FUGLEDE'S CONJECTURE ON CYCLIC GROUPS OF ORDER $p^n q$

ROMANOS-DIOGENES MALIKIOSIS AND MIHAIL N. KOLOUNTZAKIS

Abstract. We show that the spectral set conjecture by Fuglede [6] holds in the setting of cyclic groups of order $p^n q$, where p, q are distinct primes and $n \geq 1$. This means that a subset E of such a group G tiles the group by translation (G can be partitioned into translates of E) if and only if there exists an orthogonal basis of $L^2(E)$ consisting of group characters. The main ingredient of the present proof is the structure of vanishing sums of roots of unity of order N, where N has at most two prime divisors; the extension of this proof to the case of cyclic groups of order $p^n q^m$ seems therefore feasible. The only previously known infinite family of cyclic groups, for which Fuglede's conjecture is verified, is that of cyclic p-groups, i.e. $\mathbb{Z}_{p^n}$.

1. Introduction

Let Ω be a measurable subset of $\mathbb{R}^n$ of positive Lebesgue measure. Ω is called *spectral*, if it accepts an orthogonal basis of exponentials, namely $e^{i\lambda\cdot x}$, where λ ranges through $\Lambda \subseteq \mathbb{R}^n$; the set Λ is called the *spectrum* of Ω. On the other hand, Ω is called a *tile* of $\mathbb{R}^n$, if there is a set $T \subseteq \mathbb{R}^n$ such that almost every point of $\mathbb{R}^n$ can be written uniquely as $\omega + t$, where $\omega \in \Omega$ and $t \in T$; T is hence called the *tiling complement* of Ω.

Fuglede's spectral set conjecture [6] asserts that Ω is spectral if and only if Ω is a tile. For many years, there was a lot of positive evidence towards the veracity of this conjecture; Fuglede himself proved this conjecture when the spectrum or the tiling complement of Ω is a lattice. Later on, the conjecture was proved for various families of subsets by numerous authors, for example, for 2-dimensional convex bodies [7], unions of two intervals in $\mathbb{R}$ [11], etc.

Against the current of research on this subject, Tao disproved this conjecture for dimensions 5 and above [15], constructing a spectral set in 5 dimensions that does not tile the space[1]. Subsequently, works by Kolountzakis and Matolcsi [9, 10, 14] and Farkas-Matolcsi-Mora [5] showed that the conjecture is false in dimensions 3 and above in both directions, leaving it open for $\mathbb{R}$ and $\mathbb{R}^2$.

This conjecture can be naturally stated for other spaces, for example $\mathbb{Z}$ or any locally compact abelian group. These cases are not only interesting on their own, but they have connections to the original case. 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 $\mathbb{R}^5$.

Some examples of note, where Fuglede's conjecture holds, include finite cyclic p-groups [12, 4], $\mathbb{Z}_p \times \mathbb{Z}_p$ [8], and $\mathbb{Q}_p$ [3, 4], the field of p-adic numbers. Borrowing the notation from [2], we write $\mathbf{S}$-$\mathbf{T}(G)$, respectively $\mathbf{T}$-$\mathbf{S}(G)$, if the Spectral⇒Tile direction, respectively Tile⇒Spectral, holds in G; when we put $G = \mathbb{Z}_N$, it is understood that the statement holds *for all* N. The connection between the conjecture on $\mathbb{R}$ and on finite cyclic groups or $\mathbb{Z}$ is summarized below [2]:

$$\mathbf{T}\text{-}\mathbf{S}(\mathbb{R}) \Longleftrightarrow \mathbf{T}\text{-}\mathbf{S}(\mathbb{Z}) \Longleftrightarrow \mathbf{T}\text{-}\mathbf{S}(\mathbb{Z}_N),$$

and

$$\mathbf{S}\text{-}\mathbf{T}(\mathbb{R}) \Longrightarrow \mathbf{S}\text{-}\mathbf{T}(\mathbb{Z}) \Longrightarrow \mathbf{S}\text{-}\mathbf{T}(\mathbb{Z}_N).$$

2010 *Mathematics Subject Classification.* 43A46,11L03,20K01,13F20.

Key words and phrases. Spectral set, tiling in finite abelian groups, Fuglede's conjecture, vanishing sums of roots of unity.

RM is supported by a Postdoctoral Fellowship from Alexander von Humboldt Foundation.

MK received partial support for this research by Alexander von Humboldt Foundation.

[1] Any counterexample in n dimensions could be extrapolated to a counterexample in all higher dimensions.

According to the above connections, a counterexample in a finite cyclic group can be lifted to a counterexample in $\mathbb{R}$; on the other hand, if the conjecture were true for every cyclic group and $\mathbb{Z}$, this would hold no meaning for the original conjecture in $\mathbb{R}$, unless it were proven that every spectral set in $\mathbb{R}$ has a rational spectrum. We may ask nevertheless, to which extent is Fuglede's conjecture true for finite abelian groups, or even cyclic ones. Surprisingly, not much is known for cyclic groups, apart from cyclic p-groups, i.e. $\mathbb{Z}_{p^n}$ for p prime. The direction Tile⇒Spectral is known also for cyclic groups of order p^nq^m, for p, q distinct primes [1, 12]; see Section 3 below.

The novel contribution of our present work is the proof of Spectral⇒Tile direction for cyclic groups of order $N = p^nq$, thus establishing the veracity of Fuglede's conjecture in this setting. The proof relies heavily on the structure of vanishing sums of roots of unity of order N, where N is divided by at most two primes. The fact that such sums are *nonnegative* linear combinations of p- and q-cycles [13] gives efficient bounds on spectral sets $A \subseteq \mathbb{Z}_N$; we assert that these techniques can be extended to every cyclic group of order $N = p^nq^m$. Unfortunately, we have not managed to conclude our proof in this more general setting so far; hopefully, this will be the subject of a subsequent article.

