THE PHASE RETRIEVAL PROBLEM FOR CYCLOTOMIC CRYSTALS

PHILIPPE JAMING

Abstract. **Abstract :** In this survey, we present the results on the phase retrieval problem for cyclotomic crystals, following J. Rosenblatt's paper [Ro] in a simplified setting. We then present some extensions to the triple-correlation function due to the author and M. Kolountzakis [JamK] and conclude with some open problems.

1. Introduction

1.1. Phase retrieval problems.

Usually, when one measures a quantity, due to noise, poor measurement equipment, transmition in messy media... the phase of the quantity one wishes to know is lost. In mathematical terms, one wants to know a quantity $\varphi(t)$ knowing only $|\varphi(t)|$ for all $t \in \mathbb{R}^d$. Stated as this, the problem has too many solutions to be useful and one tries to incorporate *a priori* knowledge on φ to decrease the underterminancy.

A typical situation is that $\varphi = \widehat{f}$ for some compactly supported function $f \in L^2(\mathbb{R}^d)$ (in short $f \in L^2_c(\mathbb{R})$) or more generally for some compactly supported Schwartz distribution $f \in \mathcal{S}'(\mathbb{R}^d)$. Let us temporarilly concentrate on the one-dimensional case for finite-energy signals. The problem is then:

Problem 1.
Given $f \in L^2_c(\mathbb{R})$, find all $g \in L^2_c(\mathbb{R})$ such that $|\widehat{f}(\xi)| = |\widehat{g}(\xi)|$ for (almost) all $\xi \in \mathbb{R}$.

As f is compactly supported, its Fourier transform is analytic so that actually $|\widehat{f}(\xi)| = |\widehat{g}(\xi)|$ for *all* $\xi \in \mathbb{R}$.

Problem 1 has been solved by Walter [Wa] and we may now describe this solution. First note that this problem has trivial solutions $g(t) = cf(t-\alpha)$ and $g(t) = cf(-t-\alpha)$ where $c \in \mathbb{C}$ with $|c| = 1$ and $\alpha \in \mathbb{R}$. However, there may be more solutions: as $f \in L^2_c(\mathbb{R})$, with support $[-\sigma, \sigma]$, then, $\widehat{f}$ is an entire function of order 1 of type σ. By Hadamard's Factorization Theorem, one may then write

$$\widehat{f}(z) = z^k e^{az+b} \prod \left(1 - \frac{z}{z_k}\right) e^{z/z_k}$$

Key words and phrases. phase retrieval problem.

Research partially financed by:
European Commission Harmonic Analysis and Related Problems 2002-2006 IHP Network (Contract Number: HPRN-CT-2001-00273 - HARP) and Balaton probram EPFA

.

where $a, b \in \mathbb{R}$ and the z_k's are the zeroes of $\widehat{f}$ in the complex plane. Moreover, this zeroes essentially characterize $\widehat{f}$, so that if we knew $|\widehat{f}(\xi)|$ for all $\xi \in \mathbb{C}$ (and not only $\xi \in \mathbb{R}$) we would be done.

To overcome this, write $|\widehat{f}(\xi)|^2 = |\widehat{g}(\xi)|^2$ as $\widehat{f}(\xi)\overline{\widehat{f}(\overline{\xi})} = \widehat{g}(\xi)\overline{\widehat{g}(\overline{\xi})}$ and note that this equation extends to ξ in all of $\mathbb{C}$. It follows that a zero of $\widehat{g}$ is either a zero of $\widehat{f}$ or a conjugate of a zero of $\widehat{f}$. Hadamard's Factorization Theorem for $\widehat{g}$ then shows that every solution is a function of the form

$$\widehat{g}(z) = z^k e^{a'z+b'} \prod \left(1 - \frac{z}{\zeta_k}\right) e^{z/\zeta_k}$$

where $a' = a + i\alpha$, $b' = b + i\beta$ and for each k, $\zeta_k = z_k$ or $\zeta_k = \overline{z_k}$. Such a choice $\zeta_k \in \{z_k, \overline{z_k}\}$ for all k, is called a zero-flipping. Using a Theorem of Titchmarsh [Ti] on the behavior of zeroes of Fourier transforms of compactly supported functions, one can check that every zero-flipping actually gives rise to a solution of Problem 1.

Note that the trivial solutions are then obtained from α, β and either $\zeta_k = z_k$ for every k in which case $g = e^{i\beta} f(t - \alpha)$, or $\zeta_k = \overline{z_k}$ for every k in which case $g = e^{i\beta} f(-t - \alpha)$.

We refer the reader to [Hu] for more details. This book also contains many other occurences of the phase retrieval problem. Further results may be found in the survey [KST] and in the introduction of [Jam4]

1.2. **Diffraction.**

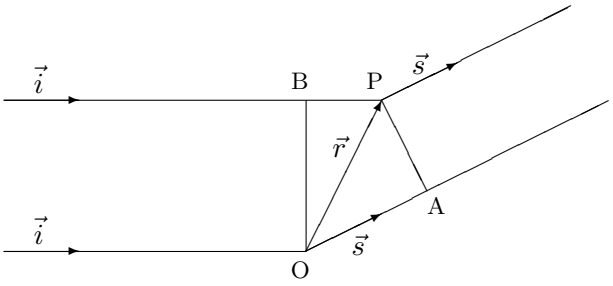
We will now concentrate on the phase retrieval problem for cyclotomic crystals. To present this, let us first give a short introduction to diffraction theory as may be found in many textbooks in physics.

Consider a monochromatic parallel beam of X-rays with amplitude 1 and wavelength λ which we will for simplicity normalize to $\lambda = 1$. Let us considerer two scattering centers O and P, which may be atoms or electrons. Without loss of generality, we may assume that this beam is in the direction $\vec{i} = (1, 0, 0)$ and O is at the origin. Let us now compute the resultant scattered radiation in a given direction $\vec{s}$. The phase of the wave scattered by the point P is ahaed of the phase of the wave scattered by the point O by a quantity

$$\delta = \frac{2\pi}{\lambda}(AO - PB) = 2\pi\langle \vec{r}, \vec{s}\rangle$$

where $\vec{r} = \vec{OP}$, A is the orthogonal projection of P on the line parallel to $\vec{s}$ issued from O and B is the orthogonal projection of O on the line parallel to $\vec{i}$ issued from P.

Thus, if a is the amplitude of the wave scattered by P, then the wave from P may be written as $a \exp 2i\pi\langle \vec{r}, \vec{s}\rangle$ where the phase of the wave scattered from O is taken to be zero. The quantity a may be called the scattering factor of P and is in general a function of $\vec{s}$.



Suppose now there is a set of N scattering points at positions $\vec{r_j}$, $j = 1, \ldots, N$ of scattering factor a_j. Then the total wave scatttered is obtained by summing the waves scattered by all scatterers in a given direction. Hence the total scattered amplitude corresponding to $\vec{s}$ is

$$F(\vec{s}) = \sum_{j=1}^{N} a_j \exp 2i\pi \langle \vec{r_j}, \vec{s} \rangle$$

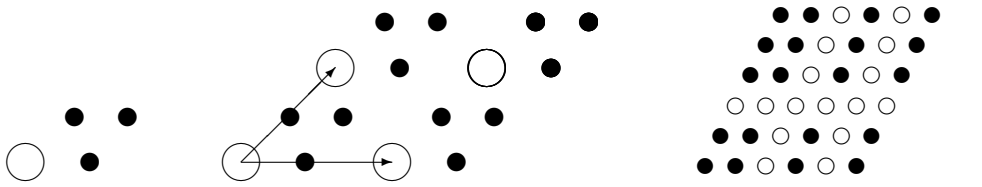
which is the Fourier transform of the linear combination of Dirac masses $\sum_{j=1}^{N} a_j \delta_{\vec{r_j}}$.

Finally, note that the measurement process allows only to get $|F(\vec{s})|$ and not F.

