On the determination of sets by their triple correlation in finite cyclic groups

Tamás Keleti*
Department of Analysis
Eötvös Loránd University,
Pázmány Péter sétány 1/C
H-1117 Budapest, Hungary.
E-mail: *elek@cs.elte.hu*.

Mihail N. Kolountzakis†
Department of Mathematics
Univ. of Crete
GR-71409 Iraklio, Greece.
E-mail: *kolount@gmail.com*.

Submitted: March 16, 2006; Accepted: May 2, 2006; Published: May 5, 2006

Abstract

Let G be a finite abelian group and E a subset of it. Suppose that we know for all subsets T of G of size up to k for how many $x \in G$ the translate $x + T$ is contained in E. This information is collectively called the k-deck of E. One can naturally extend the domain of definition of the k-deck to include functions on G. Given the group G when is the k-deck of a set in G sufficient to determine the set up to translation? The 2-deck is not sufficient (even when we allow for reflection of the set, which does not change the 2-deck) and the first interesting case is $k = 3$. We further restrict G to be cyclic and determine the values of n for which the 3-deck of a subset of $\mathbb{Z}_n$ is sufficient to determine the set up to translation. This completes the work begun by Grünbaum and Moore [GM] as far as the 3-deck is concerned. We additionally estimate from above the probability that for a random subset of $\mathbb{Z}_n$ there exists another subset, not a translate of the first, with the same 3-deck. We give an exponentially small upper bound when the previously known one was $O(1/\sqrt{n})$.

1 Introduction to the problem and results

Let G be a finite abelian group, written additively, and $f : G \to \mathbb{R}$ be a function. For $k \geq 2$ we define the k-deck or k-th order correlation of f as the function

$$N_{f,k} : G^{k-1} \to \mathbb{R}$$

defined by

$$N_{f,k}(x_1, \ldots, x_{k-1}) = \sum_{x \in G} f(x) f(x + x_1) \cdots f(x + x_{k-1}). \tag{1}$$

When $E \subseteq G$ and $f(x) = \chi_E(x)$ is the indicator function of E we also write $N_{E,k}$ in place of $N_{f,k}$. In this case, of $f = \chi_E$, it is easy to see that the number $N_{E,k}(x_1, x_2, \ldots, x_{k-1})$ is precisely the number of times the pattern

$$0, x_1, \ldots, x_{k-1}$$

*Partially supported by OTKA grants 049786 and F 43620 and by European Commission IHP Network HARP (Harmonic Analysis and Related Problems), Contract Number: HPRN-CT-2001-00273 - HARP. This research started when the first author visited the second author at the University of Crete and it continued while the first author was a visitor at the Alfréd Rényi Institute of Mathematics of the Hungarian Academy of Science.

†Partially supported by European Commission IHP Network HARP (Harmonic Analysis and Related Problems), Contract Number: HPRN-CT-2001-00273 - HARP, and by grant INTAS 03-51-5070 (2004) (Analytical and Combinatorial Methods in Number Theory and Geometry). Also by the Greek research program "Pythagoras 2" (75% European funds and 25% National funds).

can be translated by an arbitrary element of G to be contained in E. In particular $N_{E,2}$ determines the difference multiset $E-E$ of E. The k-deck may also be defined on an arbitrary locally compact abelian group, provided we replace the summation in the definition above with integration with respect to Haar measure.

As our primary interest is in indicator functions, we will mainly consider nonnegative functions f. Another reason for considering only real functions is to avoid the extra complication due to the fact that the functions f and ωf have the same k-deck whenever ω is a k-th root of unity.

It is evident that the functions $f(x)$ and $f_t(x) = f(x-t)$ have the same k-decks for all values of k. The problem we discuss in this paper is the following:

> Is the function $f : G \to \mathbb{R}^+$ determined up to translation if we know its k-deck? What if the same question is asked for indicator functions?

It is not hard to see that for $k = 2$, and even for indicator functions, the answer is negative. Indeed, suppose that we have two sets $A, B \subseteq G$ such that $-B$ is not a translate of B and suppose also that the multisets $E = A + B$ and $F = A - B$ are actually sets. Take for example $G = \mathbb{Z}_{101}$ (the cyclic group of 101 elements), $A = \{0, 10, 20, 30\}$ and $B = \{0, 1, 3\}$. Then it is easy to see that the sets E and F have the same 2-deck but are not necessarily translates of each other, e.g. in the example we mentioned.

In this paper we will restrict ourselves to finite cyclic groups and the emphasis will be on the 3-deck or triple correlation. This problem is of significance in several fields of applied science, for example crystallography and signal processing [Pet]. Another example is the method of *speckle masking* in atronomical imaging [LWW], where an averaged triple correlation of two-dimensional observation images taken in quick succession is inverted to obtain a sharper image. This process gets rid of interference due to slowly-varying inhomogeneities in the atmosphere and is apparently quite successful. For further applications see [JK] and the references therein.

Our problem is most naturally studied with the use of the Fourier Transform on G, defined for any function $f : G \to \mathbb{C}$ as a function $\widehat{f}$ on Γ, the group of characters of G (group homomorphisms into the multiplicative group $\{z \in \mathbb{C} : \ |z| = 1\}$), given by

$$\widehat{f}(\gamma) = \sum_{x \in G} f(x)\overline{\gamma(x)}.$$

In the particular case of interest to us when $G = \mathbb{Z}_n$ is the cyclic group of n elements then its dual group Γ is also isomorphic to $\mathbb{Z}_n$ and the FT of $f : \mathbb{Z}_n \to \mathbb{C}$ is a function $\widehat{f} : \mathbb{Z}_n \to \mathbb{C}$ given by

$$\widehat{f}(k) = \sum_{j=0}^{n-1} f(j)\zeta_n^{-jk}, \quad k = 0, \ldots, n-1,$$

where $\zeta_n = \exp(2\pi i/n)$ is a primitive n-th root of unity.

It is easy to see that the Fourier Transform of the function $N_{f,k} : G^{k-1} \to \mathbb{R}^+$, the function $\widehat{N_{f,k}} : \Gamma^{k-1} \to \mathbb{C}$, is given by

$$\begin{aligned} \widehat{N_{f,k}}(\xi_1, \ldots, \xi_{k-1}) &= \widehat{f}(\xi_1) \cdots \widehat{f}(\xi_{k-1})\overline{\widehat{f}(\xi_1 + \cdots + \xi_{k-1})} \\ &= \widehat{f}(\xi_1) \cdots \widehat{f}(\xi_{k-1})\widehat{f}(-(\xi_1 + \cdots + \xi_{k-1})) \ \text{ since } f \text{ is real.} \end{aligned} \tag{2}$$

This implies that

$$N_{f,k} \equiv N_{g,k} \iff \left(\xi_1 + \ldots + \xi_k = 0 \Longrightarrow \widehat{f}(\xi_1)\cdots\widehat{f}(\xi_k) = \widehat{g}(\xi_1)\cdots\widehat{g}(\xi_k)\right). \tag{3}$$

In particular, if $N_{f,k} \equiv N_{g,k}$ for two nonnegative functions f and g on G, we immediately get $\widehat{f}(0) = \widehat{g}(0)$ by setting all $\xi_j = 0$. It is also clear that $N_{f,k} \equiv N_{g,k}$ for nonnegative f and g implies $N_{f,r} \equiv N_{g,r}$ for all $2 \leq r \leq k-1$ as well, so that identity of the k-decks implies the identity of all lower order r-decks. Choosing $\xi_1 = -\xi_2 = \xi$ and $\xi_j = 0$ for $j \geq 3$ we get $\left|\widehat{f}(\xi)\right| = |\widehat{g}(\xi)|$. Note that if k is odd then we get $\left|\widehat{f}\right| \equiv |\widehat{g}|$ even for two arbitrary real functions f and g on G with $N_{f,k} = N_{g,k}$ if $\widehat{f}(0) \neq 0$ or $\widehat{g}(0) \neq 0$. Furthermore, if $k = 3$ and if we know that $\widehat{f}$ has no zeros on Γ it follows using (2) that the ratio $\widehat{f}/\widehat{g}$ is a map from G to the unit circle which is a group homomorphism, and this is equivalent to the function f being a translate of the function g.

This reveals the fact that the main difficulty in the study of this problem is the existence of zeros in the Fourier Transform of the function whose k-deck we know. Consider for example the case of the group $G = \mathbb{Z}_p$, p a prime. It is well known that the linear rank over $\mathbb{Q}$ of the set of p-th roots of unity is $p-1$, and this implies that any non-trivial $\mathbb{Q}$-linear combination of at most $p-1$ such roots cannot vanish. In other words, if we have a non-constant function $f : \mathbb{Z}_p \to \mathbb{Q}$ (e.g. the indicator function of a non-trivial subset of $\mathbb{Z}_p$), then its FT never vanishes on $\mathbb{Z}_p$ (which is the dual group of itself). By the previous discussion then the 3-deck of any function $f : \mathbb{Z}_p \to \mathbb{Q}$ determines f up to translation [RS1].

