Advances in Mathematics 494 (2026) 110932

Contents lists available at ScienceDirect

Advances in Mathematics

journal homepage: www.elsevier.com/locate/aim

Lower bounds for mask polynomials with many cyclotomic divisors

Gergely Kiss [a,b,*], Izabella Łaba [c], Caleb Marshall [c], Gábor Somlai [d,b]

[a] *Corvinus University of Budapest, Department of Mathematics, Fővám tér 13-15, Budapest, H-1093, Hungary*
[b] *HUN-REN Alfréd Rényi Mathematical Institute, Reáltanoda utca 13-15, Budapest, H-1093, Hungary*
[c] *The University of British Columbia, Department of Mathematics, 1984 Mathematics Road, Vancouver, V6T 1Z2, Canada*
[d] *Eötvös Loránd University, Institute of Mathematics, Algebra and Number Theory Department, Pázmány Péter sétány 1/C, Budapest, H-1117, Hungary*

ARTICLE INFO

Article history:
Received 17 July 2025
Received in revised form 20 February 2026
Accepted 19 March 2026
Available online xxxx
Communicated by George Andrews

MSC:
primary 05B45, 20K01, 11C08
secondary 11B75

Keywords:
Integer tilings
Factorization of polynomials

ABSTRACT

Given a nonempty set $A \subset \mathbb{N} \cup \{0\}$, define the mask polynomial $A(X) = \sum_{a \in A} X^a$. Suppose that there are $s_1, \dots, s_k \in \mathbb{N} \setminus \{1\}$ such that the cyclotomic polynomials $\Phi_{s_1}, \dots, \Phi_{s_k}$ divide $A(X)$. What is the smallest possible size of A? For $k = 1$, this was answered by Lam and Leung in 2000. Less is known about the case when $k \geq 2$; in particular, one may ask whether (similarly to the $k = 1$ case) the optimal configurations have a simple "fibered" structure on each scale involved. We prove that this is true in a number of special cases, but false in general, even if further strong structural assumptions are added. Results of this type are expected to have a broad range of applications, including Favard length

* Corresponding author.
E-mail addresses: kiss.gergely@renyi.hu (G. Kiss), ilaba@math.ubc.ca (I. Łaba), cmarshall@math.ubc.ca (C. Marshall), gabor.somlai@ttk.elte.hu, gabor.somlai@unimelb.edu.au (G. Somlai).

https://doi.org/10.1016/j.aim.2026.110932

of product Cantor sets, Fuglede's spectral set conjecture, and the Coven-Meyerowitz conjecture on integer tilings.

1. Introduction

1.1. Overview

Let A be a nonempty set in $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$. We define the *mask polynomial* of A to be

$$A(X) := \sum_a X^a.$$

Recall that the s-th cyclotomic polynomial $\Phi_s(X)$ is the unique monic irreducible polynomial in $\mathbb{Q}[x]$ whose roots are the primitive s-th roots of unity. Equivalently, Φ_s can be computed from the identity $X^n - 1 = \prod_{s|n} \Phi_s(X)$. In particular, if p is a prime number, then

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = 1 + X + X^2 + \cdots + X^{p-1}. \tag{1.1}$$

We are interested in lower bounds on the size of sets whose mask polynomials have prescribed cyclotomic divisors. A classic result of Lam and Leung [14] implies that if $\Phi_s(X) \mid A(X)$ for some $s > 1$, we must have

$$|A| \geq \min\{p : \ p \mid s, \ p \text{ is prime}\}. \tag{1.2}$$

We consider the following more general question. Let $S \subset \mathbb{N} \setminus \{1\}$ be nonempty, and let $A \subset \mathbb{N}_0$ be a nonempty set such that $\Phi_s \mid A(X)$ for all $s \in S$. What is the minimal size of A? In other words, what can we say about the quantity

$$\mathsf{MIN}(S) := \min\{|A| : \ A \neq \emptyset \text{ and } \Phi_s(X) \mid A(X) \text{ for all } s \in S\}? \tag{1.3}$$

A natural question is whether the minimum in (1.3) is attained by sets A that have a particularly simple "fibered" structure on each scale $s \in S$. (We provide the definitions in Section 1.2 below.) This turns out to be false in general, with one counterexample already given in [13, Section 6.3]. In this article, we construct such counterexamples with the additional assumption that the least common multiple of the elements of S, which we denote by $\mathrm{lcm}(S)$, has only two distinct prime factors. The latter assumption imposes strong structural constraints on any set A contributing to (1.3) (see Lemma 2.3), so that examples with two prime factors are more unexpected and significantly more difficult to construct. On the other hand, we are able to identify a number of special cases where the "fibered lower bound" does hold.

Our interest in lower bounds on $\mathsf{MIN}(S)$ is motivated by several potential applications. One concerns the Coven-Meyerowitz conjecture on characterizing finite integer tiles; we discuss the conjecture and its relation to lower bounds on (1.3) in Section 1.3. Similar issues have also arisen in the study of Fuglede's spectral set conjecture. In its original formulation [6], the conjecture states that a set $\Omega \subset \mathbb{R}^n$ of positive n-dimensional Lebesgue measure tiles $\mathbb{R}^n$ by translations if and only if the space $L^2(\Omega)$ admits an orthogonal basis of exponential functions (we refer to such sets as *spectral*). While the original conjecture is now known to be false in its full generality, there remain important special cases where its status is unknown. In dimension 1, the Coven-Meyerowitz conjecture is known to imply that tiles are spectral sets (see [5] for a summary of the argument). Conversely, to prove that spectral sets in a given group are tiles, one has to show that sets A with small cardinality and many cyclotomic divisors of $A(X)$ must have very rigid structure. See e.g., [7,8] for examples and further references.

In a different direction, the question of bounding (1.3) from below has also come up in the study of the *Favard length* of product Cantor sets in the plane, an important question in geometric measure theory; see [1,13] for more details.

1.2. The fibered lower bound

Let $N \in \mathbb{N}$, and let p be a prime such that $p \mid N$. We define

$$F_p^N(X) = \Phi_p(X^{N/p}) = 1 + X^{N/p} + \cdots + X^{(p-1)N/p}. \tag{1.4}$$

This is a special case of a *p-fiber on scale N* (see Section 2.2 for the definition). We note that

$$F_p^N(X) = \frac{X^N - 1}{X^{N/p} - 1},$$

so that $\Phi_s \mid F_p^N$ if and only if $s \mid N$ but $s \nmid \frac{N}{p}$. In other words, if α is the exponent such that $p^\alpha \parallel N$, then $\Phi_s \mid F_p^N$ if and only if $p^\alpha \mid s \mid N$. (Here and below, we use the notation $p^\alpha \parallel N$ to indicate that $p^\alpha \mid N$ but $p^{\alpha+1} \nmid N$.) In particular, the set $F_p^N = \{0, N/p, \ldots, (p-1)N/p\}$ with the mask polynomial $F_p^N(X)$ has cardinality p, but $F_p^N(X)$ may have as many cyclotomic factors as we like, depending on N. Thus a large number of cyclotomic divisors of $A(X)$ does not, by itself, guarantee that A has large cardinality. To force an increase in size, we need additional assumptions on A, S, or both. (This was already noted in [13].)

More generally, we will say that a set $A \subset \mathbb{N}_0$ is *fibered* on scale N if there exists a prime $p \mid N$ such that

$$F_p^N(X) \mid A(X). \tag{1.5}$$

Of course, if $\Phi_s \mid F_p^N$ and (1.5) holds, then Φ_s also divides $A(X)$.

For a finite and nonempty set $S \subset (\mathbb{N} \setminus \{1\})$, we define $\mathsf{FIB}(S)$ to be the smallest size of a nonempty set $A \subset \mathbb{N}_0$ such that A is fibered on each scale $s \in S$. For any such A, we clearly have $\Phi_s \mid A$ for each $s \in S$ (although A may also have other cyclotomic divisors). Hence

$$\mathsf{MIN}(S) \le \mathsf{FIB}(S). \tag{1.6}$$

An easy case when the equality holds in (1.6) is as follows.

Lemma 1.1. *Let p be a prime number. Assume that $S = \{p^{\alpha_1}, \dots, p^{\alpha_m}\}$, where $\alpha_1, \dots, \alpha_m \in \mathbb{N}$ are all distinct. Then*

$$\mathit{MIN}(S) = \mathit{FIB}(S) = p^m. \tag{1.7}$$

Proof. Suppose that $\Phi_{p^{\alpha_1}}(X) \dots \Phi_{p^{\alpha_m}}(X)$ divides $A(X)$. Then

$$p^m = \Phi_{p^{\alpha_1}}(1) \dots \Phi_{p^{\alpha_m}}(1) \;\Big|\; A(1) = |A|.$$

In particular, $|A| \ge p^m$. Furthermore, let

$$A_0 := \left\{ \sum_{j=1}^{m} a_j p^{\alpha_j - 1} : \; a_j \in \{0, 1, \dots, p-1\}, \; j = 1, \dots, m \right\}.$$

Then $|A_0| = p^m$ (it is easy to see that the elements of A_0 listed above are all distinct), and by (1.1), A_0 has the mask polynomial $A_0(X) := \Phi_{p^{\alpha_1}}(X) \dots \Phi_{p^{\alpha_m}}(X)$. Since

$$\Phi_{p^\alpha}(X) = 1 + X^{p^{\alpha-1}} + \dots + X^{(p-1)p^{\alpha-1}} = F_p^{p^\alpha}(X),$$

A_0 is fibered on each of the scales $p^{\alpha_1}, \dots, p^{\alpha_m}$. This proves the lemma. □

The question is significantly more difficult when $\operatorname{lcm}(S)$ has two or more distinct prime factors. In Section 7, we investigate several special cases when (1.6) holds with equality. In particular, we prove the following.

Theorem 1.2. *Let $S \subset (\mathbb{N} \setminus \{1\})$ satisfy $1 \le |S| \le 3$, and assume that $\operatorname{lcm}(S)$ has at most two distinct prime factors. Then $\mathit{MIN}(S) = \mathit{FIB}(S)$.*

However, it is also possible for the inequality to be strict, and this can happen even if $\operatorname{lcm}(S)$ has only two prime factors.

Theorem 1.3. *There exist finite and nonempty sets $S \subset (\mathbb{N} \setminus \{1\})$ such that*

$$\mathit{MIN}(S) < \mathit{FIB}(S)$$

and $\operatorname{lcm}(S)$ has two distinct prime factors.

1.3. Integer tilings and the Coven-Meyerowitz conjecture

Let $A \subset \mathbb{Z}$ be finite and nonempty. We say that A *tiles the integers by translations* if there exists a translation set $T \subset \mathbb{Z}$ such that every integer $n \in \mathbb{Z}$ can be written uniquely as $n = a + t$ with $a \in A$ and $t \in T$.

It is well known [17] that any tiling of $\mathbb{Z}$ by a finite set A must be periodic, so that there exists an $M \in \mathbb{N}$ and a finite set $B \subset \mathbb{Z}$ such that $T = B \oplus M\mathbb{Z}$. In other words, $A \oplus B \bmod M$ is a factorization of the cyclic group $\mathbb{Z}_M$. We write this as

$$A \oplus B = \mathbb{Z}_M. \tag{1.8}$$

By translational invariance, we may assume that $A, B \subset \mathbb{N}_0$. Then (1.8) can be rewritten in terms of the mask polynomials of A and B:

$$A(X)B(X) \equiv 1 + X + \cdots + X^{M-1} \mod (X^M - 1). \tag{1.9}$$

Since $1 + X + \cdots + X^{M-1} = \prod_{s|M, s\neq 1} \Phi_s(X)$, (1.8) is further equivalent to

$$|A||B| = M \text{ and } \Phi_s(X) \mid A(X)B(X) \text{ for all } s \mid M,\ s \neq 1. \tag{1.10}$$

Since Φ_s are irreducible in $\mathbb{Q}[x]$, each $\Phi_s(X)$ with $s \mid M$ must divide at least one of $A(X)$ and $B(X)$.

Let S_A^* be the set of all prime powers p^α such that $\Phi_{p^\alpha}(X)$ divides $A(X)$. Consider the following conditions:

(T1) $|A| = A(1) = \prod_{s\in S_A^*} \Phi_s(1)$,

(T2) if $s_1, \ldots, s_k \in S_A^*$ *are powers of distinct primes, then* $\Phi_{s_1 \ldots s_k}(X)$ *divides* $A(X)$.

Coven and Meyerowitz [3] proved the following theorem.

Theorem 1.4. *[3] Let $A \subset \mathbb{N} \cup \{0\}$ be a finite set. Then:*

- *if A satisfies (T1), (T2), then A tiles $\mathbb{Z}$;*
- *if A tiles $\mathbb{Z}$ then (T1) holds;*
- *if A tiles $\mathbb{Z}$ and $|A|$ has at most two distinct prime factors, then (T2) holds.*

Any $A \subset \mathbb{N}_0$, regardless of tiling properties, satisfies $\prod_{s\in S_A^*} \Phi_s(1) \mid |A|$. The property (T1) follows then from an easy counting argument; the same argument also implies that if $A \oplus B = \mathbb{Z}_M$, then any prime power cyclotomic polynomial Φ_{p^α} with $p^\alpha \mid M$ must divide exactly one of $A(X)$ and $B(X)$. See Lemma 9.1 in Section 9.1.

The second condition (T2) is much deeper and more difficult to prove. The statement that (T2) must hold for all finite sets A that tile the integers has become known in the literature as the *Coven-Meyerowitz conjecture*. Beyond Theorem 1.4, the methods of [3] allow further mild extensions under additional assumptions on the tiling period M, see

[9, Corollary 6.2], [15, Theorem 1.5], [23, Proposition 4.1], and the comments on [26]. More recently, further progress was made by Łaba and Londner [9–12]. The most general case where (T2) is currently known is given in [12, Corollary 1.4].

One possible avenue of approach is to consider (T1) as an upper bound on the size of A, and ask whether a set obeying this bound may have additional cyclotomic divisors that would allow a failure of (T2) for its tiling complement. The details are as follows.

Definition 1.5. Let $A \subset \mathbb{N}_0$, and let $\Phi_s(X) \mid A(X)$ for some $s \in \mathbb{N} \setminus \{1\}$. We say that Φ_s is an *unsupported divisor of* A if:

(i) for every prime p such that $p \mid s$, we have $p \mid |A|$,
(ii) for every prime power p^α such that $p^\alpha \parallel s$, we have $\Phi_{p^\alpha} \nmid A$.

Let $M \in \mathbb{N}$, and consider the following questions.

Question 1.6. If $A \subset \mathbb{Z}_M$ satisfies (T1), may it have unsupported divisors?

Question 1.7. If $A \subset \mathbb{Z}_M$ satisfies (T1) and (T2), may it have unsupported divisors?

Question 1.8. Assume that $A \oplus B = \mathbb{Z}_M$. If (T2) holds for A, must B also satisfy (T2)?

Trivially, the assumptions of Question 1.7 are stronger than those of Question 1.6, hence a positive answer to the latter for some M implies a positive answer to the former for the same M. Further, if the Coven-Meyerowitz conjecture is known to be true for some M (in other words, both sets A and B in any tiling $A \oplus B = \mathbb{Z}_M$ must satisfy (T2)), this implies a positive answer to Question 1.8 for the same M.

The next lemma states two less obvious relationships between the questions above and the Coven-Meyerowitz conjecture. To set the stage for it, we first note the following reduction from [3, Lemma 2.5] (see also [12, Lemma 6.2]). Suppose that the Coven-Meyerowitz conjecture fails for some tiling $A \oplus B = \mathbb{Z}_M$, so that one of the sets A and B does not satisfy (T2). Then there exists a tiling $A' \oplus B' = \mathbb{Z}_{M'}$ for some $M' \mid M$ (obtained from the original tiling $A \oplus B = \mathbb{Z}_M$ via an explicit reduction procedure) such that (T2) also fails for one of the sets A' and B', and, additionally, each prime factor of M' divides both $|A'|$ and $|B'|$. We may therefore focus on tilings with this additional condition.

Lemma 1.9. *Assume that $A \oplus B = \mathbb{Z}_M$ for some $M \in \mathbb{N}$, and that each prime factor of M divides both $|A|$ and $|B|$.*

(i) *Suppose that the answer to Question 1.6 is negative for this value of M. Then both sets A and B satisfy (T2).*
(ii) *Suppose that the answer to Question 1.7 is negative for this value of M. Then, if (T2) holds for A, it also must hold for B.*

Proof. Since $A \oplus B = \mathbb{Z}_M$, it follows from Theorem 1.4 that both A and B satisfy (T1). Suppose that one of the sets, say B, does not satisfy (T2). Then there exists $s \geq 2$ such that $s \mid M$ and $\Phi_s \nmid B$, but $\Phi_{p^\alpha} \mid B$ for every prime power $p^\alpha \parallel s$. By (1.10), we must have $\Phi_s \mid A$. Since (as pointed out above) no Φ_{p^α} may divide both A and B, Φ_s must be an unsupported divisor of A. This answers Question 1.6 in the negative for that value of M, and it further answers Question 1.7 in the negative for the same value of M if we assume that A satisfies (T2). □

It turns out that the answers to Questions 1.6 and 1.7, without further constraints on M, are positive. Our examples are as follows.

Theorem 1.10. *There exist $M \in \mathbb{N}$ and a nonempty set $A \subset \mathbb{Z}_M$ such that A satisfies (T1), M has two distinct prime divisors, and $A(X)$ has at least one unsupported cyclotomic divisor.*

Theorem 1.11. *There exist $M \in \mathbb{N}$ and a nonempty set $A \subset \mathbb{Z}_M$ such that A satisfies both (T1) and (T2), M has four distinct prime divisors, and $A(X)$ has at least one unsupported cyclotomic divisor.*

However, the answers may be negative under additional assumptions on the tiling period or the number of scales. Our next theorem is an example of this.

Theorem 1.12. *Assume that a nonempty set $A \subset \mathbb{Z}_M$ satisfies (T1) and (T2), and that M has at most two distinct prime divisors. Then $A(X)$ cannot have unsupported cyclotomic divisors.*

At this time, our constructions do not provide directly any new information on the Coven-Meyerowitz conjecture. Theorem 1.4 is already known when $|A|$ has at most two prime factors, and the set constructed in Theorem 1.11 does not appear to have tiling complements that do not obey (T2). Nonetheless, Lemma 1.9 implies that any counterexample to the Coven-Meyerowitz conjecture would have to involve a set that satisfies (T1) but has at least one unsupported divisor. Our examples may be viewed as a partial step in that direction. We discuss this in more detail in Section 10.2.

We end this section with a comment on Definition 1.5. If the condition (i) is dropped from that definition, then examples providing a positive answer to Questions 1.6 and 1.7 are much easier to construct. For instance, the set A in Example 8.1 satisfies (T1); it also satisfies (T2) trivially, since $|A|$ is a prime number. However, the additional cyclotomic divisor $\Phi_{p_1p_2}$ in that example satisfies $(p_1p_2, |A|) = 1$, and it is well known (see the paragraph before Lemma 1.9) that such divisors have no relevance to the Coven-Meyerowitz conjecture.

1.4. Organization of the paper

In Section 2, we transfer the problem to the setting of multisets in cyclic groups. We also review the basic cyclotomic divisibility tools available in the literature, such as array coordinates, grids, fibers, and cuboids. The fibered lower bound is discussed in detail in Section 3, where we also provide a way to evaluate it using the *assignment functions* defined there.

The next few sections are devoted to new methods developed for the purpose of this paper. We start with a truncation procedure (Section 4) that will allow us, in some cases, to simplify the question by removing "unnecessary" scales. This is also where we define the exponent sets $\mathsf{EXP}_i(S)$ used throughout the rest of the article. In Section 5, we set up multiscale cuboid arguments, similar to those in [9] and [13] (and based on them, to some extent) but adapted to our needs here. Finally, in Section 6 we prove a multiscale generalization of the de Bruijn-Rédei-Schoenberg structure theorem (Proposition 2.2) in terms of the *long fibers* defined there.

In Section 7, we identify several special cases when the equality $\mathsf{MIN}(S) = \mathsf{FIB}(S)$ holds. This includes the case when $|S| \le 3$ and $\operatorname{lcm}(S)$ has two distinct prime divisors (Theorem 7.6, proving Theorem 1.2 stated above), as well as certain cases when $\operatorname{lcm}(S)$ has more than two distinct prime factors but S has a particularly simple structure.

Examples with $\mathsf{MIN}(S) < \mathsf{FIB}(S)$ are presented in Section 8. After presenting a simple example with 3 prime factors (Example 8.1), in Section 8.2 we move on to the more difficult examples where $|A|$ has only 2 distinct prime factors. These examples prove Theorem 1.3, and, since they all satisfy (T1), they also prove Theorem 1.10.

Next, we address the more difficult Question 1.7 from Section 1.3. In Section 9.1, we prove a structure result under the (T2) assumption. In Section 9.2, we identify an easy case when the answer to Question 1.7 is negative. We then prove Theorem 1.12 in Section 9.3.

Finally, the example in Theorem 10.1 proves Theorem 1.11, with follow-up discussion in Section 10.2.

2. Cyclotomic divisibility tools

2.1. Multisets

It will be easier to work in a cyclic group setting. Suppose that we want to prove lower bounds on the size of sets $A \subset \mathbb{N}_0$ such that $\Phi_s(X) \mid A(X)$ for all s in a fixed, finite set $S \subset (\mathbb{N} \setminus \{1\})$. Let $M = \operatorname{lcm}(S)$, and consider $A \bmod M$ as a multiset in $\mathbb{Z}_M$ with the mask polynomial $A(X) \bmod (X^M - 1)$. For any $s \mid M$, we have $\Phi_s \mid (X^M - 1)$, so that $\Phi_s \mid A$ if and only if $\Phi_s \mid (A \bmod M)$. However, $A \bmod M$ need not be a set (since two or more elements of A may be congruent mod M), hence we need to introduce notation for multisets in $\mathbb{Z}_M$.

