this way, we get back the invariance by inversion, and since $d^k(\mathbf{1}_A)$ is the number of D-copies of $\{0, s_1, \ldots, s_{k-1}\}$ in A, the k-deck up to reflection is nothing more than the extension of the k-vector to a generic distribution.[7]

3.2 Z^k-relation, k-homometry, k-Homometry

As we have extended the interval vector and the Patterson function, we are now able to extend also the Z-relation and the homometry.

Definition 3.7. Sets $A_1, \ldots, A_s$ are $\mathbf{Z}^k$**-related** if $\mathbf{mv}^k(A_1)_S = \mathbf{mv}^k(A_2)_S = \ldots = \mathbf{mv}^k(A_s)_S$ for all $S \subseteq \mathbb{Z}_n$, $\#S = k$.

Definition 3.8. Distributions $E_1, \ldots, E_s$ are k-**homometric** if $d^k(E_1) = d^k(E_2) = \ldots = d^k(E_s)$.

Definition 3.9. Distributions $E_1, \ldots, E_s$ are k-**Homometric** if $D^k(E_1) = D^k(E_2) = \ldots = D^k(E_s)$.

Clearly, the Z^2-relation is the Z-relation and the 2-homometry (which is equivalent to 2-Homometry) is plain homometry. Again, for all these definitions, we will add the "non-trivially" prefix if the sets (or distributions) belong to different classes under the action of D (for Z^k-relation and k-Homometry) or T (for k-homometry). This vocabulary makes sense because of the following straightforward results.

Lemma 3.10.

(i) If $A \subset \mathbb{Z}_n$ and $B = I(T_h(A))$ or $B = I^s(T_h(A))$, $s \in \{0, 1\}$, $h \in \mathbb{Z}_n$, then $\mathbf{mv}^k(A)_S = \mathbf{mv}^k(B)_S$, for all $k \geqslant 2$, $S \subset \mathbb{Z}_n$, such that $\#S = k$.

(ii) If $E \in \mathbb{R}^{\mathbb{Z}_n}$ and $F = T_h(E)$, $h \in \mathbb{Z}_n$, then $d^k(E) \equiv d^k(F)$.

(iii) If $E \in \mathbb{R}^{\mathbb{Z}_n}$ and $F = I^s(T_h(E))$, $s \in \{0, 1\}$, $h \in \mathbb{Z}_n$, then $D^k(E) \equiv D^k(F)$.

Proof. (i) is straightforward, since there is an obvious 1-to-1 correspondence between the 3-sets embedded in A and the 3-sets embedded in $I^s(T_h(A))$; (ii) and (iii) come from an easy direct computation. □

Non-trivial Z^3-related sets exist, as first shown by Collins [8].

Example 3.11. Let us consider, in $\mathbb{Z}_{18}$, the two sets $A = \{0, 1, 2, 3, 5, 6, 7, 9, 13\}_{18}$ and $B = \{0, 1, 4, 5, 6, 7, 8, 10, 12\}_{18}$. They are not related by translation/inversion, but $\mathbf{mv}^3(A)_S = \mathbf{mv}^3(B)_S$ for all S, as illustrated by Figure 3.

[7] More precisely, if $I(\{0, s_1, \ldots, s_{k-1}\}) = T_h(\{0, s_1, \ldots, s_{k-1}\})$ for some h, each D-copy is counted twice. If we want complete accordance between the two definitions, we must treat separately that case. But this does not scupper the equivalence between $D^k(A)$ and $\mathbf{mv}^k(A)$. Besides, Definition 3.6 of the k-deck up to reflection in this form will be quite useful later.

