Commun. Math. Phys. 95, 317–343 (1984)

Communications in
Mathematical
Physics

Phase Retrieval*

Joseph Rosenblatt

Mathematics Department, Ohio State University, Columbus, OH 43210, USA

Abstract. The problem of phase retrieval arises in experimental uses of diffraction to determine intrinsic structure because the modulus of a Fourier transform is all that can usually be measured after diffraction occurs. For finite distributions, the phase retrieval problem can be solved by methods of factorization in suitable rings of polynomials; for continuous distributions with compact support, the methods of complex analysis are needed to solve the phase retrieval problem. These methods are discussed and examples are given for illustration.

1. Introduction

The problem of phase retrieval arises in all experimental uses of diffracted electromagnetic radiation for determining the intrinsic detailed structure of a diffracting object. Usually, the measurement of the diffracted wavefront gives only the approximate values of the intensity of this wave form, and not its complex amplitude. Consequently, the phase information is not known explicitly and must be determined by other methods. Because most diffracted wavefronts in experimental situations are approximated by a Fourier transform or Fourier series in one or several variables, the methods of Fourier analysis are a great help to phase retrieval procedures. Using Fourier transforms, one sees that many phase retrieval problems are algebraic in nature; this algebraic aspect of phase retrieval is one of the main themes presented here.

A point source of monochromatic electromagnetic radiation falling on an opaque screen with slits or punctures will diffract in passing through the openings of the screen and create a new wave front that can be described precisely by Kirchoff's integral representation, which is a general type of integral transform. This Fresnel diffraction simplifies if one makes the assumption that the distance of the source to the screen and of the screen to the focusing plane of diffraction are both large with respect to the size of the holes in the screen and the wave length of

* Partially supported by NSF Grant MCS 8218800

the radiation. In this extreme case, the diffraction is called Fraunhofer diffraction; in Fraunhofer diffraction, the diffracted wave front is a good approximation to the Fourier transform of the characteristic function of the apertures in the screen, and the image screen will have the absolute value (or intensity) of this Fourier transform focused on it. See references [4, 17, 19, 25, 26, 40] for the theoretical background and examples of the use of Fraunhofer diffraction of this type in spectroscopy.

In X-ray spectroscopy, similar diffraction occurs by the Babinet principle. However, if the diffracting object is a crystalline substance with a periodic cellular structure, then the diffraction is heavily biased to those frequencies which are emphasized by the cellular structure. Hence, the diffracting wave front is numerically the complex amplitude of a Fourier series adjusted to coordinates appropriate for the shape of the unit cell. Thus, in determining the structure of crystals via X-ray crystallography, the absolute value of the Fourier series in three-dimensions is sampled at various spatial coordinates. The phase retrieval problem is especially difficult here because of the periodicity inherent in the Fraunhofer diffraction; this is reflected in radical changes in the algebraic nature of the phase retrieval problem. Usually the spectroscopist needs to employ chemical or physical intuition and algorithmic fitting of the data for the recovery of the structure from the diffracted intensity; this is all the more true in X-ray crystallography. See references [3, 15, 22, 27–30, 35, 41, 44] for background in X-ray crystallography and the uses of spectroscopy in chemistry.

All types of phase retrieval problems, aperiodic or periodic, discrete or continuous, can be treated with a common theory. From the viewpoint of modern Fourier analysis, the Fourier transform and Fourier series methods are just Fourier transform methods for different underlying group structures. The phase retrieval problem becomes a question of the behavior of Fourier transforms of distributions on groups. Say D is a distribution on an abelian group G for which the Fourier transform $\hat{D}(\gamma)$ is well-defined on the dual group Γ of G. The question is how to determine D given only $|\hat{D}|$? The *Patterson function*, $D * D^*$, is completely determined from the knowledge of $|\hat{D}|$ by taking the inverse Fourier transform. Consequently, the phase retrieval problem is to determine D knowing only $D * D^*$. This is not possible in general, even allowing for some trivial changes in D like reflection, translation, or scaling. However, there are some good algebraic and analytic techniques for determining all distributions E of the same type as D with $E * E^* = D * D^*$.

In Sect. 2, the algebra of phase retrieval is introduced in the generality of compactly-supported discrete measures on abelian groups. This includes both the periodic phase retrieval of X-ray crystallography and the aperiodic phase retrieval arising in other types of spectroscopic analysis. The totally aperiodic case is the best developed one and is discussed in Sect. 2. Then the periodic case is treated in Sect. 3; this is the one most immediately applicable in X-ray crystallography. In Sect. 4, the two previous cases are combined and a general factorization theorem is proved. Namely, up to scaling and a slight enlargement of the underlying groups, if D and E are in the group ring $K[G]$ over a conjugation-closed subfield K of C, the complex numbers, and the abelian group G, then $D * D^* = E * E^*$ if and only if $D = A * B$ and $\pm E = A * B^*$ for some A and B. In Sect. 5, the analytic methods of phase retrieval for continuous distributions are described. The behavior of the holomorphic functions which are analytic extensions of Fourier transforms is critical to this type of phase retrieval. Here the general factorization scheme does not apply because there exists $f, g \in C_c^\infty(R)$, the smooth functions with compact support on R, such that $f*f^* = g*g^*$, but there is no joint factorization $f = a*b$ and $g = a*b^*$ with complex-valued functions $a, b \in C_c^\infty(R)$. To obtain a factorization theorem here requires going outside of $C_c^\infty(R)$ to more general distributions for the factors a and b. An appendix to Sects. 3 and 4 is provided which gives the details of some joint work with Joel Berman.

2. Generalities and the Aperiodic Case

Let G be an abelian group. A finite distribution D on G has the form $\sum a_g\delta_g$, where $a_g \in C$, $a_g \neq 0$ only finitely often, in the usual Dirac mass notation. The algebra of such distributions under the convolution product is isomorphic with the group ring $C[G]$. The reflection D^* of $D = \sum a_g\delta_g$ is defined to be $D^* = \sum \bar{a}_g\delta_{-g}$, where $\bar{a}_g$ is the complex conjugate of a_g.

Let Z denote the integers. When G is a direct sum $Z^M \oplus \bigoplus_{i=1}^{N} Z_{n_i}$, where $Z_{n_i} = Z/\langle n_i\rangle$ are cyclic groups of order n_i, then there is an alternate polynomial notation that is very appropriate and convenient. Suppose that $x_1, \ldots, x_M$ are free generators of the summand Z^M, and $y_i \in Z_{n_i}$ is a generator of the finite cyclic summand Z_{n_i}. Any element D of the group ring $C[G]$ has the form of a polynomial $D = \sum a(k_1, \ldots, k_M, \; l_1, \ldots, l_N)x_1^{k_1}, \ldots, x_M^{k_M}y_1^{l_1}\ldots y_N^{l_N}$, where the sum is finite, $a(k_1, \ldots, k_M, l_1, \ldots, l_N) \in C$ for all $k_1, \ldots, k_M, l_1, \ldots, l_N$ and the exponents $k_1, \ldots, k_M$, $l_1, \ldots, l_N \in Z$. The multiplication in $C[G]$ then corresponds to polynomial multiplication, with the usual rules of exponents for exponents in Z, expect that we have the relations $y_i^{N_i} = 1$ for $i = 1, \ldots, N$. Because of these relations, the exponents k_i can always be taken to be in $\{0, 1, \ldots, n_i - 1\}$ for each $i = 1, \ldots, N$. The reflection D^* of D is given by $D^* = \sum \bar{a}(k_1, \ldots, k_M, l_1, \ldots, l_N)x_1^{-k_M}\ldots x_M^{-k_M}y_1^{-l_1}\ldots y_N^{-l_N}$. Occasionally the same polynomial notation will be used with exponents in the rational numbers too.

Let Γ be the group of all homomorphisms of G into the circle group $T = \{z \in C: |z| = 1\}$. The Fourier transform of $D \in C[G]$ is defined by $\hat{D}(\gamma) = \sum a_g\overline{\gamma(g)}$ for all $\gamma \in \Gamma$, where $D = \sum a_g\delta_g$. It is easy to see that $\widehat{D^*}(\gamma) = \overline{\hat{D}(\gamma)}$ for all $\gamma \in \Gamma$. Also, it is easy to check that if D_1, $D_2 \in C[G]$, then $\widehat{D_1 * D_2}(\gamma) = \hat{D}_1(\gamma)\hat{D}_2(\gamma)$ for all $\gamma \in \Gamma$. Consequently, if the optical transform is $\hat{D}$ and $D * D^* = E * E^*$, then $|\hat{D}(\gamma)| = |\hat{E}(\gamma)|$ for all $\gamma \in \Gamma$. Furthermore, whenever $A \in C[G]$ and $\hat{A}(\gamma) = 0$ for all $\gamma \in \Gamma$, then $A = 0$. So $D * D^* = E * E^*$ if and only if $|\hat{D}(\gamma)| = |\hat{E}(\gamma)|$ for all $\gamma \in \Gamma$.

2.1. Definition. If D, $E \in C[G]$, then D and E are *homometric* if $D * D^* = E * E^*$.

The finite distributions D and E are homometric if and only if they are equivalent under Fraunhofer diffraction. The term "homometric" was originally used by Patterson [33–35] for G being T^n or R^n; he imposed the additional restriction that D and E are not equivalent up to an isometry of the underlying group, a restriction that is dropped in the definition above.

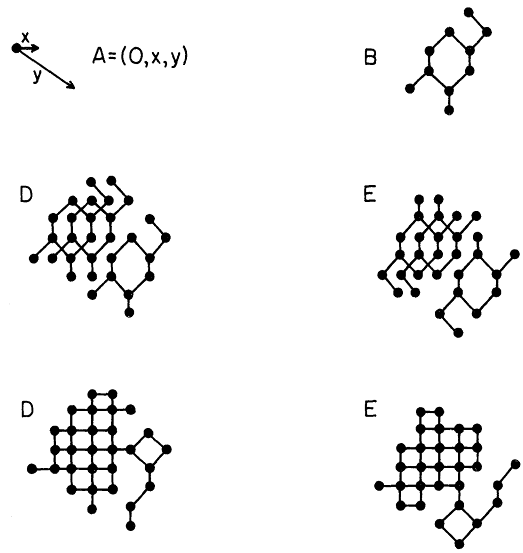


Fig. 1. Here A and B are illustrated in the first row; D and E are shown twice, the first time with B still outlined

The algebraic theory of homometric distributions for $G=R^n$ was completed in Rosenblatt and Seymour [39]. The initial observation (actually motivated by the type of factorization theorems in Sect. 5) was that if A, $B\in C[G]$, then $D=A*B$ and $E=A*B^*$ are homometric. This seems to also have been realized by Patterson and others; see Bullough [11, 12] and Hosemann and Bagchi [24, 25], but they did not realize the algebraic significance of using the ring $K[G]$ instead of $Z^+[G]$. First, let us consider some of the consequences of this construction of homometric pairs. If $A\in R^n$, then the distribution $1_A=\sum\{\delta_x : x\in A\}$ is a $\{0,1\}$-valued distribution on R^n. If A, $B\in R^n$ are well-dispersed finite sets, then $D=1_A*1_B$ and $E=1_A*1_{-B}$ will be $\{0,1\}$-valued homometric finite distributions. This method of constructing homometric pairs via convolutions is illustrated in R^2 in Fig. 1. In this figure, D and E are non-congruent point sets too. We say D, $E\subset R^n$ are *homometric* if 1_D and 1_E are homometric distributions. Generally, if D, $E\in C[G]$, then D and E are said to be *trivially homometric* if $D=c\delta_g*E$ or $D=c\delta_g*E^*$ for some $c\in C$, $|c|=1$, and $g\in G$. Clearly, non-congruent point sets do not determine trivially homometric distributions; so the example in Fig. 1 is not trivially homometric.

A natural question here is how many mutually homometric finite sets can be generated using only k points? The convolution method above gives a partial answer to this question. Let $\mathscr{P}$ be a finite set of finite sets in R^n with card$(P)=k$ for each $P\in\mathscr{P}$. Assume that if P_1, $P_2\in\mathscr{P}$, $P_1\neq P_2$, then P_1 and P_2 are homometric and noncongruent. The set $\mathscr{P}$ has some card$(\mathscr{P})$ number of elements. Define $C_n(k)$ to be the largest value of card$(\mathscr{P})$, where $\mathscr{P}$ ranges over all sets with the properties described above.

2.2. Proposition. *For* $m\geqq 1$, $C_1(3^m)\geqq 2^{m-1}$ *and* $C_n((n+1)^m)\geqq 2^{m-1}$ *if* $n\geqq 2$.

2.3. Corollary. *For any* $M\geqq 1$ *and* $n\geqq 1$, *there exists* $k\geqq 1$ *such that* $C_n(k)\geqq M$.

Proof of Proposition 2.2. It is easy to see that there exists sets $A\subset R^n$ such that, 1) $\operatorname{card}(A)=n+1$ for $n\geqq 2$, and $\operatorname{card}(A)=3$ if $n=1$, and 2) for any $x_1, x_2, y_1, y_2\in A$, if $\|x_1-x_2\|=\|y_1-y_2\|$, then $\{x_1, x_2\}=\{y_1, y_2\}$. Indeed, such sets A exist in profusion. It is not hard to see that such a set has the property that if φ is an isometry of R^n and $\varphi(A)=A$, then φ is the identity mapping. This allows us to choose sets $A_1, \ldots, A_m$, each with $\operatorname{card}(A_i)=\operatorname{card}(A)$, such that, 1) the only isometry φ with $\varphi(A_i)=A_i$ for some $i=1, \ldots, m$ is the identity mapping, and 2) for each $k=2, \ldots, m$, the shortest length of a vector $x-y$, $x, y\in A_k$, is strictly more than twice the length of the longest $x-y$, $x, y\in \varepsilon_1 A_1+\ldots+\varepsilon_{k-1}A_{k-1}$, where $\varepsilon_1, \ldots, \varepsilon_{k-1}$ range over all choices of sign ± 1.

