On the discrete Fuglede and Pompeiu problems

Gergely Kiss * Romanos Diogenes Malikiosis † Gábor Somlai ‡ Máté Vizer §

Abstract

We investigate the discrete Fuglede's conjecture and Pompeiu problem on finite abelian groups and develop a strong connection between the two problems. We give a geometric condition under which a multiset of a finite abelian group has the discrete Pompeiu property. Using this description and the revealed connection we prove that Fuglede's conjecture holds for $\mathbb{Z}_{p^n q^2}$, where p and q are different primes. In particular, we show that every spectral subset of $\mathbb{Z}_{p^n q^2}$ tiles the group. Further, using our combinatorial methods we give a simple proof for the statement that Fuglede's conjecture holds for $\mathbb{Z}_p^2$.

1 Introduction

In this article we deal with the discrete version of Fuglede's conjecture and Pompeiu problem, both originated in analysis. We build a relationship between them that helps us to provide new results for Fuglede's conjecture in the discrete setting.

The following question was asked by Pompeiu [24]. Take a continuous function f on the plane whose integral is zero on every unit disc. Does it follow that f is constant zero? The answer for this question is no, but it initiated several different type of investigations in various settings, and in some cases the answer is affirmative for an analogous question. We give an implicit characterization of the non-Pompeiu sets for finite abelian groups.

Fuglede conjectured [8] that a bounded domain $S \subset \mathbb{R}^d$ tiles the d-dimensional Euclidean space if and only if the set of $L^2(S)$ functions admits an orthogonal basis of exponential functions. This conjecture was disproved by Tao [34].

A discrete version of Fuglede's conjecture might be formulated in the following way. A subset S of a finite abelian group G tiles G if and only if the character table of G has a submatrix, whose rows are indexed by the elements of S, which is a complex Hadamard matrix. This version of Fuglede's conjecture is not only interesting for its own by also plays a crucial role in the above mentioned counterexample of Tao. Actually his counterexample (in $\mathbb{R}^5$) is based on a counterexample for elementary abelian p-groups of finite rank.

Fuglede's conjecture is especially interesting for finite cyclic groups, since e.g. every tiling of $\mathbb{Z}$ is periodic, so it goes back to a tiling of a finite cyclic group. However, not much is known for cyclic groups. A recent paper of the second author and Kolountzakis [21] shows that Fuglede's conjecture holds for any cyclic group of order $p^n q$, where p and q are different primes.

*University of Luxembourg, Faculty of Science, Mathematics Research Unit, e-mail: kigergo57@gmail.com
†Aristotle University of Thessaloniki, Department of Mathematics. e-mail: rwmanos@gmail.com
‡Eötvös Loránd University, Faculty of Science, Institute of Mathematics and MTA-ELTE Geometric and Algebraic Combinatorics Research Group. e-mail: gsomlai@cs.elte.hu
§Alfréd Rényi Institute of Mathematics, Hungarian Academy of Sciences. e-mail: vizermate@gmail.com.

Our main contribution towards Fuglede's conjecture for cyclic groups is to connect this problem with the Pompeiu problem, introduce more combinatorial ideas and verify it for yet unknown cases: cyclic groups of order $p^n q^2$, $n \geq 1$ (see Theorem 2.5).

Further using our techniques we give a neat and combinatorial proof for the previously known fact (proved by Iosevich, Mayeli and Pakianathan [12]) that Fuglede's conjecture holds for $\mathbb{Z}_p^2$ (see also Theorem 7.1).

Structure of the paper. The paper is organized as follows. Section 2 is devoted to a detailed introduction to Fuglede's conjecture and the Pompeiu problem, introducing also the discrete version of them. Further we establish a connection between the two problems. In section 3 we give some sort of solution for the Pompeiu problem for abelian groups that we apply later in Section 6. Section 4 and 5 are preparations for the proof of Theorem 2.5. In Section 4 we reduce the cases to a special one partly based on our results concerning the Pompeiu problem. In Section 5 we prove some technical lemmas, that we constantly use later. Section 6 is devoted to the main proof of Theorem 2.5. Finally, in the Appendix we give an alternative proof of Theorem 7.1.

2 Fuglede and Pompeiu problem

2.1 Fuglede's Spectral Set Conjecture

The original conjecture of Fuglede [8] was formulated as follows. Let Ω be a measurable subset of $\mathbb{R}^n$ of positive Lebesgue measure. A set $\Omega \subseteq \mathbb{R}^n$ is called *spectral* if there is a set $\Lambda \subset \mathbb{R}^n$ such that $\{e^{i\lambda \cdot x} : \lambda \in \Lambda,\ x \in \Omega\}$ is an orthogonal basis of $L^2(\Omega)$. Then $\Lambda \subseteq \mathbb{R}^n$ is called the *spectrum* of Ω.

We say that S is a *tile* of $\mathbb{R}^n$, if there is a set $T \subset \mathbb{R}^n$ such that almost every point of $\mathbb{R}^n$ can be uniquely written as $s + t$, where $s \in S$ and $t \in T$. In this case, we say that T is the *tiling complement of* S.

Fuglede's Spectral Set Conjecture (that we just call Fuglede's conjecture) [8] states the following:

Conjecture 1. Ω is spectral if and only if Ω is a tile.

The conjecture was proved by Fuglede [8] in the special case, when the tiling complement or the spectrum is a lattice in $\mathbb{R}^n$. Also it has been verified by Fuglede that the L^2-space over a triangle or a disc does not admit an orthogonal basis of exponentials. (The proof for the disc was corrected by Iosevich, Katz and Pedersen [10].) The conjecture was further verified in some other cases (see e.g. [11, 16]).

Tao [34] disproved the spectral-tile direction of the conjecture by constructing a spectral set in $\mathbb{R}^5$ that does not tile the 5 dimensional space. As an extension of Tao's work, Matolcsi [22] proved that (the same direction of) the conjecture fails in dimension 4 as well. Further, Kolountzakis and Matolcsi [14, 15] and Farkas, Matolcsi and Móra [7] provided counterexamples in dimension 3 for each direction of the conjecture.

Discrete abelian groups. Fuglede's conjecture can be naturally stated for other groups, for example $\mathbb{Z}$. These cases are not only interesting on their own, but they also have connection with the original case, since e.g. in his disproof of the 5-dimensional case, Tao constructed a spectral set in $\mathbb{Z}_3^5$ (containing 6 elements, hence not a tile, as the cardinality of any tile of a finite abelian group divides the order of the group), then he lifted this counterexample to $\mathbb{R}^5$. Similar strategy was carried out by Kolountzakis and Matolcsi in the disproof of the other direction of the original conjecture, see [15]. We also mention some examples, where Fuglede's conjecture holds. These include finite cyclic p-groups [17], $\mathbb{Z}_p \times \mathbb{Z}_p$ [12], and $\mathbb{Q}_p$ [6], the field of p-adic numbers.

Borrowing the notation from [5] and [21], we write $\mathbf{S}-\mathbf{T}(G)$ (resp. $\mathbf{T}-\mathbf{S}(G)$), if the *Spectral* $\Rightarrow$ *Tile* (resp. *Tile* $\Rightarrow$ *Spectral*) direction of Fuglede's conjecture holds in G for every bounded subset. The above mentioned connection between the conjecture on $\mathbb{R}$, on $\mathbb{Z}$ and on finite cyclic groups is summarized below [5] (where $\mathbf{T}-\mathbf{S}(\mathbb{Z}_{\mathbb{N}})$ means that $\mathbf{T}-\mathbf{S}(\mathbb{Z}_n)$ holds for every $n \in \mathbb{N}$):

$$\mathbf{T}-\mathbf{S}(\mathbb{R}) \Leftrightarrow \mathbf{T}-\mathbf{S}(\mathbb{Z}) \Leftrightarrow \mathbf{T}-\mathbf{S}(\mathbb{Z}_{\mathbb{N}}),$$

$$\mathbf{S}-\mathbf{T}(\mathbb{R}) \Rightarrow \mathbf{S}-\mathbf{T}(\mathbb{Z}) \Rightarrow \mathbf{S}-\mathbf{T}(\mathbb{Z}_{\mathbb{N}}).$$

According to this, a counterexample to the *Spectral* $\Rightarrow$ *Tile* direction in a finite cyclic group can be lifted to a counterexample in $\mathbb{R}$; on the other hand, if the same direction of the conjecture were true for every cyclic group or even in $\mathbb{Z}$, this would hold no meaning for the original conjecture in $\mathbb{R}$.

Concerning tiles in discrete groups it was proved in [23] that if S is a finite set, which tiles $\mathbb{Z}$ with tiling complement T, then T is periodic i.e. $T+N=T$ for some $N \in \mathbb{Z}$. This shows that every tiling of the integers reduces to a tile of a cyclic group $\mathbb{Z}_N$ for some $N \in \mathbb{N}$.

We also mention a related result of Rédei [29]. We say that $A_1+\ldots+A_k$ is a *factorization* of the abelian group G if every element of G can uniquely be written as the sum of one element from each A_i.

Theorem 2.1. *([29]) Let $G = A_1 + A_2 + \ldots + A_n$ be a factorization of an abelian group G, where each A_i contains 0 and is of prime cardinality. Then at least one of the sets A_i is a subgroup of G.*

Cyclic groups. Surprisingly, despite their previously described role in the discrete version of Fuglede's conjecture, not much is known for cyclic groups. A recent result of the second author and Kolountzakis [21] proved Conjecture 2 (see later) for $\mathbb{Z}_{p^n q}$. They also wrote that most probably, their result might be extended to cyclic groups of order having 2 different prime divisors but they haven't succeeded yet.

As we will mainly deal with cyclic groups, let us state the conjecture again in this setting. First let us define spectral sets and tiles in cyclic groups also.

Definition 2.2. For a set $S \subset \mathbb{Z}_N$, we say that that S is *spectral* if $L^2(S)$ has an orthogonal basis of exponentials (indexed by Λ). This is equivalent to the following two conditions to hold:

1. There is $\Lambda \subset \mathbb{Z}_N$ such that any $f : S \to \mathbb{C}$ can be written as the $\mathbb{C}$-linear combination of exponentials of the form

$$\xi_N^{\lambda \cdot x} \quad (\lambda \in \Lambda),$$

where the product $\lambda \cdot x$ is taken modulo N and $\xi_N = e^{2\pi i/N}$.

2. For any two different $\lambda, \lambda' \in \Lambda$ we have:

$$\sum_{x \in S} \xi_N^{(\lambda-\lambda')\cdot x} = 0$$

(i.e. the representations $\chi_\lambda(x) = \xi_N^{\lambda \cdot x}$ and $\chi_{\lambda'}(x) = \xi_N^{\lambda' \cdot x}$ are orthogonal).

We denote $\{\chi_\lambda \mid \lambda \in \Lambda\}$ by χ_Λ.