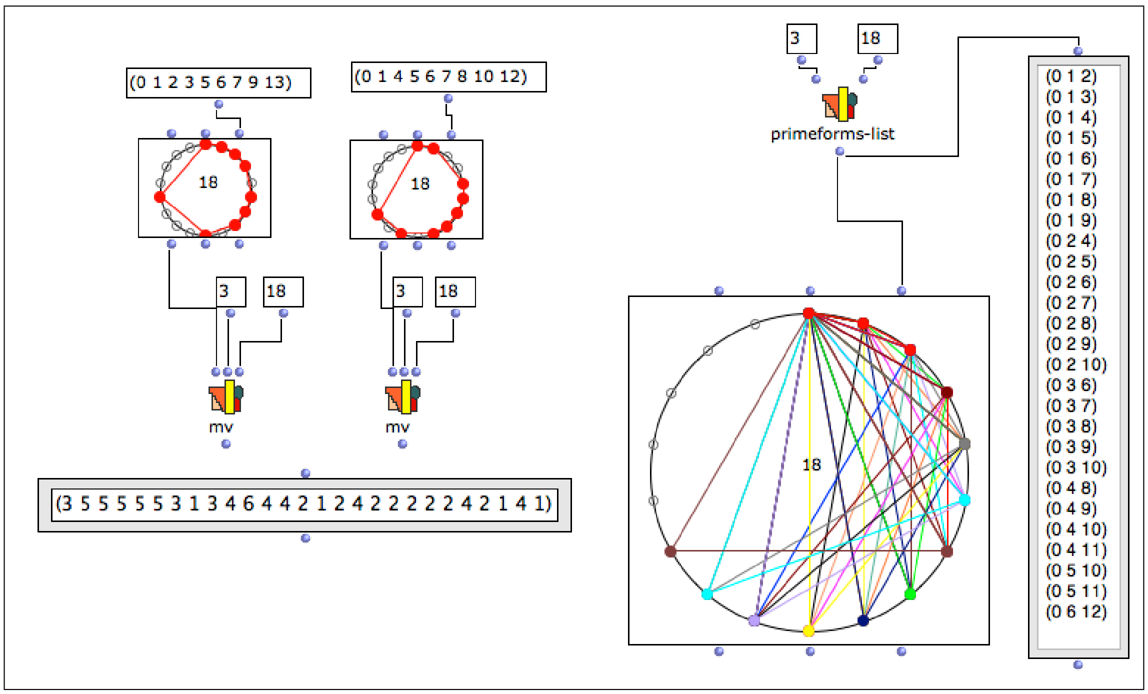

Figure 3: A non-trivial Z^3-relation in $\mathbb{Z}_{18}$. The two sets share the same 3-vector, whose entries specify the number of copies of the corresponding elements in the prime forms list (given in the right part of the figure). For instance, in both sets there are exactly 3 copies of $\{0, 1, 2\}_{18}$, 5 copies of $\{0, 1, 3\}_{18}$, and so on.

3.3 Nesting

Following Jaming[8] [11], we notice that, if $E = \sum_{g\in\mathbb{Z}_n} e_g\delta_g$ is a non negative real distribution on $\mathbb{Z}_n$ ($e_g \geqslant 0$), then $\sum_{s_1,\dots,s_{k-1}\in\mathbb{Z}_n} d^k(E)(s_1,\dots,s_{k-1}) = \left(\sum_{g\in\mathbb{Z}_n} e_g\right)^k$ and so, if two positive distributions $E = \sum_{g\in\mathbb{Z}_n} e_g\delta_g, F = \sum_{g\in\mathbb{Z}_n} f_g\delta_g$ have the same k-deck, they surely satisfy $\sum_{g\in\mathbb{Z}_n} e_g = \sum_{g\in\mathbb{Z}_n} f_g$ i.e. they have the same 1-deck. Then we notice also that

$$\sum_{s_{k-1}\in\mathbb{Z}_n} d^k(E)(s_1,\dots,s_{k-1}) = d^{k-1}(E)(s_1,\dots,s_{k-2}) \sum_{g\in\mathbb{Z}_n} e_g \tag{2}$$

and thus we immediately have the following lemma:

Lemma 3.12. *Let $E, F \in \mathbb{Q}^{\mathbb{Z}_n}$. If $d^k(E) \equiv d^k(F)$ for some k, then $d^h(E) \equiv d^h(F)$ for all $h \leqslant k$.*

This lemma is crucial, since it states that, as k increases, the information given by the k-deck is more and more precise; in particular, the sets which share the same k-deck, as k increases, are *nested*. By definition of the k-deck up to reflection, this result applies equally to the case of D. So, the k-homometric sets and the k-Homometric sets, as k increase, are nested. On the musical side, the k-vector version of the Nesting Lemma has been independently developed by Collins [8], starting from a reconstruction formula given by Lewin [15].

Lemma 3.13. *Let A, B be sets in $\mathbb{Z}_n$. If $\mathbf{mv}^k(A) \equiv \mathbf{mv}^k(B)$ for some $k \leqslant \min(\#A, \#B)$, then $\mathbf{mv}^h(A) \equiv \mathbf{mv}^h(B)$ for all $h \leqslant k$.*

4 The Extended Phase Retrieval Problem

The **extended phase retrieval problem** deals precisely with the question of where this nesting stops. If we know that in $\mathbb{Z}_n$ there exist $(r-1)$-homometric sets but no r-homometric sets, it means that r-decks provide enough information for phase retrieval.

Definition 4.1. The T**-reconstruction index** $r(n)$ is the minimum integer k for which there exist no k-homometric 0-1 distributions in $\mathbb{Z}_n$. The D**-reconstruction index** $R(n)$ is the minimum integer k for which there exist no k-Homometric 0-1 distributions in $\mathbb{Z}_n$. We define $r_{\mathbb{Q}}(n)$ and $R_{\mathbb{Q}}(n)$ analogously, but for general distributions in $\mathbb{Q}^{\mathbb{Z}_n}$.

Clearly, $r(n) \leqslant r_{\mathbb{Q}}(n)$ and $R(n) \leqslant R_{\mathbb{Q}}(n)$. By the way, it is interesting to notice how $R(n)$ finds its musical mirror-image in the concept of "uniqueness of pitch class spaces", independently developed by Collins in [8].

Direct computer search can give the values of $r(n)$, $R(n)$ for small n, but we need some algebra to explore the general cases.