Choose some $\varepsilon_1, \ldots, \varepsilon_m\in\{1, -1\}$ and define $A(\varepsilon_1, \ldots, \varepsilon_m)=\varepsilon_1 A_1+\varepsilon_2 A_2+\ldots+\varepsilon_m A_m$. By the remarks above about the convolution method, each $A(\varepsilon_1, \ldots, \varepsilon_m)$ is homometric to $A(1, \ldots, 1)$. It is not hard to show that if $(\varepsilon_1, \ldots, \varepsilon_m)\neq(\zeta_1, \ldots, \zeta_m)$, $\varepsilon_1=\zeta_1=1$, then $A(\varepsilon_1, \ldots, \varepsilon_m)$ is not congruent to $A(\zeta_1, \ldots, \zeta_m)$. Therefore, we have $C_1(3^m)\geqq 2^{m-1}$ and $C_n((n+1)^m)\geqq 2^{m-1}$ because there are 2^{m-1} possible choices of signs $\varepsilon_2, \ldots, \varepsilon_m$. and $\operatorname{card}(A(\varepsilon_1, \ldots, \varepsilon_m))=\operatorname{card}(A)^m$ for all $\varepsilon_1, \ldots, \varepsilon_m$. □

Very little else is known about $C_n(k)$ even for small values of k. Does there exist a function $m_n(k)$ with $m_n(k)$ increasing to infinity as $k\to\infty$ with $C_n(k)\geqq m_n(k)$? If k is prime, $k\geqq 5$, is $C_n(k)>1$? These questions are difficult to answer even though we know that the convolution method is theoretically the only method available to use as in Proposition 2.2. This is because it is difficult to determine conditions on a finite set $D\subset R^n$ which guarantees that it factors (in many different ways) non-trivially as $1_D=A*B$ with $A, B\in Z[R^n]$, such that $A*B^*$ is a $\{0, 1\}$-valued finite distribution too. For example, let $A(x)$, $B(x)$ be finite distributions represented in polynomial form by $A(x)=x^{5/2}(1+x+x^2+x^3+x^4+x^5+x^7)$ and $B(x)=x^{-5/2}(1-x^3+x^5)$. Then $D(x)=A(x)B(x)=1+x+x^2+x^5+x^7+x^9+x^{12}$, and $E(x)=A(x)B(x^{-1})=1+x+x^5+x^7+x^8+x^{10}+x^{12}$. Hence, $\{0, 1, 5, 7, 8, 10, 12\}$ and $\{0, 1, 2, 5, 7, 9, 12\}$ are homometric sets in Z, but they do not factor as above with positive factors in place of A and B. This behavior is an inherent difficulty for the phase retrieval problem in general.

For the remainder of this section, G will be an abelian group with no elements of finite order. We will usually restrict the coefficients of the distributions to some ring K, $Z\subset K\subset C$, such that K is closed under conjugation. If $D, E\in K[G]$, then there is a finitely-generated subgroup $H\subset G$ which contains the supports of D and E. Since G is torsion-free, there exists some $x_1, \ldots, x_m\in H$ such that $H=Zx_1\oplus\ldots\oplus Zx_m\cong Z^m$. Similarly, given a finite set of elements of $K[G]$, we can find a subgroup $H\cong Z^m$ in G which supports all the distributions. Now even in $C[G]$, the units are trivial; that is, if $U\in C[G]$ and $U*V=\delta_0$ for some $V\in C[G]$, then there exists $c\in C$, $|c|=1$, and $g\in G$ such that $U=c\delta_g$. However, $C[G]$ is not a UFD (unique factorization domain). Indeed, in polynomial notation,

$$\begin{aligned}1-x&=(1-x^{1/2})(1+x^{1/2})=(1-x^{1/4})(1+x^{1/4})(1+x^{1/2})\\&=(1-x^{1/2^{i+1}})\prod_{j=1}^{i+1}(1+x^{1/2^j})\end{aligned}$$

for all $i=0,1,2,\ldots$. So $Z[Q]$ is not a UFD. On the other hand, the observation above shows that we need only work in the subgroup ring $K[Z^m]$ for any particular finite set of finite distributions, and $K[Z^m]$ is a UFD whenever K is a UFD. *We assume then for the remainder of this section that K is a* UFD, $Z\subset K\subset C$, *with* $\bar{K}=K$. Then any element $D\in K[Z^m]$ has a unique factorization (up to units) into prime factors relative to $K[Z^m]$. Using this, we have the following theorem as in [39].

2.4. Theorem. *If $D, E\in K[G]$ are homometric, then there exists $c_1, c_2\in K$, $|c_1|=|c_2|=1$, $g_1, g_2\in G$, and $A, B\in K[G]$ such that $D=c_1\delta_{g_1}*A*B$ and $E=c_2\delta_{g_2}*A*B^*$.*

In the above $E=c_2\bar{c}_1\delta_{g_2}*c_1A*B^*$ and $D=\delta_{g_1}*c_1A*B^*$. Hence, we may assume $c_1=1$ without loss of generality. Then if also $c_2\neq -1$ and K is a field, $E=\delta_{g_2}*A_1*B_1^*$ and $D=\delta_{g_1}*A_1*B_1$, where $A_1=(1+c_2)A$ and $B_1=(1+c_2)^{-1}B$. Hence, if K is a field, then we may assume $c_1=1$ and $c_2=\pm 1$ without loss of generality. Finally, since $\delta_{g_1}=\delta_{(g_1+g_2)/2}*\delta_{(g_1-g_2)/2}$ and $\delta_{g_2}=\delta_{(g_1+g_2)/2}*(\delta_{(g_1-g_2)/2})^*$, if we use factors A and B with mass in $\frac{1}{2}G$, we may assume $g_1=g_2=0$. These observations lead to this corollary which is needed in Sect. 4.

2.5. Corollary. *If $D, E\in K[G]$ are homometric and K is a field, then there exists $\varepsilon_1, \varepsilon_2\in\{1, -1\}$ and $A, B\in K[\frac{1}{2}G]$ such that $D=\varepsilon_1 A*B$ and $E=\varepsilon_2 A*B^*$.*

Remark. If $G=Q$, R or C, then certainly $\frac{1}{2}G=G$, but generally, the factorization of type 2) cannot be obtained in G itself. See the remarks after Theorem 4.1.

The method of proof of Theorem 2.3 easily adapts to the situation where there is more than a pair of homometric elements D and E.

2.6. Theorem. *If $D_1,\ldots,D_m\in K[G]$ are homometric to one another, then there exists $c_i\in K$, $|c_i|=1$, $g_i\in G$, and $A_i\in K[G]$, $i=1,\ldots,n$ such that $D_1=c_1\delta_{g_1}*A_1*\ldots*A_n$, and $D_i=c_i\delta_{g_i}*A_1^{\varepsilon_1(i)}*\ldots*A_n^{\varepsilon_n(i)}$ for some choices of $A_k^{\varepsilon_k(i)}\in\{A_k, A_k^*\}$, $k=1,\ldots,n$, depending on $i=2,\ldots,m$.*

Remark. An improvement of 2.6 along the lines of 2.5 is generally possible.

One positive aspect of the method here is that it provides algebraic criteria for a finite distribution to be essentially determined by the intensity of its diffraction. If $D\in K[G]$, then D is *uniquely retrievable* if whenever $E\in K[G]$, and D and E are homometric, then $D=c\delta_g*E$ or $D=c\delta_g*E^*$ for some $c\in K$, $|c|=1$, and $g\in G$.

It is clear that both K and G affect whether D is uniquely retrievable. The polynomial x^2+4 is uniquely retrievable in $R[Z]$ because it is irreducible, but it is not uniquely retrievable in $C[Z]$. Indeed, $x^2+4=(x+2i)(x-2i)$. So

$$q(x)=(x+2i)(x-2i)^*=(x+2i)(x^{-1}+2i)=2ix^{-1}-3+2ix,$$

and $p(x)=x^2+4$ determine homometric elements in $C[Z]$ which are not trivially homometric. Similarly, $x-4$ is uniquely retrievable in $C[Z]$, but $x-4=(x^{1/2}-2)(x^{1/2}+2)$. So

$$\begin{aligned}q(x)&=(x^{1/2}-2)(x^{1/2}+2)^*\\&=(x^{1/2}-2)(x^{-1/2}+2)=-2x^{-1/2}-3+2x^{1/2}\end{aligned}$$

and $p(x)=x-4$ determine homometric elements in $C[\frac{1}{2}Z]$ which are not trivially homometric. Hence, enlarging K or G can affect whether a distribution is uniquely retrievable.

To characterize which finite distributions are uniquely retrievable, the notion of semi-symmetry is needed. If $D \in K[G]$, then D is *semi-symmetric* (*with symmetry constant* c) if there exists $c \in K$, $|c|=1$, and $D^* = c\delta_g * D$ for some $g \in G$.

The argument in [39] shows the following.

2.7. Theorem. *If G is finitely-generated, then $D \in K[G]$ is uniquely retrievable if and only if at most one of its prime factors in $K[G]$ is not semi-symmetric.*

3. The Periodic Case

Throughout this section, G will be a finite abelian group; so $G = \bigoplus_{i=1}^{N} Z_{n_i}$, a direct sum of cyclic groups Z_{n_i} of order n_i. The coefficient ring K is taken to be a field, $K \subset C$, which is closed under conjugation. The group ring $K[G]$ is now far from being a unique factorization domain; it is not even an integral domain because if $e = \text{order}(G)$, then $(\delta_g - \delta_0)(\delta_{(e-1)g} + \ldots + \delta_0) = \delta_{eg} - \delta_0 = 0$ for all $g \in G$. Hence, a completely different method of phase retrieval must be used to obtain the analogue of Theorem 2.4 and Corollary 2.5 in this case.

To illustrate some of the problems that periodic groups present, we will look at the one-dimensional case of Z_n first. This cyclotomic case was studied originally by Patterson [33] and later by others, including Buerger [5–10] and Chieh [18]. See also [11, 12, 24, 25] for references. The diagrammatic tool here applies equally well to the one-dimensional case with unit cell $[0,1) = \{x : 0 \leqq x < 1\}$. First choose some set A consisting of $k \geqq 2$ points in $[0,1)$. We measure lengths modulo 1, so the length of a, $a \in [0,1]$, and $1-a$ are considered the same; however, to be consistent in this, we will always choose the smaller of the two. It is convenient to illustrate this point distribution as if it were on a circle of circumference one. All pairs of points are joined by chords. The set of chords is called the *Patterson diagram of A*. Our convention is to give a chord in the Patterson diagram a length equal to the length of the smaller arc that it subtends. Typically, if the points of A are at the vertices of a regular n-sided polygon (called a *cyclotomic set*), then the lengths of the chords in the Patterson diagram are all of the form m/n, where $m \in \{1, 2, 3, \ldots\}$. If the diagram is cyclotomic, usually only the numbers m are shown (see Fig. 2 for examples). In this figure, we have illustrated two pairs of homometric cyclotomic sets which are fundamental to the classification of homometric pairs with 4 points in the unit cell $[0,1)$. These examples illustrate the importance of periodicity. The elements $D = \delta_0 + \delta_3 + \delta_4 + \delta_5$ and $E = \delta_0 + \delta_1 + \delta_3 + \delta_4$ are not homometric in $C[Z]$, but they are homometric in $C[Z_8]$. Indeed, two sets D, $E \in Z_n$ are homometric if and only if their Patterson diagrams contain the same lengths counting multiplicities. So the examples in Fig. 2 are homometric in $Z[Z_8]$ and $Z[Z_{13}]$ respectively.

In dealing with finite abelian groups, it will again be convenient to use polynomial notation. Here $K[G]$ can be identified with the polynomial ring $K[x_1, \ldots, x_N]/I$, where $x_1, \ldots, x_N$ are commuting variables and I is the ideal

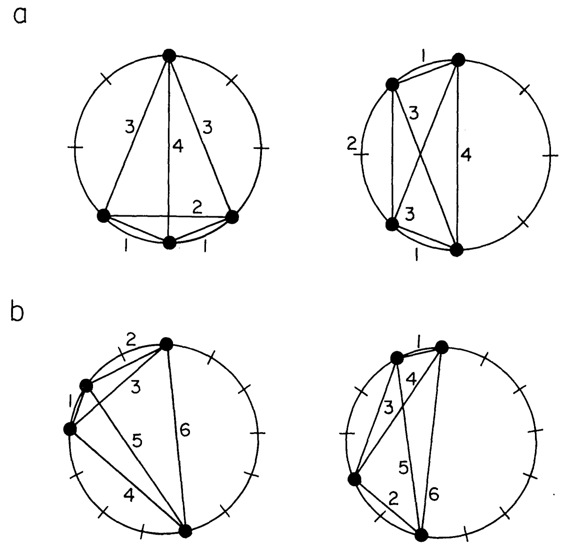


Fig. 2. a $(n, k)=(8, 4)$; **b** $(n, k)=(13, 4)$

generated by $\{x_1^{n_1}-1, \ldots, x_N^{n_N}-1\}$. Also, to compute $\hat{D}(\gamma)$ for $D \in K[G]$, we first express $D=\sum a(l_1, \ldots, l_N)\delta x_1^{k_1} * \ldots * \delta x_N^{k_N}$, or $D=\sum a(l_1, \ldots, l_N) x_1^{k_1} \ldots x_N^{k_N}$ in the polynomial form. For $\gamma \in \Gamma$, $\hat{D}(\gamma)=\sum a(l_1, \ldots, l_N)\overline{\gamma(x_1)}^{k_1} \ldots \overline{\gamma(x_N)}^{k_N}$, where $\gamma(x_i) \in C$, $i=1, \ldots, N$. But $\gamma(x_i)$ is an n_i^{th} root of unity and the values of $\gamma(x_i)$, $i=1, \ldots, N$, completely determine γ. By mapping γ to $(\overline{\gamma(x_1)}, \ldots, \overline{\gamma(x_N)})$, we map Γ isomorphically onto $\bigoplus_{i=1}^{N} \mathscr{R}(n_i)$, where $\mathscr{R}(m)$ is the multiplicative group in C of m^{th} roots of unity. Let $\gamma_i=\overline{\gamma(x_i)}$ for $i=1, \ldots, N$. Then, the polynomial evaluation $D(\gamma_1, \ldots, \gamma_N)$ equals $\hat{D}(\gamma)$. This method of computing $\hat{D}$ when D is expressed in polynomial form will be used in the sequel. An additional advantage of this notation is that if D_1, $D_2 \in K[x_1, \ldots, x_N]$, then $D_1-D_2 \in I$, thus determining identical elements of $K[G]$, if and only if $D_1(\gamma_1, \ldots, \gamma_N)=D_2(\gamma_1, \ldots, \gamma_N)$ for all $(\gamma_1, \ldots, \gamma_N) \in \bigoplus_{i=1}^{N} \mathscr{R}(n_i)$.