We use $\mathcal{M}(\mathbb{Z}_M)$ to denote the set of all multisets in $\mathbb{Z}_M$ with weights in $\mathbb{Z}$ (so that both positive and negative weights are allowed). For $a \in \mathbb{Z}_M$, we write $w_A(a)$ to denote the weight of a in A. We also define the mask polynomial of the multiset A by

$$A(X) = \sum_{a \in \mathbb{Z}_M} w_A(a) X^a. \tag{2.1}$$

In particular, $A \in \mathcal{M}(\mathbb{Z}_M)$ is a set if and only if $w_A(x) \in \{0, 1\}$ for all $x \in \mathbb{Z}_M$. In that case, the above notation is consistent with the notation used in the introduction.

We use $A + B$ to denote the "weighted union" of multisets, so that $(A + B)(X) = A(X) + B(X)$ and $w_{A+B}(x) = w_A(x) + w_B(x)$. We use convolution notation for sumsets, with $(A * B)(X) = A(X)B(X)$. If $B = \{b\}$ is a singleton, we will write $b * A = B * A$. The *support* of a multiset $A \in \mathcal{M}(\mathbb{Z}_M)$ is the set $\{x \in \mathbb{Z}_M : \ w_A(x) \neq 0\}$. If $A \in \mathcal{M}(\mathbb{Z}_M)$ (not necessarily with positive weights), and if $Y \subset \mathbb{Z}_M$ is a set, we will use $A \cap Y$ to denote the restriction of A to Y. Thus $A \cap Y \in \mathcal{M}(\mathbb{Z}_M)$, with weights

$$w_{A \cap Y}(x) = w_A(x) w_Y(x).$$

For $A \in \mathcal{M}(\mathbb{Z}_M)$, we use $|A|$ to denote the "total mass" of A, defined by

$$|A| = \sum_{a \in \mathbb{Z}_M} w_A(a).$$

We use $\mathcal{M}^+(\mathbb{Z}_M)$ to denote the set of those multisets $A \in \mathcal{M}(\mathbb{Z}_M)$ whose weights are all nonnegative and whose total mass $|A|$ is positive. (The latter requirement guarantees that A is not the empty set.) Abusing the notation slightly, we will write that two multisets $A, B \in \mathcal{M}^+(\mathbb{Z}_M)$ satisfy $A \subset B$ if $w_A(x) \leq w_B(x)$ for all $x \in \mathbb{Z}_M$.

Our main results will be proved for multisets in cyclic groups, but it is easy to translate them back to the integer setting. In particular, with the above notation, we have

$$\mathsf{MIN}(S) = \min\{|A| : \ A \in \mathcal{M}^+(\mathbb{Z}_M), \ \Phi_s \mid A \text{ for all } s \in S\}, \tag{2.2}$$

for any M such that $\operatorname{lcm}(S) \mid M$. Indeed, if $A \subset \mathbb{N}_0$ is a set such that $\Phi_s \mid A$ for all $s \in S$, then the multiset $A' := (A \bmod M)$ in $\mathcal{M}^+(\mathbb{Z}_M)$ satisfies $|A'| = |A|$ and $\Phi_s \mid A'(X)$ for all $s \in S$. Conversely, let $A' \in \mathcal{M}^+(\mathbb{Z}_M)$ be a multiset such that $\Phi_s \mid A'$ for all $s \in S$. We represent $\operatorname{supp}(A') \subset \mathbb{Z}_M$ as a subset of $\{0, 1, \ldots, M-1\}$, and let

$$A := \bigcup_{a \in \operatorname{supp}(A')} \{a, a + M, \ldots, a + (w_A(a) - 1)M\}.$$

Then $A \subset \mathbb{N}_0$ is a set with $|A'| = |A|$, and since $A(X) \equiv A'(X)$ modulo $X^M - 1$, divisibility by all Φ_s with $s \in S$ is preserved.

2.2. Coordinates, grids, fibers

Let $M = \prod_{i=1}^{K} p_i^{n_i}$ be the prime number factorization of M, where $p_1, \dots, p_K$ are distinct primes and $n_1, \dots, n_K \in \mathbb{N}$. By the Chinese Remainder Theorem, we may represent $\mathbb{Z}_M$ as

$$\mathbb{Z}_M = \bigoplus_{i=1}^{K} \mathbb{Z}_{p_i^{n_i}},$$

which may be viewed geometrically as a K-dimensional lattice. We define an explicit coordinate system on $\mathbb{Z}_M$ as follows. Let $M_i = M/p_i^{n_i} = \prod_{j \neq i} p_j^{n_j}$. Each $x \in \mathbb{Z}_M$ may then be written uniquely as

$$x = \sum_{i=1}^{K} x_i M_i, \quad x_i \in \mathbb{Z}_{p_i^{n_i}}. \tag{2.3}$$

We will often need to work on many scales $N \mid M$, each scale corresponding to a different cyclotomic divisor of $A(X)$. Given $N \mid M$, any multiset $A \in \mathcal{M}(\mathbb{Z}_M)$ induces a multiset $(A \bmod N) \in \mathcal{M}(\mathbb{Z}_N)$, with weights

$$w_A^N(x) = \sum_{y \in \mathbb{Z}_M, y \equiv x \bmod N} w_A(y).$$

To simplify the notation, we will continue to denote this multiset by A (instead of $A \bmod N$) whenever this does not cause confusion. The mask polynomial of $A \bmod N$ is $(A \bmod N)(X) = A(X) \bmod (X^N - 1)$. For any $s \mid N$ we have $\Phi_s(X) \mid X^N - 1$, so that $\Phi_s(X) \mid A(X)$ if and only if $\Phi_s(X) \mid (A \bmod N)(X)$.

For $p_j \mid N \mid M$, a *p_j-fiber on scale N* is a translate of any set F_j^N such that

$$F_j^N \equiv \{0, N/p_j, 2N/p_j, \dots, (p_j - 1)N/p_j\} \mod N \tag{2.4}$$

with p_j indicating the *direction* of the fiber. Equivalently, (2.4) may be written as

$$F_j^N(X) \equiv 1 + X^{N/p_j} + \cdots + X^{(p_j-1)N/p_j} \mod X^N - 1.$$

Note that our terminology is slightly different from the convention in [9,10]. We also note a slight inconsistency with the notation in (1.4); however, this should not cause problems, since it will always be clear from the context whether the subscript refers to the actual prime or to its index in the list $\{p_1, \dots, p_K\}$.

We will say that a multiset $A \in \mathcal{M}(\mathbb{Z}_M)$ is *fibered in the p_j direction on scale N*, or p_j-fibered on scale N for short, if there is a polynomial $Q(X)$ with nonnegative integer coefficients such that

$$A(X) \equiv Q(X)F_j^N(X) \mod X^N - 1. \tag{2.5}$$

For $D \mid N \mid M$, a *D-grid* in $\mathbb{Z}_N$ is a set of the form

$$\Lambda^N(x, D) := x * D\mathbb{Z}_N = \{x' \in \mathbb{Z}_N : \ D \mid (x - x')\}$$

for some $x \in \mathbb{Z}_N$. In other words, a D-grid is a coset of $D\mathbb{Z}_N \simeq \mathbb{Z}_{N/D}$ in $\mathbb{Z}_N$.

When $N = M$, we will omit the superscript M to simplify the notation, so that $F_j = F_j^M$ and $\Lambda(x, D) = \Lambda^M(x, D)$.

2.3. Cuboids

We will use the following notation from [9]. For multisets $\Delta \in \mathcal{M}(\mathbb{Z}_N)$, where $N \mid M$, we define the *Δ-evaluations of $A \in \mathcal{M}(\mathbb{Z}_M)$ in $\mathbb{Z}_N$:*

$$\mathbb{A}^N[\Delta] = \sum_{x \in \mathbb{Z}_N} w_A^N(x) w_\Delta^N(x). \tag{2.6}$$

The following special case is of particular interest.

Definition 2.1. Let M and N be as above, and let $\mathfrak{J} = \{j \in \{1, \ldots, K\} : \ p_j \mid N\}$. An *$N$-cuboid* is a multiset $\Delta \in \mathcal{M}(\mathbb{Z}_N)$ associated with a mask polynomial of the form

$$\Delta(X) = X^c \prod_{j \in \mathfrak{J}} (1 - X^{d_j N/p_j}) \tag{2.7}$$

with $(d_j, p_j) = 1$ for all $j \in \mathfrak{J}$.

The geometric interpretation of N-cuboids, where $N = \prod_{j=1}^K p_j^{\alpha_j}$, is as follows. Let

$$\mathcal{P}(N) := \{p : \ p \mid N, \ p \text{ is prime}\}, \tag{2.8}$$

$$D(N) := \frac{N}{\prod_{p \in \mathcal{P}(N)} p} = \prod_{j=1}^K p_j^{\gamma_j}, \quad \text{where } \gamma_j = \max(0, \alpha_j - 1) \text{ for } j = 1, \ldots, K. \tag{2.9}$$

(The denominator $\prod_{p \in \mathcal{P}(N)} p$ is also known as the *radical* of N.) Then the "vertices" of a cuboid Δ,

$$x_{\vec{\epsilon}} := c + \sum_{j \in \mathfrak{J}} \epsilon_j d_j \frac{N}{p_j} : \vec{\epsilon} \in \{0, 1\}^{|\mathfrak{J}|},$$

form a full-dimensional rectangular box in the grid $\Lambda^N(c, D(N))$, with one vertex at c and alternating ± 1 weights

$$w_\Delta(x_{\vec{\epsilon}}) = (-1)^{\sum_{j\in\Im}\epsilon_j}.$$

The following cyclotomic divisibility test has been known and used previously in the literature. The equivalence between (i) and (iii) is the de Bruijn-Rédei-Schoenberg theorem on the structure of vanishing sums of roots of unity (see [4,14,16,19,20,22]). For the equivalence (i) ⇔ (ii), see e.g. [24, Section 3], [7, Section 3].

Proposition 2.2. *Let $A \in \mathcal{M}(\mathbb{Z}_M)$. Then the following are equivalent:*

(i) $\Phi_N(X) \mid A(X)$,
(ii) *For all N-cuboids Δ, we have $\mathbb{A}^N[\Delta] = 0$,*
(iii) *A mod N is a linear combination of N-fibers, so that*

$$A(X) = \sum_{i:p_i|N} P_i(X)F_i^N(X) \mod X^N - 1,$$

where $P_i(X)$ have integer (but not necessarily nonnegative) coefficients.

Proposition 2.2 can be strengthened if N has only two distinct prime factors. This goes back to the work of de Bruijn [4]; a self-contained proof is provided in [14, Theorem 3.3].

Lemma 2.3. *Let $A \in \mathcal{M}^+(\mathbb{Z}_M)$. Assume that $\Phi_N \mid A$, where N has two distinct prime factors p_1, p_2. Then A mod N is a linear combination of N-fibers with nonnegative weights. In other words,*

$$A(X) = P_1(X)F_1^N(X) + P_2(X)F_2^N(X) \mod X^N - 1,$$

where P_1, P_2 are polynomials with nonnegative coefficients.

It is well known that the positivity in Lemma 2.3 does not hold when N has 3 or more distinct prime factors. There are many examples of this in the literature, see e.g., the "minimal relations" listed by Poonen and Rubinstein [18, Table 1] (see also [2]), or the unfibered structures in [10, Sections 5 and 6] in the case when N has 3 prime factors.

The following consequence of Proposition 2.2 will be used often.

Lemma 2.4. *Assume that $N \mid M$ and $A \in \mathcal{M}(\mathbb{Z}_M)$. Then $\Phi_N \mid A$ if and only if $\Phi_N \mid (A \cap \Lambda)$ for every $D(N)$-grid Λ in $\mathbb{Z}_M$.*

Proof. This follows by replacing $A \in \mathcal{M}(\mathbb{Z}_M)$ by $(A \bmod N) \in \mathcal{M}(\mathbb{Z}_N)$ as described above, then applying the equivalence (i) ⇔ (ii) in Proposition 2.2. □

3. Lower bound for fibered sets

Let $M = \prod_{k=1}^{K} p_k^{n_k}$, where $p_1, \dots, p_K$ are distinct primes and $n_1, \dots, n_K \in \mathbb{N}$. For $s \in \mathbb{N}$, we will use the notation

$$\mathcal{D}(s) := \{d \in \mathbb{N} : \ d \mid s, \ d \neq 1\}.$$

Let $S \subset \mathcal{D}(M)$ be non-empty, and let $\mathsf{MIN}(S)$ be given by (2.2). Recall also that in Section 1.2 we defined $\mathsf{FIB}(S)$ to be the minimal size of a nonempty set $A \subset \mathbb{N}_0$ such that A is fibered in some direction on each scale $s \in S$. By the same argument as in the proof of (2.2), we may consider multisets $A \in \mathcal{M}^+(\mathbb{Z}_M)$ instead of sets $A \subset \mathbb{N}_0$. We now indicate how to evaluate $\mathsf{FIB}(S)$.

Definition 3.1. Let $S \subset \mathcal{D}(M)$. An *assignment function* is any function $\sigma : S \to \{1, \dots, K\}$ such that

$$\sigma(s) \in \{i : p_i \mid s\}.$$

Given $A \in \mathcal{M}^+(\mathbb{Z}_M)$ and an assignment function σ, we say that A is (S, σ)-*fibered* if, for every $s \in S$, the associated multiset A mod s is fibered in the $p_{\sigma(s)}$ direction on the scale s.

Proposition 3.2. *Let $S \subset \mathcal{D}(M)$, and let $\sigma : S \to \{1, \dots, K\}$ be an assignment function. For each i, let*

$$\mathit{EXP}_i(S, \sigma) := \{\alpha \in \mathbb{N} : \exists\, s \in S \text{ with } (s, p_i^{n_i}) = p_i^{\alpha} \text{ and } \sigma(s) = i\}.$$

(We emphasize that the exponent 0 is not included above.) Let $E_i(S, \sigma) := \#\mathit{EXP}_i(S, \sigma)$, and

$$\mathit{FIB}(S, \sigma) := p_1^{E_1(S,\sigma)} \cdots p_K^{E_K(S,\sigma)}.$$

In the special case when $\sigma(s) \equiv i$ for all $s \in S$, we will write $\mathit{FIB}(S, \sigma) = \mathit{FIB}(S, i)$.

Then

$$\mathit{FIB}(S) = \min_{\sigma} \mathit{FIB}(S, \sigma), \tag{3.1}$$

with the minimum taken over all assignment functions σ. In particular, we have $\mathit{MIN}(S) \leq \min_\sigma \mathit{FIB}(S, \sigma)$.

Proof. We first prove that $\mathsf{FIB}(S) \geq \min_\sigma \mathsf{FIB}(S, \sigma)$. Indeed, suppose that $A \in \mathcal{M}^+(\mathbb{Z}_M)$ is fibered on each scale $s \in S$. Then for each $s \in S$ there exists a prime $p_{i(s)} \mid s$ such that A is fibered in the $p_{i(s)}$ direction on scale s. This defines an assignment function

via $\sigma(s) = i(s)$ such that A is (S, σ)-fibered. We fix this σ, and write $E_i := E_i(S, \sigma)$ for short.

Next, we claim that

$$\text{if } A \text{ is } (S,\sigma)\text{-fibered, then } \mathsf{FIB}(S,\sigma) \mid |A|. \tag{3.2}$$

In particular, $|A| \geq \mathsf{FIB}(S, \sigma)$ as required. To prove (3.2), it suffices to prove that $p_i^{E_i} \mid |A|$ for each $i \in \{1, \dots, K\}$. Fix such i, assume that

$$\mathsf{EXP}_i(S,\sigma) = \{\alpha_1, \dots, \alpha_{E_i}\}$$

(if this is an empty set, then $E_i = 0$ and there is nothing to prove), and let $s_1, \dots, s_{E_i}$ be elements of S such that $\sigma(s_j) = i$ and $p_i^{\alpha_j} \parallel s_j$. Since A is p_i-fibered on each scale s_j, we have

$$F_i^{s_j}(X) \mid A(X) \mod (X^{s_j} - 1),$$

where $F_i^{s_j}(X) = (X^{s_j} - 1)/(X^{s_j/p_i} - 1)$. Since $p_i^{\alpha_j}$ divides s_j but not s_j/p_i, it follows that $\Phi_{p_i^{\alpha_j}} \mid A$. Therefore

$$p_i^{E_i} = \Phi_{p_i^{\alpha_1}}(1) \dots \Phi_{p_i^{\alpha_{E_i}}}(1) \mid A(1) = |A|,$$

proving (3.2).

For the converse inequality, given an assignment function σ, we give an explicit "standard" (S, σ)-fibered set $A^\flat = A^\flat_{S,\sigma}$ such that $|A^\flat| = \mathsf{FIB}(S, \sigma)$ and $\Phi_s \mid A$ for all $s \in S$. The construction follows [3] and was also used in [9,10] in the context of integer tilings. Let $M_i := M/p_i^{n_i}$, and define

$$\begin{aligned} A^\flat(X) &= \prod_{i=1}^{K} \left[\prod_{\beta \in \mathsf{EXP}_i(S,\sigma)} \Phi_{p_i}\left(X^{M_i p_i^{\beta-1}}\right) \right] \\ &= \prod_{i=1}^{K} \left[\prod_{\beta \in \mathsf{EXP}_i(S,\sigma)} \left(1 + X^{M_i p_i^{\beta-1}} + \dots + X^{(p_i-1)M_i p_i^{\beta-1}}\right) \right]. \end{aligned} \tag{3.3}$$

Since $\Phi_p(1) = p$ for prime p, we have

$$|A^\flat| = A^\flat(1) = \prod_{i=1}^{K} \left[\prod_{\beta \in \mathsf{EXP}_i(S,\sigma)} p_i \right] = \mathsf{FIB}(S,\sigma).$$

Next, let $s \in S$, and let $i = \sigma(s)$ so that $p_i^\beta \parallel s$ for some $\beta \in \mathsf{EXP}_i(S, \sigma)$. Observe that

$$\Phi_{p_i}\big(X^{M_i p_i^{\beta-1}}\big) = \frac{1-X^{M_i p_i^{\beta}}}{1-X^{M_i p_i^{\beta-1}}} = \prod_{u \mid M_i p_i^{\beta}, u \nmid M_i p_i^{\beta-1}} \Phi_u(X), \tag{3.4}$$

$$F_i^s(X) = \frac{1-X^s}{1-X^{s/p_i}} = \prod_{u \mid s, u \nmid (s/p_i)} \Phi_u(X). \tag{3.5}$$

Hence, we have the chain of divisibility

$$\Phi_s(X) \;\Big|\; F_i^s(X) \;\Big|\; \Phi_{p_i}\left(X^{M_i p_i^{\beta-1}}\right) \;\Big|\; A^{\flat}(X),$$

proving both $\Phi_s \mid A^{\flat}$ and the fibering claim. □

4. A truncation procedure

We introduce a truncation procedure that will allow us to reduce proving upper or lower bounds on $\mathsf{MIN}(S)$ to proving similar bounds with S replaced by a simpler set. Let $M = \prod_{k=1}^{K} p_k^{n_k}$, where $p_1, \dots, p_K$ are distinct primes and $n_1, \dots, n_K \in \mathbb{N}$. We continue to use the coordinate representation

$$\mathbb{Z}_M \ni x \equiv x_1 M_1 + \cdots + x_K M_K \mod M,$$

where $M_i = M/p_i^{n_i}$ and $x_i \in \mathbb{Z}_{p_i^{n_i}}$. We will also need the p_i-adic expansion of x_i:

$$x_i \equiv x_{i,0} + x_{i,1} p_i + \cdots + x_{i,n_i-1} p_i^{n_i-1} \mod p_i^{n_i},\ x_{i,j} \in \{0, 1, \dots, p_i - 1\}. \tag{4.1}$$

For $S \subset \mathcal{D}(M)$ and $1 \le i \le K$, we define

$$\mathsf{EXP}_i(S) := \{\alpha \ge 1 :\ \exists\, s \in S \text{ with } p_i^{\alpha} \mid\mid s\}, \quad E_i := \#\mathsf{EXP}_i(S). \tag{4.2}$$

It will be useful to arrange the sets $\mathsf{EXP}_i(S)$ in increasing order:

$$\mathsf{EXP}_i(S) := \{\alpha_{i,1}, \cdots, \alpha_{i,E_i}\}, \quad 1 \le \alpha_{i,1} < \cdots < \alpha_{i,E_i}. \tag{4.3}$$

Let us use the convention $\alpha_{i,0} = 0$. We then have the following proposition.

Proposition 4.1. ***(Truncations)*** *Let $S \subset \mathcal{D}(M)$, and let $A \in \mathcal{M}(\mathbb{Z}_M)$ satisfy $\Phi_s \mid A$ for all $s \in S$. Define $M' := p_1^{E_1} \cdots p_K^{E_K}$. Then, there exists a multiset $A' \in \mathcal{M}(\mathbb{Z}_{M'})$ satisfying*

(i) $A'(1) = A(1)$,
(ii) *For every $N = p_1^{\alpha_{1,\ell_1}} \cdots p_K^{\alpha_{K,\ell_K}}$ with $\Phi_N(x) \mid A(x)$, we have $\Phi_{N'}(X) \mid A'(X)$, where $N' := p_1^{\ell_1} \cdots p_K^{\ell_K} \mid M'$.*

Furthermore, if $A \in \mathcal{M}^+(\mathbb{Z}_M)$, then $A' \in \mathcal{M}^+(\mathbb{Z}_{M'})$.