4.1 The k-deck problem

If E, F are k-homometric distributions, i.e. $d^k(E)(s_1,\dots,s_{k-1}) = d^k(F)(s_1,\dots,s_{k-1})$ for all $(s_1,\dots,s_{k-1}) \in \mathbb{Z}_n^{k-1}$, then we can take the discrete Fourier transform of these k-decks, considered as functions in the $k-1$ variables $s_1,\dots,s_{k-1}$.

[8] We correct here two small typos in the paper, concerning the exponent of the norm and a sign of an inequality.

It is then easy to check that the homometry condition is equivalent to

$$\widehat{E}(\omega_1)\widehat{E}(\omega_2)\cdots\widehat{E}(\omega_{k-1})\widehat{E}(-\omega_1-\ldots-\omega_{k-1}) = \\ = \widehat{F}(\omega_1)\widehat{F}(\omega_2)\cdots\widehat{F}(\omega_{k-1})\widehat{F}(-\omega_1-\ldots-\omega_{k-1}) \quad (3)$$

for every $(\omega_1,\ldots,\omega_{k-1}) \in \mathbb{Z}_n^{k-1}$.

We now assume that $E, F \in \mathbb{R}_+^{\mathbb{Z}_n}$, i.e. they are non negative distributions. In this case, $\widehat{E}(0) = \sum_{g\in\mathbb{Z}_g} e_g > 0$. By choosing $\omega_i = 0$ for all i, we get immediately that $(\widehat{E}(0))^k = (\widehat{F}(0))^k$, and then $\widehat{E}(0) = \widehat{F}(0)$. By choosing $\omega_1 = \omega$ arbitrary and $\omega_2 = \ldots = \omega_{k-1} = 0$ we reach the Patterson equality $\|\widehat{E}(\omega)\|^2 = \|\widehat{F}(\omega)\|^2 \quad \forall\omega$. This is not surprising (we know that the k-deck information is nested as k increase), but it tells us that $\operatorname{supp}\widehat{E} = \operatorname{supp}\widehat{F}$, i.e. either the two Fourier transforms are both nil, or they are both non-zero.[9] Moreover, the Patterson equality allows us to perform the substitution $\widehat{F}(\omega) = e^{i\phi(\omega)}\widehat{E}(\omega)$ and to get equivalently (after simplifying)

$$\phi(\omega_1+\omega_2+\ldots+\omega_{k-1}) = \phi(\omega_1)+\phi(\omega_2)+\ldots+\phi(\omega_{k-1}) \mod 2\pi \quad (4)$$

which must be valid for all $\omega_1,\ldots,\omega_{k-1} \in \operatorname{supp}\widehat{E}$ such that $\omega_1+\ldots+\omega_{k-1} \in \operatorname{supp}\widehat{E}$.

4.1.1 The Case $\operatorname{supp}\widehat{E} = \mathbb{Z}_n$

We can easily show that if the Fourier transform never vanishes on $\mathbb{Z}_n$, then the 3-deck suffices for the reconstruction. The 3-deck version of equation (4) is

$$\phi(\omega_1+\omega_2) = \phi(\omega_1)+\phi(\omega_2) \mod 2\pi \quad (5)$$

for *all* the $(\omega_1,\omega_2) \in \mathbb{Z}_n^2$, which tells us that the function $\psi\colon \omega \mapsto e^{i\phi(\omega)}$ is a character of $\mathbb{Z}_n$. Since we know the form of the characters of $\mathbb{Z}_n$, necessarily there exist a k_0 such that $\psi(\omega) = e^{2i\pi k_0\omega/n}$. But this means that

$$\widehat{F}(\omega) = e^{i\phi(\omega)}\widehat{E}(\omega) = \psi(\omega)\widehat{E}(\omega) = e^{2i\pi k_0\omega/n}\widehat{E}(\omega) = \widehat{E*\delta_{k_0}}(\omega) = \widehat{T_{k_0}(E)}(\omega)$$

where we have applied the shift theorem for the DFT. Thus $F = T_{k_0}(E)$, which means that, if the Fourier transforms never vanish, two distributions with the same 3-deck are necessarily related by transposition, and the (extended) phase retrieval is succesful.

4.1.2 The Case $\operatorname{supp}\widehat{E} \neq \mathbb{Z}_n$

If $\widehat{E}(\omega)$ vanishes for some ω, the function $\phi(\omega)$ is not everywhere defined, (5) is no more valid for all the $(\omega_1,\omega_2) \in \mathbb{Z}_n^2$, and thus ψ is no more a character, being defined only on $\operatorname{supp}\widehat{E}$. However, if we succeed in showing that we can extend $\psi(\omega) = e^{i\phi(\omega)}$ to a character on all $\mathbb{Z}_n$, we can apply the shift theorem again, and thus prove that F and E are related by transposition.

We will follow the lead of Jaming and Kolountzakis in [12], and we start by gathering some information about the position of the zeros of $\widehat{E}$.

Lemma 4.2. *If $\widehat{E}(\omega) = 0$ for some $\omega \neq 0$, then $\widehat{E}(\eta) = 0$ for all η such that* $\gcd(\omega,n) = \gcd(\eta,n)$.