Remark 2.3. We note that if S is a spectral set, then $|S| = |\Lambda|$ follows from Definition 2.2. Condition 2 further implies that

$$\Lambda - \Lambda \subseteq \{0\} \cup \Big\{ x \in \mathbb{Z}_N : \widehat{1}_S(x) = 0 \Big\}, \tag{1}$$

where 1_S is the characteristic function of S, and $\widehat{f}(x) = \sum_{y \in \mathbb{Z}_N} f(y) \xi_N^{-x \cdot y}$ is the discrete Fourier transform of $f : G \mapsto \mathbb{C}$, as usual.

Definition 2.4. Let G be a discrete abelian group. We say that $S \subset G$ *tiles* G if there exists $T \subset G$ such that $S + T = G$, where $S + T$ is the set of elements of G of the form $s + t$ $(s \in S,\ t \in T)$, counted with multiplicity, so we have each $g \in G$ exactly once. In this case we say that T is a *tiling complement* of S in G.

For cyclic groups Fuglede's conjecture can be stated as follows.

Conjecture 2. For any N and $S \subset \mathbb{Z}_N$ we have that S is spectral if and only if S tiles $\mathbb{Z}_N$.

Coven and Meyerowitz conjectured [4] that if a set tiles a cyclic group of square free order, then it is a set of coset representatives for a suitable subgroup of the cyclic group. This is equivalent to the *Tiling⇒Spectral* direction of Conjecture 2, when N is square free. They proved that for every $N \in \mathbb{N}$ a subset of $\mathbb{Z}_N$ fulfilling the conditions **(T1)** and **(T2)** (presented later in Theorem 4.11) tiles $\mathbb{Z}_N$. They also conjectured that these conditions are necessary. This conjecture for N square free was proven in Terence Tao's blog[1] and answered by Izabella Łaba[2] and Aaron Meyerowitz[3]. The *Tiling⇒Spectral* direction of Conjecture 2 was also proved recently by Shi [31].

In this paper we verify Conjecture 2 for cylic groups of order $p^n q^2$ by proving the following.

Theorem 2.5. *Let p and q be two different primes. Then we have* $\mathbf{S} - \mathbf{T}$ $(\mathbb{Z}_{p^n q^2})$*, for every* $n \geq 1$.

It was proved in [4, 17] that for any two different prime numbers p, q and two integers n, m we have $\mathbf{T} - \mathbf{S}$ $(\mathbb{Z}_{p^n q^m})$. Combining this result and Theorem 2.5 we obtain:

Theorem 2.6. *Let p and q be two different primes. Then Fuglede's conjecture holds for* $\mathbb{Z}_{p^n q^2}$*,* $n \geq 1$.

Further, using our method we give, in the Appendix, a simple proof of the theorem of Iosevich, Mayeli and Pakianathan [12], stating that Fuglede's conjecture holds for $\mathbb{Z}_p^2$.

[1] `https://terrytao.wordpress.com/2011/11/19/some-notes-on-the-coven-meyerowitz-conjecture/`

[2] `https://terrytao.wordpress.com/2011/11/19/some-notes-on-the-coven-meyerowitz-conjecture/#comment-121464`

[3] `https://terrytao.wordpress.com/2011/11/19/some-notes-on-the-coven-meyerowitz-conjecture/#comment-112975`

2.2 Pompeiu problem

The problem goes back to the seminal paper of Pompeiu [24], where he asked the following question of integral geometry:

Question 1. Let K be a compact set of positive Lebesgue measure. Is it true that if $f : \mathbb{R}^2 \to \mathbb{C}$ is a continuous function that satisfies

$$\int_{\sigma(K)} f(x,y) d\lambda_x d\lambda_y = 0 \tag{2}$$

for every rigid motion σ (here λ denotes the Lebesque measure), then f is identically zero (i.e, $f \equiv 0$)?

If K is the closed disc of radius $r > 0$, then the answer is negative. It was shown by Chakalov [3] (see also [9]) that (2) holds if $f(x,y) = \sin(a(x+iy))$ where $a > 0$ and $J_1(ra) = 0$ (J_λ denotes the Bessel function of order λ). On the other hand, for every nonempty polygon (moreover, for any convex domain with at least one corner) the answer for Question 1 is affirmative by the result of Brown, Taylor and Schreiber [2]. Recently, Ramm [28] showed that there exists a $f \not\equiv 0$ function that satisfies the 3-dimensional analogue of (2) for a bounded domain $K \subseteq \mathbb{R}^3$ with $\mathcal{C}^1$-smooth boundary if and only if K is a closed ball. Extensive literature is concerned with the Pompeiu problem. For the history of the problem see [27] and the bibliographical survey [35].

In our paper we investigate the discrete version of the *Pompeiu problem* on finite abelian groups. We note that the discrete Pompeiu problem for infinite abelian groups was studied in [13, 26, 36].

The discrete version of Pompeiu problem for an abelian group G. In the sequel we denote the binary operation acting on an abelian group G by $+$ (as the usual addition).

Definition 2.7. Let G be an abelian group.

- Let S be a nonempty finite subset of G. We say that S *has the discrete Pompeiu property* (shortly S is *Pompeiu*) if, whenever $f\colon G \to \mathbb{C}$ satisfies

  $$\sum_{s\in S} f(s+x) = 0 \text{ for every } x \in G, \tag{3}$$

  then $f \equiv 0$.

  We say that S is a *non-Pompeiu set with respect to* f if $f \not\equiv 0$ and satisfies (3).

  One can define the disrcrete Pompeiu property for multisets similarly.

- We call $w : G \to \mathbb{Q}$ a *weight function*[4] defined on G. We say that w *is a Pompeiu weight function* if for any $f : G \to \mathbb{C}$

  $$\sum_{g\in G} w(g) f(g+x) = 0 \text{ for every } x \in G \tag{4}$$

[4] Every weight function is a rational constant multiple of a weight function with integer coefficients. The Pompeiu property is invariant by a nonzero constant multiple of a Pompeiu weight function. Thus we may restrict our attention for those weight functions which take its values in $\mathbb{Z}$.

implies that $f \equiv 0$.

We say that w is a *non-Pompeiu weight function with respect to* f if $f \not\equiv 0$ and satisfies (4).

Note that S is a Pompeiu set if and only if its characteristic function is a Pompeiu weight function.

Remark 2.8. We can extend the previous definition for arbitrary finite group $(G, \cdot)$ and weight function w as follows.

Let $w : G \to \mathbb{Q}$. We denote by $Cay(G, w)$ the *Cayley graph* of G with respect to w. The vertex set of $Cay(G, w)$ is G and g is connected to h by an edge with weight $w(g^{-1}h)$ for every $g, h \in G$. We denote by A_w the adjacency matrix of $Cay(G, w)$. Using the adjacency matrix A_w of $Cay(G, w)$ we may also say w is a Pompeiu weight function if and only if $A_w f = 0$ implies $f \equiv 0$. The equation $A_w f = 0$ implies that if $f \not\equiv 0$, then f is an eigenvector of A_w with eigenvalue 0. So w is a Pompeiu weight function if and only if 0 is not an eigenvalue of A_w. In the finite case this is equivalent to A_w is invertible.

We note that if G is a cyclic group, then A_w is a circulant matrix.

The set of irreducible representations of a finite abelian group G will be denoted by $\widetilde{G}$. Every irreducible representation of an abelian group is one dimensional (a character). Thus $\widetilde{G}$ is a group which is isomorphic to G. Note that $\widetilde{G}$ is usually called the *dual group* of G.

It is well-known [32] that the set of irreducible representations form an orthogonal basis of $L^2(G)$ with respect to the natural scalar product $[\psi, \chi] := \sum_{g \in G} \psi(g)\overline{\chi(g)}$ for $\psi, \chi \in \widetilde{G}$. Thus every function $f : G \to \mathbb{C}$ can be uniquely written as

$$f(x) = \sum_{\chi \in \widetilde{G}} c_\chi \chi(x) \qquad \forall x \in G, \tag{5}$$

for some $c_\chi \in \mathbb{C}$.

The following proposition can be deduced from [33]. In order to make our paper self-contained, we provide the proof.

Proposition 2.9. *If w is a non-Pompeiu weight function with respect to a function f, then w is a non-Pompeiu weight function with respect to all irreducible representations χ which has nonzero coefficient c_χ in* (5).

Proof. Let w be a non-Pompeiu with respect to a function f, then $\sum_{s \in G} w(s) f(s + x) = 0$ for every $x \in G$. Using (5) we get

$$0 = \sum_{s \in S} w(s) \sum_{\chi \in \widetilde{G}} c_\chi \chi(s + x) = \sum_{\chi \in \widetilde{G}} c_\chi \sum_{s \in S} w(s) \chi(s + x) = \sum_{\chi \in \widetilde{G}} \big(c_\chi \sum_{s \in S} w(s) \chi(s)\big) \chi(x),$$

since χ is a character. This statement holds for every $x \in G$ so we can formulate it as follows:

$$\sum_{\chi \in \widetilde{G}} \big(c_\chi \sum_{s \in S} w(s) \chi(s)\big) \chi = 0.$$

Since the irreducible representations are linearly independent over $\mathbb{C}$, the previous equation holds if and only if $\sum_{s \in S} w(s) \chi(s) = 0$ for all χ such that $c_\chi \neq 0$. Multiplying with $\chi(x)$ we obtain $\sum_{s \in S} w(s) \chi(x + s) = 0$. Since this holds for every $x \in G$, this means that w is a non-Pompeiu with respect to such χ. ∎

We note that a stronger result was proved by Babai [1] who determined the spectrum of a Cayley graphs of abelian groups. The set of the eigenvalues of $Cay(G, S)$ is $\{\sum_{s \in S} \chi(s) \mid \chi \in \widetilde{G}\}$.

Corollary 2.10. *If S is a non-Pompeiu set in a finite abelian group, then S is non-Pompeiu with respect to some irreducible representation of G.*

Remark 2.11. Since the characters (irreducible representations) play the role of exponential functions over the abelian group G, it seems reasonable that the function $\sin(ax)$ can provide an example on the disk for the original Pompeiu problem. On the other hand, it is surprising that exponential solutions were not found in literature.

2.3 Connection of the problems

Proposition 2.12. *Let G be a finite abelian group. If $S \subset G$ is a spectral set with $|S| \geq 2$, then S is a non-Pompeiu set.*

Proof. The spectral property of S requires a set of irreducible representations, of the same cardinality of S, whose restrictions to S are pairwise orthogonal. Assume χ and ψ are different irreducible representations of G, whose restriction to S are orthogonal. Since $[\chi_{|S}, \psi_{|S}] = [(\chi\bar{\psi})_{|S}, id_{|S}]$ we obtain a representation $\phi = \chi\bar{\psi}$ such that $\sum_{s \in S} \phi(s) = 0$, which leads us back to the Pompeiu problem. Thus we get that S is a non-Pompeiu set with respect to the irreducible representation ϕ. ∎

3 Pompeiu problem for cyclic groups

In this section we consider the non-Pompeiu sets for abelian groups.