1.3. **The phase retrieval problem in crystals.**
We will now work out the nature of the diffraction pattern given by a repetitive structure scattering matter, as in a (periodic) crystal. The atoms in a crystal are arranged according to the symmetry of a three-dimensional structure with unit-cell translation vectors $\vec{a}, \vec{b}, \vec{c}$. Inside a unit cell, their are N different atoms that occur at position $\vec{r_j}$ given by

$$\vec{r_j} = x_j \vec{a} + y_j \vec{b} + z_j \vec{c}$$

with $0 \leq x_j, y_j, z_j \leq 1$.



a) unit cell b) two-dimensional crystal c) cyclotomic crystal
(o empty position • atom)

Suppose the crystal is a parallelepipedal block that contains N_a, N_b, N_c cells respectively along the direction $\vec{a}, \vec{b}, \vec{c}$. The measure of the scattering amplitude then gives

$$\begin{aligned}&\left|\sum_{a=0}^{N_a-1}\sum_{b=0}^{N_b-1}\sum_{c=0}^{N_c-1}\left(\sum_{j=1}^{N} a_j \exp 2i\pi\Big\langle r_j + a\vec{a}+b\vec{b}+c\vec{c},\vec{s}\Big\rangle\right)\right|^2\\ =&\left|\sum_{j=1}^{N} a_j \exp 2i\pi\langle r_j,\vec{s}\rangle\right|^2\left|\sum_{a=0}^{N_a-1}\sum_{b=0}^{N_b-1}\sum_{c=0}^{N_c-1}\exp 2i\pi\Big\langle a\vec{a}+b\vec{b}+c\vec{c},\vec{s}\Big\rangle\right|^2 := |F_S(\vec{s})|^2|F_L(\vec{s})|^2.\end{aligned}$$

Now write $\vec{s}$ in *reciprocal coordinates* $\vec{s} = x\vec{a}^* + y\vec{b}^* + z\vec{c}^*$ where $\vec{a}^*, \vec{b}^*, \vec{c}^*$ is the dual basis to $\vec{a}, \vec{b}, \vec{c}$, then

$$|F_L(\vec{s})|^2 = \frac{\sin^2(N_a\pi x)}{\sin^2(\pi x)}\frac{\sin^2(N_b\pi y)}{\sin^2(\pi y)}\frac{\sin^2(N_c\pi z)}{\sin^2(\pi z)}.$$

It follows that $\dfrac{|F_L(\vec{s})|^2}{(N_aN_bN_c)^2} \to \delta_{\mathbb{Z}\vec{a}^*+\mathbb{Z}\vec{b}^*+\mathbb{Z}\vec{c}^*}(\vec{s})$. As N_a, N_b and N_c are all three big, one thus considers that a diffraction experiment allows to measure $|F_S(\vec{s})|^2$ for $\vec{s} \in \mathbb{Z}\vec{a}^* + \mathbb{Z}\vec{b}^* + \mathbb{Z}\vec{c}^*$.

Let us now consider a particular case where all atoms in the crystal are identical, that is $a_j = a$ for all j and we may assume that $a = 1$. We further assume that the atoms can only occupy specific positions

$$\vec{r_j} = \frac{k_j}{p}\vec{a} + \frac{l_j}{q}\vec{b} + \frac{m_j}{r}\vec{c}, \quad 0 \le k_j \le p-1,\ 0 \le l_j \le q-1,\ 0 \le m_j \le r-1.$$

Moreover, we assume that $a_j = a^{(1)}_{k_j}a^{(2)}_{l_j}a^{(3)}_{m_j}$ (with the obvious abuse of notation) with each $a^{(1)}_{k_j}, a^{(2)}_{l_j}, a^{(3)}_{m_j} = 0$ or 1. Such a crystal is called a *cyclotomic crystal*. Then the measurement gives, for $a, b, c \in \mathbb{Z}$,

$$\begin{aligned}&|F_S(a\vec{a}^* + b\vec{b}^* + c\vec{c}^*)|^2\\ &= \left|\sum_{j=0}^{n-1} a^{(1)}_j \exp(2i\pi aj/n)\right|^2\left|\sum_{k=0}^{n-1} a^{(2)}_k \exp(2i\pi bk/n)\right|^2\left|\sum_{l=0}^{n-1} a^{(3)}_l \exp(2i\pi cl/n)\right|^2.\end{aligned}$$

This leads us to introduce the following problem n which we will now concentrate:

Problem 2 (Phase Retrieval Problem for Cyclotomic Crystals)**.**
Given $\rho_0, \dots, \rho_{n-1} \in \{0,1\}$, *find* all $\eta_0, \dots, \eta_{n-1} \in \{0,1\}$ *such that, for all* $k = 0, \dots, n-1$,

$$\left|\sum_{j=0}^{n-1} \eta_j e^{2i\pi kj/n}\right| = \left|\sum_{j=0}^{n-1} \rho_j e^{2i\pi kj/n}\right|.$$

Trivial solutions to this problem are given by

$$\eta_j = \rho_{j-j_0 \,(\mathrm{mod}\, n)} \quad \text{and} \quad \eta_j = \rho_{-j-j_0 \,(\mathrm{mod}\, n)}$$

for some $j_0 \in \{0, \dots, n-1\}$. Indeed, one respectively has

$$\sum_{j=0}^{n-1} \eta_j e^{2i\pi kj/n} = e^{2i\pi kj_0/n} \sum_{j=0}^{n-1} \rho_j e^{2i\pi kj/n}$$

and

$$\sum_{j=0}^{n-1} \eta_j e^{2i\pi kj/n} = e^{2i\pi kj_0/n} \overline{\sum_{j=0}^{n-1} \rho_j e^{2i\pi kj/n}}.$$

2. Notations and preliminaries on cyclotomic roots

Facts in this section are classical and can be found in almost any introductory book on algebra. We include them here for the sake of self-completeness.

We will now adopt the following notations:
— we fix an integer n and define $\omega = e^{2i\pi/n}$ and $\zeta = e^{i\pi/n}$.
— We will identify $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$ with $\{0, \dots, n-1\}$, $\Gamma_n := \{\omega^k,\ k = 0, \dots, n-1\}$ the set of n-th roots of unity and $\{\delta_0, \dots, \delta_{n-1}\}$ the set of Dirac masses at $0, \dots, n-1$ (seen as *e.g.* a subset of the set of measures on $\mathbb{Z}_n$). Moreover, we will say that $\mathbb{Z}_n \subset \mathbb{Z}_{2n}$ in the sense that $\Gamma_n \subset \Gamma_{2n}$.
— Next we define $\mathbb{Q}[\mathbb{Z}_n] = \{P = \sum_{g \in \mathbb{Z}_n} \rho_g \delta_g \ : \ \rho_g \in \mathbb{Q}\}$. To an element $P \in \mathbb{Q}[\mathbb{Z}_n]$, we associate a polynomial $\mathbb{P}(x) := \sum_{k=0}^{n-1} \rho_k x^k$. We define $P^* = \sum_{g \in \mathbb{Z}_n} \rho_{-g} \delta_g$ to which corresponds the polynomial $\mathbb{P}^*(x) = \sum_{k=0}^{n-1} \rho_{n-k} x^k$. Note that $P^{**} = P$.
— For $P \in \mathbb{Q}[\mathbb{Z}_n]$ and $k \in \mathbb{Z}$, we define the discrete Fourier transform as $\widehat{P}(k) = \mathbb{P}(\omega^k)$. This is obviously n-periodic and is thus defined on $\mathbb{Z}_n$. Note that $\widehat{P^*} = \overline{\widehat{P}}$.
— For $P, Q \in \mathbb{Q}[\mathbb{Z}_n]$ we define $P * Q$ as the element in $\mathbb{Q}[\mathbb{Z}_n]$ which is associated to the polynomial $\mathbb{P}(x)\mathbb{Q}(x) \pmod{x^n - 1}$. Obviously $P * Q = Q * P$ and $(P * Q)^* = P^* * Q^*$. Moreover $\widehat{P * Q} = \widehat{P}\widehat{Q}$.
— Finally, if $E \subset \mathbb{Z}_n$ we define $\chi_E = \sum_{k \in E} \delta_k \in \mathbb{Q}[\mathbb{Z}_n]$ and we call such elements of $\mathbb{Q}[\mathbb{Z}_n]$ *sets*. Note that $\chi_E^* = \chi_{n-E}$.

The n-th root of unity ω^j is said to be a *root of order* $o(j)$ where $o(j)$ is the smallest integer such that $jo(j)$ is divisible by n. Explicitly $o(j) = n/\gcd(j, n)$. If $n = p_1^{k_1} \cdots p_m^{k_m}$ is the decomposition of m into prime numbers, it follows that possible orders are $o = p_1^{l_1} \cdots p_m^{l_m}$ where $0 \leq l_j \leq k_j$.

The nth roots of a given order m constitute the roots of the so-called *cyclotomic* polynomial Π_m. These polynomials are explicitly defined by

$$\Pi_m(x) = \prod_{\substack{1\le j\le m\\ j \text{ relatively prime to } m}} \left[x - \exp\left(\frac{2i\pi j}{m}\right)\right].$$

They have integer coefficients, are irreducible over the rationals and further, if $P \in \mathbb{Q}[X]$ is such that $Q(\omega^j) = 0$ then $Q(X) = \Pi_{o(j)}(X)R(X)$ with $R \in \mathbb{Q}[X]$. In particular, $Q(\omega^k) = 0$ for all k's such that $n/\gcd(k,n) = n/\gcd(j,n)$.

