Acta Cryst. (1995). A51, 310–323

The Use of Higher-Order Invariants in the Determination of Generalized Patterson Cyclotomic Sets

BY F. ALBERTO GRÜNBAUM* AND CALVIN C. MOORE†

Department of Mathematics, University of California, Berkeley, CA 94720, USA

(*Received* 4 *February* 1994; *accepted* 9 *September* 1994)

Abstract

The three-dimensional configuration of crystallized structures is obtained by reading off partial information about the Fourier transform of such structures from diffraction data obtained with an X-ray source. We consider a discrete version of this problem and discuss the extent to which 'intensity only' measurements as well as 'higher-order invariants' can be used to settle the reconstruction problem. This discrete version is an extension of the study undertaken by Patterson in terms of 'cyclotomic sets', corresponding to arrangements of equal atoms that can occupy positions on a circle subdivided into N equally spaced markings. This model comes about when the usual three-dimensional Fourier transform is replaced by a one-dimensional discrete Fourier transform. The model in this paper considers molecules made up of atoms with possibly different (integer-valued) atomic numbers. It is shown that information of order six suffices to determine a structure uniquely.

1. Introduction

The phase problem is *the* problem in crystallography. It stems from the fact that diffraction peak intensity measurements give only the magnitudes and not the phases of the Fourier coefficients needed to accomplish the three-dimensional reconstruction of the molecules in the crystal exposed to the X-ray beam.

The work of Patterson (1934, 1935) represented an important step forward. With the introduction of the F^2 maps – widely known as the Patterson maps – one finally had a systematic way to attempt a reconstruction. In the period following Patterson's fundamental paper (Patterson, 1935), several workers used his method very successfully.

The first realization that different structures can correspond to the same diffraction data appears to have been by Pauling & Shappel (1930) in reference to the mineral bixbyite, whose structure had first been tentatively determined by Zachariasen (1928). In fact, even Patterson failed to notice this instance, and at one point he announced (Patterson, 1939) the result that a unique structure corresponds to a given set of intensities. Pauling quickly pointed out the problem and this got Patterson started in a long effort to determine homometric structures, *i.e.* those that correspond to the same Patterson map. For a beautiful account of this, as well as a wealth of information on the history of the subject, the reader should consult Glusker, Patterson & Rossi (1987). It is interesting to notice that from the beginning Patterson sought out the assistance of mathematicians. Beside Wiener, with whom he had several contacts in the early days of his work, his 1944 paper refers to conversations with J. Oxtoby and P. Erdös (Patterson, 1944). The book by Glusker, Patterson & Rossi (1987) contains an interesting article by Oxtoby (1987).

The study of so called homometric cyclotomic sets, *i.e.* arrangements of identical atoms on some of the Nth roots of unity, not determined by their 'diffraction pattern', was initiated by Patterson (1944) and continued by Buerger (1976), Chieh (1979) and Iglesias (1981).

A different line of attack on the determination of (strictly) homometric sets was undertaken by the mathematician Calderón and the crystallographer Pepinsky (Calderón & Pepinsky, 1952). Their work was later expanded by Franklin (1974) as well as by Bloom (1977) and Bloom & Golomb (1977). The examples that they produce are, however, of a different nature than those studied by Patterson. They correspond to 'strictly homometric structures', in the nomenclature of Franklin (1974).

The comments above deal with 'nonuniqueness' results based on 'intensity only' measurements. Now we take up the methods that are systematically used in structure determination. The difficulty of the problem is reduced by the presence of one or a few heavy atoms, and in fact most of the moderately complex structures determined up to the fifties exploited this feature. When such heavy atoms are not present, there are two ways out.

For really large molecules (beyond a few hundred atoms per unit cell), the method of choice in solving the 'phase problem' is a lot of hard chemistry work consisting of inserting such a heavy atom without altering the rest of the structure. This is known as the 'isomorphic replacement method', for which M. Perutz

* Research supported in part by NSF grant DMS91-01224 and by AFOSR contract F49620-92.

† Research supported in part by NSF grant DMS93-03386.

(and J. Kendrew) received the Nobel Prize for Chemistry in 1962. He used this method to determine the structure of hemoglobin, a molecule with around 10 000 atoms.

A different way to get around the difficulty of the missing phase information was proposed in a paper by Harker & Kasper (1948), which was further developed and expanded by the work of Karle & Hauptman (1950), as well as the contribution of Sayre (1952). This method has become very popular for molecules of up to around 200 atoms and it was the basis for the award in 1985 of the Nobel Prize for Chemistry to the chemist J. Karle and the mathematician H. Hauptman.

This method consists of using information pertaining to 'higher-order invariants' involving certain combinations of the Fourier coefficients of the unknown structure. The simplest invariant is the intensity of the radiation scattered in each direction k. If $F(k)$ denotes the (unknown) Fourier component of the structure under investigation, this intensity is given by

$$F(k)F(-k).$$

The 'higher-order invariants' alluded to above are products of the form

$$F(k_1)F(k_2)F(k_3)\ldots F(k_r), \quad k_1 + k_2 + \ldots + k_r = 0.$$

A product of this type is called an 'invariant of order r'. We take the attitude that these quantities are known. For a discussion of the way in which these quantities are 'estimated' in practice, as well as a good discussion of the probabilistic methods that form the backbone for this effort, one should consult Bricogne (1988), Giacovazzo (1992), Klug (1958) and Wilson (1949).

Although the 'direct methods' as usually implemented rely on statistical estimators for several linear combinations of phases based on the available intensity measurements, we assume here that these higher-order invariants are given to us as a full complex number. In particular, we strive to distinguish between a structure and its 'enantiomorph' (see Hauptman, 1991).

2. Main results

We pick any positive integer N and consider an arbitrary integer- (or, more generally, rational-) valued function

$$c_0, c_1, c_2, c_3 \ldots, c_{N-1}$$

defined on the equispaced markings on the unit circle obtained by its subdivision into N equal pieces (the Nth roots of unit). If the sequence c_j were to take values from the set $\{0,1\}$, we would be dealing with one of Patterson's 'cyclotomic' sets, while the case of integer-valued c_j allows us to consider arrangements of atoms with different atomic numbers. We can prove our results for arbitrary (including negative) integer-valued functions c_j. It is important to note that our 'counterexamples' to several 'stronger versions' of our results feature nonnegative functions c_j, and thus respect the physical notion of positivity.

Denote by d_k, $k = 0, 1, 2, \ldots N-1$, the (discrete) Fourier coefficients that correspond to the 'unknown structure' c_j, given by

$$d_k = \sum_{j=0}^{N-1} c_j w^{jk}, \quad w = \exp(2\pi i/N).$$

The sequence d_k is originally defined for $k = 0, 1, \ldots, N-1$. It is clear that the definition above allows one to extend d_k to a sequence defined for all integer values of the index k, and that the resulting sequence is periodic with period N. Any reference to the index k in the sequence d_k is to be interpreted 'modulo N', meaning that we always take away enough integer multiples of N to bring the quantity in question into the range $0, 1, 2, \ldots, N-1$. It is clear that the same considerations apply to the sequence c_j, which will be considered as defined for all integer j as a periodic function with period N.

Mathematically, it makes no difference if we are considering sequences c_j that are integer-valued or rational: after appropriate scaling, the second case reduces to the first one. We state our results for integer-valued sequences and, moreover, make the blanket assumption (which is physically natural) that

$$d_0 \neq 0.$$

We assume that we are given the 'rth-order invariants', *i.e.* all products of the form

$$d_{k_1} d_{k_2} d_{k_3} \ldots d_{k_r}, \quad k_1 + k_2 + \ldots + k_r = 0 (\mathrm{mod}\, N).$$

Our main result is that, if two sequences $c_j^{(1)}$ and $c_j^{(2)}$ have the same rth-order invariants for $r = 1, 2, 3, 4, 5, 6$, then one sequence is a shift of the other, *i.e.*

$$c_j^{(2)} = c_{j+a}^{(1)} \quad \text{for some fixed integer } a \text{ and all } j.$$

Of course, equality of first- and sixth-order invariants implies equality for the orders in between.

We show that this result cannot be improved since there are noncongruent structures with the same invariants of orders 1, 2, 3, 4 and 5. For instance, in the case of $N = 6$, the two sequences

$$[11, 25, 42, 45, 31, 14] \quad \text{and} \quad [10, 21, 39, 46, 35, 17]$$

of length six have the same invariants of orders 1, 2, 3, 4 and 5.

In the special case where the integer N is odd, we show that equality of invariants up to order four will suffice. These uniqueness results will, we hope, lead to practical reconstruction algorithms. Our results, which apply to integer sequences and not just to sequences of 0's and 1's, should allow one to apply these algorithms for values N that are smaller than they would be otherwise.