Unlike the case of $K[x_1, \ldots, x_N]$, the units of $K[x_1, \ldots, x_N]/I$ are anything but trivial. A unit $U \in K[G]$ is called a *spectral unit* if $U * U^*=\delta_0$. It is clear that U is a spectral unit if and only if U and δ_0 are homometric. The spectral units are especially important because of this theorem.

3.1. Theorem. *If D, $E \in K[G]$, then D and E are homometric if and only if there exists a spectral unit $U \in K[G]$ such that $U * D=E$.*

This theorem only presents algebraic difficulties because K is not assumed to be C. Indeed, suppose D and E are homometric. Let $u(\gamma)=\hat{E}(\gamma)/\hat{D}(\gamma)$ if $\hat{D}(\gamma) \neq 0$, and $u(\gamma)=1$ otherwise. Because G is finite, there exists $U \in C[G]$ such that $\hat{U}=u$; hence, $|\hat{U}(\gamma)|=1$ for all $\gamma \in \Gamma$, and U is a spectral unit. Moreover, $U * D=E$ because $\hat{U}\hat{D}=\hat{E}$. To insure that $U \in K[G]$, more argument is needed. The proof will be by induction on N, the number of summands of G. This lemma can be used to prove the case $N=1$ and will also be needed later for the factorization theorem.

3.2. Lemma. *If* $D \in K[Z_n]$, *there exists* $W \in K[Z_n]$ *such that* $\hat{W} = 1_{\{\gamma \in \Gamma : \hat{D}(\gamma) = 0\}}$.

Proof. We take $D \in K[Z_n]$ and write D in polynomial form. Let $F = gcd(D, x^n - 1)$ in $K[x]$. Then there exists $A, B, M_1, M_2 \in K[x]$ such that $F = AD + B(x^n - 1)$, $D = M_1 F$, and $x^n - 1 = M_2 F$. If $\gamma \in \mathscr{R}(n)$ and $D(\gamma) = 0$, then $F(\gamma) = 0$. Conversely, if $F(\gamma) = 0$, then $\gamma \in \mathscr{R}(n)$ and $D(\gamma) = 0$, Hence, for some $k \in K$, $F = k\prod\{(x - \gamma) : D(\gamma) = 0 \text{ and } \gamma^n = 1\}$. Also, if $\gamma^n = 1$ and $D(\gamma) \neq 0$, then $F(\gamma) \neq 0$ and so $M_2(\gamma) = 0$. But the roots of $x^n - 1$ are not repeated, hence, if $\gamma^n = 1$ and $D(\gamma) = 0$, then $M_2(\gamma) \neq 0$. Let $V = D + M_2$. Then $V \in K[x]$, $V(\gamma) = D(\gamma)$ if $D(\gamma) \neq 0$, $\gamma \in \mathscr{R}(n)$, while $V(\gamma) \neq 0$ for all $\gamma \in \mathscr{R}(n)$. By using the relation $x^n = 1$, we may assume $\deg(V) = n - 1$ without altering these properties.

We write $V = \sum_{i=0}^{n-1} v_i x^i$ and seek a solution $U = \sum_{i=0}^{n-1} u_i x^i \in K[x]$ to the equation $UV = 1 \bmod (x^n - 1)$. This equation is the same as the system of equations

$$\begin{aligned} 1 &= u_0 v_0 + u_1 v_{n-1} + \ldots + u_{n-1} v_1 \\ 0 &= u_0 v_1 + u_1 v_0 + \ldots + u_{n-1} v_2 \\ &\vdots \\ 0 &= u_0 v_{n-1} + u_1 v_{n-2} + \ldots + u_{n-1} v_0 \,. \end{aligned} \tag{1}$$

The circulant matrix $\mathscr{C}$ composed of the coefficients v_i has $\det\mathscr{C} \neq 0$ because $V(\gamma) \neq 0$ for all $\gamma \in \mathscr{R}(n)$. Indeed, it is well-known that $\det\mathscr{C} = \prod\{V(\gamma) : \gamma \in \mathscr{R}(n)\}$. Hence, by Cramer's Rule, the system of (1) has a solution $(u_0, u_1, \ldots, u_{n-1})$ with $u_i \in K$, $i = 0, \ldots, n-1$.

Let $W_0 = UD$. Since $U(D + M_2) = 1 \bmod (x^n - 1)$, if $D(\gamma) \neq 0$ and $\gamma \in \mathscr{R}(n)$, then $W_0(\gamma) = U(\gamma)D(\gamma) = 1$. Also, if $D(\gamma) = 0$ and $\gamma \in \mathscr{R}(n)$, then $W_0 = U(\gamma)D(\gamma) = 0$. Hence, $W = \delta_0 - W_0$ provides an element of $K[Z_n]$ such that $\hat{W} = 1_{\{\gamma \in \Gamma : \hat{D}(\gamma) = 0\}}$. □

This lemma gives immediately the following special case of Theorem 3.2.

3.3. Proposition. *If* $D, E \in K[Z_n]$, *then* D *and* E *are homometric if and only if there exists a spectral unit* $U \in K[Z_n]$ *such that* $U * D = E$.

Proof. Choose $W \in K[Z_n]$ such that $\hat{W} = 1_{\{\gamma \in \Gamma : \hat{D}(\gamma) = 0\}}$. Then let U be a solution to $U * (D + W) = E + W$. This is possible as in the proof of Lemma 3.2 because $\widehat{(D + W)}$ is never zero and Cramer's rule can be used; moreover, $U \in K[Z_n]$ too. Then $\hat{U}(\gamma)\hat{D}(\gamma) = \hat{E}(\gamma)$ if $\hat{D}(\gamma) \neq 0$, and $\hat{U}(\gamma)\hat{W}(\gamma) = \hat{U}(\gamma) = \hat{W}(\gamma) = 1$ if $\hat{D}(\gamma) = 0$, for $\gamma \in \Gamma$. If D and E are homometric, then $|\hat{U}(\gamma)| = 1$ for all $\gamma \in \Gamma$ and $\hat{U}(\gamma)\hat{D}(\gamma) = \hat{E}(\gamma)$ for all $\gamma \in \Gamma$. This establishes the non-trivial part of the proposition. □

Proof of Theorem 3.1. The proof is by induction on N where $G = \bigoplus_{i=1}^{N} Z_{n_i}$. By Proposition 3.3, we may assume $N > 1$ and the theorem is proved if G is a direct sum of cyclic groups of less than N summands. Let $D, E \in K[G]$ be homometric. Fix $\gamma \in \mathscr{R}(n_N)$. Then, using polynomial notation, $D(x_1, \ldots, x_{N-1}, \gamma)$ and $E(x_1, \ldots, x_{N-1}, \gamma)$ are homometric in $K(\gamma)\,[x_1, \ldots, x_{N-1}]$. By induction, there exists $U_\gamma \in K(\gamma)\,[x_1, \ldots, x_{N-1}]$ such that $|U_\gamma(\gamma_1, \ldots, \gamma_{N-1})| = 1$ for all $\gamma_i \in \mathscr{R}(n_i)$, $i = 1, \ldots, N-1$, and such that $U_\gamma D(x_i, \ldots, x_{N-1}, \gamma) = E(x_1, \ldots, x_{N-1}, \gamma)$.

Let γ_0 be a primitive n_Nth root of unity. Let Σ be the Galois group of automorphisms of $K(\gamma_0)$ fixing K. Because $K(\gamma_0)$ is a splitting field for $x^{n_N}-1$, the extension $K(\gamma_0)\supset K$ is normal and K is the fixed field of Σ. Let $\sigma\in\Sigma$ and define $T_\sigma: K(\gamma_0)[x_1,\dots,x_{N-1}]\to K(\gamma_0)[x_1,\dots,x_{N-1}]$ by $T_\sigma(\sum W(k_1,\dots,k_{N-1})x_1^{k_1}\dots x_{N-1}^{k_{N-1}})=\sum\sigma(W(k_1,\dots,k_{N-1}))x_1^{k_1}\dots x_{N-1}^{k_{N-1}}$. If $W\in K(\gamma_0)[x_1,\dots,x_{N-1}]$, and $T_\sigma(W)=W$ for all $\sigma\in\Sigma$, then W has coefficients in K. Notice that $T_\sigma(U_\gamma)D(x_1,\dots,x_{N-1},\sigma(\gamma))=E(x_1,\dots,x_{N-1},\sigma(\gamma))$ when $U_\gamma D(x_1,\dots,x_{N-1},\gamma)=E(x_1,\dots,x_{N-1},\gamma)$. Hence, we can choose $\{U_\gamma:\gamma\in\Gamma\}$ such that for all $\sigma\in\Sigma$, $\gamma\in\mathscr{R}(n_N)$, $T_\sigma(U_\gamma)=U_{\sigma(\gamma)}$. Indeed, choose $\alpha_1,\dots,\alpha_K\in\mathscr{R}(n_N)$ such that $\bigcup_{i=1}^{K}\Sigma(\alpha_i)=\mathscr{R}(n_N)$ and $\Sigma(\alpha_i)\cap\Sigma(\alpha_j)=\phi$ if $i\neq j$. Then for each i, choose $U_{\alpha_i}\in K(\alpha_i)[x_i,\dots,x_{N-1}]$ as above. For $\sigma\in\Sigma$, define $U_{\sigma(\alpha_i)}=T_\sigma(U_{\gamma_i})$. This is well-defined since $\sigma_1(\alpha_i)=\sigma_2(\alpha_i)$ for $\sigma_1,\sigma_2\in\Sigma$ implies $\sigma_1=\sigma_2$ on $K(\alpha_i)$ and, hence, $T_{\sigma_1}=T_{\sigma_2}$ on $K(\alpha_i)[x_1,\dots x_{N-1}]$. Now if $\sigma\in\Sigma$ and $\gamma\in\mathscr{R}(n_N)$, choose $\sigma_0\in\Sigma$ and $i=1,\dots,K$ such that $\sigma_0(\alpha_i)=\gamma$. Then we have $T_\sigma(U_\gamma)=T_\sigma(U_{\sigma_0(\alpha_i)})=T_\sigma(T_{\sigma_0}U_{\alpha_i})=T_{\sigma\sigma_0}(U_{\alpha_i})=U_{\sigma\sigma_0(\alpha_i)}=U_{\sigma(\gamma)}$.

Consider now the system of equations

$$U_\gamma(x_1,\dots,x_{N-1})=\sum_{i=0}^{n_N-1}\tilde U_i(x_1,\dots,x_{N-1})\gamma^i,\ \gamma\in\mathscr{R}(n_N),\tag{2}$$

where the unknowns $\tilde U_0,\dots,\tilde U_{n_N-1}\in C[x_1,\dots,x_{N-1}]$. If we can find a solution $(\tilde U_0,\dots,\tilde U_{n_N-1})$ with $\tilde U_0,\dots,\tilde U_{n_N-1}\in K[x_1,\dots,x_{N-1}]$, then we can define $U(x_1,\dots,x_N)=\sum_{i=0}^{n_N-1}\tilde U_i x_N^i$ and $U\in K[x_1,\dots,x_N]$. Moreover, $|U(\gamma_1,\dots,\gamma_{N-1},\gamma)|=|U_\gamma(\gamma_1,\dots,\gamma_{N-1})|=1$ for all $\gamma_i\in\mathscr{R}(n_i)$, $i=1,\dots,N-1$, and $\gamma\in\mathscr{R}(n_N)$. Also, $U(\gamma_1,\dots,\gamma_{N-1},\gamma)D(\gamma_1,\dots,\gamma_{N-1},\gamma)=E(\gamma_1,\dots,\gamma_{N-1},\gamma)$ for all $\gamma_i\in\mathscr{R}(n_i)$, $i=1,\dots,N-1$, and $\gamma\in\mathscr{R}(n_N)$. Hence, $U(x_1,\dots,x_N)D(x_1,\dots,x_N)=E(x_1,\dots,x_N)\bmod I$, and so $U(x_1,\dots,x_N)$ determines a spectral unit as in the statement of the theorem.