For instance,

$$X^m - 1 = \prod_{\substack{1\le j\le m\\ j \text{ divides } m}} \Pi_j(X).$$

3. Non-trivial solutions

3.1. **Reformulation of Problem 2.**

As $|\widehat{P}|^2 = \widehat{P}\widehat{P^*} = \widehat{P * P^*}$, we may now reformulate and generalize the Phase Retrieval Problem 2 as follows:

Problem 3.

(1) *Given $P \in \mathbb{Q}[\mathbb{Z}_n]$, find all $Q \in \mathbb{Q}[\mathbb{Z}_n]$ such that $Q * Q^* = P * P^*$.*
(2) *Given $E \subset \mathbb{Z}_n$, find all $F \subset \mathbb{Z}_n$ such that $\chi_F * \chi_F^* = \chi_E * \chi_E^*$.*

Note that if $a \in \mathbb{Z}_n$, then $\delta_a * \delta_a^* = \delta_a * \delta_{-a} = \delta_{a-a} = \delta_e$ and that $\delta_e * P = P$. Thus $(\pm\delta_a * P) * (\pm\delta_a * P)^* = \delta_a * \delta_a^* * P * P^* = P * P^*$. Also if $Q = P^*$ then $Q^{**} = P$ so that $Q * Q^* = P * P^*$.

Definition.
If P, Q are as in Problem 3(1)*, they are said to be* homometric*. If moreover there exists $a \in \mathbb{Z}_n$ such that $Q = \pm\delta_a * P$ or $Q = \pm\delta_a * P^*$, then P and Q are said to be* trivially homometric.

Remark.
Note that, as two sets E and F are homometric if and only if $|\widehat{\chi_E}(k)| = |\widehat{\chi_F}(k)|$ for all k, then in particular, for $k = 0$ we get $|E| = |F|$.

Using the properties above, it is then easy to prove the following:

Proposition 3.1.
If $A, B \in \mathbb{Q}[\mathbb{Z}_n]$ then $P = A * B$ and $Q = A^* * B$ are homometric.

Proof. Indeed $P * P^* = A * B * A^* * B^* = A * B^* * A^* * B^{**} = (A * B^*) * (A * B^*)^* = Q * Q^*$. □

Remark 3.2.
We have $\mathbb{Q}[\mathbb{Z}_n] \subset \mathbb{Q}[\mathbb{Z}_{2n}]$ in the sense that if, to $P \in \mathbb{Q}[\mathbb{Z}_n]$, we associate the polynomial $\mathbb{P}$, then the polynomial $\mathbb{P}_+$ given by$\mathbb{P}_+(Z) = \mathbb{P}(Z^2)$ is associated to an element $P_+ \in \mathbb{Q}[\mathbb{Z}_{2n}]$.

It is then obvious that if $P, Q \in \mathbb{Q}[\mathbb{Z}_n]$ are homometric if and only if P_+ and Q_+ are homometric in $\mathbb{Q}[\mathbb{Z}_{2n}]$.

In general, P and Q are not trivially homometric. Note also that if A and B are sets, P and Q need not be sets. Nevertheless, this may happen:

Example.
For this example, it is easier to work with polynomials. Let $\mathbb{A} = 1 + x + x^3$ so that $\mathbb{A}^* = 1 + x^2 + x^3$. If we take $\mathbb{B} = 1 + x^4 + x^9$ then

$$\mathbb{P} = \mathbb{A}\mathbb{B} = 1 + x + x^3 + x^4 + x^5 + x^7 + x^9 + x^{10} + x^{12}$$

while

$$\mathbb{Q} = \mathbb{A}^*\mathbb{B} = 1 + x^2 + x^3 + x^4 + x^6 + x^7 + x^9 + x^{11} + x^{12}.$$

These corespond respectively to the sets $E = \{0, 1, 3, 4, 5, 7, 9, 10, 12\}$ and $F = \{0, 2, 3, 4, , 6, 7, 9, 11, 12\}$ in $\mathbb{Z}_{13}$.

To see that E and F are not homometric, note that in E the only element that has no "neighbor (mod 13)" is 7 and in F it is 9. So if $E = F - a$ then $a = 2$ as 9 has to be translated to 7. But

$$F - 2 \pmod{13} = \{0, 1, 2, 4, 5, 7, 9, 10, 11\} \neq E \pmod{13}.$$

Now reflect F, $-F = \{0, 1, 2, 4, 6, 7, 9, 10, 11\}$ and now 4 is the only "isolated" element so if $E = -F + a$ then $a = 1$ but

$$-F + 1 = \{1, 2, 3, 5, 7, 8, 10, 11, 12\} \neq E \pmod{13}.$$

The reader should now be convinced that this is just a matter of computing length and relative position of intervals in E and F, as these are conserved by translation and symmetry. E contains one interval of length 1, $\{7\}$ which is surrounded by two intervals of length 2, $\{4, 5\}$ and $\{9, 10\}$ while F contains one interval of length 1, $\{9\}$ which is surrounded by an interval of length 2, $\{6, 7\}$ and an interval of length 3, $\{11, 12, 0\}$.

3.2. **Patterson diagrams.**

There is a more geometric way of looking at homometric sets, which actually explains the denomination.

It is convenient to represent a set $E \subset \mathbb{Z}_n$ as a set of roots of unity on circle of unit circumference in the plane: $\Gamma_E = \{\zeta^k,\ k \in E\}$. Each pair of points in Γ_E is joined by a cord. The set of cords thus obtained is called the *Patterson diagram of E*. We give to each cord in the Patterson diagram, a length equal to the length of the smaller arc that it subtends. Thus they are of the form $2\pi m/n$, $m \in \{0, \ldots, n-1\}$ and typically, only m is shown.

Then E and F are homometric if and only if, every distance that appears in the Patterson diagram of E appears in the Patterson diagram of F with same multiplicity, and vice versa.

The sets E and F are trivially homometric if their Patterson diagrams are obtained from each other by a rotation and (eventually) a symmetry.

For every set E of cardinality 1, 2 or 3, it is then easy to see that if E and F are homometric, then they are trivially homometric. For sets of cardinality 4, the situation is different. In Figure 1 and 2 we exhibit two families of non-trivially homometric sets of four elements:

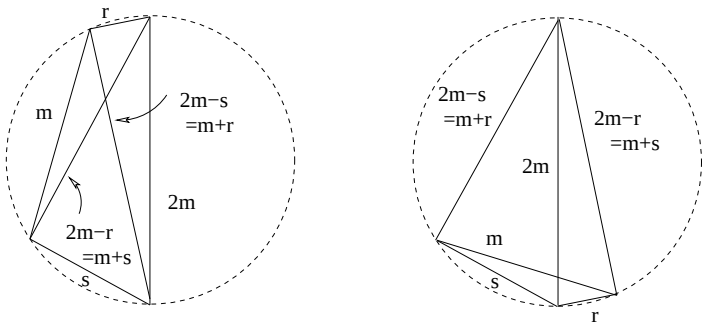


FIGURE 1. The two sets in $\mathbb{Z}/n\mathbb{Z}$ with $n = 4m$ are homometric. Here $r + s = 1/4$, the case $r = s$ was discovered by Paterson and the general case by Erdös. Such sets will be called type 1 sets.

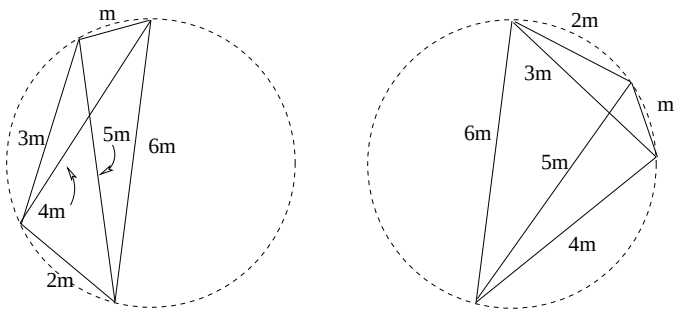


FIGURE 2. The two sets in $\mathbb{Z}/n\mathbb{Z}$ with $n = 13m$ are homometric. These were discovered by Edgar. Such sets will be called type 2 sets.

Proposition 3.3 (Berman & Rosenblatt [Ro])**.**
Let $F \subset \mathbb{Z}_n$ be a set of 4 elements. If there exists a set F that is homometric to E but not trivially homometric, then either E and F are of type 1 defined in Figure 1 or E and F are of type 2 defined in Figure 2.