Lastly, we have to emphasize that these techniques can be no further extended. Consider the following vanishing sum of roots of unity of order $N = pqr$, where p, q, r are distinct primes:

$$(\omega_p + \omega_p^2 + \cdots + \omega_p^{p-1})(\omega_q + \omega_q^2 + \cdots + \omega_q^{q-1}) + (\omega_r + \omega_r^2 + \cdots + \omega_r^{r-1}) = (-1)(-1) + (-1) = 0,$$

where $\omega_n = e^{2\pi i/n}$. It is known that this sum cannot be expressed as a nonnegative linear combination of p-, q-, or r-cycles [13], therefore we cannot obtain strong lower bounds on the size of a spectral subset of $\mathbb{Z}_N$. Whether sums such as the above lead to a counterexample in some finite cyclic group and eventually in $\mathbb{R}$, remains to be seen.

2. Preliminaries

Let $\mathbb{Z}_N$ denote the ring of integers modulo N. With every (multi)set A with elements from $\mathbb{Z}_N$, we associate a polynomial in the quotient ring $R = \mathbb{Z}[X]/(X^N - 1)$, say

$$A(X) = \sum_{a \in A} m_a X^a,$$

where m_a is the multiplicity of a in the multi-set A. A is a proper set, if and only if $A(X)$ has coefficients 0 and 1 (it is understood that we write any element in R as a linear combination of $1, X, \ldots, X^{N-1}$). $A(X)$ is called the *mask polynomial* of A; it has the following connection with the Fourier transform of the characteristic function of A:

$$\widehat{\chi}_A(n) = A(\omega^{-n}),$$

where $\omega = e^{2\pi i/N}$ throughout this paper.

A subset $A \subseteq \mathbb{Z}_N$ is called *spectral* if there is a set B with $\#A = \#B$, such that the set of exponentials

$$x \mapsto e^{\frac{2\pi i b x}{N}}, \ b \in B$$

is orthogonal on A with the usual inner product.

Theorem 2.1. *Let $A \subseteq \mathbb{Z}_N$ be spectral. Then*

$$B - B \subseteq \{0\} \cup \{n : A(\omega^n) = 0\}.$$

Proof. By definition, we get

$$\sum_{a\in A} e^{\frac{2\pi i(b-b')a}{N}} = 0,$$

whenever b, b' are distinct elements of B. This is equivalent to the condition

$$B - B \subseteq \{0\} \cup \{n : A(\omega^n) = 0\}. \qquad \square$$

There is a natural action of the Galois group

$$G = \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \cong \mathbb{Z}_N^\star$$

on the values of $A(X)$, given by

$$\sigma(A(\omega^a)) = A(\omega^{ag}), \tag{2.1}$$

where $\sigma \in G$ is determined by $\sigma(\omega) = \omega^g$, for some $g \in \mathbb{Z}_N^\star$. Therefore, in order to determine the support of $A(\omega^n)$ we only need to evaluate at the divisors of N. For any integer N, the *divisor class* of N with respect to $n > 0$, a divisor of N, is simply $n\mathbb{Z}_N^\star$, which is the set of residues $\bmod N$ whose greatest common divisor with N is equal to n. The set $\{n : A(\omega^n) = 0\}$ is just a union of divisor classes. This is equivalent to the fact that if $A(\omega^d) = 0$ for some $d \mid N$, then $\Phi_{N/d}(X) \mid A(X)$, where $\Phi_n(X)$ denotes the n-th cyclotomic polynomial.

We also denote

$$D := \{n \in \mathbb{N} : n \mid N, A(\omega^m) \neq 0, \text{ for all } m \text{ with } n \mid m \text{ and } m \mid N\}.$$

Proposition 2.2. *If $A \subseteq \mathbb{Z}_N$ is spectral and $n \in D$, then $\#A \leq n$.*

Proof. By Theorem 2.1 and the hypothesis we get

$$(B - B) \cap n\mathbb{Z}_N = \{0\}$$

for a spectrum B of A. Hence, no two distinct elements of B can have the same residue $\bmod n$, thus obtaining $\#A = \#B \leq n$. □

The following properties on polynomials were introduced by Coven and Meyerowitz [1] in their effort to characterize finite sets that tile the integers by translations. We will adapt this definition for subsets of $\mathbb{Z}_N$.

Definition 2.3. Let $A \subseteq \mathbb{Z}_N$, and let $A(X)$ be its mask polynomial. The set of prime powers dividing N is denoted by S; define

$$S_A = \{s \in S : \Phi_s(X) \mid A(X)\}.$$

We say that A satisfies the property **(T1)**, if

$$\#A = A(1) = \prod_{s\in S_A} \Phi_s(1),$$

and that it satisfies **(T2)**, if for every distinct elements $s_1, \dots, s_m$ of S_A, $\Phi_{s_1\cdots s_m}(x)$ divides $A(x)$.

Theorem 2.4 (Theorem A [1]). *If $A \subseteq \mathbb{Z}_N$ satisfies* **(T1)** *and* **(T2)**, *then A tiles $\mathbb{Z}_N$ by translations.*

Let $d \mid N$. A d-cycle is a coset by the cyclic subgroup of N with d elements, that is, a set of the form

$$\{j, j + N/d, j + 2N/d, \dots, j + (d-1)N/d\}.$$

Especially in the case when N has only two prime divisors, the following Lemma allows us to discern the structure of $n \cdot A := \{na : a \in A\}$ (a multi-set), whenever $A(\omega^n) = 0$. In particular, it says that $n \cdot A$ must be the union of p- and q-cycles.

Lemma 2.5. *Let $n \mid N$ be such that N/n has at most two prime divisors, say p and q. If $A(\omega^n) = 0$, then*

$$A(X^n) \equiv P_n(X^n)\Phi_p(X^{N/p}) + Q_n(X^n)\Phi_q(X^{N/q}) \bmod X^N - 1, \tag{2.2}$$

where P_n and Q_n have nonnegative coefficients.