But now there is a unique solution to (2) by Cramer's rule because the coefficient matrix $\Delta=(\gamma^i:\gamma\in\mathscr{R}(n_N),\ i=0,\dots,n_N-1)=(\gamma_0^{ij}:i,j=0,\dots,n_N-1)$ has non-vanishing determinant. Let Δ_j be the matrix obtained by replacing the jth column of Δ by the transpose of $(U_1,U_{\gamma_0},\dots,U_{\gamma_0^{n_N-1}})$. Then $\tilde U_j=\det(\Delta_j)/\det(\Delta)$ for $j=0,\dots,n_N-1$. But for $\sigma\in\Sigma$, $T_\sigma(\tilde U_j)=T_\sigma(\det(\Delta_j))/T_\sigma(\det\Delta)$. Notice that $T_\sigma(\det\Delta)=\det(\Delta^\sigma)$, where Δ^σ is identical to Δ except that the primitive root $\sigma(\gamma_0)$ replaces γ_0 throughout. Thus, Δ^σ is a row permutation of Δ and $\det(\Delta^\sigma)=s\cdot\det(\Delta)$, where s is the signature of that row permutation. But $T_\sigma(\det(\Delta_j))=\det((\Delta^\sigma)_j)$, where $(\Delta^\sigma)_j$ is just Δ^σ but with the jth column replaced by the transpose of $(T_\sigma(U_1),T_\sigma(U_{\gamma_0}),\dots,T_\sigma(U_{\gamma_0^{n_N-1}}))=(U_1,U_{\sigma(\gamma_0)},\dots,U_{\sigma(\gamma_0)^{n_N-1}})$. Hence, $\det((\Delta^\sigma)_j)=s\cdot\det(\Delta_j)$. This means that $T_\sigma(\tilde U_j)=\tilde U_j$ for all $\sigma\in\Sigma$ and $j=0,\dots,n_N-1$. Therefore, as remarked above $\tilde U_0,\dots,\tilde U_{n_N-1}\in K[x_1,\dots,x_{N-1}]$. □

Remark. A close inspection of the proof shows that we could have started the induction at $N=0$ and obtained a different proof of Proposition 3.3. To do this, we would only need to show that if $d,e\in K$ with $|d|=|e|$, then there exists $u\in K$ with $|u|=1$ such that $ud=e$. But since K is a field, this is obvious. This would eliminate the use of Lemma 3.1 here; but this lemma is needed later for other purposes.

One method of computing U given a homometric pair D and E is to find the general solution of $U(x_1,\dots,x_N)D(x_1,\dots,x_N)=E(x_1,\dots,x_N)$, and then impose the diophantine equations on the coefficients of U that make U a spectral unit.

3.4. Examples. a) Let $D, E \in Q[Z_8]$ be given by $D(x)=1+x+x^3+x^4$, $E(x)=1+x^3+x^4+x^5$ (see Fig. 2). Since $D(-1)=E(-1)=0$, there is not a unique solution U. Indeed, if $U(x)=1/2-a+ax+(1/2-a)x^2+ax^3+(1/2-a)x^4+ax^5+(-1/2-a)x^6+ax^7$, then $UD=E \bmod (x^8-1)$. When $a=0$, $1/4$, then $UU^*=1$ too.

b) Let D, $E \in Q[Z_{13}]$, $D=1+x+x^4+x^6$, $E=1+x^2+x^3+x^7$ (see Fig. 2). Then $\hat{D}$ never vanishes on $\mathscr{R}(13)$, and so there is a unique solution U to $UD=E \bmod (x^{13}-1)$. It is easy to compute $U(x)=(1/3)\ (x+x^2+x^3-x^4-x^5+x^7-x^8+x^9+x^{12})$.

3.5. Problems. a) Is there a useful presentation of the group of spectral units in terms of generators and relations?

b) Given $D \in Q[Z_n]$ with $D \geqq 0$, how does one determine all spectral units $U \in Q[Z_n]$ with $U * D \geqq 0$?

We now turn to the proof of the factorization theorem in this case. Again, the proof is by induction on N, but there does not seem to be a way to avoid the case $N=1$. This case is done in this section. The general case with $N>1$ is handled in Sect. 4 where one argument can be used for all groups.

3.6. Theorem. *If D, $E \in K[Z_n]$, then D and E are homometric if and only if there exists $\varepsilon_1, \varepsilon_2 \in \{1, -1\}$, $g_1, g_2 \in Z_n$ and $A, B \in K[Z_n]$ such that $D=\varepsilon_1\delta_{g_1} * A * B$ and $E=\varepsilon_2\delta_{g_2} * A * B^*$.*

Proof. Clearly this factorization is sufficient to make D and E homometric. Conversely, suppose D and E are homometric. Let $S=D^*+E^*$ and $T=D^*-E^*$. Then

$$S * D = D^* * D + E^* * D = E^* * E + E^* * D = E^* * S^* = (S * E)^* .$$

Let $B_1 = S * D$. Then $S * E = B_1^*$. If $\hat{S}$ is never zero, we can solve for $A_1 \in K[Z_n]$ such that $A_1 * S = \delta_0$ as in Lemma 3.3. Then $D = A_1 * B_1$ and $E = A_1 * B_1^*$. Since $\hat{S}$ might vanish, further computation is needed.

Let $B_2 = T * D$. Then $T * E = -B_2^*$ with an argument as above. Using Lemma 3.3, we can choose W_1, $W_2 \in K[Z_n]$ such that $\hat{W}_1 = 1_{\{\hat{D}+\hat{E}=0\}}$ and $\hat{W}_2 = 1_{\{\hat{D}-\hat{E}=0\}}$. Then $V_1 = (\delta_0 - W_2) * W_1$ has $\hat{V}_1 = 1_{\{\hat{D}-\hat{E}\neq 0\}\cap\{\hat{D}+\hat{E}=0\}}$. Also, $V_2 = W_1 * W_2$ has $\hat{V}_2 = 1_{\{\hat{D}+\hat{E}=0\}\cap\{\hat{D}-\hat{E}=0\}} = 1_{\{\hat{D}=\hat{E}=0\}}$. Let $V \in K[Z_n]$ be defined by $V = (\delta_0 - W_1) * S + V_1 * T * (\delta_1 - \delta_{n-1}) + V_2$. Then $\hat{V}(\gamma) = \hat{S}(\gamma) \neq 0$ if $\hat{D}(\gamma)+\hat{E}(\gamma) \neq 0$. If $\hat{D}(\gamma)+\hat{E}(\gamma)=0$ and $\hat{D}(\gamma)-\hat{E}(\gamma) \neq 0$, then $\hat{V}(\gamma) = \hat{T}(\gamma)\ (\gamma(1)-\gamma(n-1))$. If $\hat{D}(\gamma)+\hat{E}(\gamma)=0$ and $\hat{D}(\gamma)-\hat{E}(\gamma)=0$, then $\hat{V}(\gamma)=\hat{V}_2(\gamma)=1$. Hence, $\hat{V}(\gamma) \neq 0$ unless $\hat{D}(\gamma)+\hat{E}(\gamma)=0$ and $\hat{D}(\gamma)-\hat{E}(\gamma) \neq 0$ for some $\gamma \in \Gamma$ with $\gamma(1)=\gamma(n-1)=\gamma(-1)=\overline{\gamma(1)}$, i.e. $\gamma(1)=\pm 1$. Assume momentarily that $\hat{D}(\gamma)=\hat{E}(\gamma)$, when $\gamma(1)=\pm 1$ and $\hat{D}(\gamma)+\hat{E}(\gamma)=0$. Then $\hat{D}(\gamma)=\hat{E}(\gamma)=0$ for these γ and so $\hat{V}(\gamma) \neq 0$ for all $\gamma \in \Gamma$. Then because $V_2 * D = 0$ and $V_2 * E = 0$,

$$V * D = (\delta_0 - W_1) * B_1 + V_1 * (\delta_1 - \delta_{n-1}) * B_2 ,$$

and

$$V * E = (\delta_0 - W_1) * B_1^* + V_1 * (\delta_{n-1} - \delta_1) * B_2^* = (\delta_0 - W_1) * B_1^* + V_1 * (\delta_1 - \delta_{n-1})^* * B_2^* .$$

But $(\delta_0 - W_1)^* = \delta_0 - W_1$ and $V_1^* = V_1$ because $\hat{W}_1$ and $\hat{V}_1$ are real-valued. Hence, letting $B = V * D$, we have $V * E = B^*$. Since $\hat{V}$ is never zero, there exists $A \in K[Z_n]$ such that $A * V = \delta_0$. This gives $D = A * B$ and $E = A * B^*$.

Finally, we have to make adjustments to handle the possibility that for $\gamma \in \Gamma$ with $\gamma(1) = \pm 1$, we may have,

$$\hat{D}(\gamma) + \hat{E}(\gamma) = 0 \quad \text{and} \quad \hat{D}(\gamma) - \hat{E}(\gamma) \neq 0. \tag{3}$$

Let $\gamma_1, \gamma_2 \in \Gamma$ be defined by $\gamma_1(1) = 1$, $\gamma_2(1) = -1$. Suppose (3) holds for γ_1, but not for γ_2. Let $D_0 = -\delta_1 * D$. Then $\hat{D}_0(\gamma_1) = -\gamma_1(1)\hat{D}(\gamma_1) = -\hat{D}(\gamma_1) = \hat{E}(\gamma_1)$ and $\hat{D}_0(\gamma_2) = -\gamma_2(1)\hat{D}(\gamma_2) = \hat{D}(\gamma_2)$. Hence, (3) fails to hold for the pair (D_0, E) for both γ_1 and γ_2. If (3) holds for γ_2, but not for γ_1, then let $D_0 = \delta_1 * D$. We have $\hat{D}_0(\gamma_1) = \hat{D}(\gamma_1)$ while $\hat{D}_0(\gamma_2) = -\hat{D}(\gamma_2) = \hat{E}(\gamma_2)$. Hence, (3) fails to hold for (D_0, E) for γ_1 and γ_2. Lastly, if (3) holds for both γ_1 and γ_2, then let $D_0 = -D$. We have $\hat{D}_0(\gamma_1) = -\hat{D}(\gamma_1) = \hat{E}(\gamma_1)$ for $i = 1, 2$. Hence, (3) fails to hold for (D_0, E) for γ_1, and γ_2. In any of these cases D_0 and E are still homometric. The preceding argument gives $A, B \in K[Z_n]$ such $E = A * B^*$ and D is one of $\delta_{n-1} * A * B$, $-\delta_{n-1} * A * B$, or $-A * B$. □

We can map Z_n into Z_{2n} by an isomorphism φ and have $(1/2)\varphi(x) \in Z_{2n}$ for all $x \in Z_n$. If $g_1, g_2 \in Z_n$, then $\delta_{g_1} = \delta_{v_1} * \delta_{v_2}$ and $\delta_{g_2} = \delta_{v_1} * \delta_{-v_2}$, where $v_1, v_2 \in Z_{2n}$ are given by $v_1 = (g_1 + g_2)/2$ and $v_2 = (g_1 - g_2)/2$. As in Sect. 2, this allows us to improve the previous factorization in a way that is necessary for handling the case of more general finite groups.

3.7. Corollary. *If $D, E \in K[Z_n]$, then D and E are homometric if and only if there exists $\varepsilon_1, \varepsilon_2 \in \{1, -1\}$ and $A, B \in K[Z_{2n}]$ such that $D = \varepsilon_1 A * B$ and $E = \varepsilon_2 A * B^*$.*

3.8. Examples. a) Let $D, E \in Q[Z_8]$ be as in 3.4a). Then let $A = (1/4)\,(1 + x^3 + x^4 - x^7)$, $B = 3 + x - x^2 + x^3 + x^4 + x^5 + x^6 + x^7$. Then $D = A * B$ and $E = A * B^*$.

b) Let $D, E \in Q[Z_{13}]$ be as in 3.4b). Then let $A = (1/24)\,(23 - 9x - 17x^2 + 15x^3 + 7x^4 - x^5 - 9x^6 - 9x^7 + 23x^8 - x^9 - 17x^{10} - x^{11} - x^{12})$ and $B = 5 + 3x + 2x^2 + 2x^3 + 3x^4 + x^5 + 3x^6 + 2x^7 + x^8 + x^9 + 3x^{10} + 3x^{11} + 3x^{12}$. The $D = A * B$ and $E = A * B^*$.

We should remark also that the factors in Theorem 3.6 are far from unique. This was also true in Theorem 2.4, but there it was only because semi-symmetric factors of A or B could be included in either B or A. However, for finite groups, there is hardly any uniqueness properties of the factors A and B. Indeed, suppose $D = \varepsilon_1 \delta_{g_1} * A * B$, $E = \varepsilon_2 \delta_{g_2} * A * B^*$ as in Theorem 3.6. Choose a spectral unit U which has $\hat{U}(\gamma) = \pm 1$ for all $\gamma \in \Gamma$. Then $U^* = U$ and so $U^2 = U * U^* = \delta_0$. Consequently, $D = \varepsilon_1 \delta_{g_1} * (A * U) * (B * U)$ and $E = \varepsilon_2 \delta_{g_2} * (A * U) * (B * U)^*$ too. Moreover, if $F_1 \in K[G]$ and $\hat{F}_1$ is real-valued and never zero, then there exists $F_2 \in K[G]$ with $F_2 * F_1 = \delta_0$. So

$$D = \varepsilon_1 \delta_{g_1} * (A * F_2) * (B * F_1) \quad \text{and} \quad E = \varepsilon_2 \delta_{g_2} * (A * F_2) * (B * F_1)^*,$$

because $F_1^* = F_1$. It might be worthwhile here to have some theorem that would classify or relate the various possible factorizations as in Theorem 3.7 or more generally Theorem 4.1.

We have many parallels between the case of torsion-free groups and periodic groups as far as joint factorization of mutually homometric finite sets of finite distributions goes. However, a real gap in the theory is that it seems difficult to determine when $D \in Q[Z_n]$, or $D \in Q[G]$ for G finite, is uniquely retrievable.