Among the results found below, we give a method for constructing arbitrarily large pairs of 'cyclotomic sets' that share their invariants of orders 1, 2 and 3 but represent different structures. While the case of arbitrary integer-valued sequences requires information of order six, it is possible that, in the original case considered by Patterson (c_j either 0 or 1), a structure can be uniquely determined by information of order four. A result given in the final section of this paper points in this direction. The paper includes in the final section examples on nonuniqueness in dimensions 2 and higher that go beyond simply taking Cartesian products of one-dimensional examples. We are starting work on higher-dimensional uniqueness theorems and corresponding constructive algorithms. Let us add that some of the results given here were obtained 20 years ago following conversations with D. Sayre. Our interest in the subject was reawakened by a recent conversation with Harold Shapiro.

We should point out that this general type of reconstruction problem arises in other areas as well. In these applications, the underlying group is usually a continuous group such as the real line R, and there are general results valid for all locally compact Abelian groups (see Adler & Konheim, 1962; Chazan & Weiss, 1970). The present authors have also formulated and proved results for non-Abelian groups and homogeneous spaces of these groups, but that is the topic of another paper. One general result in the Abelian case is that knowledge of rth-order invariants for all r enables one to reconstruct the original function up to a shift, and it is easy to construct examples, for each integer r, of pairs of functions that have the same invariants up to order r but where the $r + 1$ invariants differ. One does this by means of functions whose Fourier transforms are zero 'most of the time'. It is a general principle that, the more often the Fourier transforms are nonzero, the easier it is to reconstruct functions using small-order invariants. The underlying theme of this paper is that the hypothesis that our functions on these finite cyclic groups are rational (which after appropriate scaling is reduced to being integer-valued) allows us to exert some control over where the Fourier transform vanishes, and the task is to figure out how to exploit these nonvanishing properties.

3. Mathematical tools

In this section, we collect the results about the group Z_N of integers mod N (or equivalently of Nth roots of unity) that play a useful role in this paper.

Z_N is a group under addition mod N, and one can equivalently think of the multiplicative group of Nth roots of unity

$$w^j, \quad j = 0, 1, 2, \ldots, N-1, \quad w = \exp(2\pi i/N).$$

3.1. The first important observation is that Z_N can be partitioned into classes made up of roots of different 'orders'. We say that j in Z_N (or equivalently w^j with $j = 0, 1, 2, \ldots N-1$) is a 'root of order $o(j)$' if $o(j)$ is the smallest integer such that $jo(j)$ is divisible by N, explicitly

$$o(j) = N/\text{g.c.d.}(j, N).$$

It follows that the 'possible orders' are given by the divisors of N. If N is given by

$$N = p_1^{k_1} p_2^{k_2} p_3^{k_3} \ldots p_r^{k},$$

p_i different prime numbers then the 'orders' $o(j)$ are of the form

$$o = p_1^{l_1} p_2^{l_2} p_3^{l_3} \ldots p_r^{l_r}$$

with $l_i \leq k_i$, $i = 1, 2, 3, \ldots, r$.

3.2. The Nth roots of unity of a given order m constitute the roots of the so-called (monic) cyclotomic polynomial F_m. These polynomials are explicitly defined by

$$F_m(x) = \prod_{\substack{a \text{ between 1 and } m \\ \text{relatively prime to } m}} [x - \exp(2\pi i a/m)].$$

They have integer coefficients and play a fundamental role in the factorization of *any* polynomial with integer coefficients when one is interested in roots that happen to be roots of unity. In fact, we have the following important facts:

(*a*) $$x^m - 1 = \prod_{\substack{d \text{ between 1 and } m \\ \text{that divide } m}} F_d(x);$$

(*b*) each cyclotomic polynomial is irreducible over the integers (or even over the rationals).

3.3. A key fact for us in the mathematical discussions is the so-called Chinese Remainder theorem, which states that, if we are given the integers $a_1, a_2, \ldots, a_r$ and $m_1, m_2, \ldots, m_r$ and we look for an integer solution x to the system of congruencies

$$\begin{aligned} x &\equiv a_1 (\text{mod } m_1) \\ x &\equiv a_2 (\text{mod } m_2) \\ &\vdots \\ x &\equiv a_r (\text{mod } m_r), \end{aligned}$$

then there is a solution x if, and only if, for each i, j the g.c.d. of m_i, m_j divides the difference $a_i - a_j$. A particularly simple case arises when the m_i are relatively prime, since in that case there are no conditions on the a's. This is the version of the theorem proved in most books (see for instance Ireland & Rosen, 1982). For the more general version one can consult LeVeque (1956).

3.4. Given the sequence $c_0, c_1, \ldots, c_{N_1}$, define the polynomial $P(x)$ associated with c_j by

$$P(x) = \sum_{j=0}^{N-1} c_j x^j.$$

Notice that $d_k = P(w^k)$ with $w = \exp(2\pi i/N)$.

An important operation on the polynomial $P(x)$ defined above is given by

$$P^*(x) = x^{\deg P} P(1/x).$$

The sequence corresponding to P^* is (up to a shift in case that $\deg P < N - 1$) given by

$$c_{N-1}, c_{N-2}, \ldots, c_1, c_0.$$

Notice that the Fourier coefficients of the sequence associated with the polynomial $P(1/x)$ are related to those resulting from $P(x)$ by conjugation. The effect of multiplying by the power $x^{\deg P}$ is one of adding a phase factor that disappears in forming the rth-order invariants. A consequence of this is that, in the case of $r = 2$ (ordinary intensity measurements), one cannot distinguish between a structure and its 'reversed' (or reversed and shifted) image. When one considers higher-order invariants as we do here, it is in principle possible to distinguish a structure from its reversed image: the invariant is no longer real-valued and the process of reversing the structure has the effect of conjugating the invariant. To be entirely honest, one could add that in practice one estimates the real part of these invariants. As mentioned earlier, in this paper we take the attitude that the complete complex number is known.

3.5. The expressions

$$d_{k_1} d_{k_2} d_{k_3} \ldots d_{k_r} d_{-(k_1+k_2+\ldots+k_r)}$$

and

$$\sum_{l=0}^{N-1} c_{l+l_1} c_{l+l_2} c_{l+l_a} \ldots c_{l+l_r} c_l$$

are related by a multiple Fourier transform.

The special case of $r = 1$ and a sequence c_j that takes only values in $\{0,1\}$ gives the values of

$$M(l_1) = \sum_{l=0}^{N-1} c_{l+l_1} c_l,$$

the number of elements whose mutual distances are 0, 1, 2 *etc.* This justifies the name 'homometric sets' for those with the same value of $d_k d_{-k}$, $k = 0, 1, \ldots, N$. This information (second-order invariants) is directly accessible from intensity measurements. Pairs of noncongruent homometric sets have been constructed starting with the work of Patterson (see Buerger, 1976; Chieh, 1979; Franklin, 1974; Patterson, 1944). Here is a general method for constructing homometric pairs. Take two polynomials $A(x)$ and $B(x)$ and an integer s. Define $P_1(x) = A(x)B(x)$, $P_2(x) = x^s A(x)B^*(x)$. Then, the sequences that correspond to P_1 and P_2 are homometric. This goes back to Patterson, and has been used by many other authors too, as we see in §6. It is a recent result of Rosenblatt (1984) that all examples of homometric sets can be produced in this fashion.

4. Second-order invariants

The purpose of this section is to highlight examples of 'ambiguities' in the phase problem that had been discussed earlier in the literature. The examples are selected to illustrate different aspects of the problem. The first two examples give 'strictly homometric sets' (Franklin, 1974). They can be used directly on the integers, Z, or on Z_N once $N > 12$ in the first case or $N > 17$ in the second case. The third example is an example of (nonstrictly) homometric pairs and requires $N = 8$.

We start by discussing a construction proposed by Calderón & Pepinsky in (1952) and further analyzed by Franklin (1974).

Consider the polynomials P_1 and P_2 given by

$$(x^3 + x + 1)(x^9 + x^4 + 1)$$

and

$$(x^3 + x^2 + 1)(x^9 + x^4 + 1),$$

respectively. One expands them to get

$$x^{12} + x^{10} + x^9 + x^7 + x^5 + x^4 + x^3 + x + 1$$

and

$$x^{12} + x^{11} + x^9 + x^7 + x^6 + x^4 + x^3 + x^2 + 1,$$

respectively. One sees that

$$P_1(x)P_1(1/x) = P_2(x)P_2(1/x).$$

If one considers the difference sets resulting from the exponents that go along with nonzero coefficients in P_1 and P_2, respectively, namely

$$\{0, 1, 3, 4, 5, 7, 9, 10, 12\} \text{ and } \{0, 2, 3, 4, 6, 7, 9, 11, 12\},$$

one gets the same values and the same (assorted) multiplicities. Compare this to the example due to Bloom (1977), where the multiplicities will all be equal to one. In Bloom's case, the polynomials Q_1 and Q_2 are given by

$$x^{17} + x^{12} + x^{10} + x^4 + x + 1$$

and

$$x^{17} + x^{13} + x^{11} + x^8 + x + 1,$$

respectively, and can be factorized as

$$(x^6 + x + 1)(x^{11} - x^5 + x^4 + 1)$$

and

$$(x^6 + x + 1)(x^{11} + x^7 - x^6 + 1),$$

respectively.