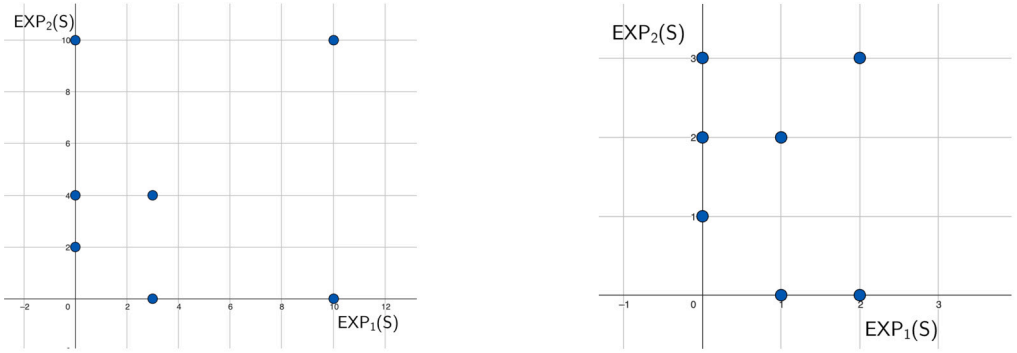


Fig. 1. The cyclotomic divisors of A and the cyclotomic divisors of A'.

Proposition 4.1 allows us to assume that $\mathsf{EXP}_i(S) = \{1, 2, \dots, E_i\}$ for every $i \in \{1, \dots, K\}$, so that there are no gaps in our set of exponents. We refer to the multiset $A' \in \mathcal{M}(\mathbb{Z}_{M'})$ in Proposition 4.1 as the *truncation of A relative to S*.

Example 4.2. Suppose that $\Phi_s \mid A$ for all $s \in S$, where

$$S := \{p_2^2, p_1^3, p_2^4, p_1^3 p_2^4, p_1^{10}, p_2^{10}, p_1^{10} p_2^{10}\}.$$

Then, $\mathsf{EXP}_1(S) = \{3, 10\}$ and $\mathsf{EXP}_2(S) = \{2, 4, 10\}$ so that $M' := p_1^{E_1} p_2^{E_2} = p_1^2 p_2^3$. Proposition 4.1 then furnishes a multiset $A' \in \mathcal{M}(\mathbb{Z}_{p_1^2 p_2^3})$ such that $A'(1) = A(1)$ and $\Phi_s \mid A'$ for all $s \in S' := \{p_1, p_2, p_1^2, p_2^2, p_1 p_2^2, p_2^3, p_1^2 p_2^3\}$. The exponent sets associated to A' are $\{1, 2\}$ and $\{1, 2, 3\}$, with no gaps (Fig. 1).

We now begin the proof of Proposition 4.1. We first define a family of mappings on $\mathbb{Z}_M$ which preserve cyclotomic divisibility on the scales we need, but remove "unnecessary" p_i-adic digits.

Definition 4.3. Let $i \in \{1, \dots, K\}$ and $1 \le \alpha \le n_i$ be given. Recalling the p_i-adic expansion of $x_i \in \mathbb{Z}_{p_i^{n_i}}$ given in (4.1), we define a mapping $T_i^\alpha : \mathbb{Z}_{p_i^{n_i}} \to \mathbb{Z}_{p_i^{n_i}}$ by writing

$$T_i^\alpha(x_i) := x_i - x_{i,\alpha-1} p_i^{\alpha-1}, \quad \forall x_i \in \mathbb{Z}_{p_i^{n_i}},$$

so that T_i^α sends the α-scale coordinate of x_i to zero. We further define a mapping $\mathbf{T}_i^\alpha : \mathbb{Z}_M \to \mathbb{Z}_M$ by writing in array coordinates,

$$\mathbf{T}_i^\alpha(x_1, \dots, x_K) := \big(x_1, \dots, T_i^\alpha(x_i), \dots, x_K\big), \quad \forall (x_1, \dots, x_K) \in \mathbb{Z}_{p_1^{n_1}} \times \cdots \times \mathbb{Z}_{p_K^{n_K}}.$$

We note that $\mathbf{T}_i^\alpha$ has the following property:

$$\forall y, z \in \mathbb{Z}_M, \quad y_{j,\beta} = z_{j,\beta} \;\Rightarrow (\mathbf{T}_i^\alpha(y))_{j,\beta} = (\mathbf{T}_i^\alpha(z))_{j,\beta} \tag{4.4}$$

for all $j \in \{1, \dots, K\}$ and $\beta \in \{0, 1, \dots, n_j - 1\}$. In other words, if some of the multiscale digits of y, z are equal, then the corresponding digits of their images under $\mathbf{T}_i^\alpha$ are also equal. The converse implication fails when $j = i$ and $\beta = \alpha - 1$, since then the corresponding (possibly non-equal) coordinates of y and z are both sent to 0.

Lemma 4.4. *Let $N \mid M$ with $p_i^\beta \parallel N$ for some $0 \le \beta \le n_i$ and let $1 \le \alpha \le n_i$ be given. Let $F \in \mathcal{M}^+(\mathbb{Z}_M)$ satisfy $F \equiv x * F_j^N$ mod N for some $p_j \mid N$ and $x \in \mathbb{Z}_N$. Assume that at least one of the following holds:*

(i) $j \neq i$,
(ii) $\beta \neq \alpha$.

Then $\mathbf{T}_i^\alpha(F) \equiv \mathbf{T}_i^\alpha(x) * F_j^N$ mod N.

Proof. Let N and F be as in the statement of the lemma. This means that F is a set of p_j elements such that if $y, z \in F$ are distinct, then $(y - z, N) = N/p_j$. It suffices to prove that for any such y, z we also have

$$(\mathbf{T}_i^\alpha(y) - \mathbf{T}_i^\alpha(z), N) = N/p_j.$$

Let $y, z \in F$ be distinct, and let $N = \prod p_\ell^{\beta_\ell}$ be the prime factorization of N, so that $\beta_i = \beta$. We need to prove that

$$\left(\mathbf{T}_i^\alpha(y) - \mathbf{T}_i^\alpha(z), p_\ell^{\beta_\ell}\right) = \begin{cases} p_\ell^{\beta_\ell} & \text{if } \ell \neq j, \\ p_j^{\beta_j - 1} & \text{if } \ell = j. \end{cases} \tag{4.5}$$

We have

$$\mathbf{T}_i^\alpha(y) - \mathbf{T}_i^\alpha(z) = (y - z) - (y_{i,\alpha-1} - z_{i,\alpha-1}) p_i^{\alpha-1} M_i.$$

We consider three cases.

- If $\ell \neq i$, then $p_\ell^{\beta_\ell} \mid M_i$, so that $(\mathbf{T}_i^\alpha(y) - \mathbf{T}_i^\alpha(z), p_\ell^{\beta_\ell}) = (y - z, p_\ell^{\beta_\ell})$ and (4.5) follows.
- Suppose $\ell = i$ but $i \neq j$. Then $p_i^\beta \mid y - z$, so that $y_{i,\gamma} = z_{i,\gamma}$ for $\gamma \le \beta - 1$. By (4.4), the same holds for the corresponding digits of $\mathbf{T}_i^\alpha(y)$ and $\mathbf{T}_i^\alpha(z)$, implying (4.5).
- Finally, assume that $\ell = i = j$. Then $p_i^{\beta-1} \parallel (y - z)$, so that $y_{i,\beta-1} \neq z_{i,\beta-1}$ and $y_{i,\gamma} = z_{i,\gamma}$ for $\gamma < \beta - 1$. By (4.4), we have $(\mathbf{T}_i^\alpha(y))_{i,\gamma} = (\mathbf{T}_i^\alpha(z))_{i,\gamma}$ for $\gamma < \beta - 1$. Furthermore, since $\beta \neq \alpha$ in this case, we have

  $$(\mathbf{T}_i^\alpha(y))_{i,\beta-1} = y_{i,\beta-1} \neq z_{i,\beta-1} = (\mathbf{T}_i^\alpha(z))_{i,\beta-1}.$$

  Hence $p_i^{\beta-1} \parallel (\mathbf{T}_i^\alpha(y) - \mathbf{T}_i^\alpha(z))$, and (4.5) holds again. □

Corollary 4.5. *Let $S \subset \mathcal{D}(M)$, and let $A \in \mathcal{M}(\mathbb{Z}_M)$ satisfy $\Phi_s \mid A$ for all $s \in S$. Assume that $\alpha \notin \mathit{EXP}_i(S)$. Then $\Phi_s \mid \mathbf{T}_i^\alpha(A)$ for all $s \in S$.*

Proof. Let S and A satisfy the assumptions of the corollary. Fix $N \in S$. By the de Bruijn-Rédei-Schoenberg theorem (the equivalence of (i) and (iii) in Proposition 2.2), we may write

$$A(X) \equiv \sum_{j:p_j \mid N} Q_j(X) F_j^N(X) \mod (X^N - 1),$$

where Q_j are polynomials with integer coefficients. Since $\alpha \notin \mathsf{EXP}_i(S)$, the assumptions of Lemma 4.4 are satisfied, hence $\mathbf{T}_i^\alpha$ maps each fiber $x * F_j^N \bmod N$ to a fiber $\mathbf{T}_i^\alpha(x) * F_j^N \bmod N$. It follows that $\mathbf{T}_i^\alpha(A)$ can also be written as a linear combination of fibers on scale N, and another application of the equivalence (i)$\Leftrightarrow$(iii) in Proposition 2.2 proves that $\Phi_N \mid \mathbf{T}_i^\alpha(A)$. □

Corollary 4.6. *For $S \subset \mathcal{D}(M)$, we define a mapping $\mathbb{T}_S : \mathbb{Z}_M \to \mathbb{Z}_M$ via*

$$\mathbb{T}_S(x_1, \dots, x_K) := \left(\sum_{\alpha_1 \in \mathit{EXP}_1(S)} x_{1,\alpha_1 - 1} p_1^{\alpha_1 - 1}, \cdots, \sum_{\alpha_K \in \mathit{EXP}_K(S)} x_{K,\alpha_K - 1} p_K^{\alpha_K - 1} \right). \quad (4.6)$$

Assume that $A \in \mathcal{M}(\mathbb{Z}_M)$ satisfies $\Phi_s \mid A$ for all $s \in S$. Then the multiset $\mathbb{T}_S(A) \in \mathcal{M}(\mathbb{Z}_M)$, with weight function

$$w_{\mathbb{T}_S(A)}(x) := \sum_{\{y:\ \mathbb{T}_S(y) = x\}} w_A(y) \quad \forall x \in \mathbb{Z}_M, \quad (4.7)$$

satisfies $\Phi_s \mid \mathbb{T}_S(A)$ for all $s \in S$. Furthermore, if $A \in \mathcal{M}^+(\mathbb{Z}_M)$, then $\mathbb{T}_S(A) \in \mathcal{M}^+(\mathbb{Z}_M)$.

Proof. This follows by observing that $\mathbb{T}_S$ is the composition of the mappings $\mathbf{T}_i^\alpha$, where (i, α) runs over all pairs such that $i \in \{1, \dots, K\}$ and $\alpha \in \{1, \dots, n_i\} \setminus \mathsf{EXP}_i(S)$, and applying Corollary 4.5 iteratively to each such mapping. The last statement is a consequence of (4.7). □

Proof of Proposition 4.1. Let S, A, and M' be as in the statement of the proposition. We enumerate the elements of each set $\mathsf{EXP}_i(S)$ in increasing order as in (4.3). We also equip $\mathbb{Z}_{M'}$ with a standard coordinate system similar to that in $\mathbb{Z}_M$.

We first let $\tilde{A} := \mathbb{T}_S(A) \in \mathcal{M}(\mathbb{Z}_M)$, then $|\tilde{A}| = |A|$ and $\Phi_s \mid A$ for all $s \in S$ by Corollary 4.6. We further have $\mathrm{supp}(\tilde{A}) \subset Y$, where

$$Y := \mathbb{T}_S(\mathbb{Z}_M) = \{y \in \mathbb{Z}_M :\ y_{i,\alpha} = 0 \text{ for all } (i, \alpha) \text{ such that } \alpha \notin \mathsf{EXP}_i(S)\}.$$

We define a bijection $\mathbb{U} : Y \to \mathbb{Z}_{M'}$ by

$$\mathbb{U}\left(\sum_{j=0}^{E_1-1} x_{1,j}p_1^{\alpha_{1,j}-1},\cdots,\sum_{j=0}^{E_K-1} x_{K,j}p_K^{\alpha_{K,j}-1}\right)=\left(\sum_{j=0}^{E_1-1} x_{1,j}p_1^{j},\cdots,\sum_{j=0}^{E_K-1} x_{K,j}p_K^{j}\right).$$

Let $A'\in\mathcal{M}(\mathbb{Z}_{M'})$ be the multiset defined via the weight equality

$$w_{A'}^{M'}(x):=w_{\tilde{A}}(\mathbb{U}^{-1}(x)),\quad \forall x\in\mathbb{Z}_{M'}. \tag{4.8}$$

We clearly have $|A'|=|\tilde{A}|=|A|$. It remains to prove that

$$\text{if } N=p_1^{\alpha_{1,\ell_1}}\cdots p_K^{\alpha_{K,\ell_K}}\in S,\ \text{then } \Phi_{N'}(X)\mid A'(X),\ \text{where } N':=p_1^{\ell_1}\cdots p_K^{\ell_K}.$$

Let $N\in S$, then $\Phi_N\mid\tilde{A}$ as noted above. By the equivalence (i)⇔(iii) in Proposition 2.2, $\tilde{A}$ may be written as a linear combination of fibers on scale N. However, $\mathbb{U}$ maps fibers on scale N in $\mathbb{Z}_M$ to fibers on scale N' in $\mathbb{Z}_{M'}$, so that A' is a linear combination of such fibers. By another application of Proposition 2.2, we have $\Phi_{N'}\mid A'$ as claimed. Finally, if $A\in\mathcal{M}^+(\mathbb{Z}_M)$, then $A'\in\mathcal{M}^+(\mathbb{Z}_{M'})$ by (4.8) and the last part of Corollary 4.6. □

5. A multiscale cuboid argument

Let $N\mid M$. Recall that we defined $D(N)$ and $\mathcal{P}(N)$ in (2.8) and (2.9). For $y\in\mathbb{Z}_N$, we continue to write

$$\Lambda(y,D(N)):=\{x\in\mathbb{Z}_N: D(N)\mid(x-y)\}. \tag{5.1}$$

Let $p\in\mathcal{P}(N)$ with $p^\alpha\mid\mid N$. For each $\nu\in\{0,1,\dots,p-1\}$, let $y_\nu=y+\nu N/p$. Then

$$\Lambda(y,D(N))=\bigcup_{\nu=0}^{p-1}\Lambda(y_\nu,pD(N)),$$

which corresponds to a decomposition of the original grid $\Lambda(y,D(N))$ into those parts which are contained in the planes $\Pi(y_\nu,p^\alpha):=\{x\in\mathbb{Z}_N: p^\alpha\mid(x-y_\nu)\}$.

Proposition 5.1. *Let $A\in\mathcal{M}^+(\mathbb{Z}_N)$. Suppose that $\Phi_N\mid A$ and that $p\in\mathcal{P}(N)$ with $p^\alpha\mid\mid N$. Then at least one of the following holds.*

(1) $\Phi_N\Phi_{N/p}\cdots\Phi_{N/p^\alpha}\mid A$.
(2) *For $\nu\in\{0,1,\dots,p-1\}$ and $a\in A$, define the multisets $A_{\nu,a}\subset A$ by*

$$A_{\nu,a}:=A\cap\Lambda(y_\nu,pD(N)) \tag{5.2}$$

where $y_\nu=a+\nu N/p$. Then there exists some $a\in A$ such that $A_{\nu,a}$ are nonempty for all $\nu\in\{0,1,\dots,p-1\}$.

The proof of Proposition 5.1 is based on multiscale cuboid argument similar to that in [9, Section 5]. To simplify notation, we fix $N \mid M$, let $\mathfrak{J} = \{j : p_j \mid N\}$, and fix some specific prime $p = p_{j_0} \mid N$. We also let $\mathfrak{J}' := \mathfrak{J} \setminus \{j_0\}$. A **flat cuboid** is then a multiset $\Delta^p \in \mathcal{M}(\mathbb{Z}_N)$ of the form

$$\Delta^p(X) = X^c \prod_{j \in \mathfrak{J}'} \left(1 - X^{d_j N/p_j}\right) \mod X^N - 1,$$

where $c, d_j \in \mathbb{Z}_N$ and $(d_j, p_j) = 1$ for every $j \in \mathfrak{J}'$. If N-cuboids correspond to $|\mathfrak{J}|$-dimensional rectangular boxes, then flat cuboids correspond to rectangular boxes of dimension $|\mathfrak{J}|$ - 1 contained in planes perpendicular to the p direction.

Flat cuboids are useful in so far as the associated Δ^p-evaluations of A in $\mathbb{Z}_N$ indicate simultaneous divisibility by multiple cyclotomic polynomials. Lemma 5.2 is taken from [9], but a similar result (in a somewhat different language) also appears in [8, Lemma 2.13].

Lemma 5.2. *[9, Example 5.9(2)] Let $A \in \mathcal{M}^+(\mathbb{Z}_N)$. Let $p^\alpha \mid\mid N$, and assume that $\mathbb{A}^N[\Delta^p] = 0$ for every flat cuboid Δ^p as defined above. Then*

$$\Phi_N \Phi_{N/p} \cdots \Phi_{N/p^\alpha} \mid A.$$

Observe that any N-cuboid Δ as in (2.7) can be written as $\Delta(X) = \Delta^p_- - \Delta^p_+$ where

$$\Delta^p_-(X) = X^c \prod_{j \in \mathfrak{J}'} \left(1 - X^{d_j N/p_j}\right) \mod X^N - 1,$$

$$\Delta^p_+(X) = X^{c+dN/p} \prod_{j \in \mathfrak{J}'} \left(1 - X^{d_j N/p_j}\right) \mod X^N - 1.$$

Together with Proposition 2.2(ii), this gives the following result for flat cuboids.

Lemma 5.3. *Let $y \in \mathbb{Z}_N$. For $\nu = 0, \ldots, p-1$, let $y_\nu := y + \nu N/p$ and*

$$\Delta^p_\nu(X) := X^{y_\nu} \prod_{j \in \mathfrak{J}'} \left(1 - X^{d_j N/p_j}\right) \mod X^N - 1.$$

If $\Phi_N \mid A$, then

$$\mathbb{A}^N[\Delta^p_\nu] = \mathbb{A}^N[\Delta^p_{\nu'}] \tag{5.3}$$

for every $0 \le \nu, \nu' \le p-1$.

Proof. For each $\nu = 0, \ldots, p-2$, the multiset $\Delta \in \mathcal{M}(\mathbb{Z}_N)$ with the mask polynomial $\Delta(X) = \Delta^p_\nu(X) - \Delta^p_{\nu+1}(X)$ is an N-cuboid. By Proposition 2.2(ii), we have

$$\mathbb{A}^N[\Delta_\nu^p] - \mathbb{A}^N[\Delta_{\nu+1}^p] = \mathbb{A}^N[\Delta] = 0,$$

for all $\nu = 0, \dots, p-2$. This proves the lemma. □

Proof of Proposition 5.1. Let $p \in \mathcal{P}(N)$ with $p^\alpha \parallel N$. Assume that $\Phi_N \mid A$, but

$$\Phi_N \cdots \Phi_{N/p^\alpha} \nmid A. \tag{5.4}$$

By the contrapositive of Lemma 5.2, there is a flat cuboid

$$\Delta_0^p(X) = X^y \prod_{j \in \mathfrak{J}'} (1 - X^{d_j N/p_j}) \mod X^N - 1,$$

where $\mathfrak{J} := \{j : p_j \mid N\}$ and $(d_j, p_j) = 1$, such that $\mathbb{A}^N[\Delta_0^p] \neq 0$. In particular, this implies that $\operatorname{supp} A \cap \operatorname{supp} \Delta_0^p \neq \emptyset$, so that without loss of generality we may assume that $y = a \in A$.

Let $y_\nu := a + \nu N/p$ and

$$\Delta_\nu^p(X) := X^{y_\nu} \prod_{j \in \mathfrak{J}'} \left(1 - X^{d_j N/p_j}\right) \mod X^N - 1.$$

By Lemma 5.3, we have $\mathbb{A}^N[\Delta_\nu^p] = c$ for each ν and some constant $c \neq 0$. In particular, $\operatorname{supp} \Delta_\nu^p \cap \operatorname{supp} A \neq \emptyset$ for each ν. Since $\operatorname{supp} \Delta_\nu^p \subset \Lambda(y_\nu, pD(N))$ for each $\nu = 0, \dots, p-1$, this completes the proof. □

Corollary 5.4. *Assume that $\Phi_N \mid A$. Then there exist a prime $p \mid N$ and elements $a_0, a_1, \dots, a_{p-1} \in A$ such that*

$$a_\nu \in \Lambda(y_\nu, pD(N)) \text{ for } \nu = 0, 1, \dots, p-1, \tag{5.5}$$

where $y_\nu := a_0 + \nu N/p$.

Proof. We induct on K. For $K = 1$ and $p_1 = p$, if $\Phi_{p^\alpha} \mid A$ for some $1 \leq \alpha \leq n_1$, then A is p-fibered on that scale, which clearly implies the conclusion.

