CAMBRIDGE
UNIVERSITY PRESS

CrossMark

RESEARCH ARTICLE

Combinatorial and harmonic-analytic methods for integer tilings

Izabella Łaba [1] and Itay Londner [2,3]

[1]Department of Mathematics, University of British Columbia, 1984 Mathematics Rd., Vancouver, BC V6T1Z2, Canada;
E-mail: ilaba@math.ubc.ca.
[2]Department of Mathematics, University of British Columbia, 1984 Mathematics Rd., Vancouver, BC V6T1Z2, Canada;
E-mail: itayl@math.ubc.ca.
[3]Current address: Department of Mathematics, Faculty of Mathematics and Computer Science, Weizmann Institute of Science, 234 Herzl Street, Rehovot, 7610001, Israel; E-mail: itay.londner@weizmann.ac.il.

Abstract

A finite set of integers A tiles the integers by translations if $\mathbb{Z}$ can be covered by pairwise disjoint translated copies of A. Restricting attention to one tiling period, we have $A \oplus B = \mathbb{Z}_M$ for some $M \in \mathbb{N}$ and $B \subset \mathbb{Z}$. This can also be stated in terms of cyclotomic divisibility of the mask polynomials $A(X)$ and $B(X)$ associated with A and B.

In this article, we introduce a new approach to a systematic study of such tilings. Our main new tools are the box product, multiscale cuboids and saturating sets, developed through a combination of harmonic-analytic and combinatorial methods. We provide new criteria for tiling and cyclotomic divisibility in terms of these concepts. As an application, we can determine whether a set A containing certain configurations can tile a cyclic group $\mathbb{Z}_M$, or recover a tiling set based on partial information about it. We also develop tiling reductions where a given tiling can be replaced by one or more tilings with a simpler structure. The tools introduced here are crucial in our proof in [24] that all tilings of period $(pqr)^2$, where p, q, r are distinct odd primes, satisfy a tiling condition proposed by Coven and Meyerowitz [2].

Contents

1. Introduction

A set $A \subset \mathbb{Z}$ *tiles the integers by translations* if $\mathbb{Z}$ can be covered by pairwise disjoint translates of A. Equivalently, there exists a set $T \subset \mathbb{Z}$ (the set of translations) such that every integer $n \in \mathbb{Z}$ can be represented uniquely as $n = a + t$ with $a \in A$ and $t \in T$. Throughout this article, we assume that A is finite and nonempty, and call it a *finite tile* if it tiles the integers. Newman [34] proved that any tiling of $\mathbb{Z}$ by a finite set A must be periodic – that is, $T = B \oplus M\mathbb{Z}$ for some finite set $B \subset \mathbb{Z}$ such that $|A||B| = M$. Equivalently, $A \oplus B$ is a factorisation of the cyclic group $\mathbb{Z}_M$, with B as the *tiling complement*.

We are interested in investigating the properties of finite tiles. While this is a natural and attractive question, surprisingly little is known on this subject.

Newman's proof provides a bound on the tiling period, $M \leq 2^{\max(A)-\min(A)}$. Thus, given a finite set $A \subset \mathbb{Z}$, the question of whether A is a tile is at least in principle computationally decidable. However, Newman's bound is exponential in diameter, and can therefore be very large even if A has only a few elements. A more effective bound was proved recently by Greenfeld and Tao [13].

Further important reductions and observations were made by Sands [37], Tijdeman [47] and Coven and Meyerowitz [2]. Sands' theorem on replacement of factors [37] states that if $A \oplus B = \mathbb{Z}_M$ and M has at most two distinct prime divisors, then at least one of A and B must be contained in a proper subgroup of $\mathbb{Z}_M$. The proof of this is based on a characterisation of tiling pairs, also due to Sands, which we state here as Theorem 2.5. Tijdeman [47] proved that if a finite set A tiles the integers, and if $r \in \mathbb{N}$ is relatively prime to $|A|$, then $rA := \{ra : a \in A\}$ also tiles $\mathbb{Z}$ with the same tiling complement. Coven and Meyerowitz [2, Lemma 2.3] used this to prove that if a finite set A tiles the integers, then it also tiles $\mathbb{Z}_M$ for some M which has the same prime factors as $|A|$.

For the last two decades, the state-of-the-art work on the subject was due to Coven and Meyerowitz [2]. In order to describe their main result, we need to introduce some notation, which we will also use throughout this article. By translational invariance, we may assume that $A, B \subset \{0, 1, \dots\}$ and that $0 \in A \cap B$. The *characteristic polynomials* (also known as *mask polynomials*) of A and B are

$$A(X) = \sum_{a \in A} X^a, \qquad B(X) = \sum_{b \in B} X^b.$$

Then $A \oplus B = \mathbb{Z}_M$ is equivalent to

$$A(X)B(X) = 1 + X + \cdots + X^{M-1} \bmod \left(X^M - 1\right). \tag{1.1}$$

Let $\Phi_s(X)$ be the sth cyclotomic polynomial – that is, the unique monic, irreducible polynomial whose roots are the primitive sth roots of unity. Alternatively, Φ_s can be defined inductively via the identity

$$X^n - 1 = \prod_{s \mid n} \Phi_s(X). \tag{1.2}$$

In particular, equation (1.1) is equivalent to

$$|A||B| = M \text{ and } \Phi_s(X) \mid A(X)B(X) \text{ for all } s \mid M, \quad s \neq 1. \tag{1.3}$$

Since Φ_s are irreducible, each $\Phi_s(X)$ with $s \mid M$ must divide at least one of $A(X)$ and $B(X)$.

Coven and Meyerowitz [2] proved the following theorem:

Theorem 1.1 ([2]). *Let S_A be the set of prime powers p^α such that $\Phi_{p^\alpha}(X)$ divides $A(X)$. Consider the following conditions:*

(T1) $A(1) = \prod_{s \in S_A} \Phi_s(1)$.
(T2) *If $s_1, \ldots, s_k \in S_A$ are powers of different primes, then $\Phi_{s_1 \cdots s_k}(X)$ divides $A(X)$.*

Then we have the following:

○ *If A satisfies (T1) and (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.*

Condition (T1) is, essentially, a counting condition, and is relatively easy to prove. For sets $A \subset \mathbb{Z}$ such that $|A|$ is a prime power, (T1) is a necessary and sufficient condition for A to be a tile [34]. (In this case, (T2) is vacuous.)

Condition (T2) is much deeper. Coven and Meyerowitz [2] proved that if (T2) holds, then $A \oplus B^\flat = \mathbb{Z}_M$ is a tiling, where $M = \operatorname{lcm}(S_A)$ and $B^\flat$ is an explicitly constructed and highly structured 'standard' tiling complement depending only on the prime-power cyclotomic divisors of $A(X)$. We prove in Section 3 that having a tiling complement of this type is in fact equivalent to (T2). While this equivalence was not stated explicitly in [2], it follows readily from the methods developed there.

The Coven–Meyerowitz proof of (T2) for all finite tiles with two distinct prime factors relies on the aforementioned structure and replacement theorems of Sands [37] and Tijdeman [47]. In [2, Lemma 2.3], the authors deduce from Tijdeman's theorem that if A tiles the integers and $|A|$ has at most two distinct prime factors, then A admits a tiling $A \oplus B = \mathbb{Z}_M$, where M has at most two distinct prime factors. By Sands' theorem, one of A and B must then be contained in a proper subgroup of $\mathbb{Z}_M$. Coven and Meyerowitz use this to set up an inductive argument.

A closer analysis of the Coven–Meyerowitz argument yields the same result in the case when $M = p_1^{n_1} \cdots p_K^{n_K}$, where $p_1, \ldots, p_K$ are distinct primes, $n_1, \ldots, n_K \in \mathbb{N}$ are arbitrary and at most two of $p_1, \ldots, p_K$ divide both $|A|$ and $|B|$. Essentially, any such case can be reduced to the two-prime case via Tijdeman's theorem and [2, Lemma 2.3], whereupon Theorem 1.1 may be applied. We provide the details in Corollary 6.2. (See also [4, 39, 46].)

The goal of the present article is to develop methods that can be used in the study of tilings $A \oplus B = \mathbb{Z}_M$, where M is permitted to have three or more prime factors dividing both $|A|$ and $|B|$. Sands' factorisation theorem does not hold in this case, with counterexamples in [25, 43]. For the same reason, the Coven–Meyerowitz proof does not extend to such tilings. We emphasise that this is not just a technical issue. Tilings with three or more distinct prime factors dividing both $|A|$ and $|B|$ are genuinely different, and

any comprehensive analysis of them must account for new phenomena that have no counterparts for two prime factors, such as Szabó's examples [43].

The simplest tilings that cannot be reduced to the two-prime case using the methods of [2] are of the form $A \oplus B = \mathbb{Z}_M$, where $|A| = |B| = p_1 p_2 p_3$ and p_1, p_2, p_3 are distinct primes. In our follow-up paper [24], we use the methods developed here to resolve this case when p_1, p_2, p_3 are odd.

Theorem 1.2 ([24]). *Let* $M = p_i^2 p_j^2 p_k^2$, *where* p_i, p_j, p_k *are distinct odd primes. Assume that* $A \oplus B = \mathbb{Z}_M$, *with* $|A| = |B| = p_i p_j p_k$. *Then both A and B satisfy* (T2).

While our complete proof of Theorem 1.2 works only under the assumptions indicated, many of our tools, methods and intermediate results apply to general tilings $A \oplus B = \mathbb{Z}_M$, raising the possibility of further extensions and improvements. We therefore chose to present them here in more generality, deferring the actual proof of Theorem 1.2 to [24], which is restricted to the three-prime setting.

We begin with the notation and preliminaries in Section 2. We identify $\mathbb{Z}_M = \mathbb{Z}_{p_1^{n_1} \cdots p_K^{n_K}}$ with $\mathbb{Z}_{p_1^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{p_K^{n_K}}$, and use the induced coordinate system to identify the given tiling with a tiling of a multidimensional lattice. This allows a geometric viewpoint, whereby we can describe the tiling in terms of objects such as lines, planes or fibers (arithmetic progressions of maximal length on certain scales). We emphasise, however, that the problem under consideration is much more specific than the study of tilings of multidimensional lattices in general. It is important in our work that the different coordinate directions correspond to distinct primes.

In Section 3, we present an alternative formulation of (T2) in terms of *standard tiling complements*. Roughly speaking, if $A \oplus B = \mathbb{Z}_M$ is a tiling, then B satisfies (T2) if and only if its tiling complement A can be replaced by a highly structured 'standard set' $A^\flat$ with the same prime-power cyclotomic divisors as A. Such standard sets were already used in [2] to prove that (T1) and (T2) imply tiling. Here, we state the formal implication in the other direction. In this formulation, condition (T2) can be viewed as a distant cousin of questions on replacement of factors in factorisation of finite abelian groups (see [44] for an overview).

In Section 4, we introduce one of our main tools, the *box product*. The idea comes from an unpublished paper [11], and our main harmonic-analytic identity, Theorem 4.7, is in fact a reprise of [11, Theorem 1] with relatively minor modifications. We are, however, able to use it much more effectively. (We caution the reader that, while [11, Theorem 1] is correct, the proof of the main tiling result in [11] contains an error that cannot be readily fixed with the methods of that paper.)

Our goal is to be able to start with an arbitrary tiling $A \oplus B = \mathbb{Z}_M$, and prove that either at least one of the sets A or B can be replaced directly by the corresponding standard tiling complement (which proves (T2), as already indicated) or else we can pass to tilings with a smaller period $N \mid M$ and apply an inductive argument. The machinery to do this is developed in Sections 5–8, and includes the following main ingredients.

Cuboids (Section 5) and fibering (Section 8) are our main tools in determining cyclotomic divisibility and proving structural properties. Cuboids have been used previously in the literature in the context of vanishing sums of roots of unity [42] and Fuglede's spectral set conjecture [16]. We often have to use both cuboids and fibering at several scales at the same time. In particular, we introduce 'multiscale' cuboids that correspond to divisibility by combinations of several cyclotomic polynomials.

In Section 6, we discuss two reductions that allow us to pass to tilings with a smaller period, with the (T2) property preserved under the decomposition. We first review the subgroup reduction from [2]. Then we introduce a 'slab reduction', which we believe to be new and which covers many cases of interest that are not covered by the subgroup reduction. We also develop a criterion for this reduction to apply. A concrete example of this is provided in Corollary 6.8.

While the subgroup reduction is sufficient to prove Theorem 1.1, tilings with three or more distinct prime factors include cases where such inductive arguments do not appear to be easily applicable. One well-known obstruction to an inductive approach is provided by Szabó-type examples [43]. However, Szabó's examples are known to satisfy (T2). This was observed already by Coven and Meyerowitz [2]; see also [4] for an explicit analysis of a class of examples based on Szabó's idea.

We do not know whether Szabó-type constructions are the only obstacle to an inductive proof of (T2) for all finite tiles. In [24], we prove that this is indeed true for classes of tilings that are broad enough to include all tilings of $\mathbb{Z}_M$ with $M = (p_1 p_2 p_3)^2$. The key new concept turns out to be *saturating sets* – subsets of A and B that saturate appropriately chosen box products (Section 7). Informally, if a tile A contains geometric configurations that indicate a lack of structure on a certain scale, we are able to use it to our advantage and locate highly structured configurations elsewhere in both A and B. In particular, the less structure we have in one of the tiles, the more structured the other one is expected to be. In the case $M = (p_1 p_2 p_3)^2$, we use this to prove that all tilings with 'unfibered grids' (see [24] for the definition) must in fact come from Szabó-type constructions. With this established, we can prove (T2) for such tilings by reduction to standard tiling complements. The full argument is carried out in [24], but we also provide examples of this procedure here in Section 8.5.

In addition to applications to proving structural conditions such as (T2), we are able to use saturating sets to identify sets $A \subset \mathbb{Z}_M$ that do *not* tile $\mathbb{Z}_M$ based on the presence of certain configurations. Results of this type include Lemma 7.10 and Proposition 7.11.

In Section 9 we discuss open questions and possible directions of study arising from our research so far.

Since the work of Coven and Meyerowitz, there has been essentially no progress in proving (T2), except for a few special cases of limited importance (such as [22]) and cases covered by Corollary 6.2 [4, 39, 46]. However, there have been significant recent developments on other questions related to tiling and cyclotomic divisibility. Notably, Bhattacharya [1] has established the periodic tiling conjecture in $\mathbb{Z}^2$, with a quantitative version due to Greenfeld and Tao [13]. In a continuous setting, there has been recent work on tilings of the real line by a function [19].

There is an important connection between the Coven–Meyerowitz tiling conditions and Fuglede's spectral set conjecture [10]. The conjecture, dating back to the 1970s, 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. A set with the latter property is called a *spectral set*. While the question originated in functional analysis, it has intriguing connections to many other areas of mathematics, from convex geometry to wavelets, oscillatory integral estimates and number theory. The conjecture is now known to be false in dimensions 3 and higher [8, 9, 20, 21, 33, 45]. Nonetheless, many important cases remain open and continue to attract attention. Iosevich, Katz and Tao [14] proved in 2003 that Fuglede's conjecture holds for convex sets in $\mathbb{R}^2$; an analogous result in higher dimensions was proved only recently, by Greenfeld and Lev [12] for $n = 3$ and by Lev and Matolcsi [29] for general n. There has also been extensive work on the finite abelian group analogue of the conjecture [7, 6, 15, 16, 17, 18, 30, 31, 39, 40, 41, 48].

Combined with a sequence of results in [23, 26, 27], proving (T2) for all finite integer tiles would resolve the 'tiling implies spectrum' part of Fuglede's spectral set conjecture for all compact tiles of the real line in dimension 1. Additionally, Dutkay and Lai [5] proved that if a similar property could be established for spectral sets, this would also resolve the converse part of the conjecture for compact sets in $\mathbb{R}$. While proving (T2) for a more narrow class of integer tiles does not have that implication, it still establishes one direction of Fuglede's conjecture for that class of tiles in the finite group setting, as well as for sets $E = \bigcup_{a \in A} [a, a + 1] \subset \mathbb{R}$, where $A \subset \mathbb{Z}$ is an integer tile in the permitted class [23].

2. Notation and preliminaries

2.1. Multisets and mask polynomials

Let $M \geq 2$ be a fixed integer. Usually, we will work in either $\mathbb{Z}_M$ or $\mathbb{Z}_N$ for some $N \mid M$. In the context of the tiling problem, we reserve M for the tiling period and N for its divisors. We also reserve K for the number of the distinct prime divisors of M, and use $p_1, \ldots, p_K$ to denote those divisors, so that

$$M = \prod_{i=1}^{K} p_i^{n_i},$$

where $p_1, \ldots, p_K$ are distinct primes and $n_1, \ldots, n_K \in \mathbb{N}$. We fix this notation and use it throughout the rest of the article. For a prime p, an integer m and a nonnegative integer α, we will say that $p^\alpha \parallel m$ if $p^\alpha \mid m$ but $p^{\alpha+1} \nmid m$.

We use $A(X)$, $B(X)$, etc., to denote polynomials modulo $X^M - 1$ with integer coefficients. If $A(X)$ is such a polynomial, we define its weight function $w_A : \mathbb{Z}_M \to \mathbb{Z}$ so that $w_A(a)$ is the coefficient of X^a in $A(X)$. Thus $A(X) = \sum_{a \in \mathbb{Z}_M} w_A(a) X^a$. If A has 0 or 1 coefficients, then w_A is the characteristic function of a set $A \subset \mathbb{Z}_M$. However, we will also consider polynomials with integer coefficients not necessarily equal to 0 or 1. In that case, $A(X)$ will correspond to a weighted multiset in $\mathbb{Z}_M$, which we will also denote by A, with weights $w_A(a)$ assigned to each $a \in \mathbb{Z}_M$. We will use $\mathcal{M}(\mathbb{Z}_M)$ to denote the family of all such weighted multisets in $\mathbb{Z}_M$, and reserve the notation $A \subset \mathbb{Z}_M$ for sets (with 0 and 1 weights). If $A \in \mathcal{M}(\mathbb{Z}_M)$, the polynomial $A(X)$ is sometimes called the *mask polynomial* of A. It will usually be clear from the context whether A refers to the weighted multiset or the corresponding polynomial; whenever there is any possibility of confusion, we will use A for the multiset and $A(X)$ for the polynomial.

If $N \mid M$, then any $A \in \mathcal{M}(\mathbb{Z}_M)$ induces a weighted multiset $A \bmod N$ in $\mathbb{Z}_N$, with the corresponding mask polynomial $A(X) \bmod (X^N - 1)$, and induced weights

$$w_A^N(x) = \sum_{x' \in \mathbb{Z}_M : x' \equiv x \bmod N} w_A(x'), \qquad x \in \mathbb{Z}_N. \tag{2.1}$$

For brevity, we will continue to write A and $A(X)$ for $A \bmod N$ and $A(X) \bmod (X^N - 1)$, respectively, while working in $\mathbb{Z}_N$.

If $A, B \in \mathcal{M}(\mathbb{Z}_M)$, we will use $A + B$ to indicate the weighted multiset corresponding to the sum of mask polynomials, or, equivalently, the sum of weight functions:

$$w_{A+B}(x) = w_A(x) + w_B(x), \qquad (A + B)(X) = A(X) + B(X).$$

We will use the convolution notation $A * B$ to denote the weighted sumset of A and B, so that $(A * B)(X) = A(X)B(X)$ and

$$w_{A*B}(x) = (w_A * w_B)(x) = \sum_{y \in \mathbb{Z}_M} w_A(x - y) w_B(y).$$

If one of the sets is a singleton, say $A = \{x\}$, we will simplify the notation and write $x * B = \{x\} * B$. The direct sum notation $A \oplus B$ is reserved for tilings – that is, $A \oplus B = \mathbb{Z}_M$ means that $A, B \subset \mathbb{Z}_M$ are both sets and $A(X)B(X) = \frac{X^M - 1}{X - 1} \bmod (X^M - 1)$.

Since we will not need to use derivatives of polynomials in this article, we will use notation such as A', A'', etc., to denote multisets and polynomials that need not have anything to do with the derivatives $\frac{d}{dX} A(X)$, $\frac{d^2}{dX^2} A(X)$ and so on.

2.2. Array coordinates

Suppose that $M = \prod_{i=1}^K p_i^{n_i}$, where $p_1, \ldots, p_K$ are distinct primes and $n_i \in \mathbb{N}$. By the Chinese remainder theorem, we have

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

which we represent geometrically as a K-dimensional lattice. The tiling $A \oplus B = \mathbb{Z}_M$ can then be interpreted as a tiling of that lattice.

It will be useful to have an explicit coordinate system on $\mathbb{Z}_M$. We fix one as follows. Let $M_i = M/p_i^{n_i} = \prod_{j \neq i} p_j^{n_j}$; then each $x \in \mathbb{Z}_M$ can be written uniquely as

$$x = \sum_{i=1}^{K} \pi_i(x) M_i, \quad \pi_i(x) \in \mathbb{Z}_{p_i^{n_i}}.$$

The mapping $x \to (\pi_1(x), \ldots, \pi_k(x))$ identifies x with an element of $\mathbb{Z}_{p_1^{n_1}} \times \cdots \times \mathbb{Z}_{p_K^{n_K}}$. We will refer to the K-tuple $(\pi_1(x), \ldots, \pi_K(x))$ as the *M-array coordinates* of x.

We state a few easy properties for future reference.

Lemma 2.1.

(i) $x \equiv \pi_i(x) M_i \bmod p_i^{n_i}$.

(ii) $(x, M) = \prod_{i=1}^{K} p_i^{\gamma_i}$ *if and only if* $p_i^{\gamma_i} \parallel \pi_i(x)$ *for each* $i = 1, \ldots, K$.

(iii) *In particular,* $x = 0$ *in* $\mathbb{Z}_M$ *if and only if* $\pi_i(x) = 0$ *for each* $i = 1, \ldots, K$.

(iv) *If* $x = \sum \pi_i(x) M_i$, $y = \sum \pi_i(y) M_i$ *and* $x + y = z = \sum \pi_i(z) M_i$ *are the respective coordinate representations, then* $\pi_i(z) \equiv \pi_i(x) + \pi_i(y) \bmod p_i^{n_i}$ *for each* $i = 1, \ldots, k$.

Each coordinate $\pi_i(x)$ of $x \in \mathbb{Z}_M$ can be subdivided further into digits as follows. With $\mathbb{Z}_{p_i^{n_i}}$ represented as $\{0, 1, \ldots, p_i^{n_i} - 1\}$ with addition and multiplication modulo $p_i^{n_i}$, we can write uniquely

$$\pi_i(x) = \sum_{j=0}^{n_i - 1} \pi_{i,j}(x) p_i^j, \quad \pi_{i,j}(x) \in \{0, 1, \ldots, p_i - 1\}.$$

Observe that $(x - x', M) = \prod_{j=1}^{K} p_i^{\gamma_i}$ if and only if for each $i = 1, \ldots, K$,

$$\gamma_i = \begin{cases} \min \{j : \pi_{i,j}(x) \neq \pi_{i,j}(x')\} & \text{if } \pi_i(x) \neq \pi_i(x'), \\ n_i & \text{if } \pi_i(x) = \pi_i(x'). \end{cases} \tag{2.2}$$

2.3. Grids, planes, lines, fibers

Definition 2.2. Let $D \mid M$. A *D-grid* in $\mathbb{Z}_M$ is a set of the form

$$\Lambda(x, D) := x + D\mathbb{Z}_M = \{x' \in \mathbb{Z}_M : D \mid (x - x')\}$$

for some $x \in \mathbb{Z}_M$.

An important case of interest is as follows. Let $N \mid M$. If $N = p_1^{\alpha_1} \cdots p_K^{\alpha_K}$, with $\alpha_1, \ldots, \alpha_K \geq 0$, we define

$$D(N) := p_1^{\gamma_1} \cdots p_K^{\gamma_K},$$

where $\gamma_i = \max(0, \alpha_i - 1)$ for $i = 1, \ldots, K$. Then a $D(N)$-grid is a 'top-level' grid on the scale N, and a natural setting to work on that scale.