Since the first factor is common to both Q's while the second factor is obtained by 'flipping the coefficients', we see that this example is similar to that of Calderón & Pepinsky (1952). The main difference is that in the first case one starts from two sets

$$X = \{0, 4, 9\} \quad \text{and} \quad Y = \{0, 1, 3\}$$

and forms $X + Y$ as well as $X - Y + 3$ and then considers the characteristic functions of these sets. In the case of Bloom's (1977) example, one gives up the requirement that each factor in Q_1, Q_2 should have positive coefficients. This example is interesting in that it gives a counterexample to a result of Piccard (1939), asserting that if two sets have distinct nonzero elements in their difference sets then they have to be rigid translations (or reflections) of each other.

Now we consider the example due to Patterson (1944) in a landmark paper that initiated the study of homometric sets. The polynomials R_1 and R_2 are given by

$$x^4 + x^3 + x + 1$$

and

$$x^5 + x^4 + x^3 + 1.$$

If one forms the difference

$$R_1(x)R_1(1/x) - R_2(x)R_2(1/x),$$

one obtains

$$-[(x-1)^2(x+1)^2(x^2+1)(x^4+1)/x^5].$$

Except for the factor

$$(1 - x)(x + 1)/x^5,$$

this is just the polynomial

$$x^8 - 1.$$

The consequence of this is that the difference in question vanishes at all 8th roots of unity. This is an example where the polynomials R_1 and R_2 have the same modulus only on these roots of unity and not on the entire unit circle. Franklin (1974) calls attention to this distinction when he talks about homometric and strictly homometric sets.

The polynomials R_1 and R_2 factorize over the integers as

$$(x+1)^2(x^2 - x + 1)$$
$$(x+1)(x^4 + x^2 - x + 1).$$

We see that in this case these polynomials are not obtained one from the other by 'flipping some zeros' with respect to the unit circle.

Of course, the situation changes entirely if one factorizes over the ring of integer polynomials modulo the polynomial $x^8 - 1$. The relevant factorization is given by Rosenblatt (1984) as an example of the general result that the polynomials should be related (essentially) by 'flipping one of the factors'.

5. Third-order invariants

In this section, we study some consequences of using third-order information for rational-valued sequences c_j. We give a mixture of uniqueness and nonuniqueness results depending on extra assumptions.

5.1. *Third-order invariants: N odd and d_1 nonzero*

The purpose of this section is to show that, if N is odd and d_1 does not vanish, then third-order information determines the original sequence up to a shift.

We start with the observation that the values of d_j in the class of primitive Nth roots are determined by one free quantity. Since $d_1 \neq 0$, we know that $d_j \neq 0$ on the whole set of primitive roots (see §3.3.). One can exploit the knowledge of the products

$$d_i d_j \bar{d}_{i+j}$$

to see that, if $\tilde{d}_j$ is another sequence with

$$d_i d_j \bar{d}_{i+j} = \tilde{d}_i \tilde{d}_j \bar{\tilde{d}}_{i+j}, \tag{1}$$

then we have

$$\tilde{d}_2 = (\tilde{d}_1/d_1)^2 d_2.$$

The result above depends on one crucial point: one can reach the integer 2 by adding 1 and 1. The integers used in the process, namely 1 (and 1), are such that d_j does not vanish on them and it is then possible to divide by d_1 at the end. This process can be repeated provided that one respects the rules given above: if an integer of the form $i + j$ can be obtained as the sum of integers i and j that have been reached earlier and are such that d_i and d_j are both nonzero, one can, by induction, obain an extension of the relation given above. In fact, from

$$\tilde{d}_i = (\tilde{d}_1/d_1)^i d_i$$

and

$$\tilde{d}_j = (\tilde{d}_1/d_1)^j d_j,$$

it readily follows that

$$\tilde{d}_{i+j} = (\tilde{d}_1/d_1)^{i+j} d_{i+j}.$$

It is important to notice that subtraction plays a role similar to addition here and that one can replace $i+j$ by $i-j$ in the arguments above. One just uses the fact that the sequence that has d_j as its discrete Fourier transform is real valued and thus

$$d_{-k} = \bar{d}_k$$

In view of this, we define an 'addition–subtraction chain' as a finite sequence of integers beginning with 1 and in which every member except 1 is the sum or difference of two not necessarily different previous members in the sequence.

We made the empirical observation that as long as N is odd it appeared that one could always reach any integer that is relatively prime to N by such an addition–subtraction chain starting from 1, without ever leaving the set of integers that are relatively prime to N. These empirical observations led H. Lenstra to the following result.

Theorem 1. Let N be an odd integer and let a be an integer that is relatively prime to N. Then there exists an addition–subtraction chain that ends with a and that consists of integers that are relatively prime to N.

The proof of this result is given by Lenstra (1993). Using the result above and the arguments given preceding it, we have

Theorem 2. Let d_i and $\tilde{d}_i$ be two sequences with the same third-order information. If N is odd and d_1 does not vanish, then, for any i between 1 and N,

$$\tilde{d}_i = z^i d_i \tag{2}$$

for some Nth root of unity z.

Proof. The arguments above prove the result for any i which is relatively prime to N with the choice

$$z = \tilde{d}_1/d_1.$$

Since the result in Theorem 1 can be trivially extended to $i = N$ [if g.c.d.$(j, N) = 1$ then g.c.d.$(N-j, N) = 1$ and N can be expressed as $j + (N-j)$], we see that the result is proved for $i = N$ and, since $d_N = d_0$ is real, we get that

$$z^N = 1.$$

Now any integer between 1 and N can be expressed as the sum of two integers i and j that are relatively prime to N. This is just a consequence of the result about 'multiplication of residue classes'.

Using (1) and the fact that (2) has already been established for integers that are relatively prime to N, we conclude that (2) holds for the integer $i+j$ as well. This proves the theorem. We can finally state

Theorem 3. If N is odd and d_k, $\tilde{d}_k$ are the discrete Fourier transforms of two (rational-valued) sequences $c_r, \tilde{c}_i$ with the same third-order information and $d_1 \neq 0$, then $\tilde{c}_i$ is a 'shifted' version of c_i.

Proof. Since z is an Nth root of unity, we have $z = w^j$ for some integer j. It now follows immediately that

$$\tilde{c}_i = c_{i+j} \quad \text{for all } i, \text{ with addition mod } N.$$

5.2. *Third-order invariants and* $d_1 = 0$

If the prime factorization of N contains at least two different primes but N is not equal to the product of these two distinct primes, then we can produce an example with $d_1 = 0$ such that third-order information is not sufficient to pin things down modulo a shift.

The construction is given below.

Put $N = p_1^{r_1} p_2^{r_2} \ldots p_s^{r_s}$ with $s > 1$. By assumption N/p_1 and N/p_2 are not relatively prime. We assume that each r_j above is positive. Moreover, we assume that if N is even we have $p_1 = 2$.

Denote by $F_d(x)$ the cyclotomic polynomial corresponding to a divisor d of N.

We define the polynomials $P(x)$ and $Q(x)$ by the rules:

$$\begin{aligned} P(x) &= (x^N - 1)/[(x-1)F_{N/p_1}(x)F_{N/p_2}(x)] \\ &\quad \times [F_{N/p_1}(x) + F_{N/p_2}(x)], \\ Q(x) &= (x^N - 1)/[(x-1)F_{N/p_1}(x)F_{N/p_2}(x)] \\ &\quad \times [F_{N/p_1}(x) + xF_{N/p_2}(x)]. \end{aligned}$$

There are two issues to consider. The first one is to establish that P and Q have the same 'third-order information'. The second one is to establish that P and Q are not shifts of each other. The first issue can be handled once one notices that both P and Q vanish in all but three of the 'classes' of Nth roots of unity. The second issue is dealt with by contradiction making use of the Chinese remainder theorem of §3.3.

This method of getting interesting different pairs of structures is used again in §6 to yield examples of structures that cannot even be distinguished by their correlations up to order four (an example with $N = 12$ is given) and order five (an example with $N = 30$ is given).

5.3. *N even*

The purpose of this section is to show that even if 'third-order information' is available it is possible to construct pairs of cyclotomic sets in the sense of Patterson that cannot be distinguished. For the construction below, it is important that N be even and greater than or equal to 30.