Assume now that $K \geq 2$ and that the corollary is true with K replaced by $K-1$. Let N and A be as in the statement of Corollary 5.4. For $a \in A$, consider the flat cuboids

$$\Delta_{a;d_1,\dots,d_{K-1}}(X) := X^a \prod_{1 \leq j \leq K-1} \left(1 - X^{d_j N/p_j}\right) \mod X^N - 1,$$

with $(d_j, p_j) = 1$ and $y_\nu := a + \nu N/p$. We consider two cases.

- Suppose first that $\mathbb{A}^N[\Delta_{a;d_1,\dots,d_{K-1}}] \neq 0$ for some $a \in A$ and $d_1, \dots, d_{K-1}$ as above. Let $y_\nu := a + \nu N/p$ for $\nu \in \{0, \dots, p_K - 1\}$. By Lemma 5.3, we have $\mathbb{A}^N[\Delta_{y_\nu;d_1,\dots,d_{K-1}}] \neq 0$ for all ν, and the conclusion holds with $a_0 = a$ and $p = p_K$.

- Assume now that $\mathbb{A}^N[\Delta_{a;d_1,\dots,d_{K-1}}] = 0$ for all $a \in A$ and for all $d_1, \dots, d_{K-1}$ as above. Recall that $M_K = M/p_K^{n_K}$, so that $N' := (N, M_K)$ is relatively prime to p_K. Let $A' := A \cap \Lambda(a, D(N'))$ for some $a \in A$. By Lemma 5.2, we have $\Phi_{N'} \mid A'$. Since N' has only $K-1$ distinct prime divisors, we may apply the inductive assumption to A' and conclude that (5.5) holds with $p = p_i$ for some $j \in \{1, \dots, K-1\}$. □

6. Long fibers

In this section, we prove a multiscale generalization of the de Bruijn-Rédei-Schoenberg structure theorem for vanishing sums of roots of unity (Proposition 2.2). Instead of assuming that A has just one cyclotomic divisor, we will assume that $\Phi_L \mid A$ for all L such that $N \mid L \mid M$ for some fixed $N \mid M$. Under that assumption, we prove that we can express A as a linear combination of "long fibers", which we now define.

Definition 6.1. (Long fibers) Let $M = \prod_{i=1}^K p_i^{n_i}$, and let $1 \le \alpha \le n_i$. We say that a set $F \subset \mathbb{Z}_M$ is a *p_i^α-fiber on scale M* if $F \equiv x * F_{i,\alpha} \bmod M$ for some $x \in \mathbb{Z}_M$, where

$$F_{i,\alpha}(X) := \prod_{\nu=1}^{\alpha} \Phi_{p_i}\big(X^{M/p_i^\nu}\big) \equiv \frac{X^M - 1}{X^{M/p_i^\alpha} - 1}.$$

We will often refer to p_i^α fibers with $\alpha > 1$ as *long fibers* in the p_i direction.

Explicitly, we have

$$F_{i,\alpha}(X) = 1 + X^{M/p_i^\alpha} + X^{2M/p_i^\alpha} + \cdots + X^{(p_i^\alpha - 1)M/p_i^\alpha}. \tag{6.1}$$

In particular, when $\alpha = 1$, the sets $x * F_{i,1}$ are the usual fibers in the p_i direction on scale M. The following simple result concerning the cyclotomic divisors of long fibers follows immediately from the definition.

Lemma 6.2. *Let M and α be as in Definition 6.1. Then $\Phi_L(X) \mid F_{i,\alpha}(X)$ if and only if $p_i^{n_i - \alpha + 1} \mid L \mid M$.*

Proposition 6.3. ***(Long fiber decomposition)*** *Let $M = \prod_{i=1}^K p_i^{n_i}$, and let $N \mid M$ satisfy $N = \prod_{i=1}^K p_i^{n_i - \alpha_i + 1}$ with $1 \le \alpha_i \le n_i$. Let $A \in \mathcal{M}(\mathbb{Z}_M)$, and assume that $\Phi_L(X) \mid A(X)$ for each $N \mid L \mid M$. Then, there exist polynomials $P_i(X) \in \mathbb{Z}[X]$ such that*

$$A(X) = P_1(X)F_{1,\alpha_1}(X) + \cdots + P_K(X)F_{K,\alpha_K}(X) \mod X^M - 1. \tag{6.2}$$

Moreover, if $A \in \mathcal{M}^+(\mathbb{Z}_M)$ and $K = 2$, then we may assume that the polynomials $P_1(X)$ and $P_2(X)$ each have non-negative coefficients.

Proof. Let $G(X) := \prod_{L:N|L|M} \Phi_L(X)$. Because each of the polynomials $\Phi_L(X)$ is irreducible in $\mathbb{Q}[X]$, we know that $G(X) \mid A(X)$. Hence, it suffices to show that G satisfies (6.2) for some polynomials $P_1, \dots, P_K$ with integer coefficients.
We first use Lemma 6.2 to observe that $G(X) = \gcd(F_{1,\alpha_1}, \dots, F_{K,\alpha_K})$ in the polynomial ring $\mathbb{Q}[X]$. This follows since

$$\begin{aligned}\Phi_L(X) \mid G(X) &\Leftrightarrow N \mid L \mid M \\ &\Leftrightarrow L \mid M \text{ while } L \nmid \frac{M}{p_i^{\alpha_i}} \text{ for all } i = 1, \dots, K.\end{aligned}$$

So, there necessarily exist polynomials $P_1, \dots, P_K \in \mathbb{Q}[X]$ such that

$$G(X) = P_1(X)F_{1,\alpha_1}(X) + \cdots + P_K(X)F_{K,\alpha_K}(X) \mod X^M - 1. \tag{6.3}$$

Moreover, the polynomials $F_{1,\alpha_1}, \dots, F_{K,\alpha_K}$ all have integer coefficients and are primitive (since they are the product of cyclotomic polynomials, which are monic polynomials). Hence, an application of Gauss's Lemma (see [27, Chapter 3]) implies that each of the polynomials $P_1, \dots, P_K$ in (6.3) can be taken to have integer coefficients. Again, using that $G(X)$ is a divisor of $A(X)$, we obtain that A is, itself, expressible as a linear combination of long fibers with integer coefficients.

It remains to show when $K = 2$ (so that $M = p_1^{n_1}p_2^{n_2}$ and $N = p_1^{n_1-\alpha_1+1}p_2^{n_2-\alpha_2+1}$) that we can take P_1 and P_2 in (6.2) to have non-negative integer coefficients. For this, we adapt the proof of Proposition 3.8(b) of [7] to the setting of long fibers.

We can assume that $A = A \cap \Lambda$ where $\Lambda = \Lambda(x, D(N))$ for some $x \in \mathbb{Z}_M$. This follows because, for each $N \mid L \mid M$, Lemma 2.4 guarantees that $\Phi_L(X) \mid (A \cap \Lambda)(X)$. To further simplify, let us assume that $x = 0$. We now make the observation that (as multisets) $\Lambda = F_{1,\alpha_1} * F_{2,\alpha_2}$. This follows because

$$(F_{1,\alpha_1} * F_{2,\alpha_2})(X) = F_{1,\alpha_1}(X)F_{2,\alpha_2}(X) = \left(\prod_{\nu=1}^{\alpha_1} \Phi_{p_1}\left(X^{M/p_1^\nu}\right)\right)\left(\prod_{\nu=1}^{\alpha_2} \Phi_{p_2}\left(X^{M/p_2^\nu}\right)\right)$$

so that $\gcd(M/p_1^{\alpha_1}, M/p_2^{\alpha_2}) \mid y$ for every $y \in F_{1,\alpha_1} * F_{2,\alpha_2}$. But

$$\gcd\left(\frac{M}{p_1^{\alpha_1}}, \frac{M}{p_2^{\alpha_2}}\right) = p_1^{n_1-\alpha_1}p_2^{n_2-\alpha_2} = \frac{N}{p_1p_2} = D(N),$$

and so $F_{1,\alpha_1} * F_{2,\alpha_2} \subset \Lambda$. The reverse containment follows similar reasoning, and is a consequence of the Chinese Remainder Theorem. We leave the details to the reader.

Having now shown that $\Lambda(0, D(N)) = F_{1,\alpha_1} * F_{2,\alpha_2}$ while also showing that we can assume that $A \cap \Lambda(0, D(N)) = A$. Together, this implies that there exist integers w_s, v_t such that

$$A(X) = \sum_{s \in F_{2,\alpha_2}} w_s X^s F_{1,\alpha_1}(X) + \sum_{t \in F_{1,\alpha_1}} v_t X^t F_{2,\alpha_2}(X) \mod X^M - 1, \tag{6.4}$$

and that $w_s + v_t \geq 0$ whenever

$$(\{s\} * F_{1,\alpha_1}) \cap (\{t\} * F_{2,\alpha_2}) \neq \emptyset. \tag{6.5}$$

We claim that there exists a modification w'_s, v'_t of each of these coefficients w_s, v_t such that $w'_s + v'_t = w_s + v_t$ for all pairs of s, t as in (6.5) and so that also $w'_s, v'_t \geq 0$ for every s, t.

To this end, let $e := \min_{x\in\Lambda} w_A^M(x)$ be the minimal weight of the multiset A in $\mathbb{Z}_M$ and choose $s_0 \in F_{2,\alpha_2}$ and $t_0 \in F_{1,\alpha_1}$ so as to satisfy $e = w_{s_0} + v_{t_0}$. We then let $w'_s := w_s + v_{t_0}$ and $v'_t = (w_{s_0} + v_t) - e$ for each $s \in F_{2,\alpha_2}$ and $t \in F_{1,\alpha_1}$. Clearly, then, $v'_t \geq 0$ for every $t \in F_{1,\alpha_1}$, since e was chosen to be the minimal value of the weights of A. Moreover, $w'_s \geq 0$, since

$$w'_s = w_s + v_{t_0} \geq w_{s_0} + v_{t_0} = e$$

and $e \geq 0$, since we are assuming that A is a non-negative multiset. Finally, we notice that

$$w'_s + v'_t = \big((w_{s_0} + v_t) - e\big) + w_s + v_{t_0} = w_s + v_t.$$

Hence, letting

$$P_1(X) := \sum_{s\in F_{2,\alpha_2}} w'_s X^s,\ P_2(X) := \sum_{t\in F_{1,\alpha_1}} v'_t X^t,$$

we see from (6.4) that

$$A(X) = P_1(X)F_{1,\alpha_1}(X) + P_2(X)F_{2,\alpha_2}(X) \mod X^M - 1,$$

and that $P_1, P_2 \in \mathbb{Z}[X]$ both have non-negative coefficients. □

7. Fibered lower bound: positive results

7.1. Two prime divisors

In this section we work in $\mathbb{Z}_M$, where $M = p_1^{n_1} p_2^{n_2}$ has two distinct prime divisors. To simplify the notation, we will abbreviate $p := p_1$ and $q := p_2$. We will continue to use the numerical indices where appropriate, so that for example F_1^N will still denote a fiber in the p direction on scale N, F_2^N will denote a fiber in the q direction, and $\mathsf{EXP}_1(S)$ will continue to denote the set of exponents of $p = p_1$ in S. We recall here that the exponent sets $\mathsf{EXP}_i(S)$ were defined in (4.2).

We first mention a special case resolved in [13].

Theorem 7.1. *[13, Theorem 1] Let $M = p^{n_1}q^{n_2}$ and $A \in \mathcal{M}^+(\mathbb{Z}_M)$. Let $S \subset \mathcal{D}(M)$ be nonempty, and assume that $\Phi_s \mid A$ for all $s \in S$. Assume further that $q \nmid |A|$. Then*

$$|A| \geq p^{E_1} = \mathit{FIB}(S, 1) \geq \mathit{FIB}(S).$$

In general, the assumption that $q \nmid |A|$ cannot be dropped. However, we are able to do that in the following special case.

Proposition 7.2. *Let $M = p^{n_1}q^{n_2}$ and $A \in \mathcal{M}^+(\mathbb{Z}_M)$. Let $S \subset \mathcal{D}(M)$ be nonempty, and assume that $\Phi_s \mid A$ for all $s \in S$. Assume further that the following holds for all $\alpha, \alpha' \in \mathit{EXP}_1(S)$ and $\beta, \beta' \in \mathit{EXP}_2(S)$ with $\alpha' < \alpha$ and $\beta' < \beta$:*

$$\text{if } p^\alpha q^\beta \in S \text{ and } p^{\alpha'} q^{\beta'} \notin S, \text{ then } \{p^{\alpha'} q^\beta, p^\alpha q^{\beta'}\} \cap S \neq \emptyset. \tag{7.1}$$

Then $|A| \geq \mathit{FIB}(S)$.

Proof. We proceed by induction on $|S|$. The case $|S| = 1$ follows from Lemma 2.3. Assume now that $|S| \geq 2$, and that the lemma is true with S replaced by any S' such that $|S'| < |S|$. Let $\alpha_0 = \min(\mathsf{EXP}_1(S))$ and $\beta_0 = \min(\mathsf{EXP}_2(S))$. Let $A \in \mathcal{M}^+(\mathbb{Z}_M)$ satisfy $\Phi_s \mid A$ for all $s \in S$.

Case 1. Assume first that there exists some $s \in S$ such that $p^{\alpha_0} \parallel s$ and A mod s contains a fiber $a * F_1^s$. For each $\nu \in \{0, 1, \ldots, p-1\}$, let $a_\nu \in A$ satisfy $a_\nu \equiv a + \nu s/p \bmod s$, and let

$$A_\nu := A \cap \Lambda(a_\nu, p^{\alpha_0}).$$

Let $\pi_{s'}$ denote the natural projection from $\mathbb{Z}_M$ to $\mathbb{Z}_{s'}$. Then each $A_\nu(X)$ is divisible by $\Phi_{s'}$ for all $s' \in S' := \{s' \in S : \ p^{\alpha_0+1} \mid s'\}$ since $\pi_{s'}(A_\nu(X))$ is the union of $D(s')$-grids for $s' \in S'$ so the claim follows from Lemma 2.4. By the inductive assumption, there are assignment functions $\sigma_\nu : S' \to \{1, 2\}$ such that $|A_\nu| \geq \mathsf{FIB}(S', \sigma_\nu)$. We now define σ as follows: choose $\mu \in \{1, \ldots, p_i\}$ such that $\mathsf{FIB}(S', \sigma_\mu)$ is smallest. For $s' \in S'$, we let $\sigma(s') := \sigma_\mu(s')$ with that μ. We complete the choice of σ by letting $\sigma(s') := 1$ for all s' with $p^{\alpha_0} \parallel s'$. Then

$$|A| \geq \sum_\nu |A_\nu| \geq p \cdot \mathsf{FIB}(S', \sigma_\mu) = \mathsf{FIB}(S, \sigma).$$

Clearly, the same argument works if the assumptions of Case 1 are satisfied with p and q interchanged (so that for some $s \in S$ we have $q^{\beta_0} \parallel s$ and A mod s contains a fiber $a * F_2^s$). Furthermore, if $s_0 := p^{\alpha_0}q^{\beta_0} \in S$, then the assumptions of Case 1 hold with $s = s_0$ for some permutation of p and q, since A mod s_0 has to contain a fiber in at least one direction.

Case 2. We now consider the complementary case when $s_0 \notin S$ and:

(i) if $s \in S$ and $p^{\alpha_0} \parallel s$, then A mod s is fibered in the q direction,
(ii) if $s \in S$ and $q^{\beta_0} \parallel s$, then A mod s is fibered in the p direction,

It follows from (i) and (ii) that $|A|$ is divisible by $p^m q^n$, where $m = \#\{s \in S : \ q^{\beta_0} \parallel s\}$ and $n = \#\{s \in S : \ p^{\alpha_0} \parallel s\}$.

We define an assignment function as follows. Let $s = p^\alpha q^\beta \in S$. By (7.1) with $\alpha' = \alpha_0$ and $\beta' = \beta_0$, at least one of $p^{\alpha_0} q^\beta, p^\alpha q^{\beta_0}$ is in S. We let $\sigma(s) = 1$ if $p^\alpha q^{\beta_0} \in S$, and $\sigma(s) = 2$ if $p^\alpha q^{\beta_0} \notin S$ but $p^{\alpha_0} q^\beta \in S$. Then

$$\mathsf{FIB}(S; \sigma) = p^m q^n \mid |A|,$$

and the proposition is proved. □

Corollary 7.3. *Let $M = p^{n_1} q^{n_2}$ and $A \in \mathcal{M}^+(\mathbb{Z}_M)$. Let $S \subset \mathcal{D}(M)$ be nonempty, and assume that $\Phi_s \mid A$ for all $s \in S$. Assume further that $|\mathsf{EXP}_i(S)| \le 2$ for some $i \in \{1, 2\}$. Then $|A| \ge \mathsf{FIB}(S)$.*

Proof. Without loss of generality, we may assume that $i = 2$. If $|\mathsf{EXP}_2(S)| = 1$, then (7.1) holds vacuously. (In the language of the proof of Proposition 7.2, we are in Case 1 throughout the inductive argument.)

Assume now that $|\mathsf{EXP}_2(S)| = 2$. We need to prove that (7.1) holds in this case. Let $\alpha, \alpha' \in \mathsf{EXP}_1(S)$ and $\beta, \beta' \in \mathsf{EXP}_2(S)$ with $\alpha' < \alpha$ and $\beta' < \beta$. Note that we must have $\mathsf{EXP}_2(S) = \{\beta', \beta\}$. Therefore, if $p^{\alpha'} q^{\beta'} \notin S$, we must have $p^{\alpha'} q^\beta \in S$, and (7.1) holds again. □

Proposition 7.4. *Let $A \in \mathcal{M}^+(\mathbb{Z}_M)$ with $M = p^{n_1} q^{n_2}$. Assume that $\Phi_{p^{m_1}} \cdots \Phi_{p^{m_r}} \Phi_{p^\alpha q^\beta} \Phi_{q^\gamma} \mid A$ for some $1 \le \alpha < m_1 < \cdots < m_r \le n_1$ and $1 \le \beta, \gamma \le n_2$. Assume further that $\beta \ne \gamma$. Then $|A| \ge p^r q \min(p, q)$. In particular, $|A| \ge \mathsf{FIB}(S)$.*

We clearly have $|A| \ge p^r q$ based on $\Phi_{p^{m_1}} \cdots \Phi_{p^{m_r}} \Phi_{q^\gamma} | A$, and independently, $|A| \ge \min(p, q)$ based on $\Phi_{p^\alpha q^\beta} | A$ by either (1.2) or Lemma 2.3. The point of the lemma is that these bounds boost each other.

Proof of Proposition 7.4. By Proposition 4.1, there exists a multiset $\tilde{A} \in \mathcal{M}^+(\mathbb{Z}_{p^{r+1} q^2})$ such that $|\tilde{A}| = |A|$ and

$$\Phi_{p^2} \cdots \Phi_{p^{r+1}} \Phi_{pq^{\beta'}} \Phi_{q^{\gamma'}} \mid \tilde{A}$$

for some β', γ' such that $\{\beta', \gamma'\} = \{1, 2\}$. It suffices to prove that $|\tilde{A}| \ge p^r q \min(p, q)$. To simplify the notation, we may assume in the rest of the proof that $\tilde{A} = A$, $\alpha = 1$, $m_j = j + 1$ for $j = 1, \ldots, r$, and $\{\beta, \gamma\} = \{1, 2\}$.

We first note that

$$p^r q = \Phi_{p^2}(1) \cdots \Phi_{p^{r+1}}(1) \Phi_{q^\gamma}(1) \mid A(1) = |A|. \tag{7.2}$$

Let $s = pq^\beta$. Since $\Phi_s \mid A$, by Lemma 2.3 A mod s is a linear combination, with nonnegative coefficients, of p-fibers and q-fibers on scale s. If A is q-fibered on scale s, then we actually have $\Phi_q\Phi_{q^2} \mid A$ and $q^2 \mid |A|$, so that we are done in this case.

It remains to consider the case when A mod s has at least one p-fiber on that scale. Thus $A(X) = A'(X) + A''(X)$, where $A', A'' \in \mathcal{M}^+(\mathbb{Z}_M)$ are multisets such that A' mod s is fibered in the p direction, A'' mod s is fibered in the q direction, and $A' \neq \emptyset$.

By definition, we have $p \mid |A'|$ and $q \mid |A''|$. It follows from (7.2) that

$$q \mid |A'| \text{ and } p \mid |A''|, \tag{7.3}$$

so that A' mod s is a union of kq many fibers in the p direction for some $k \neq 0$.

For $j = 0, 1, \dots, p-1$, let

$$R_j := \{x \in \mathbb{Z}_M : x \equiv j \bmod p\},\ A_j := A \cap R_j.$$

Then

$$A_j = (A' \cap R_j) \cup (A'' \cap R_j)$$

and $A'' \cap R_j$ is q-fibered on scale s. Hence $|A_j| = kq + \ell_j q$, where ℓ_j is the number of q-fibers in A_j that are also q-fibers of A'' on scale s.

Since $\Phi_{p^2} \dots \Phi_{p^{r+1}} \mid A$, by Lemma 2.4 we must have $\Phi_{p^2} \dots \Phi_{p^{r+1}} \mid A_j$ for each j. In particular, $p^r \mid |A_j|$. Together with the above, this yields $p^r q \mid |A_j|$ for each j. Since $k > 0$, we also have $|A_j| > 0$ for each j. Therefore

$$|A| = \sum_{j=0}^{p-1} |A_j| \geq p^{r+1} q$$

as claimed.