The question of whether $N_{f,k}$ determines f up to translation depends both on the group G on which f is defined as well as on assumed properties of f. The main cases of interest are when (a) f is any nonnegative function, (b) f is a rational-valued function, possibly restricted to be nonnegative, and (c) f is an indicator function. It is not hard to see, for instance, that on the group $\mathbb{R}$ there are, for every k, nonnegative functions which are not determined up to translation from their k-deck [JK]. The same question is open if one demands that f is an indicator function of set of finite measure although the answer is known to be positive in certain special cases of sets [JK]. On the other hand even the 3-deck determines a function $f \in L^1(\mathbb{R})$ if it is of compact support [JK].

1.1 Previous results

In the case of cyclic groups the most significant work is that of Grünbaum and Moore [GM]. This work seems largely to have gone unnoticed in the mathematical literature although it solves the most important cases of the problem for cyclic groups. This is probably due to the fact that it was published in a Crystallography journal. The following is a summary of the results in [GM] regarding reconstructing f on $\mathbb{Z}_n$ from its k-deck. Notice that in [GM] it is assumed at the outset that all functions to be reconstructed from their k-deck have a non-zero sum over the group.

1. For any n, if f and g are rational-valued functions on $\mathbb{Z}_n$ with the same 6-deck then they are translates of each other [GM, Theorem 4].

2. If n is even and at least 30 then there are sets $E, F \subseteq \mathbb{Z}_n$ which have the same 3-deck but are not translates of each other [GM, §5.3].

3. If n is odd, f and g are rational-valued functions on $\mathbb{Z}_n$ with the same 3-deck and $\widehat{f}(1) \neq 0$ then f and g are translates of each other [GM, Theorem 3]. This is heavily based on a result of Lenstra [L] (see our §2.1).

4. For any n suppose that f is a rational-valued function on $\mathbb{Z}_n$ and $E \subseteq \mathbb{Z}_n$, $g = \chi_E$. Then if f and g have the same 4-deck and $\widehat{f}(1) \neq 0$ it follows that f and g are translates of each other [GM, Theorem 5]. It is suggested in [GM] that the condition $\widehat{f}(1) \neq 0$ may be unnecessary.

5. There is no value of k such that for all n the equality of the k-deck of two *real* functions f and g on $\mathbb{Z}_n$ implies that they are translates of each other [GM, §8.2].

6. If $n = pqr$, with p and q distinct primes, and $r > 1$ is an integer then there are two rational-valued functions f and g on $\mathbb{Z}_n$ which have the same 3-deck, satisfy $\widehat{f}(1) = \widehat{g}(1) = 0$, and are not translates of each other [GM, §5.2].

Radcliffe and Scott [RS2] study the problem for infinite subsets of $\mathbb{R}$ which are subject to some sort of "local finiteness" and prove reconstructibility from the 3-deck. In [RS1] the same authors prove reconstructibility up to translation from the 3-deck in $\mathbb{Z}_p$, p a prime, show that almost all subsets of $\mathbb{Z}_n$ are determined up to translation by their 3-deck and show that any set in $\mathbb{Z}_n$ is determined up to translation by its k-deck with k being 9 times the number of distinct prime factors of n.

Pebody, Radcliffe and Scott [PRS] study a variation of the problem. They prove that any finite subset E of the plane can be reconstructed up to rigid motion if one knows for any subset A of the plane of up to 18 points how many rigid-motion copies of A are to be found in E.

Jaming and Kolountzakis [JK] study the problem both in the case of the group $\mathbb{R}$ and in cyclic groups. In the case of $\mathbb{R}$ it is pointed out that several conditions which guarantee some sort of analyticity of $\widehat{f}$ are enough to imply that the 3-deck of f determines f up to translation. It is shown that for every k there exist two nonnegative, smooth $f, g \in L^1(\mathbb{R})$ with the same k-deck, which are not translates of each other. In fact for some such f there exist even uncountably many, translation inequivalent, functions g which have the same k-deck as f.

It is also proved in [JK] that if $E \subseteq \mathbb{R}$ has finite measure, $g \in L^1(\mathbb{R})$ is nonnegative and χ_E and g have the same 3-deck, then g is itself an indicator function. Although it is still an open problem whether any $E \subseteq \mathbb{R}$ of finite measure is determined up to translation from its 3-deck, it is proved in [JK] that if E is an open set with gaps bounded below (write E as a disjoint collection of open intervals and look at the gaps so defined) then E is determined from its 3-deck.

In the case of the cyclic group $\mathbb{Z}_n$ it is proved in [JK, Theorem 3.1 and following Remark] that when $n = p^\alpha$, p a prime larger than 2, then the 3-deck of a set in $\mathbb{Z}_n$ determines the set up to translation. It is also shown that if $n = 2^\alpha$ then the 4-deck of a set determines the set up to translation (and this is mistakenly attributed to [GM]). In [JK, Theorem 3.2] it is erroneously claimed that if $n = pq$ with p and q two distinct primes then the 3-deck is enough to reconstruct a set in $\mathbb{Z}_n$. Given the results of [GM] summarized above, the condition $p, q > 2$ clearly needs to be added and then the theorem is correct. A corrected proof is given in our §2. The attempt, at the end of [JK], to explain the examples given by Grünbaum and Moore for the case $n = pqr$ (see summary above) is also erroneous.

Pebody [P] defines $r(G)$ (resp. $r_{\text{set}}(G)$) the minimum k such that the k-deck of a nonnegative rational-valued function on G (resp. subset of G) determines the function (resp. set) up to translation. Improving results for the cyclic group of Alon, Caro, Krasikov and Roditty [ACKR] and Radcliffe and Scott [RS1], Pebody, computes the number $r(G)$ for all finite abelian G and his result implies $r(\mathbb{Z}_n) \leq 6$. For the cyclic groups the result had already been proved in [GM]. In particular, Pebody gets that the 3-deck determines all nonnegative rational valued functions up to translation on the cyclic group $\mathbb{Z}_n$ ($n \geq 3$) if and only if n is a power of an odd prime or the product of two odd primes.

1.2 New results

In §2 we complete the characterization of those finite cyclic groups in which the 3-deck determines any subset up to translation. We show that

1. If $n = p^2q$, with p and q distinct odd primes then any subset of $\mathbb{Z}_n$ can be determined up to translation from its 3-deck (Theorem 2.1).
2. The same is true if $n = pqr$, with p, q, r distinct odd primes (Theorem 2.1).
3. If $n = pqrd$, with p, q distinct primes and $r, d > 1$, then there are two subsets E and F of $\mathbb{Z}_n$ with the same 3-deck which are not translates of each other (Theorem 2.23).
4. If $n = 2k$, $k \geq 6$, we give two subsets E and F of $\mathbb{Z}_n$, not translates of each other, which have the same 3-deck (Theorem 2.22). This result subsumes the above mentioned result of [GM] (for even n, $n \geq 30$) and, we think, our examples are much easier to understand.

   If n is even and at most 10 we show that there are no such examples (Proposition 2.21).

Thus we get the following.

Corollary 1.1. *Every subset of the cyclic group $\mathbb{Z}_n$ can be determined up to translation from its 3-deck if and only if n is a power of an odd prime or n is the product of at most three (not necessarily distinct) odd primes or $n \in \{2, 4, 6, 8, 10\}$.*

Remark 1.2. As we were finishing this paper we came across a manuscript by Pebody [P2] where the cases of odd n for which the 3-deck is sufficient are also determined. Our work was done independently and, apparently, almost simultaneously.

Comparing Corollary 1.1 to the last mentioned special case of the result of Pebody [P] in the previous subsection, we observe that the analogous characterization of the "good" values of n is different if we consider nonnegative rational valued functions instead of subsets.

Key to our results are theorems which significantly restrict the zero set of the Fourier Transform of indicator functions of subsets of certain cyclic groups. See for instance Lemma 2.18.

In §3 we study the number of subsets of $\mathbb{Z}_n$ which are not determined by their 3-deck up to translation. In [RS1] Radcliffe and Scott had already shown that this number is $O(2^n/\sqrt{n})$ as $n \to \infty$. We show that this number is in fact much smaller, namely $O(2^{-C_\epsilon n^{1-\epsilon}} 2^n)$, for any fixed $\epsilon > 0$ (Theorem 3.4).