Consider the polynomials

$$p(z) = z^9 - z^3 + 1$$

and

$$q_1(z) = z^6 - z^4 + z^3 - z + 1$$
$$q_2(z) = z^6 - z^5 + z^3 - z^2 + 1,$$

whose products

$$(z^6 - z^4 + z^3 - z + 1)(z^9 - z^3 + 1)$$

and

$$(z^6 - z^5 + z^3 - z^2 + 1)(z^9 - z^3 + 1)$$

can be expanded to read

$$p(z)q_1(z) = z^{15} - z^{13} + z^{12} - z^{10} + z^7 - z + 1$$

and

$$p(z)q_2(z) = z^{15} - z^{14} + z^{12} - z^{11} + z^8 - z^2 + 1,$$

respectively. Observe that, in the notation given earlier, we have

$$q_2(z) = q_1^*(z).$$

Take now the polynomial $(z^{N/2} - 1)/(z - 1) = 1 + z + z^2 + \ldots + z^{N/2-1}$, which is deliberately chosen to vanish at all the 'even' Nth roots of unity, except for 1 itself, *i.e.*

$$w^2, w^4, w^6, \ldots, w^{N-2}, \quad \text{with } w = \exp(2\pi i/N).$$

If the polynomial above is called $r(z)$, we claim that the polynomials

$$P_1(z) = r(z)p(z)q_1(z) \quad \text{and} \quad P_2(z) = r(z)p(z)q_2(z)$$

enjoy the following properties:

(1) They both have coefficients that are either 0 or 1 as soon as $N/2 - 1$ is at least 14, *i.e.* for N equal to at least 30. This follows from the fact that $r(z)$ will have at least 15 coefficients all equal to 1, while the 'partial sums' of the coefficients in $p(z)q_1(z)$ and $p(z)q_2(z)$ are either 0 or 1, regardless of which 'end' one starts from.

(2) On every Nth root of unity (for that matter for any z of unit modulus),

$$P_1(z)P_1(1/z) = P_2(z)P_2(1/z).$$

This follows directly from the fact that $P_1(z)$ and $P_2(z)$ differ by the replacement of q_1 by $q_2 = q_1^*$.

(3) For all values of j, k, we have

$$P_1(w^j)P_1(w^k)P_1(w^{-j-k}) = P_2(w^j)P_2(w^k)P_2(w^{-j-k}).$$

This follows from the presence of the factor $r(z)$ since everything vanishes unless we have one of three circumstances:

(*a*) both w^j and w^k are 'odd' Nth roots of unity;

(*b*) one of them equals 1;

(*c*) $k + j = 0 \pmod N$.

In the first case, we have that $j + k$ is even and not equal to 1, thus the last factor is zero on both sides. In either one of the remaining cases, the relation reduces to the one established in (2) above.

(4) $P_1(z)$ and $P_2(z)$ cannot be related by a 'flip' of coefficients or a shift in the form $P_1(z) = z^R P_2(z)_N$, with R an integer, and multiplication understood modulo $z^N - 1$, or a combination of these operations.

As an example, we display the polynomials corresponding to $N = 82$, which provides an explicit example of two essentially different Patterson sets with the same third-order invariants. They have degree given by $N/2 - 1 + 15 = 55$, and are given explicitly by

$$\begin{aligned} &z^{55} + z^{54} + z^{52} + z^{51} + z^{47} + z^{46} + z^{45} + z^{44} \\ &+ z^{43} + z^{42} + z^{40} + z^{39} + z^{38} + z^{37} + z^{36} + z^{35} \\ &+ z^{34} + z^{33} + z^{32} + z^{31} + z^{30} + z^{29} + z^{28} + z^{27} \\ &+ z^{26} + z^{25} + z^{24} + z^{23} + z^{22} + z^{21} + z^{20} + z^{19} \\ &+ z^{18} + z^{17} + z^{16} + z^{15} + z^{12} + z^9 + z^8 + z^7 + 1 \end{aligned}$$

and

$$\begin{aligned} &z^{55} + z^{52} + z^{48} + z^{47} + z^{46} + z^{45} + z^{44} + z^{43} \\ &+ z^{40} + z^{39} + z^{38} + z^{37} + z^{36} + z^{35} + z^{34} + z^{33} \\ &+ z^{32} + z^{31} + z^{30} + z^{29} + z^{28} + z^{27} + z^{26} + z^{25} \\ &+ z^{24} + z^{23} + z^{22} + z^{21} + z^{20} + z^{19} + z^{18} + z^{17} \\ &+ z^{16} + z^{15} + z^{13} + z^{12} + z^{10} + z^9 + z^8 + z + 1. \end{aligned}$$

Notice that in the first case we have alternating strings of 1's and 0's of respective lengths 1, 6, 3, 2, 1, 2, 26, 1, 6, 3, 2, 1, 2, 26. Notice the repetitive character. In the second case, we have lengths given by 2, 6, 3, 1, 2, 1, 26, and their repetition 2, 6, 3, 1, 2, 1, 26. If we compare the two structures, we see (among other things) that the 'gaps of length six' are surrounded by different configurations and thus cannot be obtained by any 'rigid motion' from each other. The same argument can be seen to apply for arbitrary N, as long as it is even and large enough.

6. Fourth- and fifth-order invariants

This section is devoted to exhibiting pairs of structures with *non-negative* values for c_j that cannot be distinguished from fourth- or fifth-order invariants. In fact, we can go beyond pairs, and show sets of several indistinguishable structures as we did in §2.

We start with the case of $N = 6$ and give an example that grew out of a conversation with F. Levstein (private communication). We get two structures that cannot be discriminated from information of order up to five. We use the method of §5 in two other instances: for $N = 12$ we exhibit two structures that cannot be discriminated by information of order four, then an example is given of two structures with $N = 30$ that cannot be distinguished

even if one uses all the information of order five. In these cases, we exhibit the factorization discussed by Rosenblatt (1984).

The case $N = 6$

Consider now polynomials of the form $(x+1)(x^2+x+1)(ax^2+bx+c)$, with a, b, c arbitrary integers. This is the most general polynomial that vanishes at all the sixth roots of unity of order 2 and 3.

The choices $[a=2, b=0, c=5]$ and $[a=2, b=1, c=4]$ give, respectively, $2x^5+4x^4+9x^3+12x^2+10x+5$ and $2x^5+5x^4+10x^3+12x^2+9x+4$.

These polynomials are 'reversals' of each other but have the same information of orders 2, 3, 4, 5 and this information can distinguish (in principle) among such pairs. This example can be 'strengthened' by multiplying the two polynomials (mod x^6-1) so as to disguise the relation between the two sets. The resulting polynomials are very far from being 'related': they do not share any of their coefficients!

If we multiply these polynomials by $1+3x$, we get the pair of polynomials

$$14x^5+31x^4+45x^3+42x^2+25x+11$$

and

$$17x^5+35x^4+46x^3+39x^2+21x+10.$$

This example was mentioned in §2.

This method can be used to produce lots of sequences $[c_0, c_1, c_2, \ldots, c_5]$ with a common set of invariants of orders 2 through 5, for instance,

[25620, 30367, 104747, 174380, 169633, 95253]
[93365, 24788, 31423, 106635, 175212, 168577]
[47975, 17668, 69693, 152025, 182332, 130307]
[86575, 22107, 35532, 113425, 177893, 164468]
[69348, 17613, 48265, 130652, 182387, 151735]
[36252, 21715, 85463, 163748, 178285, 114537]
[17300, 50143, 132843, 182700, 149857, 67157].

Since no two of these numbers are the same, it is clear that the seven polynomials in question are unrelated.

We now take up the method developed in the last section and use it twice. This will show that interesting examples can be found for other values of N besides $N=6$.

Take $N = 12(= 2^2 3)$ and observe that the roots of orders 4 $(= N/3)$ and 6 $(= N/2)$ are given by {3,9} and {2,10}, respetively.

We denote, as before, with F_4 and F_6, respectively, the cyclotomic polynomials with these roots; more explicitly,

$$F_4 = x^2+1, \quad F_6 = x^2-x+1.$$

We put

$$F = (x^{12}-1)/[(x-1)F_4F_6]$$

and consider the product of this factor with either of the polynomials

$$F_6 + xF_4 \quad \text{or} \quad F_6 + F_4.$$

In the first case, we obtain

$$P(x) = x^{10}+3x^9+3x^8+x^7+x^5+2x^4 + 2x^3+2x^2+2x+1;$$

in the second case, we obtain

$$Q(x) = 2x^9+3x^8+2x^7+x^6+x^5+x^4+x^3 + 2x^2+3x+2.$$

By construction, these two polynomials are nonzero only at 12th roots of unity whose orders are 1, 4 and 6. In forming products of *four* values of these two polynomials P and Q at arguments w^k with exponents k_1, k_2, k_3, k_4 that add to 0 mod 12, we only need to restrict attention to the 4-tuples.

[0, 0, 0, 0], [0, 0, 2, 10], [0, 0, 3, 9], [2, 2, 10, 10],
[2, 3, 9, 10], [3, 3, 3, 3], [3, 3, 9, 9], [9, 9, 9, 9].

Note that the polynomials P and Q coincide except when the argument is w^k with k equal to a root of order 6, *i.e.* $k = 2, 10$. At such k, one gets P by multiplying Q by w^k. Since the integers 2 and 10 appear in the set of 4-tuples above only in the company of their complement mod 12, the products formed with P or Q coincide.

We observe that the structures that correspond to P and Q can be obtained, in the manner mentioned earlier, as the result of forming products $A * B$ and $A * B^*$, respectively.