[9] We denote as $\operatorname{supp}\widehat{E}$ the support of $\widehat{E}$ i.e. the set of values on which $\widehat{E}$ does not vanish.

Proof. First recall (see 2.2.1), denoting $\zeta_n = e^{2\pi i/n}$, that $\widehat{E}(\omega) = E(\zeta_n^\omega)$, i.e. computing the Fourier transform is equivalent to the evaluation of the polynomial $E(x)$ in the powers of an n-th primitive root of unity ζ_n.

If $\widehat{E}$ vanishes on ω, then $E(\zeta_n^\omega) = 0$, which means that $(x - \zeta_n^\omega)$ divides $E(x)$. But ζ_n^ω is a primitive $n/\gcd(\omega, n)$-root of the unity, and thus if $(x - \zeta_n^\omega)$ divides $E(x)$, necessarily all the cyclotomic polynomials $\Phi_{n/\gcd(\omega,n)}(x)$, which are irreducible in $\mathbb{Q}[x]$, divide $E(x)$ in $\mathbb{Q}[x]$, and in particular it will vanish also for all other roots of unity with the same order, i.e. $E(x) = 0$ for all $x = \zeta_n^\eta$ such that $\gcd(\omega, n) = \gcd(\eta, n)$. For such η, $\widehat{E}(\eta) = E(\zeta_n^\eta) = 0$. □

This means that we can partition $\mathbb{Z}_n = \bigsqcup_{i\in\mathbb{Z}, i|n} \mathcal{C}_i$ where each $\mathcal{C}_i = \{a \in \mathbb{Z}_n : \gcd(a, n) = i\}$ and if a transform vanishes on a certain element of $\mathcal{C}_i$, then it must vanish on all the class $\mathcal{C}_i$.

Lemma 4.3. *The class $\mathcal{C}_i$ $(i < n)$ of the partition of $\mathbb{Z}_n$ is isomorphic to the multiplicative group $\mathbb{Z}^*_{n/i}$.*

Proof. Consider the subgroup $\mathbb{Z}_{n/i}$ of $\mathbb{Z}_n$, in the sense of the injection $\iota\colon \mathbb{Z}_{n/i} \to \mathbb{Z}_n$ defined by $\iota([a]_{n/i}) := [ia]_n$, $a \in \mathbb{Z}$. The generic element of $\mathcal{C}_i$ is of the type $[ia]_n$, with $\gcd(a, n) = 1$, and thus we can apply ι^{-1} to get to $[a]_{n/i}$. Since a is coprime with n, it is also coprime with n/i, and thus $[a]_{n/i} \in \mathbb{Z}^*_{n/i}$. It is immediate to see that ι^{-1} is an isomorphism between $\mathcal{C}_i$ and $\mathbb{Z}^*_{n/i}$. □

Example 4.4. We can easily decompose $\mathbb{Z}_{12} = \mathcal{C}_1 \sqcup \mathcal{C}_2 \sqcup \mathcal{C}_3 \sqcup \mathcal{C}_4 \sqcup \mathcal{C}_6 \sqcup \mathcal{C}_{12}$ where

$$\begin{array}{ll}
\mathcal{C}_1 = \{[1]_{12}, [5]_{12}, [7]_{12}, [11]_{12}\} = \mathbb{Z}^*_{12} & \mathcal{C}_4 = \{[4]_{12}, [8]_{12}\} \cong \mathbb{Z}^*_3 \\
\mathcal{C}_2 = \{[2]_{12}, [10]_{12}\} \cong \mathbb{Z}^*_6 & \mathcal{C}_6 = \{[6]_{12}\} \cong \mathbb{Z}^*_2 \\
\mathcal{C}_3 = \{[3]_{12}, [9]_{12}\} \cong \mathbb{Z}^*_4 & \mathcal{C}_{12} = \{[0]_{12}\}
\end{array}$$

Proposition 4.5. *If p is prime, in $\mathbb{R}^{\mathbb{Z}_p}$ the 3-deck suffice for the reconstruction, i.e. if $d^3_E \equiv d^3_F$ then $F = T_{k_0}E$ for some $k_0 \in \mathbb{Z}_p$.*

Proof. We have just 2 classes $\mathcal{C}_i$: $\mathcal{C}_p = \{[0]_p\}$ and $\mathcal{C}_1 = \mathbb{Z}^*_p$. Since $\widehat{E}(0) > 0$ (we're assuming that E is a positive real distribution), we have 2 cases:

1. $\operatorname{supp} \widehat{E} = \mathbb{Z}_n$, which has already been seen in section 4.1.1.
2. $\operatorname{supp} \widehat{E} = \{[0]_n\}$, which means $\widehat{E} \equiv \widehat{F}$, since $\widehat{E}(0) = \widehat{F}(0)$ (the 3-homometry implies the 1-homometry). □

With this kind of argumentations Pebody in [19, 20], and Jaming and Kolountzakis in [12] have shown that the 3-deck suffices also in the cases $n = p^a$, $n = pq$, $n = p^2q$ and $n = pqr$ $(p, q, r$ odd primes, $a > 2)$. Pebody in [19] reaches a complete determination of the function $r_{\mathbb{Q}}(n)$ (see Theorem 4.7). By the way, many steps of the proofs in [19, 20] that may not seem obvious have been well detailed in [13].