To complete the proof of the proposition, we need to prove that $p^r q \min(p, q) \geq \mathsf{FIB}(S)$. Indeed, let an assignment function σ satisfy $\sigma(p^{m_j}) = 1$ for $j = 1, \dots, r$ and $\sigma(q^\gamma) = 2$, and define $\sigma(p^\alpha q^\beta)$ so that $p_{\sigma(s_3)} = \min(p, q)$. Then $p^r q \min(p, q) = \mathsf{FIB}(S, \sigma)$. □

An analogous result can be proved if the exponents of the p-power cyclotomic divisors are smaller than α.

Proposition 7.5. *Let $A \in \mathcal{M}^+(\mathbb{Z}_M)$ with $M = p^{n_1} q^{n_2}$. Assume that $\Phi_{p^{m_1}} \cdots \Phi_{p^{m_r}} \Phi_{p^\alpha q^\beta} \Phi_{q^\gamma} \mid A$ for some $1 \leq m_1 < \cdots < m_r < \alpha \leq n_1$ and $1 \leq \gamma < \beta \leq n_2$. Then $|A| \geq p^r q \min(p, q)$. In particular, $|A| \geq \mathsf{FIB}(S)$.*

Proof. By Proposition 4.1, there exists a multiset $\tilde{A} \in \mathcal{M}^+(\mathbb{Z}_{p^{r+1}q^2})$ such that $|\tilde{A}| = |A|$ and

$$\Phi_p \cdots \Phi_{p^r} \Phi_{p^{r+1}q^2} \Phi_q \mid \tilde{A}.$$

It suffices to prove that $|\tilde{A}| \geq p^r q \min(p,q)$. To simplify the notation, we may assume in the rest of the proof that $\tilde{A} = A$, $\alpha = r+1, \beta = 2, \gamma = 1$, $m_j = j$ for $j = 1, \dots, r$, and $n_1 = r+1, n_2 = 2$.

Let $\Lambda_\nu = \Lambda(\nu, p^r)$ for $\nu = 0, 1, \dots, p^r - 1$. Since $\Phi_p \cdots \Phi_{p^r} \mid A$, we have

$$|A \cap \Lambda_\nu| = \frac{|A|}{p^r} \text{ for all } \nu.$$

Since $\Phi_q \mid A$, we have $q \mid |A|$ and so $q \mid \frac{|A|}{p^r} = |A \cap \Lambda_\nu|$. Finally, we have $\Phi_{p^{r+1}q^2} \mid A$. By Lemma 2.3, this implies that A (hence also $A \cap \Lambda_\nu$ for each ν) is the sum of p-fibers and q-fibers on that scale. Hence for each ν we have $|A \cap \Lambda_\nu| = kp + lq$ for some $k, l \geq 0$ (possibly depending on ν).

If $k = 0$ for all ν, then A is the union of q-fibers only, meaning that $\Phi_{q^2} \mid A$ and hence $\Phi_p \cdots \Phi_{p^r} \Phi_q \Phi_{q^2} \mid A$. This implies that $p^r q^2 \mid |A|$, and we are done.

Suppose now that $k > 1$ for some ν. Then $q \mid k$, since $q \mid |A \cap \Lambda_\nu| = kp + lq$. Hence $|A \cap \Lambda_\nu| \geq pq$, and thus

$$|A| = p^r \cdot |A \cap \Lambda_\nu| \geq p^{r+1} q,$$

and we are done again.

The last statement in the proposition follows as in the proof of Proposition 7.4. □

Theorem 7.6. *Let $M = p^{n_1} q^{n_2}$, and let $S \in \mathcal{D}(M)$ satisfy $|S| = 3$. Then $\mathsf{MIN}(S) = \mathsf{FIB}(S)$.*

Proof. If $|\mathsf{EXP}_i(S)| \leq 2$ for some $i \in \{1, 2\}$, then the result follows from Corollary 7.3. We may therefore assume for the rest of the proof that

$$S = \{s_1, s_2, s_3\}, \text{ where } s_i = p^{\alpha_i} q^{\beta_i}, \ i = 1, 2, 3,$$

where $0 \leq \alpha_1 < \alpha_2 < \alpha_3 \leq n_1$, and where the exponents $\beta_1, \beta_2, \beta_3 \in \{0, 1, \dots, n_2\}$ are all distinct.

Let $A \in \mathcal{M}^+(\mathbb{Z}_M)$ satisfy $\Phi_s \mid A$ for all $s \in S$. Suppose that $\alpha_1 \geq 1$, and that A mod s_1 contains a fiber in the p direction. By the same argument as in the proof of Proposition 7.2, Case 1, we reduce the proof of the theorem in this case to proving that $\mathsf{MIN}(\{s_2, s_3\}) = \mathsf{FIB}(\{s_2, s_3\})$; however, for a 2-element set $\{s_2, s_3\}$, this equality again follows from Corollary 7.3.

If on the other hand $\alpha_1 \geq 1$ and A mod s_1 is fibered in the q direction, then $A(X)$ is also divisible by $\Phi_{q^{\beta_1}}$. We replace the set S with the set $S' := \{s_1', s_2, s_3\}$, where $s_1' = q^{\beta_1}$, note that $\Phi_s \mid A$ for all $s \in S'$, and continue with the rest of the proof.

Similarly, let $\mu \in \{1,2,3\}$ be the index such that $\beta_\mu = \min(\beta_1, \beta_2, \beta_3)$. If A mod s_μ contains a fiber in the q direction, we proceed as in the proof of Proposition 7.2, Case 1, to reduce S to a 2-element set covered in Corollary 7.3. If on the other hand A mod s_μ is fibered in the p direction, then $A(X)$ is also divisible by $\Phi_{p^{\alpha_\mu}}$, so that we may also replace s_μ by p^{α_μ}.

By the above reductions, we may assume for the rest of the proof that

$$0 = \alpha_1 < \alpha_2 < \alpha_3 \le n_1, \quad \min(\beta_1, \beta_2, \beta_3) = \beta_\mu = 0.$$

Since $1 \notin S$, we have $\mu \in \{2,3\}$.

Assume first that $\beta_3 = 0$. Then

$$\Phi_{q^{\beta_1}} \Phi_{p^{\alpha_2} q^{\beta_2}} \Phi_{p^{\alpha_3}} \mid A,$$

with $0 < \alpha_2 < \alpha_3$. This places us in the situation described in Proposition 7.4 with $r = 1$. Let $\sigma(s_1) = 2$, $\sigma(s_3) = 1$, and define $\sigma(s_2)$ so that $p_{\sigma(s_2)} = \min(p, q)$. By Proposition 7.4, we have

$$|A| \ge pq \min(p,q) = \mathsf{FIB}(S, \sigma) \ge \mathsf{FIB}(S),$$

and we are done in this case.

It remains to consider the case when $\beta_2 = 0$. Thus

$$\Phi_{q^{\beta_1}} \Phi_{p^{\alpha_2}} \ \Phi_{p^{\alpha_3} q^{\beta_3}} \mid A.$$

If $0 < \beta_3 < \beta_1$, we are again in the situation described in Proposition 7.4, but with p and q interchanged. The theorem follows as above.

We are left with the case when

$$0 = \alpha_1 < \alpha_2 < \alpha_3, \quad 0 = \beta_2 < \beta_1 < \beta_3.$$

This is a special case of Proposition 7.5 with $r = 1$, and we are done again. □

7.2. The diagonal case

We return to the setting where M has arbitrarily many prime divisors, and consider the following simple case.

Lemma 7.7. *Let $M = \prod_{k=1}^{K} p_k^{n_k}$. Assume that $S = \{s_1, \dots, s_m\} \subset \mathcal{D}(M)$ satisfies*

$$s_j \mid D(s_{j+1}) \text{ for } j = 1, \dots, m-1. \tag{7.4}$$

Then $\mathsf{MIN}(S) \ge \prod_{j=1}^{m} \min_{i: p_i \mid s_j} p_i = \mathsf{FIB}(S)$.

Proof. We proceed by induction in m. If $m = 1$ and $S = \{s\}$, then the conclusion follows from (1.2). Assume now that $m > 1$, and that the conclusion is true when $|S| = m - 1$. Let $A \in \mathcal{M}^+(\mathbb{Z}_M)$ satisfy $\Phi_{s_j} \mid A$ for $j = 1, \dots, m$. Since $\Phi_{s_1} \mid A$, we have that A mod s_1 satisfies the conclusion (5.5) of Corollary 5.4 for some $a \in A$ and $p \mid s_1$. Fix that p. For $\nu = 0, 1, \dots, p-1$, let $y_\nu := a + \nu s_1/p$ and

$$A_\nu := A \cap \Lambda(y_\nu, pD(s_1)).$$

Then the sets A_ν are nonempty and pairwise disjoint. By (7.4), we have $pD(s_1) \mid D(s_j)$ for $j = 2, \dots, m$. It follows from Lemma 2.4 that $\Phi_{s_j} \mid A_\nu$ for all $j = 2, \dots, m$ and $\nu = 1, \dots, p$. Applying the inductive assumption to A_ν, we get

$$|A| \geq \sum_{j=1}^{p} |A_\nu| \geq p \prod_{j=2}^{m} \min_{i : p_i \mid s_j} p_i \geq \prod_{j=1}^{m} \min_{i : p_i \mid s_j} p_i.$$

By Proposition 3.2 we have that

$$\mathsf{FIB}(S) = \min_{\sigma} \mathsf{FIB}(S, \sigma), \tag{7.5}$$

with the minimum taken over all assignment functions σ. This minimum is clearly taken for the assignment function σ defined via $\sigma(s) = p_s$ for every $s \in S$, where p_s is the smallest prime divisor of s. This implies that

$$\prod_{j=1}^{m} \min_{i : p_i \mid s_j} p_i = \mathsf{FIB}(S). \quad \square$$

7.3. Many primes with a growth condition

Theorem 7.8. *Let $A \in \mathcal{M}^+(\mathbb{Z}_M)$ with $M = \prod_{k=1}^{K} p_k^{n_k}$ satisfying*

$$p_K > \cdots > p_2 > p_1^{n_1}. \tag{7.6}$$

Let $S \subset \mathcal{D}(M)$ be nonempty, and assume that $\Phi_s \mid A$ for all $s \in S$. Then $|A| \geq p_1^{E_1}$, where

$$E_1 := \#\mathit{EXP}_1(S) := \#\{\alpha \geq 1 : \exists\, s \in S \text{ with } p_1^\alpha \mid\mid s\}.$$

In particular, we have $|A| \geq \mathsf{FIB}(S)$ under the assumptions of the theorem, so that $\mathsf{MIN}(S) \geq \mathsf{FIB}(S)$ if (7.6) holds. Indeed, let $\sigma : S \to \{1, \dots, K\}$ be an assignment function. If $\sigma(s) \geq 2$ for any $s \in S$, we have $\mathsf{FIB}(S, \sigma) \geq p_2 > p_1^{n_1} \geq p_1^{E_1}$. If on the other hand $\sigma(s) = 1$ for all $s \in S$ (note that this can only happen when $p_1 \mid s$ for all $s \in S$), then $\mathsf{FIB}(S, \sigma) = p_1^{E_1}$. The claim follows in both cases.

Proof of Theorem 7.8. We induct on K. When $K = 1$, we have $S = \{p_1^{\alpha_1}, \dots, p_1^{\alpha_{E_1}}\}$ for some $1 \le \alpha_1 < \dots, < \alpha_{E_1} \le n_1$, so that

$$\Phi_{p_1^{\alpha_1}} \cdots \Phi_{p_1^{\alpha_{E_1}}}(X) \mid A(X) \Rightarrow p_1^{E_1} \mid |A|,$$

and so we clearly have $|A| \ge p_1^{E_1}$. Assume now that $K \ge 2$ and that the result holds for any $1 \le K_0 \le K - 1$. Let

$$\mathcal{C} := \{s \in S_A : p_K \mid s\}, \quad M' := M/p_K^{n_K} = p_1^{n_1} \cdots p_{K-1}^{n_{K-1}},$$

and note that the size assumption $p_{K-1} > \cdots > p_1^{E_1}$ is still satisfied for M' (vacuously if $K = 2$). There are two cases to consider, corresponding to the conclusions (1) and (2) of Proposition 5.1.

Case 1: We first assume that the conclusion of Proposition 5.1 (1) fails for some $s \in \mathcal{C}$. Assume that $p_K^{\alpha} \parallel s$. Then the failure of (1) means that there exists $1 \le \beta \le \alpha$ such that $\Phi_{s/p_K^{\beta}} \nmid A$. Applying Proposition 5.1 (2) with $N = s$ and $p = p_K$, we find $a \in A$ such that

$$|A| = A(1) \ge \sum_{\nu=0}^{p_K - 1} A_{\nu,a}(1) \ge p_K$$

where each $A_{\nu,a} \in \mathcal{M}(\mathbb{Z}_N)$ is as in (5.2). Since we assume that $p_K > p_1^{n_1} \ge p_1^{E_1}$, this establishes Theorem 7.8 in this case.

Case 2: We now suppose that for all $s \in \mathcal{C}$, we necessarily have that

$$\Phi_s \cdots \Phi_{s/p_K^{\alpha}} \mid A, \tag{7.7}$$

where $\alpha = \alpha(s) \ge 1$ is the unique exponent such that $p_K^{\alpha} \parallel s$. Let

$$S' := \{(s, M') : \ s \in S\}, \quad A' := (A \bmod M') \in \mathcal{M}^+(\mathbb{Z}_{M'}).$$

By (7.7), we have $\Phi_{s'} \mid A$ for all $s \in S'$. Since $S' \subset \mathcal{D}(M')$, this also implies that $\Phi_{s'} \mid A$ for all $s \in S'$. The key observation is that

$$\#\{\alpha \ge 1 : \exists\, s \in S' \text{ with } p_1^{\alpha} \parallel s\} = \#\{\alpha \ge 1 : \exists\, s \in S \text{ with } p_1^{\alpha} \parallel s\} = E_1.$$

Indeed, if $s \in S \setminus \mathcal{C}$, then $s \in S'$, and if $s \in \mathcal{C}$, then $(s, M') \in S'$ and $\mathsf{EXP}_1(s) = \mathsf{EXP}_1((s, M'))$. Applying the inductive hypothesis to A' and M', we see that

$$|A| = |A'| \ge p_1^{E_1'} = p_1^{E_1}. \quad \square$$

8. Examples where the fibered lower bound fails

8.1. Recombination effects for 3 or more prime factors

In general, if we increase the complexity of S, we may have $\mathsf{MIN}(S) < \mathsf{FIB}(S)$. It is easiest to give examples of this when $M := \mathrm{lcm}(S)$ has 3 or more prime factors. The idea is to use a certain *recombination effect*, as follows. Write $M = PQ$, where $(P, Q) = 1$, so that $\mathbb{Z}_M = \mathbb{Z}_P \oplus \mathbb{Z}_Q$. Let $A' \in \mathcal{M}^+(\mathbb{Z}_P)$ and $A'' \in \mathcal{M}^+(\mathbb{Z}_Q)$ be two multisets with $|A'| = |A''|$. Then we may construct a multiset $A \in \mathcal{M}^+(\mathbb{Z}_M)$ so that its Chinese Remainder Theorem projections onto $\mathbb{Z}_P$ and $\mathbb{Z}_Q$ are, respectively, A' and A''. While each of A' and A'', independently, must have large enough cardinality to accommodate its own cyclotomic divisors, there need not be any additional increases in the size of A due to sharing the cyclotomic divisors of both A' and A''.

One example of this, with M equal to a product of 4 primes, is given in [13, Section 6.3]. An additional constraint imposed in [13] (coming from the intended application to the Favard length problem) was that $|A|$ should be relatively prime to M. If we drop that constraint, then a simpler example is as follows.

Example 8.1. Let $2 = p_1 < p_2 < p_3$ be distinct primes such that $p_1 + p_2 = p_3$. Let $M = p_1p_2p_3$ and $S = \{p_1p_2, p_3\}$. Consider any set $A \in \mathcal{M}^+(\mathbb{Z}_M)$ simultaneously satisfying the equations

$$\begin{aligned} A(X) &\equiv X^{a_1} F_1^{p_1p_2}(X) + X^{a_2} F_2^{p_1p_2}(X) \mod X^{p_1p_2} - 1, \\ A(X) &\equiv X^{a_3} F_3^{p_3}(X) \mod X^{p_3} - 1 \end{aligned} \tag{8.1}$$

for some $a_1, a_2, a_3 \in \mathbb{Z}_M$. Such a set can be easily constructed via the Chinese Remainder Theorem. Since the same idea is also used in the more difficult example in Proposition 8.2, we provide the details as a warm-up. We recall the array coordinate expansion of elements $x \in \mathbb{Z}_M$:

$$x = x_1M_1 + x_2M_2 + x_3M_3,$$

where $x_j \in \{0, 1, \dots, p_j - 1\}$ and (in this case) $M_j = M/p_j$. Then (8.1) is equivalent to saying that $|A| = p_3$ and

$$\begin{aligned} \{(a_1, a_2) :\ a \in A\} &= \{(0,0), (1,0)\} \cup \{(0,0), (0,1), \dots, (0, p_2 - 1)\}, \\ \{a_3 :\ a \in A\} &= \{0, 1, \dots, p_3 - 1\}, \end{aligned}$$

where the first equation should hold in the sense of multisets, with two different triples of the form $(0, 0, a_3)$ in A. In each equation above, the cardinality of A matches that of the set on the right side; furthermore, A is a set (not just a multiset) since all its elements are distinct mod p_3. The key point is that the two conditions above involve

different coordinates of the elements of A, hence they can be imposed independently of each other.

By Proposition 2.2, the first equation in (8.1) implies that $\Phi_{p_1p_2}(X) \mid A(X)$, and the second one implies that $\Phi_{p_3}(X) \mid A(X)$. Hence $\mathsf{MIN}(S) \le |A| = p_3$. By (1.2), we also have $\mathsf{MIN}(S) \ge p_3$ (using that $p_3 \in S$), so that $\mathsf{MIN}(S) = p_3$.

On the other hand, we must have $\sigma(p_1p_2) \in \{1,2\}$ and $\sigma(p_3) = 3$ for any assignment function $\sigma : S \to \{1,2,3\}$. Hence, $\mathsf{FIB}(S) = \min_\sigma \mathsf{FIB}(S,\sigma) \ge \min(p_1,p_2) \cdot p_3 = 2p_3$, showing that $\mathsf{MIN}(S) < \mathsf{FIB}(S)$.

8.2. Recombination for two prime factors

More surprisingly, we may have $\mathsf{MIN}(S) < \mathsf{FIB}(S)$ even if $M = \mathrm{lcm}(S)$ has only two distinct prime factors. In this case, it follows from Corollary 7.3 that, unlike in Example 8.1, we cannot produce such examples using only two cyclotomic divisors and a single scale. However, we can construct them using multiple scales instead.

Proposition 8.2. *Let $M = p^n q^m$ with $n \ge 9$ and $m \ge 6$, and let $p = 2, q = 3$. Then there exists a set $A \subset \mathbb{Z}_M$ such that*

$$\Phi_{p^n}\Phi_{p^{n-1}}\Phi_{p^{n-2}}\Phi_{q^m}\Phi_{q^{m-1}}\Phi_{q^{m-2}}\Phi_{pq} \mid A$$

and $|A| = p^3q^3$.

Proof. We first define a multiset $B \in \mathcal{M}^+(\mathbb{Z}_{pq})$ with $p = 2, q = 3$ via the table below. It is easy to check explicitly that $\mathbb{B}^{pq}[\Delta] = 0$ for all pq-cuboids Δ (there are 3 such cuboids). By Proposition 2.2, it follows that $\Phi_{pq} \mid B$.

	0 mod 3	1 mod 3	2 mod 3	row sum
0 mod 2	74	47	47	21· 8
1 mod 2	34	7	7	6· 8
column sum	4· 27	2· 27	2· 27	

(8.2)

Notice that $27 \mid |B \cap \Lambda(i,q))|$ for every $i \in \{0,1,2\}$. Similarly, $8 \mid |B \cap \Lambda(j,p))|$ for every $j \in \{0,1\}$.

We would like to construct a set $A \subset \mathbb{Z}_M$ such that $A \equiv B \bmod pq$ (so that divisibility by Φ_{pq} is preserved), but A also has the additional cyclotomic divisors listed in the proposition. Let $M = p^n q^m$, with n and m large enough (to be determined later). We will again use the array coordinates mod M: for each $x \in \mathbb{Z}_M$ we write

$$x \equiv x_1M_1 + x_2M_2 \bmod M, \quad x_1 \in \{0,1,\dots,p^n-1\}, \quad x_2 \in \{0,1,\dots,q^m-1\},$$

where $M_1 = q^m = M/p^n$ and $M_2 = p^n = M/q^m$. We will further need the digit expansions

$$x_1 = x_{1,0} + x_{1,1}p + \cdots + x_{1,n-1}p^{n-1}, \quad x_2 = x_{2,0} + x_{2,1}q + \cdots + x_{2,m-1}q^{m-1},$$

where $x_{1,j} \in \{0,1\}$ and $x_{2,i} \in \{0,1,2\}$.

Let $A \subset \mathbb{Z}_M$ with $|A| = p^3q^3$; we will now impose conditions on the digits of the elements of A so that A has the required cyclotomic divisors. We first ask that $A \equiv B \bmod pq$; to this end, it suffices to ensure that the digits $a_{1,0}$ and $a_{2,0}$ of the elements of A have the distribution indicated in the table above.