Proof. By definition, $A(\omega^n)$ is a vanishing sum of roots of unity of order N/n, in particular

$$0 = A(\omega^n) = \sum_{a\in A} \omega^{na}.$$

As N/n has at most two prime divisors, p and q, the above sum can be written as linear combination with *nonnegative integer coefficients* of sums of the form

$$\omega^k(1 + \omega_p + \omega_p^2 + \cdots + \omega_p^{p-1})$$

or

$$\omega^k(1 + \omega_q + \omega_q^2 + \cdots + \omega_q^{q-1}),$$

due to Theorem 3.3 from [13], which shows that $n{\cdot}A$ is the union of p- and q-cycles, as multi-sets. Every p-cycle has a mask polynomial of the form $X^k\Phi_p(X^{N/p})$; union of multi-sets corresponds to addition of the mask polynomials, thus obtaining (2.2). We note that the argument of P_n, Q_n is X^n, simply because $A(X^n)$ can be expressed in terms of powers of X^n, as $n \mid N$. □

Remark. If N/n has only one prime divisor, say p, then it is understood that $Q_n \equiv 0$.

It is also useful to find conditions under which $n \cdot A$ cannot be written as a union of p-cycles or q-cycles only, or equivalently, $P_nQ_n \not\equiv 0$, for every such possible choice of P_n and Q_n.

Proposition 2.6. *Let N have only two prime divisors, say p and q, and $A(\omega^n) = 0$, for some $n \mid N$, so that*

$$A(X^n) \equiv P_n(X^n)\Phi_p(X^{N/p}) + Q_n(X^n)\Phi_q(X^{N/q}) \bmod X^N - 1.$$

If $A(\omega^{np^a}) \neq 0$ for some $a > 0$, then $P_n \not\equiv 0$, and if $A(\omega^{nq^b}) \neq 0$ for some $b > 0$, then $Q_n \not\equiv 0$.

Proof. If $Q_n \equiv 0$, then

$$A(X^{nq^b}) \equiv P_n(X^{nq^b})\Phi_p(X^{Nq^b/p}) \equiv P_n(X^{nq^b})\Phi_p(X^{N/p}),$$

thus obtaining $A(\omega^{nq^b}) = 0$. The other case is proven similarly. □

(T1) and **(T2)** are conjectured to hold if and only if A tiles $\mathbb{Z}_N$ [1] (this conjecture was initially formulated in $\mathbb{Z}$). For every set $A \subseteq \mathbb{Z}_N$, however, a weaker property than **(T1)** holds, that is very useful for bounding $\#A$.

Proposition 2.7. *Let $A \subseteq \mathbb{Z}_N$. Then $\prod_{s\in S_A} \Phi_s(1)$ divides $\#A$. In particular, if p is a prime divisor of N, and there are m integers $0 < a_1 < a_2 < \cdots < a_m$ such that $A(\omega^{N/p^{a_i}}) = 0$ for all $1 \leq i \leq m$, then $p^m \mid \#A$, where $p^{a_m} \mid N$.*

Proof. By definition, $A(X)$ is divided by $\prod_{s\in S_A} \Phi_s(X)$ in $\mathbb{Z}[X]$. Putting $X = 1$, we get the desired result. □

In the rest of this paper we will prove Fuglede's conjecture on $\mathbb{Z}_N$, where $N = p^nq$, for $p \neq q$ primes. The direction Tile⇒Spectral can be deduced from the work of Coven-Meyerowitz [1] and Łaba [12] in the more general case when N has at most two prime divisors, and is shown in Section 3. The direction Spectral⇒Tile is proven in section 5. For completeness, we will also present the Spectral⇒Tile proof for $N = p^n$ in section 4 due to its elegance and brevity, although a proof for this case follows from [12]; a different proof also appeared in [4].

One final tool that will be very useful in this note, is the following:

Lemma 2.8. *Let $m, n > 0$ be two relatively prime integers, and $0 < k < mn$ another integer. Then, there is at most one pair (s, t) of nonnegative integers, such that $k = sm+tn$. If $k = mn$, then there are exactly two such pairs, namely $(n, 0)$ and $(0, m)$.*

Proof. Assume that $0 < k < mn$ and there is a pair (s, t) such that $k = sm + tn$, with $s, t \geq 0$. All other pairs of integer solutions (s', t') to the Diophantine equation $k = s'm + t'n$, satisfy $s' = s - nx$, $t' = t + mx$, for $x \in \mathbb{Z}$. If $x > 0$, then $s' \leq s - n \leq k/m - n < 0$, whereas if $x < 0$ we get $t' \leq t - m \leq k/n - m < 0$. The case $k = mn$ is proven similarly. □

3. Tile⇒Spectral, $N = p^n q^m$

In this section, we will review the proof of the fact that, if $A \subseteq \mathbb{Z}_N$ tiles $\mathbb{Z}_N$ by translations, then A is spectral, where N has at most two prime factors, say p and q. The proof is not new, and is based on combined arguments from [12] and [1], even though the case for finite cyclic groups is not explicitly mentioned. We will need the following tools from [1] and [12].

Lemma 3.1 (Lemma 1.3, [1]). *Let N be an integer and let A and B be finite multisets of nonnegative integers with mask polynomials $A(X)$ and $B(X)$. Then the following statements are equivalent. Each forces A and B to be sets such that $\#A\#B = A(1)B(1) = N$.*

(1) *$A \oplus (B \oplus N\mathbb{Z}) = \mathbb{Z}$ is a tiling.*
(2) *$A \oplus B$ is a complete set of residues modulo N.*
(3) *$A(X)B(X) \equiv 1 + X + \cdots X^{N-1} \bmod X^N - 1$.*
(4) *$N = A(1)B(1)$ and for every factor $t > 1$ of N, the cyclotomic polynomial $\Phi_t(X)$ is a divisor of $A(X)$ or $B(X)$.*

Lemma 3.2 (Lemma 2.1, [1]). *Let $A(X)$ and $B(X)$ be polynomials with coefficients 0 and 1, $N = A(1)B(1)$, and S the set of prime power factors of N. If $\Phi_t(X)$ divides $A(X)$ or $B(X)$ for every factor $t > 1$ of N, then*