While a grid Λ is always an arithmetic progression in $\mathbb{Z}_M$, it is often helpful to represent $\mathbb{Z}_M$ by a K-dimensional coordinate array as in Section 2.2 and, accordingly, assign a geometric interpretation to Λ. We point out several useful special cases.

A *line* through $x \in \mathbb{Z}_M$ in the p_i direction is the set

$$\ell_i(x) := \Lambda(x, M_i),$$

and a $(K-1)$-*dimensional plane* through $x \in \mathbb{Z}_M$ perpendicular to the p_i direction is a set of the form

$$\Pi\left(x, p_i^{\alpha_i}\right) := \Lambda\left(x, p_i^{\alpha_i}\right). \tag{2.3}$$

Note that formula (2.3) defines a plane on the scale $M_i p_i^{\alpha_i}$, which may be different from M.

An *M-fiber in the p_i direction* is a set of the form $x * F_i$, where $x \in \mathbb{Z}_M$ and

$$F_i = \{0, M/p_i, 2M/p_i, \ldots, (p_i - 1)M/p_i\}. \tag{2.4}$$

Thus $x * F_i = \Lambda(x, M/p_i)$. (More complicated multiscale fiber chains will be defined later.) A set $A \subset \mathbb{Z}_M$ is *M-fibered in the p_i direction* if there is a subset $A' \subset A$ such that $A = A' * F_i$.

2.4. Cyclotomic polynomials and cyclotomic divisibility

We state a few basic facts about cyclotomic polynomials for future reference. By equation (1.2), we have

$$1 + X + X^2 + \cdots + X^{n-1} = \prod_{s|n, s \neq 1} \Phi_s(X). \tag{2.5}$$

In particular, if p is a prime number, then $\Phi_p(X) = 1 + X + \cdots + X^{p-1}$ and, more generally, by induction,

$$\Phi_{p^\alpha}(X) = \Phi_p\left(X^{p^{\alpha-1}}\right) = 1 + X^{p^{\alpha-1}} + X^{2p^{\alpha-1}} + \cdots + X^{(p-1)p^{\alpha-1}}, \quad \alpha \geq 1.$$

Thus $\Phi_{p^\alpha}(1) = p$, and this together with equation (2.5) implies that $\Phi_s(1) = 1$ for all s that are not prime powers.

Suppose that $A \oplus B = \mathbb{Z}_M$, with $M = \prod_{i=1}^K p_i^{n_i}$ as before. By equation (1.1), we have $A(X)B(X) = 1 + X + \cdots + X^{M-1} \bmod \left(X^M - 1\right)$. For every prime power $s = p^\alpha \mid M$, we must have $\Phi_s(X) \mid A(X)B(X)$, so that

$$M = \prod_{i=1}^K \prod_{\alpha_i=1}^{n_i} \Phi_{p_i^{\alpha_i}}(1) \mid A(1)B(1) = |A||B| = M.$$

It follows that

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

and similarly for B, with S_A, S_B defined as in Theorem 1.1; this is the proof of the tiling condition (T1) given in [2]. Moreover, for any prime power $s = p^{\alpha_i} \mid M$, we have that $\Phi_s(X)$ divides exactly one of $A(X)$ and $B(X)$. (This is not true for $s \mid M$ with two or more distinct prime factors. For such s, the corresponding cyclotomic polynomial $\Phi_s(X)$ may divide either one or both of $A(X)$ and $B(X)$.)

Divisibility by prime-power cyclotomics has the following combinatorial interpretation. For $A \subset \mathbb{Z}_M$, the condition $\Phi_{p_i} \mid A$ means that the elements of A are uniformly distributed modulo p_i, so that

$$|A \cap \Pi(x, p_i)| = |A|/p_i \quad \forall x \in \mathbb{Z}_M.$$

More generally, for $1 \leq \alpha \leq n_i$, we have $\Phi_{p_i^\alpha}(X) \mid A(X)$ if and only if

$$\left|A \cap \Pi\left(x, p_i^\alpha\right)\right| = \frac{1}{p_i}\left|A \cap \Pi\left(x, p_i^{\alpha-1}\right)\right| \quad \forall x \in \mathbb{Z}_M, \tag{2.6}$$

so that the elements of A are uniformly distributed mod p_i^α within each residue class mod $p_i^{\alpha-1}$. In particular, this implies the following bound on the number of points of a tile in a plane on a scale $M_i p_i^{n_i - \alpha_i}$ or, equivalently, in an arithmetic progression of step $p_i^{n_i - \alpha_i}$:

Lemma 2.3 (Plane bound). *Let $A \oplus B = \mathbb{Z}_M$, where $M = \prod_j p_j^{n_j}$ and $|A| = \prod_j p_j^{\beta_j}$. Then for every $x \in \mathbb{Z}_M$ and $0 \le \alpha_i \le n_i$ we have*

$$\left| A \cap \Pi \left(x, p_i^{n_i - \alpha_i} \right) \right| \le p_i^{\alpha_i} \prod_{\nu \ne i} p_\nu^{\beta_\nu}. \tag{2.7}$$

This bound is, in general, sharp. For example, if $A \subset p_i^{n_i - 1} \mathbb{Z}_M$ and $\Phi_{p_i^{n_i}} \mid A$, then $\left| A \cap \Pi \left(x, p_i^{n_i} \right) \right| = |A|/p_i$, so that estimate (2.7) holds with equality for $\alpha_i = 0$. Examples of sets $A \subset \mathbb{Z}_M$ with the foregoing properties are easy to construct using the standard tiling sets defined in Section 3.

We also note the following. Let $N \mid M$. Then the condition

$$\Phi_s \mid A \quad \forall s \mid N, s \ne 1,$$

means that $1 + X + \cdots + X^{N-1}$ divides $A(X)$ or, equivalently, that the elements of A are uniformly distributed mod N. For example, let $N = p_1 p_2 \cdots p_K$. Suppose that $|A| = N$ and that $\Phi_{p_i} \mid A$ for all $i = 1, \ldots, K$. Then A satisfies (T2) if and only if $\Phi_s \mid A$ for all $s \mid N$ with $s \ne 1$ or, equivalently, if and only if each residue class mod N contains exactly one element of A.

2.5. *Divisor set and divisor exclusion*

Definition 2.4 (Divisor set). For a set $A \subset \mathbb{Z}_M$, define

$$\mathrm{Div}(A) = \mathrm{Div}_M(A) := \{(a - a', M) : a, a' \in A\}. \tag{2.8}$$

Informally, we will refer to the elements of $\mathrm{Div}(A)$ as the *divisors of A* or *differences in A*. We also define

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

for $A \subset \mathbb{Z}_M$ and $N \mid M$.

Divisor sets will be a key concept in our analysis, thanks to the following theorem due to Sands [37]:

Theorem 2.5 (Divisor exclusion [37]). *If $A, B \subset \mathbb{Z}_M$ are sets, then $A \oplus B = \mathbb{Z}_M$ if and only if $|A||B| = M$ and*

$$\mathrm{Div}(A) \cap \mathrm{Div}(B) = \{M\}. \tag{2.9}$$

An alternative proof of Sands' theorem, based on Theorem 4.7 and due to [11], is included in Remark 4.10.

3. A reformulation of (T2)

3.1. *Standard tiling complements*

We continue to assume that $M = \prod_{i=1}^K p_i^{n_i}$, where $p_1, \ldots, p_K$ are distinct primes and $n_i > 0$. We equip $\mathbb{Z}_M$ with the array coordinate system from Section 2.2 and use the notation of that section. Recall also that the divisor set $\mathrm{Div}(A)$ for a set $A \subset \mathbb{Z}_M$ was defined in definition (2.8) which is a little bit circular.

Definition 3.1. Let A, B be sets in $\mathbb{Z}_M$ such that $A \oplus B = \mathbb{Z}_M$. Let

$$\mathfrak{A}_i(A) = \left\{ \alpha_i \in \{1, 2, \ldots, n_i\} : \Phi_{p_i^{\alpha_i}}(X) \mid A(X) \right\}.$$

The *standard tiling set* $A^\flat$ is defined via its mask polynomial

$$
\begin{aligned}
A^\flat(X) &= \prod_{i=1}^{K} \prod_{\alpha_i \in \mathfrak{A}_i(A)} \Phi_{p_i}\left(X^{M_i p_i^{\alpha_i-1}}\right) \\
&= \prod_{i=1}^{K} \prod_{\alpha_i \in \mathfrak{A}_i(A)} \left(1 + X^{M_i p_i^{\alpha_i-1}} + \cdots + X^{(p_i-1)M_i p_i^{\alpha_i-1}}\right).
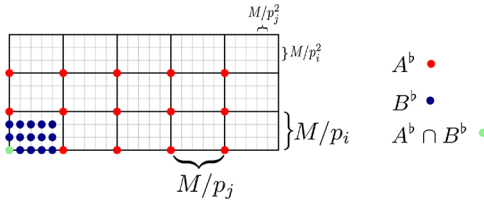\end{aligned}
\tag{3.1}
$$

Figure 1. *The standard sets $A^\flat, B^\flat \subset \mathbb{Z}_{p_i^2 p_j^2}$ with $p_i = 3$, $p_j = 5$ and $\Phi_{p_i^2}\Phi_{p_j^2} \mid A$, $\Phi_{p_i}\Phi_{p_j} \mid B$.*

Lemma 3.2. *Define $A^\flat$ as before. Then $A^\flat(X)$ satisfies (T2) and has the same prime-power cyclotomic divisors as $A(X)$.*

Proof. Set $\alpha \in \{1, 2, \ldots, n_i\}$. Then $\Phi_{p_i^\alpha}(X) \mid A^\flat(X)$ if and only if it divides one of the factors $\Phi_{p_i}(X^{M_i p_i^{\alpha_i-1}})$ with $\alpha_i \in \mathfrak{A}_i(A)$. By Lemma 3.3, this happens if and only if $\alpha = \alpha_i$. Furthermore, in that case we also have $\Phi_{dp_i^{\alpha_i}}(X) \mid A^\flat(X)$ for all $d \mid M_i$, so that in particular (T2) holds for $A^\flat$. $\qquad \square$

Lemma 3.3. *Let*

$$
\Psi(X) = 1 + X^{Np^{\alpha-1}} + X^{2Np^{\alpha-1}} + \cdots + X^{(p-1)Np^{\alpha-1}} = \Phi_p\left(X^{Np^{\alpha-1}}\right),
$$

where $(N, p) = 1$. Then $\Phi_s(X) \mid \Psi(X)$ if and only if $s = dp^\alpha$ for some $d \mid N$.

Proof. We have $\Phi_s(X) \mid \Psi(X)$ if and only if $\Psi\left(e^{2\pi i/s}\right) = 0$ – that is, $\left(e^{2\pi i/s}\right)^{Np^{\alpha-1}}$ is a root of Φ_p. This happens if and only if $\left(Np^{\alpha-1}\right)/s = k/p$ for some integer k such that $(k, p) = 1$. Equivalently, $Np^\alpha = ks$ with $(k, p) = 1$. This means that $k \mid N$ and $s = \frac{N}{k}p^\alpha = dp^\alpha$, where $d = N/k$ is a divisor of N. $\qquad \square$

Observe that the standard set $A^\flat$, while not necessarily a grid, is highly structured. In terms of array coordinates, we have

$$
\begin{aligned}
A^\flat &= \left\{ x \in \mathbb{Z}_M : \pi_i(x) = \sum_{\alpha_i \in \mathfrak{A}_i(A)} \pi_{i,\alpha_i-1}(x) p_i^{\alpha_i-1}, \quad \pi_{i,\alpha_i-1}(x) \in \{0, 1, \ldots, p_i - 1\} \right\} \\
&= \left\{ x \in \mathbb{Z}_M : \pi_{i,\alpha_i-1}(x) = 0 \text{ for all } i, \alpha_i \text{ such that } \alpha_i \notin \mathfrak{A}_i(A) \right\}.
\end{aligned}
\tag{3.2}
$$

The *standard divisor set* for A is

$$
\text{Div}\left(A^\flat\right) = \left\{ \prod_{i=1}^{K} p_i^{\alpha_i-1} : \alpha_i \in \mathfrak{A}_i(A) \cup \{n_i + 1\}, \quad i = 1, \ldots, K \right\}.
\tag{3.3}
$$

We will refer to the elements of $\text{Div}(A^\flat)$ as *standard divisors* of A. The set $B^\flat$ is defined similarly.

With these definitions, we have the following alternative formulations of (T2):

Proposition 3.4. *Suppose that $A \oplus B = \mathbb{Z}_M$. Then the following are equivalent:*

(i) $\mathrm{Div}(A^{\flat}) \cap \mathrm{Div}(B) = \{M\}$.
(ii) $A^{\flat} \oplus B = \mathbb{Z}_M$.
(iii) *B satisfies (T2).*
(iv) $\left| B \cap (x * A^{\flat}) \right| = 1$ *for every* $x \in \mathbb{Z}_M$.

Proof. The equivalence between (i) and (ii) is a special case of Theorem 2.5. The implication (iii) $\Rightarrow$ (ii) follows from the construction in the proof of [2, Theorem A]; the converse implication (ii) $\Rightarrow$ (iii) was not pointed out there, but it also follows from the same construction. Specifically, by Lemma 3.3, $A^{\flat}(X)$ is divisible by every cyclotomic polynomial Φ_s such that $p_i^{\alpha} \parallel s$ for some $i \in \{1, \ldots, K\}$ and $\alpha \geq 1$ such that $\Phi_{p_i^{\alpha}} \mid A$. In other words, the only s such that $s \mid M$ but Φ_s does not divide $A(X)$ are those with $s = \prod_{i=1}^{k} p_i^{\beta_i}$, where for each i we have either $\beta_i = 0$ or $\Phi_{p_i^{\beta_i}}(X) \mid B(X)$. Let $\mathcal{S}_B$ be the set of such s.

If B satisfies (T2), then all Φ_s with $s \in \mathcal{S}_B$ divide $B(X)$, which implies (ii). Conversely, suppose that (ii) holds. Then each Φ_s with $s \mid M$ has to divide $A(X)B(X)$. By Lemma 3.3 again, if $s \in \mathcal{S}_B$, then Φ_s does not divide $A(X)$, so it must divide $B(X)$. Therefore (T2) holds for B.

For (iv), we shall prove that (ii) implies (iv) and (iv) implies (i). Suppose that (ii) holds. We first claim that

$$\left| B \cap \left(x * A^{\flat} \right) \right| \leq 1 \quad \forall x \in \mathbb{Z}_M. \tag{3.4}$$

Indeed, if $b, b' \in B \cap (x * A^{\flat})$, then $b = x + a$ and $b' = x + a'$ for some $a, a' \in A^{\flat}$, so that $b - a = b' - a'$, contradicting (ii) unless $b = b'$ and $a = a'$.

It remains to prove that $(x_0 * A^{\flat}) \cap B \neq \emptyset$ for each $x_0 \in \mathbb{Z}_M$. Set $x_0 \in \mathbb{Z}_M$. Since $\mathrm{Div}(B) = \mathrm{Div}(-B)$, we have $A^{\flat} \oplus (-B) = \mathbb{Z}_M$ by Theorem 2.5. It follows that there must exist $a_0 \in A^{\flat}$ and $-b_0 \in (-B)$ such that $a_0 - b_0 = -x_0$. The latter means $a_0 + x_0 = b_0$, implying $(x_0 * A^{\flat}) \cap B \neq \emptyset$, as claimed. Hence (iv) follows.

Finally, suppose that (i) fails. Then there exist $b, b' \in B$ and $m \in \mathrm{Div}(A^{\flat}) \setminus \{M\}$ such that $(b - b', M) = m$. But then $b, b' \in B \cap (b * A^{\flat})$ with $b \neq b'$, contradicting (iv). $\qquad \square$

Remark 3.5. If $A \oplus B$ tiles $\mathbb{Z}_M$, where $M = p^n$ is a prime power, then (T2) holds vacuously for both sets. Hence we have both $A \oplus B^{\flat} = \mathbb{Z}_M$ and $A^{\flat} \oplus B = \mathbb{Z}_M$.

It is tempting to try to prove that if $A \oplus B = \mathbb{Z}_M$, then we should have $\mathrm{Div}(A^{\flat}) \subseteq \mathrm{Div}(A)$. By Proposition 3.4, this would imply that B satisfies (T2). However, the following example shows that $\mathrm{Div}(A)$ does not in fact have to contain $\mathrm{Div}(A^{\flat})$:

Example 3.6. Let $M = p^2 q$, where p, q are distinct primes with $p > q$, and let A be the set of numbers whose array coordinates in $\mathbb{Z}_M$ are $(i + jp, i), i = 0, 1, \ldots, q - 1, j = 0, 1, \ldots, p - 1$. Then $A \oplus B = \mathbb{Z}_M$ with $B = \{(j, 0) : j = 0, 1, \ldots, p - 1\}$, and both sets satisfy (T2). Since Φ_{p^2} and Φ_q divide $A(X)$, we have $A^{\flat} = \{(jp, i) : i = 0, 1, \ldots, q - 1, j = 0, 1, \ldots, p - 1\}$, and in particular $p \in \mathrm{Div}(A^{\flat})$. However, $p \notin \mathrm{Div}(A)$. To see this, consider $a, a' \in A$ with coordinates $(i + jp, i)$ and $(i' + j'p, i')$. If $i \neq i'$, then $(a - a', M) = 1$. If, on the other hand, $i = i'$ but $a \neq a'$, then $(a - a', M) = pq$.

This shows that the condition $\mathrm{Div}(A^{\flat}) \subseteq \mathrm{Div}(A)$ is not necessary for a tiling, nor is it simply a consequence of $A(X)$ having the requisite prime-power cyclotomic divisors. Note, however, that in this example we still have $p \notin \mathrm{Div}(B)$.

3.2. (T2)-equivalence

Definition 3.7. We say that the tilings $A \oplus B = \mathbb{Z}_M$ and $A' \oplus B = \mathbb{Z}_M$ are *(T2)-equivalent* if

$$A \text{ satisfies (T2)} \Leftrightarrow A' \text{ satisfies (T2)}. \tag{3.5}$$

Since the sets A and A' tile the same group $\mathbb{Z}_M$ with the same tiling complement B, they must have the same cardinality and the same prime-power cyclotomic divisors, as discussed in Section 2.4. For brevity, we will sometimes say simply that A is (T2)-equivalent to A' if both M and B are clear from context.

In practice, A' will be a set obtained from A using certain permitted manipulations such as fiber shifts. We will use (T2)-equivalence to reduce proving (T2) for the initial tiling to proving (T2) for related tilings that are increasingly more structured. In particular, the following reduction is sufficient to prove (T2) for both sets in the given tiling:

Corollary 3.8. *Suppose that the tiling $A \oplus B = \mathbb{Z}_M$ is (T2)-equivalent to the tiling $A^\flat \oplus B = \mathbb{Z}_M$. Then A and B satisfy (T2).*

Proof. Since $A^\flat$ satisfies (T2), A does also by equivalence (3.5). By Proposition 3.4, B satisfies (T2) as well. □

4. Box product

4.1. Box-product characterisation of tiling

We continue to assume that $M = \prod_{i=1}^{K} p_i^{n_i}$, where $p_1, \ldots, p_K$ are distinct primes. We will use ϕ and μ to denote, respectively, the Euler totient function and the Möbius function: if $n = \prod_{j=1}^{L} q_j^{r_j}$, where $q_1, \ldots, q_L$ are distinct primes, then

$$\phi(n) = n \prod_{j=1}^{L} \frac{q_j - 1}{q_j} = \prod_{j=1}^{L} (q_j - 1) q_j^{r_j - 1},$$

$$\mu(n) = \begin{cases} (-1)^L & \text{if } r_1 = r_2 = \cdots = r_L = 1, \\ 0 & \text{if } \exists j \in \{1, \ldots, L\} \text{ such that } r_j \geq 2. \end{cases}$$

Let $N \mid M$. Reordering the primes if necessary, we may assume that $N = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, with $1 \leq k \leq K$ and $\alpha_1, \ldots, \alpha_k \geq 1$.

Definition 4.1 (*N-boxes*). An *N-box* is a k-dimensional matrix

$$\mathbb{A} = \left(\mathbb{A}_{(\gamma_1, \ldots, \gamma_k)} \right)_{0 \leq \gamma_j \leq \alpha_j, j = 1, \ldots, k}$$

of size $(\alpha_1 + 1) \times \cdots \times (\alpha_k + 1)$, with entries $\mathbb{A}_{(\gamma_1, \ldots, \gamma_k)} \in \mathbb{R}$. Since each multi-index $(\gamma_1, \ldots, \gamma_k)$ with $0 \leq \gamma_j \leq \alpha_j$ can be uniquely associated with a divisor m of N given by $m = p_1^{\gamma_1} \cdots p_k^{\gamma_k}$, we will use such divisors to index the entries of $\mathbb{A}$, so that

$$\mathbb{A} = (\mathbb{A}_m)_{m \mid N}, \quad \mathbb{A}_m = \mathbb{A}_{(\gamma_1, \ldots, \gamma_k)} \text{ for } m = p_1^{\gamma_1} \cdots p_k^{\gamma_k}.$$

For any $N \mid M$, N-boxes form a vector space over $\mathbb{R}$, with addition of boxes and multiplication of a box by a scalar defined in the obvious way. We also equip this space with an inner product structure as follows:

Definition 4.2 (*Box product*). If $\mathbb{A}$ and $\mathbb{B}$ are N-boxes, define

$$\langle \mathbb{A}, \mathbb{B} \rangle = \sum_{m \mid N} \frac{1}{\phi(N/m)} \mathbb{A}_m \mathbb{B}_m. \tag{4.1}$$

Of course, this equation depends on N, but since N is determined by the fact of $\mathbb{A}$ and $\mathbb{B}$ being N-boxes, we will not use additional subscripts or superscripts to indicate that.

The N-boxes associated with multisets in $\mathbb{Z}_N$ are as follows:

Definition 4.3 (Boxes associated with multisets). Set $A \in \mathcal{M}(\mathbb{Z}_M)$ and let $N \mid M$. Consider the induced multiset $A \in \mathcal{M}(\mathbb{Z}_N)$, with the weight function mod N defined in equation (2.1). For $x \in \mathbb{Z}_N$, define $\mathbb{A}^N[x] = (\mathbb{A}_m^N[x])_{m|N}$, where

$$\mathbb{A}_m^N[x] = \sum_{a \in \mathbb{Z}_N : (x-a,N)=m} w_A^N(a).$$

In particular, if $A \subset \mathbb{Z}_N$ is a set, we have

$$\mathbb{A}_m^N[x] = \#\{a \in A : (x - a, N) = m\}.$$

If $N = M$, we will skip the superscript and write $\mathbb{A}_m[x] = \mathbb{A}_m^M[x]$ whenever there is no possibility of confusion.

Theorem 4.4 explains the reason for Definition 4.2. The theorem is based on [11, Theorem 1] (see Sections 4.2 and 4.3 for details). The equivalence between $A \oplus B = \mathbb{Z}_M$ and the condition in (ii) provides an alternative proof of Theorem 2.5; however, Sands' proof is easier and does not require Theorem 4.4. The point of Theorem 4.4 is that tiling also implies the formally stronger condition (4.2) for all $N \mid M$ and $x, y \in \mathbb{Z}_M$.

Theorem 4.4 (Box-product characterisation of tiling).