2 For which cyclic groups the 3-deck determines a set up to translation

2.1 Positive results

The main result of this subsection is the following:

Theorem 2.1. *Let n be a power of an odd prime or the product of at most three (not necessarily distinct) odd primes. Then every subset of $\mathbb{Z}_n$ is uniquely determined up to translation by its 3-deck.*

For completeness and because it needs no extra effort, our proof will cover not only the new results but also the known ones. We shall use only the same theorem of H. W. Lenstra that was used by Grünbaum and Moore in [GM]:

Lenstra's Theorem [L]. *If N is an odd integer, and m and N are coprime then there exists a finite sequence $x_1, \dots, x_l$ of relative primes to N such that $x_1 = 1$, $x_l = m$ and every member except the first is the sum or difference of two not necessarily different previous members of the sequence.*

As we saw in the Introduction, the 3-deck determines a nonnegative function up to translation if its Fourier Transform has no zero. We shall show that if n is a power of an odd prime or n is the product of at most three (not necessarily distinct) odd primes then the support of the Fourier Transform of a characteristic function on $\mathbb{Z}_n$ is always rich enough to get the same conclusion. Our method can be considered as a generalization of the methods in [GM] and [JK].

The concept of *extendable domain*, defined below, is central to the problem and the techniques of this paper. In fact, this is the right notion for what we called "rich enough" in the previous paragraph.

Definition 2.2. We say that $A \subset \mathbb{Z}_n$ is an *extendable domain* if for every $h : A \to \mathbb{R}/\mathbb{Z}$ additive (by which we mean that $h(x+y) = h(x) + h(y)$ whenever $x, y, x+y \in A$) function there exists an $L \in \mathbb{R}$ such that $h(k) = Lk \pmod 1$ for every $k \in A$.

Reconstructing f (up to translation) from its 3-deck is simple if $\operatorname{supp} \widehat{f}$ is an extendable domain.

Lemma 2.3. *(1) If f and g are nonnegative functions on $\mathbb{Z}_n$ with the same 3-deck and $\operatorname{supp} \widehat{f}$ is an extendable domain then f and g are translates of each other.*

(2) If f and g are real valued functions on $\mathbb{Z}_n$ with the same 3-deck, $\widehat{f}(0) \neq 0$ or $\widehat{g}(0) \neq 0$ and $\operatorname{supp} \widehat{f}$ is an extendable domain then f and g are translates of each other.

Proof. Suppose that f and g satisfy the conditions of (1) or (2). We saw in the Introduction that in these cases having the same 3-deck implies that $\widehat{f}$ and $\widehat{g}$ have the same modulus. Hence there exists a function $h : \operatorname{supp} \widehat{f} \to \mathbb{R}/\mathbb{Z}$ such that $\widehat{g}(l) = e^{2\pi i h(l)} \widehat{f}(l)$. Substituting this to (3) we get that h must be additive as defined in Definition 2.2. Then, since $\operatorname{supp} \widehat{f}$ is an extendable domain, h must be linear, thus $e^{2\pi i h(l)}$ is the restriction of a character to $\operatorname{supp} \widehat{f}$, and so f and g are translates of each other. □

Therefore, to prove Theorem 2.1 it is enough to prove the following:

Proposition 2.4. *If n is a power of an odd prime or n is the product of at most three (not necessarily distinct) odd primes then the support of the Fourier Transform of a characteristic function on $\mathbb{Z}_n$ is always an extendable domain.*

To prove this proposition we need several facts and lemmas, some of which may be known and/or interesting in themselves. The following five facts are surely known but for completeness, and because it is easier to prove them than to find them in the literature, we present their proofs.

Notation 2.5. Let (k,l) denote the greatest common divisor of k and l. For $a|n$ let

$$\langle a\rangle_n = \{k \in \mathbb{Z}_n : (k,n) = a\} \quad \text{and}$$

$$a\mathbb{Z}_n = \left\{0,\ a,\ 2a,\ \ldots\ ,\ \left(\frac{n}{a}-1\right)a\ \right\} \subset \mathbb{Z}_n.$$

Fact 2.6. *If $f : \mathbb{Z}_n \to \mathbb{Q}$ then* $\operatorname{supp}\widehat{f}$ *is the union of sets of the form $\langle a\rangle_n$ for some $a|n$.*

Proof. We can write $\widehat{f}(k) = \sum_{j=0}^{n-1} f(j)\zeta_{n,k}^j$, where $\zeta_{n,k} = e^{-2\pi ik/n}$ is the k-th root of unity of order n. The right hand side is a rational polynomial evaluated at the roots of unity. It is well known that $\zeta_{n,k}$ is an algebraic conjugate of $\zeta_{n,l}$ over $\mathbb{Q}$ if and only if $(n,k) = (n,l)$. □

Fact 2.7. *For $a|n$ a function $f : \mathbb{Z}_n \to \mathbb{C}$ is a-periodic if and only if* $\operatorname{supp}\widehat{f} \subset \frac{n}{a}\mathbb{Z}_n$.

Proof. The space of a-periodic functions on $\mathbb{Z}_n$ has dimension a and it is clearly spanned by the characters $\chi_l(j) = e^{2\pi i\frac{ln}{a}j}$, $l = 0, 1, \ldots, a-1$. □

Fact 2.8. *For a function $f : \mathbb{Z}_n \to \mathbb{C}$ we have* $\operatorname{supp}\widehat{f} \subset a_1\mathbb{Z}_n \cup \ldots \cup a_k\mathbb{Z}_n$ *if and only if f can be written in the form $f = f_1 + \ldots + f_k$, where $f_j : \mathbb{Z}_n \to \mathbb{C}$ is $\frac{n}{a_j}$-periodic ($j = 1, \ldots, k$).*

Proof. The splitting $f = \sum f_j$ is accomplished by arbitrarily splitting $\widehat{f} = \sum \widehat{f_j}$, in a way that $\widehat{f_j}$ is supported on $a_j\mathbb{Z}_n$, inverting the Fourier Transform and using Fact 2.7. □

Fact 2.9. *If n is odd then any integer k can be written as $k = a+b$ where $(a,n) = (b,n) = 1$.*

Proof. We can clearly assume that n is squarefree; that is, it is of the form $n = p_1 \cdots p_r$, where $p_1, \ldots, p_r$ are distinct primes. For each $j = 1, \ldots, r$ let $a_j = 2$ and $b_j = -1$ if $k = 1 \pmod{p_j}$ and let $a_j = 1$ and $b_j = k-1$ otherwise. By the Chinese Remainder theorem there exist a and b such that $a = a_j \pmod{p_j}$ and $b = b_j \pmod{p_j}$ for $j = 1, \ldots, r$. Now $a+b = k \pmod{p_j}$ for each $j = 1, \ldots, r$, so $a + b = k \pmod{n}$. By choosing a properly, by which we mean that we add a multiple of n to a if necessary, we can guarantee that $a + b = k$. Since each $p_j > 2$, we have $a_j, b_j \neq 0 \pmod{p_j}$, so $(a,n) = (b,n) = 1$. □

Fact 2.10. *If there are two equivalence relations on a set such that both contain at least two classes then there exist two elements which are inequivalent w.r.t. both relations.*

Proof. If not then any two elements which are inequivalent w.r.t. the first relation should be equivalent w.r.t. the second. This easily implies that there is only one equivalence class w.r.t. the second relation, a contradiction. □

The following will be used repeatedly in the sequel.

Lemma 2.11. *If a is a divisor of the odd n and $\langle a\rangle_n \subset A \subset a\mathbb{Z}_n$ then A is an extendable domain.*

Proof. Let $h : A \to \mathbb{R}/\mathbb{Z}$ be an additive function. It is enough to prove that

$$m \in \mathbb{Z}, ma \in A \Longrightarrow h(ma) = mh(a) \pmod 1, \tag{4}$$

since then for any $L \in \mathbb{R}$ such that $h(a) = La \pmod 1$ we get that $h(ma) = mh(a) = Lma \pmod 1$, which is exactly what we want to show.

Let $N = n/a$. Note that $ma \in \langle a\rangle_n$ holds if and only if m and N are coprime. Using the previously stated Lenstra's Theorem for $N = n/a$ and an m such that m and N are coprime we get a sequence $x_1, \dots, x_l$ of relative primes to N such that $x_1 = 1$, $x_l = m$ and every member except the first is the sum or difference of two not necessarily different previous members of the sequence. Note that, since x_i and n/a are coprime, $x_i a \in \langle a\rangle_n \subset A$ for each i. Then by induction we get that $h(x_i a) = x_i h(a)$, and so (4) holds whenever m and n/a are coprime. Then (4) in the general case follows by using Fact 2.9. □

Corollary 2.12. *If n is odd, $f : \mathbb{Z}_n \to \mathbb{Q}$ and $a \in \operatorname{supp} \widehat{f} \subset a\mathbb{Z}_n$ then $\operatorname{supp} \widehat{f}$ is an extendable domain.*

In particular, the following two statements hold:

(i) If n is odd, $f : \mathbb{Z}_n \to \mathbb{Q}$ and $\widehat{f}(1) \neq 0$ then $\operatorname{supp} \widehat{f}$ is an extendable domain.

(ii) If n is a power of an odd prime and $f : \mathbb{Z}_n \to \mathbb{Q}$ then $\operatorname{supp} \widehat{f}$ is an extendable domain.