(1) *$A(1) = \prod_{s \in S_A} \Phi_s(1)$ and $B(1) = \prod_{s \in S_B} \Phi_s(1)$.*
(2) *S_A and S_B are disjoint sets whose union is S.*

Now, assume that A tiles $\mathbb{Z}_N$ by translations, and let B be the complementary tile.We may assume that $A \subseteq \{0, 1, 2, \ldots, N-1\}$, and also assume that A tiles $\mathbb{Z}$ by translations; furthermore, this tiling has period N, i. e. $A \oplus (B \oplus N\mathbb{Z}) = \mathbb{Z}$. We warn the reader, that not only do we have to prove that A, as a subset of $\mathbb{Z}$, is spectral, but also that the spectrum is a subset of $N^{-1}\mathbb{Z}$, in order to claim that A, *as a subset of* $\mathbb{Z}_N$, is spectral.

We see that conditions (1) and (2) of Lemma 3.1 are satisfied, hence (4) is satisfied as well, which is just the hypothesis of Lemma 3.2. By (2) of Lemma 3.2, we get that $S_A \subseteq S$. Next, we will use the following two theorems:

Theorem 3.3 (Theorems B1 and B2, [1]). *Let A be a finite set of nonnegative integers with corresponding polynomial $A(x) = \sum_{a \in A} x^a$. If A tiles the integers, and $\#A$ is divided by at most two primes, then A satisfies* **(T1)** *and* **(T2)**.

Theorem 3.4 (Theorem 1.5(i), [12]). *If $A \subseteq \mathbb{Z}$ satisfies* **(T1)** *and* **(T2)**, *then A has a spectrum.*

Remark. The important part of the proof, is that the spectrum is explicitly constructed with respect to S_A, namely, the set of all

$$\sum_{s \in S_A} \frac{k_s}{s},$$

where $k_s \in \{0, 1, \ldots, p-1\}$, $s \in S_A$ and $s = p^\alpha$, is proven to be a spectrum of A, when it satisfies **(T1)** and **(T2)** (see the beginning of Section 2 [12]).

So, if $A \subseteq \{0, 1, \ldots, N-1\}$ tiles $\mathbb{Z}$ by translations, the tiling having period N, which has at most two prime divisors, then A satisfies (T1) and (T2) by Theorem 3.3, as $\#A$ divides N. Next, by Theorem 3.4 we get that A is spectral; by Lemma 3.2 and the Remark above, we get that the spectrum belongs to $N^{-1}\mathbb{Z}$, hence $A \subseteq \mathbb{Z}_N$ is spectral, completing the proof.

4. Spectral⇒Tile, $N = p^n$

Suppose $\Lambda \subseteq \mathbb{Z}_N$ is a spectrum of A and let $p^{\nu_1}, \ldots, p^{\nu_k}$ be the divisors d of N such that

$$\Phi_d(X) \mid A(X) = \sum_{a \in A} X^a.$$

We have

$$\Phi_{p^{\nu_i}}(X) = 1 + X^{p^{\nu_i - 1}} + X^{2p^{\nu_i - 1}} + \cdots + X^{(p-1)p^{\nu_i - 1}}.$$

Write $E_\nu = \{0, p^{\nu-1}, 2p^{\nu-1}, \ldots, (p-1)p^{\nu-1}\}$ so that $E_{\nu_i}(X) = \Phi_{p^{\nu_i}}(X)$. Define next the set

$$E = E_{\nu_1} + E_{\nu_2} + \cdots E_{\nu_k}, \tag{4.1}$$

and notice the sum is direct as $e_1 + \cdots + e_k \in E$ is determines $e_i \in E_{\nu_i}$ from the ν_i-th digit in its expansion to base p. This observation implies that $|E| = p^k$.

Notice also that $A(X)$ and $E(X)$ have the same zeros at the N-th roots of unity. This implies that Λ is also orthogonal on E as this is determined by the zeros of $E(X)$ at the N-th roots of unity. From the orthogonality we obtain

$$|A| = |\Lambda| \leq |E| = p^k.$$

Let $B \subseteq \mathbb{Z}_N$ be the sum of those E_ν, $\nu = 1, 2, \ldots, n$, not appearing in (4.1). This sum is again direct, as with the sum (4.1), so we obtain

$$|B| = p^{n-k}.$$

It follows that $A(X)B(X)$ vanishes on all N-th roots of unity except 1, which implies that $A + B$ is a tiling of $\mathbb{Z}_N$ at some level ℓ. Then

$$\ell p^n = |A| \cdot |B| = p^k p^{n-k} = p^n,$$

so that $\ell = 1$ and $A + B$ is a tiling of $\mathbb{Z}_N$ at level 1.

5. Spectral⇒Tile, $N = p^n q$

We distinguish two cases, depending on whether q belongs to D.

5.1. $\boxed{q \in D}$**.** We have $\#A \leq q$ from Proposition 2.2. Furthermore, the property **(T2)** holds vacuously, so we only need to prove **(T1)** due to Theorem 2.4. If $\#A = 1$, $A(X)$ is a monomial and has no root of the form ω^d, in particular, $A(\omega^{p^n}) \neq 0$ and **(T1)** holds.

If $\#A > 1$, and A is spectral, then $B - B \neq \{0\}$ for a spectrum B, so $A(\omega^d)$ must vanish somewhere. Since $q \in D$, there must be some nonnegative $a \leq n$ such that $A(\omega^{p^a}) = 0$, so that

$$A(X^{p^a}) \equiv P(X^{p^a})\Phi_p(X^{N/p}) + Q(X^{p^a})\Phi_q(X^{N/q}) \mod X^N - 1,$$

by Lemma 2.5. $q \in D$ yields $A(\omega^{p^a q}) \neq 0$, hence by Proposition 2.6 we get $Q \not\equiv 0$, so that $\#A = A(1) = pP(1) + qQ(1) \geq q$, leading to $P \equiv 0$ and $Q(1) = 1$. This certainly implies that $A(\omega^{p^n}) = 0$, $A(1) = q$, hence **(T1)** holds in any case where A is spectral and $q \in D$. By Theorem 2.4, A tiles $\mathbb{Z}_N$ by translations.