(i) *Suppose that $A \oplus B = \mathbb{Z}_M$ is a tiling. Then for any $N \mid M$ and any $x, y \in \mathbb{Z}_M$, we have*

$$\left\langle \mathbb{A}^N[x], \mathbb{B}^N[y] \right\rangle = \frac{|A||B|}{N} = \frac{M}{N}. \tag{4.2}$$

In particular,

$$\left\langle \mathbb{A}^M[x], \mathbb{B}^M[y] \right\rangle = 1 \quad \forall x, y \in \mathbb{Z}_M. \tag{4.3}$$

(ii) *Conversely, suppose that $A, B \subset \mathbb{Z}_M$ are sets such that $|A||B| = M$ and $\left\langle \mathbb{A}^M[a], \mathbb{B}^M[b] \right\rangle = 1$ for all $a \in A$ and $b \in B$. Then $A \oplus B = \mathbb{Z}_M$.*

Corollary 4.5. *Under the assumptions of Theorem 4.4, let $\mathcal{L}^N(A)$ be the linear space spanned by the boxes $\mathbb{A}^N[x]$ – that is,*

$$\mathcal{L}^N(A) = \left\{ \sum_{x \in \mathbb{Z}_N} c_x \mathbb{A}^N[x] : c_x \in \mathbb{R} \right\},$$

and similarly for B. Then for any N-boxes $\mathbb{A} \in \mathcal{L}^N(A)$ and $\mathbb{B} \in \mathcal{L}^N(B)$, we have

$$\langle \mathbb{A}, \mathbb{B} \rangle = \frac{1}{N} \Sigma(\mathbb{A}) \Sigma(\mathbb{B}), \tag{4.4}$$

where $\Sigma(\mathbb{A}) = \sum_{m|N} \mathbb{A}_m$.

N-boxes $\mathbb{A}^N[x]$, $x \in \mathbb{Z}_M$, are a convenient way of encoding structural information about A. Theorem 4.4 provides a tiling criterion for $A \oplus B = \mathbb{Z}_M$ in terms of the box product, and it is also possible to express cyclotomic divisibility in terms of N-boxes. However, this convenience comes with some loss of information. In [24], we have to work with the actual sets A and B, not just with the N-boxes representing them. We do not know whether it is possible to give a proof of properties such as (T2) purely in terms of the N-boxes associated with the sets.

Remark 4.6. The equivalence between Proposition 3.4(iii) and (iv) can be stated in terms of M-boxes. Suppose that $A \oplus B = \mathbb{Z}_M$ is a tiling. Then the following are equivalent:

 (i) B satisfies (T2).
(ii) $\sum_{m \in \mathrm{Div}(A^\flat)} \mathbb{B}_m[y] = 1$ for all $y \in \mathbb{Z}_M$.

Indeed, Proposition 3.4(iv) can be rewritten as follows: For any $y \in \mathbb{Z}_M$, there exist unique $b \in B$ and $a \in A^\flat$ such that $b = y + a$, or equivalently, $y - b = -a$. Since $\{a \in \mathbb{Z}_M : (-a, M) \in \mathrm{Div}(A^\flat)\} = A^\flat$, this implies the claim.

4.2. A Fourier-analytic identity

Fix $N = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, where $p_1, \ldots, p_k$ are distinct primes and $\alpha_1, \ldots, \alpha_k \in \mathbb{N}$. Set $A, B, C, D \in \mathcal{M}(\mathbb{Z}_N)$. For $m \mid N$, we define

$$\mathbb{A}_m^N[C] := \sum_{c \in C} \mathbb{A}_m^N[c] w_C(c) = \sum_{a,c \in \mathbb{Z}_N} w_A(a) w_C(c) \mathbf{1}_{(a-c,N)=m}.$$

In particular, if $A(X)$ is a polynomial with 0 or 1 coefficients corresponding to a set $A \subset \mathbb{Z}_N$, then

$$\mathbb{A}_m^N[A] = \#\{(a, a') \in A \times A : (a - a', N) = m\}.$$

This defines N-boxes in the sense of Definition 4.3, and in particular we may consider the box product

$$\langle \mathbb{A}^N[C], \mathbb{B}^N[D] \rangle = \sum_{m \mid N} \frac{1}{\phi(N/m)} \mathbb{A}_m^N[C] \mathbb{B}_m^N[D].$$

The following theorem is a slight generalisation of the main identity from [11]. Specifically, [11, Theorem 1] states that equation (4.6) holds when $A(X)$ and $B(X)$ are polynomials corresponding to multisets $A, B \subset \mathbb{Z}_N$. We will need an extension of it to four polynomials, not necessarily with nonnegative coefficients. The proof is essentially the same, but since [11] remains unpublished, we include it here for completeness.

Theorem 4.7. *Let $A(X), B(X), C(X), D(X)$ be polynomials modulo $X^N - 1$ with integer coefficients. Then*

$$\langle \mathbb{A}^N[C], \mathbb{B}^N[D] \rangle = \sum_{d \mid N} \frac{1}{N\phi(d)} \left[\sum_{\zeta : \Phi_d(\zeta)=0} A(\zeta)\overline{C(\zeta)} \right] \left[\sum_{\zeta : \Phi_d(\zeta)=0} B(\zeta)\overline{D(\zeta)} \right]. \tag{4.5}$$

In particular,

$$\langle \mathbb{A}^N[A], \mathbb{B}^N[B] \rangle = \sum_{d \mid N} \frac{1}{N\phi(d)} \mathcal{E}_d(A)\mathcal{E}_d(B), \tag{4.6}$$

where

$$\mathcal{E}_d(A) = \sum_{\zeta : \Phi_d(\zeta)=0} |A(\zeta)|^2.$$

The rest of this section is devoted to the proof of Theorem 4.7. We will use the discrete Fourier transform in $\mathbb{Z}_N$: If $f : \mathbb{Z}_N \to \mathbb{C}$ is a function, then

$$\widehat{f}(\xi) = \sum_{x \in \mathbb{Z}_N} f(x) e^{2\pi i x \xi / N}, \quad \xi \in \mathbb{Z}_N.$$

Lemma 4.8. *Define*

$$\Lambda_m := \{x \in \mathbb{Z}_N : m \mid x\},$$

$$H_m := \{x \in \mathbb{Z}_N : (x, N) = m\} = \Lambda_m \setminus \bigcup_{m':m\mid m'\mid N, m'\neq m} \Lambda_{m'}.$$

Then $\widehat{\mathbf{1}_{H_m}}(\xi) = G_\xi(N/m)$, *where*

$$G_\xi(v) = \sum_{d\mid(v,\xi)} \mu(v/d)d. \tag{4.7}$$

Proof. Using the fact that

$$\widehat{\mathbf{1}_{\Lambda_m}}(\xi) = \frac{N}{m}\mathbf{1}_{\Lambda_{N/m}}(\xi),$$

we get by inclusion-exclusion

$$\widehat{\mathbf{1}_{H_m}}(\xi) = \sum_{d\mid\frac{N}{m}} \mu(d)\widehat{\mathbf{1}_{\Lambda_{md}}}(\xi)$$

$$= \sum_{d\mid\frac{N}{m}} \mu(d)\frac{N}{md}\mathbf{1}_{\Lambda_{N/md}}(\xi)$$

$$= \sum_{d'\mid\frac{N}{m}} \mu\left(\frac{N}{md'}\right)d'\mathbf{1}_{\Lambda_d}(\xi)$$

$$= \sum_{d'\mid(\frac{N}{m},\xi)} \mu\left(\frac{N}{md'}\right)d'$$

$$= G_\xi(N/m).$$

$\square$

Proposition 4.9. *We have*

$$\sum_{v\mid N} \frac{1}{\phi(v)}G_\xi(v)G_{\xi'}(v) = \begin{cases} \frac{N}{\phi(N/d)} & \text{if } (\xi, N) = (\xi', N) = d, \\ 0 & \text{if } (\xi, N) \neq (\xi', N). \end{cases} \tag{4.8}$$

Proof. We first claim that for every ξ, the function $G_\xi(v)$ is multiplicative in v. Indeed, let $(x, y) = 1$, $(x, \xi) = t$ and $(y, \xi) = s$. Then $(t, s) = 1$ and $(xy, \xi) = ts$. Writing $u = u' \cdot u''$, $u' \mid x$ and $u'' \mid y$, we get

$$G_\xi(xy) = \sum_{u\mid(xy,\xi)} \mu\left(\frac{xy}{u}\right)u = \sum_{u'\mid(x,\xi),u''\mid(y,\xi)} \mu\left(\frac{x}{u'}\right)\mu\left(\frac{y}{u''}\right)u'u'' = G_\xi(x)G_\xi(y).$$

Therefore, $G_\xi(v)$ is entirely determined by its values $G_\xi(v)$ on prime powers p_i^j, $j = 0, 1, \ldots, \alpha_i$, $i = 1, \ldots, k$. Let $\xi = p_1^{\nu_1} \cdots p_k^{\nu_k}$. Then $p_i^\kappa \parallel (p_i^j, \xi)$ for $\kappa = \min(j, \nu_i)$. If $j = 0$, we have $\kappa = 0$ and $G_\xi(p_i^0) = G_\xi(1) = 1$. If $j \geq 1$, we have

$$G_\xi\left(p_i^j\right) = \sum_{u\mid p_i^\kappa} \mu\left(\frac{p_i^j}{u}\right)u = \begin{cases} p_i^j - p_i^{j-1} & \text{if } \kappa = j, \\ -p_i^{j-1} & \text{if } \kappa = j - 1, \\ 0 & \text{if } \kappa < j, \end{cases}$$

which is equivalent to

$$G_\xi\left(p_i^j\right) = \begin{cases} p_i^j - p_i^{j-1} = \phi\left(p_i^j\right) & \text{if } j \le \nu_i, \\ -p_i^{\nu_i} & \text{if } j = \nu_i + 1, \\ 0 & \text{if } j > \nu_i + 1. \end{cases} \tag{4.9}$$

Next, if F is a multiplicative function, then

$$\sum_{\nu|N} F(\nu) = \sum_{0 \le j_1 \le \alpha_1, \ldots, 0 \le j_k \le \alpha_k} F\left(p_1^{j_1} \cdots p_k^{j_k}\right) = \prod_{i=1}^k \left(\sum_{j_i=0}^{\alpha_i} F\left(p_i^{j_i}\right)\right).$$

Applying this with $F(\nu) = G_\xi(\nu) G_{\xi'}(\nu)$ for fixed ξ, ξ', we get

$$\sum_{\nu|N} \frac{1}{\phi(\nu)} G_\xi(\nu) G_{\xi'}(\nu) = \prod_{i=1}^k \left(\sum_{j_i=0}^{\alpha_i} \frac{1}{\phi\left(p_i^{j_i}\right)} G_\xi\left(p_i^{j_i}\right) G_{\xi'}\left(p_i^{j_i}\right)\right). \tag{4.10}$$

Fix a prime divisor $p_i \mid N$, and consider the corresponding factor in equation (4.10). Suppose that $0 \le \nu, \nu' \le \alpha_i$ are such that $p_i^\nu \| \xi, p_i^{\nu'} \| \xi'$. Without loss of generality, we may assume that $\nu \le \nu'$. In accordance with equation (4.9), we have three cases.

○ If $\nu < \nu' \le \alpha_i$, then $\nu + 1 \le \alpha_i$ and

$$\sum_{j=0}^{\alpha_i} \frac{1}{\phi\left(p_i^j\right)} G_\xi\left(p_i^j\right) G_{\xi'}\left(p_i^j\right) = 1 + \sum_{j=1}^{\nu} \frac{1}{\phi\left(p_i^j\right)} \phi\left(p_i^j\right)\left(p_i^j - p_i^{j-1}\right) + \frac{1}{\phi\left(p_i^{\nu+1}\right)} \phi\left(p_i^{\nu+1}\right)\left(-p_i^n\right)$$

$$= 1 + \sum_{j=1}^{\nu}\left(p_i^j - p_i^{j-1}\right) - p^\nu = 0.$$

○ If $\nu = \nu' < \alpha_i$, then $\nu + 1 = \nu' + 1 \le \alpha_i$ and

$$\sum_{j=0}^{\alpha_i} \frac{1}{\phi\left(p_i^j\right)} G_\xi\left(p_i^j\right) G_{\xi'}\left(p_i^j\right) = 1 + \sum_{j=1}^{\nu}\left(p_i^j - p_i^{j-1}\right) + \frac{1}{p_i^{\nu+1} - p_i^\nu}\left(-p_i^\nu\right)^2 = \frac{p_i^{\nu+1}}{p_i - 1}.$$

○ If $\nu = \nu' = \alpha_i$, then

$$\sum_{j=0}^{\alpha_i} \frac{1}{\phi\left(p_i^j\right)} G_\xi\left(p_i^j\right) G_{\xi'}\left(p_i^j\right) = 1 + \sum_{j=1}^{\alpha_i}\left(p_i^j - p_i^{j-1}\right) = p_i^{\alpha_i}.$$

Since

$$\frac{p_i^{\alpha_i}}{\phi\left(p_i^{\alpha_i-\nu}\right)} = \begin{cases} p^{\alpha_i} & \text{if } \nu = \alpha_i, \\ \dfrac{p^{\alpha_i}}{(p_i-1)p_i^{\alpha_i-\nu-1}} = \dfrac{p_i^{\nu+1}}{p_i-1} & \text{if } \nu < \alpha_i, \end{cases}$$

we conclude that

$$\sum_{j=0}^{\alpha_i} \frac{1}{\phi\left(p_i^j\right)} G_\xi\left(p_i^j\right) G_{\xi'}\left(p_i^j\right) = \begin{cases} 0 & \text{if } \nu \ne \nu', \\ \dfrac{p_i^{\alpha_i}}{\phi(p_i^{\alpha_i-\nu})} & \text{if } \nu = \nu'. \end{cases}$$

We now plug this into equation (4.10), and since p_i is no longer fixed, we write v_i and v_i' instead of v and v'. If $(\xi, N) \neq (\xi', N)$, then $v_i \neq v_i'$ for at least one p_i, so that

$$\sum_{v \mid N} \frac{1}{\phi(v)} G_\xi(v) G_{\xi'}(v) = 0.$$

If, on the other hand, $(\xi, N) = (\xi', N)$, we get

$$\sum_{v \mid N} \frac{1}{\phi(v)} G_\xi(v) G_{\xi'}(v) = \prod_{i=1}^k \frac{p_i^{\alpha_i}}{\phi\left(p_i^{\alpha_i - v_i}\right)} = \frac{N}{\phi(N/(\xi, N))},$$

which proves the proposition. □

In order to finish the proof of Theorem 4.7, we write

$$\mathbb{A}_m^N[C] = \sum_{x,y,z \in \mathbb{Z}_N} w_A(x) w_C(y) \mathbf{1}_{H_m}(z) \mathbf{1}_{x-y=z}$$

$$= \frac{1}{N} \sum_{x,y,z \in \mathbb{Z}_N} w_A(x) w_C(y) \mathbf{1}_{H_m}(z) \sum_{\xi \in \mathbb{Z}_N} e^{-2\pi i \xi (x-y+z)/N}$$

$$= \frac{1}{N} \sum_{\xi \in \mathbb{Z}_N} \widehat{w_A}(\xi) \overline{\widehat{w_C}(\xi)} \widehat{\mathbf{1}_{H_m}}(\xi)$$

$$= \frac{1}{N} \sum_{\xi \in \mathbb{Z}_N} \widehat{w_A}(\xi) \overline{\widehat{w_C}(\xi)} G_\xi(N/m).$$

Therefore

$$\langle \mathbb{A}^N[C], \mathbb{B}^N[D] \rangle = \frac{1}{N^2} \sum_{v \mid N} \frac{1}{\phi(v)} \left(\sum_{\xi \in \mathbb{Z}_N} \widehat{w_A}(\xi) \overline{\widehat{w_C}(\xi)} G_\xi(v) \right) \left(\sum_{\xi' \in \mathbb{Z}_N} \widehat{w_B}(\xi') \overline{\widehat{w_D}(\xi')} G_{\xi'}(v) \right)$$

$$= \frac{1}{N^2} \sum_{\xi, \xi' \in \mathbb{Z}_N} \widehat{w_A}(\xi) \overline{\widehat{w_C}(\xi)} \widehat{w_B}(\xi') \overline{\widehat{w_D}(\xi')} \left[\sum_{v \mid N} \frac{1}{\phi(v)} G_\xi(v) G_{\xi'}(v) \right].$$

By Proposition 4.9,

$$\langle \mathbb{A}^N[C], \mathbb{B}^N[D] \rangle = \frac{1}{N^2} \sum_{d \mid N} \frac{N}{\phi(N/d)} \left(\sum_{\xi : (\xi, N) = d} \widehat{w_A}(\xi) \overline{\widehat{w_C}(\xi)} \right) \left(\sum_{\xi' : (\xi', N) = d} \widehat{w_B}(\xi') \overline{\widehat{w_D}(\xi')} \right),$$

which is equation (4.6), since $\widehat{w_A}(\xi) = A\left(e^{-2\pi i \xi/N}\right)$ and $\zeta = e^{-2\pi i \xi/N}$ is a root of $\Phi_d(X)$ if and only if $(\xi, N) = N/d$.

4.3. *Proof of Theorem 4.4*

(i) Assume that $A \oplus B = \mathbb{Z}_M$. Let $N \mid M$, and let $C = \{x\}$ and $D = \{y\}$ for $x, y \in \mathbb{Z}_N$. By equation (4.5), we have

$$\langle \mathbb{A}^N[x], \mathbb{B}^N[y] \rangle = \sum_{d \mid N} \frac{1}{N\phi(d)} \left[\sum_{\zeta : \Phi_d(\zeta)=0} A(\zeta) \overline{C(\zeta)} \right] \left[\sum_{\zeta : \Phi_d(\zeta)=0} B(\zeta) \overline{D(\zeta)} \right].$$

If $d \neq 1$, then $\Phi_d(X)$ divides at least one of $A(X)$ and $B(X)$. Hence the only nonzero contribution is from $d = 1$, which yields

$$\langle \mathbb{A}^N[x], \mathbb{B}^N[y] \rangle = \frac{1}{N} A(1)C(1)B(1)D(1) = \frac{|A||B|}{N}.$$

This proves equation (4.2).

(ii) Suppose that $A, B \subset \mathbb{Z}_M$ satisfy $\langle \mathbb{A}^M[a], \mathbb{B}^M[b] \rangle = 1$ for all $a \in A, b \in B$. Then

$$\langle \mathbb{A}^M[A], \mathbb{B}^M[B] \rangle = \sum_{a \in A, b \in B} \langle \mathbb{A}^M[a], \mathbb{B}^M[b] \rangle$$

$$= \sum_{a \in A, b \in B} 1 = |A||B| = M.$$

By equation (4.6), this implies that

$$\sum_{d|M} \frac{1}{\phi(d)} \mathcal{E}_d(A)\mathcal{E}_d(B) = M^2.$$

However, we are also assuming that $\mathcal{E}_1(A)\mathcal{E}_1(B) = |A|^2|B|^2 = M^2$. Hence $\mathcal{E}_d(A)\mathcal{E}_d(B) = 0$ for all $d \mid M, d \neq 1$, so that $A \oplus B = \mathbb{Z}_M$ as claimed.

Remark 4.10. We indicate a proof of Theorem 2.5 based on equation (4.6). Suppose that $A \oplus B = \mathbb{Z}_M$ is a tiling, and apply equation (4.6) with $N = M$. Since $\Phi_d(X) \mid A(X)B(X)$ for all $d \mid M, d \neq 1$, we get

$$\sum_{m|M} \frac{1}{\phi(M/m)} \mathbb{A}_m^M[A]\mathbb{B}_m^M[B] = \frac{|A(1)|^2|B(1)|^2}{M} = M.$$

But we also have $\mathbb{A}_M^M[A]\mathbb{B}_M^M[B] = |A||B| = M$. Hence all other terms $\mathbb{A}_m^M[A]\mathbb{B}_m^M[B]$ with $m \neq M$ must vanish. This proves Theorem 2.5.

5. Cuboids

5.1. Definitions

Definition 5.1. Let $M = \prod_{i=1}^K p_i^{n_i}$.

(i) A *cuboid type* $\mathcal{T}$ on $\mathbb{Z}_N$ is an ordered triple $\mathcal{T} = (N, \vec{\delta}, T)$, where
   ○ $N = \prod_{i=1}^K p_i^{n_i - \alpha_i}$ is a divisor of M, with $0 \leq \alpha_i \leq n_i$ for each $i = 1, \ldots, K$;
   ○ $\vec{\delta} = (\delta_1, \ldots, \delta_K)$, with $0 \leq \delta_i \leq n_i - \alpha_i$ for $i = 1, \ldots, K$;
   ○ $T \subset \mathbb{Z}_N$ is a nonempty set.
   We will refer to N as the *scale* of $\mathcal{T}$, and to T as its *template*. We also define $\mathfrak{J} = \mathfrak{J}_{\vec{\delta}} := \{j : \delta_j \neq 0\}$.

(ii) Let $\mathcal{T} = (N, \vec{\delta}, T)$ be a cuboid type as described. A *cuboid* Δ of type $\mathcal{T}$ is a weighted multiset corresponding to a mask polynomial of the form

$$\Delta(X) = X^c \prod_{j \in \mathfrak{J}} \left(1 - X^{d_j} \right), \tag{5.1}$$

where c, d_j are elements of $\mathbb{Z}_M$ such that $(d_j, N) = N/p_j^{\delta_j}$. The *vertices* of Δ are the points

$$x_{\vec{\epsilon}} = c + \sum_{j \in \mathfrak{J}} \epsilon_j d_j : \vec{\epsilon} = (\epsilon_j)_{j \in \mathfrak{J}} \in \{0, 1\}^{|\mathfrak{J}|}, \tag{5.2}$$

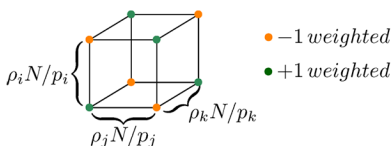with weights $w_\Delta(x_{\vec{\epsilon}}) = (-1)^{\sum_{j \in \mathfrak{J}} \epsilon_j}$.

Figure 2. *An N-cuboid with N having three prime factors.*

(iii) Set $A \in \mathcal{M}(\mathbb{Z}_N)$, and let Δ be a cuboid of type $\mathcal{T}$. Then the (Δ, T)-*evaluation of A* is

$$\mathbb{A}^{\mathcal{T}}[\Delta] = \mathbb{A}_N^N[\Delta * T] = \sum_{\vec{\epsilon} \in \{0,1\}^k} w_{\Delta}(x_{\vec{\epsilon}}) \, \mathbb{A}_N^N[x_{\vec{\epsilon}} * T],$$

where we recall that $x * T = \{x + t : t \in T\}$, so that

$$\mathbb{A}_N^N[x_{\vec{\epsilon}} * T] := \sum_{t \in T} \mathbb{A}_N^N[x_{\vec{\epsilon}} + t].$$

For consistency, we will also write

$$\mathbb{A}^{\mathcal{T}}[x] = \mathbb{A}_N^N[x * T], \quad x \in \mathbb{Z}_M.$$

In some situations, it will be easier to write out Δ in its polynomial form. We will then identify the polynomial $\Delta(X)$ with the corresponding weighted multiset Δ, and write $\mathbb{A}^{\mathcal{T}}[\Delta(X)]$ instead of $\mathbb{A}^{\mathcal{T}}[\Delta]$.