The structure corresponding to P is obtained by convolving

$$A = \{256, -62, 73, 34, -68, -71, -44, -74, -59, 46, 64, -83\}/72$$

with

$$B = \{12, 11, 8, 7, 8, 9, 10, 11, 10, 7, 6, 9\}.$$

One obtains Q by replacing the second structure with

$$B^* = \{12, 9, 6, 7, 10, 11, 10, 9, 8, 7, 8, 11\}.$$

Observe too that the second structure has *positive* coefficients. It can be used *all by itself* to produce two structures B and B^* (reversed and shifted versions of each other), which cannot be distinguished by information of order up to and including four.

Finally, we use again the method of the last section to produce examples where information of order up to five is not enough.

Take $N = 30$ and consider the partition of Z_{30} into 'classes' made up of 30th roots of unity of orders given by the divisors $N = 30$.

We have, with $\langle o \rangle$ denoting the roots of order o,

$$\begin{aligned}
\langle 1 \rangle &= \{0\} \\
\langle 2 \rangle &= \{15\} \\
\langle 3 \rangle &= \{10, 20\} \\
\langle 5 \rangle &= \{6, 12, 18, 24\} \\
\langle 6 \rangle &= \{5, 25\} \\
\langle 10 \rangle &= \{3, 9, 21, 27\} \\
\langle 15 \rangle &= \{2, 4, 8, 14, 16, 22, 26, 28\} \\
\langle 30 \rangle &= \{1, 7, 11, 13, 17, 19, 23, 29\}.
\end{aligned}$$

The cyclotomic polynomials that vanish on the roots of orders 1, 6 and 10 are given by

$$F_1(x) = x - 1, \quad F_6(x) = x^2 - x + 1$$

and

$$F_{10}(x) = x^4 - x^3 + x^2 - x + 1,$$

respectively.

The product of the remaining cyclotomic factors is given by

$$F(x) = (x^{30} - 1)/[F_1(x)F_6(x)F_{10}(x)].$$

Since the degree of this polynomial is 23, the most general integer-coefficient polynomial that vanishes at all the roots of orders 2, 3, 5, 15 and 30 is of the form

$$(a_0 + a_1x + a_2x^2 + a_3x^3 + \ldots + a_7x^7)F(x)$$

for integer coefficients a_j.

The polynomials P_1 and P_2 to be constructed below result from choosing the first factor to be

$$F_6(x) + F_{10}(x) = x^4 - x^3 + 2x^2 - 2x + 2$$

and

$$F_6(x) + xF_{10}(x) = x^5 - x^4 + x^3 + 1,$$

respectively.

Following the recipe of Rosenblatt (1984) one gets polynomials A, B such that

$$\begin{aligned}
P_1 &= AB \\
P_2 &= AB^*
\end{aligned}$$

and one has

$$\begin{aligned}
P_1(x) = {} & x^{27} + 2x^{26} + 3x^{25} + 3x^{24} + 2x^{23} + 2x^{22} + 3x^{21} \\
& + 3x^{20} + 2x^{19} + x^{18} + 2x^{15} + 4x^{14} + 4x^{13} + 3x^{12} \\
& + 2x^{11} + x^{10} + x^9 + 2x^8 + 2x^7 + x^6 + x^5 + 2x^4 \\
& + 3x^3 + 4x^2 + 4x + 2,
\end{aligned}$$

$$\begin{aligned}
P_2(x) = {} & x^{28} + 2x^{27} + 2x^{26} + 2x^{25} + 2x^{24} + 2x^{23} + 3x^{22} \\
& + 4x^{21} + 3x^{20} + x^{19} + x^{16} + 3x^{15} + 4x^{14} + 3x^{13} \\
& + 2x^{12} + 2x^{11} + 2x^{10} + 2x^9 + 2x^8 + x^7 + x^5 \\
& + 3x^4 + 4x^3 + 4x^2 + 3x + 1.
\end{aligned}$$

In this instance, too, the coefficients of the second factor B happen to all be *non-negative*. This is important because it shows that, if one distinguishes a structure from its 'reversed version', then the polynomial B can already give rise to two different (but enantiomorphic) and physically meaningful structures. The inclusion of the extra factor A allows one (once again) to get equivalent pairs that look much more different from each other. These have the same data for orders 2, 3, 4 and 5. Note, however, that the coefficients are no longer 0's and 1's as were the examples at the end of §5.

7. The main result: sixth-order information suffices

For the convenience of the reader, we break the discussion into three parts; first the statement of the result, then a brief discussion of the overall strategy of the proof, then, in the Appendix, the details of the proof.

7.1. *The statement of the result*

Theorem 4. (1) Given N, if two rational-valued sequences $c_j^{(1)}$ and $c_j^{(2)}$, $j = 0, 1, \ldots, N-1$, with Fourier sequences given by $d_k^{(1)}$ and $d_k^{(2)}$, respectively, share the values of their rth-order invariants for $r = 1, 2, 3, 4, 5, 6$, *i.e.*

$$d_{k_1}^{(1)} d_{k_2}^{(1)} d_{k_3}^{(1)} \ldots d_{k_r}^{(1)} = d_{k_1}^{(2)} d_{k_2}^{(2)} d_{k_3}^{(2)} \ldots d_{k_r}^{(2)},$$

any time that $k_1 + k_2 + \ldots + k_r = 0 (\mathrm{mod}\, N)$ or, equivalently,

$$\sum_{j=0}^{N-1} c_j^{(1)} c_{j+j_1}^{(1)} c_{j+j_2}^{(1)} \ldots c_{j+j_p}^{(1)} = \sum_{j=0}^{N-1} c_j^{(2)} c_{j+j_1}^{(2)} c_{j+j_2}^{(2)} \ldots c_{j+j_p}^{(2)},$$

for arbitrary choice of $j_1, j_2, \ldots, j_p$ and $p = 1, 2, 3, 4, 5$, then the sequences are 'translations' of each other:

$$c_j^{(1)} = c_{j+a}^{(1)} \quad \text{for a fixed integer } a \text{ and all } j,$$

or, equivalently,

$$d_k^{(2)} = d_k^{(1)} w^{ak} \quad \text{for all } k, \text{ with } w = \exp(2\pi i/N).$$

(2) If N is odd, and if the rational sequences $c_j^{(1)}$ and $c_j^{(2)}$ have the same invariants up to order four, *i.e.* for $r = 1, 2, 3$ and 4, then one is a shift of the other.

In the language of group theory, one says that $d_k^{(2)}$ is obtained from $d_k^{(1)}$ by multiplication by the character w_a, *i.e.* the function that assigns to k the value w^{ak}. Recall that the sequences can be considered as periodic functions of the integer index j, with period N, and that addition is then considered mod N.

7.2. *The strategy of the proof*

We first decribe the strategy of the proof of part (1) of the theorem.

We want to produce a function $\lambda(k)$, defined on Z_N, which extends the ratio $d_k^{(2)}/d_k^{(1)}$ when this is well defined and satisfies $\lambda(k_1)\lambda(k_2) = \lambda(k_1 + k_2)$, or, in other words, is a character mod N. The real difficulty, as seen in the examples of the previous sections, is that these sequences can vanish for several 'classes' of Nth roots of unity.

The first step is to consider the case when $d^{(2)}$ (and hence also $d^{(1)}$) does not vanish on Z_N^*, the set of elements in Z_N of order relatively prime to N. In Lemma 1, we show how to extend the ratio $d^{(2)}/d^{(1)}$ to a character λ defined on all of Z_N in this case. Then, we consider the case when $d^{(2)}$ does not vanish on Z_M^* for Z_M contained in Z_N. The restrictions of $d^{(2)}$ and $d^{(1)}$ to Z_M are the discrete Fourier transforms on integer sequences of length M, so we can find a character λ_M on Z_M for each M such that $d^{(2)}$ does not vanish on Z_M^*. We can assume that these Z_M generate Z_N and then the problem is to piece together these λ_M's into a single character λ on Z_N. This we do using the Chinese remainder theorem as described in Lemma 2 in the Appendix. Finally, once the proof of part (1) of Theorem 4 is finished, we tackle part (2).

The details of the proof are given in the Appendix at the end of the paper.

8. Miscellaneous results and future directions

8.1. *Coefficients* 0 *and* 1

There is one additional result related to the main theorem of the previous section that should be mentioned. This brings us back to an earlier theme in the paper when the sequences c_j are sequences of 0's and 1's. In other words, we are returning to the case of Patterson's cyclotomic sets. The result says that, with a minor restriction (which may in fact be unnecessary), the equality of fourth-order invariants suffices in this case.

Theorem 5. Let $c_j^{(1)}$ and $c_j^{(2)}$, $j = 0, 1, \ldots, N-1$, be rational sequences, so that one of them is a sequence of 0's and 1's, and suppose that $d_1^{(1)} = d_1^{(2)} \neq 0$. Then, if the invariants for $r = 1, 2, 3$ and 4 for the two sequences are the same, they are shifts of each other.