5.2. $\boxed{q \notin D}$. The size of a spectral set $A \subseteq \mathbb{Z}_N$ depends on the number of roots of $A(X)$ of the form $\omega^{p^a q}$.

Definition 5.1. The numbers $0 \leq a_1 < \cdots < a_m \leq n-1$ are such that $\{a : A(\omega^{p^a q}) = 0\} = \{a_1, \ldots, a_m\}$. If no such root exists, we simply put $m = 0$. Also, if A is spectral and B a spectrum of A, we denote $B_i = \{b \in B : b \equiv i \bmod q\}$. The p-adic expansion of the least nonnegative residue modp^n of $b \in B$ has the form

$$b \equiv b_0 + b_1 p + \cdots + b_{n-1} p^{n-1} \bmod p^n,$$

where $0 \leq b_i \leq p-1$ for all i. We say that the p-adic expansions of b and b' coincide at $a_1, \ldots, a_m$, if $b_i = b'_i$ for $1 \leq i \leq m$, that is, they have the same p-adic digits at those places. Finally, $p^i \parallel b$ exactly when b_i is the smallest nonzero p-adic digit of b.

We have seen in the previous subsection that Spectral⇒Tile holds when $m = 0$. By induction, we may assume that Spectral⇒Tile holds for all nonnegative integers up to $m-1$, for some $m > 0$, where $\{a : A(\omega^{p^a q}) = 0\} = \{a_1, \ldots, a_m\}$, exactly as in the Definition above.

Proposition 5.2. *Suppose that $A \subseteq \mathbb{Z}_N$ is spectral and $\#A > p^m$. Then*

1. *$\#A = p^m q$.*
2. *$\#B_i = p^m$ for all i, and the elements of B_i have all the possible p-adic expansions at $a_1, \ldots, a_m$, each appearing exactly once.*
3. *For every i, j and every $b \in B$, there is b' such that $p^{a_j} \parallel b - b'$.*
4. *There is some $a \neq a_i$ for all i, such that $b - b' \in p^a \mathbb{Z}_N^\star$ for some $b, b' \in B$, and $A(\omega^{p^a}) = 0$.*
5. *If $a > a_m$, then $A(\omega^{p^{a_j}}) = 0$ for all j, as well as $A(\omega^{p^{a'}}) = 0$ for all $a' \geq a$; in particular, $A(\omega^{p^n}) = 0$, or equivalently, $p^n \notin D$.*
6. *If $a < a_m$, then $A(X^{p^{a_m} q}) \equiv p^{m-1} q X^k \Phi_p(X^{N/p}) \bmod X^N - 1$, for some k.*

Proof. As $\#B > p^m$, there are at least two distinct elements of B, say b, b', that have the same digits at places $a_1, a_2, \ldots, a_m$. If $q \mid b - b'$, then $b - b' \notin \bigcup_{1 \leq i \leq m} p^{a_i} q \mathbb{Z}_N^\star$, contradicting the fact that $A(X)$ has exactly m roots of the form $\omega^{p^a q}$, due to Theorem 2.1. Hence $q \nmid b - b'$, and $b - b' \in p^a \mathbb{Z}_N^\star$, so that $A(\omega^{p^a}) = 0$ by Theorem 2.1, where a is the first place where the p-adic expansions of b and b' differ, therefore $a \neq a_i$ for all i, proving (4).

With the same argument we can show that $\#B_i \leq p^m$ for all i; in this case any two elements $b, b' \in B_i$ satisfy $q \mid b - b'$, so by Theorem 2.1 and the hypothesis, they must have at least one different digit at places $a_1, \ldots, a_m$, yielding $\#B_i \leq p^m$, and $\#B = \#A \leq p^m q$. For convenience, put $n_i = p^{a_i} q$ and $d = p^a$. By Lemma 2.5 we get

$$A(X^d) \equiv P_d(X^d) \Phi_p(X^{N/p}) + Q_d(X^d) \Phi_q(X^{N/q}) \bmod X^N - 1, \tag{5.1}$$

where $Q_d \not\equiv 0$ due to Proposition 2.6, as $A(\omega^{p^a q}) \neq 0$.

Now, consider the largest index i, such that $a > a_i$, assuming first that there is such an index, i. e. $a > a_1$; otherwise, we put $i = 0$. Put $u = dq = p^a q$, and denote by $\|A(X)\|_\infty$ the largest coefficient of $A(X)$ in $R = \mathbb{Z}[X]/(X^N - 1)$ written as a linear combination of $1, X, \ldots, X^{N-1}$.

Claim 1. $\|A(X^u)\|_\infty \geq p^i q$.

Proof of Claim. From (5.1) we obtain

$$A(X^u) \equiv P_d(X^u) \Phi_p(X^{N/p}) + q Q_d(X^u) \bmod X^N - 1. \tag{5.2}$$

If $i = 0$, then from $Q_d \not\equiv 0$ we get that some coefficient of $A(X^u)$ is at least as large as q, as desired. Suppose that $i > 0$. By repeated application of Lemma 2.5, we have

$$A(X^{n_j}) \equiv P_{n_j}(X^{n_j}) \Phi_p(X^{N/p}),$$

for all j. For $j = 1$, if we replace X by X^{n_2/n_1}, we also get $A(X^{n_2}) \equiv p P_{n_1}(X^{n_2})$, and comparing this with $A(X^{n_2}) \equiv P_{n_2}(X^{n_2}) \Phi_p(X^{N/p})$, we deduce that $\Phi_p(X^{N/p})$ divides $P_{n_1}(X^{n_2})$, thus obtaining $A(X^{n_2}) \equiv pP^1_{n_1}(X^{n_2})\Phi_p(X^{N/p})$, for some polynomial $P^1_{n_1}$ with positive integer coefficients. Proceeding inductively, we can get