Definition 5.2. Set $A \in \mathcal{M}(\mathbb{Z}_M)$, and let $\mathcal{T} = (N, \vec{\delta}, T)$ be a cuboid type as before. We will say that *A is $\mathcal{T}$-null* if for every cuboid Δ of type $\mathcal{T}$,

$$\mathbb{A}^{\mathcal{T}}[\Delta] = 0. \tag{5.3}$$

Lemma 5.3. *Set $A \in \mathcal{M}(\mathbb{Z}_M)$, and let $\mathcal{T} = (N, \vec{\delta}, T)$ be a cuboid type. Suppose that for all $m \mid N$, the cyclotomic polynomial $\Phi_m(X)$ divides at least one of $A(X)$, $T(X)$, or $1 - X^{N/p_j^{\delta_j}}$ for some $j \in \mathfrak{J}(\vec{\delta})$. Then A is $\mathcal{T}$-null.*

Proof. This follows, for example, from Theorem 4.7 applied to $A(X)$ and $C(X) = \Delta(X)T(X)$, with $B = D = \{0\}$. □

5.2. Classic cuboids

Definition 5.4. An *N-cuboid* is a cuboid of type $\mathcal{T} = (N, \vec{\delta}, T)$, where $N \mid M$, $T(X) = 1$ and $\delta_j = 1$ for all j such that $p_j \mid N$. Thus, N-cuboids have the form

$$\Delta(X) = X^c \prod_{p_j \mid N} \left(1 - X^{\rho_j N/p_j}\right)$$

with $(\rho_j, p_j) = 1$ for all j, and the associated Δ-evaluation of a multiset $A \in \mathcal{M}(\mathbb{Z}_N)$ is

$$\mathbb{A}_N^N[\Delta] = \sum_{\vec{\epsilon} \in \{0,1\}^{|\mathfrak{J}|}} w_{\Delta}(x_{\vec{\epsilon}}) \, \mathbb{A}_N^N[x_{\vec{\epsilon}}],$$

where $\mathfrak{J} = \{j : p_j \mid N\}$ and the cuboid vertices $x_{\vec{\epsilon}}$ are defined in equation (5.2). If $\mathcal{T}$ is as before and $A \in \mathcal{M}(\mathbb{Z}_N)$ is $\mathcal{T}$-null, we will also say for short that *A is N-null*.

The geometric interpretation of N-cuboids Δ is as follows. With notation as in Definition 5.4, recall that $D(N) = N/\prod_{j \in \mathfrak{J}} p_j$. Then the vertices $x_{\vec{\epsilon}}$ of Δ form a full-dimensional rectangular box in the grid

$\Lambda(c, D(N))$, with one vertex at c and alternating ± 1 weights. We reserve the term 'N-cuboid', without cuboid type explicitly indicated, to refer to cuboids as in Definition 5.4; for cuboids of any other type, we will always specify $\mathcal{T}$.

The following cyclotomic divisibility test has been known and used previously in the literature (see, for example, [42, Section 3] in the context of vanishing sums of roots of unity, or [16, Section 3] and [17] with applications to the 'spectral implies tiling' direction of Fuglede's conjecture.

Proposition 5.5. *Set* $A \in \mathcal{M}(\mathbb{Z}_N)$. *Then the following are equivalent:*

 (i) $\Phi_N(X)|A(X)$.
(ii) *For all N-cuboids Δ, we have*

$$\mathbb{A}_N^N[\Delta] = 0. \tag{5.4}$$

Proof. Let $m \mid N$ satisfy $m \neq N$. Then $m \mid (N/p_i)$ for some i such that $p_i \mid N$, so that $\Phi_m \mid (1 - X^{N/p_i})$. The implication (i) $\Rightarrow$ (ii) now follows from Lemma 5.3.

An alternative proof that (i) implies (ii) (without using Theorem 4.7; compare [16, 42]) is as follows. By classic results on vanishing sums of roots of unity [3, 28, 32, 35, 36, 38], $\Phi_N(X) \mid A(X)$ if and only if $A(X)$ is a linear combination of the polynomials $\Phi_p(X^{N/p})$, where p runs over all prime divisors of N, with integer (but not necessarily nonnegative) coefficients. Equivalently, $\Phi_N(X) \mid A(X)$ if and only if A can be represented as a linear combination of N-fibers. It is very easy to see that equation (5.4) holds for all N-cuboids Δ if A mod N is an N-fiber; therefore it also holds if A mod N is a linear combination of such fibers.

The proof that (ii) implies (i) is by induction on the number of prime divisors of N (this argument was also known previously in the literature; see, for example, [42, Proposition 2.4]). We present it here for completeness.

If $N = p^\alpha$ is a prime power, the claim follows from equation (2.6). Suppose that the claim is true for all N' with at most k prime divisors. Suppose that N has $k + 1$ prime divisors, and that $A \in \mathcal{M}(\mathbb{Z}_N)$ obeys equation (5.4) for all N-cuboids Δ in $\mathbb{Z}_N$. Let p be a prime divisor of N, and let $N' = N/p^\alpha$, where $(N', p) = 1$.

Assume first that

$$A \in \mathcal{M}\left(p^{\alpha-1}\mathbb{Z}_N\right). \tag{5.5}$$

Write $A(X) = \sum_{j=0}^{p-1} X^{jN/p} A_j(X)$, where $A_j \in \mathcal{M}(p^\alpha \mathbb{Z}_N)$. Each 'layer' A_j can be identified in the obvious manner with a multiset in $\mathbb{Z}_{N'}$.

For $j = 0, 1, \ldots, p - 1$, let $A_{j,0}$ be the weighted multiset defined via $A_{j,0}(X) = A_j(X) - A_0(X)$. The condition (5.4) implies that, with the obvious notation,

$$\left(\mathbb{A}_{j,0}\right)^{N'}[\Delta'] = 0$$

for every full-dimensional cuboid Δ' in $\mathbb{Z}_{N'}$. By the inductive assumption, $\Phi_{N'}(X) \mid A_{j,0}(X)$. By the structure theorem for vanishing sums of roots of unity, $A_{j,0}$ is a linear combination of N'-fibers in $\mathbb{Z}_{N'}$. Returning to $\mathbb{Z}_N$ now, and summing in j, we get that $A(X) = A'(X) + A''(X)$, where the following are true:

○ $A'(X) = \sum_{j=0}^{p-1} X^{jN/p} A_{j,0}(X)$. By the foregoing argument, A' is a linear combination of fibers in directions perpendicular to p.
○ $A'' = \sum_{j=0}^{p-1} X^{jN/p} A_0(X)$. This is a linear combination of fibers in the p direction.

Thus A is a linear combination of fibers, and therefore $\Phi_N(X) \mid A(X)$.

Finally, in the general case without assumption (5.5), we can write A as a union of multisets $A^{(i)}$, $i = 0, 1, \ldots, p^{\alpha-1} - 1$, where each $A^{(i)}$ is a translate of a multiset satisfying assumption (5.5). If equation

(5.4) holds for A, then it also holds for each $A^{(i)}$. By the previous argument, we get that $\Phi_N(X) \mid A^{(i)}(X)$ for each i, and therefore it divides $A(X)$. This completes the proof that (ii) implies (i). $\qquad\square$

Remark 5.6. Proposition 5.5 implies in particular that for any $N \mid M$, Φ_N divides A if and only if it divides the mask polynomial of $A \cap \Lambda(x, D(N))$ for every $x \in \mathbb{Z}_M$. Indeed, the vertices of any N-cuboid Δ are all contained in the same $D(N)$-grid. Hence the divisibility of A by Φ_M is associated with the structure of A on such grids.

5.3. Multiscale cuboids

In many situations, we need to work with cuboids on several scales simultaneously. This happens, for example, when we investigate the divisibility of a polynomial $A(X)$ by combinations of cyclotomic polynomials, or when we try to reduce a tiling of $\mathbb{Z}_M$ to tilings of cosets of a subgroup. We will use cuboids with nontrivial templates to facilitate such multiscale cuboid analysis.

Definition 5.7 (Folding templates). Let $M = \prod_{i=1}^{K} p_i^{n_i}$ and $N = \prod_{i=1}^{K} p_i^{n_i - \alpha_i}$, with $0 \leq \alpha_i \leq n_i$ for $i = 1, \ldots, K$. The *folding template* T_N^M is given by

$$T_N^M(X) \equiv \prod_{i:p_i \mid \frac{M}{N}} \prod_{\nu_i = 1}^{\alpha_i} \Psi_{M/p_i^{\nu_i}}(X) \equiv \frac{X^M - 1}{X^N - 1} \bmod \left(X^M - 1 \right),$$

where

$$\Psi_{M/p_i^\delta}(X) = \Phi_{p_i}\left(X^{M/p_i^\delta} \right) = 1 + X^{M/p_i^\delta} + X^{2M/p_i^\delta} + \cdots + X^{(p_i - 1)M/p_i^\delta}. \qquad (5.6)$$

When M is fixed, we will sometimes write T_N instead of T_N^M, for simplicity.

Strictly speaking, Ψ_{M/p_i^δ} depends on both M and p_i^δ, not just on their quotient; however, both numbers will always be clear from the context. We also note that $\Psi_{M/p_i} = F_i$.

Definition 5.7 allow us to consider N-cuboids as cuboids with templates in $\mathbb{Z}_M$. Specifically, let $N \mid M$ be as in Definition 5.7. Then for any $A \in \mathcal{M}(\mathbb{Z}_M)$ and $x \in \mathbb{Z}_M$,

$$\mathbb{A}_N^N[x] = \mathbb{A}_M^M\left[x * T_N^M \right]. \qquad (5.7)$$

Consequently, we have the following:

Lemma 5.8. *With M and N as in Definition 5.7, let $\mathcal{T} = (M, \vec{\delta}, T_N^M)$, where*

$$\delta_i = \begin{cases} \alpha_i + 1 & \text{if } \alpha_i < n_i, \\ 0 & \text{if } \alpha_i = n_i, \end{cases} \quad i \in \{1, \ldots, K\}. \qquad (5.8)$$

We will sometimes write $\vec{\delta} = \vec{\delta}_N^M$ to indicate the dependence on M and N. Let $A \in \mathcal{M}(\mathbb{Z}_M)$ be a multiset. Then the following are equivalent:

○ $\Phi_N \mid A$;
○ *A is $\mathcal{T}$-null in $\mathbb{Z}_M$;*
○ *the multiset induced by A in $\mathbb{Z}_N$ is N-null (see Definition 5.4).*

Let

$$\Delta = X^c \prod_{i:p_i \mid N} \left(1 - X^{d_i} \right), \quad c \in \mathbb{Z}_M, \quad (M, d_i) = M/p_i^{\alpha_i + 1}, \qquad (5.9)$$
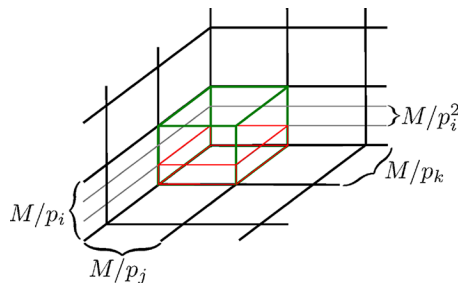
Figure 3. *A classic M-cuboid (green) vs. a multiscale cuboid (red) corresponding to the product* $\Phi_M \Phi_{M/p_i}$.

be a cuboid of type $\mathcal{T}$ as in Lemma 5.8. Then the cuboid Δ mod N, induced by Δ in $\mathbb{Z}_N$, is an N-cuboid. Conversely, any N-cuboid Δ' in $\mathbb{Z}_N$ can be written (not necessarily uniquely) as $\Delta \pmod{N}$, where Δ is a cuboid of the form (5.9) in $\mathbb{Z}_M$. Therefore, whenever working on scales N and M simultaneously, we will represent N-cuboids as cuboids of the form (5.9) in $\mathbb{Z}_M$. In this notation, a multiset $A \in \mathcal{M}(\mathbb{Z}_M)$ satisfies any one (therefore all) of the conditions in Lemma 5.8 if and only if

$$\mathbb{A}_N^N[\Delta] = \mathbb{A}^{\mathcal{T}}[\Delta] = \mathbb{A}_M^M\left[\Delta * T_N^M\right] = 0$$

for all Δ as in equation (5.9). Transitions between several intermediate scales $N_1, N_2, \ldots \mid M$ will be handled similarly, with $\mathbb{Z}_M$ as the default ambient space.

Cuboids with more general templates can be used to indicate divisibility by combinations of several cyclotomic polynomials. We will be particularly interested in implications of the form 'if $\Phi_{s_1}, \ldots, \Phi_{s_l}$ divide $A(X)$, then A is $\mathcal{T}$-null for a given cuboid type $\mathcal{T}$. It will not be necessary to aim for 'if and only if' conditions such as those in Lemma 5.8.

Example 5.9. Let $M = \prod_{i=1}^K p_i^{n_i}$.

(1) Assume that $n_i \geq 2$ for some $i \in \{1, \ldots, K\}$. Let $\mathcal{T} = (M, \vec{\delta}, 1)$ and $\mathcal{T}' = (M, \vec{\delta}, T_{M/p_i}^M)$, with $\delta_i = 2$ and $\delta_j = 1$ for $j \neq i$. Then

$$\Phi_{M/p_i} \mid A \Leftrightarrow A \text{ is } \mathcal{T}'\text{-null},$$
$$\Phi_M \Phi_{M/p_i} \mid A \Leftrightarrow A \text{ is } \mathcal{T}\text{-null}.$$

The first equivalence follows from Lemma 5.8. The second one is easy to check directly. Specifically, if Δ is a cuboid of type $\mathcal{T}$, then $\Phi_m \mid \Delta$ for all $m \mid M$ except for $m \in \{M/p_i, M\}$; conversely, both M-cuboids and M/p_i-cuboids can be expressed as linear combinations of cuboids of type $\mathcal{T}$. (A similar result appears in [17, Lemma 2.13], where it is stated in terms of 'n-dimensional cube rules' and applied to Fuglede's conjecture on cyclic groups.)

(2) Set $2 \leq \alpha \leq n_i$. Then

$$\Phi_M \Phi_{M/p_i} \cdots \Phi_{M/p_i^\alpha} \mid A$$

if and only if A is $\mathcal{T}_\alpha$-null, where $\mathcal{T}_\alpha = (M, \vec{\delta}, 1)$, $\delta_i = \alpha + 1$ if $\alpha_i < n_i$, $\delta_i = 0$ if $\alpha_i = n_i$ and $\delta_j = 1$ for $j \neq i$. This can be proved in the same way as in the previous example.

(3) Assume that $n_i \geq 2$ for some $i \in \{1, \ldots, K\}$. Let $\mathcal{T} = (M, \vec{\delta}, T)$, where $\delta_i = 3$ if $n_i \geq 3$, $\delta_i = 0$ if $n_i = 2$, $\delta_j = 1$ for $j \neq i$ and

$$T(X) = \frac{X^{M/p_i} - 1}{X^{M/p_i^2} - 1} = 1 + X^{M/p_i^2} + \cdots + X^{(p_i-1)M/p_i^2}.$$

We claim that if $\Phi_M \Phi_{M/p_i^2} \mid A$, then A is $\mathcal{T}$-null. Indeed, if $n_i \geq 3$, cuboids of type $\mathcal{T}$ have the form

$$\Delta(X) = X^c \left(1 - X^{\mu_i M/p_i^3}\right) \prod_{j \neq i} \left(1 - X^{\mu_j M/p_j}\right),$$

where $(\mu_i, M) = (\mu_j, M) = 1$. It follows that $\Delta(X)T(X)$ is divisible by all cyclotomic polynomials $\Phi_m(X)$, $m \mid M$, except for Φ_{M/p_i^2} and Φ_M. If $n_i = 2$, the same argument applies, except that there is no factor $1 - X^{\mu_i M/p_i^3}$ in $\Delta(X)$.

6. Tiling reductions

6.1. Subgroup reduction

In this section, we discuss two ways in which the question of proving (T2) for a tiling $A \oplus B = \mathbb{Z}_M$ (and, more generally, investigating the structure of such tilings) may be reduced to the analogous question for tilings $A' \oplus B' = \mathbb{Z}_N$, where $N \mid M$ and $N \neq M$. We start with a recap, in a slightly more general setting, of the reduction that Coven and Meyerowitz used in [2] to prove Theorem 1.1.

Theorem 6.1 (Subgroup reduction [2, Lemma 2.5]; see also [4, Theorem 4.4]). *Assume that $A \oplus B = \mathbb{Z}_M$, where $M = \prod_{i=1}^K p_i^{n_i}$, and that:*

(i) *there exists an $i \in \{1, \ldots, K\}$ such that $A \subset p_i \mathbb{Z}_M$ and*
(ii) *(T2) holds for both A' and B' in any tiling $A' \oplus B' = \mathbb{Z}_{N_i}$, where $N_i = M/p_i$, $|A'| = |A|$ and $|B'| = |B|/p_i$.*

Then A and B satisfy (T2).

Proof. We have $A(X) = A'(X^{p_i})$ for some $A' \subset \mathbb{Z}_{N_i}$. Write also

$$B(X) \equiv \sum_{\nu=0}^{p_i-1} X^{\nu M/p_i^{n_i-1}} B_\nu(X^{p_i}) \bmod X^M - 1,$$

where $B_\nu \subset \mathbb{Z}_{N_i}$ for $\nu = 0, 1, \ldots, p_i - 1$. If $b \in B$ and $b \equiv r \bmod p_i$, then $a + b \equiv r \bmod p_i$ for all $a \in A$; in other words, the tiling breaks down into separate tilings of residue classes mod p_i, with $A' \oplus B_\nu = \mathbb{Z}_{N_i}$ for each ν.

By assumption (ii), A' and B_ν satisfy (T2) for all ν. We need to check that this is still true for A and B. We first claim that for any polynomial $F(X)$ and any $s \in \mathbb{N}$,

$$\Phi_{\tau(s)}(X) \mid F(X^{p_i}) \Leftrightarrow \Phi_s(X) \mid F(X), \tag{6.1}$$

where

$$\tau(s) = \begin{cases} s & \text{if } p_i \nmid s, \\ p_i s & \text{if } p_i \mid s. \end{cases}$$

Indeed, we have $\Phi_{\tau(s)}(X) \mid F(X^{p_i})$ if and only if $F(e^{2\pi i p_i/\tau(s)}) = 0$. This means that $F(e^{2\pi i/s}) = 0$ if $p_i \mid s$, and $F(e^{2\pi i p_i/s}) = 0$ if $p_i \nmid s$. In both cases, this is equivalent to $\Phi_s \mid F$.

Observe first that, by equation (2.6), we must have

$$\Phi_{p_i} \mid B.$$

Suppose that $s_1, \ldots, s_k$ are powers of distinct primes such that $\Phi_{s_1} \cdots \Phi_{s_k} \mid A$. As already noted, we cannot have $s_j = p_i$ for any j. Let $s_j' = s_j/p_i$ if s_j is a power of p_i, and $s_j' = s_j$ otherwise. Then s_j' are

prime powers, and $s_j = \tau(s'_j)$. By equivalence (6.1), $\Phi_{s'_1} \cdots \Phi_{s'_k} \mid A'$, and since (T2) holds for A', we have $\Phi_{s'_1 \cdots s'_k} \mid A'$. Since $\tau(s'_1 \cdots s'_k) = s_1 \cdots s_k$, we get that $\Phi_{s_1 \cdots s_k} \mid A$.

Suppose now that $s_1, \ldots, s_k$ are powers of distinct primes such that $\Phi_{s_1} \cdots \Phi_{s_k} \mid B$ and $s_1, \ldots, s_k \neq p_i$, and define $s'_1, \ldots, s'_k$ as before. Then for $j = 1, \ldots, k$ we have $\Phi_{s_j} \nmid A$, and therefore $\Phi_{s'_j} \nmid A'$ and, since $A' \oplus B_\nu = \mathbb{Z}_{N_i}$ is a tiling, $\Phi_{s'_j} \mid B_\nu$ for each ν. Since B_ν satisfies (T2), we have $\Phi_{s'_1 \cdots s'_k} \mid B_\nu$. It follows that $\Phi_{s_1 \cdots s_k} \mid B_\nu(X^{p_i})$ for each ν, and therefore $\Phi_{s_1 \cdots s_k} \mid B$.

Finally, suppose that $s_1, \ldots, s_k$ are powers of distinct primes such that $\Phi_{s_1} \cdots \Phi_{s_k} \mid B$ and $s_1, \ldots, s_k$ are not powers of p_i, and consider $\Phi_{p_i s}$ with $s = s_1 \cdots s_k$. We have

$$B\left(e^{2\pi i/p_i s}\right) = \sum_{\nu=0}^{p_i-1} e^{2\pi i \nu M/s p_i^{n_i}} B_\nu\left(e^{2\pi i s}\right) = 0,$$

by (T2), for each B_ν. □

Corollary 6.2. *Let $A \oplus B = \mathbb{Z}_M$, where $M = p_1^{n_1} p_2^{n_2} p_3^{n_3} \cdots p_K^{n_K}$. Assume that for each $i \geq 3$, the prime factor p_i divides at most one of $|A|$ and $|B|$. (This happens, for example, if $n_i = 1$ for $i \notin \{1, 2\}$). Then both A and B satisfy (T2).*

Proof. This is not stated explicitly in [2], but it follows by a very similar argument. (See also [[4], 39, 46].) We proceed by induction in the number of prime factors. If $K = 2$ and $M = p_1^{n_1} p_2^{n_2}$, this is Theorem 1.1. Suppose that $K \geq 3$ and that (T2) holds for both A' and B' in any tiling $A' \oplus B' = \mathbb{Z}_{M/p_K}$. By the assumption of the lemma, at least one of $|A|$ and $|B|$ is not divisible by p_K. Assume without loss of generality that $p_K \nmid |A|$. By Tijdeman's theorem [47, Theorem 1] (see also [2, Lemma 2.2]), $\tilde{A} \oplus B = \mathbb{Z}_M$ is again a tiling, where $\tilde{A}(X) = A(X^{p_K})$. We have $\tilde{A} \subset p_K \mathbb{Z}_M$, so that we may apply Theorem 6.1 to conclude that $\tilde{A}$ and B satisfy (T2). By equivalence (6.1), this also means that A satisfies (T2), since the (T2) condition for A involves only cyclotomic polynomials Φ_s with $(s, p_K) = 1$. □

6.2. Slab reduction

Our second tiling reduction also involves passing from a tiling $A \oplus B = \mathbb{Z}_M$ to a tiling of a smaller cyclic group. However, instead of restricting to residue classes and thus constructing a family of tilings of a subgroup $p_i \mathbb{Z}_M$, we will use periodicity. Recall that M-fibers F_i and M-fibered sets were defined in Section 2.3 (see formula (2.4)). Let $M = \prod_{i=1}^K p_i^{n_i}$, and define

$$A_{p_i} = \left\{ a \in A : 0 \leq \pi_i(a) \leq p_i^{n_i-1} - 1 \right\}, \tag{6.2}$$

where π_i is the array coordinate defined in Section 2.2. Suppose that we have $S \oplus B = \mathbb{Z}_M$, where S is the M/p_i-periodic extension of A_{p_i} to $\mathbb{Z}_M$:

$$S(X) = A_{p_i}(X) F_i(X). \tag{6.3}$$

Then we may reduce the period of the tiling and write $A_{p_i} \oplus B = \mathbb{Z}_{M/p_i}$, where A_{p_i} and B are now considered mod M/p_i.

As a motivating example, suppose that $A \oplus B = \mathbb{Z}_M$, with M as before, and that A is M-fibered in the p_i direction. Let A' be a set obtained from A by choosing one point from each fiber, so that $|A'| = |A|/p_i$ and $A = A' * F_i$. Then A is the periodic extension of A', and we have $A' \oplus B = \mathbb{Z}_{M/p_i}$.

Our main results in this section are Theorem 6.5 and Corollary 6.7, where we develop a criterion for A_{p_i} to admit periodic tilings as described, and prove that passing to such tilings preserves the (T2) property.