It turns out that, while the behaviour of the functions $r_{\mathbb{Q}}(n)$ is completely known (see [19] and for details), the same thing is *almost* true for $r(n)$: Pebody in [20] gives all the boundaries for odd n, and conjectures that $r(n) = 4$ for n even and greater than 10. There is a previous attempt at proving what Pebody conjectured in [10, Theorem 5]; however, since it uses the restrictive hypothesis that the Fourier transform does not vanish on $\mathbb{Z}^*_n$, and since some points in [10] resisted to clarification, we do not retain it.

Computer calculation shows that $r(2) = 1$, $r(4) = 2$, $r(6) = r(8) = r(10) = 3$; to complete the boundaries a bit, we prove the following.

Lemma 4.6. *If n is an even integer, $n \geqslant 12$, then $r(n) \geqslant 4$.*

Proof. Let $n = 2m$ and consider $A = \{0, 1, 2, \ldots, m-4, m-1, 2m-3, 2m-2\}_{2m}$ and $B = \{0, 1, 2, \ldots, m-4, m-2, m-1, 2m-3\}_{2m}$

Notice that B is obtained from A by a one-pitch shift of m (which is very similar to what Althuis and Göbel did in [1] to find some Z-related families). More precisely: $C = \{0, 1, 2, \ldots, m-4, m-1, 2m-3\}_{2m}$, $A = C \cup \{2m-2\}_{2m}$, $B = C \cup \{m-2\}_{2m}$. So we just need to show that there's a 1-to-1 correspondence between the 3-subsets of A containing $2m-2$ and the 3-subsets of B containing $m-2$. We shall give it explicitely. Let $a \in \{0, 1, 2, \ldots, m-4\}_{2m}$. Then the correspondence is the following one:

$$\begin{aligned}
\{2m-2, a, a+1\}_{2m} &\mapsto \{m-4-a, m-2, m-1\}_{2m}, \text{ for } a \neq [m-4]_{2m} \\
\{2m-2, a, a+k\}_{2m} &\mapsto \{3m–a–4–k, m–2–k, m–2\}_{2m}, \text{ for } k \in \{[2]_{2m}, \ldots, [m-4-a]_{2m}\} \\
\{a, m-1, 2m-2\}_{2m} &\mapsto \{a-1, m-2, 2m-3\}_{2m}, \text{ for } a \neq [0]_{2m} \\
\{0, m-1, 2m-2\}_{2m} &\mapsto \{m-2, 2m-3, m-4\}_{2m} \\
\{m-1, 2m-3, 2m-2\}_{2m} &\mapsto \{0, m-2, m-1\}_{2m} \\
\{a, 2m-3, 2m-2\}_{2m} &\mapsto \{m-2, m-5-a, m-4-a\}_{2m}, \text{ for } a \neq [m-4]_{2m} \\
\{m-4, 2m-3, 2m-2\}_{2m} &\mapsto \{2m-3, m-2, m-1\}_{2m}
\end{aligned}$$

Notice that, as requested, $2m-2$ is always present in the left 3-subsets and $m-2$ is always present in the right ones. So A and B have the same 3-deck.

To complete the proof, we notice that, if $n \geqslant 12$, the homometry is non-trivial - just look at the intervals between the pitch classes and at the order of the intervals bigger than 1 ($3, m-2, 2$ for A and $2, m-2, 3$ for B), which cannot be related by transposition if $m \geqslant 6$. Instead, for $n = 10$ the sets become $A = \{0, 1, 4, 7, 8\}$ and $B = \{0, 1, 3, 4, 7\}$ which are transpositionally related. The same thing happens for $n = 8$. $\square$

We are ready to summarize all the results in the following theorem.

Theorem 4.7. *Let p, q be odd primes and let α, β be integers $\alpha \geqslant 1$, $\beta > 1$. Then*

$$r_{\mathbb{Q}}(n) = \begin{cases} 1 & \textit{if } n = 1 \\ 2 & \textit{if } n = 2 \\ 3 & \textit{if } n = p^\alpha \textit{ or} \\ & \textit{if } n = pq \\ 4 & \textit{if } n \textit{ is any other} \\ & \textit{ odd number or} \\ & \textit{if } n = 2^\beta \textit{ or} \\ & \textit{if } n = 2p^\alpha \\ 5 & \textit{if } n = 2^\beta p^\alpha \\ 6 & \textit{if } n \textit{ is any other} \\ & \textit{ even number} \end{cases} \qquad r(n) = \begin{cases} 1 & \textit{if } n = 1, 2, 3 \\ 2 & \textit{if } n = 4, 5 \\ 3 & \textit{if } n = p^\alpha > 5 \textit{ or} \\ & \textit{if } n \textit{ has less than 4} \\ & \textit{ not-necessarily distinct} \\ & \textit{ odd prime factors or} \\ & \textit{if } n = 6, 8, 10 \\ 4 & \textit{if } n \textit{ is any other odd number} \\ 4, 5 or\ 6 & \textit{if } n \textit{ if any other even number} \end{cases}$$