$$A(X^{n_i}) \equiv p^{i-1}P^{i-1}_{n_1}(X^{n_i})\Phi_p(X^{N/p}),$$

hence

$$A(X^u) \equiv p^i P^{i-1}_{n_1}(X^u), \tag{5.3}$$

since $a_i < a < a_{i+1}$, where $P^{i-1}_{n_1}$ has positive integer coefficients. Comparing (5.2) and (5.3), we get that p^i divides all coefficients of $A(X^u)$. Furthermore, since $A(\omega^u) \neq 0$, we deduce that there is at least a p-cycle on which the elements of $n_m \cdot A$ do not have the same multiplicity; using (5.2) again, we deduce that two such multiplicities must differ by a multiple of q. Therefore, by (5.3) we conclude that their difference is a multiple of $p^i q$, and since they are both nonnegative and distinct, we finally get $\|A(X^u)\|_\infty \geq p^i q$. □

If $a > a_m$ the claim yields $\|A(X^u)\|_\infty \geq p^m q$, while on the other hand $A(1) \leq p^m q$, therefore, $A(X^u) \equiv p^m q X^{uk}$, for some k. Then, (5.2) yields $P_d \equiv 0$, so for all $a' \geq a$ (5.2) gives

$$A(X^{p^{a'}}) \equiv Q_d(X^{p^{a'}})\Phi_q(X^{N/q}) \bmod X^N - 1$$

establishing (5) (and (1) when $a > a_m$).

For the rest of the proof, we suppose $a < a_m$, and we will estimate $\|A(X^{n_m})\|_\infty$.

Claim 2. $\|A(X^{n_{j+1}})\|_\infty \geq p\|A(X^{n_j})\|_\infty$.

Proof of Claim. Since $A(\omega^{n_j}) = 0$, we obtain from Lemma 2.5 $A(X^{n_j}) \equiv P_{n_j}(X^{n_j})\Phi_p(X^{N/p})$. The largest coefficient of $A(X^{n_j})$ would appear in a p-cycle, hence $\|A(X^{n_j+1})\|_\infty \geq p\|A(X^{n_j})\|_\infty$, and finally, $\|A(X^{n_{j+1}})\|_\infty \geq \|A(X^{n_j+1})\|_\infty \geq p\|A(X^{n_j})\|_\infty$, as desired. □

Applying the last two claims, we obtain $\|A(X^{n_m})\|_\infty \geq p^{m-1}q$. The largest coefficient of $A(X^{n_m})$ would appear on a p-cycle, since $A(\omega^{n_m}) = 0$, so we would get $\#A = A(1) \geq p^m q$; but we have already shown that $\#A \leq p^m q$, so $A(1) = p^m q$ and $A(X^{n_m}) \equiv p^{m-1}qX^k\Phi_p(X^{N/p})$ thus proving (6) and (1) in all cases. (2) follows immediately from (1), as $\#B = p^m q$, hence $\#B_i = p^m$ for all i. Finally, (3) is a direct consequence of (2); let i and $b \in B_i$ be arbitrary. For every j, there is some $b' \in B_i$ whose p-adic expansion is the same on $a_1, \dots, a_{j-1}$ but differs on a_j, due to (2). Then, $b - b' \in p^c q\mathbb{Z}_N^\star$, for some $c \leq a_j$. By Theorem 2.1 and the hypothesis, $c = a_l$, for some l, but $c = a_l$ cannot hold for $l < j$, thus $l = j$, completing the proof. □

Next, we will make use of the induction assumption.

Proposition 5.3. *Let $A \subseteq \mathbb{Z}_N$ spectral and $\{a : A(\omega^{p^a q}) = 0\} = \{a_1, \dots, a_m\}$. Define a partition of A into sets $A_0, A_1, \dots, A_{p-1}$ such that*

$$a \in A_j \Longleftrightarrow p^{a_m}qa \in [\frac{N}{p}j, \frac{N}{p}(j+1)).$$

Then, all A_j have the same cardinality, and if $d \mid p^{a_m-1}q$ (assuming $a_m > 1$) with $A(\omega^d) = 0$, then $A_j(\omega^d) = 0$ for all j. Furthermore, $A_j(\omega^{p^{a_m}q}) \neq 0$.

Proof. By Proposition 2.6 we have $A(X^{p^{a_m}q}) \equiv P(X^{p^{a_m}q})\Phi_p(X^{N/p}) \bmod X^N - 1$, and without loss of generality we have $\deg P(X^{p^{a_m}q}) < N/p$. The hypothesis implies that

$$A_j(X^{p^{a_m}q}) \equiv P(X^{p^{a_m}q})X^{\frac{N}{p}j} \bmod X^N - 1,$$

so that $A_j(1) = P(1)$ for all j, proving the first part.

Now, let $d = p^k q^c$ with $A(\omega^d) = 0$, where $k < a_m$ and $c = 0$ or 1. We will use the language of multi-sets for this part; $d \cot A$ is a union of p- and q-cycles, as multi-sets. We will show that every such cycle must belong exclusively to one of the mutli-sets $d \cdot A_j$, hence each $d \cdot A_j$ is also a union of p- and q-cycles, leading to $A_j(\omega^d) = 0$, for all j.

Indeed, suppose that da is a part of such a cycle; the other member of said cycle are $da+lN/r$, where $r=p$ or q, and $0\leq l\leq r-1$. Define d' by $dd'=p^{a_m}q$. Then, for every l,

$$d'da\equiv d'(da+lN/r) \bmod N,$$

since $d'l\equiv 0 \bmod r$. This is true in case where $r=p$, because $p\mid d'$. If $r=q$, we can have q-cycles only if $c=0$, or equivalently $q\mid d'$. The above congruence clearly shows that any such cycle belongs to one of the multi-sets $d\cot A_j$ (we remark that these multi-sets are mutually exclusive).