Lemma 6.3. *Set $A \in \mathcal{M}(\mathbb{Z}_M)$, with M as before. Assume that $\Phi_d \mid A$ for some d such that $p_i^{n_i} \mid d \mid M$. Then for every $1 \le \alpha_i \le n_i$,*

$$\Phi_{d/p_i^{\alpha_i}} \mid A \Rightarrow \Phi_{d/p_i^{\alpha_i}} \mid A_{p_i}.$$

Proof. Let $d = M/\prod_{j \ne i} p_j^{\alpha_j}$ and $d' = d/p_i^{\alpha_i}$. Assume that $\Phi_d \Phi_{d'} \mid A$. We would like to show that $\Phi_{d'} \mid A_{p_i}$. To this end, we define cuboid types $\mathcal{T} = (M, \vec{\delta}, T_d)$ and $\mathcal{T}' = (M, \vec{\delta}', T_{d'})$, where $T_d = T_d^M$, $T_{d'} = T_{d'}^M$ are the folding templates from Definition 5.7 and $\vec{\delta} = \vec{\delta}_d^M$, $\vec{\delta}' = \vec{\delta}_{d'}^M$ are defined as in equation (5.8), with $N = d$ and $N = d'$, respectively.

Let S be the periodic extension of A_{p_i} to $\mathbb{Z}_M$ defined in equation (6.3). We have $\Phi_d \mid F_i$ but $\Phi_{d'} \nmid F_i$, so that $\Phi_{d'} \mid S$ if and only if $\Phi_{d'} \mid A_{p_i}$. We need to prove that

$$\mathbb{S}_{d'}^{d'}[\Delta] = 0$$

for all cuboids Δ of type $\mathcal{T}'$. Fix such a cuboid

$$\Delta(X) = X^y \cdot \prod_j \left(1 - X^{d_j}\right), \quad y \in \mathbb{Z}_M, (d_j, M) = M/p_j^{\delta'_j}.$$

Let

$$\Delta_i(X) = X^y \cdot \prod_{j \ne i} \left(1 - X^{d_j}\right)$$

so that

$$\Delta(X) = \begin{cases} \left(1 - X^{d_i}\right) \Delta_i(X) & \text{if } \alpha_i < n_i, \\ \Delta_i(X) & \text{if } \alpha_i = n_i. \end{cases}$$

Observe that if $\rho_i \in \mathbb{Z}_M$ satisfies $(\rho_i, M) = M/p_i$, then $(1 - X^{\rho_i})\Delta_i(X)$ is a cuboid of type $\mathcal{T}$. Since A is $\mathcal{T}$-null, we have $\mathbb{A}_d^d[(1 - X^{\rho_i}) \Delta_i(X)] = 0$, so that

$$\mathbb{A}_d^d[\Delta_i] = \mathbb{A}_d^d[\rho_i * \Delta_i].$$

Averaging the last equality over all $\rho_i \in \{M/p_i, 2M/p_i, \ldots, (p_i - 1)M/p_i\}$, we get

$$\mathbb{A}_d^d[\Delta_i] = \frac{1}{\phi(p_i)} \mathbb{A}_d^d[\Delta_i * (F_i - 1)].$$

Clearly we may take linear combinations of the latter – that is, for any set $V \subset \mathbb{Z}_M$,

$$\mathbb{A}_d^d[\Delta_i * V] = \frac{1}{\phi(p_i)} \mathbb{A}_d^d[\Delta_i * (F_i - 1) * V]. \tag{6.4}$$

Let $\Psi \subset \mathbb{Z}_M$ be a set such that $\Psi(X) \equiv \prod_{\nu=2}^{\alpha_i} \Psi_{M/p_i^\nu}(X) \bmod X^{M/p_i} - 1$, and

$$0 \le \pi_i(y + z) \le p_i^{n_i - 1} - 1 \quad \forall z \in \Psi. \tag{6.5}$$

Then

$$T_{d'}(X) = T_d(X) F_i(X) \Psi(X)$$
$$= T_d(X) \Psi(X) + (F_i - 1) T_d(X) \Psi(X),$$

so that

$$
\begin{aligned}
\mathbb{A}_{d'}^{d'}[\Delta_i] &= \mathbb{A}_M^M [\Delta_i * T_{d'}] \\
&= \mathbb{A}_M^M [\Delta_i * T_d * \Psi] + \mathbb{A}_M^M [\Delta_i * (F_i - 1) * T_d * \Psi] \\
&= \mathbb{A}_d^d [\Delta_i * \Psi] + \mathbb{A}_d^d [\Delta_i * (F_i - 1) * \Psi].
\end{aligned}
$$

By equation (6.4) with $V = \Psi$, we get

$$
\mathbb{A}_{d'}^{d'}[\Delta_i] = \frac{p_i}{\phi(p_i)} \mathbb{A}_d^d [\Delta_i * \Psi]. \tag{6.6}
$$

The proof of equation (6.6) used only the fact that $\Phi_d \mid A$. Since S has the same property, it follows that

$$
\mathbb{S}_{d'}^{d'}[\Delta_i] = \frac{p_i}{\phi(p_i)} \mathbb{S}_d^d [\Delta_i * \Psi],
$$

By inequality (6.5), we also have

$$
\mathbb{A}_d^d [\Delta_i * \Psi] = \mathbb{S}_d^d [\Delta_i * \Psi].
$$

Assume first that $\alpha_i < n_i$, and note that all of the foregoing arguments apply with Δ_i replaced by $d_i * \Delta_i$, yielding the same conclusions with Ψ replaced by Ψ', such that inequality (6.5) holds with y replaced by $y + d_i$. Recall that A is $\mathcal{T}'$-null, so that

$$
\begin{aligned}
0 &= \mathbb{A}_{d'}^{d'}[\Delta] \\
&= \mathbb{A}_{d'}^{d'}[\Delta_i] - \mathbb{A}_{d'}^{d'}[d_i * \Delta_i] \\
&= \frac{p_i}{\phi(p_i)} \left(\mathbb{A}_d^d [\Delta_i * \Psi] - \mathbb{A}_d^d [d_i * \Delta_i * \Psi'] \right) \\
&= \frac{p_i}{\phi(p_i)} \left(\mathbb{S}_d^d [\Delta_i * \Psi] - \mathbb{S}_d^d [d_i * \Delta_i * \Psi'] \right).
\end{aligned}
$$

Taking the convolution with Ψ_{M/p_i}, and using the fact that $\Psi(X)\Psi_{M/p_i}(X) \equiv \Psi'(X)\Psi_{M/p_i}(X)$ mod $(X^M - 1)$, we conclude that

$$
\begin{aligned}
0 &= \mathbb{S}_d^d \left[\Delta * \Psi * \Psi_{M/p_i} \right] \\
&= \mathbb{S}_{d'}^{d'}[\Delta].
\end{aligned}
$$

It follows that S is $\mathcal{T}'$-null, as required.

If $\alpha_i = n_i$, the proof is the same except that then $\Delta = \Delta_i$, and so the terms with $d_i * \Delta_i$ do not appear in the calculation. □

Lemma 6.4. *Set $A \in \mathcal{M}(\mathbb{Z}_M)$, with M as before, and let $p_i^{n_i} \mid d \mid M$ and $1 \leq \alpha_i \leq n_i$. Assume that $\Phi_{d/p_i^{\alpha_i}} \mid A'_{p_i}$ for all translates A' of A. Then $\Phi_d \Phi_{d/p_i^{\alpha_i}} \mid A$.*

Proof. Let $d = M/\prod_{j \neq i} p_j^{\alpha_j}$ and $d' = d/p_i^{\alpha_i}$. Define the cuboid types $\mathcal{T} = (M, \vec{\delta}, T_d)$ and $\mathcal{T}' = (M, \vec{\delta}', T_{d'})$ as in the proof of Lemma 6.3.

In order to prove that $\Phi_{d'} \mid A$, it suffices to show $\mathbb{A}_{d'}^{d'}[\Delta] = 0$ for all cuboids of the form

$$
\Delta'(X) = X^y \cdot \prod_j \left(1 - X^{d_j} \right), \quad y \in \mathbb{Z}_M, (d_j, M) = M/p_j^{\delta'_j}. \tag{6.7}
$$

We write $A(X) = \sum_{\nu=0}^{p_i-1} A_\nu(X)$, where

$$A_\nu = \left\{ a \in A \mid 0 \leq \pi_i(a) - \nu p_i^{n_i-1} \leq p_i^{n_i-1} - 1 \right\}, \quad \nu = 0, 1, \ldots, p_i - 1. \tag{6.8}$$

Then

$$\mathbb{A}_{d'}^{d'}[\Delta'] = \sum_{\nu=0}^{p_i-1} (\mathbb{A}_\nu)_{d'}^{d'}[\Delta'] = 0$$

using the assumption that A_ν are $\mathcal{T}'$-null for all ν.

We now prove that $\Phi_d \mid A$. It suffices to show $\mathbb{A}_d^d[\Delta] = 0$ for any cuboid of the form

$$\Delta(X) = \left(1 - X^{M/p_i}\right) \Delta_i(X), \tag{6.9}$$

where $y \in \mathbb{Z}_N$, and

$$\Delta_i(X) = X^y \cdot \prod_{j \neq i} \left(1 - X^{d_j}\right), \quad y \in \mathbb{Z}_M, (d_j, M) = M/p_j^{\delta_j}.$$

Indeed, any cuboid of type $\mathcal{T}$ can be written as a linear combination of cuboids as in equation (6.9).

Let $\Psi(X) = \prod_{\nu=2}^{\alpha_i} \Psi_{M/p_i^\nu}(X)$, and

$$\Delta''(X) = \begin{cases} \left(1 - X^{M/p_i^{\alpha_i+1}}\right) \Delta_i(X) & \text{if } \alpha_i < n_i, \\ \Delta_i(X) & \text{if } \alpha_i = n_i. \end{cases}$$

Define also

$$A_i' = \left\{ a \in A : 0 \leq \pi_i(a - y) \leq p_i^{n_i-1} - 1 \right\},$$

$$A_i'' = \left\{ a \in A : 1 \leq \pi_i(a - y) \leq p_i^{n_i-1} \right\}.$$

By our assumption on A, $\Phi_{d'}$ divides both A_i' and A_i''. Suppose first that $\alpha_i < n_i$. Then

$$0 = \left(\mathbb{A}_i'\right)_{d'}^{d'}[\Delta''] = \mathbb{A}_d^d[\Delta_i * \Psi] - \mathbb{A}_d^d\left[\left(M/p_i^{\alpha_i+1}\right) * \Delta_i * \Psi\right],$$

$$0 = \left(\mathbb{A}_i''\right)_{d'}^{d'}[\Delta''] = \mathbb{A}_d^d[\Delta_i * \Psi'] - \mathbb{A}_d^d\left[\left(M/p_i^{\alpha_i+1}\right) * \Delta_i * \Psi\right],$$

where $\Psi'(X) = \Psi - 1 + X^{M/p_i}$. Taking the difference, we get

$$0 = \left(\mathbb{A}_i'\right)_{d'}^{d'}[\Delta''] - \left(\mathbb{A}_i''\right)_{d'}^{d'}[\Delta'']$$

$$= \mathbb{A}_d^d[\Delta_i * \Psi] - \mathbb{A}_d^d[\Delta_i * \Psi']$$

$$= \mathbb{A}_d^d[\Delta],$$

which proves the claim.

If $\alpha_i = n_i$, the proof is the same, except that the terms with $(M/p_i^{\alpha_i+1}) * \Delta_i$ are replaced by 0 in the calculation. $\qquad\square$

Theorem 6.5. *Assume that $A \oplus B = \mathbb{Z}_M$ and $\Phi_{p_i^{n_i}} \mid A$. Then the following are equivalent:*

(i) *For any translate A' of A, we have $A'_{p_i} \oplus B = \mathbb{Z}_{M/p_i}$.*

(ii) *For every d such that $p_i^{n_i} \mid d \mid M$, at least one of the following holds:*

$$\Phi_d \mid A, \tag{6.10}$$

$$\Phi_{d/p_i} \Phi_{d/p_i^2} \cdots \Phi_{d/p_i^{n_i}} \mid B. \tag{6.11}$$

(iii) *For every $p_i^{n_i} \mid m \mid M$,*

$$m \in \mathrm{Div}(A) \Rightarrow m/p_i \notin \mathrm{Div}(B). \tag{6.12}$$

Proof. Let $N_i = M/p_i$. The assumption that $\Phi_{p_i^{n_i}} \mid A$ implies that for any translate A' of A, we have $|A'_{p_i}| = |A|/p_i$, so that

$$|A'_{p_i}| |B| = N_i. \tag{6.13}$$

(i) $\Rightarrow$ (ii): Assume that (i) holds, and suppose that condition (6.11) fails for some $p_i^{n_i} \mid d \mid M$. Then there is an α_i such that $1 \leq \alpha_i \leq n_i$ and $\Phi_{d/p_i^{\alpha_i}} \nmid B$. Then $\Phi_{d/p_i^{\alpha_i}} \mid A'_{p_i}$ for any translate A' of A. By Lemma 6.4, condition (6.10) must hold.

(ii) $\Rightarrow$ (i): Assume that (ii) holds. With equation (6.13) in place, it suffices to prove that for every $d' \mid N_i$, $d' > 1$, $\Phi_{d'}$ divides at least one of $A'_{p_i}(X)$ and $B(X)$. Let $d' \mid N_i$, $d' > 1$, and suppose that $\Phi_{d'} \nmid B$. Then $d' = d/p_i^{\alpha_i}$ for some $p_i^{n_i} \mid d \mid M$ and $1 \leq \alpha_i \leq n_i$. By (ii), we must have $\Phi_d \mid A$. Since $A \oplus B = \mathbb{Z}_M$ is a tiling, we must also have $\Phi_{d'} \mid A$. By Lemma 6.3, we must have $\Phi_{d'} \mid A'_{p_i}$ as claimed.

(i) $\Rightarrow$ (iii): Assume that (i) holds. This implies in particular that A'_{p_i} and $B \bmod \mathbb{Z}_{N_i}$ are sets, so that $N_i \notin \mathrm{Div}(B)$ and condition (6.12) holds for $m = M$.

Next, Theorem 2.5 applied to the tiling $A'_{p_i} \oplus B = \mathbb{Z}_{N_i}$ implies that

$$\mathrm{Div}_{N_i}(A) \cap \mathrm{Div}_{N_i}(B) = \{N_i\}. \tag{6.14}$$

Suppose that condition (6.12) fails for some $m \neq M$ such that $p_i^{n_i} \mid m \mid M$, so that $m \in \mathrm{Div}(A)$ and $m/p_i \in \mathrm{Div}(B)$. Then $m/p_i \neq N_i$ and $m/p_i \in \mathrm{Div}_{N_i}(A) \cap \mathrm{Div}_{N_i}(B)$. But this contradicts equation (6.14).

(iii) $\Rightarrow$ (i): Assume that (iii) holds. By Theorem 2.5, it suffices to prove that $A'_{p_i}, B \bmod \mathbb{Z}_{N_i}$ are sets such that equation (6.14) holds.

We first verify that $A'_{p_i}, B \bmod \mathbb{Z}_{N_i}$ are sets. Indeed, if $a, a' \in A'_{p_i}$ and $a \equiv a' \bmod N_i$, then $a = a'$ by the definition of A'_{p_i}. On the other hand, $M \in \mathrm{Div}(A)$ trivially, and by formula (6.12) it follows that $N_i \notin \mathrm{Div}(B)$, so that $B \bmod N_i$ is also a set.

Suppose now that equation (6.14) fails, with $m_1 \in (\mathrm{Div}_{N_i}(A) \cap \mathrm{Div}_{N_i}(B)) \setminus \{N_i\}$. Since $\mathrm{Div}(A) \cap \mathrm{Div}(B) = \{M\}$, we must have $m_1 = m_2/p_i$ for some m_2 with $p_i^{n_i} \mid m_2 \mid M$, so that

$$m_j \in \mathrm{Div}(A'_{p_i}), \quad m_k \in \mathrm{Div}(B)$$

for some permutation (j, k) of $(1, 2)$. By the definition of A'_{p_i}, we cannot have $p_i^{n_i-1} \| s$ for $s \in \mathrm{Div}(A'_{p_i})$, so that $j = 2$, $k = 1$. But this contradicts condition (6.12). $\square$

Remark 6.6. In the special case when A is M-fibered in the p_i direction, the condition (6.11) of Theorem 6.5 is satisfied, since then $\Phi_d \mid A$ for all $p_i^{n_i} \mid d \mid M$. It is also easy to verify directly that condition (6.12) holds in this case.

Corollary 6.7 (Slab reduction). *Assume that $A \oplus B = \mathbb{Z}_M$, where $M = \prod_{i=1}^{K} p_i^{n_i}$, and that the following are true:*

○ (T2) holds for both A' and B' in any tiling $A' \oplus B' = \mathbb{Z}_{N_i}$, where $N_i = M/p_i$, $|A'| = |A|/p_i$ and $|B'| = |B|$;
○ there exists an $i \in \{1, \dots, K\}$ such that $\Phi_{p_i^{n_i}} \mid A$ and A, B obey one (therefore all) of Theorem 6.5(i)–(iii).

Then A and B satisfy (T2).

Proof. We are assuming that $A'_{p_i} \oplus B = \mathbb{Z}_{M/p_i}$ for any translate A' of A. By the inductive part of the assumption, A'_{p_i} and B satisfy (T2). It remains to prove (T2) for A. Suppose that $d = \prod_{j \in J} p_j^{\alpha_j}$, where $J \subset \{1, \dots, K\}$, $1 \le \alpha_j \le n_j$ for all $j \in J$, and $\Phi_{p_j^{\alpha_j}}(X) \mid A(X)$ for all $j \in J$. For each prime power $p_j^{\alpha_j}$ with $\alpha_j \neq 0$, the polynomial $\Phi_{p_j^{\alpha_j}}(X)$ can divide only one of A and B in the tiling $A \oplus B = \mathbb{Z}_M$, hence

$$\Phi_{p_j^{\alpha_j}} \nmid B \quad \forall j \in J. \tag{6.15}$$

Write $A(X) = \sum_{\nu=0}^{p_i - 1} A_\nu(X)$, where A_ν are as in formula (6.8), so that $A_\nu \oplus B = \mathbb{Z}_{N_i}$ for each ν. We consider two cases:

○ Assume that either $i \notin J$, or $i \in J$ but $\alpha_i \neq n_i$. By formula (6.15), we have $\Phi_{p_j^{\alpha_j}} \mid A_\nu$ for all $j \in J$ and $\nu = 0, 1, \dots, p_i - 1$. We are assuming that (T2) holds for A_ν, so that $\Phi_d \mid A_\nu$. Summing over ν, we get that $\Phi_d \mid A$.
○ Assume now that $i \in J$ and $\alpha_i = n_i$, and let $d' = d/p_i^{n_i}$. Then $\Phi_{d'} \mid A'_{p_i}$ for any translate A' of A, by the argument in the first case applied to A' instead of A. By Lemma 6.4, it follows that $\Phi_d \mid A$.   □

We note the following special case:

Corollary 6.8. *Assume that $A \oplus B = \mathbb{Z}_M$, where $M = p_1^{n_1} p_2^{n_2} p_3^{n_3}$ and p_1, p_2, p_3 are distinct primes. Moreover, assume that there is a permutation (i, j, k) of $(1, 2, 3)$ such that $|A| = p_i p_j^{\alpha_j} p_k^{\alpha_k}$ for some $0 \le \alpha_j \le n_j$, $0 \le \alpha_k \le n_k$, and that A is M-fibered in the p_i direction. Then A and B satisfy (T2).*

Proof. This follows from Corollaries 6.7 and 6.2.   □

7. Saturating sets

7.1. Preliminaries

Definition 7.1 (Restricted N-boxes). Set $A, X \subseteq \mathbb{Z}_M$, and $x \in \mathbb{Z}_M$. The *restriction of $\mathbb{A}^N[x]$ to X* is the N-box $\mathbb{A}^N[x \mid X]$ with entries

$$\mathbb{A}_m^N[x \mid X] = \sum_{a \in X : (x-a, N) = m} w_A^N(a), \quad m \mid N.$$

In particular,

$$\mathbb{A}_m^M[x \mid X] = \#\{a \in A \cap X : (x - a, M) = m\}.$$

The next definition is the key to our analysis of unfibered tilings in [24]. While it could be extended in an obvious way to N-boxes with $N \mid M$, our current arguments only use the M-box version here.

Definition 7.2 (Saturating sets). Set $A, B \subseteq \mathbb{Z}_M$, and $x, y \in \mathbb{Z}_M$. Define

$$A_{x,y} := \{a \in A : (x - a, M) = (y - b, M) \text{ for some } b \in B\},$$

$$A_x := \bigcup_{b \in B} A_{x,b}.$$

Equivalently,

$$A_x = \{a \in A : (x - a, M) \in \text{Div}(B)\}. \tag{7.1}$$

We will refer to A_x as the *saturating set* for x. The sets $B_{y,x}$ and B_y are defined similarly, with A and B interchanged.

With this notation, $A_{x,y}$ is the minimal set that saturates (the A-side of) the product $\langle \mathbb{A}^M[x], \mathbb{B}^M[y] \rangle$, in the sense that

$$\langle \mathbb{A}^M[x \mid X], \mathbb{B}^M[y] \rangle = \langle \mathbb{A}^M[x], \mathbb{B}^M[y] \rangle \tag{7.2}$$

holds for $X = A_{x,y}$, and if $X \subset \mathbb{Z}_M$ is any other set for it holds, then $A_{x,y} \subset X$. The set A_x is the minimal set such that

$$\langle \mathbb{A}^M[x \mid A_x], \mathbb{B}^M[b] \rangle = \langle \mathbb{A}^M[x], \mathbb{B}^M[b] \rangle \quad \forall b \in B. \tag{7.3}$$

While Definition 7.2 makes sense for general sets $A, B \subseteq \mathbb{Z}_M$, our intended application is to the tiling situation $A \oplus B = \mathbb{Z}_M$. In that case, by Theorem 4.4, the box products on the right side of equations (7.2) and (7.3) evaluate to 1. Hence $A_{x,y}$ is the smallest set such that

$$\langle \mathbb{A}^M[x \mid A_{x,y}], \mathbb{B}^M[y] \rangle = 1, \tag{7.4}$$

and A_x is the smallest set such that

$$\langle \mathbb{A}^M[x \mid A_x], \mathbb{B}^M[b] \rangle = 1 \quad \forall b \in B. \tag{7.5}$$

Observe in particular that a saturating set for any $x \in \mathbb{Z}_M$ must be nonempty, and that by Theorem 2.5,

$$A_a = \{a\} \quad \forall a \in A. \tag{7.6}$$

In the next few definitions and lemmas, we will work toward geometric descriptions of saturating sets. Assume that $A \oplus B = \mathbb{Z}_M$. Set $x \in \mathbb{Z}_M \setminus A$, and suppose that $a \in A_x$. By equation (7.1) and divisor exclusion, we must have $(x - a, M) \notin \text{Div}(A)$, and in particular $(x - a, M) \neq (a' - a, M)$ for all $a' \in A$. This motivates the following definition:

Definition 7.3. Let $M = p_1^{n_1} \cdots p_K^{n_K}$, where $p_1, \ldots, p_K$ are distinct primes, and set $x, x' \in \mathbb{Z}_M$, $x \neq x'$. Suppose that $(x - x', M) = p_1^{\alpha_1} \cdots p_K^{\alpha_K}$, with $0 \leq \alpha_j \leq n_j$ for $j = 1, \ldots, K$.

Define

$$\text{Span}(x, x') = \bigcup_{i : \alpha_i < n_i} \Pi \left(x, p_i^{\alpha_i + 1} \right),$$

$$\text{Bispan}(x, x') = \text{Span}(x, x') \cup \text{Span}(x', x). \tag{7.7}$$

Example 7.4. Let $M = p_1^{n_1} p_2^{n_2} p_3^{n_3}$, where p_1, p_2, p_3 are distinct primes and $n_1, n_2, n_3 \geq 2$. Set $x, x' \in \mathbb{Z}_M$, and let $m = (x - x', M)$.