Next, we need to ensure that A is divisible by

$$\Phi_{p^n}(X)\Phi_{p^{n-1}}(X)\Phi_{p^{n-2}}(X) = \frac{X^{p^n}-1}{X^{p^{n-3}}-1} = F_{p,3}^{p^n}.$$

In other words, $A \bmod p^n$ needs to be a union of long p^3-fibers; furthermore, in order for A to be a set, we will make sure that these p^3-fibers are disjoint. We write $A = A_0 \cup A_1$, where $A_j = \{a \in A : \ a \equiv j \bmod 2\}$. By (6.1), we have $F_{p,3}^{p^n} = p^{n-3}\mathbb{Z}_{p^n}$. Hence, it suffices to have

$$A_j(X) \equiv X^j C_j(X) F_{p,3}^{p^n} \mod (X^{p^n}-1), \ j = 0,1,$$

where $C_j \subset \mathbb{Z}_M$ is a set whose all elements are divisible by p but distinct mod p^{n-3}. This is possible when

$$\#\{c_{1,1}p + c_{1,2}p^2 + \cdots + c_{1,n-4}p^{n-4} : \ c_{1,j} \in \{0,1\}\} \geq 21, \tag{8.3}$$

since we have to place 21 long fibers in A_0 and 6 long fibers in A_1. Since $32 = 2^5 > 21$, it suffices to take $n-4 \geq 5$, so that $n \geq 9$. Note that the entire operation above involved only the $a_{1,i}$ digits of $a \in A$ with $i \geq 1$.

To ensure that $\Phi_{q^m}\Phi_{q^{m-1}}\Phi_{q^{m-2}} \mid A$, we proceed similarly, but with p and q interchanged so that we are now adjusting the $a_{2,i}$ digits of $a \in A$ with $i \geq 1$. This can clearly be done independently of the choices already made above. The condition (8.3) is replaced by $3^{m-4} \geq 8$. Since $9 = 3^2 > 8$, it suffices to take $m-4 \geq 2$, so that $m \geq 6$. □

In the proof of Proposition 8.2, the fact that A is a set is guaranteed in the simplest possible way by forcing both $A \bmod p^n$ and $A \bmod q^m$ to be sets. However, it would be enough to assume that one of them is a set (with an arbitrary bijection between this set and the other multiset). It could be possible to lower the exponents n and m further so that both $A \bmod p^n$ and $A \bmod q^m$ are multisets, but then the construction requires further analysis and details. There is no such construction with $|A|$ equal to $2^2 \cdot 3^3$ or any of its divisors.

We expect that there are other choices of primes (not necessarily $p = 2$, $q = 3$) for which similar examples could be constructed. However, Proposition 8.3 below shows that p and q cannot be chosen completely arbitrarily in this type of examples.

Proposition 8.3. *Let $1 \le a < n$ and $1 \le b < m$. Assume that $p > q^b$ and*

$$\Phi_{p^n} \dots \Phi_{p^{n-a+1}} \Phi_{q^m} \dots \Phi_{q^{m-b+1}} \Phi_{pq} \mid A$$

for some $A \in \mathcal{M}^+(\mathbb{Z}_{p^n q^m})$. Then $|A| > p^a q^b$.

Proof. Based on the prime power cyclotomic divisors, we have $p^a q^b \mid |A|$, hence $|A| \ge p^a q^b$. Furthermore, $|A_i| = |A \cap \Lambda(i,p)|$ is divisible by p^a for every $i = 0, 1, \dots, p-1$.

Assume indirectly that $|A| = p^a q^b$. Since $p > q^b$, we have that $|A_i|$ is zero for some i. On the other hand, since $\Phi_{pq} \mid A$, by Lemma 2.3 we have that A mod pq is a nonnegative linear combination of p-fibers and q-fibers. With $A_i = \emptyset$ for some i, A must in fact be a sum of q-fibers only, so that $\Phi_q \mid A$. It follows that $q^{b+1} \mid A$, contradicting the assumption that $|A| = p^a q^b$. □

In the next example, the exponents of p and q in the extra composite divisor of $A(X)$ are higher than those in the prime power divisors.

Proposition 8.4. *Let $M = p^4 q^4$, $p = 2, q = 3$. There exists a set $A \subset \mathbb{Z}_M$ such that*

$$\Phi_p \Phi_{p^2} \Phi_{p^3} \Phi_q \Phi_{q^2} \Phi_M \mid A$$

and $|A| = p^3 q^2 = 72$.

Proof. The following table represents a multiset $B \in \mathcal{M}^+(\mathbb{Z}_{72})$, where the cyclic group $\mathbb{Z}_{72}$ is written as $\mathbb{Z}_8 \oplus \mathbb{Z}_9$, rows represent cosets of $\mathbb{Z}_9$, and columns represent cosets of $\mathbb{Z}_8$. Similarly to (8.2), the entry in the i-th row and j-th column is equal to $w_B^{72}(b)$, where b is the element of $\mathbb{Z}_{72}$ such that $b \equiv i \bmod 8$ and $b \equiv j \bmod 9$.

5	0	0	0	0	2	0	0	2
3	4	0	0	0	2	0	0	0
0	0	5	2	0	0	0	0	2
0	0	3	2	0	0	0	4	0
0	0	0	0	5	2	0	0	2
0	4	0	0	3	2	0	0	0
0	0	0	0	0	0	5	2	2
0	0	0	4	0	0	3	2	0

It is easy to verify that the entries in each column add up to 8, and the entries in each row add up to 9. In other words, we have $|B \cap \Lambda^{72}(x,9)| = 8$ and $|B \cap \Lambda^{72}(x,8)| = 9$ for all $x \in \mathbb{Z}_{72}$. This guarantees that

$$\Phi_p \Phi_{p^2} \Phi_{p^3} \Phi_q \Phi_{q^2} \mid B. \tag{8.4}$$

Let $M = p^4q^4$. We want to construct a set $A \subset \mathbb{Z}_M$ such that $B \equiv A \bmod p^3q^2$ and, furthermore, $\Phi_M \mid A$. Let $\pi : \mathbb{Z}_M \to \mathbb{Z}_{p^3q^2}$ be the natural projection defined by $\pi(x) = x \bmod p^3q^2$. Then for each $x \in \mathbb{Z}_{p^3q^2}$, its preimage $\pi^{-1}(x) = \Lambda(x, p^3q^2)$ contains at least two grids $\Lambda(y, p^3q^3)$ and $\Lambda(z, p^3q^3)$ disjoint from each other.

Each positive entry (2, 3, 4, 5) in the table is a nonnegative integer coefficient linear combination of 2 and 3. Accordingly, for each $x \in \mathbb{Z}_{p^3q^2}$ such that $w_B^{72}(x) \neq 0$, we may define $A \cap \Lambda(x, p^3q^2)$ to be either just a single 2-fiber, or a single 3-fiber, or two 2-fibers, or a 3-fiber and a 2-fiber, where each fiber is on scale M. Furthermore, in those cases when $A \cap \Lambda(x, p^3q^2)$ consists of two fibers, we may place them in different p^3q^3-grids, guaranteeing that they do not overlap. Hence A is a set, we have $A \equiv B \bmod 72$, and, by Proposition 2.2, $\Phi_{p^4q^4} \mid A$. Since p, p^2, p^3, q, q^2 all divide 72, A inherits the property (8.4) from B. Hence A satisfies all conclusions of the theorem. □

We remark that the same proof would also work for any $M = p^mq^n$ such that

$$\frac{D(M)}{p^3q^2} = \frac{p^{m-1}q^{n-1}}{p^3q^2} = p^{m-4}q^{n-3} \geq 2.$$

For example, we could take $M = p^5q^3$.

In Proposition 8.2 and 8.4, we used $p = 2$ and $q = 3$. We now give a similar construction for any pair of distinct odd primes p and q. If one of the primes is 2, then the construction can be easily modified (and it is somewhat simpler), but we omit the details. We will need two easy number-theoretic lemmas.

Lemma 8.5. *Let p, q be distinct primes. If $pq \leq K \in \mathbb{N}$, then there exist $s_K, r_K \in \mathbb{N}_0$ such that $s_Kp + r_Kq = K$.*

Lemma 8.6. *Let p, q be distinct odd primes. Then for every $\ell \in \mathbb{N}$ there exist $a, b \in \mathbb{N}$ such that $p^a \equiv q^b \equiv 1 \bmod 2^\ell$.*

Theorem 8.7. *Let p, q be distinct odd primes. We define the parameters $k, a, b, n, m \in \mathbb{N}$, in that order, so that the following hold.*

(i) *Choose k so that $2^k \geq pq + 1$.*
(ii) *Choose a, b so that the conclusion of Lemma 8.6 holds with $\ell = 2k$. Thus, we have $p^a = C_1 4^k + 1$ and $q^b = C_2 4^k + 1$ for some $C_1, C_2 \in \mathbb{N}$.*
(iii) *Assume that $p^a > q^b$ (otherwise we interchange p and q).*
(iv) *Define $N = p^aq^b$ and $M = p^nq^m$, with $n > a$ and $m > b$ large enough so that $D(M)/N \geq q^b$.*

Then there is a set A of size $|A| = N = p^aq^b$ that satisfies

$$\Phi_p\Phi_{p^2} \cdots \Phi_{p^a}\Phi_q\Phi_{q^2} \cdots \Phi_{q^b}\Phi_M \mid A. \tag{8.5}$$

Proof. As in the proof of Proposition 8.4, we first construct a multiset $B \in \mathcal{M}^+(\mathbb{Z}_N)$ such that $|B| = N$,

$$\Phi_p \Phi_{p^2} \cdots \Phi_{p^a} \Phi_q \Phi_{q^2} \cdots \Phi_{q^b} \mid B, \tag{8.6}$$

and each entry $w_B^N(x)$ for $x \in \mathbb{Z}_N$ is either zero or large enough so that we can apply Lemma 8.5. We then lift it to a set $A \subset \mathbb{Z}_M$ such that $A \equiv B \bmod N$ and, additionally, $\Phi_M \mid A$.

We write $\mathbb{Z}_N$ as $\mathbb{Z}_{p^a} \oplus \mathbb{Z}_{q^b}$. The set B will be defined via a $q^b \times p^a$ matrix with entries $w_B^N(x_{ij})$, where x_{ij} is the element of $\mathbb{Z}_N$ such that $x_{ij} \equiv i \bmod q^b$ and $x_{ij} \equiv j \bmod p^a$. We start with some building blocks. We define the square matrices G and H so that G is a $2^k \times 2^k$ matrix with all entries equal to 2^k, and H is a $2^{2k} \times 2^{2k}$ matrix with blocks equal to G along the diagonal and zeroes everywhere else. We use 0 to denote zero matrices as needed.

$$G = \underbrace{\begin{bmatrix} 2^k & \cdots & 2^k \\ \vdots & \ddots & \vdots \\ 2^k & \cdots & 2^k \end{bmatrix}}_{2^k}, \qquad H = \underbrace{\begin{bmatrix} G & 0 & \cdots & 0 \\ 0 & G & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & G \end{bmatrix}}_{2^k \text{ blocks}}$$

Note that, in both G and H, each row and each column adds up to $2^k \cdot 2^k = 4^k$.

Let Y be the matrix with $p^a = C_1 4^k + 1$ columns and $q^b = C_2 4^k + 1$ rows, defined as follows. We start with a matrix with $C_1 4^k$ columns and $C_2 4^k$ rows that consists of concatenated blocks equal to H. (The total number of such blocks is $C_1 C_2$.) Then we add one row and one column where the entries are all equal to 1, as shown below. For $n \geq 1$, we use 1_n to denote the row vector $(1, 1, \ldots, 1)$ with n entries, and 1_n^t to denote its transpose.

$$Y = \left[\begin{array}{ccc||c} H & \cdots & H & 1_{4^k}^t \\ \vdots & \ddots & \vdots & \vdots \\ H & \cdots & H & 1_{4^k}^t \\ \hline\hline 1_{4^k} & \cdots & 1_{4^k} & 1 \end{array}\right]$$

This matrix defines a multiset B_0 in $\mathbb{Z}_N$. Note that each row of Y adds up to $C_1 4^k + 1 = p^a$, and each column of Y adds up to $C_2 4^k + 1 = q^b$. It follows that $|B_0| = p^a q^b = N$, and

$$\Phi_p \Phi_{p^2} \cdots \Phi_{p^a} \Phi_q \Phi_{q^2} \cdots \Phi_{q^b} \mid B_0. \tag{8.7}$$

We now define an "adding a cuboid" operation[1] that preserves row and column sums. Given a 2×2 submatrix of Y with entries a_1, a_2, a_3, a_4, we may replace it by a submatrix with entries $a_1+1, a_2-1, a_3-1, a_4+1$ as shown below:

$$\begin{array}{|c|c|}\hline a_1 & a_2 \\ \hline a_3 & a_4 \\ \hline \end{array} \quad \to \quad \begin{array}{|c|c|}\hline a_1+1 & a_2-1 \\ \hline a_3-1 & a_4+1 \\ \hline \end{array} = \begin{array}{|c|c|}\hline a_1 & a_2 \\ \hline a_3 & a_4 \\ \hline \end{array} + \begin{array}{|c|c|}\hline 1 & -1 \\ \hline -1 & 1 \\ \hline \end{array}, \tag{8.8}$$

and the matrix thus obtained has the same row sums and column sums as Y. The same remains true if we iterate a sequence of such operations or its inverses.

Our goal is to use the operation in (8.8) to get a new multiset $B \in \mathcal{M}^+(\mathbb{Z}_N)$ so that $|B| = |B_0|$, (8.7) continues to hold for B, and additionally all nonzero entries in B are large enough so that we could apply Lemma 8.5. Specifically, we need to replace all the 1 entries by either 0 or a number greater than or equal to pq.

Recall that $p^a > q^b$, so that $C_1 > C_2$. Then Y has the block decomposition

$$Y = \begin{array}{|c||c||c|c|c|c||c|}\hline Y_0 & Y_1 & Y_2 & \cdots & Y_{(C_1-C_2)2^k} & 1^t_{C_2 4^k} \\ \hline 1_{C_2 4^k} & 1_{2^k} & 1_{2^k} & \cdots & 1_{2^k} & 1 \\ \hline \end{array},$$

where Y_0 is a square matrix of size $C_2 4^k$, and each Y_j matrix with $j \geq 1$ has $C_2 4^k$ rows and 2^k columns. We now apply the operation in (8.8) to the blocks shown above, indicating only those entries that are involved in the operation (all other entries will remain unchanged).

We first remove the 1 entries below Y_0 and to the right of it, by adding all cuboids whose top left vertex is on the diagonal of Y_0, bottom left vertex is in the last row of Y, top right vertex is in the last column of Y, and bottom right vertex is at the bottom right corner of Y. (There are $C_2 4^k$ such cuboids.) This is illustrated below.

$$\begin{array}{|c||c|}\hline Y_0 & 1^t_{C_2 4^k} \\ \hline 1_{C_2 4^k} & 1 \\ \hline \end{array} = \begin{array}{|cccc||c|}\hline 2^k & \cdots & \cdots & \cdots & 1 \\ \cdots & 2^k & \cdots & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \cdots & \cdots & \cdots & 2^k & 1 \\ \hline 1 & 1 & \cdots & 1 & 1 \\ \hline \end{array} \quad \to \quad \begin{array}{|cccc||c|}\hline 2^k+1 & \cdots & \cdots & \cdots & 0 \\ \cdots & 2^k+1 & \cdots & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \cdots & \cdots & \cdots & 2^k+1 & 0 \\ \hline 0 & 0 & \cdots & 0 & C_2 4^k+1 \\ \hline \end{array}$$

At this point, we have replaced Y with the matrix

$$\begin{array}{|c||c|c|c|c||c|}\hline Y_0' & Y_1 & Y_2 & \cdots & Y_{(C_1-C_2)2^k} & 0 \\ \hline 0 & 1_{2^k} & 1_{2^k} & \cdots & 1_{2^k} & C_2 4^k+1 \\ \hline \end{array},$$

[1] In terms of mask polynomials, the operation in (8.8) corresponds to adding a polynomial of the form $X^c(1-X^{d_1 N/p^a})(1-X^{d_2 N/q^d})$, with $d_1 \in \{1,2,\dots,p^a-1\}$ and $d_2 \in \{1,2,\dots,q^b-1\}$. This means that we are adding either an N-cuboid as defined in (2.7), or else an N'-cuboid for some $pq \mid N' \mid N$.

where all entries of Y_0' are either zero or at least 2^k. We still need to remove all the 1 entries below the blocks Y_j with $j \geq 1$. Pick one such block, and note that it contains at least one square subblock equal to G. We will only work with that subblock and the row of 1's at the bottom; all other entries will remain unchanged. We add all cuboids whose top left vertex is on the diagonal of that block except for the last diagonal entry, bottom left vertex is in the last row of Y, and top right vertex is in the last column of Y_j. (There are $2^k - 1$ such cuboids.) This is shown below.

$$\begin{array}{|c|}\hline Y_j \\ \hline 1_{2^k} \\ \hline \end{array} = \left|\begin{array}{ccccc} \vdots & \vdots & \vdots & \vdots & \vdots \\ \hline 2^k & \cdots & \cdots & \cdots & 2^k \\ \cdots & 2^k & \cdots & \cdots & 2^k \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \cdots & \cdots & \cdots & 2^k & 2^k \\ \cdots & \cdots & \cdots & \cdots & 2^k \\ \hline \vdots & \vdots & \vdots & \vdots & \vdots \\ \hline 1 & 1 & \cdots & 1 & 1 \end{array}\right| \quad \rightarrow \quad \left|\begin{array}{ccccc} \vdots & \vdots & \vdots & \vdots & \vdots \\ \hline 2^k+1 & \cdots & \cdots & \cdots & 2^k-1 \\ \cdots & 2^k+1 & \cdots & \cdots & 2^k-1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \cdots & \cdots & 2^k+1 & \cdots & 2^k-1 \\ \cdots & \cdots & \cdots & \cdots & 2^k \\ \hline \vdots & \vdots & \vdots & \vdots & \vdots \\ \hline 0 & 0 & 0 & \cdots & 2^k \end{array}\right|$$

Applying this procedure to all blocks Y_j, we get a matrix Y' with row sums p^a, column sums q^b, and all entries either zero or at least $2^k - 1$. Further, all entries of Y' are bounded by $C_2 4^k + 1 = q^b$. The corresponding multiset $B \in \mathcal{M}^+(\mathbb{Z}_N)$ has total weight $|B| = N$ and satisfies (8.6).

We now construct a set $A \subset \mathbb{Z}_M$ that inherits the above properties from B and, additionally, satisfies $\Phi_M \mid A$. As in the proof of Proposition 8.4, let $\pi : \mathbb{Z}_M \to \mathbb{Z}_N$ be the natural projection defined by $\pi(x) = x \bmod N$. For each $x \in \mathbb{Z}_N$, its preimage $\pi^{-1}(x) = \Lambda(x, N)$ is a union of $D(M)/N$ pairwise disjoint grids $\Lambda(y, D(M))$ with $y \in \pi^{-1}(x)$.

By the assumption (i), each nonzero entry in B is greater than or equal to pq. By Lemma 8.5, we can write each such entry as a linear combination of p and q with coefficients in $\mathbb{N}_0$; note that the sum of these coefficients is bounded trivially by the size of the largest entry in Y', that is, by q^b. Thus, for each $x \in \mathbb{Z}_N$ such that $w_B^N(x) \neq 0$, we may define $A \cap \Lambda(x, N)$ as a union of at most q^b fibers in the p and q direction. By the assumption (iv) of the theorem, we have $D(M)/N > q^b$, so that we may place each such fiber in a different $D(M)$-grid, ensuring that A is a set. By Proposition 2.2, it follows that $\Phi_M \mid A$. Furthermore, since $A \equiv B \bmod N$, we have $|A| = |B| = N$ and (8.5) is inherited from (8.6). Hence, A satisfies all requirements of the theorem. □

We note that the cuboid-adding operation (8.8) was also the key to the constructions in Propositions 8.2 and 8.4. The matrices in both of these propositions can be obtained, by adding and subtracting cuboids, from a "uniform" matrix with all entries equal to 1.

We did not try to optimize the exponents m and n in Theorem 8.7, opting instead for clarity of the presentation. For example, we could have used (8.8) more efficiently to get Y' with all nonzero entries of size about 2^k, reducing the size of m and n.

The construction in Theorem 8.7 admits two natural directions of generalization. One is that we could modify it to guarantee *simultaneous divisibility* by a block of the form

$$\prod_{L:L_0|L|M} \Phi_L(X),$$

where $L_0 = p^\alpha q^\beta \mid M = p^n q^m$. This can be achieved by replacing the single p- and q-fibers with long $p^{n-\alpha+1}$- and $q^{m-\beta+1}$-fibers, using Proposition 6.3. The argument remains valid in this setting, as long as the associated multiplicative constraints are satisfied and the disjointness of the fiber structure is maintained.

The construction also extends inductively to the case of *arbitrary finite sets of primes* $\{p_1, \dots, p_r\}$, provided that the parameters involved are chosen sufficiently large. In particular, one may invoke a multivariate analogue of Lemma 8.6 to guarantee the necessary congruences modulo 2^ℓ, and apply the additive decomposition as in Lemma 8.5 recursively. The key structural requirements (separability of fibers, modular compatibility, and size bounds) scale in a controlled way as the number of primes increases. However, this would complicate the construction considerably, and in any case simpler examples (such as Example 8.1) are available when 3 or more prime factors are allowed.

9. Lower bounds under the (T2) assumption

9.1. Structure results under the (T2) assumption

Assume that $M = \prod_{i=1}^K p_i^{n_i}$ and that $K \geq 2$. In this section we prove structure results for sets $A \subset \mathbb{Z}_M$ obeying the conditions (T1) and (T2). We first prove the short counting lemma mentioned in the introduction.