4. The converse to Proposition 3.1: Rosenblatt's Theorem

In Proposition 3.1 we have shown how to construct homometric polynomials. We will now show, following Rosenblatt [Ro], that this construction actually descibes *all* homometric paires.

Theorem 4.1 (Rosenblatt [Ro])**.**
Let $P, Q \in \mathbb{Q}[\mathbb{Z}_n]$. The following are equivalent:

(i) *P and Q are homometric;*
(ii) *there exists $\varepsilon_1, \varepsilon_2 \in \{-1, 1\}$, $k_1, k_2 \in \mathbb{Z}_n$, $A, B \in \mathbb{Q}[\mathbb{Z}_n]$ such that*
$$P = \varepsilon_1 \delta_{k_1} * A * B \quad \text{and} \quad Q = \varepsilon_2 \delta_{k_2} * A^* * B;$$
(iii) *there exists $\varepsilon_1, \varepsilon_2 \in \{-1, 1\}$, $A, B \in \mathbb{Q}[\mathbb{Z}_{2n}]$ such that*
$$P = \varepsilon_1 A * B \quad \text{and} \quad Q = \varepsilon_2 * A^* * B;$$

Proof. From Remark 3.2, (iii) clearly implies (i).

If we have (ii), then consider $k_1, k_2 \in \mathbb{Z}_n \subset \mathbb{Z}_{2n}$ then $v_1 = (k_1 - k_2)/2$ and $v_2 = (k_1 + k_2)/2$ both make sense in $\mathbb{Z}_{2n}$. Moreover, $\delta_{k_1} = \delta_{v_1} * \delta_{v_2}$ while $\delta_{k_2} = \delta_{-v_1} * \delta_{v_2} = \delta^*_{v_1} * \delta_{v_2}$. Then set $A_1 = \delta_{v_1} * A$ and $B_1 = \delta_{v_2} * B$ so that $P = \varepsilon_1 A_1 * B_1$ and $Q = \varepsilon_2 A_1^* * B_1$.

To prove the remaining part of the theorem, we will need several intermediate results.

Lemma 4.2.
Let $V \in \mathbb{Q}[\mathbb{Z}_n]$ such that, for all k, $\widehat{V}(k) \neq 0$. Then for every $W \in \mathbb{Q}[\mathbb{Z}_n]$, there exists $U \in \mathbb{Q}[\mathbb{Z}_n]$ such that $U * V = W$.

Proof of Lemma 4.2. To U, V, W let us associate the polynomials $\mathbb{U}, \mathbb{V}, \mathbb{W}$ and let us write $\mathbb{U}(x) = \sum_{j=0}^{n-1} u_j x^j$, $\mathbb{V}(x) = \sum_{j=0}^{n-1} v_j x^j$ and $\mathbb{W}(x) = \sum_{j=0}^{n-1} w_j x^j$. Then $U * V = W$ is equivalent to $\mathbb{U}\mathbb{V} = \mathbb{W} \pmod{x^n - 1}$. Since

$$\mathbb{U}\mathbb{V} \pmod{x^n - 1} = \sum_{j=0}^{n-1} \left(\sum_{k=0}^{n-1} u_k v_{j-k \pmod n} \right) x^j$$

we want that

$$\begin{pmatrix} v_0 & v_{n-1} & \cdots & v_1 \\ v_1 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & v_{n-1} \\ v_{n-1} & \cdots & v_1 & v_0 \end{pmatrix} \begin{pmatrix} u_0 \\ \vdots \\ \vdots \\ u_{n-1} \end{pmatrix} = \begin{pmatrix} w_0 \\ \vdots \\ \vdots \\ w_{n-1} \end{pmatrix}. \tag{4.1}$$

Let us write this in matrix form as $\mathcal{C}(V)\mathcal{U} = \mathcal{V}$. Note that the transpose ${}^t\mathcal{C}(V)$ of $\mathcal{C}(V)$ is a circulant matrix so that its eigenvectors are known to be

$$\{(1^k, \omega^k, \omega^{2k}, \ldots, \omega^{(n-1)k}),\ k = 0, \ldots, n-1\}.$$

A simple computation then shows that the corresponding eigenvalues are $\widehat{V}(k)$, $k = 0, \ldots, n-1$. As these are assumed to be nonzero, $\det \mathcal{C}(V) = \det {}^t\mathcal{C}(V) \neq 0$, and as $v_0, \ldots, v_{n-1} \in \mathbb{Q}$, $\det \mathcal{C}(V) \in \mathbb{Q}$. It then follows that for every W, Equation (4.1) has a solution. Moreover, Cramer's Formula shows that $u_0, \ldots, u_{n-1} \in \mathbb{Q}$. □

We then need the following lemma:

Lemma 4.3.
For every $P \in \mathbb{Q}[\mathbb{Z}_n]$ there exist $\widetilde{P} \in \mathbb{Q}[\mathbb{Z}_n]$ such that

$$\widehat{\widetilde{P}}(k) = \begin{cases} 1 & \text{if } \widehat{P}(k) = 0 \\ 0 & \text{else} \end{cases} = \chi_{\{k \in \mathbb{Z}_n :\ \widehat{P}(k) = 0\}}.$$

Remark.
The key point of the lemma is that $\widetilde{P}$ is actually in $\mathbb{Q}[\mathbb{Z}_n]$ and not in $\mathbb{C}[\mathbb{Z}_n]$. Note also that if we consider $\delta_0 - P$ then the roles of 0 and 1 are exchanged: $\widehat{\delta_0 - P} = \chi_{\{k \in \mathbb{Z}_n :\ \widehat{P}(k) \neq 0\}}$. This is actually the polynomial constructed in the proof.

Proof. Let us write $\mathbb{P} = \Pi\mathbb{P}_1$ where Π is a product of cyclotomic polynomials and $\mathbb{P}_1 \in \mathbb{Q}[\mathbb{Z}_n]$ is such that $\widehat{\mathbb{P}_1}(k) \neq 0$ for all k. Write $x^n - 1 = \Pi\widetilde{\Pi}$ where $\widetilde{\Pi} \in \mathbb{Q}[\mathbb{Z}_n]$ is also a product of cyclotomic polynomials so that $\widehat{\widetilde{\Pi}}(k) = 0$ if and only if $\widehat{\Pi}(k) \neq 0$ *i.e.* if and only if $\widehat{\mathbb{P}}(k) \neq 0$.

Let $\mathbb{V} = \mathbb{P} + \widetilde{\Pi}$ so that $\mathbb{V} \in \mathbb{Q}[\mathbb{Z}_n]$ and $\widehat{\mathbb{V}}(k) \neq 0$ for all k. According to the previous lemma, there exists $\mathbb{U} \in \mathbb{Q}[\mathbb{Z}_n]$ such that $\mathbb{U}\mathbb{V} = 1 \bmod(x^n - 1)$. In particular $\widehat{\mathbb{U}}(k)\widehat{\mathbb{V}}(k) = 1$ for all k.

Finally, let $\mathbb{W} = \mathbb{U}\mathbb{P} \bmod(x^n - 1)$ so that, if $\widehat{\mathbb{P}}(k) = 0$ then $\widehat{\mathbb{W}}(k) = \widehat{\mathbb{U}}(k)\widehat{\mathbb{P}}(k) = 0$. Otherwise, if $\widehat{\mathbb{P}}(k) \neq 0$ then $\widehat{\widetilde{\Pi}}(k) = 0$. Thus

$$\widehat{\mathbb{W}}(k) = \widehat{\mathbb{U}}(k)\widehat{\mathbb{P}}(k) = \widehat{\mathbb{U}}(k)(\widehat{\mathbb{P}}(k) + \widehat{\widetilde{\Pi}}(k)) = \widehat{\mathbb{U}}(k)\widehat{\mathbb{V}}(k) = 1.$$

This corrects a small mistake in [Ro]. □

Definition.
An element $U \in \mathbb{Q}[Z_n]$ is called a spectral unit *if $U^* * U = \delta_0$ or equivalently $|\widehat{U}| = 1$.*

Proposition 4.4.
Let $P, Q \in \mathbb{Q}[\mathbb{Z}_n]$, then P and Q are homometric if and only if there exists a spectral unit U such that $U * P = Q$.

Proof. Choose $R \in \mathbb{Q}[\mathbb{Z}_n]$ such that $\widehat{R} = \chi_{\{k\in\mathbb{Z}_n\,:\,\widehat{P}(k)=0\}}$. Then $P + R, Q + R \in \mathbb{Q}[\mathbb{Z}_n]$ and $\widehat{P+R} = \widehat{P} + \chi_{\{k\in\mathbb{Z}_n\,:\,\widehat{P}(k)=0\}}$ never vanishes. Lemma 4.2 gives then the existence of a solution $U \in \mathbb{Q}[\mathbb{Z}_n]$ of $U * (P + R) = Q + R$.