Because of the existence of many spectral units, it seems generally not likely for $D \in Q[Z_n]$ to be uniquely retrievable. No good results have been achieved in this direction.

Of even more importance would be a restricted type of unique retrievability. With applications in X-ray spectroscopy in mind, let $D \subset G$ be a finite set. Then D is said to be *uniquely retrievable* if whenever $E \subset G$, E finite, with D and E homometric, then $D = g + E$ or $D = g - E$ for some $g \in G$. Many point sets have this property, but no general criterion for this have been found. Of course, the important variation on this theme is to determine from D, in a reasonable fashion, all $E \subset G$ which are homometric to it. Both the above problems can be phrased in the class $Z^+[G]$, G finite, which is the space of distributions of classical X-ray crystallography. This type of classification of homometric pairs is helped only theoretically by the theorems above because no effective algorithms have been developed in $Z^+[G]$ for implementing a phase retrieval procedure using the ideas in Theorems 3.2 or 3.6.

We conclude this section with a description of the classification of all sets D, $E \subset Z_n$, $n \geqq 2$, $\mathrm{card}(D) = \mathrm{card}(E) = 4$, which are non-trivially homometric. The case where $\mathrm{card}(D) \geqq 5$ seems at this time very difficult to classify. The classification below is joint work with Joel Berman. This theorem was just as easy to prove for D in the circle group, $\mathrm{card}(D) = 4$, as for the general cyclotomic case. Consequently, we state the theorem here in that context.

3.9. Theorem. *If D, E are subsets of the circle group with* $\mathrm{card}(D) = \mathrm{card}(E) = 4$, *with D and E non-trivially homometric, then D and E are one of the following two types up to rotation:*

i) *there exists r, $0 < r < 1/4$, such that $D = \delta_0 + \delta_r + \delta_{r+(1/4)} + \delta_{1/2}$ and $E = \delta_0 + \delta_{r+(1/4)} + \delta_{1/2} + \delta_{r+(1/2)}$,*

ii) $D = \delta_0 + \delta_{1/13} + \delta_{4/13} + \delta_{6/13}$ *and* $E = \delta_0 + \delta_{2/13} + \delta_{3/13} + \delta_{7/13}$.

Remark. We have used both these cases for examples in this section. We can factor case i) as in Theorem 3.6, but the presence of a parameter r makes it more suitable to discuss later in Sect. 4 (see examples 4.3a)). The proof of Theorem 3.9 is given in the appendix after Sect. 5.

4. The General Abelian Group

The results of the previous two sections show that a characterization of homometry in terms of joint factorizations occurs in the extremes of torsion-free abelian groups or finite abelian groups. Using the results Corollary 2.5 and Theorem 3.6, and a technique similar to the one in Theorem 3.2, we get the following.

4.1. Theorem. *Let G be an abelian group and suppose D, $E \in K[G]$ for some conjugation-closed field $K \subset C$. Then D and E are homometric if and only if there exists $\varepsilon_1, \varepsilon_2 \in \{1, -1\}$ and A, $B \in K[\frac{1}{2}G]$ such that*

$$D = \varepsilon_1 A * B \quad \textit{and} \quad D_2 = \varepsilon_2 A * B^* .$$

Proof. We may assume that G is finitely-generated and $G=Z^m\oplus\left(\bigoplus_{i=1}^{N} Z_{n_i}\right)$. The case $N=0$ is Corollary 2.5 and the case $m=0$, $N=1$ is Theorem 3.6. Therefore, we may need only show that if the theorem is true for the subgroup $H\subset G$, then it is also true for $H\oplus Z_n$. So let $D, E\in K[H\oplus Z_n]$ be homometric and write $D=D(x,y)$, $E=E(x,y)$ with $x\in H$, $y\in Z_n$. For each $\gamma\in\mathscr{R}(n)$, $D(x,\gamma)$ and $E(x,\gamma)$ are homometric in $K(\gamma)[H]$. By induction, there exists ε_1^γ, $\varepsilon_2^\gamma\in\{1,-1\}$ and A_γ, $B_\gamma\in K(\gamma)[\frac{1}{2}H]$ such that $D(x,\gamma)=\varepsilon_1^\gamma A_\gamma * B_\gamma$ and $E(x,\gamma)=\varepsilon_2^\gamma A_\gamma * B_\gamma^*$. Moreover, as in the proof of Theorem 3.2, we can arrange the choices of A_γ, B_γ such that $T_\sigma(A_\gamma)=A_{\sigma(\gamma)}$ and $T_\sigma(B_\gamma)=B_{\sigma(\gamma)}$ for all $\gamma\in\mathscr{R}(n)$ and Galois automorphisms σ of $K(\gamma_0)$ over K. But then, as in Theorem 3.2, there exist unique solutions $\tilde{A}_0,\ldots,\tilde{A}_{n-1}$, $\tilde{B}_0,\ldots,\tilde{B}_{n-1}\in K(\gamma_0)[\frac{1}{2}H]$ to the equations $A_\gamma(x)=\sum_{i=0}^{n-1}\tilde{A}_i(x)\gamma^i$, $B_\gamma(x)=\sum_{i=0}^{n-1}\tilde{B}_i(x)\gamma^i$ for $\gamma\in\mathscr{R}(n)$. Because of the invariance under all Galois automorphisms σ of $K(\gamma_0)$ over K, the solutions $\tilde{A}_i$, $\tilde{B}_i\in K[\frac{1}{2}H]$ for $i=0,\ldots,n-1$. Define $\mathscr{A},\mathscr{B}\in K[\frac{1}{2}H\oplus Z_n]$ by $\mathscr{A}(x,y)=\sum_{i=0}^{n-1}\tilde{A}_i(x)y^i$, $\mathscr{B}(x,y)=\sum_{i=0}^{n-1}\tilde{B}_i(x)y^i$. We also need to factor ε_1^γ, ε_2^γ. But $U_i(\gamma)=\varepsilon_i^\gamma$, $\gamma\in\mathscr{R}(n)$, defines a spectral unit in $Q[Z_n]$. Hence, by Corollary 3.7, there exists $\varepsilon_{ij}\in\{1,-1\}$, i, $j=1,2$, and $V_{ij}\in Q[\frac{1}{2}Z_n]$ such that for $i=1$, 2, $U_i=\varepsilon_{i1}V_{i1}*V_{i2}$, $\delta_0=\varepsilon_{i2}V_{i1}*V_{i2}^*$. This gives

$$D=U_1*\mathscr{A}*\mathscr{B}=\varepsilon_{11}\varepsilon_{22}V_{11}*V_{12}*V_{21}*V_{22}^**\mathscr{A}*\mathscr{B}$$

and

$$E=U_2*\mathscr{A}*\mathscr{B}^*=\varepsilon_{21}\varepsilon_{12}V_{21}*V_{22}*V_{11}*V_{12}^**\mathscr{A}*\mathscr{B}^*.$$

Let $\varepsilon_1=\varepsilon_{11}\varepsilon_{22}$, $\varepsilon_2=\varepsilon_{21}\varepsilon_{12}$. Let $A=V_{11}*V_{21}*\mathscr{A}$ and $B=V_{12}*V_{22}^**\mathscr{B}$. Then $D=\varepsilon_1 A*B$ and $E=\varepsilon_2 A*B^*$, giving the desired factorization in $K[\frac{1}{2}(H\oplus Z_n)]$. □

Remarks. a) This theorem includes the special case of G having no elements of infinite order; this is the theorem promised in Sect. 3. In Hosemann and Bagchi [24, 25], some references to private communications of Patterson indicate that he knew of the convolution method used in Sect. 2. There is no other published indication that he suspected that Theorem 4.1 might be true. Also, see Bullough [11, 12].

b) It should be noted here that the use of $\frac{1}{2}G$ in the factorization theorem is absolutely essential. Consider the example $D=(1+x)/2+(1-x)y/2$. If $x^2=y^2=1$, then D determines an element of $Q[Z_2\oplus Z_2]$ which is a spectral unit. However, the joint factorization in Theorem 4.1 cannot be achieved in $R[Z_2\oplus Z_2]$. Also, if y is not restricted and $x^2=1$, then again U and δ_0 are homometric, but the factorization cannot be done in $C[Z_2\oplus Z]$. One can also prove this generalization of Theorem 2.6.

4.2. Theorem. *If $D_1,\ldots,D_m\in K[G]$ are homometric to one another, then there exists $\varepsilon_i\in\{1,-1\}$ and $A_1,\ldots,A_n\in K[\frac{1}{2}G]$ such that $D_i=\varepsilon_i A_1^{\varepsilon_1(i)}*\ldots*A_n^{\varepsilon_n(i)}$ for some choice of $A_k^{\varepsilon_k(i)}\in\{A_k, A_k^*\}$, $k=1,\ldots,n$, depending on $i=1,\ldots,m$.*

4.3. Examples. a) Consider the parametrized sequence of pairs from Theorem 3.9, $D=\delta_0+\delta_r+\delta_{r+(1/4)}+\delta_{1/2}$, $E=\delta_0+\delta_{r+(1/4)}+\delta_{1/2}+\delta_{r+(1/2)}$. Although the parameter r can be a rational, hence making D and E cyclotomic for some possibly large degree, there is no a priori reason thatt r cannot be irrational. Hence, we can think of D and E as a homometric pair in $Q[x, y]$ with $y^4=1$ by writing $D=1+x+yx+y^2$ and $E=1+yx+y^2+y^2x$. Then following the lines of proof of Theorem 4.1 allows one to obtain a joint factorization of D and E. Indeed, one gets easily that if $A=(1/4)\ (2+3xy+xy^2+2y^2-xy^3+x)$ and $B=(1/2)\ (3-y+y^2+y^3)$, we have $D=A*B$ and $E=A*B^*$. Notice that in this example, there is even a spectral unit $U\in Q[y]$ such that $U*D=E$. An example of such U is $(1/2)(1+y+y^2-y^3)$ which is found directly using the proof of Theorem 4.1; one uses this and Theorem 3.6 to obtain the factors A and B above. If we want to specialize this to $r=1/4$ to recapture Examples 3.4a) and 3.8a), then we let $x^2=y$ and $y^4=1$. Then $U(y)=(1/2)(1+x^2+x^4-x^6)$ which is one of the spectral units in 3.4a). But the factorization of D and E in $Q[Z_8]$ has factors $A=(1/8)\ (2+x+3x^3+2x^4+x^5-x^7)$ and $B=3-x^2+x^4+x^6$. This gives $D=A*B$ and $E=A*B^*$ in a completely different fashion than 3.8a) did.

b) The way in which Patterson's Example 3.4a) occurs as a special case of a parametric family of non-trivial homometric pairs in Theorem 3.11 does not carry over to Theorem 3.11 type ii). For instance, consider $D\in Q[T]$ given additively by $D=\delta_0+\delta_r+\delta_{r+(3/13)}+\delta_{r+(5/13)}$. In polynomial form, $D=1+x+y^3x+y^5x$ with $y^{13}=1$. Theorem 3.11 shows that for any $r\neq 1/13$, D is uniquely retrievable among four point distributions in T. However, when $r=1/13$, this is no longer true because then $D=\delta_0+\delta_{1/13}+\delta_{4/13}+\delta_{6/13}$ which is homometric to $E=\delta_0+\delta_{2/13}+\delta_{3/13}+\delta_{7/13}$ modulo 1.

c) The earliest reference to non-uniqueness causing a problem for X-ray crystallography is in Pauling and Shappell [36] where the structure of bixbyite was determined. Bixbyite was found to be a solid solution of Mn_2O_3 and Fe_2O_3 by Pauling and Shappell, and others. By a study of X-ray data, the arrangement of the metal atoms was shown to have the equivalent positions provided by T_h^7 (see the international tables [49] for a reference). Further detailed work showed that the arrangement of the (Fe, Mn) pairs had to be 8(Mn, Fe) in 8*e* and 24(Mr, Fe) in 24*e* where 8*e* and 24*e* are the following distributions in the cubical unit cell:

8*e*: 1/4, 1/4, 1/4; 1/4, 3/4, 3/4; 3/4, 1/4, 3/4; 3/4, 3/4, 1/4; 3/4, 3/4, 3/4; 3/4, 1/4, 1/4; 1/4, 3/4, 1/4; 1/4, 1/4, 3/4.

24*e*: u, 0, 1/4; $-u$, 1/2, 1/4; $1/2-u$, 0, 3/4; $u+1/2$, 1/2, 3/4; 1/4, u, 0; 1/4, $-u$, 1/2; 3/4, $1/2-u$, 0; 3/4; $u+1/2$, 1/2; 0, 1/4, u; 1/2, 1/4, $-u$; 0, 3/4, $1/2-u$; 1/2, 3/4, $u+1/2$; $-u$, 0, 3/4; u, 1/2, 3/4; $u+1/2$, 0, 1/4; $1/2-u$, 1/2, 1/4; 3/4, $-u$, 0; 3/4, u, 1/2; 1/4, $u+1/2$, 0; 1/4, $1/2-u$, 1/2; 0, 3/4, $-u$; 1/2, 3/4, u; 0, 1/4, $u+1/2$; 1/2, 1/4, $1/2-u$.

Here u is a parameter with approximate value determined to be ± 0.030. However, the two choices of u give homometric distributions; only an assumption about (Mn, Fe)–O and O–O distances allowed Pauling and Shappell to determine that $u=-0.030\pm 0.005$ was the correct value of u.