○ Suppose that $m = M/p_1 p_2 p_3$, so that $\alpha_i = n_i - 1$ for $i = 1, 2, 3$, and represent $\mathbb{Z}_M$ as a 3-dimensional M-array. Then $\text{Span}(x, x')$ is the union of the 2-dimensional planes $\Pi(x, p_i^{n_i})$ with $i = 1, 2, 3$, all passing through x, and similarly for $\text{Span}(x', x)$, with x and x' interchanged. Geometrically, $\text{Bispan}(x, x')$ is the union of those 2-dimensional planes at the top scale that contain at least one 2-dimensional face of the 3-dimensional rectangular box 'spanned' by x and x'.

○ Suppose now that $m = M/p_i$ for some $i \in \{1, 2, 3\}$. Then $\text{Span}(x, x') = \Pi(x, p_i^{n_i})$ is a single plane passing through x and perpendicular to the p_i direction, and similarly for $\text{Span}(x', x) = \Pi(x', p_i^{n_i})$.

○ If $m = M/p_i p_j$ for some $i \neq j$, then $\text{Span}(x, x') = \Pi(x, p_i^{n_i}) \cup \Pi(x, p_j^{n_j})$ is a union of two planes.

The higher-dimensional case has a similar interpretation. As should be clear from the foregoing example, the definition is not symmetric with respect to x, x', so that $\mathrm{Span}(x, x') \neq \mathrm{Span}(x', x)$. However, we have the following:

Lemma 7.5. *Set* $x, x' \in \mathbb{Z}_M$. *Then*

$$x' \in \mathrm{Span}(x, z) \Leftrightarrow x \in \mathrm{Span}(x', z).$$

Proof. We have $x' \in \mathrm{Span}(x, z)$ if and only if there exist $i \in \{1, \ldots, K\}$ and $0 \leq \alpha_i < n_i$ such that $p_i^{\alpha_i} \parallel x - z$, $p_i^{\alpha_i} \parallel x' - z$ and $p_i^{\alpha_i + 1} \mid x - x'$. These conditions are clearly symmetric with respect to x and x'. □

Lemma 7.6. *If* $(x - x', M) = (x - x'', M) = m$, *then* $\mathrm{Span}(x, x') = \mathrm{Span}(x, x'')$.

Proof. This follows directly from the definition. □

Lemma 7.7. *Set* $A, B \subset \mathbb{Z}_M$, $x, x' \in \mathbb{Z}_M$ *and* $a \in A$. *If* $(x - a, M) \neq (x' - a, M)$, *then* $a \in \mathrm{Bispan}(x, x')$.

Proof. Suppose that $(x - a, M) \neq (x' - a, M)$. It follows that $(x - a, p_i^{n_i}) \neq (x' - a, p_i^{n_i})$ for some $i \in \{1, \ldots, K\}$. Interchanging x and x' if necessary, we may assume that $p_i^{\alpha_i} \parallel x - a$ and $p_i^{\alpha_i + 1} \mid x' - a$ for some $\alpha_i \in \{0, 1, \ldots, n_i - 1\}$. Hence $p_i^{\alpha_i} \parallel x - x'$, and $a \in \mathrm{Span}(x', x)$. □

Lemma 7.8. *Let* $A, B \subset \mathbb{Z}_M$ *be fixed. Then the following are true:*

(i) *For any* $x, x', y \in \mathbb{Z}_M$, *we have*

$$A_{x', y} \subset A_{x, y} \cup \mathrm{Bispan}(x, x'). \tag{7.8}$$

(ii) *Suppose that* $A \oplus B = \mathbb{Z}_M$. *Then for any* $x \in \mathbb{Z}_M$,

$$A_x \subset \bigcap_{a \in A} \mathrm{Bispan}(x, a). \tag{7.9}$$

Proof. To prove (i), suppose that $a \in A_{x', y}$. Then $(x' - a, M) = (y - b, M)$ for some $b \in B$. If $(x - a, M) = (x' - a, M)$, it follows that $a \in A_{x, y}$. If, on the other hand, $(x - a, M) \neq (x' - a, M)$, then by Lemma 7.7 we must have $a \in \mathrm{Bispan}(x, x')$. This proves inclusion (7.8). Part (ii) follows from (i) and equation (7.6), since $a \in \mathrm{Span}(a, x)$. □

We note a lemma which will be useful in the evaluation of saturating sets:

Lemma 7.9 (Enhanced divisor exclusion). *Let* $A \oplus B = \mathbb{Z}_M$, *with* $M = \prod_{i=1}^{K} p_i^{n_i}$. *Let* $m = \prod_{i=1}^{K} p_i^{\alpha_i}$ *and* $m' = \prod_{i=1}^{K} p_i^{\alpha'_i}$, *with* $0 \leq \alpha_i, \alpha'_i \leq n_i$. *Assume that at least one of* m, m' *is different from* M, *and that for every* $i = 1, \ldots, K$ *we have either* $\alpha_i \neq \alpha'_i$ *or* $\alpha_i = \alpha'_i = n_i$. *Then for all* $x, y \in \mathbb{Z}_M$ *we have*

$$\mathbb{A}_m^M[x] \mathbb{A}_{m'}^M[x] \mathbb{B}_m^M[y] \mathbb{B}_{m'}^M[y] = 0.$$

In other words, there are no configurations $(a, a', b, b') \in A \times A \times B \times B$ *such that*

$$(a - x, M) = (b - y, M) = m, \qquad (a' - x, M) = (b' - y, M) = m'. \tag{7.10}$$

Proof. If we did have a configuration as in equation (7.10), then under the assumptions of the lemma we would have

$$(a - a', M) = (b - b', M) = \prod_{i=1}^{K} p_i^{\min(\alpha_i, \alpha'_i)},$$

with the right side different from M. But that is prohibited by Theorem 2.5. □

7.2. Examples and applications

We first provide examples of using Lemma 7.8 to derive geometric constraints on saturating sets. For simplicity, in these examples we return to the three-prime case with $M = p_1^{n_1} p_2^{n_2} p_3^{n_3}$, where p_1, p_2, p_3 are distinct primes and $n_1, n_2, n_3 \geq 2$. Assume that $A \oplus B = \mathbb{Z}_M$ is a tiling, and set $x \in \mathbb{Z}_M$.
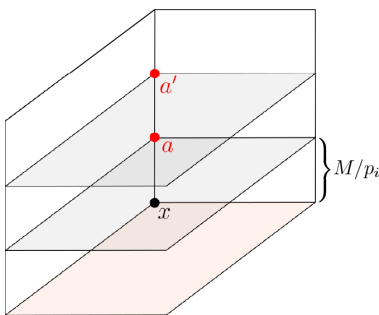
○ Suppose that $(x - a, M) = M/p_i$ for some $a \in A$ and $i \in \{1, 2, 3\}$. Then

$$A_x \subset \mathrm{Bispan}(x, a) = \Pi\left(x, p_i^{n_i}\right) \cup \Pi\left(a, p_i^{n_i}\right).$$
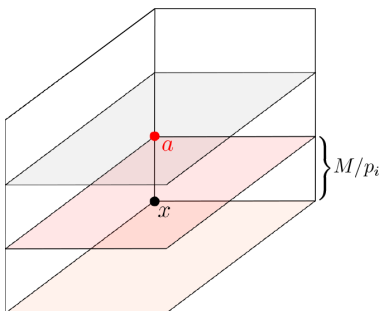
○ Suppose that there are two distinct elements $a, a' \in A$ such that $(x - a, M) = (x - a', M) = M/p_i$. Then

$$A_x \subset \mathrm{Bispan}(x, a) \cap \mathrm{Bispan}(x, a') = \Pi\left(x, p_i^{n_i}\right).$$

○ Suppose that there are two elements $a_i, a_j \in A$ such that $(x - a_i, M) = M/p_i$ and $(x - a_j, M) = M/p_j$, with $i, j \in \{1, 2, 3\}$ distinct. Then

$$A_x \subset \mathrm{Bispan}(x, a_i) \cap \mathrm{Bispan}(x, a_j) = \ell_k(x) \cup \ell_k(a_i) \cup \ell_k\left(a_j\right) \cup \ell_k\left(x_{ij}\right),$$

where $\{1, 2, 3\} \setminus \{i, j\} = \{k\}$, and $x_{ij} \in \mathbb{Z}_M$ is the unique point such that $(x_{ij} - a_i, M) = M/p_j$ and $(x_{ij} - a_j, M) = M/p_i$.

○ Suppose that $(x - a, M) = M/p_i p_j$ for some $a \in A$ and $i, j \in \{1, 2, 3\}$ distinct. Then

$$A_x \subset \Pi\left(x, p_i^{n_i}\right) \cup \Pi\left(a, p_i^{n_i}\right) \cup \Pi\left(x, p_j^{n_j}\right) \cup \Pi\left(a, p_j^{n_j}\right).$$

○ We leave it as an easy exercise for the reader to verify that if there are $a, a', a'' \in A$ such that $(z - z', M) = M/p_i p_j$ for all pairs of distinct elements $z, z' \in \{x, a, a', a''\}$, then

$$A_x \subset \Pi\left(x, p_i^{n_i}\right) \cup \Pi\left(x, p_j^{n_j}\right).$$

○ Suppose that $x \in \mathbb{Z}_M \setminus A$ and $y \in \mathbb{Z}_M \setminus B$ with

$$(x - a, M) = (y - b, M) = M/p_i \text{ for some } a \in A, b \in B. \tag{7.11}$$

We claim that

$$A_{x,y} \subset \Pi\left(x, p_i^{n_i-1}\right), \qquad B_{y,x} \subset \Pi\left(y, p_i^{n_i-1}\right). \tag{7.12}$$

One way to prove this is as follows. Let $a \in A$ and $b \in B$ be as in equation (7.11). As in the first example here, we have $A_{x,b} \subset \text{Bispan}(x, a) \subset \Pi(x, p_i^{n_i-1})$. Hence $B_{b,x} \subset \Pi(b, p_i^{n_i-1}) = \Pi(y, p_i^{n_i-1})$. Applying inclusion (7.8) to B, and using the fact that $\text{Bispan}(y, b) \subset \Pi(y, p_i^{n_i-1})$, we get that $B_{y,x} \subset \Pi(y, p_i^{n_i-1})$ as claimed. This also implies the first half of claim (7.12). Alternatively, claim (7.12) can also be deduced from Lemma 7.9.

Saturating sets are very useful in identifying configurations that *cannot* occur in tiling complements. For example, we have the following easy but important lemma:

Lemma 7.10 (No missing joints). *Let $A \oplus B = \mathbb{Z}_M$, where $M = p_1^{n_1} \cdots p_K^{n_K}$. Suppose that*

$$\{D(M) \mid m \mid M\} \cap \text{Div}(B) = \emptyset, \tag{7.13}$$

and that for some $x \in \mathbb{Z}_M$ there exist $a_1, \ldots, a_K \in A$ such that

$$(x - a_i, M) = M/p_i \quad \forall i \in \{1, \ldots, K\}. \tag{7.14}$$

Then $x \in A$.

Proof. Suppose that $x \notin A$, and let Δ be the M-cuboid with vertices $x, a_1, \ldots, a_K$. By formulas (7.14) and (7.9), the saturating set A_x is contained in the vertex set of Δ. But that is impossible by disjointness condition (7.13). □

As an application, we prove the following restriction on fibered grids that can be a part of a tiling set:

Proposition 7.11. *Let $M = p_1^{n_1} p_2^{n_3} p_2^{n_3}$. Assume that $A \oplus B = \mathbb{Z}_M$ is a tiling, and that there exists a $D(M)$-grid Λ such that $A \cap \Lambda$ is a nonempty union of disjoint M-fibers. Then there is a subset $\{\nu_1, \nu_2\} \subset \{1, 2, 3\}$ of cardinality 2 such that $A \cap \Lambda$ is a union of disjoint M-fibers in the p_{ν_1} and p_{ν_2} directions.*

Proof. Fix A and Λ as in the statement of the proposition. We will say that $\kappa : A \cap \Lambda \to \{1, 2, 3\}$ is an *assignment function* if $A \cap \Lambda$ can be written as

$$A \cap \Lambda = \bigcup_{a \in A \cap \Lambda} \left(a * F_{\kappa(a)}\right),$$

where for any $a, a' \in A \cap \Lambda$, the fibers $a * F_{\kappa(a)}$ and $a' * F_{\kappa(a')}$ are either identical or disjoint. Thus if $a' \in a * F_{\kappa(a)}$, then $\kappa(a') = \kappa(a)$. Note that κ is not necessarily unique, since there exist sets that can be split into nonintersecting fibers in more than one way. We will use Ξ to denote the set of all assignment functions for $A \cap \Lambda$.

It suffices to prove that any assignment function $\kappa \in \Xi$ may take at most two values. To prove this, assume for contradiction that there exists $\kappa \in \Xi$ such that $\kappa(a_1) = 1, \kappa(a_2) = 2, \kappa(a_3) = 3$ for some $a_1, a_2, a_3 \in A \cap \Lambda$. Then the fibers $a_1 * F_1, a_2 * F_2, a_3 * F_3$ are contained in A and pairwise disjoint.

Let $x \in \Lambda$ be the point such that

$$\Pi\left(a_1, p_2^{n_2}\right) \cap \Pi\left(a_2, p_3^{n_3}\right) \cap \Pi\left(a_3, p_1^{n_1}\right) = \{x\}.$$
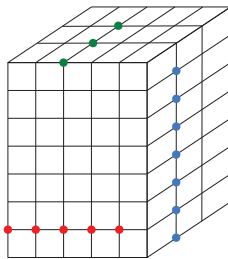
Figure 4. A $D(M)$-grid with disjoint M-fibers in all three directions.

Then there are points $a'_1 \in a_1 * F_1, a'_2 \in a_2 * F_2, a'_3 \in a_3 * F_3$ such that

$$(x - a'_1, M) = M/p_3, \qquad (x - a'_2, M) = M/p_1, \qquad (x - a'_3, M) = M/p_2.$$

Moreover, $\{D(M) \mid m \mid M\} \subset \mathrm{Div}(A \cap \Lambda)$, and hence disjointness condition (7.13) holds. By Lemma 7.10, we must have $x \in A$. However, there is no permitted value for $\kappa(x)$, since $x * F_1$ intersects $a_2 * F_2$, $x * F_2$ intersects $a_3 * F_3$ and $x * F_3$ intersects $a_1 * F_1$. This contradicts the definition of κ. □

For example, under the assumptions of Proposition 7.11, if $A \oplus B = \mathbb{Z}_M$ is a tiling, then $A \cap \Lambda$ cannot consist of three nonintersecting fibers in different directions.

Remark 7.12. Suppose that $\Phi_M \mid A$, where $M = p_1^{n_1} p_2^{n_2} p_3^{n_3}$. Let Λ be a $D(M)$-grid such that $A \cap \Lambda \neq \emptyset$. As discussed in Section 5.2, $A \cap \Lambda(X)$ can be written as

$$(A \cap \Lambda)(X) = \sum_{\nu \in \{1,2,3\}} Q_\nu(X) F_\nu(X), \tag{7.15}$$

where Q_1, Q_2, Q_3 are polynomials with integer coefficients depending on both A and Λ. If, in addition, Q_1, Q_2, Q_3 are polynomials with *nonnegative* coefficients, then $A \cap \Lambda$ is a nonempty union of disjoint M-fibers. By Proposition 7.11, if $A \oplus B = \mathbb{Z}_M$ is a tiling, then $A \cap \Lambda$ can be written in the form of equation (7.15) with at least one of Q_1, Q_2, Q_3 equal to 0.

It is likely that some consistency conditions of this type occur more broadly in tiling sets. For example, in [24, Theorem 9.1(IIa)], we prove a much more difficult and technical result of this type on a lower scale.

8. Fibers and cofibers

8.1. Fibers and fiber chains

Definition 8.1. Let $N \mid M$, and assume that $p_i^\delta \mid N$ for some $\delta \geq 1$. Define

$$\Psi_{N/p_i^\delta}(X) := \Phi_{p_i}\left(X^{N/p_i^\delta}\right) = 1 + X^{N/p_i^\delta} + X^{2N/p_i^\delta} + \cdots + X^{(p_i-1)N/p_i^\delta}. \tag{8.1}$$

This is the same notation as in formula (5.6), but here we are using it for a different purpose. Specifically, we will use polynomials of the form (8.1) as building blocks for multiscale fibers and fiber chains. While Ψ_{N/p_i^δ} depends on both N/p_i^δ and p_i, both numbers will always be clear from the context. We will also use the fact that

$$\Psi_{N/p_i^\delta}(X) = \frac{X^{N/p_i^{\delta-1}} - 1}{X^{N/p_i^\delta} - 1} = \prod_{s \mid M : s \neq 1, p_i^{\gamma-\delta+1} \| s} \Phi_s(X), \tag{8.2}$$

where $\gamma \geq 1$ is the exponent such that $p_i^\gamma \| N$.

Definition 8.2 (Fibers and fiber chains). Let $N \mid M$, and assume that $p_i \mid N$.

(i) A set $F_0 \subset \mathbb{Z}_M$ is *an N-fiber in the p_i direction* if $F_0 \bmod N$ has the mask polynomial

$$F_0(X) \equiv cX^a \Psi_{N/p_i}(X) \bmod X^N - 1, \tag{8.3}$$

with fixed $c \in \mathbb{N}$ and $a \in \mathbb{Z}_N$. Equivalently, $F_0 \bmod N$ is a multiset in $\mathbb{Z}_N$ with weights

$$w_{F_0}^N(x) = \begin{cases} c & \text{if } x \in \{a, a+N/p_i, a+2N/p_i, \ldots, a+(p_i-1)N/p_i\}, \\ 0 & \text{otherwise.} \end{cases}$$

If a fiber F_0 has the form (8.3), we will refer to c as its *multiplicity*, and will say that the fiber is *rooted at a* or *passes through a*.

(ii) A set $A \subset \mathbb{Z}_M$ is *N-fibered in the p_i direction* if it can be written as a union of disjoint N-fibers in the p_i direction, all with the same multiplicity.

(iii) Let $\mathcal{P} \subset \{1, 2, \ldots, n_i\}$ be nonempty, where $p_i^{n_i} \| M$. A set $F \subset \mathbb{Z}_M$ is *a $\mathcal{P}$-fiber chain in the p_i direction* if $|F| = p_i^{|\mathcal{P}|}$ and F is N-fibered in the p_i direction for each $N = M/p_i^{\alpha-1}$, where $\alpha \in \mathcal{P}$. We will also use the convention that if $\mathcal{P} = \emptyset$, then a $\mathcal{P}$-fiber chain in any direction is any singleton set $\{x\}$ with $x \in \mathbb{Z}_M$.

(iv) A set $A \subset \mathbb{Z}_M$ is *$\mathcal{P}$-fibered in the p_i direction* if it can be written as a union of disjoint $\mathcal{P}$-fiber chains in the p_i direction.

We list a few examples. Observe that although we will not use $\mathcal{P}$-fiber chains with multiplicities greater than 1, Definition 8.2(iii) does require the concept of N-fibers with multiplicity.

○ A $\{1\}$-fiber chain in the p_i direction is simply an M-fiber in that direction, and a $\{1\}$-fibered set in the p_i direction with multiplicity 1 is M-fibered in that direction, as defined in Section 2.3.

○ A $\{2\}$-fiber chain in the p_i direction is a set $F \subset \mathbb{Z}_M$ such that for some $a \in \mathbb{Z}_M$ we have $F(x) \equiv X^a(1 + X^{M/p_i^2} + X^{2M/p_i^2} + \cdots + X^{(p_i-1)M/p_i^2}) \bmod (X^{M/p_i} - 1)$. Note that $|F| = p_i$.

○ A $\{1,2\}$-fiber chain in the p_i direction is a set $F \subset \mathbb{Z}_M$ such that for some $a \in \mathbb{Z}_M$ we have $F(x) \equiv X^a(1 + X^{M/p_i^2} + X^{2M/p_i^2} + \cdots + X^{(p_i^2-1)M/p_i^2}) \bmod (X^M - 1)$. Note that $|F| = p_i^2$, F is M-fibered in the p_i direction with multiplicity 1 and M/p_i-fibered in the p_i direction with multiplicity p_i.

Lemma 8.3 (Properties of fibered sets). *Assume that $A \subset \mathbb{Z}_M$ is $\mathcal{P}$-fibered in the p_i direction for some $\mathcal{P} \subset \{1, 2, \ldots, n_i\}$. Then the following hold:*

(i) *We have*

$$\prod_{\alpha \in \mathcal{P}} \Psi_{M/p_i^\alpha}(X) \mid A(X). \tag{8.4}$$

In particular, $\Phi_s(X) \mid A(X)$ for all $s \mid M$, $s \neq 1$, such that $s = p_i^{n_i-\alpha+1}s'$, where $\alpha \in \mathcal{P}$ and $(s', p_i) = 1$.

(ii) *We have $p_i^{|\mathcal{P}|} \mid |A|$. In particular, a $\mathcal{P}$-fiber chain F as in Definition 8.2(iii) is a minimal set that is $\mathcal{P}$-fibered in the p_i direction.*

(iii) $\{M/p_i^\alpha : \alpha \in \mathcal{P}\} \subset \mathrm{Div}(A)$.

(iv) *Let $F \subset \mathbb{Z}_M$ be a $\mathcal{P}$-fiber chain with multiplicity 1 in the p_i direction. Translating F if necessary, we may assume that $0 \in F$. Let $\gamma = \max \mathcal{P}$. Then $F \subset (M/p_i^\gamma)\mathbb{Z}_M \subset \ell_i(0)$, and F tiles $(M/p_i^\gamma)\mathbb{Z}_M \simeq \mathbb{Z}_{p_i^\gamma}$ with the standard tiling complement G, where*

$$G(X) = \prod_{\tau: 1 \leq \tau < \gamma, \tau \notin \mathcal{P}} \Psi_{M/p_i^\tau}(X).$$

(We use the convention that an empty product is equal to 1.*)*

Proof. Part (i) follows directly from the definition, and (ii) follows from (i) since $\Phi_{M/p_i^\alpha}(1) = p_i$. For (iii), set $\alpha \in \mathcal{P}$, and let $a, a' \in A$ be elements that belong to the same $M/p_i^{\alpha-1}$-fiber in the p_i direction, but not to the same M/p_i^β-fiber in the p_i direction for any $\beta < \alpha - 1$. Then $(a - a', M) = M/p_i^\alpha$, as claimed.

We now prove (iv). Assume that $0 \in F$. Since $\Psi_{M/p_i^\alpha}(X) = \Phi_{p_i^{\gamma-\alpha+1}}(X^{M/p_i^\gamma})$ for $\alpha \leq \gamma$, by (i) we have $F(X) \equiv Q(X)\Psi(X^{M/p_i^\gamma}) \mod (X^M - 1)$, where

$$\Psi(X) = \prod_{\alpha \in \mathcal{P}} \Phi_{p_i^{\gamma-\alpha+1}}(X).$$

Since $\Psi(1) = \prod_{\alpha \in \mathcal{P}} p_i = |F|$, we have $Q(1) = 1$. Splitting up the weighted multiset corresponding to $Q(X)$ into residue classes mod M/p_i^γ, and using the fact that F is a set, we see that $Q \in \mathcal{M}((M/p_i^\gamma)\mathbb{Z}_M)$. Hence $F \subset (M/p_i^\gamma)\mathbb{Z}_M$.