Proof. The first statement follows immediately from Lemma 2.11 and Fact 2.6. If $a = 1$ then we get (i). Statement (ii) is also a special case of the first statement since if $n = p^k$ and l is minimal such that $p^l \in \operatorname{supp} \widehat{f}$ then $p^l \in \operatorname{supp} \widehat{f} \subset p^l\mathbb{Z}_n$. □

The next lemma shows that the sum of two periodic functions with coprime periods cannot have too small a range.

Lemma 2.13. *If $\chi_E = f_a + f_b$, and f_a and f_b are periodic $\mathbb{Z} \to \mathbb{C}$ functions with coprime periods a and b then χ_E is periodic with period a or b.*

Proof. Using the periodicity and $\chi_E = f_a + f_b$, for any $k, n, l \in \mathbb{N}$ we get

$$f_b(ak + bn + l) = f_b(ak + l) = \chi_E(ak + l) - f_a(ak + l) = \chi_E(ak + l) - f_a(l). \tag{5}$$

Since a and b are coprime, for any fixed $l \in \mathbb{Z}$ every integer can be written in the form $ak + bn + l$. Thus (5) implies that for any fixed $l \in \mathbb{Z}$ the range of f_b is a subset of $R_l = \{-f_a(l), 1 - f_a(l)\}$, as witnessed by the right hand side of (5).

If f_b is a constant function then we have the desired conclusion as χ_E is then a-periodic. If f_b is not a constant then the range of f_b is equal to the set R_l, for any integer l, and this implies that R_l is independent of l, or, in other words, that f_a is a constant. In that case χ_E is b-periodic. □

Lemma 2.14. *Suppose that a and b are divisors of n, n/a and n/b are coprime, $E \subset \mathbb{Z}_n$, and $\operatorname{supp} \widehat{\chi_E} \subset a\mathbb{Z}_n \cup b\mathbb{Z}_n$. Then $\operatorname{supp} \widehat{\chi_E} \subset a\mathbb{Z}_n$ or $\operatorname{supp} \widehat{\chi_E} \subset b\mathbb{Z}_n$.*

Proof. By Fact 2.8, $\operatorname{supp} \widehat{\chi_E} \subset a\mathbb{Z}_n \cup b\mathbb{Z}_n$ implies the existence of an n/a-periodic function f and an n/b periodic function g such that $\chi_E = f + g$. Since n/a and n/b are coprime, by Lemma 2.13, we get that χ_E must be n/a-periodic or n/b periodic. By Fact 2.7, this implies that $\operatorname{supp} \widehat{\chi_E} \subset a\mathbb{Z}_n$ or $\operatorname{supp} \widehat{\chi_E} \subset b\mathbb{Z}_n$. □

Lemma 2.15. *Suppose that a and b are coprime divisors of n, $E \subset \mathbb{Z}_n$,*

$$\operatorname{supp} \widehat{\chi_E} \subset (a\mathbb{Z}_n \cup b\mathbb{Z}_n \setminus ab\mathbb{Z}_n) \cup \{0\}.$$

Then $\operatorname{supp} \widehat{\chi_E} \subset a\mathbb{Z}_n$ *or* $\operatorname{supp} \widehat{\chi_E} \subset b\mathbb{Z}_n$.

Proof. Let $c = \frac{n}{ab}$. By Fact 2.8, $\operatorname{supp} \widehat{\chi_E} \subset a\mathbb{Z}_n \cup b\mathbb{Z}_n$ implies that χ_E can be written in the form $\chi_E = f_a + f_b$, where f_a is bc-periodic and f_b is ac-periodic. Applying Lemma 2.13 we get that for each $t = 0, 1, \ldots, c-1$ the function $\chi_E(kc+t)$ is a-periodic or b-periodic. Let m_t be the number of points of the form $kc+t$ in E. Then

$$m_t \in \{0, 1, \ldots, ab\} \text{ is divisible by } a \text{ or } b; \\ \text{by } a \text{ if } \chi_E(kc+t) \text{ is } b\text{-periodic and by } b \text{ if } \chi_E(kc+t) \text{ is } a\text{-periodic.} \quad (6)$$

A straightforward calculation shows that for any $s \in \mathbb{Z}$

$$\widehat{\chi_E}(sab) = \sum_{t=0}^{c-1} m_t \left(e^{\frac{2\pi i s}{c}}\right)^t.$$

Since we assumed that $\widehat{\chi_E}(sab) = 0$ for $s = 1, \ldots, c-1$, we get that the $c-1$ c-th roots of unity $e^{\frac{2\pi i s}{c}}$ $(s = 1, \ldots, c-1)$ are all roots of the $(c-1)$-th order polynomial $\sum_{t=0}^{c-1} m_t z^t$. Hence $\sum_{t=0}^{c-1} m_t z^t$ must be a constant multiple of $\prod_{s=1}^{c-1}(z - e^{\frac{2\pi i s}{c}}) = \sum_{t=0}^{c-1} z^t$ and so all m_t must be the same. Using (6) and that a and b are coprime this implies that $\chi_E(kc+t)$ is a-periodic for each t or b-periodic for each t. Thus χ_E is ac-periodic or bc-periodic hence, by Fact 2.7, $\operatorname{supp} \widehat{\chi_E} \subset a\mathbb{Z}_n$ or $\operatorname{supp} \widehat{\chi_E} \subset b\mathbb{Z}_n$. □

Lemma 2.16. *If a and b are coprime divisors of the odd n and $\langle a \rangle_n \cup \langle b \rangle_n \cup \{ab\} \subset A \subset a\mathbb{Z}_n \cup b\mathbb{Z}_n$ then A is an extendable domain.*

Proof. Let $h : A \to \mathbb{R}/\mathbb{Z}$ be an additive function. We have to find an $L \in \mathbb{R}$ such that $h(k) = Lk \pmod 1$ for every $k \in A$.

By Lemma 2.11, $A \cap a\mathbb{Z}_n$ and $A \cap b\mathbb{Z}_n$ are extendable domains, so there exist L_a and L_b such that

$$h(k) = L_a k \pmod 1 \quad \text{if } k \in A \cap a\mathbb{Z}_n, \qquad \text{and} \qquad h(k) = L_b k \pmod 1 \quad \text{if } k \in A \cap b\mathbb{Z}_n. \quad (7)$$

Note that for any $u, v \in \mathbb{Z}$, L_a can be replaced by $L_a + \frac{u}{a}$ and L_b can be replaced by $L_b + \frac{v}{b}$ in (7). Thus it is enough to find $u, v \in \mathbb{Z}$ such that $L_a + \frac{u}{a} = L_b + \frac{v}{b}$, which is equivalent to

$$ub - va = L_a ab - L_b ab. \quad (8)$$

Using $ab \in A$ and (7), we get $L_a ab = h(ab) = L_b ab \pmod 1$, so $L_a ab - L_b ab \in \mathbb{Z}$. Then, since a and b are coprime, there exists $u, v \in \mathbb{Z}$ for which (8) holds, which completes the proof. □

In the sequel we shall use Fact 2.6 in the proofs many times without explicitly citing it.

Lemma 2.17. *Let the odd $n = pqd$, where p and q are two distinct primes, and d is a prime or $d = 1$. If $E \subset \mathbb{Z}_n$ and* $\operatorname{supp} \widehat{\chi_E} \subset p\mathbb{Z}_n \cup q\mathbb{Z}_n$ *then* $\operatorname{supp} \widehat{\chi_E}$ *is an extendable domain.*

Proof. If $p, q \in \operatorname{supp} \widehat{\chi_E}$ then, applying Lemma 2.15 for $a = p$, $b = q$, we get that $\operatorname{supp} \widehat{\chi_E} \cap pq\mathbb{Z}_n \neq \{0\}$, which implies that $pq \in \operatorname{supp} \widehat{\chi_E}$. Then we can apply Lemma 2.16 to get that $\operatorname{supp} \widehat{\chi_E}$ is indeed an extendable domain.

So we can suppose by symmetry that $q \notin \operatorname{supp} \widehat{\chi_E}$. Then $\operatorname{supp} \widehat{\chi_E} \subset p\mathbb{Z}_n \cup q\mathbb{Z}_n$ implies that $\operatorname{supp} \widehat{\chi_E} \subset p\mathbb{Z}_n \cup qd\mathbb{Z}_n$. Then, in case of $d \neq p$ by Lemma 2.14, in case of $d = p$ clearly, we have $\operatorname{supp} \widehat{\chi_E} \subset p\mathbb{Z}_n$ or $\operatorname{supp} \widehat{\chi_E} \subset qd\mathbb{Z}_n$.

If $\operatorname{supp} \widehat{\chi_E} \subset qd\mathbb{Z}_n$ then $\operatorname{supp} \widehat{\chi_E} = \langle qd \rangle_n \cup \{0\}$ or $\operatorname{supp} \widehat{\chi_E} = \{0\}$, so we are done by Lemma 2.11.