First consider the distribution $24e$ by itself. We use polynomial notation with $\alpha=(1/4,0,0)$, $\beta=(0,1/4,0)$, $\gamma=(0,0,1/4)$, $x=(u,0,0)$, $y=(0,u,0)$, $z=(0,0,u)$. The distribution D is $24e$ and E is the same with (x,y,z) replaced by (x^{-1}, y^{-1}, z^{-1}). Rewriting $24e$ in polynomial notation and grouping terms gives

$$\begin{aligned}
D &= x(\gamma+\beta^2\gamma^3+\alpha^2\gamma+\alpha^2\beta^2\gamma^3)+x^{-1}(\gamma^3+\beta^2\gamma+\alpha^2\gamma^3+\alpha^2\beta^2\gamma)\\
&\quad +y(\alpha+\alpha^3\gamma^2+\alpha\beta^2+\alpha^3\beta^2\gamma^2)+y^{-1}(\alpha^3+\alpha\gamma^2+\alpha^3\beta^2+\alpha\beta^2\gamma^2)\\
&\quad +z(\beta+\alpha^2\beta^3+\beta\gamma^2+\alpha^2\beta^3\gamma^2)+z^{-1}(\beta^3+\alpha^2\beta+\beta^3\gamma^2+\alpha^2\beta\gamma^2)\\
&= x\gamma(1+\beta^2\gamma^2)(1+\alpha^2)+x^{-1}\gamma^3(1+\beta^2\gamma^2)(1+\alpha^2)\\
&\quad +y\alpha(1+\alpha^2\gamma^2)(1+\beta^2)+y^{-1}\alpha^3(1+\alpha^2\gamma^2)(1+\beta^2)\\
&\quad +z\beta(1+\alpha^2\beta^2)(1+\gamma^2)+z^{-1}\beta^3(1+\alpha^2\beta^2)(1+\gamma^2).
\end{aligned}$$

Following the method of proof of Theorem 4.1, one sees that there is a spectral unit $U\in Q[\alpha,\beta,\gamma]$ such that $UD=E$ modulo $\alpha^4=\beta^4=\gamma^4=1$. Here $U=1-(1/4)V_1$, where

$$\begin{aligned}
V_1 &= (1-\beta^2)(1+\beta^2\gamma^2)(1+\alpha^2)+(1-\gamma^2)(1+\alpha^2\gamma^2)(1+\beta^2)\\
&\quad +(1-\alpha^2)(1+\alpha^2\beta^2)(1+\gamma^2).
\end{aligned}$$

In this case, $U=W^2$ for a spectral unit W in $Q[\alpha,\beta,\gamma]$. Hence $D=W*D*W^*$ and $E=W*D*W$. After some simple computations, such a W can be found. For instance, define

$$\begin{aligned}
V_2 &= \beta(1-\beta^2)(1+\beta^2\gamma^2)(1+\alpha^2)+\gamma(1-\gamma^2)(1+\alpha^2\gamma^2)(1+\beta^2)\\
&\quad +\alpha(1-\alpha^2)(1+\alpha^2\beta^2)(1+\gamma^2),
\end{aligned}$$

and let $W=V_2+1-(1/8)U$.

Now consider the two distributions $24e$ and $8e$ together. Let D be this distribution and E be the one obtained by replacing u by $-u$. Then D and E are homometric again. Moreover, it happens that $U*D=E$ here too. Hence, with this new D and E the same factorization occurs, $D=W*D*W^*$ and $E=W*D*W$.

5. The Non-Discrete Case

Most experimental uses of diffraction of non-discrete distributions employ a distribution with an essentially continuous density of compact support in R^n. This is true in the extremes of signal analysis, spectroscopic analysis of diffuse stellar objects, and studies of changing ionic distributions via spectroelectrochemistry. The fact that the diffracting objects are often atomic in nature does not significantly enter into the diffraction in these cases. See [13, 20, 21, 31, 38, 43, 46, 47] for references to some of this literature. However, the problem of phase retrieval is equally well present here as in the use of diffraction to study finite distributions. See [2, 32, 42, 48] for background and notation concerning distributions.

5.1. Definition. If $D, E\in\mathcal{S}_c(R^n)$, the Schwartz distributions with compact support on R^n, then D and E are homometric if and only if $|\hat{D}|=|\hat{E}|$ everywhere on R^n.

As before, if $A, B \in \mathscr{S}_c(R^n)$, then $B = A * B$ and $E = A * B^*$ are homometric. The general question, yet incompletely resolved, is to what extent this factorization characterizes homometric pairs. The theorems in Sect. 2 handle this problem for finite distributions in R^n by an entirely algebraic method. However, if D and E are in $C_c^\infty(R^n)$, the smooth functions with compact support, then the methods that give at least approximate factorizations are more analytic in nature.

If $D \in \mathscr{S}_c(R)$, then $\hat{D}(x)$ can be extended to an entire function $\hat{D}(x+iy)$ such that $|\hat{D}(x+iy)| \leqq C(1+(x^2+y^2)^{1/2})^N e^{B|y|}$ for some constants C and B. If $D \in C_c^\infty(R)$, then for all $n \geqq 1$, $|\hat{D}(x+iy)| \leqq C_n(1+(x^2+y^2)^{1/2})^{-n} e^{B|y|}$ for some constants C_n and B. As observed by Walther [47], this makes $\hat{D}(z)$, $z = x+iy$, satisfy $|\hat{D}(z)| \leqq Ce^{B|z|}$ for some constants C and B. Consequently, $\hat{D}$ is an entire function of order 1 and has an infinite product factorization of a special type by Hadamard's factorization theorem (see [1, 28]). If $\hat{D}$ has a finite number of zeros $z_1, \ldots, z_N \in C\backslash\{0\}$, then

$$\hat{D}(z) = e^{\alpha_0 + \alpha_1 z} z^k \prod_{n=1}^{N} (1 - z/z_n) e^{z/z_n}.$$

Otherwise, there are infinitely many zeros $(z_n : n = 1, 2, 3, \ldots) \subset C\backslash\{0\}$, and

$$\hat{D}(z) = e^{\alpha_0 + \alpha_1 z} z^k \prod_{n=1}^{\infty} (1 - z/z_n) e^{z/z_n}. \tag{1}$$

In order to allow for multiplicities, repetitions are allowed in (z_n). By the theorem of Titchmarsh [45], see also Cartwright [16], if $D \in L_1(R)$ too, then there must be infinitely many zeros. The product representations of $\hat{D}$ converge uniformly and absolutely on compact subsets of R.

5.2. Theorem (Walther). *If $D, E \in \mathscr{S}_c(R)$, then D and E are homometric if and only if, given the expression* 1) *for $\hat{D}$, with the product possibly finite, there exists $c \in C$, $|c| = 1$, $d \in R$, and a choice $z_n^{e(n)} \in \{z_n, \bar{z}_n\}$, $n = 1, 2, 3, \ldots$, such that for all $z \in C$,*

$$\hat{E}(z) = ce^{idz} e^{\alpha_0 + \alpha_1 z} z^k \prod_{n=1}^{\infty} (1 - z/z_n^{e(n)}) e^{z/z_n^{e(n)}}.$$

Walther calls the operation in Theorem 5.1 zero-flipping. It is clear from general theory that zero-flipping on the product representation 1) always gives a new series which again determines an entire function. However, if one does a zero-flipping on $\hat{D}$ where there are infinitely many zeros, it may no longer be the case that the product represents a Fourier transform extended to C. The same ideas as above prove this result.

5.3. Theorem. *If $D, E \in \mathscr{S}_c(R)$, then D and E are homometric if and only if there exist entire functions $f_1, f_2 : C \to C$ such that $\hat{D}(z) = f_1(z) f_2(z)$ and $\hat{E}(z) = f_1(z)\overline{f_2(\bar{z})}$, for all $z \in C$.*

Instead of proving this corollary, one just proves this more general fact using the Weierstrass factorization theorem. We omit the simple proof.

5.4. Proposition. *Let g_1, g_2 be entire functions on C. Then the following are equivalent:*

1) *for all* $x \in R$, $|g_1(x)| = |g_2(x)|$,

2) *there exist entire functions* f_1, f_2 *on* C *with* $g_1(z) = f_1(z) f_2(z)$ *and* $g_2(z) = f_1(z)\overline{f_2(\bar{z})}$ *for all* $z \in C$.

5.5. Corollary. *If* $D, E \in \mathcal{S}_c(R)$ *with* D *and* E *homometric, then there exists polynomials* $p_n(z)$, $q_n(z)$ *such that* $\hat{D}(z) = \lim_{n\to\infty} p_n(z) q_n(z)$, $\hat{E}(z) = \lim_{n\to\infty} p_n(z)\overline{q_n(\bar{z})}$ *uniformly on compacta.*

Remark. This corollary justifies a phase retrieval program along the following lines. Given $|\hat{D}(x)|$ in some interval $I \subset R$, approximate $|\hat{D}(x)|$ on I by a polynomial $P(x)$. Then perform the zero-flipping procedure on the zeros of $P(x)$ in C to obtain polynomials $Q(x)$, at least one of which will approximate $\hat{D}(x)$ on I. The main difficulty in this method will be in making a reasonable choice of $P(x)$. This method and others are currently being applied to experimental situations as described in [40].

To see in more detail what effect zero-flipping has on $D \in \mathcal{S}_c(R)$, we need to know the Fourier transform of the zero-flipping $z \mapsto (z-\bar{a})/(z-a)$.

5.6. Proposition. *Let* $D \in \mathcal{S}_c(R)$ *with* $\hat{D}(a) = 0$. *Then there exists* $E \in \mathcal{S}_c(R)$ *such that* $\hat{E}(z) = (z-\bar{a})\hat{D}(z)/(z-a)$. *If* $D \in C_c^\infty(R)$ *too, then* $E \in C_c^\infty(R)$ *also.*

Proof. By the Paley-Wiener theorem, an entire function $\varphi = \hat{D}$ for some $D \in \mathcal{S}_c(R)$ if and only if $|\varphi(z)| \leqq C(1+|z|)^N e^{|\mathrm{Im}(z)|}$ for some constants B, C and some $N \in Z^+$. If $|z| \geqq 2|a|+1$, then $|z-a| \geqq (|z|+1|)/2$ and

$$\begin{aligned}|(z-\bar{a})\hat{D}(z)/(z-a)| &\leqq 2C(1+|z|)^{N-1}|z-a| e^{B|\mathrm{Im}(z)|}\\ &\leqq C_1(1+|z|)^N e^{B|\mathrm{Im}(z)|}\end{aligned}$$

for some constant C_1. Hence, $(z-\bar{a})\hat{D}(z)/(z-a)$ satisfies the growth condition needed to make it a Fourier transform $\hat{E}$ for some $E \in \mathcal{S}_c(R)$. The argument that $E \in C_c^\infty(R)$ if $D \in C_c^\infty(R)$ is similar. □

Remark. Because B does not change in the above, the smallest closed interval $[-b, b]$, $b \geqq 0$, containing the support of D, also contains the support of E. Also, as in Burge et al. [13], one can compute E in terms of D. Let $H(t)$ be the Heaviside distribution, $H(t) = 1_{[0,\infty)}(t)$, then if $a = c + id$, we have $E = D + 2d(e^{itc}e^{-dt}H(t) * D(t))$. One can prove Proposition 5.6 directly using this formula.

5.7. Example. Let $D = e\delta_{-1/2} - \delta_{1/2}$. Then $\hat{D}(i) = 0$ while $\hat{D}(-i) \neq 0$; define $\hat{E}$ by $\hat{E}(z) = (z+i)\hat{D}(z)/(z-i)$. Using the formula for E in terms of D above with $c=0$ and $d=1$, one gets E to be

$$e\delta_{-1/2}(t) - \delta_{1/2}(t) + 2i[ee^{-i(t+(1/2))} - e^{-i(t-(1/2))}]1_{(-1/2,1/2)}(t)d\lambda(t),$$

where λ is the Lebesgue measure on R. Hence, while D is a finite distribution, E is not of the same type.

The fact that zero-flipping one zero leaves $\mathcal{S}_c(R)$ invariant makes it clear that $D \in \mathcal{S}_c(R)$ is uniquely retrievable in $\mathcal{S}_c(R)$ if and only if all of the zeros of $\hat{D}$ are real.

This is a much stronger restriction than assuming that D is semi-symmetric, which only guarantees that the zeros of $\hat{D}$ occur in conjugate pairs. However, if D, $E \in \mathscr{S}_c(R)$ are semi-symmetric, then D and E are homometric if and only if there exists $c \in C$, $|c|=1$, $x \in R$, such that E is $c\delta_x * D$ or $c\delta_x * D^*$. This is readily apparent from Theorem 5.2.

One question that is unresolved here is which (if not all) sequences of zero-flippings will convert $\hat{D}$ into an $\hat{E}$ for some $E \in \mathscr{S}_c(R)$? This question is closely related to the following problem.

5.7. Problem. If D, $E \in \mathscr{S}_c(R)$ with D and E homometric, does there exist A, $B \in \mathscr{S}_c(R)$ such that $D=A*B$ and $E=A*B^*$?

On the other hand, it is clear that the factorization Theorem 4.1 does not have an analogue in $C_c^\infty(R)$. To see this, we need to construct $f \in C_c^\infty(R)$ such that the zeros of $\hat{f}$ have certain properties. By Titchmarsh [45], $\hat{f}$ always has an infinite number of zeros which are distributed with certain very regular properties. Indeed, if $\hat{f}$ had only finitely-many zeros, then $\hat{f}(z)$ would be a polynomial up to a factor $e^{\alpha_0+\alpha_1 z}$, and such an analytic function cannot satisfy $\lim_{x\to\infty} \hat{f}(x)=0$. It is easy to construct f_1, $f_2 \in C_c^\infty(R)$ with these properties:

1) $f_1 \geqq 0$, $f_1(-x)=f_1(x)$ for all $x \in R$; so $\overline{\hat{f}_1(\bar{z})}=\hat{f}_1(z)$ for $z \in C$,
2) $\hat{f}_1(x) \neq 0$ for all $x \in R$,
3) $f_2(-x)=-f_2(x)$ for all $x \in R$; so $\overline{\hat{f}_2(\bar{z})}=-\hat{f}_2(z)$ for $z \in C$,
4) $\hat{f}_2(z)=0$ implies $z \in R$.