Every representation of a finite abelian group is linear, so it factorizes through a faithful representation of a cyclic group since the finite subgroups of $\mathbb{C} \setminus \{0\}$ are cyclic. This shows that some sort of description for non-Pompeiu sets of finite abelian groups is given by understanding the non-Pompeiu weight functions of cyclic groups with respect to faithful representations.

Let $(\mathbb{Z}_N, +)$ be the cyclic group of order N. Note that for all $k \mid N$ there is a unique normal subgroup $\mathbb{Z}_k \leq \mathbb{Z}_N$ of order k. The group generated this way contains exactly the elements of $\mathbb{Z}_N$ divisible by $\frac{N}{k}$ so this subgroup of $(\mathbb{Z}_N, +)$ will also be denoted by $H_{\frac{N}{k}}$.

We use the following isomorphism between $\mathbb{Z}_N$ and $\widetilde{\mathbb{Z}}_N$: fix a primitive N'th root of unity α, a generator g of $\mathbb{Z}_N$. Then for any $j \in \mathbb{Z}_N$ the function $\psi_j(g^i) = \alpha^{ji}$ gives a homomorphism from $\mathbb{Z}_N$ to $\mathbb{C}^*$ hence it is an irreducible representation. Now $j \to \psi_j$ gives the isomorphism from $\mathbb{Z}_N$ to $\widetilde{\mathbb{Z}}_N$; throughout the text, we will use the isomorphism that arises from $\alpha = \xi_N$. From now on the subgroup of $\widetilde{\mathbb{Z}}_N$ isomorphic to $H \leq \mathbb{Z}_N$ will be denoted by $\widetilde{H}$.

Hereinafter we use the notion of mask polynomial.

Definition 3.1. Let G be a cyclic group and $w : G \to \mathbb{Q}$ be a weight function. We call

$$m_w(x) = \sum_{h \in G} w(h) x^h$$

the *mask polynomial* of w, where $w(h)$ denotes the weight of $h \in G$. This might be considered as an element of $\mathbb{Q}[x]/(x^n-1)$. For a (multi)set S of G we define the *mask polynomial* of S by

$$S(x) = \sum_{s \in S} c_s x^s,$$

where c_s denotes the cardinality of $s \in S$.

Let $\Phi_k(x)$ denote the k'th cyclotomic polynomial, which is of degree $\varphi(k)$, where φ denotes the Euler totient function. Note that for fixed N and prime $p \mid N$ the mask polynomial of $\mathbb{Z}_p \leq \mathbb{Z}_N$ is $\Phi_p(x^{N/p})$. The following is one of the key preliminary observations. Basically, this can be considered as a statement on roots of unity. There is a vast literature on vanishing sums of roots of unity. This particular statement gives a generalization of Theorem 3.3 of [19]. Similar results might appear in many other papers.

Proposition 3.2. *Let G be a cyclic group of order N and let α be a primitive N'th root of unity. We denote by P_N the set of prime divisors of N. Further let w be a weighted function. Then w is non-Pompeiu with respect to the faithful representation ψ_α if and only if*

$$w = \sum_{g \in G} \sum_{p \in P_N} w_{p,g} 1_{\mathbb{Z}_p + g}$$

for some $w_{p,g} \in \mathbb{Q}$, where $1_{\mathbb{Z}_p+g}$ denotes the characteristic function of the coset $\mathbb{Z}_p + g$.

Proof. The fact that w is a non-Pompeiu weight function with respect to the faithful representation ψ_α means that α is the root of the mask polynomial m_w of w, since $m_w(\alpha) = \sum_{i=0}^{N-1} w(i)\alpha^i = 0$. On the other hand, for a given $N \in \mathbb{N}$ every $p \in P_N$ we have that α is the root of the mask polynomial of $\mathbb{Z}_p \leq \mathbb{Z}_N$, that is $\Phi_p(x^{N/p})$. Indeed, α is a primitive N'th root of unity so $\alpha^{\frac{N}{p}} \neq 1$. Clearly, $\alpha^{\frac{N}{p}} \Phi_p(\alpha^{N/p}) = \Phi_p(\alpha^{N/p})$, so it implies $\Phi_p(\alpha^{N/p}) = 0$.

Then α is also a root of the polynomial $m_w(x) + \sum_{p \in P_N} a_p(x)\Phi_p(x^{N/p})$, where $a_p(x) \in \mathbb{Q}[x]$. By using Euclidean division there are polynomial $q(x), r(x) \in \mathbb{Q}[x]$ such that

$$m_w(x) = q(x)\Phi_N(x) + r(x)$$

with either $r(x)$ to be the constant zero function or $deg(r(x)) < \varphi(N)$.

The common roots of the polynomials $\Phi_p(x^{N/p})$ $(p \in P_N)$ are exactly the primitive N'th roots of unity. The multiplicity of these roots in all of these polynomials is 1. These polynomials are all in $\mathbb{Q}[x]$ so the greatest common divisor in the ring $\mathbb{Q}[x]$ of the polynomials $\Phi_p(x^{N/p})$ $(p \in P_N)$ is $\Phi_N(x)$. Thus

$$\Phi_N(x) = \sum_{p \in P_N} a_p(x)\Phi_p(x^{N/p})$$

(with some $a_p(x) \in \mathbb{Q}[x]$). Substituting this to the previous equation we obtain that $m_w(x) - \sum_{p \in P_N} q(x)a_p(x)\Phi_p(x^{N/p})$ is of degree less than $\varphi(N)$ or $m_w(x) - \sum_{p \in P_N} q(x)a_p(x)\Phi_p(x^{N/p})$ is the constant zero function. Since $\Phi_N(x)$ is the minimal polynomial of α over $\mathbb{Q}$, we have $m_w(x) - \sum_{p \in P_N} q(x)a_p(x)\Phi_p(x^{N/p}) = 0$. Thus

$$m_w(x) = \sum_{p \in P_N} q(x)a_p(x)\Phi_p(x^{N/p}).$$

It is clear that $x^k\Phi_p(x^{N/p})$ is the mask polynomial of a coset of $\mathbb{Z}_p$ for every $0 \le k < N$. Hence we have

$$w(x) = \sum_{g\in G}\sum_{p\in P_N} w_{p,g}1_{\mathbb{Z}_p+g}(x)$$

with some $w_{p,g} \in \mathbb{Q}$.

The other direction follows from the fact that $\Phi_p(\alpha^{N/p}) = 0$ for every $p \in P_N$. ∎

We note that using Proposition 3.2 one can simply construct the asymmetric minimal sums of roots of unity appearing in [19].

In terms of mask polynomials the previous proposition can be stated as follows.

Corollary 3.3. *Let $S(x) \in \mathbb{Z}_{\ge 0}[x]$ with $S(\xi_N) = 0$, where $N = p_1^{m_1}\cdots p_n^{m_n}$ and $p_1,\dots,p_n$ are primes. Then,*

$$S(x) \equiv P_1(x)\Phi_{p_1}(x^{N/p_1}) + \ldots + P_n(x)\Phi_{p_n}(x^{N/p_n}) \bmod (x^N - 1),$$

for some $P_1(x),\dots,P_n(x) \in \mathbb{Q}[x]$.

The following is an easy consequence of Proposition 3.2.

Corollary 3.4. *Let G be a cyclic group of order N and Ψ be a faithful representation of G. Assume w is a non-Pompeiu weight function with respect to Ψ. Then the restriction of w to each $\mathbb{Z}_{\mathsf{Rad}(N)}$-coset is the weighted sum of characteristic functions of $\mathbb{Z}_{p_i}$-cosets, where $\mathsf{Rad}(N)$ denotes the square free radical of N.*

We will consider $\mathbb{Z}_{\prod_{i=1}^d p_i} \cong \prod_{i=1}^d \mathbb{Z}_{p_i}$ as a grid in $\mathbb{R}^d$, whose points have integer coordinates. More precisely for $\mathbb{Z}_{\prod_{i=1}^d p_i}$ we assign

$$\mathcal{G} = \{x \in \mathbb{Z}^d \mid 0 \le x_i \le p_i - 1 \quad \text{for } 1 \le i \le d\},$$

where x_i denotes the i'th coordinate of x. The cosets of $\mathbb{Z}_{p_i}$ coincide with collections of parallel line segments (containing p_i grid points of $\mathcal{G}$. A d dimensional grid-cuboid will be a collection of 2^d grid points, whose convex hull forms a d-dimensional cuboid in $\mathbb{R}^d$. Let $P \subset \mathcal{G}$ be a d-dimensional grid-cuboid and fix a point $y \in P$. For a point of $z \in P$ let $\pi(z)$ denote the Hamming distance between z and y. Note that w can also be considered as a function from $\mathcal{G}$ to $\mathbb{Q}$.

The following statement makes the Pompeiu property for weight functions easily recognizable.

Proposition 3.5. *Let w be a non-Pompeiu weight function on the set of $\mathbb{Z}_{\prod_{i=1}^d p_i}$, where p_i are mutually different primes. If w is the weighted sum of characteristic functions of $\mathbb{Z}_{p_i}$-cosets, then for every d dimensional grid-cuboid P we have*

$$\sum_{c\in P}(-1)^{\pi(c)}w(c) = 0. \tag{6}$$

Proof. It is easy to see that each coset of $\mathbb{Z}_{p_i}$ for any $p_i \mid n$ contains either 2 or 0 elements of the cuboid P. Substituting the characteristic function of any coset of $\mathbb{Z}_{p_i}$ as a weight function to the left-hand side of (6), it is clearly reduced to a sum of at most two elements with different sign, thus (6) holds. ∎

Remark 3.6. The converse of the previous statement also holds. We leave it to the reader to work out the details of the proof .

Now we describe a few special cases which will be later used for the proof of Theorem 2.5. In the proof of the next proposition we use the following definition.

Definition 3.7. Let $S \subseteq \mathbb{Z}_N$. For every $j \in \mathbb{Z}$ and $d \mid N$, we define the following subsets

$$S_{j \bmod d} = \{s \in S : s \equiv j \bmod d\}.$$

Proposition 3.8.

(a) *Every non-Pompeiu set in $\mathbb{Z}_{pq}$ with respect to a faithful representation is either the union of cosets of $\mathbb{Z}_p$ or those of $\mathbb{Z}_q$.*

(b) *Let $N = p^m q^n$ and let S be a non-Pompeiu multiset in $\mathbb{Z}_N$ with respect to a faithful representation. Then there are some polynomials $P(x), Q(x) \in \mathbb{Z}_{\geq 0}[x]$ such that*

$$S(x) \equiv P(x)\Phi_p(x^{N/p}) + Q(x)\Phi_q(x^{N/q}) \bmod (x^N - 1).$$

Proof. (a) Let S be a non-Pompeiu set in $\mathbb{Z}_{pq}$ with respect to a faithful representation and let w be the characteristic function of S. Using Proposition 3.2 we might write $w = \sum_{i=0}^{q-1} a_i 1_{\mathbb{Z}_p+i} + \sum_{j=0}^{p-1} b_j 1_{\mathbb{Z}_q+j}$, where $a_i, b_j \in \mathbb{Q}$. Then the range of w is $Ran(w) = \{a_i + b_j \mid \ 0 \leq i \leq p-1,\ 0 \leq j \leq q-1\}$. We have that $Ran(w) = \{0, 1\}$. Thus there are at most two different a_i and two different b_j.