So we can suppose that $\{0\} \neq \operatorname{supp} \widehat{\chi_E} \subset p\mathbb{Z}_n$. If $p \in \operatorname{supp} \widehat{\chi_E}$ then by Corollary 2.12 $\operatorname{supp} \widehat{\chi_E}$ is an extendable domain, so we can suppose that $p \notin \operatorname{supp} \widehat{\chi_E}$. Then, by Fact 2.6, $\operatorname{supp} \widehat{\chi_E}$ can be only $\langle pd \rangle_n \cup \{0\}$ or $\langle pq \rangle_n \cup \{0\}$ or $\langle pq \rangle_n \cup \langle pd \rangle_n \cup \{0\}$ with $d \neq 1, q$. The last case is impossible by Lemma 2.14 (for $a = pq, b = pd$), while in the first two cases Lemma 2.11 implies that $\operatorname{supp} \widehat{\chi_E}$ is an extendable domain. □

The following lemma about the possible support of the Fourier Transform of characteristic functions on $\mathbb{Z}_n$ is the key for handling the hardest case when n is the product of three distinct primes. This statement might be useful in other applications, too.

Lemma 2.18. *Suppose p, q and r are pairwise coprime, but not necessarily primes. Let $n = pqr$ and let $E \subset \mathbb{Z}_n$. Then*

$$p, q \in \operatorname{supp} \widehat{\chi_E} \subset p\mathbb{Z}_n \cup q\mathbb{Z}_n \cup r\mathbb{Z}_n \Longrightarrow (\exists z \in \{1, 2, \dots, r-1\}) \;\; zpq \in \operatorname{supp} \widehat{\chi_E}.$$

Proof. Suppose that for each $z = 1, 2, \dots, r-1$ we have

$$0 = \widehat{\chi_E}(zpq) = \sum_{c=0}^{r-1} \sum_{k=0}^{pq-1} \chi_E(kr + c) e^{-2\pi i \frac{(kr+c)zpq}{pqr}} = \sum_{c=0}^{r-1} \left(\sum_{k=0}^{pq-1} \chi_E(kr + c) \right) \left(e^{-2\pi i \frac{z}{r}} \right)^c.$$

This implies that $\sum_{k=0}^{pq-1} \chi_E(kr + c)$ must be the same for each $c \in \mathbb{Z}_r$; that is,

$$\sum_{k=0}^{pq-1} \chi_E(kr + c_1) - \chi_E(kr + c_2) = 0 \qquad (c_1, c_2 \in \mathbb{Z}_r). \tag{9}$$

For each $j \in \mathbb{Z}_n$ ($n = pqr$) let $(a_j, b_j, c_j) \in \mathbb{Z}_p \times \mathbb{Z}_q \times \mathbb{Z}_r$ be the unique triple such that

$$j = a_j \bmod p, \qquad j = b_j \bmod q \quad \text{and} \quad j = c_j \bmod r,$$

and let ϕ be the inverse of the above $\mathbb{Z}_n \to \mathbb{Z}_p \times \mathbb{Z}_q \times \mathbb{Z}_r$ bijections; that is, $\phi(a, b, c)$ ($a \in \mathbb{Z}_p, b \in \mathbb{Z}_q, c \in \mathbb{Z}_r$) is the unique element of $\mathbb{Z}_n$ for which

$$\phi(a, b, c) = a \bmod p, \qquad \phi(a, b, c) = b \bmod q \quad \text{and} \quad \phi(a, b, c) = c \bmod r.$$

Since $\operatorname{supp} \widehat{\chi_E} \subset p\mathbb{Z}_n \cup q\mathbb{Z}_n \cup r\mathbb{Z}_n$, χ_E can be written as $\chi_E = f + g + h$, where f is qr-periodic, g is pr periodic and h is pq-periodic.

Since f is qr-periodic, $f(\phi(a, b, c))$ does not depend on a, so $f \circ \phi$ can be written in the form $f(\phi(a, b, c)) = F(b, c)$. Similarly $g \circ \phi$ and $h \circ \phi$ can be written as $g(\phi(a, b, c)) = G(a, c)$ and $h(\phi(a, b, c)) = H(a, b)$. So using the notation $E' = \phi^{-1}(E) \subset \mathbb{Z}_p \times \mathbb{Z}_q \times \mathbb{Z}_r$ we get that

$$\chi_{E'}(a, b, c) = F(b, c) + G(a, c) + H(a, b) \qquad a \in \mathbb{Z}_p, b \in \mathbb{Z}_q, c \in \mathbb{Z}_r.$$

We claim that there exist $c_1, c_2 \in \mathbb{Z}_r$ such that neither the $\mathbb{Z}_q \to \mathbb{R}$ function $F(\cdot\,, c_1) - F(\cdot\,, c_2)$, nor the $\mathbb{Z}_p \to \mathbb{R}$ function $G(\cdot\,, c_1) - G(\cdot\,, c_2)$ is constant. Indeed, $F(\cdot\,, c_1) - F(\cdot\,, c_2)$ being constant defines an equivalence relation on $\mathbb{Z}_r$ and so does $G(\cdot\,, c_1) - G(\cdot\,, c_2)$ being constant. If there is only one equivalence class w.r.t. the first relation then F can be written as $F(b, c) = u(b) + v(c)$ which implies

$$\chi_E(j) = \chi_{E'}(a_j, b_j, c_j) = v(c_j) + G(a_j, c_j) + u(b_j) + H(a_j, b_j),$$

and this would in turn imply $\widehat{\chi_E}(p) = 0$, contradicting our assumption. Hence there are at least two classes w.r.t. the first relation. Similarly there are two classes w.r.t. the second relation and using Fact 2.10 we obtain our claim.

On the other hand, since

$$(F(b, c_1) - F(b, c_2)) + (G(a, c_1) - G(a, c_2)) = \chi_{E'}(a, b, c_1) - \chi_{E'}(a, b, c_2) \in \{-1, 0, 1\}$$

for any $a \in \mathbb{Z}_p, b \in \mathbb{Z}_q$, we have

$$\mathrm{Range}(F(\cdot\,, c_1) - F(\cdot\,, c_2)) + \mathrm{Range}(G(\cdot\,, c_1) - G(\cdot\,, c_2)) \subset \{-1, 0, 1\}.$$

Since by the previous paragraph $\mathrm{Range}(F(\cdot\,, c_1) - F(\cdot\, c_2))$ and $\mathrm{Range}(G(\cdot\,, c_1) - G(\cdot\,, c_2))$ have at least two elements, this implies that they must be of the form

$$\mathrm{Range}(F(\cdot\,, c_1) - F(\cdot\,, c_2)) = \{A, A + 1\},$$

$$\mathrm{Range}(G(\cdot\,, c_1) - G(\cdot\,, c_2)) = \{-A, -A - 1\}$$

for some $A \in \mathbb{R}$.

Let $l_1 \in \{1, \ldots, q-1\}$ be the number of elements $b \in \mathbb{Z}_q$ for which $F(b, c_1) - F(b, c_2)) = A$ and $l_2 \in \{1, \ldots, p-1\}$ be the number of elements $a \in \mathbb{Z}_p$ for which $G(a, c_1) - G(a, c_2)) = -A$.

Then, combining this with (9) we get

$$\begin{aligned}
0 &= \sum_{k=0}^{pq-1} \chi_E(kr + c_1) - \chi_E(kr + c_2) \\
&= \sum_{a \in \mathbb{Z}_p} \sum_{b \in \mathbb{Z}_q} \chi_{E'}(a, b, c_1) - \chi_{E'}(a, b, c_2) \\
&= \sum_{a \in \mathbb{Z}_p} \sum_{b \in \mathbb{Z}_q} F(b, c_1) - F(b, c_2) + G(a, c_1) - G(a, c_2) \\
&= pl_1 A + p(q - l_1)(A + 1) + ql_2(-A) + q(p - l_2)(-A - 1) \\
&= -l_1 p + l_2 q,
\end{aligned}$$

which is a contradiction since $l_1 p$ cannot be divisible by q. □

Lemma 2.19. *Let $n = pqr$ with p, q, r three distinct primes, $E \subset \mathbb{Z}_n$. Then*

$$p, q, r \in \mathrm{supp}\, \widehat{\chi_E} \subset p\mathbb{Z}_n \cup q\mathbb{Z}_n \cup r\mathbb{Z}_n \Longrightarrow \mathrm{supp}\, \widehat{\chi_E} = p\mathbb{Z}_n \cup q\mathbb{Z}_n \cup r\mathbb{Z}_n.$$