It follows that, for $k \in \mathbb{Z}_n$,
— if k is such that $\widehat{P}(k) \neq 0$ so that $\widehat{R}(k) = 0$,

$$\widehat{U}(k)\widehat{P}(k) = \widehat{U}(k)\big(\widehat{P}(k) + \widehat{R}(k)\big) = \widehat{Q}(k) + \widehat{R}(k) = \widehat{Q}(k),$$

thus, as $|\widehat{P}(k)| = |\widehat{Q}(k)|$, we get $|\widehat{U}(k)| = 1$;
— otherwise $\widehat{P}(k) = 0$ so that $\widehat{R}(k) = 1$ thus

$$\widehat{U}(k) = \widehat{U}(k)\big(\widehat{P}(k) + \widehat{R}(k)\big) = \widehat{Q}(k) + \widehat{R}(k) = 1.$$

Moreover in this case, as $0 = |\widehat{P}(k)| = |\widehat{Q}(k)|$ we also have $\widehat{U}(k)\widehat{P}(k) = \widehat{Q}(k)$.

It follows that for all $k \in \mathbb{Z}_n$, $|\widehat{U}(k)| = 1$ and $\widehat{U}(k)\widehat{P}(k) = \widehat{Q}(k)$. This establishes the first implication in the proposition, the converse being trivial. □

We can now conclude the proof of Rosenblatt's Theorem.

Let P, Q be two homometric elements of $\mathbb{Q}[\mathbb{Z}_n]$. Let $R = P^* + Q^*$ and $S = P^* - Q^*$. Then

$$R * P = P^* * P + Q^* * P = Q^* * Q + Q^* * P = Q^* * R^* = (R * Q)^*.$$

Set $A_1 = R * P$ so that $R * Q = A_1^*$.

Assume for a moment that $\widehat{R}$ never vanishes, then from Lemma 4.2, there exists $B_1 \in \mathbb{Q}[\mathbb{Z}_n]$ such that $B_1 * R = \delta_0$. Then $P = B_1 * A_1 = A_1 * B_1$ while $Q = A_1^* * B_1$. As $\widehat{R}$ might vanish, further computations are needed.

We now set $A_2 = S * P$ and a computation as above then shows that $S * Q = -A_2^*$. If $\widehat{S}$ never vanishes, a similar argument to the above would allow us to conclude. Again, this may

not be the case. Using Lemma 4.3, we can choose $W_1, W_2 \in \mathbb{Q}[\mathbb{Z}_n]$ such that $\widehat{W_1} = \chi_{\{\widehat{P}+\widehat{Q}=0\}}$ and $\widehat{W_2} = \chi_{\{\widehat{P}-\widehat{Q}=0\}}$. Let $V_1 = (\delta_0 - W_2) * W_1 \in \mathbb{Q}[\mathbb{Z}_n]$ and $V_2 = W_1 * W_2 \in \mathbb{Q}[\mathbb{Z}_n]$ so that

$$\widehat{V_1} = \chi_{\{\widehat{P}-\widehat{Q}\neq 0\}\cap\{\widehat{P}+\widehat{Q}=0\}} \quad \text{and} \quad \widehat{V_2} = \chi_{\{\widehat{P}-\widehat{Q}=0\}\cap\{\widehat{P}+\widehat{Q}=0\}} = \chi_{\{\widehat{P}=0\}\cap\{\widehat{Q}=0\}}.$$

Finally, let $V = (\delta_0 - W_1) * R + (\delta_1 - \delta_{n-1}) * V_1 * S + V_2$.[1] Then

$$\widehat{V}(k) = \begin{cases} \widehat{R}(k) \neq 0 & \text{if } \widehat{P}(k) + \widehat{Q}(k) \neq 0 \\ (\omega^k - \omega^{(n-1)k})\widehat{S}(k) & \text{if } \widehat{P}(k) + \widehat{Q}(k) = 0 \text{ and } \widehat{P}(k) - \widehat{Q}(k) \neq 0 \\ \widehat{V_2}(k) = 1 & \text{if } \widehat{P}(k) + \widehat{Q}(k) = 0 \text{ and } \widehat{P}(k) - \widehat{Q}(k) = 0 \end{cases}.$$

Note that $\omega^k - \omega^{(n-1)k} = 0$ if and only if $k = 0$ or $k = n/2$ and this last case is only possible when n is even. Hence $\widehat{V}(k) \neq 0$ unless $\widehat{P}(0) + \widehat{Q}(0) = 0$ and $\widehat{P}(0) - \widehat{Q}(0) \neq 0$ or, when n is even, $\widehat{P}(n/2) + \widehat{Q}(n/2) = 0$ and $\widehat{P}(n/2) - \widehat{Q}(n/2) \neq 0$.

Assume for a moment that P and Q are such that if $\widehat{P}(0)+\widehat{Q}(0) = 0$ then also $\widehat{P}(0)-\widehat{Q}(0) = 0$ and, in the case n is even, if $\widehat{P}(n/2) + \widehat{Q}(n/2) = 0$ then also $\widehat{P}(n/2) - \widehat{Q}(n/2) = 0$. Then $\widehat{P}(k) = \widehat{Q}(k)$ for all k such that $\widehat{V}(k) = 0$. Further, as $V_2 * P = V_2 * Q = 0$,

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

and

$$\begin{aligned} V * Q &= (\delta_0 - W_1) * B_1^* - (\delta_1 - \delta_{n-1}) * V_1 * B_2^* \\ &= (\delta_0 - W_1) * B_1^* + (\delta_1 - \delta_{n-1})^* * V_1 * B_2^*. \end{aligned}$$

But, as $\widehat{W_1}$ and $\widehat{V_1}$ are real valued, $(\delta_0 - W_1)^* = \delta_0 - W_1$ and $V_1^* = V_1$. Hence, letting $A = V * P$, then $A^* = V * Q$. Since $\widehat{V}$ is never zero, we get from Lemma 4.2 that there exists $B \in \mathbb{Q}[\mathbb{Z}_n]$ such that $B * V = \delta_0$. This gives then $P = A * B$ and $Q = A^* * B$.

We will now make the necessary adjustments.

— Assume first that n is odd and that $\widehat{P}(0) + \widehat{Q}(0) = 0$ while $\widehat{P}(0) - \widehat{Q}(0) \neq 0$. Then we just have to replace P by $P_0 = -P$ which is trivially homometric to P thus homometric to Q. The previous argument gives a factorization $P = -A * B$ and $Q = A^* * B$.

— Assume now that n is even. Assume further that $\widehat{P}(0) + \widehat{Q}(0) = \widehat{P}(n/2) + \widehat{Q}(n/2) = 0$ while $\widehat{P}(0) - \widehat{Q}(0) \neq 0$ and $\widehat{P}(n/2) - \widehat{Q}(n/2) \neq 0$. Then, again we replace P by $P_0 = -P$ and we conclude as above.

— Assume now that $\widehat{P}(0) + \widehat{Q}(0) = 0$ but $\widehat{P}(n/2) + \widehat{Q}(n/2) \neq 0$ and $\widehat{P}(0) - \widehat{Q}(0) \neq 0$. Consider $P_0 = -\delta_1 * P$ which is trivially homometric to P, thus homometric to Q. Then $\widehat{P_0}(0) = -\widehat{P}(0)$ so that $\widehat{P_0}(0) + \widehat{Q}(0) \neq 0$ while $\widehat{P_0}(n/2) = -\omega^{n/2}\widehat{P}(n/2) = \widehat{P}(n/2)$ so that $\widehat{P_0}(n/2) + \widehat{Q}(n/2) \neq 0$ and we are back in the previous case. We thus obtain a factorization $P_0 = A * B$ thus $P = -\delta_{n-1} * A * B$ and $Q = A^* * B$.

— Finally, assume that $\widehat{P}(n/2)+\widehat{Q}(n/2) = 0$ but $\widehat{P}(0)+\widehat{Q}(0) \neq 0$ and $\widehat{P}(n/2)-\widehat{Q}(n/2) \neq 0$. We then set $P_0 = \delta_1 * P$ which is homometric to Q and for which $\widehat{P_0}(0) = \widehat{P}(0)$ and

[1]The factor $\delta_1 - \delta_{n-1}$ could be replaced by any factor $E \in \mathbb{Q}[\mathbb{Z}_n]$ such that $E^* = -E$ and for which we know the zeroes of $\widehat{E}$. But such an E necessarily has $\widehat{E} = -\overline{\widehat{E}}$, thus $\widehat{E}(0) = 0$ and, if n is even $\widehat{E}(n/2) = 0$, since these two numbers are real. So $E = \delta_1 - \delta_{n-1}$ is the simplest possible choice.