For the last part, we just note that $P(\omega^{p^{a_m}q})\neq 0$, otherwise $\Phi_p(X^{N/p})$ would be a factor of $P(X^{p^{a_m}q})$, an impossibility, since the degree of the latter does not exceed N/p. □

Proposition 5.4. *Let $A\subseteq\mathbb{Z}_N$ be spectral with $\left\{a : A(\omega^{p^{a_m}})=0\right\}=\{a_1,\dots,a_m\}$ and B a spectrum. Consider the partition of A into $A_0,A_1,\dots,A_{p-1}$ as in Proposition 5.3. Suppose that the maximal $a\notin\{a_1,\dots,a_m\}$ with $0\leq a\leq n$ and $(B-B)\cap p^a\mathbb{Z}_N^\star\neq\varnothing$ (if it exists!) satisfies $a<a_m$. Then, each A_j is spectral (if such a does not exist, we have the same conclusion).*

Proof. Let B^i be the subset of elements B whose p-adic digit at a_m is equal to i. By hypothesis and Proposition 5.3,

$$(B^i-B^i)\subseteq(B-B)\setminus(p^{a_m}\mathbb{Z}_N^\star\cup p^{a_m}q\mathbb{Z}_N^\star)\subseteq\left\{d : A(\omega^d)=0\right\}\setminus p^{a_m}\mathbb{Z}_N\subseteq d : A_j(\omega^d)=0.$$

By pigeonhole principle, we may select one B^i such that $\#B^i\geq\frac{1}{p}\#B=A_j(1)$. This can only be possible if we have equality, thus showing that each A_j is spectral by Theorem 2.1, having the same spectrum (actually, any B^i would serve as such). □

If $A(1)=p^mq$ and $A(X)$ has at least m roots of the form ω^d, where d is a power of p, then A has a special structure.

Proposition 5.5. *Let $A\subseteq\mathbb{Z}_N$ with $A(1)=p^mq$. Suppose that $A(X^{d_i})=0$, where d_i are increasing powers of p, $1\leq i\leq m$ and $d_i\leq p^n$. Then either*

$$A(X^{d_j})\equiv P_{d_j}(X^{d_j})\Phi_p(X^{N/p}) \bmod X^N-1$$

for all j, where $P_{d_j}\not\equiv 0$ have nonnegative coefficients, or

$$A(X^{d_m})\equiv Q_{d_m}(X^{d_m})\Phi_q(X^{N/q}) \bmod X^N-1,$$

where $Q_{d_m}\not\equiv 0$ has nonnegative coefficients.

Proof. By Lemma 2.5 we obtain

$$A(X^{d_j})\equiv P_{d_j}(X^{d_j})\Phi_p(X^{N/p})+Q_{d_j}(X^{d_j})\Phi_q(X^{N/q}) \bmod X^N-1,$$

while on the other hand we can show inductively

$$A(X^{d_{j+1}})\equiv p^jP_{d_1}^j(X^{d_{j+1}})\Phi_p(X^{N/p})+\sum_{i=0}^{j}p^iQ_{d_1}^i(X^{d_{j+1}})\Phi_q(X^{N/q}) \bmod X^N-1,$$

for all j, where all the polynomials appearing in these two formulae have nonnegative coefficients, and satisfy the reccurence relations

$$P_{d_1}^j(X^{d_{j+2}})\equiv P_{d_1}^{j+1}(X^{d_{j+2}})\Phi_p(X^{N/p})+Q_{d_1}^{j+1}(X^{d_{j+2}})\Phi_q(X^{N/q}) \bmod X^N-1.$$

Without loss of generality we can write

$$P_{d_j}(X^{d_j})\equiv p^{j-1}P_{d_1}^{j-1}(X^{d_j}),Q_{d_j}(X^{d_j})\equiv\sum_{i=0}^{j-1}p^iQ_{d_1}^i(X^{d_j}),$$

for all j. Putting $j=m-1$ and $X=1$ we get

$$p^mq=A(1)=p^mP_{d_1}^{m-1}(1)+q\sum_{i=0}^{m-1}p^iQ_{d_1}^i(1),$$

so by Lemma 2.8 we have either $P_{d_1}^{m-1}(1) = q$ and $\sum_{i=0}^{m-1} p^i Q_{d_1}^i(1) = 0$, or $P_{d_1}^{m-1}(1) = 0$ and $\sum_{i=0}^{m-1} p^i Q_{d_1}^i(1) = p^m$. In the former case, we have $Q_{d_1}^i \equiv 0$ for all i, hence $Q_{d_j} \equiv 0$ for all j, and $A(X^{d_j}) \equiv P_{d_j}(X^{d_j})\Phi_p(X^{N/p})$. Otherwise, $P_{d_1}^{m-1} \equiv 0$, so in this case we get $A(X^{d_m}) \equiv Q_{d_m}(X^{d_m})\Phi_q(X^{N/q})$, as desired. □

Now, we can proceed with the conclusion of the Spectral⇒Tile proof. If $p^n \in D$, **(T2)** holds vacuously, so we need only prove **(T1)**, namely $A(1) = p^m$. Suppose on the contrary that $A(1) > p^m$, hence by Proposition 5.2(1) we have $A(1) = p^m q$. If a spectrum B satisfies the hypothesis of Proposition 5.4, then each A_j is spectral, so by induction they satisfy **(T1)**. Since $A_j(1) = p^{m-1}q$, we must have $A_j(\omega^{p^n}) = 0$ for all j, yielding $A(\omega^{p^n}) = 0$, contradicting our assumption that $p^n \in D$. If the maximal a such that $(B - B) \cap p^a\mathbb{Z}_N^\star \neq \varnothing$ satisfies $a > a_m$, then by Proposition 5.2(5) we get that $A(\omega^{p^{a_i}}) = 0$ for all $1 \leq i \leq m$. Taking $\{d_1, \dots, d_m\} = \{p^{a_1}, \dots, p^{a_{m-1}}, p^a\}$ and applying Proposition 5.5 we get either

$$A(X^{d_m}) \equiv P_{d_m}(X^{d_m})\Phi_p(X^{N/p}) \bmod X^N - 1$$

or

$$A(X^{d_m}) \equiv Q_{d_m}(X^{d_m})\Phi_q(X^{N/q}) \bmod X^N - 1,$$

where in each case $P_{d_m}, Q_{d_m} \not\equiv 0$ have nonnegative coefficients. However, this contradicts Proposition 2.6, since $A(\omega^{p^n})A(\omega^{p^a q}) \neq 0$. We conclude that A must satisfy **(T1)** as well, thus tiling $\mathbb{Z}_N$ by translations due to Theorem 2.4.