Let $F' = \{\frac{x}{M/p_i^\gamma} : x \in F\}$, so that $F' \subset \mathbb{Z}_{p_i^\gamma}$ and $\Psi(X) \mid F'(X)$, with $\Psi(1) = |p_i|^{|\mathcal{P}|} = |F'|$. This is the (T1) tiling condition for F'. Hence F' tiles $\mathbb{Z}_{p_i^\gamma}$ with the standard tiling complement (see Remark 3.5). Rescaling back to $F \subset \mathbb{Z}_M$, we get (iv). $\qquad\square$

8.2. Cofibers and cofibered structures

Given a tiling $A \oplus B = \mathbb{Z}_M$, we will be interested in the occurrences of 'complementary' fiber chains in A and B, in the following sense:

Definition 8.4 (Cofibers). Set $A, B \subset \mathbb{Z}_M$, and fix $1 \leq \gamma \leq n_i$. Let $\mathcal{P}_A, \mathcal{P}_B$ be two disjoint sets such that

$$\mathcal{P}_A \cup \mathcal{P}_B = \{1, 2, \ldots, \gamma\}. \tag{8.5}$$

We say that $F \subset A, G \subset B$ are $(\mathcal{P}_A, \mathcal{P}_B)$-*cofibers* in the p_i direction if:

○ F is a $\mathcal{P}_A$-fiber chain in the p_i direction and
○ G is a $\mathcal{P}_B$-fiber chain in the p_i direction.

We will also refer to (F, G) as a $(\mathcal{P}_A, \mathcal{P}_B)$-*cofiber pair*.

Note that if $\gamma = 1$, then one of the sets $\mathcal{P}_A$ and $\mathcal{P}_B$ must be empty. If $\gamma = 1$ and $\mathcal{P}_A = \emptyset$, then F is a singleton and G is an M-fiber in the p_i direction.

Our goal will be to find global cofibered structures, as we will describe. If $A \oplus B = \mathbb{Z}_M$ is a tiling pair, having a cofibered structure will often allow us to reduce proving (T2) for (A, B) to proving it to an equivalent but simpler tiling pair. In order to allow for intermediate steps involving sets that are only partially fibered, we state the definition for arbitrary sets $A, B \subset \mathbb{Z}_M$:

Definition 8.5 (Cofibered structure and cofibered sets). Set $A, B \subset \mathbb{Z}_M$, and fix $1 \leq \gamma \leq n_i$. Let $\mathcal{P}_A, \mathcal{P}_B$ be two disjoint sets obeying condition (8.5).

(i) We say that the pair (A, B) has a $(\mathcal{P}_A, \mathcal{P}_B)$-*cofibered structure* in the p_i direction if:
    ○ B is $\mathcal{P}_B$-fibered in the p_i direction and
    ○ A contains at least one 'complementary' $\mathcal{P}_A$-fiber chain $F \subset A$ in the p_i direction, which we will call a *cofiber* for this structure. We will say that F is rooted at $a \in A$ if $a \in F$.
(ii) We say that the pair (A, B) is $(\mathcal{P}_A, \mathcal{P}_B)$-*cofibered* in the p_i direction if:
    ○ A is $\mathcal{P}_A$-fibered in the p_i direction and
    ○ B is $\mathcal{P}_B$-fibered in the p_i direction.

We emphasise that part (i) of the definition is *not* symmetric with respect to A and B. Our convention is that the *second* set in the pair must be fibered in its entirety. While a cofibered structure may have

more than one cofiber in A, we do not require that the entire pair (A, B) be cofibered. We will refer to the number γ in Definitions 8.4 and 8.5 as the *depth* of, respectively, the cofiber pair or the cofibered structure.

If A and B satisfy Definition 8.5(i), then by Lemma 8.3,

$$\left\{M/p_i^{\alpha} : \alpha \in \mathcal{P}_A\right\} \subseteq \mathrm{Div}(A), \qquad \left\{M/p_i^{\beta} : \beta \in \mathcal{P}_B\right\} \subseteq \mathrm{Div}(B), \tag{8.6}$$

$$\prod_{\beta \in \mathcal{P}_B} \Psi_{M/p_i^{\beta}}(X) \mid B(X), \tag{8.7}$$

and if a cofiber F is rooted at some $a \in A$, then

$$X^a \prod_{\alpha \in \mathcal{P}_A} \Psi_{M/p_i^{\alpha}}(X) \mid F(X). \tag{8.8}$$

Remark 8.6. Assume that $A, B \subset \mathbb{Z}_M$ satisfy $\mathrm{Div}(A) \cap \mathrm{Div}(B) = \{M\}$, and fix $1 \leq \gamma \leq n_i$. Let $\mathcal{P}_A, \mathcal{P}_B$ be two disjoint sets obeying condition (8.5). Assume that

$$\left\{M/p_i^{\alpha} : \alpha \in \mathcal{P}_A\right\} \cap \mathrm{Div}(B) = \emptyset. \tag{8.9}$$

(In particular, if $A \oplus B = \mathbb{Z}_M$ and A contains a $\mathcal{P}_A$-fiber chain in the p_i direction, then this equation holds by Lemma 8.3(iii) and divisor exclusion.) Then, in order to prove that B is $\mathcal{P}_B$-fibered in the p_i direction, it suffices to verify that every $b \in B$ belongs to a $\mathcal{P}_B$-fiber chain $F(b)$ in the p_i direction. Indeed, by Lemma 8.3 (iv), every $F(b)$ is a maximal subset of $b * (M/p_i^{\gamma})\mathbb{Z}_M$ such that $\mathrm{Div}(F(b)) \cap \{M/p_i^{\alpha} : \alpha \in \mathcal{P}_A\} = \emptyset$. Hence, under the given assumptions, any two fiber chains $F(b)$ and $F(b')$ with $b, b' \in B$ must be either identical or disjoint.

8.3. Fiber shifting

Cofibered structures are important for two reasons. On one hand, they arise naturally from 1-dimensional saturating spaces (see Lemma 8.10). On the other hand, with a cofibered structure in place, Lemma 8.7 allows us to shift the cofibers in A as indicated while maintaining both the tiling property and the (T2) status of A. Applying such shifts repeatedly, we are able to reduce many cases to simpler tilings where (T2) is easy to verify.

Lemma 8.7 (Fiber-shifting lemma). *Let $A \oplus B = \mathbb{Z}_M$. Assume that the pair (A, B) has a $(\mathcal{P}_A, \mathcal{P}_B)$-cofibered structure, with a cofiber $F \subset A$. Let A' be the set obtained from A by shifting F by M/p_i^{β} for any $\beta \in \mathcal{P}_B$. Then $A' \oplus B = \mathbb{Z}_M$, and A is (T2)-equivalent to A'.*

Proof. We have

$$A'(X) = A(X) + (X^{kM/p_i^{\beta}} - 1)F(X)$$

for some k with $(k, p_i) = 1$.

We must prove that $\Phi_s(X) \mid A'(X)B(X)$ for all $s \mid M, s \neq 1$. Fix such s, and write it as $s = p_i^{n_i - \gamma} s'$, where $(s, p_i) = 1$. Consider three cases:

○ If $\gamma \geq \beta$, then $\Phi_s(X) \mid (X^{kM/p_i^{\beta}} - 1)$, and therefore it divides A if and only if it divides A'.
○ If $\gamma < \beta$ and $\gamma \in \mathcal{P}_B$, then $\Phi_s(X) \mid \Psi_{M/p_i^{\gamma}}(X) \mid B(X)$.
○ If $\gamma < \beta$ and $\gamma \in \mathcal{P}_A$, then $\Phi_s(X) \mid \Psi_{M/p_i^{\gamma}}(X) \mid F(X)$, therefore Φ_s divides A if and only if it divides A'.

This implies the first part of the lemma.

Suppose furthermore that Φ_s is a (T2) cyclotomic polynomial of A, in the sense that $s = s_1 \cdots s_{\tau}$, where $s_1, \ldots, s_{\tau}$ are powers of distinct primes such that $\Phi_{s_1} \cdots \Phi_{s_{\tau}} \mid A$. In particular, we must have

$\Phi_{p_i^{n_i-\gamma}} \mid A$, and therefore $\Phi_{p_i^{n_i-\gamma}} \nmid B$. By the foregoing analysis applied to $p_i^{n_i-\gamma}$ instead of s, we must have either $\gamma \geq \beta$ or $\gamma \in \mathcal{P}_A$. In both cases, we get that Φ_s divides A if and only if it divides A', so that the (T2) property is preserved when we pass from A to A'. $\square$

8.4. Fibers and 1-dimensional saturating spaces

We now prove that 1-dimensional saturating sets imply cofibered structures.

Lemma 8.8. *Assume that $A \oplus B = \mathbb{Z}_M$, and let $x, y \in \mathbb{Z}_M$.*

(i) *Let $1 \leq \alpha, \alpha' \leq n_i$, with $\alpha \neq \alpha'$. Then*

$$\mathbb{A}_{M/p_i^\alpha}[x]\mathbb{B}_{M/p_i^\alpha}[y]\mathbb{A}_{M/p_i^{\alpha'}}[x]\mathbb{B}_{M/p_i^{\alpha'}}[y] = 0.$$

In particular, if $A_{x,y} \subset \ell_i(x)$, then the product $\langle \mathbb{A}[x], \mathbb{B}[y] \rangle$ is saturated by a single divisor.

(ii) *Suppose that $A_x \subset \ell_i(x)$. Then there exists an α with $0 \leq \alpha \leq n_i$ such that*

$$\mathbb{A}_{M/p_i^\alpha}[x]\mathbb{B}_{M/p_i^\alpha}[b] = \phi\left(p_i^\alpha\right) \text{ for all } b \in B.$$

Proof. Part (i) is a special case of Lemma 7.9, and part (ii) follows from inclusion (7.9). $\square$

Definition 8.9. Set $\mathcal{P} \subset \{1, 2, \ldots, n_i\}$, and let $F \subset \mathbb{Z}_M$ be a $\mathcal{P}$-fiber chain in the p_i direction.

(i) An element $x \in \mathbb{Z}_M$ is at *distance* m from F if $m \mid M$ is the maximal divisor such that $(z-x, M) = m$ for some $z \in F$.

(ii) If $1 \leq \delta \leq n_i$, we will write $\mathcal{P}[\delta] = \mathcal{P} \cap \{1, 2, \ldots, \delta\}$.

If $x \in \mathbb{Z}_M$ and $F \subset \mathbb{Z}_M$ is a $\mathcal{P}$-fiber chain in the p_i direction, then for all $z \in F$ we have $(z - x, M) = m' p_i^{\alpha(z)}$, where $m' \mid (M/p_i^{n_i})$ is the same for all $z \in F$. In particular, the distance from x to F is well defined and is equal to $m' p_i^{\max_{z \in F} \alpha(z)}$.

Lemma 8.10 (The structure of 1-dimensional saturating spaces). *Assume that $A \oplus B = \mathbb{Z}_M$ is a tiling.*

(i) *Suppose that $x, y \in \mathbb{Z}_M$ satisfy $x \notin A$ and*

$$\mathbb{A}_{M/p_i^\gamma}^M[x]\mathbb{B}_{M/p_i^\gamma}^M[y] = \phi\left(p_i^\gamma\right) \tag{8.10}$$

for some $0 < \gamma \leq n_i$. Then there exist two disjoint sets $\mathcal{P}_A, \mathcal{P}_B$ with

$$\mathcal{P}_A \cup \mathcal{P}_B = \{1, \ldots, \gamma - 1\}, \tag{8.11}$$

$$\left\{M/p_i^\alpha : \alpha \in \mathcal{P}_A\right\} \subseteq \mathrm{Div}(A), \qquad \left\{M/p_i^\beta : \beta \in \mathcal{P}_B\right\} \subseteq \mathrm{Div}(B), \tag{8.12}$$

such that the following holds. Let $A_0 \subset A_{x,y}$ be a maximal subset such that for all $a, a' \in A_0$ with $a \neq a'$ we have $(a - a', M) = M/p_i^\gamma$, and let B_0 be a similar subset of $B_{y,x}$. Then one of the sets A_0 and B_0 has cardinality 1, the other has cardinality $p_i - 1$, and furthermore

$$A_{x,y} = \bigcup_{a \in A_0} F(a), \qquad B_{y,x} = \bigcup_{b \in B_0} G(b), \tag{8.13}$$

where $F(a)$ is a $\mathcal{P}_A$-fiber chain in the p_i direction rooted at a and $G(b)$ is a $\mathcal{P}_B$-fiber chain in the p_i direction rooted at b.

(ii) *Suppose that $x \in \mathbb{Z}_M \setminus A$ and $A_x \subset \ell_i(x)$, with*

$$\mathbb{A}_{M/p_i^\gamma}^M[x]\mathbb{B}_{M/p_i^\gamma}^M[b] = \phi\left(p_i^\gamma\right) \text{ for all } b \in B, \tag{8.14}$$

where $0 < \gamma \leq n_i$ (as follows from Lemma 8.8(ii)). Then the pair (A, B) has a $(\mathcal{P}_A, \mathcal{P}_B \cup \{\gamma\})$-cofibered structure, with A_x as a $\mathcal{P}_A$-cofiber at a distance M/p_i^γ from x.

Proof. We first prove (i). Define A_0 and B_0 as before. Since $A_0 \subset x * (M/p_i^\gamma)\mathbb{Z}_M$ and each element of $A_0 \cup \{x\}$ is contained in a different residue class mod M/p_i^γ, we have $|A_0| \leq p_i - 1$, and similarly for B_0. By divisor exclusion, at most one of these sets has cardinality greater than 1.

Next, let $A_1 \subset x * (M/p_i^\gamma)\mathbb{Z}_M$ be a maximal subset of $A_{x,y}$ such that

$$\forall a, a' \in A_1 \text{ with } a \neq a', \text{ we have } (a - a', M) = M/p_i^{\gamma-1},$$

and define B_1 similarly. Then $|A_1| \leq p_i|A_0|$, since for each $a \in A_1$ there must be a 'parent' $a_0 \in A_0$ with $M/p_i^{\gamma-1} \mid a - a_0$, and each a_0 can have at most p_i such 'children' $a \in A_1$ (we allow $a = a_0$, so that $A_0 \subset A_1$). Similarly, $|B_1| \leq p_i|B_0|$. Moreover, if $|A_1| > |A_0|$, then we must have $M/p_i^{\gamma-1} \in \text{Div}(A)$, and similarly for B, so that at least one of $|A_1| = |A_0|$ and $|B_1| = |B_0|$ must hold. If $|A_1| > |A_0|$, we place $\gamma - 1$ in $\mathcal{P}_A$; otherwise we place it in $\mathcal{P}_B$.

We continue by induction, constructing a sequence of sets

$$A_0 \subset A_1 \subset A_2 \subset \cdots \subset A_{\gamma-1} = A_{x,y}, \qquad B_0 \subset B_1 \subset B_2 \subset \cdots \subset B_{\gamma-1} = B_{y,x},$$

and two disjoint sets $\mathcal{P}_A, \mathcal{P}_B$ obeying condition (8.11), so that for each $l = 1, 2, \ldots, \gamma - 1$:

○ if $l \in \mathcal{P}_A$, then $|A_{\gamma-l+1}| \leq p_i |A_{\gamma-l}|$, $|B_{\gamma-l+1}| = |B_{\gamma-l}|$ and $M/p_i^{\gamma-l} \notin \text{Div}(B)$; and
○ if $l \in \mathcal{P}_B$, then the same holds with A and B interchanged.

It follows that

$$\mathbb{A}^M_{M/p_i^\gamma}[x]\mathbb{B}^M_{M/p_i^\gamma}[y] \leq |A_0||B_0|p_i^{|\mathcal{P}_A|}p_i^{|\mathcal{P}_B|} \leq (p_i - 1)p_i^{\gamma-1} = \phi\left(p_i^\gamma\right).$$

Furthermore, for the equality to hold, one of the sets A_0, B_0 must have cardinality $p_i - 1$; for each $a \in A_0$, the set $F(a) := \{a \in A_{x,y} : M/p_i^{\gamma-1} \mid a - a_0\}$ must be a full $\mathcal{P}_A$-fiber chain in the p_i direction rooted at a; and a similar statement must hold for B. This yields the structure described in part (i).

For part (ii), assume that condition (8.14) holds, and let $B_0(b)$ be the set from formula (8.12) with $y = b$ for each $b \in B$. Since $M/p_i^\gamma \in \text{Div}(B)$, we must have $|A_0| = 1$ and $|B_0(b)| = p_i - 1$. Fix $b \in B$, so that

$$B_{b,x} = \bigcup_{b' \in B_0(b)} G(b').$$

Set $b' \in B_0(b)$, and apply part (i) of the lemma with $y = b'$. Since $b \in B_{b',x}$, there is a $\mathcal{P}_B$-fiber chain $G(b) \subset B$ rooted at b, so that

$$B_{b',x} = G(b) \cup \bigcup_{b'' \in B_0(b), b'' \neq b'} G(b'').$$

Thus $\bigcup_{b'' \in B_0(b) \cup \{b\}} G(b'')$ is a $(\mathcal{P}_B \cup \{\gamma\})$-fiber chain in B, rooted at b. Applying this argument to all $b \in B$, and using Remark 8.6, we get the cofibered structure as indicated. $\square$

The following special case will be used frequently in [24]:

Corollary 8.11. *Assume that $A \oplus B = \mathbb{Z}_M$ is a tiling. Suppose that $x \in \mathbb{Z}_M \setminus A$, $b \in B$, $M/p_i \in \text{Div}(A)$ and*

$$\mathbb{A}^M_{M/p_i^2}[x]\mathbb{B}^M_{M/p_i^2}[b] = \phi\left(p_i^2\right). \tag{8.15}$$

Then there exists a $(\{1\}, \{2\})$-cofiber pair (F, G) such that $F \subset A$ is at distance M/p_i^2 from x, $G \subset B$ is rooted at b and

$$\mathbb{A}^M_{M/p_i^2}[x \mid F]\mathbb{B}^M_{M/p_i^2}[b \mid G] = \phi\left(p_i^2\right). \tag{8.16}$$

In particular, if $M/p_i \in \mathrm{Div}(A)$ and $A_x \subset \ell_i(x)$ with M/p_i^2 as the contributing divisor (compare Lemma 8.8(ii)), then the pair (A, B) has a $(\{1\}, \{2\})$-cofibered structure.

For simplicity, when M is fixed, we will write '$(1, 2)$-cofiber pair' instead of '$(\{1\}, \{2\})$-cofiber pair', and similarly for cofibered structures.

8.5. *Examples and applications*

Let $M = p_1^{n_1} \cdots p_K^{n_K}$ with $K \geq 3$ and $p_1, \ldots, p_K \geq 3$. Assume that $A \oplus B = \mathbb{Z}_M$ and $|A| = p_1 \cdots p_K$. Let also Λ be a fixed $D(M)$-grid, and assume that $0 \in A \cap \Lambda$.

Example 8.12. By Lemma 7.10, we cannot have $\Lambda \setminus A = \{x\}$ for a single point $x \in \Lambda$. Similarly, we cannot have $A \cap \Lambda = A_0$ if A_0 is obtained from Λ by deleting a few more points in an 'unstructured' way so that the assumptions of Lemma 7.10 still apply.

Suppose, however, that $A_0 = \Lambda \setminus (x * F_i)$ for some $x \in \Lambda$ and $i \in \{1, \ldots, K\}$. Then Lemma 7.10 is no longer applicable, and indeed, it is possible to have $A \cap \Lambda = A_0$. However, as we now show, this determines the structure of the entire set A, and in particular, both A and B satisfy (T2).

Indeed, we have $\mathbb{A}_{M/p_j}[x] \geq 2$ for all $j \neq i$. It follows by inclusion (7.9) that $A_x \subset \ell_i(x)$. By Proposition 8.10, the pair (A, B) has a $(\mathcal{P}_A, \mathcal{P}_B)$-cofibered structure of depth $\gamma \geq 2$, with $1 \in \mathcal{P}_A$ since $M/p_i \in \mathrm{Div}(A)$. In particular, A must contain an M-fiber in the p_i direction at distance M/p_i^γ from x. By Lemma 8.7, we can shift that fiber to x, proving that A is (T2)-equivalent to Λ. Thus $A^\flat = \Lambda$, and Corollary 3.8 implies (T2) for both A and B.

We note that the same argument still applies if $A \cap \Lambda$ has several fibers missing (possibly in different directions). This is the case in, for example, Szabó-type examples in [25, 43].

Example 8.13. We now consider a more difficult example where saturating sets are not as obvious. Let $M = p_i^2 p_j^2 p_k^2$ with $p_i, p_j, p_k \geq 3$, and assume that $|A| = p_i p_j p_k$ tiles $\mathbb{Z}_M$. Suppose that there exists an element $x \in \Lambda \setminus A$ such that

$$\mathbb{A}_{M/p_i}[x] = \phi(p_i), \qquad \mathbb{A}_{M/p_j p_k}[x] = \phi\left(p_j p_k\right) \tag{8.17}$$

and $\mathbb{A}_m[x] = 0$ for all $m \in \{D(M) \mid m \mid M\} \setminus \{M/p_i, M/p_j p_k\}$. In the terminology of [24], this is a p_i-*full plane structure*. We prove in [24, Section 7] that for a broader class of tilings including this situation, we have $A^\flat = \Lambda$ and the tiling $A \oplus B = \mathbb{Z}_M$ is (T2)-equivalent to $\Lambda \oplus B = \mathbb{Z}_M$ via fiber shifts. By Corollary 3.8, both A and B satisfy (T2). For expository purposes, we restrict our attention here to this specific structure.

Consider the saturating set A_x, with x as before. This time, geometric restrictions alone are not sufficient to confine A_x to a single line through x. Nonetheless, with an additional argument we have the following lemma:

Lemma 8.14. *Under the assumptions of Example 8.13, we have either $A_x \subset \ell_j(x)$ or $A_x \subset \ell_k(x)$.*

Proof. By inclusion (7.9), we have

$$A_x \subset \ell_j(x) \cup \ell_k(x). \tag{8.18}$$

Set $b \in B$. Suppose that $A_{x,b} \cap \ell_j(x)$ is nonempty. Since $M/p_j \in \mathrm{Div}(A)$, we must have

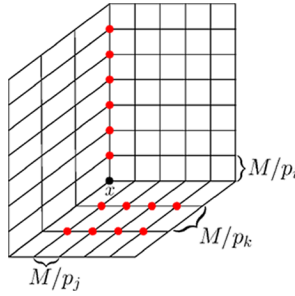$$\mathbb{A}_{M/p_j^2}[x]\mathbb{B}_{M/p_j^2}[b] > 0. \tag{8.19}$$

Figure 5. *A p_i-full plane structure on a $D(M)$-grid.*

If we also had $A_{x,b} \cap \ell_k(x) \neq \emptyset$ for the same b, that would imply that

$$\mathbb{A}_{M/p_k^2}[x]\mathbb{B}_{M/p_k^2}[b] > 0; \tag{8.20}$$

however, having inequalities (8.19) and (8.20) at the same time would contradict Lemma 7.9. Therefore we must have either $A_{x,b} \subset \ell_j(x)$ or $A_{x,b} \subset \ell_k(x)$. Notice that in the former case we have

$$\mathbb{A}_{M/p_j^2}[x]\mathbb{B}_{M/p_j^2}[b] = \phi(p_j^2). \tag{8.21}$$

Since $M/p_j \in \mathrm{Div}(A)$, this can only happen if

$$\mathbb{A}_{M/p_j^2}[x] = p_j \text{ and } \mathbb{B}_{M/p_j^2}[b] = \phi(p_j). \tag{8.22}$$

In other words, the pair $(A \cap \ell_j(x), B \cap \ell_j(b))$ contains a $(1, 2)$-cofiber pair in the p_j direction. If $A_{x,b} \subset \ell_k(x)$, equations (8.21) and (8.22) hold with j replaced by k.