4.2 The problem of the k-deck up to reflection

Let us try to do the same thing with the problem of the k-deck up to reflection, which is the case we are most interested in, since there is an exact correspondence between k-Homometry and Z^k-

relation. If E, F are k-Homometric distributions, $D^k(E)(s_1,\ldots,s_{k-1}) = D^k(F)(s_1,\ldots,s_{k-1})$ i.e. $d^k(E)(s_1,\ldots,s_{k-1}) + d^k(E)(-s_1,\ldots,-s_{k-1}) = d^k(F)(s_1,\ldots,s_{k-1}) + d^k(F)(-s_1,\ldots,-s_{k-1})$, and taking again the Fourier transform, we get

$$\operatorname{Re}\left(\widehat{E}(\omega_1)\widehat{E}(\omega_2)\cdots\widehat{E}(\omega_{k-1})\widehat{E}(-\omega_1-\ldots-\omega_{k-1})\right) = \\ = \operatorname{Re}\left(\widehat{F}(\omega_1)\widehat{F}(\omega_2)\cdots\widehat{F}(\omega_{k-1})\widehat{F}(-\omega_1-\ldots-\omega_{k-1})\right) \quad (6)$$

The difference between (3) and (6), the real parts, is the main obstacle in pursuing the analysis. Indeed, (6) leads to either one of the following equations:

$$\widehat{E}(\omega_1)\cdots\widehat{E}(\omega_{k-1})\overline{\widehat{E}(\omega_1+\ldots+\omega_{k-1})} = \widehat{F}(\omega_1)\cdots\widehat{F}(\omega_{k-1})\overline{\widehat{F}(\omega_1+\ldots+\omega_{k-1})} \quad (7)$$

$$\widehat{E}(\omega_1)\cdots\widehat{E}(\omega_{k-1})\overline{\widehat{E}(\omega_1+\ldots+\omega_{k-1})} = \overline{\widehat{F}(\omega_1)\cdots\widehat{F}(\omega_{k-1})}\widehat{F}(\omega_1+\ldots+\omega_{k-1}) \quad (8)$$

and things are complicated because (7) might be valid for some values of ω_i's while (8) might be valid for others.

By choosing $\omega_i = 0$ for all i, we still get to $\widehat{E}(0) = \widehat{F}(0)$, and by arbitrarily choosing $\omega_1 = \omega$ and $\omega_2 = \ldots = \omega_{k-1} = 0$ we get again the Patterson equality $\|\widehat{E}(\omega)\|^2 = \|\widehat{F}(\omega)\|^2 \quad \forall\omega$ which is little surprising, since the 2-deck and the 2-deck up to reflection coincide.

Considering these obstacles, the best we can do is to provide a list of computer-calculated values for $n \leqslant 37$:

Proposition 4.8.

$$R(n) = \begin{cases} 1 & \textit{if } n = 1,2,3 \\ 2 & \textit{if } n = 4,5,6,7,9,11 \\ 3 & \textit{if } n = 8,10,12,13,14,15,16,17,19,22,23,25,29,31,37 \\ 4 & \textit{if } n = 18,20,21,24,26,27,28,30,32,33,34,35 \\ 5 & \textit{if } n = 36 \end{cases}$$

4.2.1 An upper bound

As a direct consequence of Theorem 4 in [23], by Radcliffe and Scott, one easily gets $R(n) \leqslant 2r(n)$. Thus $R(n) \leqslant 2 \times 6 = 12$.

4.2.2 Existence of Z^4-related Sets

Notice, in particular, that $R(36) = 5$, which means that there are some non trivially Z^4-related sets.

To stress the interest of the research in the problem of the k-deck up to reflection, and the intimate difference with the k-deck problem, we finish with an explicit example of Z^4-related sets, obtained by computer search. In $\mathbb{Z}_{36}$ consider the sets

$$A = \{0,1,2,3,4,5,7,10,12,15,19,20,22,23,24,25,27,28\}_{36}$$
$$B = \{0,1,2,3,4,5,6,9,14,17,18,19,21,22,24,26,27,29\}_{36}$$

They are not related by transposition or inversion, but $\mathbf{mv}^4(A) \equiv \mathbf{mv}^4(B)$, or equivalently $D^4(A) \equiv D^4(B)$, see Figure 4.