Proof. Suppose that $p, q, r \in \mathrm{supp}\, \widehat{\chi_E} \subset p\mathbb{Z}_n \cup q\mathbb{Z}_n \cup r\mathbb{Z}_n$. By Lemma 2.18 we have $\langle pq \rangle_n \cup \langle pr \rangle_n \cup \langle qr \rangle_n \subset \mathrm{supp}\, \widehat{\chi_E}$. Since E cannot be empty, $\langle pqr \rangle_n \subset \mathrm{supp}\, \widehat{\chi_E}$. Since $p\mathbb{Z}_n \cup q\mathbb{Z}_n \cup q\mathbb{Z}_n = \langle p \rangle_n \cup \langle q \rangle_n \cup \langle r \rangle_n \cup \langle pq \rangle_n \cup \langle pr \rangle_n \cup \langle qr \rangle_n \cup \langle pqr \rangle_n$, this completes the proof. □

Lemma 2.20. *If $a, b, c \in \mathbb{Z}$ are pairwise coprime then $a\mathbb{Z}_n \cup b\mathbb{Z}_n \cup c\mathbb{Z}_n$ is an extendable domain.*

Proof. Let $A = a\mathbb{Z}_n \cup b\mathbb{Z}_n \cup c\mathbb{Z}_n$ and let $h : A \to \mathbb{R}/\mathbb{Z}$ be additive. Then it is easy to show that for $\alpha = h(a)/a, \beta = h(b)/b, \gamma = h(c)/c$ we have

$$h(ma) = \alpha ma, \quad h(mb) = \beta mb, \quad h(mc) = \gamma mc \pmod 1 \quad (m \in \mathbb{Z}). \tag{10}$$

It is enough to find $u, v, w \in \mathbb{Z}$ such that

$$\alpha + \frac{u}{a} = \beta + \frac{v}{b} = \gamma + \frac{w}{c} \tag{11}$$

since then $h(x) = Lx \pmod 1$ would follow for $L = \alpha + \frac{u}{a} = \beta + \frac{v}{b} = \gamma + \frac{w}{c}$ from (10).

For $v \in \mathbb{Z}$ there exist u and w such that (11) holds if

$$va = \alpha ab - \beta ab \pmod b \quad \text{and } vc = \gamma bc - \beta bc \pmod b,$$

which hold for some $v \in \mathbb{Z}$ if and only if

$$\alpha ab - \beta ab \in \mathbb{Z}, \quad \gamma bc - \beta bc \in \mathbb{Z} \text{ and } c(\alpha ab - \beta ab) = a(\gamma bc - \beta bc) \pmod b. \tag{12}$$

Using (10) for $m = a, b, c$ we get that

$$\alpha ab = \beta ab, \qquad \beta bc = \gamma bc \quad \text{and} \quad \alpha ac = \beta ac \qquad \pmod 1,$$

which implies (12) and so completes the proof. □

Proof. (Proposition 2.4) By Corollary 2.12 we are done if n is a power of an odd prime or if $1 \in \operatorname{supp} \widehat{\chi_E}$. So we can suppose that $1 \notin \operatorname{supp} \widehat{\chi_E}$ and $n = pqr$, where p and q are different primes and r is a prime or $r = 1$. If $r = 1$ or $r = p$ or $r = q$ then n equals pq or p^2q or pq^2 and so $1 \notin \operatorname{supp} \widehat{\chi_E}$ implies that $\operatorname{supp} \widehat{\chi_E} \subset p\mathbb{Z}_n \cup q\mathbb{Z}_n$, hence we are done by Lemma 2.17.

Therefore we can suppose that $1 \notin \operatorname{supp} \widehat{\chi_E}$ and $n = pqr$, where p, q and r are distinct primes. Then we have $\operatorname{supp} \widehat{\chi_E} \subset p\mathbb{Z}_n \cup q\mathbb{Z}_n \cup r\mathbb{Z}_n$.

If $p, q, r \in \operatorname{supp} \widehat{\chi_E}$ then, by Lemma 2.19, we have $\operatorname{supp} \widehat{\chi_E} = p\mathbb{Z}_n \cup q\mathbb{Z}_n \cup r\mathbb{Z}_n$, which is an extendable domain by Lemma 2.20.

Otherwise, we can suppose by symmetry that $r \notin \operatorname{supp} \widehat{\chi_E}$ and so $\operatorname{supp} \widehat{\chi_E} \subset p\mathbb{Z}_n \cup q\mathbb{Z}_n$. Then we are done by Lemma 2.17

This completes the proof of Proposition 2.4 and so also the proof of Theorem 2.1. □

If n is even then we get positive results for small n:

Proposition 2.21. *For $n = 2, 4, 6, 8$ and 10 every subset of $\mathbb{Z}_n$ is uniquely determined up to translations by its 3-deck.*

For $n = 2, 4$ and 6 this statement follows very easily from the definition of 3-deck. For both $n = 8$ and $n = 10$ one can provide proofs using the lemmas and the method of this section. However, in these cases there are only 2^8 and 2^{10} subsets of $\mathbb{Z}_n$, so one can easily check (and we indeed did check) the statement by computer. Hence we omit the quite complicated detailed proof, in which many cases have to be distinguished and no new idea is needed.

2.2 Negative results

Theorem 2.22. *Let $n = 2k$ with $k \geq 6$ integer. Then there exists $E, F \subset \mathbb{Z}_n$ such that they are not translates of each other, however they have the same 3-deck.*

Proof. Let

$$E = \{0\} \cup \{3, 4, \ldots, k-1\} \cup \{k+1, k+2\}, \quad \text{and} \quad F = \{0, 1\} \cup \{3, 4, \ldots, k-1\} \cup \{k+2\}.$$

Since $k \geq 6$, both E and F contain a unique block of $k-3$ consecutive numbers. Thus if a translation takes E to F then this block of E must be taken to the block of F. Since these blocks are identical, the translation must be the identity. But $E \neq F$, so we proved that they are not the translates of each other.

By (2), for checking that E and F have the same 3-deck we have to show that for the Fourier Transforms of their characteristic function we have

$$s_1 + s_2 + s_3 = 0 \pmod{2k} \Longrightarrow \widehat{\chi_E}(s_1)\widehat{\chi_E}(s_2)\widehat{\chi_E}(s_3) = \widehat{\chi_F}(s_1)\widehat{\chi_F}(s_2)\widehat{\chi_F}(s_3). \tag{13}$$

Letting $z = \zeta_{2k}^{-s} = e^{-2\pi i \frac{s}{2k}}$ we have

$$\begin{aligned} \widehat{\chi_E}(s) &= \zeta_{2k}^{-0s} + \left(\zeta_{2k}^{-3s} + \zeta_{2k}^{-4s} + \ldots + \zeta_{2k}^{-(k-1)s}\right) + \zeta_{2k}^{-(k+1)s} + \zeta_{2k}^{-(k+2)s} \qquad (14) \\ &= 1 + (z^3 + z^4 + \ldots + z^{k-1}) + z^{k+1} + z^{k+2} = (1 - z + z^3)(1 + z + \ldots + z^{k-1}), \end{aligned}$$

and similarly

$$\widehat{\chi_F}(s) = 1 + z + (z^3 + z^4 + \ldots + z^{k-1}) + z^{k+2} = (1 - z^2 + z^3)(1 + z + \ldots + z^{k-1}). \tag{15}$$

If s is even but $s \neq 0 \pmod{2k}$ then

$$1 + z + \ldots + z^{k-1} = \frac{z^k - 1}{z - 1} = \frac{e^{-2\pi i \frac{ks}{2k}} - 1}{e^{-2\pi i \frac{s}{2k}} - 1} = 0,$$

and so $\widehat{\chi_E}(s) = \widehat{\chi_F}(s) = 0$.

Since $s_1 + s_2 + s_3 = 0 \pmod{2k}$ implies that at least one of s_1, s_2 and s_3 is even, we get that (13) clearly holds unless at least one of s_1, s_2 and s_3 is zero.