Lemma 9.1. *[3, Lemma 2.1] Assume that $A \oplus B = \mathbb{Z}_M$. Let S_A^* be the set of prime powers p^α such that $\Phi_{p^\alpha}(X)$ divides $A(X)$ and let S_M^* be the set of all prime powers that divide M. Then*

$$|A| = \prod_{s \in S_A^*} \Phi_s(1), \ |B| = \prod_{s \in S_B^*} \Phi_s(1).$$

Moreover, the sets S_A^* and S_B^* are disjoint, and $S_A^* \cup S_B^* = S_M^*$.

Proof. The equality $S_A^* \cup S_B^* = S_M^*$ follows from (1.10). Furthermore, we have $\Phi_s(1) = p$ if $s = p^\alpha$ is a prime power, and $\Phi_s(1) = 1$ otherwise. This implies the divisibility chain

$$M = \prod_{s \in S_M^*} \Phi_s(1) \ \Big| \ \prod_{s \in S_A^*} \Phi_s(1) \prod_{s \in S_B^*} \Phi_s(1) \ \Big| \ A(1)B(1) = M.$$

Hence equality must hold at each step, and the lemma follows. □

Recall that the truncation $A' \in \mathcal{M}^+(\mathbb{Z}_{M'})$ of a multiset $A \subset \mathcal{M}^+(\mathbb{Z}_M)$ relative to a set of divisors $S \subset \mathcal{D}(M)$ was introduced in Proposition 4.1 and defined formally in (4.8). The next lemma says that if A obeys (T2), then its truncation A' is uniformly distributed mod M'.

Lemma 9.2. *Let $A \in \mathcal{M}^+(\mathbb{Z}_M)$ and set $S = S_A^*$, defined in Lemma 9.1. Let $A' \in \mathcal{M}^+(\mathbb{Z}_{M'})$ be the truncation of A relative to S. If A satisfies (T2), then*

$$1 + X + \cdots + X^{M'-1} \,\big|\, A'(X). \tag{9.1}$$

Proof. If A satisfies (T2), then $\Phi_s(X) \mid A'(X)$ for every $1 \neq s \mid M'$ by applying Proposition 4.1 (ii) for $S = S_A^*$. Since

$$1 + X + \cdots + X^{M'-1} = \prod_{1 \neq s \mid M'} \Phi_s(X),$$

the divisibility (9.1) of $A'(X)$ then follows. □

9.2. A diagonal argument

Our first result carries no restrictions on the number of prime factors of M. For each $i \in \{1, \dots, K\}$, we use the notation

$$\beta_i := \max\{\beta \in \mathbb{N} : \ \Phi_{p_i^\beta} \mid A\}.$$

Proposition 9.3. *Assume that $M := \prod_{i=1}^K p_i^{n_i}$ for $K \geq 2$, where $p_1, \dots, p_K$ are distinct primes. Suppose that $A \in \mathcal{M}^+(\mathbb{Z}_M)$ satisfies (T2). Then, if there exists some $N = p_1^{\gamma_1} \cdots p_K^{\gamma_K}$ such that $\Phi_N(X) \mid A(X)$ and $\gamma_i > \beta_i$ for all $i \in \{1, \dots, K\}$, then*

$$A(1) \geq \min(p_1, \dots, p_K) \prod_{s \in S_A^*} \Phi_s(1).$$

In particular, this gives a negative answer to Question 1.7 in the introduction under the additional assumption that the additional unsupported divisor Φ_N is as indicated in the proposition.

Proof. Choose $A' \in \mathcal{M}^+(\mathbb{Z}_{M'})$ to be the truncation of A relative to $S = S_A^* \cup \{N\}$. Notice, then, that $(A' \equiv A'' \mod M'')$, where $A'' \in \mathcal{M}^+(\mathbb{Z}_{M''})$ is the truncation of A relative to S_A^*. This is illustrated in Fig. 2 (where M' and M'' are both labeled, for reference).

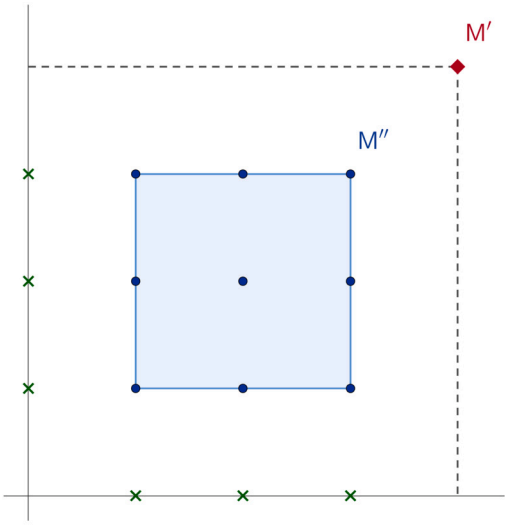


Fig. 2. When N is maximal, the truncation of A relative to $S_A^* \cup \{N\}$ has a full block of cyclotomic divisors below an unsupported divisor $\Phi_{M'}(X)$.

Proposition 4.1 combined with Lemma 9.2 then imply that

$$A'(X) = w\big(1 + X + \cdots + X^{M''-1}\big) \mod X^{M''} - 1, \tag{9.2}$$

for some integer weight $w \geq 1$. We claim that $w \geq \min(p_1, \ldots, p_K)$. This follows because, for each $x \in \mathbb{Z}_{M'}$, we have

$$w_A^{M''}(x) := \sum_{\{\bar{x} \in \mathbb{Z}_N : \bar{x} \equiv x \bmod M''\}} w_A^{M'}(\bar{x}).$$

However, since $D(M') = M''$, we see that $\{\bar{x} \in \mathbb{Z}_{M'} : \bar{x} \equiv x \bmod M''\} = \Lambda(x, D(M'))$. Since

$$\Phi_{M'}(X) \mid A(X) \Leftrightarrow \Phi_{M'}(X) \mid (A \cap \Lambda(x, D(M'))),$$

for each $x \in \mathbb{Z}_{M'}$, the bound (1.2) of Lam and Leung gives $w \geq \min(p_1, \ldots, p_K)$. This, together with (9.2) and the fact that $\prod_{s \in S_A^*} \Phi_s(1) = M''$, gives the result. □

9.3. (T2) lower bounds for two prime factors

In this subsection, we will assume that M has two distinct prime factors p_1 and p_2. As in Section 10, we will abbreviate $p := p_1$ and $q := p_2$. We will continue to use the numerical indices where appropriate, so that for example F_1^N will still denote a fiber in the p direction on scale N and $\mathsf{EXP}_1(S)$ will denote the set of exponents of $p = p_1$ in S.

Under these assumptions upon M, we then have the following general size increase when A satisfies $(T2)$ and admits an unsupported divisor N.

Theorem 9.4. *Let $M = p^m q^n$ and suppose that $A \in \mathcal{M}^+(\mathbb{Z}_M)$ satisfies (T2). If there exists some $N = p^\gamma q^\eta$ such that $\Phi_N(X) \mid A(X)$ and $\Phi_{p^\gamma}(X), \Phi_{q^\eta}(X) \nmid A(X)$, then*

$$A(1) > \prod_{s \in S_A^*} \Phi_s(1). \tag{9.3}$$

Of course, we always have that

$$A(1) \geq \prod_{s \in S_A^*} \Phi_s(1),$$

for any multiset $A \in \mathcal{M}^+(\mathbb{Z}_M)$. Theorem 9.4 is an improvement because it shows that this inequality must be strict if A admits an unsupported divisor.

We will prove Theorem 9.4 in four cases depending upon the location of the unsupported divisor. Proposition 9.3 already handles the case where N has maximal p_1 and p_2 exponents. The remaining three cases are the content of Proposition 9.5 and Corollary 9.7. Of the remaining cases to consider, the situation where both γ and η are neither maximal nor minimal contains the most new ideas. We present the proof of this result first, often referencing the key ideas which are developed in the proof of later cases.

To this end, let

$$\alpha_i := \min\{\alpha \in \mathbb{N} : \Phi_{p_i^\alpha}(X) \mid A(X)\}$$

denote the minimal prime power exponents associated to cyclotomic divisors of $A(X)$. We will also use the notation

$$\mathsf{EXP}^*(i) := \{v \in \mathbb{N} : \Phi_{p_i^v}(X) \mid A(X)\}$$

to denote the exponents associated to prime power cyclotomic divisors of A.

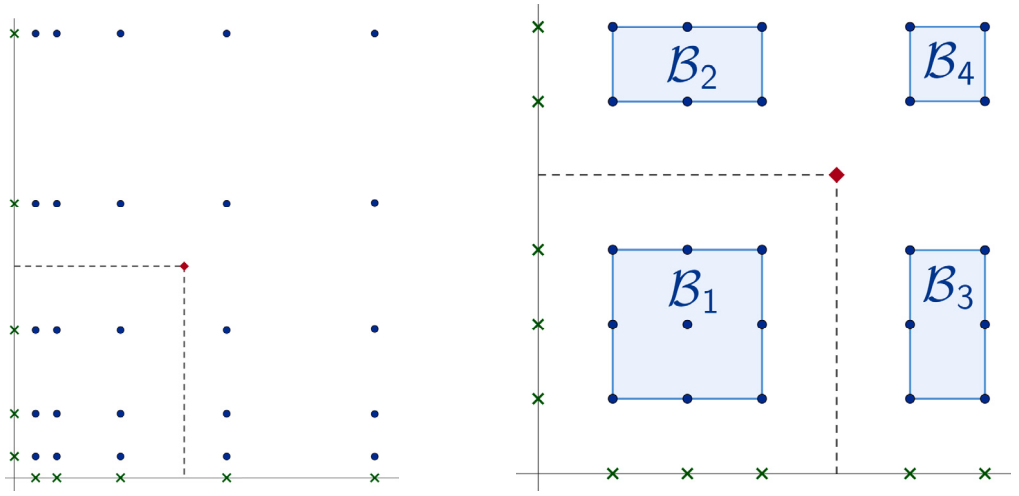
Proposition 9.5. *Let $M = p^m q^n$ and $A \in \mathcal{M}^+(\mathbb{Z}_{p^m q^n})$. Suppose that A satisfies (T2) and also has an unsupported divisor $\Phi_N(X) \mid A(X)$ with $N = p^\gamma q^\eta$ satisfying $\alpha_1 < \gamma < \beta_1$ and $\alpha_2 < \eta < \beta_2$. Then A has the size increase given in (9.3).*

Proof. Using Proposition 4.1, we assume that

$$\mathsf{EXP}^*(1) := \{1, \dots, \gamma - 1, \gamma + 1, \dots, m\}, \quad \mathsf{EXP}^*(2) := \{1, \dots, \eta - 1, \eta + 1, \dots, n\}.$$

In this case, inequality (9.3) becomes $A(1) > p^{m-1} q^{n-1}$. We assume, in contradiction, that $A(1) = p^{m-1} q^{n-1}$. This configuration of cyclotomic divisors is illustrated in Fig. 3. Let

$$\begin{aligned} M_1 &= p^{\gamma-1} q^{\eta-1}, & M_2 &= p^{\gamma-1} q^n, & M_3 &= p^m q^{\eta-1}, & M_4 &= p^m q^n \\ N_1 &= pq, & N_2 &= pq^{\eta+1}, & N_3 &= p^{\gamma+1} q^n, & N_4 &= p^{\gamma+1} q^{\eta+1} \end{aligned}$$



(A) Before truncation (B) After truncation

Fig. 3. Green cross points are prime power divisors, blue circle points are $(T2)$ divisors, and the red diamond point is the unsupported divisor. After truncation, we have four complete blocks of divisors.

so that each M_l (resp. N_l) denotes the upper-right (resp., lower left) vertex of the block $\mathcal{B}_l$ which are shown in Fig. 3. Notice that, as A satisfies $(T2)$ (and has been uniformized), our blocks are the clusters $\mathcal{B}_l := \{s \in \mathcal{D}(M) : N_i \mid s \mid M_i\}$. We carefully demarcate when we work in each of the clusters $\mathcal{B}_1, \dots, \mathcal{B}_4$, as the corresponding steps are repeated in proofs of later results.

Block $\mathcal{B}_4$: Applying Proposition 6.3 to the block $\mathcal{B}_4$ produces polynomials $P_1(X), P_2(X) \in \mathbb{Z}[M]$ with non-negative coefficients such that

$$A(X) = P_1(X)F^{M_4}_{1,m-\gamma}(X) + P_2(X)F^{M_4}_{2,n-\eta}(X) \mod X^{M_4} - 1. \tag{9.4}$$

We may assume that $P_1 \not\equiv 0$, and so we will work with the block $\mathcal{B}_2$ in the next step (this is where we rely on the fact that both $\mathcal{B}_2$ and $\mathcal{B}_3$ are contained in S_A).

Block $\mathcal{B}_2$ or $\mathcal{B}_3$: Our next goal is to show that $A \bmod M_2$ can be expressed as a linear combination of long fibers in the q direction alone. Applying Proposition 6.3 to the block $\mathcal{B}_2$ produces polynomials $Q_1(X), Q_2(X) \in \mathbb{Z}[X]$ with non-negative coefficients such that

$$A(X) = Q_1(X)F^{M_2}_{1,\gamma-1}(X) + Q_2(X)F^{M_2}_{2,n-\eta}(X) \mod X^{M_2} - 1. \tag{9.5}$$

We want to show that we can take $Q_1 \equiv 0$ in this long fiber decomposition.

We now make use of the fact that $\Phi_{q^{\eta+1}}(X), \dots, \Phi_{q^n}(X) \mid A(X)$. All $q^{n-\eta}$-fibers at scale M_2 are necessarily constant mod q^s for every $s \in \{\eta+1, \dots, n\}$. Hence, the number of $p^{\gamma-1}$-fibers at scale M_2 must be equidistributed along these same q^s cosets. However, the length of each such $p^{\gamma-1}$-fiber at scale M_2 is maximal in $\mathbb{Z}_{M_2}$, which follows from the fact that $p^{\gamma-1} \mid\mid M_2$. Hence, equidistribution in number is equivalent to being a complete

grid (at least, in this special case where our long fibers have maximal length). This lets us then assume that $Q_1 \equiv 0$ in (9.5).

Recall that we are assuming that $A \bmod M_4$ has mask polynomial (9.4) with $P_1 \not\equiv 0$. This means that $A \bmod M_4$ has (at least) one $p^{m-\gamma}$ long fiber in the p direction with a positive weight. This long fiber collapses to a point $y \in \mathbb{Z}_{M_2}$ with multiplicity at least $p^{m-\gamma}$ (which just means that $w_A^{M_2}(y) \geq p^{m-\gamma}$). Since we have assumed that $A \bmod M_2$ is a linear combination of $q^{n-\eta}$-fibers, there exists a set $F \in \mathcal{M}^+(\mathbb{Z}_{M_4})$ such that

$$F(X) = X^y F_{2,n-\eta}^{M_2}(X) \mod X^{M_2} - 1,$$

and such that

$$(A \cap F)(X) := w\, F_{2,n-\eta}^{M_2}(X) \mod X^{M_2} - 1 \Rightarrow (A \cap F)(1) = w\, q^{n-\eta}, \tag{9.6}$$

where the weight $w \in \mathbb{N}$ is constant and satisfies $w \geq p^{m-\gamma}$. We remind the reader that the multiset $A \cap F \in \mathcal{M}^+(\mathbb{Z}_M)$ is defined via the equality of weights

$$w_{A\cap F}^M(x) = w_A^M(x) w_F^M(x), \quad \forall x \in \mathbb{Z}_M.$$

Block $\mathcal{B}_1$: The multiset $A \cap F$ collapses to a single point $x \in \mathbb{Z}_{M_1}$ which satisfies $w_A^{M_1}(x) \geq p^{m-\gamma} q^{n-\eta}$. Observe that, by Lemma 9.2 and the assumption that $A(1) = p^{m-1} q^{n-1}$, one has

$$A(X) = p^{m-\gamma} q^{n-\eta} \big(1 + X + \cdots + X^{M_1}\big) \mod X^{M_1} - 1. \tag{9.7}$$

Hence, we must have that

$$(A \cap F)(1) = w_A^{M_1}(x) = w\, q^{n-\eta} = p^{m-\gamma} q^{n-\eta} \Rightarrow w = p^{m-\gamma}. \tag{9.8}$$

Consequently, we know that

$$(A \cap F)(X) = p^{m-\gamma} F_{2,n-\eta}^{M_2}(X) \mod X^{M_2} - 1. \tag{9.9}$$

We obtain that $A \cap F \mod X^{M_4} - 1$ is a union of $p^{m-\gamma}$-fibers.

The unsupported divisor N: In fact, we now want to work with the set $A \cap F \bmod N$, in addition to considering the whole set $A \bmod N$. This which amounts to only examining the part of A which intersected the long fiber as in (9.9). Hence, let $B \in \mathcal{M}^+(\mathbb{Z}_N)$ satisfy $B \equiv (A \cap F) \bmod N$.

Since $\Phi_N(X) \mid A(X)$, there exist polynomials $R_1(X), R_2(X) \in \mathbb{Z}[X]$ with non-negative coefficients such that

$$A(X) = R_1(X) F_1^N(X) + R_2(X) F_2^N(X) \mod X^N - 1. \tag{9.10}$$

We also remark that (9.9) implies that

$$B(X) = p^{m-\gamma} q^{n-\eta} X^z \mod X^{N/p} - 1 \tag{9.11}$$

for some $z \in \mathbb{Z}_{N/p}$.

We now rely upon the fact that $P_1 \not\equiv 0$ in (9.4). Any $p^{m-\gamma}$-fiber at scale M_4 collapses to a single point in $\mathbb{Z}_N$ with multiplicity $p^{m-\gamma}$. As we have seen earlier, the preimage of multiset B mod N taken mod M_4 is actually a union of $p^{m-\gamma}$-fibers. Hence, $p^{m-\gamma} \mid w_B^N(z')$ for every $z' \in \mathbb{Z}_N$. We distinguish two cases.

In case where $(z' * F_2^N) \subset A \bmod N$ (i.e., z' belongs to a q-fiber at scale N), the congruence for $A(X)$ implies

$$w_A^{M_1}(z') = w_A^{N/p}(z') = w_B^{N/p}(z') = p^{m-\gamma} q^{n-\eta},$$

which further implies that

$$w_A^{N/p}(z' + \frac{jN}{pq}) = 0 \text{ and } w_A^N(z' + \frac{jN}{q}) = 0, \quad \text{for } j \not\equiv 0 \bmod q.$$

Therefore, $w_A^{M_1}(z') \geq p^{m-\gamma} q^{n-\eta+1}$, contradiction.

Otherwise, if $z' \in \mathbb{Z}_N$ belongs to a single p-fiber at scale N, then $w_B^{N/p}(z') = p w_B^N(z')$, which is divisible by $p^{m-\gamma+1}$, contradiction. □

Remark 9.6. Notice that the conditions $\alpha_i < \gamma_i < \beta_i$ for $i \in \{1, 2\}$ guarantee that all of the blocks $\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3, \mathcal{B}_4$ which were utilized in the proof of Proposition 9.5 are non-empty. However, if $\gamma_i \notin [\alpha_i, \beta_i]$ for some $i \in \{1, 2\}$, then a corresponding combination of blocks will be empty. One such example is illustrated in Fig. 4. Even in these cases, however, the proof of Proposition 9.5 applies—with the caveat that one must omit any steps which correspond to empty blocks. This gives the following Corollary.

Corollary 9.7. *Let $M = p^m q^n$ and $A \in \mathcal{M}^+(\mathbb{Z}_{p^m q^n})$. Suppose that A satisfies (T2) and also has an unsupported divisor $\Phi_N(X) \mid A(X)$ with $N = p^{\gamma_1} q^{\gamma_2}$ with $\gamma_i \notin [\alpha_i, \beta_i]$ for some $i \in \{1, 2\}$. Then, A has the size increase (9.3).*

Proof. Left to the interested reader (see Remark 9.6). □

Notice that Proposition 9.4 furnishes a negative answer to Question 2 from Section 1 in the following special case.

Corollary 9.8. *Suppose that $A \subset \mathbb{N}_0$ satisfies (T1) and (T2), and that $lcm(S_A) = p^m q^n$ for two distinct prime factors p, q. Then A_0 does not have any unsupported divisors.*

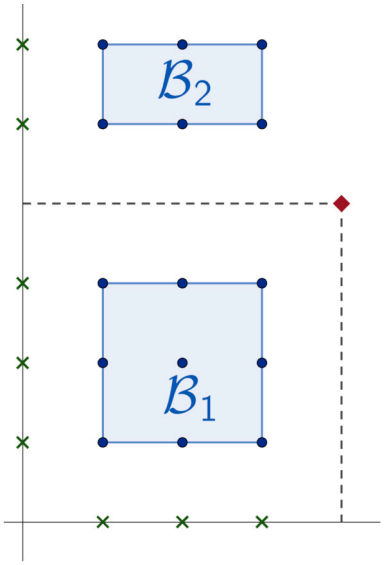


Fig. 4. An example of a configuration of cyclotomic divisors where $N = p^{\gamma_1}q^{\gamma_2}$ satisfies $\gamma_1 \notin [\alpha_1, \beta_1]$. Notice that, in this scenario, the blocks $\mathcal{B}_3$ and $\mathcal{B}_4$ are necessarily empty. As before: green cross points are prime power divisors, blue circle points are $(T2)$ divisors and the red diamond point is an unsupported divisor.

10. An example with 4 prime factors

10.1. An example

In this section, we prove Theorem 1.11 and give an affirmative answer to Question 1.7 from Section 1.3. Theorem 10.1 describes our example in more detail. While the set A below is constructed in a cyclic group $\mathbb{Z}_M$, we can clearly map it to a subset of $\mathbb{N}_0$.