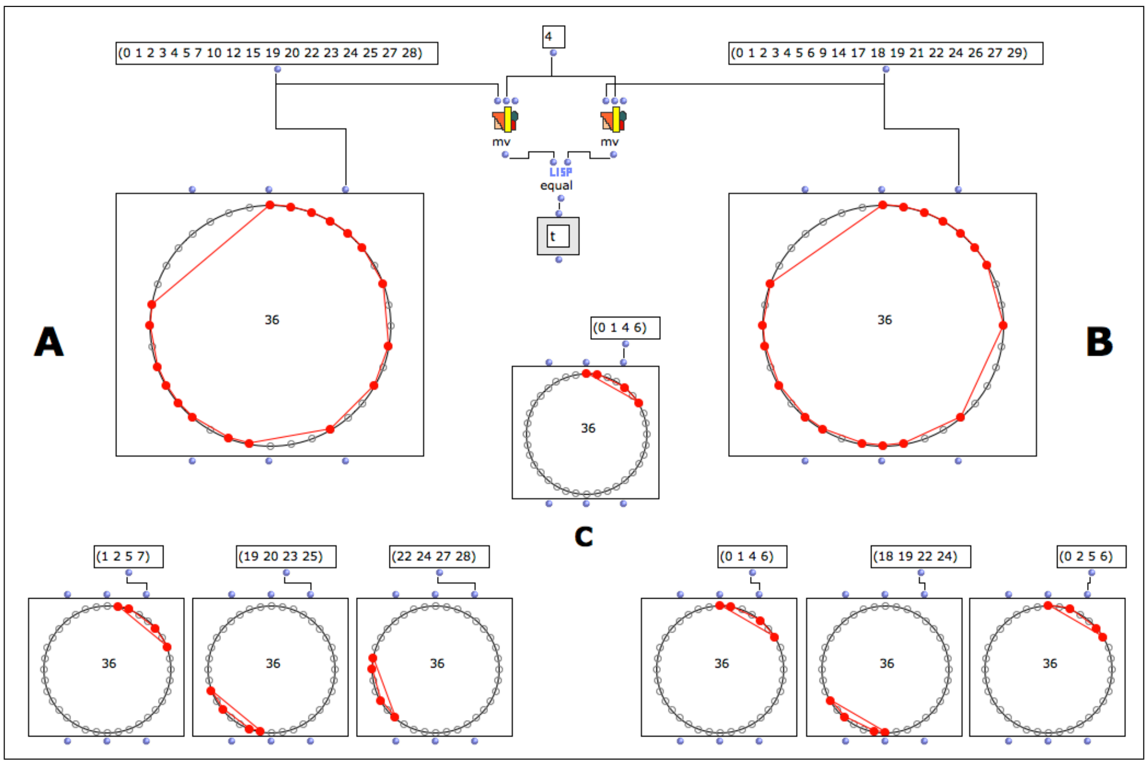

Figure 4: Two Z^4-related sets A and B in $\mathbb{Z}_{36}$. As an example, we consider the subset $C = \{0, 1, 4, 6\}_{36}$, and we show that the same number of copies, up to transposition and inversion (3, in this case) are included in the two initial sets. The OpenMusic patch shows also that this is true for any other 4-subset, by comparing the two $\mathbf{mv}^4$ functions.

5 Conclusion and open problems

After providing the general definition of the phase retrieval problem, we have summed up the recent results on the characterization of the homometry and the k-homometry, then have begun the analysis of the k-Homometry, and finally concluded with the first example of Z^4-related sets.

A number of outstanding open problems still remains. In particular:

- there is still no constructive characterization of the homometry, i.e. there is no reasonable way to determine, given a set (a distribution, respectively), whether it is non-trivially Z-related to other sets (homometric to other distributions, respectively) and to reconstruct them;
- the phase retrieval problem in the GIS of time spans [17, Sec. 5] is still to be solved; because of the non-commutativity of the group, the usual approach based on Fourier transform cannot be used, which calls for the search of new mathematical constructions, as suggested, for example, by Pebody in [19]; [18] uses a technique which is effective in abelian and hamiltonian[10] groups, but the time spans group is not hamiltonian;
- $r(n)$ still has to be fully determined (see Theorem 4.7);
- the behaviour of $R(n)$ as n increase is still unknown. It is likely to have a finite upper bound, like $r(n)$; given the example in section 4.2.2, we only know that the upper bound of $R(n)$ is greater or equal than 5; to study $R(n)$, we will probably need a way to circumvent the problem of dealing with potentially two different relations (7) and (8).

Although we have implemented original algorithms for searching Z and Z^k related sets, an extensive review and assessment of them will be necessary for a real application in computer-assisted musical composition and analysis. In particular, finding Z-and Z^k relations in existing musical works should help judging about the musical interest of Z and Z^k-relation in general.

Acknowledgments

The revision of the manuscript benefited crucially from the details comments and critiques provided by the two anonymous reviewers to which we are immensely grateful. Special thanks go to our colleague Pierre Beauguitte for having carefully proofread old versions of the two articles and suggested many pertinent mathematical corrections.

References

[1] T.A. Althuis and F. Göbel. Z-related pairs in microtonal systems. Memorandum 1524, University of Twente, April 2000.

[2] Emmanuel Amiot. Eine Kleine Fourier Musik. In *Mathematics and Computation in Music*, number 37-3 in Communications in Computer and Information Science, pages 469–476, Berlin, 2007. SMCM, Springer. Available from: `http://www.springerlink.com/content/rv46154m2n668630/`.