$\widehat{P_0}(n/2) = -\widehat{P}(n/2)$. It is then immediate to see that we are in the previous case and that we obtain a factorization $P = \delta_{n-1} * A * B$ and $Q = A^* * B$. □

5. A remark on trivial solutions

Trivial solutions appear in every phase retrieval problem, but with no precise definition of what such a solution should be. In [BGJam] we proposed a definition that adapts to every problem. In our case, this would read:

Definition.
A trivial solution *is a linear map* $T : \mathbb{Q}[\mathbb{Z}_n] \to \mathbb{Q}[\mathbb{Z}_n]$ *such that*

1. *for every* $P \in \mathbb{Q}[\mathbb{Z}_n]$, P *and* TP *are homometric.*
2. *for every set* $E \subset \mathbb{Z}_n$, *there exist a set* $F \subset \mathbb{Z}_n$ *such that* $T\chi_E = \chi_F$.

Remark : According to Proposition 4.4, if we omit Condition 2 in the above definition, for every spectral unit U, $TP = U * P$ is a trivial solution and every solution is trivial.

Proposition 5.1.
Every trivial solution is either of the form $TP = \delta_k * P$ *or of the form* $TP = \delta_k * P^*$.

Proof. Let us recall that if χ_E and χ_F are homometric, then E and F have same cardinality.

Now if $E = \{k\}$, the set F given by $\chi_F = T\chi_E$ has only one element, call it j_k. If $E = \{k, \ell\}$ then $\chi_F = T\chi_E = T(\delta_k + \delta_\ell) = T\delta_k + T\delta_\ell = \delta_{j_k} + \delta_{j_\ell}$ and as F has to have 2 elements, $j_k \neq j_\ell$, thus $k \mapsto j_k$ is one to one from $\mathbb{Z}_n \to \mathbb{Z}_n$ thus also onto, that is, there exists a permutation σ such that $j_k = \sigma(k)$.

Finally, $\{0, k\}$ and $\{\sigma(0), \sigma(k)\}$ are homometric if and only if for all $j \in \{0, \dots, n-1\}$,

$$|1 + \omega^{jk}|^2 = |\omega^{j\sigma(0)} + \omega^{j\sigma(k)}|^2$$

that is, $\cos \dfrac{2\pi jk}{n} = \cos \dfrac{2\pi j\big(\sigma(k) - \sigma(0)\big)}{n}$. So either $j\big(\sigma(k) - \sigma(0)\big) = jk \bmod n$ and $\sigma(k) = k + \sigma(0) \bmod n$ or $j\big(\sigma(k) - \sigma(0)\big) = -jk \bmod n$ and $\sigma(k) = -k + \sigma(0) \bmod n$.

It is then easy to check that in the first case $TP = \delta_{\sigma(0)} * P$ and in the second $TP = \delta_{\sigma(0)} * P^*$. □

6. Higher order invariants

A direct inspection shows that, $P = \sum p_k \delta_k, Q = \sum q_k \delta_k \in \mathbb{Q}[\mathbb{Z}_n]$ are homometric if and only if, for all $k \in \mathbb{Z}_n$,

$$\sum p_j p_{j+k} = \sum q_j q_{j+k}.$$

It is sometimes possible to measure the more general quantity

$$N_P^{(r)}(k_1, \dots, k_{r-1}) = \sum_{j=0}^{n-1} p_j p_{j+k_1} \cdots p_{j+k_{r-1}}$$

where $r \geq 2$ is a fixed integer and $k_1, \dots, k_{k-1}$ run over $\mathbb{Z}_n$. $N^{(r)}$ is called an *invariant of order* r. The invariant of order 2 is also called the *Patterson function*. If $P = \chi_E$, we will simply write $N_E^{(r)} = N_P^{(r)}$. This leads to the following problem:

Problem 4.

(i) *Fixed $r \geq 3$, does $N_P^{(r)} = N_Q^{(r)}$ imply that $q_j = \varepsilon p_{j+j_0}$ for some $j_0 \in \mathbb{Z}_n$ and $\varepsilon = 1$ if r is even while $\varepsilon \in \{+1, -1\}$ if r is odd?*
If yes, what is the smallest r for which this is possible.

(ii) *What is the answer to the previous question when P and/or Q are further restricted to sets, i.e. does $N_Q^{(r)} = N_E^{(r)}$ imply that $Q = \pm\chi_{E-k_0}$ for some $k_0 \in \mathbb{Z}_n$?*

Restriction on P and Q.
As our primary interest is in Problem 4(ii), it is natural to assume that $p_j, q_j \geq 0$ for all j and at least one is nonzero. We will write $P, Q \in \mathbb{Q}_+[\mathbb{Z}_n]$. In particular, this removes the parameter ε in Problem 4(i). This also implies that $\widehat{P}(0) = \sum p_j = \|p\|_1 > 0$ and also implies that $\widehat{P}(-k) = \overline{\widehat{P}(k)}$.

Remark.
Note that $\displaystyle\sum_{k_1,\dots,k_{r-1}=0}^{n-1} N_P^{(r)}(k_1, \dots, k_{r-1}) = \|P\|_1^n$ so that if $N_P^{(r)} = N_Q^{(r)}$ then $\|P\|_1 = \|Q\|_1$.
Further

$$\sum_{k_{r-1}=0}^{n-1} N_P^{(r)}(k_1, \dots, k_{r-1}) = N_P^{(r-1)}(k_1, \dots, k_{r-2})\|P\|_1.$$

It follows that if $N_P^{(r)} = N_Q^{(r)}$ then, for all $r' \leq r$, $N_P^{(r')} = N_Q^{(r')}$. Therefore, the second part of Problem 4(i) makes sense.

Taking the discrete Fourier transform of $N_P^{(r)}$ in the $k_1, \dots, k_{r-1}$ variable, it is easy to check that $N_P^{(r)} = N_Q^{(r)}$ if and only if

$$\widehat{Q}_{j_1} \cdots \widehat{Q}_{j_{r-1}} \overline{\widehat{Q}_{j_1+\cdots+j_{r-1}}} = \widehat{P}_{j_1} \cdots \widehat{P}_{j_{r-1}} \overline{\widehat{P}_{j_1+\cdots+j_{r-1}}} \tag{6.2}$$

for all $j_1, \dots, j_{r-1} \in \mathbb{Z}_n$.

First, taking $j_1 = \cdots = j_{r-1} = 0$ in (6.2), and using the fact that $\widehat{Q}(0) = \sum q_j$ is real (rational), we get that $\widehat{Q}(0)^r = \widehat{P}(0)^r$. Thus $\widehat{Q}(0) = \widehat{P}(0)$ if r is odd and $\widehat{Q}(0) = \pm\widehat{P}(0)$ if r is even. There is no loss of generality in assuming that $\widehat{Q}(0) = \widehat{P}(0)$.

Next, take $j_1 = j$ arbitrary and $j_2 = \cdots = j_{r-1} = 0$ in (6.2), then we get $|\widehat{q}(j)|^2 = |\widehat{p}(j)|^2$. We may thus write $q_j = e^{i\varphi_j} p_j$. Reintroducing this in (6.2), we see that Problem 4 amounts to solving the functional equation

$$\varphi_{j_1+\cdots+j_{r-1}} \equiv \varphi_{j_1} + \cdots + \varphi_{j_{r-1}} \pmod{2\pi} \tag{6.3}$$

for all $j_1, \dots, j_{r-1} \in \operatorname{supp} \widehat{p}$ such that $j_1 + \cdots + j_{r-1} \in \operatorname{supp} \widehat{P}$.

The main difficulty will be to handle the holes of $\operatorname{supp} \widehat{P}$.

Remark 6.1.
If $\operatorname{supp} \widehat{P} = \mathbb{Z}_n$ and that $N_Q^{(3)} = N_P^{(3)}$. then, with $r = 3$, $j_1 = j$, $j_2 = k$, (6.3) reduces to $\varphi_{j+k} = \varphi_j + \varphi_k$, therefore $k \to e^{2i\pi\varphi_k}$ is a character of $\mathbb{Z}_n$, thus there exists $j_0 \in \mathbb{Z}_n$ such that for all $k \in \mathbb{Z}_n$, $c\omega^{kj_0}$ for some $c \in \mathbb{C}$ with $|c| = 1$.