Theorem 10.1. *Let* $M = (p_1p_2p_3p_4)^4$, *where*

$$p_1 > 40 \text{ and } p_i < p_{i+1} < 2p_i \text{ for } i = 1, 2, 3. \tag{10.1}$$

(The existence of primes satisfying (10.1) is guaranteed by Bertrand's Postulate.) Then there exists a set $A \subset \mathbb{Z}_M$ *such that:*

(i) *the prime power cyclotomic divisors of* $A(X)$ *are* $\Phi_{p_i^\alpha}(X)$ *for all* $i = 1, 2, 3, 4$ *and* $\alpha = 2, 3, 4$,
(ii) A *satisfies both (T1) and (T2), so that in particular we have* $|A| = (p_1p_2p_3p_4)^3$,
(iii) *additionally,* $A(X)$ *has the unsupported cyclotomic divisor* $\Phi_{p_1p_2p_3p_4}(X)$.

Proof. Let $N = p_1p_2p_3p_4$ for short, and recall that

$$F_{i,3}(X) = \frac{X^M - 1}{X^{M/p_i^3} - 1} \text{ for } i = 1, 2, 3, 4.$$

Define a set $U \subset \mathbb{Z}_M$ via

$$U(X) = \prod_{i=1}^{4} F_{i,3}(X),$$

so that $U = N\mathbb{Z}_M \simeq \mathbb{Z}_{D(M)}$. By Lemma 6.2, $F_{i,3}$ is divisible by all Φ_s such that $p_i^2 \mid s \mid M$, since then we have $s \mid M$ but $s \nmid (M/p_i^3)$. It follows that U has the prime power cyclotomic divisors indicated in (i), and satisfies both (T1) and (T2). In the terminology of [9], U is a standard tiling set with these cyclotomic divisors. We also have $U \oplus B = \mathbb{Z}_M$, where

$$B(X) = \prod_{i=1}^{4} (1 + X^{M_i} + \cdots + X^{(p_i-1)M_i}). \tag{10.2}$$

We do not have $\Phi_N \mid U$, since U modulo N is simply the point 0 with weight $|U| = N^3$. However, we will now rearrange the long fibers (i.e., sets with mask polynomial $X^l F_{i,3}(X)$ for some l) in U to get a set A whose mask polynomial does have Φ_N as an additional divisor.

We first construct a decomposition

$$U = U_1 \cup U_2 \cup U_3 \cup U_4,$$

where the sets U_i are nonempty, pairwise disjoint, and each U_i is a union of long fibers in the p_i direction. Specifically, let d_1, d_2, d_3 be integers such that

$$1 \le d_i < p_i^3 - 1, \ \ i = 1, 2, 3. \tag{10.3}$$

For any $x \in U$, we can represent its array coordinates (x_1, x_2, x_3, x_4) as $x_i = p_i \bar{x}_i$. We then define

$$U_i := Q_i * F_{i,3}, \quad i = 1, 2, 3, 4,$$

where

$$\begin{aligned}
Q_1 &:= \{(0, x_2, x_3, x_4) \in U : \ d_3 \le \bar{x}_2 < p_2^3, \ 0 \le \bar{x}_3 < d_1, \ \bar{x}_4 \text{ arbitrary}\}, \\
Q_2 &:= \{(x_1, 0, x_3, x_4) \in U : \ 0 \le \bar{x}_1 < d_2, \ d_1 \le \bar{x}_3 < p_3^3, \ \bar{x}_4 \text{ arbitrary}\}, \\
Q_3 &:= \{(x_1, x_2, 0, x_4) \in U : \ d_2 \le \bar{x}_1 < p_1^3, \ 0 \le \bar{x}_2 < d_3, \ \bar{x}_4 \text{ arbitrary}\}, \\
Q_4 &:= \{(x_1, x_2, x_3, 0) \in U : \ 0 \le \bar{x}_1 < d_2, \ 0 \le \bar{x}_2 < d_3, \ 0 \le \bar{x}_3 < d_1\} \\
&\quad \cup \{(x_1, x_2, x_3, 0) \in U : \ d_2 \le \bar{x}_1 < p_1^3, \ d_3 \le \bar{x}_2 < p_2^3, \ d_1 \le \bar{x}_3 < p_3^3\}.
\end{aligned} \tag{10.4}$$

We check that each $x \in U$ belongs to exactly one of the sets U_i. The proof is as follows. Let $x \in U$.

- Suppose first that $\bar{x}_1 < d_2$. If $\bar{x}_3 \geq d_1$, then $x \in U_2$. If $\bar{x}_3 < d_1$ and $\bar{x}_2 \geq d_3$, then $x \in U_1$. If $\bar{x}_3 < d_1$ and $\bar{x}_2 < d_3$, then $x \in U_4$. These choices are unique.
- Assume now that $\bar{x}_1 \geq d_2$. If $\bar{x}_2 < d_3$, then $x \in U_3$. If $\bar{x}_2 \geq d_3$ and $\bar{x}_3 < d_1$, then $x \in U_1$. If $\bar{x}_2 \geq d_3$ and $\bar{x}_3 \geq d_1$, then $x \in U_4$. These choices, again, are unique.

Next, we claim that the parameters d_1, d_2, d_3 may be chosen so that

$$p_i \mid |Q_i| \text{ for } i = 1, 2, 3, 4. \tag{10.5}$$

We already have $p_i^3 \mid |U_i|$ by construction (since $p_i^3 \mid |F_{i,3}|$); by (10.5), we actually have $p_i^4 \mid |U_i|$ for each i.

To ensure (10.5), we let $d_1 := p_1 p_4$, $d_2 := k p_2$ for some $k \in \mathbb{N}$ to be chosen later, and $d_3 := p_3$. Then:

- $|Q_1| = d_1(p_2^3 - d_3) = p_1 p_4 (p_2^3 - d_3) p_4^3$ is divisible by p_1,
- $|Q_2| = d_2(p_3^3 - d_1) = k p_2 (p_3^3 - d_1) p_4^3$ is divisible by p_2,
- $|Q_3| = d_3(p_1^3 - d_2) = p_3 (p_1^3 - d_2) p_4^3$ is divisible by p_3.

We now consider Q_4, with

$$|Q_4| = d_1 d_2 d_3 + (p_1^3 - d_2)(p_2^3 - d_3)(p_3^3 - d_1).$$

We have $p_4 \mid d_1 \mid d_1 d_2 d_3$. To ensure that p_4 also divides the second term in $|Q_4|$, it suffices to choose k so that p_4 divides $p_1^3 - d_2$. The numbers $p_1^3 - k p_2$ with $k = 1, 2, \ldots, p_4$ all have distinct residues mod p_4, so that there exists a value of k such that p_4 divides $p_1^3 - k p_2$, as claimed.

It remains to check that the above values of d_1 and d_2 are permissible, in the sense that they obey (10.3). It suffices to ensure that

$$p_1 p_4 < p_3^3 - 1 \text{ and } p_4 p_2 < p_1^3 - 1.$$

This follows if we verify that $p_i p_j < p_1^3 - 1$ for any choice of distinct indices i, j since $p_1^3 - 1 \leq p_k^3 - 1$ for every k. By (10.1), we have

$$p_i p_j \leq p_3 p_4 < (4p_1)(8p_1) = 32 p_1^2 < p_1^3 - 1,$$

as claimed.

We are now ready to rearrange our initial set U to produce A. For each $i = 1, 2, 3, 4$, we divide Q_i into p_i pairwise disjoint subsets of cardinality $|Q_i|/p_i$ each:

$$Q_i = Q_{i,1} \cup \cdots \cup Q_{i,p_i}, \quad |Q_{i,1}| = \cdots = |Q_{i,p_i}| = |Q_i|/p_i.$$

We then let

$$A_i := \bigcup_{j=1}^{p_i} \bigcup_{x \in Q_{i,j}} (x + jM_i) * F_{i,3}.$$

In other words, if $x * F_{i,3}$ is a long fiber in U_i, we shift that fiber in the p_i direction (consistently with the direction of $F_{i,3}$) by an increment of jM_i, where j is chosen based on which set $Q_{i,j}$ contains x. This is similar to the "fiber shifting" constructions of Szabó [25] (see also [10,11]).

Let $A = A_1 \cup A_2 \cup A_3 \cup A_4$. We prove that A is a set. To do so, it suffices to verify that A_1, A_2, A_3, A_4 are pairwise disjoint. Let $a \in A_i$ and $a' \in A_j$ for some $i \neq j$. Then $a = u + \nu M_i$ and $a' = u' + \nu' M_j$ for some $u \in U_i$, $u' \in U_j$, $\nu \in \{1, \dots, p_i\}$, and $\nu' \in \{1, \dots, p_j\}$. We claim that

$$\exists k \notin \{i, j\} \text{ such that } u_k \neq u'_k. \tag{10.6}$$

Then $a_k = u_k \neq u'_k = a'_k$, so that $a \neq a'$ as claimed.

The proof of (10.6) is by direct case-by-case verification based on (10.4).

i, j	1,2	1,3	1,4	2,3	2,4	3,4
k	3	2	2 or 3	1	1 or 3	1 or 2

In the third and last two cases, the value of k depends on whether $(u'_1, u'_2, u'_3, 0)$ belongs to the first or second set in the definition of Q_4 in (10.4).

Since $|A_i| = |U_i|$ for each i, it follows that $|A| = |U| = N^3$, where we recall that $N = p_1p_2p_3p_4$. We now check that $\Phi_N \mid A$, where $N = p_1p_2p_3p_4$. It suffices to check that $\Phi_N \mid A_i$ for each $i = 1, 2, 3, 4$. Fix such i. For each $x \in Q_{i,j}$, we have $x \equiv 0$ and $F_{i,3}(X) \equiv 0 \mod N$, so that the fiber $(x + jM_i) * F_{i,3}$ reduced modulo N is simply the point $j'N/p_i$ with multiplicity p_i^3, where $j' \equiv j(N/p_i)^3 \pmod{p_i}$. Thus A_i reduced modulo N is the fiber F_i^N with multiplicity $p_i^{-1}|Q_i|p_i^3 = |Q_i|p_i^2$. It follows that A_i is divisible by Φ_N as required.

We now present two different methods of verification that A has the cyclotomic divisors claimed in parts (i) and (ii) of the theorem. Each method provides a different insight as to whether a similar construction could also furnish a counterexample to the Coven-Meyerowitz conjecture; we discuss this in more detail after the proof of the theorem is completed.

Method 1: Divisor sets. We note that the set B defined in (10.2) is a *standard tiling complement* in the terminology of [9]. If we can prove that

$$A \oplus B = \mathbb{Z}_M, \tag{10.7}$$

it follows that $\Phi_s \mid A$ for all $s \mid M$ such that $s \neq 1$ and $\Phi_s \nmid B$. This includes all $\Phi_{p_i^\alpha}(X)$ for all $i = 1, 2, 3, 4$ and $\alpha = 2, 3, 4$ (by Lemma 9.1, A cannot have any other prime power cyclotomic divisors), as well as all cyclotomic divisors required by (T2) (see [9, Proposition 3.4]).

By Sands's Theorem [21], (10.7) will follow if we prove that $\mathrm{Div}(A) \cap \mathrm{Div}(B) = \{M\}$, where

$$\mathrm{Div}(A) = \{(a - a', M) : \ a, a' \in A\}$$

and similarly for B. Let us write $d = \prod_{i=1}^{4} p_i^{\delta_i}$, where $\delta_i \in \{0, 1, 2, 3, 4\}$ for a divisor of M. We have

$$\mathrm{Div}(B) = \{d = \prod_{i=1}^{4} p_i^{\delta_i} \in \mathbb{Z}_M : \ \forall i \in \{1, 2, 3, 4\}, \ \text{either } \delta_i = 0 \text{ or } \delta_i = 4\}.$$

In other words $d_i = 0$ or $p_i \nmid d_i$ if we write $d = \sum_{i=1}^{4} d_i M_i$. It therefore suffices to prove that

$$\mathrm{Div}(A) \subset \{M\} \cup \{d \in \mathbb{Z}_M : \ \exists k \in \{1, 2, 3, 4\} \text{ such that } \delta_k \notin \{0, 4\}\}. \tag{10.8}$$

Indeed, suppose that $a, a' \in A$ satisfy $a \neq a'$. As before, we write $a = u + \nu M_i$ and $a' = u' + \nu' M_j$ for some $u \in U_i$, $u' \in U_j$, $\nu \in \{1, \dots, p_i\}$, and $\nu' \in \{1, \dots, p_j\}$. We need to prove that $(a - a', M)$ belongs to the set on the right-hand side of (10.8). We consider the following cases.

- If $i \neq j$, we choose k as in (10.6); since p_k divides both u_k and u'_k, the claim in (10.8) is true with this value of k.
- If $i = j$ and there exists $k \neq i$ such that $u_k \neq u'_k$, then the claim is true for this k.
- If $i = j$ and $u_\ell = u'_\ell$ for all $\ell \neq i$, we must have $\nu \neq \nu'$, so that the claim is true with $k = i$.

Method 2: Direct verification. We need to prove that $\Phi_s \mid A$ for all $s = \prod_{j \in J} p_j^{\alpha_j}$, where $J \subset \{1, 2, 3, 4\}$, $J \neq \emptyset$, and $\alpha_j \in \{2, 3, 4\}$ for all $j \in J$. We fix such s for the rest of the proof.

For all $i \in J$, we have $\Phi_s \mid F_{i,3}$ by Lemma 6.2. It follows that

$$\Phi_s \mid U_i \text{ and } \Phi_s \mid A_i \text{ for all } i \in J. \tag{10.9}$$

Further, since $\Phi_s \mid U$ as noted above, we also have

$$\Phi_s(X) \ \Big| \ U(X) - \sum_{i \in J} U_i(X) = \sum_{i \notin J} U_i(X). \tag{10.10}$$

Let $L = \prod_{j \in J} p_j^4$. Then $s \mid L$, so that for any polynomial $G(X)$ we have $\Phi_s \mid G$ if and only if $\Phi_s \mid (G \bmod L)$. In particular, Φ_s divides $\sum_{i \notin J} U_i(X) \bmod X^L - 1$. However, we have $U_i \equiv A_i \bmod L$ for all $i \notin J$, so that

$$\sum_{i\notin J} U_i(X) \equiv \sum_{i\notin J} A_i(X) \mod X^L - 1.$$

It follows from (10.10) that $\Phi_s \mid \sum_{i\notin J} A_i(X)$. This together with (10.9) implies that $\Phi_s \mid A$ as claimed. □

10.2. Further remarks

We have not tried to optimize the size of M or the conditions on the size of the primes, so that improvements in that regard may be possible. On the other hand, no similar construction based on shifting fibers can work when M has only three distinct prime factors, since the three-prime analogue of U does not admit a decomposition similar to (10.4). We do not know whether the answer to Question 1.7 in $\mathbb{Z}_M$ is positive or negative in that case.

We do not know whether some modification of the construction in Theorem 10.1 could be used to give a counterexample to the Coven-Meyerowitz conjecture. We do not see an obvious reason why this could not ultimately work, but there are also significant obstacles, which we now discuss.

We adopt the notation from the proof of Theorem 10.1. As explained in the introduction, one could try to construct a tiling $A \oplus B' = \mathbb{Z}_M$, where B' is not divisible by Φ_N. It is easy to find sets B' that satisfy some (but not all) of the requirements to be a tiling complement for A. For instance, let B' be any set in $\mathbb{Z}_M$ such that

$$B'(X) \equiv \frac{X^N - 1}{X - 1} + \prod_{i=1}^{4} (X^{N/p_i} - 1) \mod X^N - 1.$$

Then $\Phi_s \mid B'$ for all s such that $s \in \mathcal{D}(N) \setminus \{N\}$ (in particular $\Phi_{p_i} \mid B'$ for all $i \in \{1, 2, 3, 4\}$), but $\Phi_N \nmid B'$. This, however, is not sufficient to produce a tiling.

An argument similar to that in the Method 2 part of the proof of Theorem 10.1 shows that $\Phi_s \mid A$ for $s = \prod_i p_i^{\alpha_i}$, where $\alpha_i = 1$ for exactly one value of i. However, this leaves out all Φ_s with $\alpha_i = 1$ for two or three values of i. We do not see how to ensure that, in addition to all of the above properties, at least one of A or B' has those divisors.

Alternatively, one could consider the divisor sets of A and B'. In constructions like the one above (possibly with minor modifications of the parameters), we expect that $\mathrm{Div}(A)$ will occupy most of the set in (10.8). The only elements of that set that we know to *not* belong to $\mathrm{Div}(A)$ are those d for which $p_i \mid d_i \neq 0$ for one value of i, and $p_j \nmid d_j$ for all $j \neq i$. This does not leave much room to construct a tiling complement that is substantively different from the standard tiling set B (or its easy modifications such as dilates).

We cannot exclude the possibility that, starting from a similar construction for A but with more scales or distinct prime factors, alternative tiling complements not satisfying (T2) could in fact be found.

Acknowledgment

We express our gratitude to the anonymous referee for their comments and suggestions, which significantly improved the clarity and precision of the paper. In particular, we are thankful for the simplification at the end of the proof of Proposition 9.4.

The research was partly carried out at the Erdős Center, Rényi Institute, in the framework of the semester "Fourier analysis and additive problems".

The first author was supported by Hungarian National Foundation for Scientific Research NKFIH, Grants STARTING 150576, FK 142993, Excellence 154121 and by the János Bolyai Research Fellowship of the Hungarian Academy of Sciences. The second author was supported by NSERC Discovery Grant 22R80520. The third author was supported by NSERC Discovery Grants 22R80520 and GR010263. The fourth author was supported by Hungarian National Foundation for Scientific Research, Grants OTKA K138596 and STARTING 150576, and by ARC Discovery Project DP250104965.

References

[1] M. Bond, I. Łaba, A. Volberg, Buffon needle estimates for rational product Cantor sets, Amer. J. Math. 136 (2014) 357–391.
[2] L. Christie, K. Dykema, I. Klep, Classifying minimal vanishing sums of roots of unity, preprint, arXiv:2008.11268.
[3] E. Coven, A. Meyerowitz, Tiling the integers with translates of one finite set, J. Algebra 212 (1999) 161–174.
[4] N.G. de Bruijn, On the factorization of cyclic groups, Indag. Math. 15 (1953) 370–377.
[5] D.E. Dutkay, C-K. Lai, Some reductions of the spectral set conjecture to integers, Math. Proc. Cambridge Philos. Soc. 156 (2014) 123–135.
[6] B. Fuglede, Commuting self-adjoint partial differential operators and a group-theoretic problem, J. Funct. Anal. 16 (1974) 101–121.
[7] G. Kiss, R.D. Malikiosis, G. Somlai, M. Vizer, On the discrete Fuglede and Pompeiu problems, Analysis & PDE 13 (2020) 765–788.
[8] G. Kiss, R.D. Malikiosis, G. Somlai, M. Vizer, Fuglede's conjecture holds for cyclic groups of order $pqrs$, J. Fourier Anal. Appl. 28 (2022), Article # 79.
[9] I. Łaba, I. Londner, Combinatorial and harmonic-analytic methods for integer tilings, Forum of Mathematics - Pi 10 (e8) (2022) 1–46.
[10] I. Łaba, I. Londner, The Coven-Meyerowitz tiling conditions for 3 odd prime factors, Invent. Math. 232 (1) (2023) 365–470.
[11] I. Łaba, I. Londner, The Coven-Meyerowitz tiling conditions for 3 prime factors: the even case, Res. Math. Sci. 12 (2025) 1–56, Article no. 43.
[12] I. Łaba, I. Londner, Splitting for integer tilings, IMRN 2025 (8) (2025) 1–21.
[13] I. Łaba, C. Marshall, Vanishing sums of roots of unity and the Favard length of self-similar product sets, Discrete Analysis (2022) 19.
[14] T.Y. Lam, K.H. Leung, On vanishing sums of roots of unity, J. Algebra 224 (2000) 91–109.
[15] R.D. Malikiosis, On the structure of spectral and tiling subsets of cyclic groups, Forum Math. Sigma 10 (e23) (2022) 1–42.
[16] H.B. Mann, On Linear Relations Between Roots of Unity, Mathematika 12 (2) (1965) 107–117.
[17] D.J. Newman, Tesselation of integers, J. Number Theory 9 (1977) 107–111.
[18] B. Poonen, M. Rubinstein, Number of Intersection Points Made by the Diagonals of a Regular Polygon, SIAM J. Disc. Math. 11 (1998) 135–156.
[19] L. Rédei, Über das Kreisteilungspolynom, Acta Math. Hungar. 5 (1954) 27–28.
[20] L. Rédei, Natürliche Basen des Kreisteilungskörpers, Abh. Math. Sem. Univ. Hamburg 23 (1959) 180–200.
[21] A. Sands, On Keller's conjecture for certain cyclic groups, Proc. Edinb. Math. Soc. 2 (1979) 17–21.

[22] I.J. Schoenberg, A note on the cyclotomic polynomial, Mathematika 11 (1964) 131–136.
[23] R. Shi, Fuglede's conjecture holds on cyclic groups $\mathbb{Z}_{pqr}$, Discrete Analysis (2019) 14.
[24] J.P. Steinberger, Minimal vanishing sums of roots of unity with large coefficients, Proc. London Math. Soc. 97 (3) (2008) 689–717.
[25] S. Szabó, A type of factorization of finite abelian groups, Discrete Math. 54 (1985) 121–124.
[26] T. Tao, Some notes on the Coven-Meyerowitz conjecture, blog post available at, https://terrytao.wordpress.com/2011/11/19/some-notes-on-the-coven-meyerowitz-conjecture/.
[27] F. Winkler, Polynomial Algorithms in Computer Science, Springer, Vienna, 1996.