One can treat the case when a_i and b_j are constants as a function of i and j, respectively. Thus we may assume that $a_k < a_l$ for some $0 \leq k, l \leq p-1$. Then clearly $a_k + b_j = 0$ and $a_l + b_j = 1$ for all b_j, in particular all b_j's are the same. Therefore, we may write

$$w = b + \sum_{i=0}^{p-1} a_i 1_{\mathbb{Z}_p+i} = \sum_{i=0}^{p-1} (b + a_i) 1_{\mathbb{Z}_p+i},$$

finishing the proof of the statement.

(b) By Corollary 3.3, it is clear that

$$S(x) \equiv P(x)\Phi_p(x^{N/p}) + Q(x)\Phi_q(x^{N/q}) \bmod (x^N - 1)$$

for some $P(x), Q(x) \in \mathbb{Q}[x]$. Now we show that P and Q can be chosen such that $P(X), Q(x) \in \mathbb{Z}_{\geq 0}[x]$.

The subgroups $\mathbb{Z}_p$ and $\mathbb{Z}_q$ generate $\mathbb{Z}_{pq}$. Thus S can be written as the disjoint union

$$S = \cup_{k \in C} S_{k \bmod N/pq}$$

for $k = 0, \ldots, N/pq - 1$, where k runs through a set of representatives C of the cosets of $\mathbb{Z}_{pq}$. Thus we are given the following:

$$S_{k \bmod N/pq} = \sum_{a \in A} c_a(\mathbb{Z}_p + a) + \sum_{b \in B} d_b(\mathbb{Z}_q + b),$$

where $c_a + d_b \in \mathbb{Z}_{\geq 0}$ and A and B are sets of coset representatives of $\mathbb{Z}_p$ and $\mathbb{Z}_q$, respectively, in $\mathbb{Z}_{pq} + k$. We want to modify the coefficients c_a, d_b so that they produce the same multiset but all of them are nonnegative.

Let $e = c_a + d_b$ be one of the minimal weights of the multiset S. Then the values $d'_x = (c_a + d_x) - e$ are nonnegative for every $x \in B$ and let $c'_y = c_y + d_b$, which are nonnegative since these values are given by the multiset S only.

Now $c'_y + d'_x = ((c_a + d_x) - e) + c_y + d_b = c_y + d_x$ for every $x \in B$ and $y \in A$, finishing the proof of the lemma. ■

4 Reduction (of Fuglede's conjecture)

Before we proceed to the proof of Theorem 2.5 we make a few general observations.

Lemma 4.1. *Let G be a finite abelian group. Assume that $S \subset G$ is a spectral set having Λ as a spectrum.*

(a) $S + t$ is spectral with the same spectrum Λ for every $t \in G$.

(b) $\Lambda + \omega$ is a spectrum for S for every $\omega \in G$.

(c) S is a spectrum for Λ.

Proof. (a) If $\sum_{s \in S} \chi_\delta(s) = 0$ for some $\delta \in \Lambda - \Lambda$, then since χ_δ is a homomorphism, we have

$$\sum_{u \in (S+t)} \chi_\delta(u) = \chi_\delta(t) \sum_{s \in S} \chi_\delta(s) = 0.$$

Thus the orthogonality of the representations corresponding to the spectrum is preserved under translation.

(b) Similarly, the orthogonality of the representations corresponding to $\Lambda + \omega$ follows from the fact that $\Lambda - \Lambda = (\Lambda + \omega) - (\Lambda + \omega)$.

(c) This follows by the fact that a finite abelian group is canonically isomorphic to its double dual. ■

Corollary 4.2. *It is enough to prove Theorem 2.5 for spectral sets S with $0 \in S$ and with spectrum Λ that contains 0.*

From now on we assume $0 \in S$ and $0 \in \Lambda$.

Lemma 4.3. *Let G be a finite abelian group and let S be spectral in G, that does not generate G. Assume that for every proper subgroup H of G we have $\mathbf{S} - \mathbf{T}(H)$. Then S tiles G.*

Proof. Let S be a spectral set with orthogonal basis $\{\chi_\lambda : \lambda \in \Lambda\} = \chi_\Lambda \subset \widetilde{G}$ and let $\langle S \rangle = H < G$. Since every χ_λ is 1 dimensional, we have $\{\chi_{\lambda|H} \mid \lambda \in \Lambda\} \subseteq \widetilde{H}$ and clearly these are still orthogonal on S, since $S \subset H$. Then using that $\mathbf{S} - \mathbf{T}$(H) holds, there is a set $T \subset H$ with $S + T = H$. Now let U be a complete set of coset representatives of G/H. Then we have $S + (T + U) = G$. ■

Now we prove a similar lemma reducing the possible structure of Λ.

Lemma 4.4. *Let G by a cyclic group of order N and let us suppose that* $\mathbf{S}-\mathbf{T}(G/H)$ *holds on every proper factor G/H. Let S be a spectral set of G and Λ be the corresponding spectrum. Assume that the intersection of the kernels of the elements of χ_Λ contains $H_{\frac{N}{\ell}} \neq 1$ for some $1 < \ell \mid N$. Then S tiles G.*

Proof. By our assumptions that the elements of χ_Λ can be considered as irreducible representations of $G/H_{\frac{N}{\ell}}$ since their kernel is contained in $H_{\frac{N}{\ell}}$.

Let S_ℓ denote the multiset obtained as the image of S by the canonical projection π_ℓ of G to $G/H_{\frac{N}{\ell}} \cong H_\ell$. We claim that multiset S_ℓ is a set in H_ℓ. Indeed there can not be two elements of S in the same coset of $H_{\frac{N}{\ell}}$ since otherwise each element of χ_Λ would have the same value on them, contradicting the fact that these representations form a basis of the set of complex valued function on S. Thus S_ℓ is a set. Now it is easy to derive that $\Lambda/H_{\frac{N}{\ell}}$ is a spectrum with respect to S_ℓ in $G/H_{\frac{N}{\ell}}$ since $\chi_\lambda(\pi_\ell(s)) = \chi_\lambda(s)$ for every $s \in S$ and $\lambda \in \Lambda$.

We know $\mathbf{S}-\mathbf{T}(G/H_{\frac{N}{\ell}})$ holds. As S_ℓ is a spectral set in $G/H_{\frac{N}{\ell}}$ there is $T_\ell \subset G/H_{\frac{N}{\ell}}$ with $S_\ell + T_\ell = G/H_{\frac{N}{\ell}}$. Then if T is the preimage of T_l under the canonical projection from G to $G/H_{\frac{N}{\ell}}$, then we have $S + T = G$. ■

Observation 4.5. Let us recall that $S(x)$ is the mask polynomial of the spectral set S. Note that for $\chi \in \widetilde{G}$ of order k, then $\sum_{s\in S} \chi(s) = 0$ is equivalent to the fact that a primitive k'th root of unity ξ_k is a root of $S(x)$. Since $\Phi_k(x)$ is irreducible over $\mathbb{Q}$ we have $\Phi_k(x) \mid S(x)$ hence every primitive k'th root of unity is the root of $S(x)$ and $\sum_{s\in S} \chi'(s) = 0$ for every $\chi' \in \widetilde{G}$ of the same order. If $\Lambda \subseteq G$ is a spectrum of S, the above can be summarized to

$$S(\xi_{\mathrm{ord}(\lambda-\lambda')}) = 0, \tag{7}$$

for every $\lambda \neq \lambda'$ in a spectrum Λ, using (1).

The question whether our techniques can be generalized naturally arises. We point out here that in the next proposition we heavily use the assumption that the order of cyclic groups is divisible by at most two different primes.

Proposition 4.6. *Let G be a cyclic group of order $p^k q^\ell$ and let $|S| \geq 2$ be a spectral set. Assume further that Λ is a spectrum for S such that the elements of χ_Λ do not have a nontrivial common kernel. Then for every faithful representation ψ of G we have $\sum_{s\in S} \psi(s) = 0$.*

Proof. Note that by Observation 4.5, it is enough to prove the statement for one faithful representation.

Since the elements of χ_Λ do not have a common kernel we have a $\lambda_1 \in \Lambda$ with $p \nmid \lambda_1$. If $q \nmid \lambda_1$, then we are done so we assume $q \mid \lambda_1$. Similarly, we might assume that there exists $\lambda_2 \in \Lambda$ with $q \nmid \lambda_2$ and $p \mid \lambda_2$. In this case $\chi_{\lambda_1-\lambda_2}$ generates $\widetilde{G}$ so we have $\sum_{s\in S} \chi_{\lambda_1-\lambda_2}(s) = 0$. ■

This has the following interpretation in terms of mask polynomials.

Corollary 4.7. *Let (S, Λ) be a spectral pair in $\mathbb{Z}_N$, where $N = p^k q^\ell$, such that $0 \in S$, $0 \in \Lambda$, and each of S, Λ generates $\mathbb{Z}_N$. Then*

$$S(\xi_N) = \Lambda(\xi_N) = 0.$$

Proposition 4.8. *Let S be a spectral set in $\mathbb{Z}_N$ and let p be a prime divisor of N. Assume that for every proper factor group $\mathbb{Z}_N/H$ of $\mathbb{Z}_N$ we have $\mathbf{S}-\mathbf{T}(\mathbb{Z}_N/H)$. Assume further that S is the disjoint union of cosets of $\mathbb{Z}_p$. Then S tiles $\mathbb{Z}_N$.*