But then $\widehat{Q}(k) = c\omega^{kj_0}\widehat{P}(k)$ thus $q_k = cp_{k-k_0}$.

A more refined argument, based on a Lemma of Lenstra [Le] gives the following result ([GM, Theorem 3]):

Theorem 6.2 (Grünbaum & Moore)**.**
Let n be an odd integer and let $P, Q \in \mathbb{Q}_+[\mathbb{Z}_n]$ be such that $N_Q^{(3)} = N_P^{(3)}$. Assume further that $\widehat{P}(1) \neq 0$, then there exists $k_0 \in \mathbb{Z}_n$ such that for all $k \in \mathbb{Z}_n$, $q_k = p_{k-k_0}$.

Moreover, Grünbaum and Moore also proved the following:

Theorem 6.3 (Grünbaum & Moore)**.**

(i) *Let n be an odd integer and let $P, Q \in \mathbb{Q}_+[\mathbb{Z}_n]$ be such that $N_Q^{(4)} = N_P^{(4)}$. Then there exists k_0 such that for all $k \in \mathbb{Z}_n$, $q_k = p_{k-k_0}$.*
(ii) *Let n be an even integer and let $P, Q \in \mathbb{Q}_+[\mathbb{Z}_n]$ be such that $N_Q^{(6)} = N_P^{(6)}$. Then there exists k_0 such that for all $k \in \mathbb{Z}_n$, $q_k = p_{k-k_0}$.*
(iii) *Let n be an even integer and let $E \subset \mathbb{Z}_n$ be such that $\widehat{\chi_E}(1) \neq 0$. Every $Q \in \mathbb{Q}_+[\mathbb{Z}_n]$ such that $N_Q^{(4)} = N_P^{(4)}$ is of the form $q_k = p_{k-k_0}$ for some $k_0 \in \mathbb{Z}_n$.*

From this and a little bit of number theory, one may then get the following ([JamK, Theorem 3]):

Proposition 6.4 (Jaming & Kolountzakis)**.**
Let $a \geq 1$ be an integer and $\wp \geq 3$ a prime. Let $n = \wp^a$ and let $P, Q \in \mathbb{Q}_+[\mathbb{Z}_n]$ be such that $N_Q^{(3)} = N_P^{(3)}$. Then there exists $k_0 \in \mathbb{Z}_n$ such that $F = E - k_0$.

Proof. If $a = 1$ *i.e.* $n = \wp$. As $\widehat{P}(0) \neq 0$, there are only two possibilities:
— either $\widehat{P}(k) = 0$ for some k and then $\widehat{P}(k) = 0$ for all $k \neq 0$, thus $P = c\chi_{\mathbb{Z}_n}$ and the same holds for Q;
— or $\widehat{P}$ does not vanish and we conclude with Remark 6.1.
Assume now we have proved the Theorem for $n = \wp^b$ for $b = 0, \dots, a-1$ and let $P \in \mathbb{Q}[\mathbb{Z}_{\wp^a}]$. This time, there are four possibilities:
— $\widehat{P}(k) = 0$ for all $k \neq 0$ and we conclude as above;
— $\widehat{P}(k) \neq 0$ and Remark 6.1 gives the result;
— $\widehat{P}(k) = 0$ only for those k of the form $k = \ell\wp^{a-b}$, $1 \leq \ell \leq \wp^b$, $b \geq 1$ and then Theorem 6.2 gives the result;
— or $\widehat{P}(k) \neq 0$ only for those k of the form $k = \ell\wp^{a-b}$, $1 \leq \ell \leq \wp^b$, $b \geq 1$. But then $\widehat{P}$ is supported in a subgroup of $\mathbb{Z}_{p^a}$ and so is then $\widehat{Q}$. We may thus assume that $P, Q \in \mathbb{Q}[\mathbb{Z}_{p^a}]$ and have same 3-deck there and we conclude with the induction hypothesis. □

This result was already known in the case $n = \wp$ a prime, but the above proof is simpler *see* [JamK] for references. The second result proved in [JamK] is the following:

Proposition 6.5 (Jaming & Kolountzakis)**.**
Let $p \geq 3$ and $q \geq 3$ be two distinct prime numbers and $n = pq$. Let $E \subset \mathbb{Z}_n$ and assume that $Q \in \mathbb{Q}_+[\mathbb{Z}_n]$ has $N_Q^{(3)} = N_E^{(3)}$, then $Q = \chi_{E-k}$ for some $k \in \mathbb{Z}_n$.

Proof. There was a small gap in the proof of [JamK], so we take here the occasion to correct this.

In this case there are 4 cyclotomic classes $\{0\}$, $\mathcal{C}_p$ the nonzero multiples of p, $\mathcal{C}_q$ the nonzero multiples of q and $\mathcal{R}$ all other numbers. We have to study the zero set of $\widehat{\chi_E}$. First $\widehat{\chi_E}(0) \neq 0$ so there are only 5 cases left: $\widehat{\chi_E}$ may either

— never vanish, in this case we conclude with Remark 6.1;

— vanish on $\mathcal{C}_p \cup \mathcal{C}_q \cup \mathcal{R}$, that is everywhere except at 0, but then $E = \mathbb{Z}_n$ qui $Q = \chi_{\mathbb{Z}_n}$;

— vanish on $\mathcal{C}_p$ on $\mathcal{C}_q$ or on $\mathcal{C}_p \cup \mathcal{C}_q$ only. Then, as $p, q \geq 3$, $\widehat{\chi_E}(1) \neq 0$ and we conclude with Theorem 6.2;

— vanish on $\mathcal{C}_p \cup \mathcal{R}$ or on $\mathcal{C}_q \cup \mathcal{R}$. In this case E is supported respectively on the subgroups $q\mathbb{Z}_p$ and $p\mathbb{Z}_q$ of $\mathbb{Z}_{pq}$ and we conclude with Proposition 6.4;

— vanish on $\mathcal{R}$. But in [JamK], we proved that this can not happen for sets! □

Finally, note that if $p, q, r \geq 3$ are three prime numbers $p \neq q$, then Grünbaum and Moore constructed two *functions* $P, Q \in \mathbb{Q}[\mathbb{Z}_n]$ that are not translates of each other but that have $N_P^{(3)} = N_Q^{(3)}$. In [JamK], we over-interpreted the results in [GM] by saying that these were *sets*. This was finally solved in [KK].

7. Some open problems

7.1. **Are non-trivial homometric sets exceptional?**

Radcliffe and Scott proved that generically, the 3-deck problem has only trivial solutions:

Theorem 7.1 (Radcliffe & Scott [RS])**.**
The proportion of subsets of $\mathbb{Z}_n$ that are not determined up to translations by their 3-deck goes to 0 as $n \to +\infty$.

Proof. In order for a set $E \subset \mathbb{Z}_n$ not to be determined by its 3-deck, a necessary condition is that its Fourier transform vanishes. But, Kleitmans's extension [Kl] of Erdös's theorem on the Littlewood-Offord problem states that, *if $(x_j)_{j=1,\dots,n}$ is some collections of vectors of a normed linear space with $\|x_j\| \geq 1$, then at most $\binom{n}{[n/2]}$ of the sums of the form $\sum_{j\in E} x_j$ can belong to any fixed set of diameter at most* 1. As a consequence, if we consider for fixed i the collection of complex numbers $\{\omega^{ij},\ j = 0, \dots, n-1\}$ then there are at most $\binom{n}{[n/2]}$ subsets E of $\mathbb{Z}_n$ such that

$$\widehat{\chi_E}(i) := \sum_{j\in E} \omega^{ij} = 0.$$

Moreover, if $\widehat{\chi_E}$ vanishes, then it aso vanishes for some integer d that dividees n. We thus get that the proportion of sets that are not determined by their 3-deck is at most

$$\frac{d(n)\binom{n}{[n/2]}}{2^n},$$

where $d(n)$ is the number of divisors of n. As, for any $\varepsilon > 0$, $d(n) = O(n^\varepsilon)$, we get that this proportion goes to 0 with n. □

An improved estimate of the proportion of sets not determined up to translation by their 3-deck is given in [KK].

It is then natural to ask if a similar phenomena occurs for the phase retrieval problem:

Problem 5 (Radcliffe & Scott [RS])**.**
Does the proportion of subsets of $\mathbb{Z}_n$ for which the phase retrieval problem has non trivial solutions go to 0 with n?

7.2. **Number of non-trivial homometric sets.**

Definition.
For $k \geq 1$, let $C(k)$ be the maximal number of mutually non-trivial homometric sets of cardinal k.

In other words, we want that there exist $n \in \mathbb{Z}$ and $E_1, \dots, E_{C(k)} \subset \mathbb{Z}_n$ such that none of them is a translate of any other and which are all homometric.