We say only a few words about the proof. Of course, if N is odd, this is a special case of the second part of Theorem 4 of the previous section, so we can assume that N is even. As $d_1^{(1)} \neq 0$, we know that $d^{(1)}$ and $d^{(2)}$ do not vanish on Z_N^*, and we then use the type of argument from the proof of the second part of Theorem 4 to conclude that $\lambda(x) = d^{(2)}(x)/d^{(1)}(x)$ can be extended to a well defined function on $Z_{N/2}$ satisfying $\lambda(x)\lambda(y) = \lambda(x+y)$ if x is in $Z_{N/6}$. This produces a character on $Z_{N/6}$ which we can extend to Z_N and then, after shifting by it, we can assume $\lambda(x) = 1$ on $Z_{N/6}$. Then λ is essentially determined by its value g on the coset $1 + Z_{N/6}$ of $Z_{N/6}$. The problem is to show that $g^6 = 1$ so that λ would be a character. One may show that if $d^{(2)}(x)$ is nonzero anywhere in the three cosets $2 + Z_{N/6}$, $3 + Z_{N/6}$ and $4 + Z_{N/6}$, then $g^6 = 1$ follows by equality of fourth-order invariants. Hence, we can assume that $d^{(1)}(x) = d^{(2)}(x) = 0$ on these three cosets. This implies that the polynomials

$$P^{(i)}(w) = \sum c_j^{(i)} w^j$$

are divisible by the polynomials that define these three cosets. Then we use the fact that one of these polynomials, say $P^{(1)}$, has coefficients that are 0's and 1's, and an explicit calculation shows that $d^{(1)}$ must also vanish in the cosets $Z_{N/6}$ and $5 + Z_{N/6}$, which contradicts the assumptions. This completes the proof.

8.2. *Real-valued coefficients*

In this very short section, we see the effect of allowing real-valued coefficients c_j. For an arbitrary but fixed *odd* N, consider a sequence whose Fourier coefficients d_k satisfy the following:

$$d_0 = 1 \quad d_1 = d_{-1} = b, \quad d_k = 0, \quad \text{for all other } k.$$

This means that c_j is given by

$$c_j = d_0 + 2b \cos 2\pi/N_j.$$

Consider now the value of any rth-order invariant

$$d_{k_1} d_{k_2} d_{k_3} \ldots d_{k_r}$$

with $k_1 + k_2 + \ldots + k_r = 0$. The value of this product will be zero unless the indices are restricted to lie in the set $\{0, 1, -1\}$. Take r as small relative to N and notice that the fact that the sum of the indices is zero forces the number of indices that are equal to 1 to balance those that are equal to -1. This has the effect that we can only read off the value of the quantity b^2, and not that of b itself. Of course, once r is large enough, say N, we can reach 0 by adding together N times the index 1, *i.e.* Nth-order invariants will distinguish (if N is odd) between a configuration and the one obtained by exchanging b into $-b$.

Denoting by d_k the sequence defined above and with $\tilde{d}_k$ the sequence (of Fourier coefficients) resulting from a change of b into $-b$, we consider the possibility that an integer a might exist such that, for all $k = 1, 2, \ldots, N$, we have

$$\tilde{d}_k = d_k w^{ak}, \quad w = \exp(2\pi i/N).$$

For $k = 1$, we get that $a = N/2$, which is impossible if N is odd.

This shows that, once we admit real-valued coefficients c_j, it is impossible to produce a value of r (independent of N) such that the invariants of order less than or equal to r determine a sequence up to a shift. This

fits within a general theory for Abelian groups as given by Adler & Konheim (1962).

8.3. We are presently trying to convert several of the 'uniqueness results' proved in this paper under different restrictions into constructive algorithms that could prove applicable. At the same time, we are exploring the two- and three-dimensional versions of our results and of their 'constructive counterparts'. We close this section with the display of two entirely different structures in $Z_6 \times Z_6$, which have the same invariants of orders 2, 3, 4 and 5. One can also produce these examples in dimension three.

We display the value of c_{ij}, $0 \le i, j \le 5$. The first structure is given by

$$\begin{bmatrix} 729 & 872 & 495 & 587 & 608 & 571 \\ 803 & 558 & 687 & 565 & 579 & 653 \\ 511 & 632 & 601 & 624 & 596 & 631 \\ 477 & 680 & 661 & 615 & 528 & 401 \\ 723 & 653 & 691 & 597 & 338 & 377 \\ 608 & 748 & 769 & 385 & 432 & 687 \end{bmatrix}$$

and the second one by

$$\begin{bmatrix} 740 & 863 & 471 & 552 & 625 & 576 \\ 832 & 553 & 677 & 568 & 573 & 671 \\ 530 & 657 & 587 & 613 & 603 & 669 \\ 512 & 663 & 656 & 604 & 537 & 425 \\ 720 & 659 & 673 & 568 & 343 & 387 \\ 619 & 741 & 731 & 366 & 407 & 701 \end{bmatrix}.$$

One could, of course, just take Cartesian products of the one-dimensional examples we have already produced, but these would not be intrinsically multidimensional examples. However, the examples we present here are not just products of one-dimensional examples.

APPENDIX
The details of the proof

The proof [of part (1)] depends on two lemmas. In the first, we initially assume that M is even. At the end of the proof, we indicate how to deal with the (simpler) case of M odd. Although the statement of the lemma is independent of the parity of M, the proof is different in the two cases.

We adopt the following notation: $d_k^{(2)} = f(k)$, $d_k^{(1)} = g(k)$, $Z_{M/2}$ = the subgroup of Z_M made up of all the even integers in Z_M, *i.e.* $\{0, 2, 4, \ldots\}$. For any M, Z_M^* denotes the set of 'primitive roots' in Z_M, *i.e.* those of order M. From the observations in §3, for M odd we have $Z_M^* + Z_M^* = Z_M$; for M even, we have $Z_M^* + Z_M^* = Z_{M/2}$. This difference accounts for the separate treatment of the cases M odd and M even.

Lemma 1. Assume that f and g are nonzero on Z_M^*. Then the quotient $f(k)/g(k)$, defined on Z_M^* and on all elements of Z_M where $g(k)$ [and thus $f(k)$] does not vanish, can be extended to a character λ defined on the entire group Z_M. There exists an a such that

$$\lambda(k) = w^{ak}$$

with

$$w = \exp(2\pi i/M), \quad k = 0, 1, 2, \ldots, M-1.$$

Proof (M *even*). On Z_M^* we define λ as the ratio f/g. Observe that in Z_M^* λ has the 'additive property', *i.e.* for k_1, k_2, $k_1 + k_2$ in Z_M^*,

$$\lambda(k_1)\lambda(k_2) = \lambda(k_1 + k_2).$$

By definition, this amounts to showing that

$$f(k_1)f(k_2)/f(k_1 + k_2) = g(k_1)g(k_2)/g(k_1 + k_2).$$

Observe that all these operations are legitimate since f and g are nonzero for all the arguments involved.

Now from the fact that $f(-k) = f^*(k) = [1/f(k)][f(k)f^*(k)]$ and the identity of the second-order invariants for f and g, namely

$$f(k)f(-k) = f(k)f^*(k) = g(k)g^*(k) = g(k)g(-k),$$

it follows that we have to prove

$$f(k_1)f(k_2)f(-k_1 - k_2) = g(k_1)g(k_2)g(-k_1 - k_2),$$

which is valid since we have assumed that third-order invariants coincide. We now use the fact that $Z_{M/2} = Z_M^* + Z_M^*$ to define λ on $Z_{M/2}$ by the rule: if z in $Z_{M/2}$ is given by $z = x + y$, with x, y in Z_M^*, then we put $\lambda(z) = \lambda(x)\lambda(y) = [f(x)/g(x)][f(y)/g(y)]$.

We have to show three different things: (i) that λ is well defined; (ii) that it really extends to $Z_{M/2}$ the values of the ratio f/g for those values of the argument when the ratio is well defined (f and g nonvanishing); and (iii) that the 'additive property' carries over to λ defined now on $Z_{M/2}$.

(i) If z in $Z_{M/2}$ can be written as $z = x_1 + y_1 = x_2 + y_2$ with x_1, x_2, y_1, y_2 in Z_M^*, we need to see that

$$[f(x_1)/g(x_1)][f(y_1)/g(y_1)] = [f(x_2)/g(x_2)][f(y_2)/g(y_2)].$$

Notice, once again, that f and g are nonzero at all the arguments involved. With the same relations that were used earlier, this is equivalent to showing

$$f(x_1)f(y_1)f(-x_2)f(-y_2) = g(x_1)g(y_1)g(-x_2)g(-y_2),$$

which is true because $x_1 + y_1 - x_2 - y_2 = 0$ by assumption and because fourth-order invariants agree.

(ii) Suppose now that z in $Z_{M/2}$ is such that $f(z)$ [and $g(z)$] is nonzero and that $z = x + y$ with x, y in Z_M^*. We need to show that

$$\lambda(z) = [f(x)/g(x)][f(y)/g(y)] = f(z)/g(z).$$

But this amounts to showing that

$$f(x)f(y)f(-x-y) = g(x)g(y)g(-x-y),$$

which is true by the identity of third-order invariants.