So suppose that at least one of s_1, s_2 and s_3 is zero. Then, in order to check (13), we have to show that

$$\widehat{\chi_E}(s)\widehat{\chi_E}(-s) = \widehat{\chi_F}(s)\widehat{\chi_F}(-s) \qquad (s \in \mathbb{Z}_{2k}). \tag{16}$$

This is just a restatement of the fact that E and F have the same 2-deck, which is clearly true as E is a translate of $-F$. □

Theorem 2.23. *Let $n = pqrd$ with p, q two distinct primes and $r, d > 1$ integers. Then there exist $E, F \subset \mathbb{Z}_n$ such that they are not translates of each other, however they have the same 3-deck.*

Proof. Let

$$A = \left\{ \frac{l_1 n}{q} + kd : k \in \{0, 1, \ldots, r-1\}, l_1 \in \{0, 1, \ldots, q-1\} \right\},$$

$$B = \left\{ \frac{l_2 n}{p} + kd : k \in \{0, 1, \ldots, r-1\}, l_2 \in \{0, 1, \ldots, p-1\} \right\},$$

$$E = A \cup (B+1) \qquad \text{and} \qquad F = A \cup (B+d+1).$$

Then

$$\widehat{\chi_E}(s) = \underbrace{\left(\sum_{k=0}^{r-1} e^{-2\pi i \frac{kds}{n}}\right)}_{0 \text{ if } pq|s \text{ but } pqr\nmid s} \cdot \left(\underbrace{\sum_{l_1=0}^{q-1} e^{-2\pi i \frac{l_1 s}{q}}}_{q \text{ if } q|s,\ 0 \text{ if } q\nmid s} + e^{-2\pi i \frac{s}{n}} \cdot \underbrace{\sum_{l_2=0}^{p-1} e^{-2\pi i \frac{l_2 s}{p}}}_{p \text{ if } p|s,\ 0 \text{ if } p\nmid s} \right)$$

and

$$\widehat{\chi_F}(s) = \left(\sum_{k=0}^{r-1} e^{-2\pi i \frac{kds}{n}}\right) \cdot \left(\sum_{l_1=0}^{q-1} e^{-2\pi i \frac{l_1 s}{q}} + e^{-2\pi i \frac{s(d+1)}{n}} \cdot \sum_{l_2=0}^{p-1} e^{-2\pi i \frac{l_2 s}{p}} \right).$$

Thus

$$\widehat{\chi_E}(s) \neq 0 \Longleftrightarrow \widehat{\chi_F}(s) \neq 0 \Longleftrightarrow (p|s \text{ or } q|s) \text{ and } (pq\nmid s \text{ or } pqr|s),$$

hence

$$\operatorname{supp} \widehat{\chi_E} = \underbrace{\{s \in \mathbb{Z}_n : p|s, q\nmid s\}}_{S_p} \cup \underbrace{\{s \in \mathbb{Z}_n : q|s, p\nmid s\}}_{S_q} \cup \underbrace{\{s \in \mathbb{Z}_n : pqr|s\}}_{S_{pqr}}.$$

For checking that E and F have the same 3-deck we have to show that

$$s_1 + s_2 + s_3 = 0 (\operatorname{mod} n) \Longrightarrow \widehat{\chi_E}(s_1)\widehat{\chi_E}(s_2)\widehat{\chi_E}(s_3) = \widehat{\chi_F}(s_1)\widehat{\chi_F}(s_2)\widehat{\chi_F}(s_3). \tag{17}$$

We have nothing to prove unless $s_1, s_2, s_3 \in \operatorname{supp} \widehat{\chi_E}$. So suppose that $s_1, s_2, s_3 \in \operatorname{supp} \widehat{\chi_E}$.

Note that $\widehat{\chi_E}(s) = \widehat{\chi_F}(s)$ unless $s \in S_p$. Thus if none of s_1, s_2, s_3 are in S_p then we are done.

It is impossible that exactly one of them is in S_p (because of divisibility by q).

If two of them, say s_1 and s_2, are in S_p then s_3 is in S_p or in S_{pqr}. In both cases it is easy to check (17).

Finally, suppose that $F = E + t \pmod n$. Since both E and F have qr elements that are 0 mod d and pr elements that are 1 mod d, t must be of the form $t = md$. Thus we must have $A = A + md$ and $B + d = B + md \pmod n$. But B consists of blocks which are arithmetic progressions of length r and step d, and these are regularly spaced at intervals of length qrd. Hence $B + d = B + md \pmod n$ can only happen if $d - md$ is a multiple of qrd, or, equivalently, if $m = 1 \bmod qr$. On the other hand, by the similar structure of A it follows that $m = 0 \bmod pr$, which is a contradiction. □

2.3 Results about real-valued functions

Given the results we have proved so far we can also characterize those values of n for which the 3-deck determines the characteristic function of any nonempty subset of $\mathbb{Z}_n$ up to translation even among all $\mathbb{Z}_n \to \mathbb{R}$ functions.

Theorem 2.24. *For $n \geq 3$ the following three statements are equivalent.*

(i) n is a power of an odd prime or n is the product of at most 3 (not necessarily distinct) odd primes.

(ii) The support of the Fourier Transform of any characteristic function on $\mathbb{Z}_n$ is an extendable domain.

(iii) If for some $\emptyset \neq E \subset \mathbb{Z}_n$ and $g : \mathbb{Z}_n \to \mathbb{R}$, χ_E and g have the same 3-deck then they are translates of each other.

Proof. (i)⇒(ii): This is exactly Proposition 2.4.

(ii)⇒(iii): If $E \neq \emptyset$ then $\widehat{\chi_E}(0) \neq 0$ and so by Lemma 2.3 (2) we get that χ_E and g are indeed translates of each other.

(iii)⇒(i): If n is odd and (i) does not hold then, by Theorem 2.23, there exists counterexamples for (iii), even with g being a characteristic function.

Now suppose that $n > 2$ is even and let $E = \{1, 2, \ldots, n/2\}$. It is easy to check that $\operatorname{supp} \widehat{\chi_E} = \{0, 1, 3, 5, \ldots, n-1\}$. Let

$$h_\alpha(l) = \begin{cases} \alpha & \text{if} \quad l = 1, \\ -\alpha & \text{if} \quad l = -1, \\ 0 & \text{otherwise.} \end{cases}$$

Let g_α be the inverse Fourier Transform of the function $G_\alpha(l) = e^{2\pi i h_\alpha(l)} \cdot \widehat{\chi_E}(l)$ on $\mathbb{Z}_n$. Since h_α is an odd function, $G_\alpha(-l) = \overline{G_\alpha(l)}$, and so g_α is a real valued function. Since h_α is additive on $\operatorname{supp} \widehat{\chi_E}$, the right hand side of (3) holds for $k = 3$, f and $g = g_\alpha$, and so $N_{\chi_E,3} = N_{g_\alpha,3}$. This way we get continuum many distinct $g_\alpha : \mathbb{Z}_n \to \mathbb{R}$ functions. Since χ_E has only finitely many translates (iii) cannot hold for every g_α. □

Example 2.25. Let $n \geq 4$ be arbitrary, $f = 0$ on $\mathbb{Z}_n$ and $g(k) = \cos \frac{2k\pi}{n}$ $(k \in \mathbb{Z}_n)$. Then clearly $\widehat{f} = 0$ and one can check that

$$\widehat{g}(l) = \begin{cases} n/2 & \text{if} \quad l = 1, \\ -n/2 & \text{if} \quad l = -1, \\ 0 & \text{otherwise.} \end{cases}$$

Then it is easy to check that the righthand-side of (3) holds for $k = 3$, so $N_{f,3} = N_{g,3}$, however f and g are clearly not translates of each other.

This shows that if we allow $E = \emptyset$ in (iii) of Theorem 2.24 then (i)⇒(iii) is not true any more.

Remark 2.26. It is proved in [JK] (Proposition 2.7) that if f is the characteristic function of a subset of $\mathbb{R}$ of finite measure and $g \in L^1(\mathbb{R})$ is a nonnegative function such that $N_{f,3} = N_{g,3}$ then there g must be equal to a characteristic function almost everywhere.

One can check that the same proof works on $\mathbb{Z}_n$ as well. This has the following consequences.

1. The characteristic functions on $\mathbb{Z}_n$ are determined up to translation by their 3-deck among nonnegative functions if and only if they are determined up to translation among characteristic functions; that is, by Corollary 1.1, if and only if n is a power of an odd prime or n is the product of at most three (not necessarily distinct) odd primes or $n \in \{2, 4, 6, 8, 10\}$.

2. Only the (at most finitely many) characteristic functions can be nonnegative among the (continuum many) g_α functions of the proof of (iii)⇒(i) of Theorem 2.24.

3 The percentage of subsets of $\mathbb{Z}_n$ not determined by their 3-deck up to translation

As we mentioned in the Introduction, in [RS1] Radcliffe and Scott proved that almost all subsets of $\mathbb{Z}_n$ are determined up to translation by their 3-deck. More specifically they proved that the fraction of subsets of $\mathbb{Z}_n$ whose Fourier Transform vanishes somewhere is at most $C_\epsilon/n^{1/2-\epsilon}$, for any $\epsilon > 0$, and, since any set whose FT does not vanish is uniquely determined from its 3-deck, this proves that a fraction at most $C_\epsilon/n^{1/2-\epsilon}$ of the possible sets are not determined by their 3-deck.

Furthermore, it is easy to see that the probability of having the FT of a random subset of $\mathbb{Z}_n$ vanish somewhere is at least $C/\sqrt{n}$. For this one takes n to be even and examines the FT of the random set at $n/2$. The vanishing there is equivalent to a random subset of a set of $n/2$ ones and $n/2$ minus-ones having a vanishing sum. This probability is equal to $\binom{n}{n/2}/2^n \sim C/\sqrt{n}$.