[10] By definition, a hamiltonian group is a non-abelian group G such that every subgroup of G is normal.

[3] Emmanuel Amiot. Discrete Fourier Transform and Bach's Good Temperament. *Music Theory Online*, 15(2), 2009. Available from: http:///mto.societymusictheory.org/issues/mto.09.15.2/mto.09.15.2.amiot.html.

[4] Emmanuel Amiot. On the group of rational spectral units with finite order. arXiv, 5 July 2009. Available from: http://arxiv.org/abs/0907.0857.

[5] Emmanuel Amiot and William A. Sethares. An Algebra for Periodic Rhythms and Scales. Preprint, 2009. Available from: http://canonsrythmiques.free.fr/pdf/AlgScales.pdf.

[6] John Adrian Bondy. A graph reconstructor's manual. In D. Keedwell, editor, *Surveys in Combinatorics 1991*, volume London Mathematical Society Lecture Notes Series, pages 221–252, Cambridge, 1991. Cambridge University Press. Available from: http://www.ecp6.jussieu.fr/pageperso/bondy/research/papers/recon.pdf.

[7] John Adrian Bondy and Robert Louis Hemminger. Graph reconstruction - a survey. *J. Graph Theory*, 1(3):227–268, 1977.

[8] Nick Collins. Uniqueness of Pitch Class Spaces, Minimal Bases and Z Partners. In *Proceedings of the Diderot Forum on Mathematics and Music*, Vienna, 1999.

[9] Daniele Ghisi. Vettori intervallari: non degenerazione e Z-relation. Bachelor's thesis, 2006.

[10] Francisco Alberto Grünbaum and Calvin C. Moore. The Use of Higher-Order Invariants in the Determination of Generalized Patterson Cyclotomic Sets. *Acta Cryst. Sect. A*, 51, 1995.

[11] Philippe Jaming. The phase retrieval problem for cyclotomic crystals. In T. Erdelyi, B. Saffari, and G. Tenenbaum, editors, *Topics on the Interface between Harmonic Analysis and Number Theory*, Marseille, 2005. CIRM. Cannot find volume publication reference nor editor on the WWW. Available from: http://www.univ-orleans.fr/mapmo/membres/jaming/recherche/habilitation/art17.pdf.

[12] Philippe Jaming and Mihail N. Kolountzakis. Reconstruction of functions from their triple correlations. *New York J. Math.*, 9, 2003. Available from: http://hal.archives-ouvertes.fr/hal-00005817/.

[13] Guillaume Lachaussée. Théorie des ensembles homométriques. Undergraduate thesis, June 2010. Available from: http://articles.ircam.fr/index.php?Action=ShowArticle&IdArticle=3785&ViewType=1.

[14] David Lewin. Intervallic Relations Between Two Collections of Notes. *J. Music Theory*, 3(2), 1959.

[15] David Lewin. *Generalized Musical Intervals and Transformations*. Yale University Press, second edition by Oxford University Press, 2007 edition, 1987.

[16] John Mandereau. Étude des ensembles homométriques et leur application en théorie mathématique de la musique et en composition assistée par ordinateur. Master's thesis, Université Pierre-et-Marie-Curie, June 2009. Available from: http://articles.ircam.fr/index.php?Action=ShowArticle&IdArticle=3934&ViewType=1.

[17] John Mandereau, Daniele Ghisi, Emmanuel Amiot, Moreno Andreatta, and Carlos Agon. Z-Relation and Homometry in Musical Distributions. *J. Math. & Music*, 5, 2011.

[18] Valery B. Mnukhin. The k-Orbit Reconstruction for Abelian and Hamiltonian Groups. *Acta Appl. Math.*, 52:149–162, 1998.

[19] Luke Pebody. The Reconstructibility of Finite Abelian Groups. *Combin. Probab. & Comput.*, 13(6):867–892, 2004.

[20] Luke Pebody. Reconstructing Odd Necklaces. *Combin. Probab. & Comput.*, 16(4), 2007.

[21] Ian Quinn. *A Unified Theory of Chord Quality in Equal Temperaments.* PhD thesis, Eastman School of Music, 2004. Available from: `http://music101.pbworks.com/f/Quinn,Ian-Diss.pdf`.

[22] Andrew John Radcliffe and Alexander David Scott. Reconstructing subsets of Zn. *J. Combin. Theory Ser. A*, 83(2):169–187, August 1998.

[23] Andrew John Radcliffe and Alexander David Scott. Reconstructing under Group Actions. *Graphs and Combinatorics*, 22(3), November 2006. Available from: `http://people.maths.ox.ac.uk/~scott/Papers/actions.pdf`.

[24] Hans Reiter. *Classical Harmonic Analysis and Locally Compact Groups.* Oxford University Press, 1968.

[25] Joseph Rosenblatt and Paul D. Seymour. The Structure of Homometric Sets. *SIAM J. Algebraic Discrete Methods*, 3(3):343–350, 1982.