Proof. By our assumptions $|S| = pr = |\Lambda|$ for some $r \in \mathbb{N}$ and Λ is a spectrum for S. Thus at least one of the cosets of H_p contains at least r elements of Λ. By Lemma 4.1 (b) we may assume that $|H_p \cap \Lambda| \geq r$. The elements $\chi_\Lambda \subseteq \widetilde{H}_p$ are representations having a common kernel $\mathbb{Z}_p = H_{\frac{N}{p}}$. By our assumption S is the disjoint union of $\mathbb{Z}_p$-cosets, so it can be written as $\mathbb{Z}_p + B$ for some $B \subseteq \mathbb{Z}_N/\mathbb{Z}_p$. The representations in $\widetilde{H}_p \cap \chi_\Lambda$ are constant on every coset of $\mathbb{Z}_p$. Hence for every $\chi_1 \neq \chi_2 \in \widetilde{H}_p \cap \chi_\Lambda$ we have

$$\begin{aligned} 0 &= \sum_{s\in S} \chi_1(s)\bar{\chi}_2(s) = \sum_{s\in\mathbb{Z}_p+B} \chi_1(s)\bar{\chi}_2(s) = \sum_{t\in B}\sum_{x\in\mathbb{Z}_p} \chi_1(t+x)\bar{\chi}_2(t+x) \\ &= \sum_{t\in B}\sum_{x\in\mathbb{Z}_p} \chi_1(t)\chi_1(x)\bar{\chi}_2(t)\bar{\chi}_2(x) = \sum_{t\in B} p\chi_1(t)\bar{\chi}_2(t) = p\sum_{t\in B}\chi_1(t)\bar{\chi}_2(t), \end{aligned}$$

since the kernel of χ_1 and χ_2 contains $\mathbb{Z}_p$. Thus we obtain a set of $r = |B|$ representations of $\mathbb{Z}_N/\mathbb{Z}_p$, which are mutually orthogonal, hence forming a basis of $L^2(B)$. Thus B is a spectral set in $\mathbb{Z}_N/\mathbb{Z}_p$ and using our assumption we obtain that there exists T with $B + T = \mathbb{Z}_N/\mathbb{Z}_p$. So finally we get $S + T = (\mathbb{Z}_p + B) + T = \mathbb{Z}_p + (B + T) = \mathbb{Z}_p + \mathbb{Z}_N/\mathbb{Z}_p = \mathbb{Z}_N$. ∎

Before we start to detail the proof of Theorem 2.5 we summarize that we have already proved in the previous sections about the structure of a spectral set S in $\mathbb{Z}_{p^nq^2}$. Note that we may assume by induction on n that $\mathbf{S}-\mathbf{T}(H)$ holds for every proper subgroup or factor H of $\mathbb{Z}_{p^nq^2}$. Indeed, Fuglede's Conjecture holds for $\mathbb{Z}_{pq^2}$ and for $\mathbb{Z}_{p^nq}$ by [21], which corresponds to the base case of our induction.

If $|S| = 1$, then S is clearly a spectral set and also a tile. By Lemma 4.4 we might assume that the elements of χ_Λ do not have a common kernel so by Proposition 4.6 we might assume that $|S| \geq 2$ is a non-Pompeiu set with respect to a faithful representation of $\mathbb{Z}_{p^nq^2}$. Hence by Proposition 3.2 we have

$$S = \sum_{g\in A} u_g(\mathbb{Z}_p + g) + \sum_{h\in B} v_h(\mathbb{Z}_q + h),$$

where $u_g, v_h \in \mathbb{Q}$ and A and B are sets of coset representatives of $\mathbb{Z}_p$ and $\mathbb{Z}_q$, respectively. Thus S is the weighted sum of cosets of $\mathbb{Z}_p$ and $\mathbb{Z}_q$. Until now we have only seen that the weights are rational numbers. Now we prove that all weights are 0 or 1.

The subgroups $\mathbb{Z}_p$ and $\mathbb{Z}_q$ generate $\mathbb{Z}_{pq}$, so we write S as the disjoint union

$$S = \cup_{k\in C} S_{k \bmod N/pq},$$

where k runs through a set of representatives C of the cosets of $\mathbb{Z}_{pq}$ for $k = 0, \ldots, N/pq - 1$. Now

$$S_{k \bmod N/pq} = \sum_{g\in A,\ g+\mathbb{Z}_p\subset k+\mathbb{Z}_{pq}} u_g(\mathbb{Z}_p + g) + \sum_{h\in B,\ h+\mathbb{Z}_q\subset k+\mathbb{Z}_{pq}} v_h(\mathbb{Z}_q + h) \tag{8}$$

for every $k \in C$, so $S_{k \bmod N/pq}$ inherits its weights from S. Now it follows from Proposition 3.8 that in (8) $u_g = 0$ for every $g \in A,\ g+\mathbb{Z}_p \subset k+\mathbb{Z}_{pq}$ or $v_h = 0$ for every $h \in B,\ h+\mathbb{Z}_q \subset k+\mathbb{Z}_{pq}$. Since $S_{k \bmod N/pq}$ is a set, the remaining coefficients are 0 or 1. Then $S_{k \bmod N/pq}$ is the disjoint nontrivial union of $\mathbb{Z}_p$-cosets or $\mathbb{Z}_q$-cosets. Only one type appears for every fixed $k = 0, \ldots, N/pq - 1$ except in the obvious case as follows:

It can happen that S contains a whole $\mathbb{Z}_{pq}$-coset, in which case it can be considered as the union of only $\mathbb{Z}_p$-cosets and only $\mathbb{Z}_q$-cosets as well. Thus S is the disjoint union of $\mathbb{Z}_p$-cosets and $\mathbb{Z}_q$-cosets.

Beside the case when S contains both $\mathbb{Z}_p$-cosets and $\mathbb{Z}_q$-cosets, by Proposition 4.8 we are done. Thus, we may assume S contains both $\mathbb{Z}_p$-cosets and $\mathbb{Z}_q$-cosets; we shall call such sets *nontrivial unions* of $\mathbb{Z}_p$- and $\mathbb{Z}_q$-cosets, to emphasize that they cannot be expressed as unions consisting solely of $\mathbb{Z}_p$-cosets, or $\mathbb{Z}_q$-cosets.

The above also follows from Corollary 4.7 and the structure of vanishing sums of roots of unity of order N, where N has at most two distinct prime factors [19]. We added also a condition that shows when such a vanishing sum corresponds to a nontrivial union of $\mathbb{Z}_p$- and $\mathbb{Z}_q$-cosets, which is a consequence of Corollary 3.3 and Proposition 3.8(b) or alternatively of Proposition 2.6 in [21].

Theorem 4.9. *Let $F(x) \in \mathbb{Z}_{\geq 0}[x]$ and $N = p^m q^n$, where p, q are different primes. Then, $F(\xi_N) = 0$ if and only if*

$$F(x) \equiv P(x)\Phi_p(x^{N/p}) + Q(x)\Phi_q(x^{N/q}) \bmod (x^N - 1),$$

for some $P(x), Q(x) \in \mathbb{Z}_{\geq 0}[x]$. If $F(\xi_N^{p^k}) \neq 0$ (respectively, $F(\xi_N^{q^\ell}) \neq 0$) for some $1 \leq k \leq m$ (resp. $1 \leq \ell \leq n$), then we cannot have $P(x) \equiv 0 \bmod (x^N - 1)$ (resp. $Q(x) \equiv 0 \bmod (x^N - 1)$).

We will repeatedly use the above in Section 6 in order to obtain information about the structure of S and Λ from the vanishing of their mask polynomials on various N'th roots of unity. Regarding the case when S is a union of $\mathbb{Z}_p$-cosets (or $\mathbb{Z}_q$-cosets), there is a characterization in terms of the mask polynomial. This follows from a special case of Ma's Lemma [20] (see also Lemma 1.5.1 [30], or Corollary 1.2.14 [25]), adapted to the cyclic case, using the polynomial notation.

Lemma 4.10. *Suppose that $S(x) \in \mathbb{Z}[x]$, and let $\mathbb{Z}_N$ be a cyclic group such that $p^m \mid N$, but $p^{m+1} \nmid N$. If $S(\xi_d) = 0$, for every $p^m \mid d \mid N$, then*

$$S(x) \equiv P(x)\Phi_p(x^{N/p}) \bmod (x^N - 1).$$

If the coefficients of S are nonnegative, then P can be taken with nonnegative coefficients as well. In particular, if $S \subseteq \mathbb{Z}_N$ satisfies $S(\xi_d) = 0$, for every $p^m \mid d \mid N$, then S is a union of $\mathbb{Z}_p$-cosets.

We summarize the reductions made so far in the following list.

Reduction 1. We might assume that a spectral set $S \subset \mathbb{Z}_{p^n q^2}$ along with a spectrum Λ, have the following structure:

(a) $0 \in S$, $0 \in \Lambda$ and each of S and Λ generates $\mathbb{Z}_{p^n q^2}$.

(b) Both S and Λ can be written as the disjoint nontrivial union of $\mathbb{Z}_p$-cosets and $\mathbb{Z}_q$-cosets and this holds for $S \cap (\mathbb{Z}_{pq} + g)$ and $\Lambda \cap (\mathbb{Z}_{pq} + h)$ for every $g, h \in \mathbb{Z}_{p^n q^2}$ as well.

(c) There is a $\mathbb{Z}_{pq}$-coset which intersects S and its complement. Further the intersection is the union of $\mathbb{Z}_p$-cosets. The same holds for another $\mathbb{Z}_{pq}$-coset with $\mathbb{Z}_q$-cosets as well.

(d) Fuglede's conjecture holds for all $\mathbb{Z}_M$, with $M \mid p^n q^2$, $M < p^n q^2$ (induction assumption).

Proof. (a) Follows from Lemma 4.1 and Proposition 4.3.

(b) Immediate consequence of part (a), Lemma 3.2, Proposition 3.8 and Corollary 4.7.

(c) Follows from Proposition 4.8.

(d) It was proved in [21] that Fuglede's conjecture holds for $N = p^n q$, and also for $N = pq^2$, so the given statement certainly holds for p^2q^2, which is the base case for the inductive argument. ■

Now we turn to the main tool already used in [21] to prove that a spectral set tiles $\mathbb{Z}_{p^nq^2}$. Clearly, sets coincide with mask polynomials having only coefficients 0 and 1. The following theorem was proved in [4]. Let H_S be the set of prime powers r^a dividing N such that $\Phi_{r^a}(x) \mid S(x)$.

Theorem 4.11. *If $S \subset \mathbb{Z}_N$ satisfies the following two conditions* **(T1)** *and* **(T2)***, then S tiles $\mathbb{Z}_N$.*

(T1) $S(1) = \prod_{d \in H_S} \Phi_d(1)$.

(T2) *For pairwise relative prime elements s_i of H_S, $\Phi_{\prod s_i} \mid S(x)$.*

Note that $\Phi_{p^a}(1) = p$ for a prime p and $\Phi_k(1) = 1$ if k has at least two different prime divisors.

5 Preliminary lemmas

We introduce an extra notation for divisibility. Fix $N \in \mathbb{N}$. For a natural number k we write $\ell \parallel_N k$ if ℓ is the largest divisor of N, which divides k. In our case N will be $p^n q^2$ so we simply write $\ell \parallel k$.

We review first the equations (1) and (7) for a spectral pair (S, Λ) in $\mathbb{Z}_N$. First, we define as usual

$$\mathbb{Z}_N^\star = \{g \in \mathbb{Z}_N : \gcd(g, N) = 1\},$$

the group of *reduced residues* mod$N$. It is precisely the subset of elements of N of order exactly N. Similarly, the subset of $\mathbb{Z}_N$ of elements of order N/d, where $d \mid N$, is

$$d\mathbb{Z}_N^\star = \{g \in \mathbb{Z}_N : \gcd(g, N) = d\}.$$

The zero set

$$Z(S) = \left\{d \in \mathbb{Z}_N : S(\xi_N^d) = 0\right\}$$

is then a union of subsets of the form $d\mathbb{Z}_N^\star$, for some $d \mid N$, and (1) and (7) can be rewritten as

$$\Lambda - \Lambda \subseteq \{0\} \cup \bigcup_{d \mid N, S(\xi_N^d) = 0} d\mathbb{Z}_N^\star. \tag{9}$$

Of course, by Lemma 4.1(c), the roles of S and Λ can be reversed.