However, here we show that the probability that a random subset of $\mathbb{Z}_n$ is not uniquely determined up to translation by its 3-deck is exponentially small (Theorem 3.4). When talking about random sets in this section we mean that all subsets of $\mathbb{Z}_n$ are equally probable. This is the same as tossing an independent fair coin for each element of $\mathbb{Z}_n$ to decide membership in the random set.

Lemma 3.1. *Suppose $u_1, \ldots, u_m$ are vectors in a vector space V and that the collection $u_1, \ldots, u_D$, $D \leq m$, are linearly independent. Suppose also that ϵ_j, $j = 1, \ldots, m$, are $\{0,1\}$-valued random variables which are unbiased and independent. Then*

$$\mathbb{P}r\left[\sum_{j=1}^{m} \epsilon_j u_j = 0\right] \leq 2^{-D}. \tag{18}$$

Proof. Since $u_1, \ldots, u_D$ are independent, for any fixed $\epsilon_{D+1}, \ldots, \epsilon_m$, the 2^D possible values of $\sum_{j=1}^{m} \epsilon_j u_j$ are all distinct, so only at most one of them can be zero. □

Corollary 3.2. *If $E \subseteq \mathbb{Z}_n$ is random then*

$$\mathbb{P}r\left[\widehat{\chi_E}(k) = 0\right] \leq 2^{-Cn/(k,n)\log\log n},$$

for some absolute constant $C > 0$ and for all $k \in \mathbb{Z}_n$.

Proof. Let $\omega = e^{2\pi i/n}$. Then

$$\widehat{\chi_E}(k) = \sum_{j=0}^{n-1} \epsilon_j \omega^{kj}, \tag{19}$$

where the ϵ_j, $j = 0, \ldots, n-1$, are independent, unbiased, $\{0,1\}$-valued random variables.

It is well known that the algebraic order of ω^k over the field $\mathbb{Q}$ is $\phi(n/(k,n))$, where $\phi(n)$ is the Euler function which counts how many numbers from 1 to n are coprime to n. It is also well known [HW] that $\phi(n) \geq Cn/\log\log n$. This means that if $P(x)$ is a polynomial with rational coefficients and degree $< Cn/(k,n)\log\log n$ then $P(\omega^k) \neq 0$. This, in turn, implies that the complex numbers

$$1, \omega^k, \omega^{2k}, \ldots, \omega^{(Cn/(k,n)\log\log n)\cdot k}$$

are $\mathbb{Q}$-linearly independent. Applying Lemma 3.1 to the random sum (19) in the vector space $\mathbb{C}$ over $\mathbb{Q}$ we get our result. □

Corollary 3.3. *If n is odd then the probability that a random subset of $\mathbb{Z}_n$ is not uniquely determined by its 3-deck is at most $2^{-Cn/\log\log n}$.*

Proof. We make use of a result of Grünbaum and Moore [GM] (see §1.1) which states that if n is odd, $E \subseteq \mathbb{Z}_n$, and $\widehat{\chi_E}(1) \neq 0$ then E is determined by its 3-deck. The rest follow from Corollary 3.2 with $k = 1$. □

For arbitrary n we lose a little in the exponent. Probably this is unnecessary.

Theorem 3.4. *If E is a random subset of $\mathbb{Z}_n$ the probability that E is not determined by its 3-deck is at most*

$$2^{-C_\epsilon n^{1-\epsilon}},$$

for any $\epsilon > 0$.

For the proof we use some notions (recall Definition 2.2 and Notation 2.5) and lemmas from §2.1 and also some new ones. Write

$$A_x = \{k \in \mathbb{Z}_n : (k, n) \leq x\},$$

and write $\mathrm{GAP}(B)$ for the size of the largest interval contained in the complement of $B \subseteq \mathbb{Z}_n$.

Lemma 3.5. $\mathrm{GAP}(A_{d(n)}) \leq d(n)$*, where $d(n)$ denotes the number of divisors of n.*

Proof. Suppose that $I = \{a, a+1, \ldots, a+d(n)\} \subseteq A^c_{d(n)}$ is an interval of size $d(n)+1$, and $i, j \in I$, $i \neq j$. Then $(i, n) > d(n)$ and $(j, n) > d(n)$. It follows that $(i, n) \neq (j, n)$, otherwise we would have $|i - j| \geq (i, n) > d(n)$, which cannot happen as all distances in I are at most $d(n)$. Thus, to each $i \in I$ there corresponds a different divisor of n, namely (i, n). But this cannot happen as I has $d(n) + 1$ members but there are only $d(n)$ different divisors of n. □

Lemma 3.6. *If $\{0, 1, \ldots, d\} \subset A \subset \mathbb{Z}_n$ and $\mathrm{GAP}(A) \leq d$ then A is an extendable domain.*

Proof. Let $h : A \to \mathbb{R}/\mathbb{Z}$ be an additive function. We prove that h satisfies $h(j) = jh(1) \pmod 1$, for all $j \in A$, which means, by definition, that A is indeed an extendable domain.

If $1 \leq j \leq d$ then $h(j) = h(j-1) + h(1) \pmod 1$, since $1, j-1, j$ all belong to A, hence by induction we have our claim for j up to d. Suppose $d < J \in A$ and that we have proved $h(j) = jh(1) \pmod 1$ for all $j \in A$, $j < J$. Since $\mathrm{GAP}(A) \leq d$, it follows that there is a $j' \in A \cap \{J - d, \ldots, J - 1\}$. By our inductive assumption we have $h(j') = j'h(1) \pmod 1$ and we also know $h(J - j') = (J - j')h(1) \pmod 1$, as $J - j' \leq d$. The additivity of h on A implies $h(J) = Jh(1) \pmod 1$. □

Lemma 3.7. *If $E \subset \mathbb{Z}_n$ and $\{1, 2, \ldots, d(n)\} \subset \operatorname{supp} \widehat{\chi_E}$ then E is determined up to translation by its 3-deck.*

Proof. By Fact 2.6, $\{1, 2, \ldots, d(n)\} \subset \operatorname{supp} \widehat{\chi_E}$ implies that $A_{d(n)} \subset \operatorname{supp} \widehat{\chi_E}$. Thus by Lemma 3.5, $\mathrm{GAP}(\operatorname{supp} \widehat{\chi_E}) \leq d(n)$. Hence by Lemma 3.6, $\operatorname{supp} \widehat{\chi_E}$ is an extendable domain. Therefore by Lemma 2.3 (1), E is determined up to translation by its 3-deck. □

Proof. (Theorem 3.4) By Corollary 3.2,

$$\begin{aligned}\mathbb{P}r\left[\exists j \in \{1,2,\ldots,d(n)\} : \widehat{\chi_E}(j) = 0\right] &\leq d(n)2^{-Cn/d(n)\log\log n} \\ &\leq C_\epsilon n^\epsilon 2^{-C_\epsilon n^{1-\epsilon}} \\ &\leq 2^{-C_{\epsilon'} n^{1-\epsilon'}},\end{aligned}$$

where $\epsilon' > 0$ is again arbitrary, and we used the fact that $d(n) = O(n^\epsilon)$ for all $\epsilon > 0$ [HW]. By Lemma 3.7, this completes the proof of Theorem 3.4. □

References

[ACKR] N. Alon, Y. Caro, I. Krasikov and Y. Roditty, Combinatorial reconstruction problems, J. Combin. Theory Ser. B **47** (1989), 2, 153–161.

[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), no. 3, 310–323.

[HW] G.H. Hardy and E.M. Wright, *An introduction to the theory of numbers*, Fifth Edition, Oxford Univ. Press, 1978.

[JK] P. Jaming and M.N. Kolountzakis, Reconstruction of functions from their triple correlations, New York J. Math. **9** (2003), 149-164.

[L] H.W. Lenstra, Generating units modulo an odd integer by addition and subtraction, Acta Arith. **64**, 4, 383–388.

[LWW] A. Lohmann, G. Weigelt and B. Wirnitzer, Speckle masking in astronomy: triple correlation theory and application, Appl. Opt. **22** (1983), 4028–4037.

[P] L. Pebody, The reconstructibility of finite abelian groups, Comb. Probab. Computing **13** (2004), 867-892.

[P2] L. Pebody, Reconstructing odd necklaces, `manuscript`.

[PRS] L. Pebody, A.J. Radcliffe and A.D. Scott, Finite subsets of the plane are 18-reconstructible, SIAM J. Discr. Math. **16** (2003), 2, 262-275.

[Pet] A. Petropulu, Higher-order spectral analysis, in *Digital Signal Processing Handbook*, V.K. Madisetti and D.B. Williams, editors, Chapman & Hall/CRCnetBASE, 1999.

[RS1] A. J. Radcliffe and A. D. Scott Reconstructing subsets of $\mathbb{Z}_n$, J. Combin. Theory Ser. A **83** (1998), no. 2, 169–187.

[RS2] A. J. Radcliffe and A. D. Scott *Reconstructing subsets of reals*, Electron. J. Combin. **6** (1999), no. 1, Research Paper 20, 7 pp. (electronic)