Lastly, we suppose that $p^n \notin D$, so that $A(\omega^{p^n}) = 0$. In this case, $q \mid A(1)$ by Proposition 2.7, hence $A(1) > p^m$ and $A(1) = p^m q$ by Proposition 5.2(1). Therefore, **(T1)**, and it remains to prove **(T2)**, namely $A(\omega^{p^{a_i}}) = 0$ for all i. If the maximal a for which $(B-B) \cap p^a\mathbb{Z}_N^\star \neq \varnothing$ holds, satisfies $a > a_m$, for a spectrum B, then by applying Proposition 5.2(5) we deduce that **(T2)** holds. Otherwise, B satisfies the conditions of Proposition 5.4. Therefore, each A_j is spectral and satisfies **(T2)**, yielding $A_j(\omega^{p^{a_i}}) = 0$ for all j and $1 \leq i \leq m-1$, hence $A(\omega^{p^{a_i}}) = 0$ for $1 \leq i \leq m-1$. It remains to show that $A(\omega^{p^{a_m}}) = 0$. We remark that an a as described in Proposition 5.4 *actually exists* in this case due to Proposition 5.2(4), and $a < a_m$. We apply Proposition 5.5 for $\{d_1, \dots, d_m\} = \{p^{a_1}, \dots, p^{a_{m-1}}, p^a\}$; if

$$A(X^{d_j}) \equiv P_{d_j}(X^{d_j})\Phi_p(X^{N/p}) \bmod X^N - 1$$

for all j, where $P_{d_j} \not\equiv 0$ have nonnegative coefficients, then $A(\omega^{p^a q}) = 0$, a contradiction. Therefore,

$$A(X^{d_m}) \equiv Q_{d_m}(X^{d_m})\Phi_q(X^{N/q}) \bmod X^N - 1,$$

where $Q_{d_m} \not\equiv 0$ has nonnegative coefficients. Substituting X by $X^{p^{a_m}/d_m}$, we get $A(X^{p^{a_m}}) \equiv Q_{d_m}(X^{p^{a_m}})\Phi_q(X^{N/q})$, yielding $A(\omega^{p^{a_m}}) = 0$, completing the proof.

References

1. Ethan M. Coven and Aaron Meyerowitz, *Tiling the integers with translates of one finite set*, J. Algebra **212** (1999), no. 1, 161–174.
2. Dorin Ervin Dutkay and Chun-Kit Lai, *Some reductions of the spectral set conjecture to integers*, Math. Proc. Cambridge Philos. Soc. **156** (2014), no. 1, 123–135.
3. Aihua Fan, Shilei Fan, Lingmin Liao, and Ruxi Shi, *Fuglede's conjecture holds in $\mathbb{Q}_p$*, 24pp., `https://arxiv.org/abs/1512.08904`.
4. Aihua Fan, Shilei Fan, and Ruxi Shi, *Compact open spectral sets in $\mathbb{Q}_p$*, J. Funct. Anal. **271** (2016), no. 12, 3628–3661.
5. Bálint Farkas, Máté Matolcsi, and Péter Móra, *On Fuglede's conjecture and the existence of universal spectra*, J. Fourier Anal. Appl. **12** (2006), no. 5, 483–494.
6. Bent Fuglede, *Commuting self-adjoint partial differential operators and a group theoretic problem*, J. Functional Analysis **16** (1974), 101–121.
7. Alex Iosevich, Nets Katz, and Terence Tao, *The Fuglede spectral conjecture holds for convex planar domains*, Math. Res. Lett. **10** (2003), no. 5-6, 559–569.

8. Alex Iosevich, Azita Mayeli, and Jonathan Pakianathan, *The fuglede conjecture holds in $\mathbb{Z}_p \times \mathbb{Z}_p$*, 9pp., `https://arxiv.org/abs/1505.00883`.
9. Mihail N. Kolountzakis and Máté Matolcsi, *Complex Hadamard matrices and the spectral set conjecture*, Collect. Math. (2006), no. Vol. Extra, 281–291.
10. ———, *Tiles with no spectra*, Forum Math. **18** (2006), no. 3, 519–528.
11. I. Łaba, *Fuglede's conjecture for a union of two intervals*, Proc. Amer. Math. Soc. **129** (2001), no. 10, 2965–2972 (electronic).
12. ———, *The spectral set conjecture and multiplicative properties of roots of polynomials*, J. London Math. Soc. (2) **65** (2002), no. 3, 661–671.
13. T. Y. Lam and K. H. Leung, *On vanishing sums of roots of unity*, J. Algebra **224** (2000), no. 1, 91–109.
14. Máté Matolcsi, *Fuglede's conjecture fails in dimension 4*, Proc. Amer. Math. Soc. **133** (2005), no. 10, 3021–3026 (electronic).
15. Terence Tao, *Fuglede's conjecture is false in 5 and higher dimensions*, Math. Res. Lett. **11** (2004), no. 2-3, 251–258.

RM: Technische Universität Berlin, Institut für Mathematik, Sekretariat MA 4-1, Strasse des 17. Juni 136, D-10623 Berlin, Germany
E-mail address: `malikios@math.tu-berlin.de`

MK: Department of Mathematics and Applied Mathematics, University of Crete, Voutes Campus, 700 13 Heraklion, Greece.
E-mail address: `kolount@gmail.com`