(iii) Finally, suppose that an element of $Z_{M/2}$, z_1, can be written as the sum of two other elements in $Z_{M/2}$, z_2 and z_3. We then have

$$z_1 = x_1 + y_1, \quad z_2 = x_2 + y_2, \quad z_3 = x_3 + y_3,$$

with all x_i and y_i in Z_M^*, and we need to show that

$$\lambda(z_1) = \lambda(z_2 + z_3) = \lambda(z_2)\lambda(z_3).$$

The left-hand side is

$$[f(x_1)/g(x_1)][f(y_1)/g(y_1)]$$

and the right-hand side is

$$[f(x_2)/g(x_2)][f(y_2)/g(y_2)][f(x_3)/g(x_3)][f(y_3)/g(y_3)].$$

The desired identity follows from

$$f(x_1)f(y_1)f(-x_2)f(-y_2)f(-x_3)f(-y_3) = g(x_1)g(y_1)g(-x_2)g(-y_2)g(-x_3)g(-y_3),$$

which holds because $x_1 + y_1 - x_2 - y_2 - x_3 - y_3 = 0$ and we have assumed that the sixth-order invariants coincide.

Thus far, we have shown that $\lambda(k)$ defined for all k in $Z_{M/2}$ (*i.e.* all even k, $k = 0, 2, 4, \ldots$) is well defined, agrees with the value of $f(k)/g(k)$ when this makes sense and satisfies the additivity property.

From the last property, it follows that for any k we have

$$\lambda(2k) = \lambda(2)^k.$$

Since we have $\lambda(0) = 1$ {$0 = x - y$ with x in Z_M^* implies $\lambda(0) = [f(x)/g(x)][f(-x)/g(-x)]$ and this is 1 by the identity of the second-order invariants}, we conclude that

$$\lambda(0) = \lambda(M) = \lambda(2)^{M/2} = 1$$

and, therefore, $\lambda(2)$ is an $(M/2)$th root of unity, *i.e.* $\lambda(2) = w^{2a}$ for some integer a and $w = \exp(2\pi i/M)$.

In summary, we have seen that for all k the values of $f(2k)$ and $g(2k)$ are related as follows:

$$f(2k) = g(2k)\lambda(2k) = g(2k)w^{a2k}.$$

we now define λ on the remaining values of k, *i.e.* odd k, according to

$$\lambda(2k+1) = \lambda(2k)\lambda(1).$$

Recall that $\lambda(1) = f(1)/g(1)$.

We have to show that this definition (i) makes sense, *i.e.* it should agree with the values of λ as previously defined on Z_M^*, (ii) agrees with the value of the ratio $f(k)/g(k)$ when this is well defined and (iii) has the 'additive property' on the whole of z_M.

(i) This follows from $\lambda(0) = 1$.

(ii) If $f(2k+1)$ and $g(2k+1)$ are nonzero, we should check that

$$\lambda(2k+1) = \lambda(k_1 + k_2)\lambda(1) = f(2k+1)/g(2k_1).$$

In the expression above, k_1 and k_2 are Z_M^* and such that $k_1 + k_2 = 2k$. Therefore, we have to show that

$$[f(k_1)/g(k_1)][f(k_2)/g(k_2)][f(1)g(1)] = f(k_1 + k_2 + 1)/g(k_1 + k_2 + 1),$$

which follows once again on the basis of identity of fourth-order invariants.

(iii) As to the additive property of λ on the whole of Z_M, if both arguments are even, *i.e.* in $Z_{M/2}$, this has been checked earlier. If one argument is even and one odd, we get

$$\begin{aligned}\lambda(2k_1)\lambda(2k_2+1) &= \lambda(2k_1)\lambda(2k_2)\lambda(1)\\ &= \lambda[2(k_1+k_2)]\lambda(1)\\ &= \lambda[2(k_1+k_2)+1].\end{aligned}$$

Finally, if both arguments are odd, we have to see that

$$\begin{aligned}\lambda(2k_1+1)(2k_2+1) &= \lambda(2k_1)\lambda(1)\lambda(2k_2)\lambda(1)\\ &= \lambda[2(k_1+k_2)+2].\end{aligned}$$

Observe that the last term is $w^{a2(k_1+k_2+1)}$, while the middle term is $w^{a2(k_1+k_2)}[\lambda(1)]^2$. The identity in question results from the fact that

$$\lambda(1) = w^a \quad \text{or} \quad -w^a,$$

a fact that follows from $\lambda(2) = \lambda(1)^2 = w^{2a}$.

In conclusion, λ has been defined on the whole of Z_M, it extends the values of the ratio f/g when this is well defined and it has the additive property. Reasoning as before, we see that, for any k in $\{0, 1, 2, 3, \ldots, M-1\}$,

$$\lambda(k) = \lambda(1)^k.$$

From $\lambda(1)^M = \lambda(M) = \lambda(0) = 1$, we conclude that $\lambda(1) = w^b$ for some integer b. More is already known, b can be taken to be either equal to a or to $a + M/2$ [which amounts to a change in the sign of $\lambda(1)$]. For simplicity, we denote the integer b by a, and we have thus shown that, for all k,

$$f(k) = g(k)w^{ak}.$$

This concludes the proof of the lemma in the case of M even.

For M odd, we define λ first on Z_M^* as before. We then extend it to the whole of Z_M by the rule: if $z = x + y$ with z, y in Z_M^*, then $\lambda(z) = \lambda(x)\lambda(y)$.

The same arguments given earlier can be used to show that this function is well defined, extends the ratio f/g when this makes sense and enjoys the additivity property. We are now finished with the proof of Lemma 1.

We now turn to the general case when f and g may vanish on Z_N^*. We make a list of all the subgroups Z_M of Z_N such that f (and hence also g) do not vanish on Z_M^*. Let these be $Z_{M(1)}, Z_{M(2)}, \ldots, Z_{M(k)}$. One easily argues that these subgroups must generate all of Z_N for otherwise all considerations can be restricted to the subgroup of Z_N so generated. This means that $N = \text{l.c.m.}[M(1), M(2), \ldots, M(k)]$.

Lemma 1 above will produce a character $\lambda_{M(i)}$ on each $Z_{M(i)}$, which extends the function f/g wherever it is defined on $Z_{M(i)}$. If we are fortunate enough that some $Z_{M(i)} = Z_N$, we are done, but in general we are not so fortunate and the next step is to show that these characters $\lambda_{M(i)}$ defined on $Z_{M(i)}$ fit together to give us a character $\lambda = \lambda_N$ on Z so that $\lambda_{M(i)} = \lambda_N$ on $Z_{M(i)}$. This will do the trick. The tool we use here is the Chinese remainder theorem that was reviewed in §3.3. Specifically, we have Lemma 2.

Lemma 2. If $\lambda_{M(i)}$ is a character on $Z_{M(i)}$ with $N = \text{l.c.m.}[M(1), M(2), \ldots, M(k)]$ then there is a character λ on Z_N with $\lambda_{M(i)} = \lambda$ on $M(i)$ if and only if $\lambda_{M(i)} = \lambda_{M(j)}$ on $Z_{M(i)} \cap Z_{M(j)}$ $(\equiv Z_{gcd[M(i),M(j)]})$ for each pair i, j.

Proof. This is literal transcription of the Chinese remainder theorem. The set of characters of Z_N is a cyclic group of order N and can be identified with the residues mod N. Thus, each $\lambda_{M(i)}$ is a residue $r_i \bmod M(i)$ and the hypothesis of the lemma translates into $r_i = r_j \bmod \text{g.c.d.}[M(i), M(j)]$. The desired character λ of Z_N is a residue mod N that is congruent to $r_i \bmod M(i)$. That such a residue exists is ensured by the Chinese remainder theorem. Conversely, the hypothesis of the lemma is clearly necessary for the existence of such a λ.

In order to complete the proof, we need to check that $\lambda_{M(i)} = \lambda_{M(j)}$ on $Z_{M(i)} \cap Z_{M(j)}$. If x is in this intersection, then x is the sum of either two or three elements in $Z_{M(i)}$ and $Z_{M(j)}$ so $x = k_1 + k_2(+k_3) = j_1 + j_2(+j_3)$, with k_s in $Z_{M(i)}^*$ and j_t in $Z_{M(j)}^*$, where the final summand may or may not be needed. Then the relation $\lambda_{M(i)}(x) = \lambda_{M(j)}(x)$ follows from equality of sixth-order invariants [or fourth- or fifth-order ones if only two elements in $M(i)$ or $m(j)$ are required].

The proof of part (1) is now complete, and we turn to the proof of part (2) of the theorem. In the case of N odd, we can, by being a little more careful, do somewhat better and establish the result using only invariants up to fourth order as stated in the theorem. If we examine the argument above carefully, we see that the only place invariants above fourth order were used was in establishing the additivity property in the case when $d^{(2)}$ is nonvanishing on Z_N^*. That is, we need to know that

$$\lambda(x_1)\lambda(x_2)\lambda(y_1)\lambda(y_2) = \lambda(z_1)\lambda(z_2), \tag{3}$$

when x_i, y_i and z_i are in Z_N^* and $x_1 + x_2 + y_1 + y_2 = z_1 + z_2$.