Definition 5.1. Let $S \subseteq \mathbb{Z}_N$. Recall that for every $j \in \mathbb{Z}$ and $d \mid N$, we define the following subsets

$$S_{j \bmod d} = \{s \in S : s \equiv j \bmod d\}.$$

We say that S is *equidistributed* mod$d$, if

$$|S_{j \bmod d}| = \frac{1}{d}|S|,$$

for every j. Equivalently, every $\mathbb{Z}_{N/d}$-coset of $\mathbb{Z}_N$ contains the same amount of elements of S.

Lemma 5.2.

(a) Assume $\Phi_p(x) \mid S(x)$. Then every $\mathbb{Z}_{N/p}$-coset of $\mathbb{Z}_N$ contains the same amount of elements of S.

(b) Assume $\Phi_k(x) \mid S(x)$ for every $1 < k \mid d$. Then every $\mathbb{Z}_{N/d}$-coset of $\mathbb{Z}_N$ contains the same amount of elements of S.

Proof. (a) $\Phi_p(x) \mid S(x)$ is equivalent to the fact that S is a non-Pompeiu set with respect to an irreducible representation of order p, whose kernel is $\mathbb{Z}_{N/p}$. It is easy to see that a non-Pompeiu multiset on $\mathbb{Z}_p$ has to be constant we obtain the result.

(b) Consider the formula

$$S(x) \equiv \sum_{j=0}^{d-1} |S_{j \bmod d}| x^j \bmod (x^d - 1), \tag{10}$$

which holds for every $S \subseteq \mathbb{Z}_N$. It holds $S(\xi_k) = 0$ for every $1 < k \mid d$ if and only if

$$1 + x + \cdots + x^{d-1} = \prod_{1<k|d} \Phi_k(x) \mid S(x),$$

or equivalently $S(x) = (1 + x + \cdots + x^{d-1})G(x)$. The latter implies

$$S(x) \equiv (1 + x + \cdots + x^{d-1})G(1) \bmod (x^d - 1),$$

so by (10), we get $|S_{j \bmod d}| = G(1)$ for all j. Conversely, if $|S_{j \bmod d}| = c$ for all j, then

$$S(x) \equiv c(1 + x + \cdots + x^{d-1}) \bmod (x^d - 1),$$

due to (10), which easily gives $S(\xi_k) = 0$ for every $1 < k \mid d$, as desired. ∎

Let (S, Λ) be a spectral pair in $\mathbb{Z}_N$ satisfying the conditions of Reduction 1, where $N = p^n q^2$. An immediate consequence of Reduction 1(c) is that $S - S$ contains the difference set of both a $\mathbb{Z}_p$-coset and a $\mathbb{Z}_q$-coset, thus

$$\frac{N}{p}\mathbb{Z}_N \cup \frac{N}{q}\mathbb{Z}_N \subseteq S - S,$$

whence

$$\Lambda(\xi_p) = \Lambda(\xi_q) = 0, \tag{11}$$

by (7), and we obtain in particular,

$$|\Lambda_{i \bmod p}| = \frac{1}{p}|\Lambda|, \ |\Lambda_{j \bmod q}| = \frac{1}{q}|\Lambda|, \tag{12}$$

for all i, j, by Lemma 5.2. This shows that pq divides $|S| = |\Lambda|$.

6 Proof of Theorem 2.5

A significant special case will be shown first.

Lemma 6.1. *Let $S \subseteq \mathbb{Z}_N$ be spectral. If $q^2 \mid |S|$, then S tiles $\mathbb{Z}_N$.*

Proof. Let $H_S(p) = \{p^m : S(\xi_{p^m}) = 0, 1 \leq m \leq n\}$, and similarly define $H_\Lambda(p)$, for a spectrum $\Lambda \subseteq \mathbb{Z}_N$. Suppose that

$$H_\Lambda(p) = \{p^{m_1}, \dots, p^{m_k}\},$$

where $1 \leq m_1 < m_2 < \cdots < m_k \leq n$. For every j, it holds

$$S_{j \bmod q^2} - S_{j \bmod q^2} \subseteq (S - S) \cap q^2\mathbb{Z}_N \subseteq \{0\} \cup \bigcup_{i=0}^{k} \frac{N}{p^{m_i}} \mathbb{Z}_N^\star, \tag{13}$$

by (9). Consider the p-adic expansion of every $s \in S$ taken modp^n, as follows

$$s \equiv s_0 + s_1 p + \cdots + s_{n-1}p^{n-1} \bmod p^n,\ 0 \leq s_i \leq p-1,\ 0 \leq i \leq n-1.$$

Due to (13), the elements of each $S_{j \bmod q^2}$ cannot have the same p-adic digits corresponding to p^{n-m_i}, $1 \leq i \leq k$, yielding

$$|S_{j \bmod q^2}| \leq p^k,\ 0 \leq j < q^2,$$

thus, $|S| \leq p^k q^2$. On the other hand, we have

$$\prod_{i=1}^{k} \Phi_{p^{m_i}}(x) \mid \Lambda(x),$$

and putting $x = 1$ we obtain $p^k \mid |\Lambda|$; we then get by hypothesis $p^k q^2 \mid |S|$, whence $|S| = p^k q^2$, and

$$|S_{j \bmod q^2}| = p^k,\ 0 \leq j < q^2.$$

Since S is equidistributed modq^2, we must also have $S(\xi_q) = S(\xi_{q^2}) = 0$ by Lemma 5.2. We note that each element of $S_{j \bmod q^2}$ is unique modp^n, so the reduction modp^n map

$$\pi : \mathbb{Z}_N \mapsto \mathbb{Z}_{p^n}$$

is injective on each $S_{j \bmod p^n}$; fix some j, and let $\pi(S_{j \bmod p^n}) = S'$. Since $q^2 \mid s - s'$ for every $s, s' \in S_{j \bmod q^2}$, we conclude that the order of $s - s'$ in $\mathbb{Z}_N$ is the same as the order of $\pi(s - s')$ in $\mathbb{Z}_{p^n}$, which gives

$$S' - S' \subseteq \{0\} \cup \bigcup_{i=0}^{k} p^{n-m_i} \mathbb{Z}_{p^n}^\star.$$

Consider now the set $\Lambda' \subseteq \mathbb{Z}_{p^n}$ whose mask polynomial is given by

$$\Lambda'(x) \equiv \prod_{i=1}^{k} \Phi_{p^{m_i}}(x) \bmod (x^{p^n} - 1).$$

We have $|S'| = |\Lambda'| = p^k$ and

$$S' - S' \subseteq \{0\} \cup \Big\{d \in \mathbb{Z}_{p^n} : \Lambda'(\xi_{p^n}^d) = 0\Big\},$$

therefore, (S', Λ') is a spectral pair in $\mathbb{Z}_{p^n}$ by (9). Since

$$\Phi_{p^{m_i}}(x) = 1 + x^{p^{m_i-1}} + x^{2p^{m_i-1}} + \ldots + x^{(p-1)p^{m_i-1}}$$

we obtain

$$(\Lambda' - \Lambda') \cap p^{n-m_i+1}\mathbb{Z}_{p^n}^\star \neq \varnothing,\ 1 \leq i \leq k,$$

therefore,

$$\bigcup_{i=0}^{k} p^{n-m_i+1}\mathbb{Z}_{p^n}^\star \subseteq \Big\{d \in \mathbb{Z}_{p^n} : S'(\xi_{p^n}^d) = 0\Big\},$$

by (9), or equivalently

$$\prod_{i=0}^{k} \Phi_{n-m_i+1}(x) \mid S_{j \bmod q^2}(x),$$

since

$$S_{j \bmod q^2}(x) \equiv S'(x) \bmod (x^{p^n} - 1).$$

Moreover, by $S(x) = \sum_{j=0}^{q^2-1} S_{j \bmod q^2}(x)$ and $|S| = p^k q^2$, we conclude that

$$H_S = \{p^{n-m_k+1}, \ldots, p^{n-m_1+1}, q, q^2\},$$

hence S satisfies **(T1)**.

Consider next the polynomial $F(X)$ satisfying

$$S_{j \bmod q^2}(x) \equiv x^j F(x^{q^2}) \bmod (x^N - 1),$$

for a fixed j. Since $\Phi_{p^{n-m_i+1}}(x) \mid F(x^{q^2})$ for all $1 \leq i \leq k$ and q^2 is prime to p^{n-m_i+1}, we also get that $\Phi_{p^{n-m_i+1}}(x) \mid F(x)$. Therefore, for $\ell = 1$ or 2 we get

$$S_{j \bmod q^2}(\xi_{p^{n-m_i+1}q^\ell}) = \xi_{p^{n-m_i+1}q^\ell}^j F(\xi_{p^{n-m_i+1}q^\ell}^{q^2}) = \xi_{p^{n-m_i+1}q^\ell}^j F(\xi_{p^{n-m_i+1}}^{q^{2-\ell}}) = 0,$$

for all j, which shows that S satisfies **(T2)**. This completes the proof. ■

We distinguish now the following cases:

$\boxed{S(\xi_N^q) = S(\xi_N^{q^2}) = 0}$ Then, since $S(\xi_N) = 0$ by Corollary 4.7, S is a union of $\mathbb{Z}_p$-cosets by Lemma 4.10 and S tiles due to Reduction 1(c).

$\boxed{S(\xi_N^q)S(\xi_N^{q^2}) \neq 0}$ Consider the difference sets $\Lambda_{j \bmod q} - \Lambda_{j \bmod q}$. They are always subsets of $(\Lambda - \Lambda) \cap q\mathbb{Z}_N$, but since they avoid $q\mathbb{Z}_N^\star \cup q^2\mathbb{Z}_N^\star$ in this case by (9), we get

$$\Lambda_{j \bmod q} - \Lambda_{j \bmod q} \subseteq pq\mathbb{Z}_N,$$

for all j. This shows that every element of $\Lambda_{j \bmod q}$ has the same remainder mod$p$, or equivalently, for every j there is an $i = i(j)$ such that

$$\Lambda_{j \bmod q} \subseteq \Lambda_{i(j) \bmod p}.$$

This, in particular, shows that $p < q$, and that every $\Lambda_{i \bmod p}$ is the disjoint union of sets of the form $\Lambda_{j \bmod q}$, namely

$$\Lambda_{i \bmod p} = \bigcup_{i(j)=i} \Lambda_{j \bmod q}.$$

Suppose that the number of sets appearing in the union are ℓ. Then, the above equation along with (12) implies $1/p = \ell/q$, which leads to a contradiction (no such spectrum can exist).