This can also be done so that if $f=f_1+f_2$ then $f \geqq 0$. Now if $\hat{f}(z)=0$, then $0=\overline{\hat{f}(z)}=\hat{f}_1(\bar{z})-\hat{f}_2(\bar{z})$. Hence, if $x \in R$, then $\hat{f}(x)=0$ forces $\hat{f}_1(x)+\hat{f}_2(x)=0$ and $\hat{f}_1(x)-\hat{f}_2(x)=0$ which contradicts 2). But $f \geqq 0$ implies $\hat{f}(ix)=\int_{-\infty}^{\infty} e^{xy} f(y)dy>0$ for all $x \in R$. Finally, not both $\hat{f}(z)$ and $\hat{f}(\bar{z})$ can be zero at $z \in C$ because this would force $0=\hat{f}_1(z)+\hat{f}_2(z)$ and $0=\hat{f}_1(z)-\hat{f}_2(z)$. Hence, $\hat{f}_1(z)=\hat{f}_2(z)=0$ and by 4) $z \in R$, while by 2), $z \notin R$.

Given f with the properties above, choose some $a \in C$, $\hat{f}(a)=0$. Then let $g \in C_c^\infty(R)$ be defined by $\hat{g}(z)=(z-\bar{a})\hat{f}(z)/(z-a)$. By Theorem 5.2, g exists and is homometric to f. But also, suppose $f=A*B$ and $g=A*B^*$ for some $A, B \in \mathscr{S}_c(R)$. If $\hat{B}(b)=0$, $b \neq a$, then it would follow that $\hat{g}(\bar{b})=0$ while $\hat{g}(z)=0$ if and only if $\hat{f}(z)=0$ or $z=\bar{a}$. Since $\hat{f}(b)=0$ and $\hat{f}(\bar{b})=0$ is impossible, we have $b=a$ a contradiction. Hence, $\hat{B}(z)=0$ only if $z=a$. But then B cannot be integrable, let alone in $C_c^\infty(R)$.

5.8. Proposition. *There exist homometric $f, g \in C_c^\infty(R)$ such that there does not exist A, $B \in L_1(R) \cap \mathscr{S}_c(R)$ with $f=A*B$ and $g=A*B^*$.*

In conclusion, the phase retrieval problem in $\mathscr{S}_c(R^n)$ or $C_c^\infty(R^n)$, $n \geqq 2$, requires much more analysis. Because the zero sets of Fourier transforms are no longer discrete, there is no currently devised method of phase retrieval analogous to Walther's zero flipping method. One can conjecture that if $F \in \mathscr{S}_c(R^n)$. then

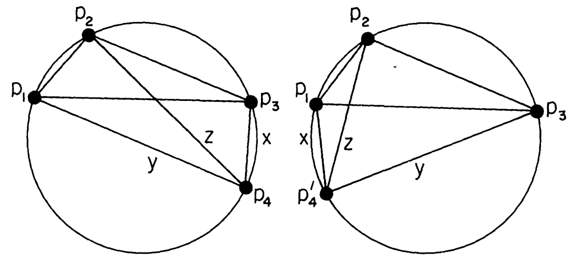


Fig. 3

$\{E \in \mathscr{S}_c(R^n) : D$ and E are homometric$\}$ is a discrete subset in the usual topology on $\mathscr{S}_c(R^n)$. But what this set is and how to describe it remains unclear.

6. Appendix

This appendix provides a proof of Theorem 3.9. We use the Patterson diagram as a conceptual tool in this classification. The classification of homometric pairs of 4 point sets will depend on the observations that when three points form a triangle with chord lengths a, b, and c, then $\mathrm{a}+\mathrm{b}=\mathrm{c}$ if the triangle does not contain the center of the circle, and $a+b+c=1$ if the triangle does contain the center. Moreover, the largest inter-point distance will be a chord nearest the center of the circle in the Patterson diagram.

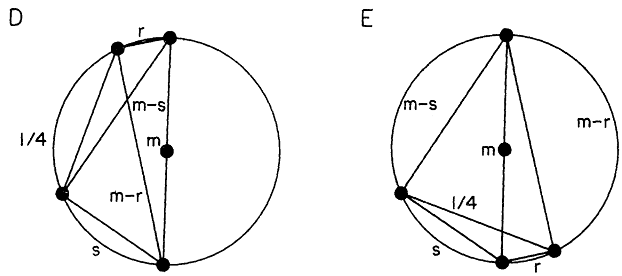
Lemma 1. *If two homometric Patterson diagrams with $k=4$ points contain three points which determine congruent triangles, and if the fourth point in both diagrams is in an arc of the circle subtended by chords of the triangles of equal length, then the diagrams are congruent.*

Proof. Let p_1, p_2, and p_3 be the three points of the triangle. Let p_4 be the fourth point in one diagram and let p_4' be the fourth point in the other. Let x, y, and z be the three lengths of chords emerging from p_4; these are the same three lengths if p_4 is replaced by p_4'. By observing where the center lies, the shortest of these lengths, say x, must be for a chord to a vertex of the subtending chord. Also, we may assume that the diagrams appear as in Fig. 3 (since the length x determines uniquely the length y). But then the distance from p_2 to p_4 is the distance from p_2 to p_4'. So the distance from p_2 to p_3 is the distance from p_2 to p_1. This means that the diagrams are reflections of one another and so they are congruent. □

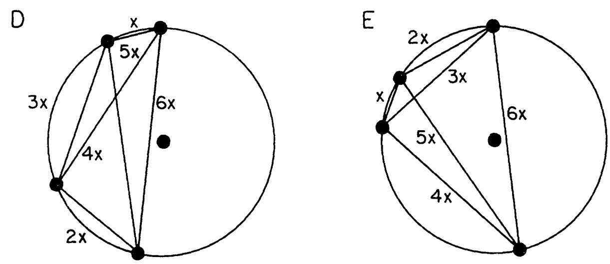
We are now ready to state and prove the theorem. Bear in mind throughout the proof of the theorem that without the various cases and subcases that we use, and our congruent triangle lemma, there would be a truly impossible number of cases to consider. We do not assume any diagrams are cyclotomic, so the lengths shown are the true lengths. Also, the center of the circle will be marked by a dot.

Theorem 3.9. *If D and E are homometric Patterson diagrams with 4 points in each, then D and E are one of the following two types:*

i) *Choose* r, $s \in (0/4)$ *with* $r+s=1/4$ *and let* $m=1/2$.



ii) *Let* $x=1/13$.



Remark. Type i) appears in Patterson, 1944 [33]. For $r=s$, there are Patterson's discovery, while Erdös pointed out the general case of i). Type ii) is new and was discovered by Edgar using a computer.

Proof of Theorem 3.9. The proof is given by looking at the individual cases. We distinguish two basic possibilities for homometric diagrams D and E. A diagram is called *outer* (*inner*) if the largest chord length m is for a chord on the boundary (in the interior) of the diagram. In Fig. 4, we illustrate the two types in standard position which can be achieved without loss of generality in this manner. For A, rotate the diagram so that m, $0<m\leqq 1/2$, is vertical (we will refer to chords by the symbol representing their length in this manner for the rest of this proof). Then reflect so that $x \leqq y$. If the center is interior, then $z=1-m-x-y$. If the center is exterior, then $z=m-x-y$. For B, rotate the diagram so that m is horizontal and above the center. Since m is longest, the lower triangle $(b, m, 1-m-b)$ contains the center. Reflect the diagram so the triangle $(a, b, a+b)$ does not contain the center, except possibly on its boundary.

At least part of our analysis proceeds by considering the shortest and second shortest chords. We give a table for these pairs in Fig. 4. Notice that for A the table uses $x \leqq y$ and the fact that neither $x+z$ nor $y+z$ can be shortest or second shortest. For B, $a+b$ is neither shortest nor second shortest and $1-m-b \geqq a$ because of the position of the center relative to the intersection of the chords m and $a+b$. Moreover, $m-a \geqq b$ since otherwise m is not largest. So this leaves only a and b for the shortest and one of $\{a, b, m-a, 1-m-b\}$ for the second shortest. Finally, we cannot have the pair $(a, m-a)$ or $(b, 1-m-b)$ as the only possible shortest and second shortest pair because in either case $m<a+b$.

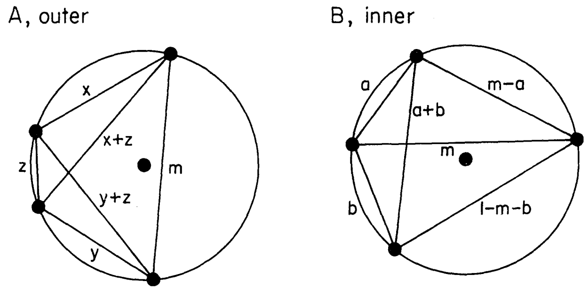


Table of pairs of shortest and second shortest chords		
	shortest chord	second shortest chord
A	x	y
	x	z
	z	x
B	a	b
	b	a
	a	1-m-b
	b	m-a

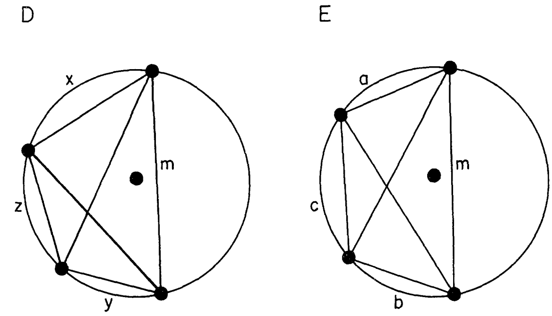
Fig. 4. The two basic types, outer and inner

Suppose now that D and E are homometric Patterson diagrams with 4 points. We have three cases to consider: Case I) D, E are outer, Case II) D, E are inner, and Case III) D is outer, E is inner. For Case III), we will have the further possibilities: Subcase a) the center is not in the interior of the convex hull of D, Subcase b) the center is in the interior of the convex hull of D. We will see that because we are assuming D and E are not congruent, we only get non-empty cases in Case I) which gives ii) and Case III) Subcase a) which gives i).

Case I. Both D and E are outer and the location of the center of the circle is otherwise unspecified. So $z=1-m-x-y$ or $z=1-x-y$. See Fig. 5 for the illustration and subcases affecting Case I). In all four cases where there are two obvious congruent triangles, Lemma 1 shows D and E would be congruent.

Case I.1. Now $a=x$ and $b=y$. To avoid congruent diagrams, one diagram must contain the center and one must not contain the center in its convex hull. Assume that the convex hull of P does not contain the center; so $z=m-x-y$ and $c=1-m-x-y$. The sets $\{z, z+x, z+y\}$ and $\{c, c+a, c+y\}=\{1-m-x-y, 1-m-y, 1-m-x\}$ are identical. Equating the smallest in these two sets gives $z=m-x-y=1-m-x-y$. So $2m=1$ and the longest chord is a diagonal; this means D and E are congruent and Case I.1) is vacuous.

Case I.2. Now $a=x$ and $c=y$. To avoid congruent triangles with chords a and m, we may suppose again that D does not contain the center and E does contain the center. Then $2m<1$ and $z=m-x-y$, $b=1-m-x-y$. Of the three remaining



Here $x \leq y$ and $a \leq b$

Table of shortest and second shortest pairs for D and E			
	(a,b)	(a,c)	(c,a)
(x,y)	Case I.1	Case I.2	Case I.3
(x,z)	symmetric to Case I.2	$\Delta(a,c,a+c) = \Delta(x,z,x+z)$	$\Delta(c,a,a+c) = \Delta(x,z,x+z)$
(z,x)	symmetric to Case I.3	$\Delta(a,c,a+c) = \Delta(z,x,x+z)$	$\Delta(c,a,a+c) = \Delta(z,x,x+z)$

Fig. 5. *D* and *E* both outer

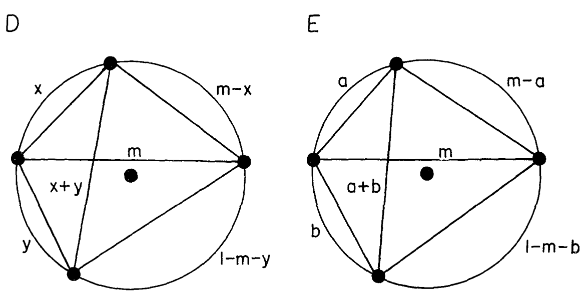


Table of shortest and second shortest pairs for D and E				
	(a,b)	(a,1-m-b)	(b,a)	(b,m-a)
(x,y)	congruent	congruent	congruent	symmetric to Case II.1
(x,1-m-y)	congruent	congruent	symmetric to Case II.2	symmetric to Case II.3
(y,x)	congruent	Case II.2	congruent	congruent
(y,m-x)	Case II.1	Case II.3	congruent	congruent

Fig. 6. Both *D* and *E* are inner

lengths in P, z, $z+x$, and $z+y=m-x$, $m-x$ must be the longest. But in E the remaining lengths are b, $b+c$, and $a+c$. Hence, $m-x=b+c=1-m-a=1-m-x$, but then $1=2m$, a contradiction.