This follows immediately from equality of sixth-order invariants; equality of fourth-order invariants tells us that $\lambda(u_1)\lambda(u_2) = \lambda(v_1)\lambda(v_2)$ if u_i, v_i are in Z_N^* and $u_1 + u_2 = v_1 + v_2$. But suppose in (3) that we could find an element u in Z_N such that $y_1 + u$, $y_2 - u$ and $x_1 + x_2 + y_1 + u$ are in Z_N^*. Then, from equality of fourth-order invariants, we conclude that

$$\lambda(y_1)\lambda(y_2) = \lambda(y_1 + u)\lambda(y_2 - u),$$

$$\lambda(x_1)\lambda(x_2)\lambda(y_1 + u) = \lambda(x_1 + x_2 + y_1 + u)$$

and

$$\lambda(x_1 + x_2 + y_1 + u)\lambda(y_2 - u) = \lambda(z_1)\lambda(z_2).$$

Evidently, (3) follows from combining these three equations.

Now we have to find a u satisfying the three conditions above. The group Z_N has one maximal subgroup for each prime p dividing N, namely the cyclic group $Z_{N/p}$. Evidently, an element u of Z_N is in Z_N^* if and only if it is not in any of these maximal subgroups $Z_{N/p(i)}$ for each of the primes $p(i)$ dividing N. The three conditions on u above simply mean that, for each $p(i)$, u must not lie in three cosets of Z. Hence, if $p(i) \neq 3$, we can always select an element u meeting these conditions at $p(i)$ and, therefore, if 3 does not divide N, we can always find a u. This completes the proof in this case.

If $p = 3$, suppose that $x_1 + x_2$ is in $Z_{N/3}$. Then, the initial condition on u coincides with the first and we can select a u meeting the conditions. It follows that

$$\lambda(x)\lambda(y) = \lambda(x + y)$$

if x is in $Z_{N/3}$. In particular, λ is a character on $Z_{N/3}$ and as such it can be extended to a character on all of Z_N, say λ. Let us shift one of the original sequences by λ' and relabel them $c^{(1)}$ and $c^{(2)}$. Then, the new $\lambda(x) = d^{(2)}(x)/d^{(1)}(x)$ must satisfy $\lambda(x)\lambda(y) = \lambda(x + y)$ if x is in $Z_{N/3}$ and $\lambda(x) = 1$ if x is in $Z_{N/3}$. This means that λ is a constant on the cosets of $z_{N/3}$ and equality of fourth-order invariants easily implies that is a character. This completes the proof.

References

ADLER, R. & KONHEM, A. (1962). *Proc. Am. Math. Soc.* **13**, 425–428.

BLOOM, G. (1977). *J. Comb. Theory A*, **22**, 378–379.

BLOOM, G. & GOLOMB, S. (1977). *Proc. IEEE*, **65**, No. 4, 562–570.

BRICOGNE, G. (1988). *Acta Cryst.* A**44**, 517–545.

BUERGER, M. (1976). *Z. Kristallogr.* **143**, 79–98.

CALDERÓN, A. & PEPINSKY, R. (1952). *Computing Methods and the Phase Problem in X-ray Crystal Analyis*, pp. 319–338. Pennsylvania State College, College Park, PA, USA.

CHAZAN, D. & WEISS, B. (1970). *Inf. Control*, **16**, 378–383.

CHIEH, C. (1979). *Z. Kristallogr.* **150**, 261–277.

FRANKLIN, J. (1974). *Acta Cryst.* A**30**, 698–702.

GIACOVAZZO, C. (1992). *Fundamentals of Crystallography*. IUCr/ Oxford Science Publications.

GLUSKER, J., PATTERSON, B. & ROSSI, M. (1987). *Patterson and Pattersons. Fifty Years of the Patterson Function*. IUCr/Oxford Univ. Press.
HARKER, D. & KASPER, J. S. (1948). *Acta Cryst.* **1**, 70–75.
HAUPTMAN, H. (1991). *Rep. Prog. Phys.* **54**, 1427–1454.
IGLESIAS, J. (1981). *Z. Kristallogr.* **156**, 187–196.
IRELAND, K. & ROSEN, M. (1982). *A Classical Introduction to Modern Number Theory*. New York/Heidelberg/Berlin: Springer-Verlag.
KARLE, J. & HAUPTMAN, H. (1950). *Acta Cryst.* **3**, 181–187.
KLUG, A. (1958). *Acta Cryst.* **11**, 515–543.
LENSTRA, H. W. (1993). *Acta Arith.* **64**, 383–388.
LEVEQUE, W. J. (1956). *Topics in Number Theory*. Reading, MA: Addison-Wesley.
OXTOBY, J. (1987). In *Patterson and Pattersons. Fifty Years of the Patterson Function*, edited by J. GLUSKER, B. PATTERSON & M. ROSSI. IUCr/Oxford Univ. Press.
PATTERSON, L. (1934). *Phys. Rev.* **46**, 372–376.
PATTERSON, L. (1935). *Z. Kristallogr.* **90**, 517–542.
PATTERSON, L. (1939). *Phys. Rev.* **15**, 682.
PATTERSON, L. (1944). *Phys. Rev.* **65**, 195–201.
PAULING, L. & SHAPPEL, M. (1930). *Z. Kristallogr.* **75**, 128–142.
PICCARD, S. (1939). *Mem. Univ. Neuchâtel*, No. 13. Paris: Librairie Gauthier-Villars.
ROSENBLATT, J. (1984). *Commun. Math. Phys.* **95**, 317–343.
SAYRE, D. (1952). *Acta Cryst.* **5**, 60–65.
WILSON, A. (1949). *Acta Cryst.* **2**, 318–321.
ZACHARIASEN, W. (1928). *Z. Kristallogr.* **67**, 455–464.

Acta Cryst. (1995). A**51**, 323–328

Theoretical *Ab Initio* Calculations of the Structure Factors of Fluorite (CaF_2)

BY ALBERT LICHANOT AND MICHEL RÉRAT

Laboratoire de Chimie Structurale URA 474, *Université de Pau, IFR, rue J. Ferry*, 64000 *Pau, France*

AND MICHELE CATTI

Dipartimento di Chimica Fisica ed Elettrochimica, Università di Milano, via Golgi 19, *I*-20133 *Milano, Italy*

(*Received* 25 *July* 1994; *accepted* 4 *November* 1994)

Abstract

Ab initio calculations of static structure factors of fluorite (CaF_2) are performed by a linear combination of atomic orbitals Hartree–Fock method as implemented in the *CRYSTAL* program. The effect of thermal motion is then introduced by taking into account the atomic mean square displacements given in the literature at different temperatures and leads to dynamic structure factors. Finally, a very slight displacement of fluorine ions with respect to their ideal position is considered, to simulate an anharmonic vibration or disordered structure so as to improve the agreement with experimental data.

Introduction

In a recent theoretical study of fluorite (CaF_2), Catti, Dovesi, Pavese & Saunders (1991) perfected and used an atomic orbitals (AO) basis set for calcium and fluorine, which allowed them to calculate and compare successfully with experiment some ground-state properties: lattice parameter, binding energy, electronic and band structures, and elastic constants. The fully ionic nature of fluorite is clearly shown.

In the present work, we have calculated the static structure factors of fluorite from the wave functions and density matrix obtained by *CRYSTAL*, an *ab initio* periodic Hartree–Fock program (Dovesi, Pisani, Roetti, Causà & Saunders, 1989; Dovesi, Roetti & Saunders, 1992) by using the same all-electron basis set and computational parameters as those previously defined by Catti *et al.* (1991).

A perturbation of the Fock matrix by thermal motion, assuming that atomic displacements are independent and that the atomic orbitals follow nuclear movements (Azavant, Lichanot, Rérat & Chaillet, 1994), allows us to calculate dynamic structure factors at any temperature by introducing the thermal mean square amplitudes of the atoms given in the literature. Thus, it becomes possible to compare theoretical and experimental values, provided that the latter have been corrected for secondary factors (scale, Lorentz, polarization, absorption, extinction, anomalous scattering, thermal diffuse scattering). For comparison with our calculations, we have considered all the experimental data sets obtained for fluorite in the last 30 years since Togawa's (1964) work. They include: (i) the measurements obtained on the same crystal (American Crystallographic Association single-crystal intensity project) by Abrahams *et al.* (1967) and their assessment and analysis done respectively by Mackenzie & Maslen (1968) and by Cooper (1970); (ii) the data obtained by Zachariasen (1968) with a small spherical crystal; (iii) the data set collected from a crystal of 90 μm by Bachmann, Kohler, Schulz & Weber (1985). These authors have also obtained intensities with synchrotron radiation for the same crystal and for a