$\boxed{S(\xi_N^q) = 0 \neq S(\xi_N^{q^2})}$ We apply Theorem 4.9 to $S(x) \bmod (x^{N/q} - 1)$. We obtain

$$S(x) \equiv P(x)\Phi_p(x^{N/pq}) + Q(x)\Phi_q(x^{N/q^2}) \bmod (x^{N/q} - 1),$$

since $S(\xi_{N/q}) = 0$, where $P(x)$ and $Q(x)$ have nonnegative coefficients. Furthermore, since $S(\xi_N^{q^2}) \neq 0$, we cannot have $Q \equiv 0$. Due to the nonnegativity of P and Q, we obtain the existence of $s, s' \in S$ such that

$$s - s' \equiv \frac{N}{q^2} \bmod \frac{N}{q},$$

hence $p^n \mid s - s'$ but $q \nmid s - s'$, yielding $s - s' \in p^n \mathbb{Z}_N^\star$ and

$$\Lambda(\xi_{q^2}) = 0,$$

which further gives $q^2 \mid |\Lambda|$, so by Lemma 6.1, S tiles $\mathbb{Z}_N$.

$\boxed{S(\xi_N^q) \neq 0 = S(\xi_N^{q^2})}$ We will prove the following:

Claim 1. $(S - S) \cap \frac{N}{pq^2}\mathbb{Z}_N^\star \neq \varnothing$.

Proof of Claim. By Theorem 4.9, the multiset[5] $q^2 S$ is a union of $\mathbb{Z}_p$-cosets, or equivalently

$$|S_{i \bmod p^n}| = |S_{i+kp^{n-1} \bmod p^n}|, \tag{14}$$

for every i, k. We partition the above sets mod$p^n q$:

$$S_{i \bmod p^n} = \bigcup_{\ell=0}^{q-1} S_{i+\ell p^n \bmod p^n q},$$

and

$$S_{i+kp^{n-1}q \bmod p^n} = \bigcup_{\ell=0}^{q-1} S_{i+kp^{n-1}q+\ell p^n \bmod p^n q}.$$

If for every i existed some ℓ such that

$$S_{i+kp^{n-1}q \bmod p^n} = S_{i+kp^{n-1}q+\ell p^n \bmod p^n q},$$

[5]Here, we consider the elements $q^2 s \bmod N$, $s \in S$, counting multiplicities. For example, if $N = 4$ and $S = \{0, 2\}$, then $2S$ is the multiset whose only element is 0, appearing with multiplicity 2.

for every k, then qS would also be a union of $\mathbb{Z}_p$-cosets. Indeed, as for every i there is at most one value of $0 \le \ell \le q-1$ such that $S_{i+\ell p^n \bmod p^n q} \neq \varnothing$, and by the above condition the cardinalities of $S_{i+kp^{n-1}q+\ell p^n \bmod p^n q}$ are the same for $0 \le k \le p-1$. Therefore, $S(\xi_{p^n q}) = 0$ by Theorem 4.9 (or equivalently by Proposition 3.2), contradicting the hypothesis. Thus, there exists i such that there are nonempty $S_{i+\ell p^n \bmod p^n q}$ and $S_{i+\ell' p^n \bmod p^n q}$, with $0 \le \ell < \ell' \le q-1$. Clearly, $S_{i+\ell p^n \bmod p^n q} \subseteq S_{i \bmod p^n}$, so $S_{i \bmod p^n}$ is nonempty. Using (14) we have $S_{i+p^{n-1} \bmod p^n}$ is nonempty.

Now let $s \in S_{i+p^{n-1} \bmod p^n}$, $s' \in S_{i+\ell p^n \bmod p^n q}$ and $s'' \in S_{i+\ell' p^n \bmod p^n q}$, so that $p^{n-1} \parallel s-s'$ and $p^{n-1} \parallel s-s''$. Since $s''-s' \equiv (\ell'-\ell)p^n \bmod p^n q$, we get $q \nmid s''-s'$, so either $q \nmid s-s'$ or $q \nmid s-s''$ would hold, yielding $(S-S) \cap p^{n-1}\mathbb{Z}_N^\star \neq \varnothing$, as desired. ■

This implies
$$\Lambda(\xi_{pq^2}) = 0, \tag{15}$$
by (7). If $\Lambda(\xi_{q^2}) = 0$ then we would have $q^2 \mid |S|$ and S would tile $\mathbb{Z}_N$ by virtue of Lemma 6.1. So, we may assume $\Lambda(\xi_{q^2}) \neq 0$.

By (15) and Theorem 4.9 we get
$$\Lambda(x) \equiv \sum_{j=0}^{pq^2-1} |\Lambda_{j \bmod pq^2}| x^j \equiv P(x)\Phi_p(x^{N/p}) + Q(x)\Phi_q(x^{N/q}) \bmod (x^{pq^2}-1),$$
for some $P(x), Q(x) \in \mathbb{Z}_{\ge 0}[x]$ and $P(x) \not\equiv 0$ by $\Lambda(\xi_{q^2}) \neq 0$. We note that the function $f(j) = |\Lambda_{j \bmod pq^2}|$ restricted on a $\mathbb{Z}_{pq}$-coset of $\mathbb{Z}_{pq^2}$ is supported either on a $\mathbb{Z}_p$-coset or a $\mathbb{Z}_q$-coset; otherwise, there would exist $\lambda \in \Lambda_{j \bmod pq^2}$ and $\lambda' \in \Lambda_{j' \bmod pq^2}$ where j, j' satisfy
$$j - j' \in q\mathbb{Z}_{pq^2}^\star.$$
This shows that $q \parallel \lambda-\lambda'$ and $p \nmid \lambda-\lambda'$, thus $\lambda-\lambda' \in q\mathbb{Z}_N^\star$ and $S(\xi_N^q) = 0$ by (9), contradicting the hypothesis.

Next, consider a nonempty subset $\Lambda_{j \bmod pq^2}$; the polynomials with nonnegative coefficients $P(x)\Phi_p(x^{N/p})$ and $Q(x)\Phi_q(x^{N/q})$ contribute to the coefficient of x^j of $\Lambda(x) \bmod (x^{pq^2} - 1)$. If both contributions are positive, then all subsets $\Lambda_{j+kq^2 \bmod pq^2}$ and $\Lambda_{j+\ell pq \bmod pq^2}$ are nonempty, for $0 < k < p$ and $0 < \ell < q$. Then, for $\lambda \in \Lambda_{j+q^2 \bmod pq^2}$ and $\lambda' \in \Lambda_{j+pq \bmod pq^2}$, we have $q \parallel \lambda - \lambda'$, hence $\lambda - \lambda' \in q\mathbb{Z}_N^\star$, which contradicts $S(\xi_N^q) \neq 0$, due to (7).

Let $\Gamma(x)$ be $\Lambda(x) \bmod (x^{pq^2}-1)$. The previous argument shows that the coefficient of x^j of $\Gamma(x)$ is determined completely either from $P(x)\Phi_p(x^{N/p})$ or $Q(x)\Phi_q(x^{N/q})$. Moreover, if $q \parallel j-j'$, then we cannot have that both the coefficients of x^j and $x^{j'}$ in $\Gamma(x)$ are nonzero by the same argument. This means that $f(j) = |\Lambda_{j \bmod pq^2}|$ restricted on a $\mathbb{Z}_{pq}$-coset of $\mathbb{Z}_{pq^2}$ is supported either on a $\mathbb{Z}_p$-coset or a $\mathbb{Z}_q$-coset and constant restricted to this coset.

This shows that for each j such that $\Lambda_{j \bmod pq^2} \neq \varnothing$, either
$$|\Lambda_{j+kq^2 \bmod pq^2}| = \frac{1}{p}|\Lambda_{j \bmod q^2}| = \frac{1}{p}|\Lambda_{j \bmod q}|,\ 0 \le k < p, \tag{16}$$
or
$$|\Lambda_{j+\ell pq \bmod pq^2}| = |\Lambda_{j+\ell pq \bmod q^2}| = \frac{1}{q}|\Lambda_{j \bmod q}|,\ 0 \le \ell < q \tag{17}$$

holds. If (17) holds for some j, then $q^2 \mid |\Lambda|$, so by Lemma 6.1 we get that S tiles $\mathbb{Z}_N$. Therefore, we may assume that (16) holds for all j with $\Lambda_{j \bmod pq^2} \neq \varnothing$. For such j, we have

$$\Lambda_{j \bmod q} - \Lambda_{j \bmod q} = \Lambda_{j \bmod q^2} - \Lambda_{j \bmod q^2} \subseteq (\Lambda - \Lambda) \cap q^2\mathbb{Z}_N,$$

hence $\Lambda - \Lambda$ completely avoids $q\mathbb{Z}_N \setminus q^2\mathbb{Z}_N$. On the other hand, $(S - S) \cap p^n\mathbb{Z}_N^\star = \varnothing$ by (9) and the assumption $\Lambda(\xi_{q^2}) \neq 0$, hence the polynomials

$$\overline{S}(x) \equiv S(x)\Phi_q(x^{p^n}) \bmod (x^N - 1)$$

and

$$\overline{\Lambda}(x) \equiv \Lambda(x)\Phi_q(x^{N/q}) \bmod (x^N - 1)$$

are mask polynomials of subsets of $\mathbb{Z}_N$, say $\overline{S}$ and $\overline{\Lambda}$, i.e. their coefficients are 0 or 1. We claim that $(\overline{S}, \overline{\Lambda})$ is a spectral pair. They obviously have the same cardinality of $q|S|$, and an element of $\overline{\Lambda} - \overline{\Lambda}$ can be expressed as $\lambda - \lambda' + lN/q$, where $\lambda, \lambda' \in \Lambda$, $|l| < q$.

If $\lambda - \lambda' \in p^k\mathbb{Z}_N^\star$, then $q \nmid \lambda - \lambda' + lN/q$, hence $\lambda - \lambda' + lN/q \in p^k\mathbb{Z}_N^\star$ as well, yielding $S(\xi_N^{\lambda - \lambda' + lN/q}) = 0$, since $N/q = p^n q$.