Case I.3. Now $c=x$ and $a=y$. We may make the same initial assumptions as in Case I.2); so $z=m-x-y$, $c=1-m-a-b$. Solving for b gives $b=1-m-a-c=1-m-x-y$. The three remaining lengths in D are $\{m-x-y, m-x, m-y\}$ and in E are $\{b, b+c, a+c\}=\{1-m-x-y, 1-m-y, x+y\}$. Equating the largest in these sets gives $m-x=1-m-y$ since $b+c=1-m-y \geqq a+c=x+y$. Hence, $1=2m-x+y$. Of the remaining pair of lengths, if $1-m-x-y=m-x-y$, then $1=2m$, a contradiction. Therefore, $1-m-x-y=m-y$ and $x+1=1-x-y$. So $m=2(x+y)$ and $1=2m+x$. Since, $1=2m-x+y$, we have $-x+y=x$ and so $y=2x$. Solving for all variables in terms of x gives $1=13x$, $(x, y, z, x+z, y+z, m)=(x, 2x, 3x, 4x, 5x, 6x)$, and $(a, b, c, a+c, b+c, m)=(2x, 4x, x, 3x, 5x, 6x)$. This is ii) in the statement of the theorem.

Case II. Both D and E are inner and the center is located only to the extent that standard positions in Fig. 6 indicate. See Fig. 6 for the illustrations and subcases affecting Case II). When "congruent" is written in the table, it means that there is an obvious pair of congruent triangles to which Lemma 1 applies and that D and E would have to be congruent. Also, Lemma 1 and a simple argument show that if $2m=1$, then D and E are congruent again.

Case II.1. Now $a=y$ and $b=m-x$. The remaining lengths in D are $\{x, x+y, 1-m-y\}$ and in E are $\{m-a, a+b, 1-m-b\}=\{m-y, m-x+y, 1-2m+x\}$. Adding these lengths in D gives $1-m+2x$, while adding them in E gives 1. So $2x=m$ and, since $b=m-x$, we have $b=x$. Hence, $(a,b)=(y,x)$ and Lemma 1 proves that the diagrams are congruent.

Case II.2. Now $a=y$ and $1-m-b=x$. So $b=1-m-x$. The remaining lengths in D are $\{x+y, m-x, 1-m-y\}$ and in E are $\{b, a+b, m-a\}$. Equating the sums of these three lengths gives $1=m+2b$. But then $b=1-m-b=x$ and so $(a,b)=(x,y)$. Hence, D and E are congruent.

Case II.3. Now $a=y$ and $1-m-b=m-x$. Solving for b gives $b=1-2m+x$. The remaining three lengths to consider for D and E are $\{x, x+y, 1-m-y\}$ and $\{b, m-a, a+b\}$ respectively. Equating sums of these two sets gives $m+2b=1-m+2x$. Substituting $b=1-2m+x$ gives $1=2m$, and so D and E are congruent as we commented above.

Case III. Now D is outer and E is inner. We have to break this case into two subcases. The diagrams for D and E are as in Fig. 4 with $A=D$ and $B=E$. Note that no assumptions on whether we are in Subcase a) or b) is intended despite the illustration of $A=D$ in Fig.4.

Subcase III.a. Now the center is not interior to the convex hull of D. The five lengths for D and E, other than the longest m, are $\{x, y, z, x+z, y+z\}$ and $\{a, b, a+b, m-a, 1-m-b\}$ respectively. Equating the sums of these two sets gives $2m+z=1+a+b$. If $2m<1$, then $z>a+b$. But then z cannot be smallest or second smallest, and $x \leqq y<z<x+z \leqq y+z$. Also, $a+b$ is not smallest or second smallest, and $z>a+b$. This is impossible. Hence, we have $1=2m$ and $z=a+b$. So $a<z$ and $b<z$; consulting the table in Fig. 4, we see that since z is third largest in D, we must have $\{a,b\}$ containing the smallest and second smallest in E. But then $\{x,y\}=\{a,b\}$ and $z=x+y$. Also, $m=x+y+z$ and so $m=2(x+y)=2z$. This gives

$x+y=z=1/4$ and $m=1/2$. Also, any matching of $\{a, b\}$ with $\{x, y\}$ will give us, up to congruence, the homometric pair D and E of i) in Theorem 3.11.

Subcase III.b. Now the center is interior to the convex hull of D and so $z=1-m-x-y$, or $1-m=z+x+y$. Adding the remaining five lengths gives this formula:

$$1-m+2z+x+y=1+a+b. \tag{1}$$

Since D contains the center in the interior of its convex hull, $m>z+y\geqq z+x$ gives the three largest lengths in D. In E, the largest length after m is $m-a$, $a+b$, or $1-m-b$. Hence, we have three further subcases depending on which length is second largest in D. A consequence of 1) and $1-m=z+x+y$ is that $2(1-m)+z=1+a+b$, and so $a+b-z=2(1-m)-1=1-2m>0$. Hence, $a+b>z$. Here are the three subcases.

Subcase III.b.1. Now $z+y=m-a$. Subtract both from 1) to get $1-m+z+x=1-m+2a+b$. Hence, $z+x=2a+b$, and so $x>a$ because $a+b>z$. But since x is the smallest or second smallest in P, we have $z=a$. This means $x=a+b$, contradicting the fact that x is second shortest.

Subcase III.b.2. Now $z+y=a+b$. Subtracting from 1) gives $1-m+z+x=1$; so $z+x=m$. But $z+x<m$, a contradiction.

Subcase III.b.3. Now $z+y=1-m-b$. But also $z+y=1-m-x$. Equating these gives $1-m-b=1-m-x$. Hence, $b=x$. Now, in E the only possibilities for third largest are $a+b$ and $m-a$, and in P the only possibilities are $z+x$ and y.

Subcase III.b.3.1. If $a+b=z+x$, then $b=x$ implies $a=z$. This gives congruent triangles to which Lemma 1 applies, so D and E are congruent.

Subcase III.b.3.2. If $a+b=y$, then the final chords to match are $\{a, m-a\}$ and $\{z, x+z\}$. But $z=m-a$ together with $y=a+b$ would say $z+y=m+b>m$, a contradiction. And $z=a$ together with $b=x$ gives us congruent triangles to which Lemma 1 applies to prove D and E are congruent.

Subcase III.b.3.3. If $m-a=z+x$, then we only have to match $\{a, a+b\}$ and $\{y, z\}$. We cannot have $a+b=z$, since $a+b>z$ throughout Subcase III.b). Hence, $a=z$ and $y=a+b$. But then $a=z$ and $b=x$ gives congruent triangles to which Lemma 1 applies to show D and E are congruent.

Subcase III.b.3.4. If $m-a=y$, then we have yet to match only $\{z, x+z\}$ and $\{a, a+b\}$. Clearly, $a=z$ is the only choice. Since $b=x$, for one last time we apply Lemma 1 to prove D and E are congruent. □

See Caelli [17] where a similar problem has been studied in the plane.

Acknowledgments. I would like to thank Prof. Joel Berman, Prof. Paul Seymour, and Prof. V. Ja. Kreinovič for their help in this research.

References

1. Ahlfors, L.: Complex analysis. New York: McGraw-Hill 1966
2. Arsac, J.: Transformation de Fourier et théorie des distributions. Paris: Dunod 1961
3. Avrami, M.: A method of direct determination of crystal structure from X-ray data. Z. Kristallogr. **100**, 381–393 (1939)
4. Born, M., Wolf, L.: Principles of optics. Oxford: Pergamon Press 1970
5. Buerger, M.J.: Interpoint distances in cyclotomic sets. Can. Mineral. **16**, 301–314 (1978)

6. Buerger, M.J.: Exploration of cyclotomic point sets in tautoeikomic complementary pairs. Z. Kristallogr. **145**, 371–411 (1977)
7. Buerger, M.J.: Proofs and generalizations of Patterson's theorems on homometric complementary pairs. Z. Kristallogr. **143,** 79–98 (1976)
8. Buerger, M.J.: The algebra and geometry of convolutions. Atti. Acad. Noz. Jincei. Mem. Cl. Sci. Math. Nat. Sez. **II(8)**, 683–695 (1962)
9. Buerger, M.J.: An algebraic representation of the images of sets of points. Atti. Acad. Sci. Torino Cl. Sci. Fis. Math. Nat. **96**, 175–192 (1961/1962)
10. Buerger, M.J.: Vector sets. Acta Crystallogr. **3**, 87–97 (1950)
11. Bullough, R.K.: On homometric sets. II. Sets obtained by singular transformations. Acta Crystallogr. **17**, 295–308 (1964)
12. Bullough, R.K.: On homometric sets. I. Some general theorems. Acta Crystallogr. **14**, 257–268 (1961)
13. Burge, R.E., Fiddy, M.A., Greenway, A.H., Ross, G.: The phase problem. Proc. R. Soc. London A**350**, 191–212 (1976)
14. Caelli, T.M.: On generating spatial configurations with identical interpoint distance distributions. Comb. Math. VII, Proc., New Castle, Australia. In: Lecture Notes in Mathematics, Vol. 829. Berlin, Heidelberg, New York: Springer 1979, pp. 69–75
15. Carpenter, G.: Principles of crystal structure determination. New York: Benjamin 1969
16. Cartwright, M.L.: The zeros of certain integral functions. Q. J. Math. **1**, 38–59 (1930)
17. Champeney, D.C.: Fourier transforms and their physical applications. London: Academic Press 1973
18. Chung Chieh: Analysis of cyclotomic sets. Z. Kristallogr. **150**, 261–277 (1979)
19. Cowley, J.: Diffraction physics. New York: North-Holland 1975
20. Fowle, E.N.: The design of FM pulse compression signals. IEEE Trans. IT-**10**, 61–67 (1964)
21. Harger, R.O.: Realization of ambiguity functions. TEEE Trans. SET-**9**, 127–130 (1963)
22. Hartman, P., Winter, A.: On the maxima of the Patterson functions. Phys. Rev. **81**, 271–273 (1951)
23. Hille, E.: Analytic function theory. Vols. I, II. New York: Chelsea 1973 and 1976
24. Hosemann, R., Bagchi, S.N.: On homometric sets. Acta Crystallogr. **7**, 237–241 (1954)
25. Hosemann, R., Bagchi, S.N.: Direct analysis of diffraction by matter. New York: North-Holland 1962
26. Kline, M., Kay, I.: Electromagnetic theory and geometrical optics. New York: Wiley 1965
27. Ladd, M.F.C., Palmer, R.A.: Structure determination by X-ray crystallography. New York: Plenum Press 1977
28. Lipson, H., Cochran, W.: The determination of crystal structures. Ithaca: Cornell University Press 1966
29. McLachlan, D.: X-ray crystal structure. New York: McGraw-Hill 1957
30. Morgan, S.P.: On the mathematical question of phase reconstruction, Misc. 10, Restoration of atmospherically degraded images, Vol. 3, Woods Hole Summer Study, Nat. Acad. Sci. and NRC, pp. 53–60 (1966)
31. O'Neill, E.L., Walther, A.: The question of phase in image formation. Optica Acta **10**, 33–40 (1962)
32. Paley, R.E.A.C., Wiener, N.: Fourier transforms in the complex domain. AMS Colloquim Publ. Vol. 19. New York, 1934
33. Patterson, A.L.: Ambiguities in the X-ray analysis of crystal structure. Phys. Rev. **65**, 195–201 (1944)
34. Patterson, A.L.: Homometric structures. Nature **143**, 939–940 (1939)
35. Patterson, A.L.: A direct method for the determination of the components of interatomic distances in crystals. Z. Kristallogr. **90**, 517–542 (1935)
36. Pauling, L., Shappell, M.D.: The crystal structure of bixbyite and the *C*-modification of the sesquioxides. Z. Kristallogr. **75**, 128–142 (1930)
37. Rau, V.G. et al.: On the calculation of possible Patterson cyclotomic sets. Proc. Acad. Sci. USSR **225**, 1110–1113 (1980)

38. Readhead, A.C.S., Wilkinson, R.N.: The mapping of compact radio sources from VLBI data, Astrophys. J. **223**, 25–36 (1978)
39. Rosenblatt, J., Seymour, P.: The structure of homometric sets, SIAM J. Alg. Disc. Meth. **3**, 343–350 (1982)
40. Rossi, P., McMurdy, C.W., McCreery, R.L.: Diffractive spectroelectrochemistry; use of diffracted light for monitoring electrogenerated chromophores. J. Am. Chem. Soc. **103**, 2524–2529 (1981)
41. Rothbauer, R.: On the separation of the unknown parameters of the problem of crystal-structure analysis. Acta. Crystallogr. A **36**, 27–32 (1980)
42. Schwartz, L.: Théorie des distributions. Paris: Hermann 1966
43. Silver, S.: Microwave antenna theory and design. MIT Rad. Lab. Series, Vol. 12, pp. 279–282. New York: McGraw-Hill 1949
44. Stout, G., Jensen, L.: X-ray structure determination. London: MacMillan 1968
45. Titchmarsh, E.C.: The zeros of certain integral functions. Proc. London Math. Soc. **(2) 25**, 283–307 (1926)
46. Toraldo Di Francia, G.: Resolving power and information. J. Opt. Soc. Am. **45**, 497–501 (1955)
47. Walther, A.: The question of phase retrieval in optics. Optica Acta **10**, 41–49 (1963)
48. Wiener, N.: Generalized harmonic analysis. Acta Math. **55**, 117–258 (1930)
49. International tables for X-ray crystallography. Vol. I. Birmingham, England: The Kunech Press 1965

Communicated by B. Simon

Received October 5, 1983; in revised form May 21, 1984

Added in Proof. The answer to Problem 5.7 is negative. There exists homometric $f, g \in C_c^\infty(R)$ such that for no $A, B \in \mathscr{S}_c(R)$ is $f = A * B$ and $g = A * B^*$. This construction and the answers to other questions left unresolved in Sect. 5 are to appear in a forthcoming paper.