The only thing that is known about $C(k)$ is the following:

Proposition 7.2 (Rosenblatt)**.**
For every $m \geq 1$, $C(3^m) \geq 2^m$.

Proof. First note that, as there is no restriction on n, by taking n big enough, periodicity has no importance.

Let $A = \{0, 1, 3\}$. This set has the property that if $x_1, x_2, y_1, y_2 \in A$ are such that $|x_1 - x_2| = |y_1 - y_2|$ then $\{x_1, x_2\} = \{y_1, y_2\}$. Let $A_m = 3^m + A$ and, for $\varepsilon_1, \dots, \varepsilon_m \in \{-1, 1\}$, define $A(\varepsilon_1, \dots, \varepsilon_m) = \varepsilon_1 A_1 + \dots + \varepsilon_m A_m \subset \mathbb{Z}$. It is then easy to see that all $A(\varepsilon_1, \dots, \varepsilon_m)$'s are all homometric to $A(1, \dots, 1)$ and are not translates of each other. □

Problem 6 (Rosenblatt)**.**

(i) *Is $C(k) > 1$ if $k \geq 5$?*
(ii) *Is there an increasing function $m(k)$ such that $C(k) \geq m(k)$?*

One of the difficulties here is that, even though we have a characterization of homometric pairs in Theorem 4.1, it is very difficult to use this to construct *sets*. The following example given by J. Rosenblatt shows that well. To descibe this example, we will work with polynomials. Let

$$A(x) = x^{-5/2}(1 - x^3 + x^5) \quad \text{and} \quad B(x) = x^{5/2}(1 + x + x^2 + x^3 + x^4 + x^5 + x^7)$$

so that $P(x) = A(x)B(x) = 1 + x + x^2 + x^5 + x^7 + x^9 + x^{12}$ and $Q(x) = A(1/x)B(x) = 1 + x + x^5 + x^7 + x^8 + x^10 + x^{12}$. It follows that the sets $E = \{0, 1, 2, 5, 7, 9, 12\}$ and $F = \{0, 1, 5, 7, 8, 10, 12\}$ are homometric (say in $\mathbb{Z}_{25}$). The reader may nevertheless check that P and Q can not be factored by polynomials that have only non-negative coefficients.

7.3. **The heavy atom method.**

The heavy atom method consist in modifying the crystal by adding a heavy atom to each unit cell and then doing a second diffraction experiment.

In other words, one does a first experiment which measures $|\widehat{P}|^2$. In the second experiment, P is replaced by $P + C\delta_k$ where $C > 0$ is the electron density of the addet atom and k is its position. Without loss of generality, we may assume that $k = 0$. One then measure $|\widehat{P + C\delta_0}|^2 = |\widehat{P} + C|^2$.

The question is then to decide whether $|\widehat{Q}| = |\widehat{P}|$ and $|\widehat{Q + C\delta_k}| = |\widehat{P + C\delta_0}|$ for some $k \in \mathbb{Z}_n$ implies that $q_j = p_{\pm j - k}$.

Indeed

$$|\widehat{Q+C\delta_k}(j)|^2 = |\widehat{Q}(j)+C\omega^{kj}|^2 = |\widehat{Q}(j)|^2 + C^2 + 2C\mathrm{Re}\,\omega^{-kj}\widehat{Q}(j)$$

while $|\widehat{P+C\delta_0}(j)|^2 = |\widehat{P}(j)|^2 + C^2 + 2C\mathrm{Re}\,\widehat{P}(j)$. Thus the two constraints imply that $\mathrm{Re}\,\omega^{-kj}\widehat{Q}(j) = \mathrm{Re}\,\widehat{P}(j)$. Then, as

$$\big(\mathrm{Re}\,\omega^{-kj}\widehat{Q}(j)\big)^2 + \big(\mathrm{Im}\,\omega^{-kj}\widehat{Q}(j)\big)^2 = |\omega^{-kj}\widehat{Q}(j)|^2 = |\widehat{P}(j)|^2 = \big(\mathrm{Re}\,\widehat{P}(j)\big)^2 + \big(\mathrm{Im}\,\widehat{P}(j)\big)^2$$

we also have $\mathrm{Im}\,\omega^{-kj}\widehat{Q}(j) = \varepsilon_j \mathrm{Im}\,\widehat{P}(j)$ with $\varepsilon_j \in \{-1,1\}$. Now, up to replacing q_j by q_{j-k}, we may assume that $k=0$. Then, $\widehat{Q} = \widehat{P}\chi_{\{\varepsilon_j=1\}} + \widehat{P^*}\chi_{\{\varepsilon_j=-1\}}$. Conversely, every $Q \in \mathbb{Q}[\mathbb{Z}_n]$ such that $\widehat{Q}$ can be written as $\widehat{Q} = \widehat{P}\chi_E + \widehat{P^*}\chi_{\mathbb{Z}_n\setminus E}$ is a solution of the problem.

The difficulty here is to find all sets E for which $Q \in \mathbb{Q}[\mathbb{Z}_n]$. Nevertheless, to find such a set, it is enough to take $R \in \mathbb{Q}[\mathbb{Z}_n]$ and then set $\varepsilon_j = 1$ if and only if $\widehat{R}(j) \neq 0$. According to Lemma 4.3, there exists $\widetilde{R} \in \mathbb{Q}[\mathbb{Z}_n]$ such that $\chi_{\{\varepsilon_j=1\}} = \widehat{\widetilde{R}}$. It then follows that $\widehat{Q} = \widehat{P}\widehat{\widetilde{R}} + \widehat{P^*}(1-\widehat{\widetilde{R}})$ thus $Q = (P-P^*) * \widetilde{R} + P^*$. This is in strong contrast with what happens in $L^2(\mathbb{R})$, see [KST].

Problem 7.

(i) *If P is a set, can one construct a Q as above that is also a set?*

(ii) *Are all solutions described this way? In other terms, if $E \subset \mathbb{Z}_n$ is a set such that $\chi_E = \widehat{R}$ for some $R \in \mathbb{Q}[\mathbb{Z}_n]$, is E a zero set of a Fourier transform of some $S \in \mathbb{Q}[\mathbb{Z}_n]$?*

THANKS

Research partially financed by: *European Commission* Harmonic Analysis and Related Problems 2002-2006 IHP Network (Contract Number: HPRN-CT-2001-00273 - HARP) and Balaton probram EPFA

References

[BGJam] A. Bonami, G. Garrigós & Ph. Jaming *Discrete radar ambiguity problems*, Preprint (2005).

[GM] F. A. Grünbaum and C. C. Moore *The use of higher-order invariants in the determination of generalized Patterson cyclotomic sets*, Acta Cryst. Sect. A **51** (1995), 310–323.

[Hu] N. E. Hurt *Phase Retrieval and Zero Crossing (Mathematical Methods in Image Reconstruction)*, Kluwer Academic Publisher *Math. and Its Appl.*, 1989.

[KK] T. Keleti & M. N. Kolountzakis *On the determination of sets by their triple correlation in finite cyclic groups*, Online J. Analytic Combinatorics **1** (2006), #4.

[Kl] D. J. Kleitman *On a lemma of Littlewood and Offord on the distribution of certain sums*, Math. Zeitschr. **90** (1965), 251–259.

[Jam4] Ph. Jaming *Phase retrieval techniques for radar ambiguity problems*, J. Fourier Anal. Appl. **5** (1999), 309–329.

[JamK] Ph. Jaming & M. N. Kolountzakis *Reconstruction of functions from their triple correlation*, New York J. Math. **9** (2003), 149–164.

[KST] M. V. Klibanov, P. E. Sacks & A. V. Tikhonravov *The phase retrieval problem* Inverse problems **11** (1995), 1–28.

[Le] H. W. Lenstra *Generating units modulo an odd integer by addition and subtraction* Acta Arith. **64** (1993), 383–388.

[RS] A. J. Radcliffe & A. D. Scott *Reconstructing subsets of* $\mathbb{Z}_n$, J. Combin. Theory Ser. A **83** (1998), 169–187.

[Ro] J. Rosenblatt *Phase retrieval* Comm. Math. Phys. **95** (1984), 317–343.

[Ti] E. Titchmarsh *The zeroes of certain integral functions* Proc. London Math. Soc. (2) **25** (1926), 283–307.

[Wa] A. Walter *The question of phase retrieval in optics* Opt. Acta **10** (1963), 41–49.

Université d'Orléans, Faculté des Sciences, MAPMO, BP 6759, F 45067 Orléans Cedex 2, France

E-mail address: Philippe.Jaming@univ-orleans.fr