The remaining case is $\lambda - \lambda' \in p^k q^2\mathbb{Z}_N^\star$, where $0 \leq k \leq n-1$, as $\Lambda - \Lambda$ avoids $q\mathbb{Z}_N \setminus q^2\mathbb{Z}_N$. In this case, $\lambda - \lambda' + lN/p \in p^k q\mathbb{Z}_N^\star$ if $1 \leq l \leq q-1$, and $\Phi_q(\xi_{p^k q}^{p^n}) = \Phi_q(\xi_q^{p^{n-k}}) = 0$, so

$$\overline{S}(\xi_N^{\lambda - \lambda' + lN/p}) = 0.$$

If $l = 0$, then clearly $\lambda - \lambda' \in \Lambda - \Lambda$. Considering all of these cases we have $\overline{\Lambda} - \overline{\Lambda} \subseteq \{0\} \cup Z(\overline{S})$, proving that the pair $(\overline{S}, \overline{\Lambda})$ is spectral by virtue of (9). Since $q^2 \mid \overline{S}$ we have $\overline{S}$ tiles $\mathbb{Z}_N$ by Lemma 6.1, thus there is $T \subseteq \mathbb{Z}_N$ such that

$$S(x)\Phi_q(x^{p^n})T(x) \equiv \overline{S}(x)T(x) \equiv 1 + x + \cdots + x^{N-1} \bmod (x^N - 1),$$

so $\Phi_q(x^{p^n})T(x)$ is the mask polynomial of a tiling complement of S using Lemma 1.3 in [4], completing the proof. ■

7 Appendix

Theorem 7.1. *Let S be a subset of $\mathbb{Z}_p^2$. Then S tiles $\mathbb{Z}_p^2$ if and only if S is spectral.*

Iosevich et al. [12] has already proved this theorem, but we provide an easy combinatorial proof for one of the two directions and a short one for the other direction using Rédei's theorem.

Proposition 7.2. *Let S be a spectral set of $\mathbb{Z}_p^2$. Then S tiles $\mathbb{Z}_p^2$.*

Proof. Let S be a spectral set. We might assume $|S| > 1$, since one element sets clearly tile every group. The corresponding spectrum Λ is also of size at least 2. Then there is a nontrivial irreducible representation ψ of $\mathbb{Z}_p^2$ such that $\sum_{s \in S} \psi(s) = 0$. We may also assume $|S| = |\Lambda| < p^2$.

Representations of $\mathbb{Z}_p^2$ can be parametrized by the elements of $\mathbb{Z}_p^2$. For $u \in \mathbb{Z}_p^2$ let $\chi_u(v) = e^{\frac{2\pi i \langle u, v\rangle}{p}}$, where the scalar product of $\langle u, v\rangle$ is taken modulo p. This can be written as $\sum_{j=0}^{p-1} a_j e^{\frac{2\pi i}{p} j}$, where a_j's are integers, which are determined in the following way.

From now on we may also think of $\mathbb{Z}_p^2$ as a 2 dimensional vector space over $\mathbb{Z}_p$. Cosets of 1 dimensional subspaces are called lines. Let u' be a nonzero vector orthogonal to u. Then $\langle u, v\rangle$ is constant on every coset of the subgroup generated by u'. Basically, we count the intersection of S with the elements the set of lines parallel with $\langle u'\rangle$. The expression $\sum_{j=0}^{p-1} a_j e^{\frac{2\pi i}{p}j} = 0$ if and only if a_j is a constant sequence so every element of this class of parallel lines contains the same amount of elements of S (i.e. S is equidistributed on these set of parallel lines). As a consequence we get that $p \mid |S|$.

If $|S| = p$, then by the previous argument we have that S intersects each element of a class of parallel lines once. Then S clearly tiles $\mathbb{Z}_p^2$.

Thus we may assume $p+1 < 2p \leq |\Lambda| = |S| < p^2$. It is enough to show that such spectral set does not exist. Each class of parallel lines consists of p lines. Thus we have that for every class of parallel lines, at least one line contains at least two elements of Λ. Thus using the argument above we have that every element of every class of parallel lines contains the same amount of elements of S. This means that every line contains k elements of S for some fixed number $p > k \geq 2$.

Let $x \in \mathbb{Z}_p^2 \setminus S$. Take every line containing x. These lines give a disjoint cover of $\mathbb{Z}_p^2 \setminus \{x\}$. Since each of them contains $k \geq 2$ elements we have $|S| = (p+1)k$, which is not divisible by p, a contradiction. ∎

Proposition 7.3. *Let S be a set in $\mathbb{Z}_p^2$, which tiles. Then S is spectral.*

Proof. We may assume that $1 < |S| < p^2$. Then S and its tiling complements are of cardinality p. Using Theorem 2.1 we obtain that either S or T is a subgroup of $\mathbb{Z}_p^2$.

Subgroups are clearly spectral sets. If T is a subgroup, then S is a complete set of coset representatives of T. Let U denote the subgroup of $\mathbb{Z}_p^2$ consisting of vectors orthogonal to T. Then clearly S is equidistributed on the orthogonal lines for $u \in U$ so U is a spectrum for S. ∎

Acknowledgement

Research of G. Kiss was supported by the Hungarian National Foundation for Scientific Research, Grant No. K 124749 and the internal research project R-AGR-0500.
Research of M. Vizer was supported by the Hungarian National Foundation for Scientific Research, Grant No. SNN 116095, 129364, KH 130371 and K 116769.

References

[1] L. Babai. Spectra of Cayley graphs. *Journal of Combinatorial Theory, Series B*, **27**(2), 180–189, 1979.

[2] L. Brown, B. Schreiber, B. A. Taylor. Spectral synthesis and the Pompeiu problem, *Annales de l'institut Fourier* **23**(3), 125–154, 1973.

[3] L. Chakalov. Sur un probleme de D. Pompeiu. *Godishnik Univ. Sofia, Fac. Phys.-Math.*, Livre 1, **40**, 1–14, 1944.

[4] E. M. Coven, A. Meyerowitz. Tiling the integers with translates of one finite set. *Journal of Algebra*, **212**(1), 161–174, 1999.

[5] D. E. Dutkay, C. K. Lai. Some reductions of the spectral set conjecture to integers. *Mathematical Proceedings of the Cambridge Philosophical Society*, **156**(1), 123–135, 2014.

[6] A. Fan, S. Fan, L. Liao, R. Shi. Fuglede's conjecture holds in $\mathbb{Q}_p$. *ArXiv preprint*, 2015: `https://arxiv.org/abs/1512.08904`

[7] B. Farkas, M. Matolcsi, P. Móra. On Fuglede's conjecture and the existence of universal spectra. *Journal of Fourier Analysis and Applications*, **12**(5), 483–494, 2006.

[8] B. Fuglede. Commuting self-adjoint partial differential operators and a group theoretic problem. *Journal of Functional Analysis*, **16**(1), 101–121, 1974.

[9] N. Garofalo. A new result on the Pompeiu problem. *Rend. Sem. Mat. Univ. Pol. Torino* P.D.E and Geometry, 25–38, 1988.

[10] Iosevich, N. Katz, S. Pedersen. Fourier bases and a distance problem of Erdős. *Math. Res. Lett.*, **6** (2), 251–255, 1999.

[11] A. Iosevich, N. Katz, T. Tao. The Fuglede spectral conjecture holds for convex planar domains. *Mathematical Research Letters*, **10**(5), 559–569, 2003.

[12] A. Iosevich, A. Mayeli, J. Pakianathan. The Fuglede conjecture holds in $\mathbb{Z}_p \times \mathbb{Z}_p$. *Analysis & PDE*, **10**(4), 757–764, 2017.

[13] G. Kiss, M. Laczkovich, Cs. Vincze. The discrete Pompeiu problem on the plane. *Monatshefte für Mathematik*, **186**(2), 299–314, 2018.

[14] M. N. Kolountzakis, M. Matolcsi. Complex Hadamard matrices and the spectral set conjecture. *Collectanea Mathematica*, Vol. Extra, 281–291, 2006.

[15] M. N. Kolountzakis, M. Matolcsi. Tiles with no spectra. *Forum Mathematicum* **18**(3), 519–528, 2006.

[16] I. Łaba. Fuglede's conjecture for a union of two intervals. *Proceedings of the American Mathematical Society*, **129**(10), 2965–2972, 2001.

[17] I. Łaba. The spectral set conjecture and multiplicative properties of roots of polynomials. *Journal of the London Mathematical Society*, **65**(3), 661–671, 2002.

[18] M. Laczkovich, G. Székelyhidi. Harmonic analysis on discrete abelien group. *Proc. Am. Math. Soc.* **133**(6), 1581–1586, 2004.

[19] T. Y. Lam, K. H. Leung. On Vanishing Sums of Roots of Unity. *Journal of Algebra* **224**, 91–109, 2000.

[20] S. L. Ma. Polynomial addition sets. *Ph.D. thesis*, University of Hong Kong, 1985.

[21] R. D. Malikiosis, M. N. Kolountzakis. Fuglede's conjecture on cyclic groups of order $p^n q$. *Discrete Analysis*, 2017:12, 16pp.

[22] M. Matolcsi. Fuglede's conjecture fails in dimension 4. *Proceedings of the American Mathematical Society*, **133**(10), 3021–3026, 2005.

[23] D.J. Newman. Tesselations of integers. *J. Number Theory* **9**, 107–111, 1997.

[24] D. Pompeiu. Sur une propriété intégrale des fonctions de deux variables réelles. *Bull. Sci. Acad. Roy. Belgique*, **5**(15), 265–269, 1929.

[25] Alexander Pott. Finite geometry and character theory. *Lecture Notes in Mathematics*, vol. 1601, Springer-Verlag, Berlin, 1995.

[26] M. J. Puls. The Pompeiu problem and discrete groups. *Monatshefte für Mathematik*, **172**(3-4), 415–429, 2013.

[27] A. G. Ramm. The Pompeiu problem. *Applicable Analysis*, **64**(1-2), 19–26, 1997.

[28] A. G. Ramm. Solution to the Pompeiu problem and the related symmetry problem. *Applied Mathematics Letters*, **63**, 28–33, 2017.

[29] L. Rédei. Die neue Theorie der endlichen abelschen Gruppen und Verallgemeinerung des Hauptsatzes von Hajós. *Acta Math. Acad. Sci. Hung.*, **16**, 329–373, 1965.

[30] B. Schmidt. Characters and cyclotomic fields in finite geometry. *Lecture Notes in Mathematics*, vol. 1797, Springer-Verlag, Berlin, 2002.

[31] R. Shi. Fuglede's conjecture holds on cyclic groups $\mathbb{Z}_{pqr}$. *ArXiv preprint*, 2018: `https://arxiv.org/abs/1805.11261`

[32] B. Steinberg. Representation theory of finite groups: An introductory approach. *Springer Science and Business media*, 2012.

[33] L. Székelyhidi. A Wiener Tauberian theorem on discrete Abelian torsion groups. *Ann. Acad. Paedag. Cracov. Studia Math. I*, **4**, 147–150, 2001.

[34] T. Tao. Fuglede's conjecture is false in 5 and higher dimensions. *Mathematical Research Letters*, **11**(2), 251–258, 2004.

[35] L. Zalcman. A bibliographic survey of the Pompeiu problem. *Approximation by solutions of partial differential equations*, Kluwer Acad., Dordrecht. **365**, 185–194, 1992.

[36] D. Zeilberger. Pompeiu's problem in discrete space. *Proc. Nat. Acad. Sci. USA* **75**(8), 3555–3556, 1978.