We claim that either $A_x \subset \ell_j(x)$ or $A_x \subset \ell_k(x)$. Indeed, assume for contradiction that there exist $b_j, b_k \in B$ such that $A_{x,b_j} \subset \ell_j(x)$ and $A_{x,b} \subset \ell_k(x)$. It follows from equation (8.22) that

$$
\begin{aligned}
\left| A \cap \Pi\left(x, p_i^{n_i}\right) \right| &\geq \mathbb{A}_{M/p_j^2}[x] + \mathbb{A}_{M/p_k^2}[x] + \mathbb{A}_{M/p_j p_k}[x] \\
&= p_j + p_k + (p_j - 1)(p_k - 1) \\
&= p_j p_k + 1.
\end{aligned}
$$

This, however, contradicts Lemma 2.3. □

Assume, without loss of generality, that $A_x \subset \ell_j(x)$. By Corollary 8.11, the pair (A, B) has a $(1, 2)$-cofibered structure in the p_j direction, with a cofiber in A at distance M/p_j^2 from x. By Lemma 8.7, we may shift the cofiber to x. Let A' be the set thus obtained, so that $A' \cap \Lambda$ contains all points of $A \cap \Lambda$ plus, additionally, the fiber $x * F_j \subset A'$. Moreover, A' is (T2)-equivalent to A, and $A' \oplus B = \mathbb{Z}_M$.

In this example, we do not get (T2)-equivalence to a standard set right away. Instead, the new set A' contains a structure we call a p_j-*corner* [24], consisting of two nonintersecting M-fibers in the p_i and p_k directions in Λ. We then have to work further with that structure to prove that, ultimately, A' (therefore A) is (T2)-equivalent to Λ.

9. Conjectures and open questions

9.1. Tiling reductions

We first consider the question of whether proving properties such as (T2) or, more generally, proving structure and classification results for tilings, could be accomplished by inductive arguments involving reduction to tilings of smaller groups.

Let $A \oplus B = \mathbb{Z}_M$ be a tiling, and assume for convenience that $0 \in A \cap B$. If M has at most two distinct prime factors, then Sands' theorem [37] states that at least one of A, B must be contained in $p\mathbb{Z}_M$ for some prime $p \mid M$. Thus we can always use Theorem 6.1 to decompose such a tiling into tilings of residue classes, with at least one of the sets A and B tiling $p\mathbb{Z}_M$. This was the route taken in [2].

Suppose now that $M = \prod_{i=1}^{K} p_i^{n_i}$, where p_i are distinct primes and $K \geq 3$. Sands' theorem no longer holds in that setting, with counterexamples given by Szabó [43] (see also [25]). However, it is conceivable that other inductive arguments, not based on Theorem 6.1, may still apply. For example, the following question is open:

Question 1. Let $A \oplus B = \mathbb{Z}_M$ with $M = \prod_{i=1}^{K} p_i^{n_i}$.

(i) *(Strong version)* Suppose that $\Phi_{p_i^{n_i}} \mid A$ for some $i \in \{1, 2, \ldots, K\}$. Is it always true that, in the notation of Theorem 6.5, we have $A'_{p_i} \oplus B = \mathbb{Z}_{M/p_i}$ for every translate A' of A?

(ii) *(Weak version)* Must there always exist some $i \in \{1, 2, \ldots, K\}$ such that either $A'_{p_i} \oplus B = \mathbb{Z}_{M/p_i}$ for every translate A' of A, or $A \oplus B'_{p_i} = \mathbb{Z}_{M/p_i}$ for every translate B' of B?

We do not know of any counterexamples to this. Szabó's examples [43] satisfy the conditions of Theorem 6.5, as do all tilings of period $M = p_1^2 p_2^2 p_3^2$, where p_1, p_2, p_3 are all odd [24].

Assume that $\Phi_{p_i^{n_i}} \mid A$ for some $i \in \{1, 2, \ldots, K\}$. By Proposition 3.4, property (T2) for B is equivalent to $A^\flat \oplus B = \mathbb{Z}_M$, where $A^\flat$ is the corresponding standard tiling complement. Heuristically, the slab reduction could be thought of as going part of the way in that direction, with the original tile A replaced by a new tile S which keeps some of the structure of A but, additionally, is periodic in the p_i direction. On the other hand, even if we assume a priori that both A and B satisfy (T2), this does not appear to imply the slab reduction in any obvious formal way. We do not know whether it is always possible to start with the original tiling and reach $A^\flat \oplus B = \mathbb{Z}_M$ via a sequence of slab reductions or other similar steps. While it does follow from [24] that all tilings of odd period $M = p_1^2 p_2^2 p_3^2$ satisfy the conditions of Theorem 6.5, this is obtained a posteriori as a consequence of our classification of all such tilings, with (T2) and the classification results obtained by other means in some cases.

It is worthwhile to describe Szabó-type examples in more detail. (For the purpose of this paper, we use a modification of Szabó's original construction in [43], which was set in a different abelian group but was nonetheless based on the same idea. See also the examples in [25] and [4].) We start with the standard tiling $A^\flat \oplus B^\flat = \mathbb{Z}_M$, where $M = p_1^2 p_2^2 p_3^2$, $A^\flat$ is the standard tiling set with $\Phi_{p_i^2} \mid A$ for all $i \in \{1, 2, 3\}$ and $B^\flat$ is the standard tiling set with $\Phi_{p_i} \mid B$ for all $i \in \{1, 2, 3\}$. We then use fiber shifts (Lemma 8.7) to modify $A^\flat$ so that for each i, one M-fiber in $A^\flat$ in the p_i direction is shifted by a distance M/p_i^2. For $K = 3$, the M-fibers in all three directions can be selected so that all three shifts can be performed independently without destroying the tiling property. This produces a new tiling $A \oplus B^\flat = \mathbb{Z}_M$ in which neither A nor $B^\flat$ is contained in a proper subgroup of $\mathbb{Z}_M$.

Noting that the pair $(A, B^\flat)$ in this construction has a $(1, 2)$-cofibered structure in all three directions, one might ask whether one of A or B must in fact be contained in a proper subgroup if no such obstructions are present. This motivates the following question:

Question 2. Let $A \oplus B = \mathbb{Z}_M$ with $M = \prod_{i=1}^{K} p_i^{n_i}$. Suppose that $\Phi_{p_i^{n_i}} \mid A$ for some $i \in \{1, 2, \ldots, K\}$. Is it always true that at least one of the following must hold?

(i) *(Subgroup tiling)* $A \subset \mathbb{Z}_{M/p_i}$.

(ii) *(Obstruction)* There exists an element $x \in \mathbb{Z}_M \setminus A$ such that $A_x \subset \ell_i(x)$. Furthermore, the pair (A, B) has a $(\mathcal{P}_A, \mathcal{P}_B)$-cofibered structure of depth at least 2, with $1 \in \mathcal{P}_A$.

It is possible that, at least for $K \geq 4$, more complicated obstructions may occur that cannot be reduced to 1-dimensional saturating spaces. However, the results of [24] show that the answer is affirmative if $M = p_1^2 p_2^2 p_3^2$. It seems reasonable to conjecture the following:

Conjecture 9.1. *The answers to Questions 1 (both versions) and 2 are affirmative when M has at most three distinct prime factors.*

Proposition 3.4 also relates the (T2) property to divisor sets, in the sense that B satisfies (T2) if and only if its divisor set $\mathrm{Div}(B)$ is disjoint from $\mathrm{Div}(A^\flat)$. The equivalence between Theorem 6.5(ii) and (iii) establishes a more granular result in this direction, by connecting a smaller family of differences in A to the corresponding family of cyclotomic polynomials. Specifically, if we write $S_i := \{m : p_i^{n_i} \mid m \mid M\}$ for a fixed $i \in \{1, \dots, K\}$, then Theorem 6.5 establishes a fundamental connection between the set of differences $m \in \mathrm{Div}(A) \cap S_i$ and the collection of all cyclotomic polynomials Φ_d dividing A, for $d \in S_i$. It would be interesting to know whether such relationships exist on the level of individual differences and cyclotomic polynomials. As an extreme example of a hypothetical result of this type, we state the following:

Conjecture 9.2. *If $\Phi_{p_i^{n_i}} \mid A$, then $M/p_i \notin \mathrm{Div}(B)$.*

This conjecture can be stated purely in terms of differences, since $\Phi_{p_i^{n_i}} \mid A$ if and only if $M/p_i \in \mathrm{Div}(A^\flat)$. It is obviously necessary in order for (T2) to hold, though not sufficient. Absent a proof of (T2) in its full generality, this might be an interesting direction to explore.

Our saturating-set techniques provide partial support for the conjecture, as follows. Suppose that $M/p_i \in \mathrm{Div}(B)$, with $(b - b', M) = M/p_i$ for some $b, b' \in B$. Suppose further that Conjecture 9.2 is true. Then $\Phi_{p_i^{n_i}} \nmid A$, so that $\Phi_{p_i^{n_i}} \mid B$. In particular,

$$\left| B \cap \Pi\left(y, p_i^{n_i}\right) \right| = \frac{1}{p_i} \left| B \cap \Pi\left(b, p_i^{n_i - 1}\right) \right|$$

for every $y \in \mathbb{Z}_M$ with $(y - b, M) = M/p_i$. We do not know how to prove this, but we can prove the weaker statement that $B \cap \Pi(y, p_i^{n_i}) \neq \emptyset$ for each such y. Indeed, if $y \in B$, this is obvious. If, on the other hand, $y \notin B$, then by inclusion (7.9) we have $B_y \subset \Pi(y, p_i^{n_i})$, and in particular $B \cap \Pi(y, p_i^{n_i})$ is nonempty.

We note that fibering plays a significant role in all our tiling arguments. For instance, if A is M-fibered in some direction, this is sufficient to apply slab reduction (see Remark 6.6). At the other extreme, if $\Phi_M \mid A$ but A fails to be M-fibered on some $D(M)$-grid, our strategy in [24] is to identify and use cofibered structures, which in particular implies fibering in B on a lower scale. Motivated by this, we conjecture the following:

Conjecture 9.3. *For every i there exists $1 \le \alpha_i < n_i$ such that either A or B is $M/p_i^{\alpha_i}$-fibered in the p_i direction. In particular, if M has three prime factors, $\Phi_M \mid A$ and there exists a $D(M)$-grid Λ such that $A \cap \Lambda$ is not fibered in any direction, then B is fibered in all directions on some scale. (This happens, for example, in Szabó's examples.)*

9.2. Saturating sets

We have seen in Lemma 8.10 and Corollary 8.11 that if $A_x \subset \ell_i(x)$ for some $i \in \{1, \dots, K\}$ and $x \in \mathbb{Z} \setminus A$, this implies a cofibered structure in (A, B). By Lemma 8.7, this allows us to shift M-fibers in A in the given direction. We use this in [24] to reduce $A \oplus B = \mathbb{Z}_M$ to (T2)-equivalent tilings $A' \oplus B = \mathbb{Z}_M$, where A' has additional regularity properties. It would therefore be interesting to either find a structure theorem (an analogue of Lemma 8.10) for saturating sets contained in higher-dimensional subspaces or, alternatively, to find a systematic way of adding geometric constraints on saturating sets until we find a cofibered structure.

In all examples where we have been able to determine saturating sets, we found that they enjoy pleasant 'splitting' properties. For example, suppose that $(x - a, M) = M/p_i$ for some $a \in A$ and $i \in \{1, \dots, K\}$. By inclusion (7.9), we have

$$A_x \subset \mathrm{Bispan}(x, a) = \Pi\left(x, p_i^{n_i}\right) \cup \Pi\left(a, p_i^{n_i}\right). \tag{9.1}$$

However, what actually tends to happen is that either $A_x \subset \Pi(x, p_i^{n_i})$ or $A_x \subset \Pi(a, p_i^{n_i})$. For instance, if $\mathbb{A}_{M/p_i}[a] > 0$, then $\mathbb{A}_{M/p_i}[x] \geq 2$ and

$$A_x \subset \Pi\left(x, p_i^{n_i}\right).$$

If, however, $\mathbb{B}_{M/p_i}[b] > 0$, then

$$A_{x,b} \subset \Pi\left(a, p_i^{n_i}\right).$$

For an example of a less-obvious situation where this happens, see, for example, [24, Lemma 9.18].

Similarly, suppose that $K = 3$ and set $x \in \mathbb{Z}_M$. Assume that there are two elements $a_i, a_j \in A$ such that $(x - a_i, M) = M/p_i$ and $(x - a_j, M) = M/p_j$, with $i, j \in \{1, 2, 3\}$ distinct. Then, by formula (7.9) again,

$$A_x \subset \mathrm{Bispan}(x, a_i) \cap \mathrm{Bispan}\left(x, a_j\right) = \ell_k(x) \cup \ell_k(a_i) \cup \ell_k\left(a_j\right) \cup \ell_k\left(x_{ij}\right),$$

where $x_{ij} \in \mathbb{Z}_M$ is the unique point such that $(x_{ij} - a_i, M) = M/p_j$ and $(x_{ij} - a_j, M) = M/p_i$. However, in all tiling examples that we have worked out, A_x is in fact contained in just one of these lines. An example of this type of situation is provided by [24, Lemma 4.6]. See also Lemma 8.14 for a different example where the initial geometric constraints restrict the saturating set to a union of two lines (inclusion 8.18), but then additional arguments show that only one of these lines may participate.

Returning to the 'two planes' situation as in inclusion (9.1), we can in fact say a little bit more. By inclusion (9.1), we have for any $b \in B$,

$$1 = \sum_{p_i^{n_i} | m} \frac{1}{\phi(M/m)} \left(\mathbb{A}_m[x]\mathbb{B}_m[b] + \mathbb{A}_{m/p_i}[x]\mathbb{B}_{m/p_i}[b]\right).$$

Suppose that $\mathbb{B}_m[b]$ and $\mathbb{B}_{m/p_i}[b]$ are both nonzero for some m with $p_i^{n_i} \mid m \mid M$. If there were an $a' \in A$ with $(x - a', M) \in \{m, m/p_i\}$, then we would also have $(a - a', M) \in \{m, m/p_i\}$, contradicting divisor exclusion. Moreover, if $\mathbb{B}_{m/p_i}[b] \neq 0$, then any $a' \in A$ with $(x - a', M) \in \{m, m/p_i\}$ must lie in the plane $\Pi(a, p_i^{n_i})$. Hence

$$1 = \sum_{p_i^{n_i} | m} \frac{1}{\phi(M/m)} \left(\delta_m \mathbb{A}_m[x]\mathbb{B}_m[b] + (1 - \delta_m)\mathbb{A}_m[a]\mathbb{B}_{m/p_i}[b]\right), \tag{9.2}$$

where $\delta_m \in \{0, 1\}$ for all $p_i^{n_i} \mid m$.

It appears reasonable to conjecture the following:

Conjecture 9.4. *Let $A \oplus B = \mathbb{Z}_M$ be a tiling, and assume that $(x - a, M) = M/p_i$ for some $a \in A$, $x \in \mathbb{Z}_M \setminus A$ and $i \in \{1, \ldots, K\}$. Then either $A_x \subset \Pi(x, p_i^{n_i})$ or $A_x \subset \Pi(a, p_i^{n_i})$. Furthermore, either $\delta_m = 1$ for all m or $\delta_m = 0$ for all m, depending only on the choice of $a \in A$ and $b \in B$.*

A similar reasoning, with only slightly more effort, applies to $A_{x,y}$ and $B_{y,x}$ as in formula (7.12) with $x \in \mathbb{Z}_M \setminus A$ and $y \in \mathbb{Z}_M \setminus B$.

9.3. Subspace bounds

The special case of Lemma 2.3 with $K = 3$ and $\alpha_i = 0$ is a simple but very effective tool in [24]. It would be useful to have similar bounds for lower-dimensional subspaces, for example lines in the three-prime case. In this regard, we formulate the following modest conjecture:

Conjecture 9.5. *Suppose that $p_i^{\alpha_i} \| |A|$ with $\alpha_i < n_i$. Then for all $x \in \mathbb{Z}_M$,*

$$|A \cap \ell_i(x)| < p_i^{n_i}. \tag{9.3}$$

This is clearly true when:

○ $p_i^{n_i}$ exceeds the plane bounds $\left| A \cap \Pi(x, p_j^{n_j}) \right|$ for $j \neq i$ and

○ A satisfies (T2) (in this case, $A \oplus B^\flat = \mathbb{Z}_M$ and there exists β_i so that $M/p_i^{\beta_i} \notin \text{Div}(A)$).

Conflicts of Interest: None.

References

[1] S. Bhattacharya, 'Periodicity and decidability of tilings of $\mathbb{Z}^2$', *Amer. J. Math.* **142**(1) (2020), 255–266.

[2] E. Coven and A. Meyerowitz, 'Tiling the integers with translates of one finite set', *J. Algebra* **212**(1) (1999), 161–174.

[3] N. G. de Bruijn, 'On the factorization of cyclic groups', *Indag. Math.* **15** (1953), 370–377.

[4] D. E. Dutkay and I. Kraus, 'On spectral sets of integers', in *Frames and Harmonic Analysis*, Contemporary Mathematics vol. 706 (American Mathematical Society, Providence, RI, 2018), 215–234.

[5] D. E. Dutkay and C.-K. Lai, 'Some reductions of the spectral set conjecture to integers', *Math. Proc. Cambridge Philos. Soc.* **156**(1) (2014), 123–135.

[6] T. Fallon, G. Kiss and G. Somlai, 'Spectral sets and tiles in $\mathbb{Z}_p^2 \times \mathbb{Z}_q^2$', Preprint, 2021, arXiv:2105.10575.

[7] T. Fallon, A. Mayeli and D. Villano, 'The Fuglede conjecture holds in F_p^3 for $p = 5, 7$', *Proc. Amer. Math. Soc.*, forthcoming.

[8] B. Farkas, M. Matolcsi and P. Móra, 'On Fuglede's conjecture and the existence of universal spectra', *J. Fourier Anal. Appl.* **12**(5) (2006), 483–494.

[9] B. Farkas and S. G. Révész, 'Tiles with no spectra in dimension 4', Math. Scand. **98**(1) (2006), 44–52.

[10] B. Fuglede, 'Commuting self-adjoint partial differential operators and a group-theoretic problem', *J. Funct. Anal.* **16** (1974), 101–121.

[11] A. Granville, I. Łaba and Y. Wang, 'A characterization of finite sets that tile the integers, Preprint, 2001, arXiv:math/0109127.

[12] R. Greenfeld and N. Lev, 'Fuglede's spectral set conjecture for convex polytopes', *Anal. PDE* **10**(6) (2017), 1497–1538.

[13] R. Greenfeld and T. Tao, 'The structure of translational tilings in $\mathbb{Z}^d$', *Discrete Anal.* 2021, Paper No. 16, 28 pp.

[14] A. Iosevich, N. Katz and T. Tao, 'The Fuglede spectral conjecture holds for convex planar domains', *Math. Res. Lett.* **10**(5-6) (2003), 559–569.

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

[16] G. Kiss, R. D. Malikiosis, G. Somlai and M. Vizer, 'On the discrete Fuglede and Pompeiu problems', *Anal. PDE* **13**(3) (2020), 765–788.

[17] G. Kiss, R. D. Malikiosis, G. Somlai and M. Vizer, 'Fuglede's conjecture holds for cyclic groups of order pqrs', Preprint, 2000, arXiv:2011.09578.

[18] G. Kiss and S. Somlai, 'Fuglede's conjecture holds on $\mathbb{Z}_p^2 \times \mathbb{Z}_q$', *Proc. Amer. Math. Soc.* **149**(10) (2021), 4181–4188.

[19] M. N. Kolountzakis and N. Lev, 'Tiling by translates of a function: results and open problems', *Discrete Anal.* 2021, Paper No. 12, 24 pp.

[20] M. N. Kolountzakis and M. Matolcsi, 'Complex Hadamard matrices and the spectral set conjecture', *Collect. Math.* **Extra** (2006), 281–291.

[21] M. N. Kolountzakis and M. Matolcsi, 'Tiles with no spectra', *Forum Math.* **18**(3) (2006), 519–528.

[22] S. Konyagin and I. Łaba, 'Spectra of certain types of polynomials and tiling the integers with translates of finite sets', *J. Number Theory* **103**(2) (2003), 267–280.

[23] I. Łaba, 'The spectral set conjecture and multiplicative properties of roots of polynomials', *J. London Math. Soc. (2)* **65** (2002), 661–671.

[24] I. Łaba and I. Londner, 'The Coven-Meyerowitz tiling conditions for 3 odd prime factors', Preprint, 2021, arXiv:2106.14044.

[25] J.C. Lagarias and S. Szabó, 'Universal spectra and Tijdeman's conjecture on factorization of cyclic groups', *J. Fourier Anal. Appl.* **1**(7) (2001), 63–70.

[26] J. C. Lagarias and Y. Wang, 'Tiling the line with translates of one tile', *Invent. Math.* **124**(1-3) (1996), 341–365.

[27] J. C. Lagarias and Y. Wang, 'Spectral sets and factorization of finite abelian groups', *J. Funct. Anal.* **145**(1) (1997), 73–98.

[28] T. Y. Lam and K. H. Leung, 'On vanishing sums of roots of unity', *J. Algebra* **224**(1) (2000), 91–109.

[29] N. Lev and M. Matolcsi, 'The Fuglede conjecture for convex domains is true in all dimensions', *Acta Math.*, forthcoming, arXiv:1904.12262.

[30] R. D. Malikiosis, '*On the structure of spectral and tiling subsets of cyclic groups*', Preprint, 2020, arXiv:2005.05800.

[31] R. D. Malikiosis and M. N. Kolountzakis, 'Fuglede's conjecture on cyclic groups of order $p^n q$', *Discrete Anal.* 2017, Paper No. 12, 16 pp.

[32] H. B. Mann, 'On linear relations between roots of unity', *Mathematika* **12**(2) (1965), 107–117.

[33] M. Matolcsi, 'Fuglede's conjecture fails in dimension 4', *Proc. Amer. Math. Soc.* **133**(10) (2005), 3021–3026.

[34] D. J. Newman, 'Tesselation of integers', *J. Number Theory* **9**(1) (1977), 107–111.

[35] L. Rédei, 'Über das Kreisteilungspolynom', *Acta Math. Hungar.* **5** (1954), 27–28.

[36] L. Rédei, 'Natürliche Basen des Kreisteilungskörpers', *Abh. Math. Sem. Univ. Hambg.* **23** (1959), 180–200.

[37] A. Sands, 'On Keller's conjecture for certain cyclic groups', *Proc. Edinb. Math. Soc.* (**2**) **22**(1) (1979).

[38] I. J. Schoenberg, 'A note on the cyclotomic polynomial', *Mathematika* **11** (1964), 131–136.

[39] R. Shi, 'Fuglede's conjecture holds on cyclic groups $\mathbb{Z}_{p^2qr}$', *Discrete Anal.* 2019, Paper No. 14, 14 pp.

[40] R. Shi, 'Equi-distribution on planes and spectral set conjecture on $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$', *J. Lond. Math. Soc. (2)* **102**(2) (2020), 1030–1046.

[41] G. Somlai, 'Spectral sets in $\mathbb{Z}_{p^2qr}$ tile', Preprint, 2019, arXiv:1907.04398.

[42] J. P. Steinberger, 'Minimal vanishing sums of roots of unity with large coefficients', *Proc. Lond. Math. Soc. (3)* **97**(3) (2008), 689–717.

[43] S. Szabó, 'A type of factorization of finite abelian groups', *Discrete Math.* **54**(1) (1985), 121–124.

[44] S. Szabó, *Topics in Factorization of Abelian Groups* (Hindustan Book Agency, Basel, 2004).

[45] T. Tao, 'Fuglede's conjecture is false in 5 and higher dimensions', *Math. Res. Lett.* **11**(2-3) (2004), 251–258.

[46] T. Tao, 'Some notes on the Coven-Meyerowitz conjecture' (2011). URL:https://terrytao.wordpress.com/2011/11/19/some-notes-on-the-coven-meyerowitz-conjecture/.

[47] R. Tijdeman, 'Decomposition of the integers as a direct sum of two subsets', in *Number Theory (Paris 1992–1993),* London Mathematical Society Lecture Note Series vol. 215 (Cambridge University Press, Cambridge, UK, 1995), 261–276.

[48] T. Zhang, 'Fuglede's conjecture holds in $\mathbb{Z}_p \times \mathbb{Z}_{p^n}$', Preprint, 2021, arXiv:2109:08400.