# Lower Bounds from Cyclotomic Divisors of Mask Polynomials

Gergely Kiss

Budapest Corvinus University and Alfréd Rényi Insitute of Mathematics

Joint work with Caleb Marshall, Izabella Łaba, Gábor Somlai

International Conference on Tiling and Fourier Bases
Xidian University, Xi'an
September 18, 2025

# Tilings of the integers



Let $A \subset \mathbb{Z}$ be a finite set.
We say that $A$ tiles $\mathbb{Z}$ (by translation) if there is a $T \subset \mathbb{Z}$ such that $\forall n \in \mathbb{Z}$ can be uniquely expressed as a sum $a + t = n$, with $a \in A$ and $t \in T$.

# Tilings of the integers



Let $A \subset \mathbb{Z}$ be a finite set.
We say that $A$ tiles $\mathbb{Z}$ (by translation) if there is a $T \subset \mathbb{Z}$ such that $\forall n \in \mathbb{Z}$ can be uniquely expressed as a sum $a + t = n$, with $a \in A$ and $t \in T$. This property we denote by $A \oplus T = \mathbb{Z}$.

# Tilings of the integers



Let $A \subset \mathbb{Z}$ be a finite set.
We say that $A$ tiles $\mathbb{Z}$ (by translation) if there is a $T \subset \mathbb{Z}$ such that $\forall n \in \mathbb{Z}$ can be uniquely expressed as a sum $a + t = n$, with $a \in A$ and $t \in T$. This property we denote by $A \oplus T = \mathbb{Z}$.

**Proposition (Newman, Hajós)**

*$T$ is periodic, i.e. $\exists M \in \mathbb{N}$ and a finite set $B \in \mathbb{Z}$ such that $T = B \oplus M\mathbb{Z}$.*

# Tilings of the integers



Let $A \subset \mathbb{Z}$ be a finite set.
We say that $A$ tiles $\mathbb{Z}$ (by translation) if there is a $T \subset \mathbb{Z}$ such that $\forall n \in \mathbb{Z}$ can be uniquely expressed as a sum $a + t = n$, with $a \in A$ and $t \in T$. This property we denote by $A \oplus T = \mathbb{Z}$.

**Proposition (Newman, Hajós)**

*$T$ is periodic, i.e. $\exists M \in \mathbb{N}$ and a finite set $B \in \mathbb{Z}$ such that $T = B \oplus M\mathbb{Z}$.*

For such a $B$ we have $|A||B| = M$ and $A \oplus B = \mathbb{Z}_M$. All results on $\mathbb{Z}_M$ can be translated back to the integer setting. Thus, from now on, we will work on $\mathbb{Z}_M$.

For any $s|M$, we have $\Phi_s \mid (X^M - 1)$, so that $\Phi_s|A$ if and only if $\Phi_s \mid (A \bmod M)$.

Note that $A \bmod M$ need not be a set hence we introduce the multiset notation.

- $\mathcal{M}(\mathbb{Z}_M)$ denote the set of all multisets in $\mathbb{Z}_M$ with weights in $\mathbb{Z}$ (so that both positive and negative weights are allowed)
- $\mathcal{M}^+(\mathbb{Z}_M)$ if we only allow positive weights.

For $a \in \mathbb{Z}_M$, let $w_A(a)$ denote the weight of $a$ in $A$.

The mask polynomial of the multiset $A$ by

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

In particular, $A \in \mathcal{M}(\mathbb{Z}_M)$ is a set if and only if $w_A(x) \in \{0, 1\}$ for all $x \in \mathbb{Z}_M$.

Using the mask polynomials $A \oplus B = \mathbb{Z}_M$ is equivalent to

$$A(X)B(X) = 1 + X + \ldots + X^{M-1} \mod (X^M - 1).$$

Using the mask polynomials $A \oplus B = \mathbb{Z}_M$ is equivalent to

$$A(X)B(X) = 1 + X + \ldots + X^{M-1} \mod (X^M - 1).$$

Equivalently,

$$|A||B| = M \text{ and } \forall 1 \neq m|M, \Phi_m(X) \mid A(X) \text{ or } \Phi_m(X) \mid B(X),$$

where $\Phi_m$ be the cyclotomic polynomial of order $m$.

Using the mask polynomials $A \oplus B = \mathbb{Z}_M$ is equivalent to

$$A(X)B(X) = 1 + X + \ldots + X^{M-1} \mod (X^M - 1).$$

Equivalently,

$$|A||B| = M \text{ and } \forall 1 \neq m|M, \Phi_m(X) \mid A(X) \text{ or } \Phi_m(X) \mid B(X),$$

where $\Phi_m$ be the cyclotomic polynomial of order $m$.

Given a set $S = \{s_1, s_2, \ldots, s_k\}$ of divisors of $M$.

Our goal would be to decide whether there exists a set / tile $A$ satisfying $\Phi_{s_j}(X) \mid A(X)$ $(1 \leq j \leq k)$, and

$$|A| = A(1) = \prod_{p_i^{m_i} \in S} \Phi_{p_i^{m_i}}(1).$$

# Coven-Meyerowitz theorem



Theorem (Coven and Meyerowitz, 1999)

*Let $A$ be a finite set of integers and*

$$S_A^* := \{p^\alpha \,:\, p^\alpha \text{ is a prime power and } \Phi_{p^\alpha}(X) | A(X)\}.$$

*Consider the following two conditions*
*(T1)* $|A| = A(1) = \prod_{s \in S_A^*} \Phi_s(1)$,
*(T2) if* $s_1, \ldots, s_k \in S_A^*$ *are powers of different primes, then* $\Phi_{s_1 \ldots s_k}(X) | A(X)$.

# Coven-Meyerowitz theorem



Theorem (Coven and Meyerowitz, 1999)

*Let $A$ be a finite set of integers and*

$$S_A^* := \{p^\alpha \,:\, p^\alpha \text{ is a prime power and } \Phi_{p^\alpha}(X) | A(X)\}.$$

*Consider the following two conditions*
*(T1)* $|A| = A(1) = \prod_{s \in S_A^*} \Phi_s(1)$,
*(T2) if* $s_1, \ldots, s_k \in S_A^*$ *are powers of different primes, then* $\Phi_{s_1 \ldots s_k}(X) | A(X)$.
*Then*

- *If $A$ satisfies both (T1) and (T2) then $A$ tiles $\mathbb{Z}$.*

# Coven-Meyerowitz theorem



## Theorem (Coven and Meyerowitz, 1999)

*Let $A$ be a finite set of integers and*

$$S_A^* := \{p^\alpha \ : \ p^\alpha \ \text{ is a prime power and } \ \Phi_{p^\alpha}(X) | A(X)\}.$$

*Consider the following two conditions*
*(T1)* $|A| = A(1) = \prod_{s \in S_A^*} \Phi_s(1)$,
*(T2) if* $s_1, \ldots, s_k \in S_A^*$ *are powers of different primes, then* $\Phi_{s_1 \ldots s_k}(X) | A(X)$.
*Then*

- *If $A$ satisfies both (T1) and (T2) then $A$ tiles $\mathbb{Z}$.*
- *If $A$ tiles $\mathbb{Z}$ then it must satisfy (T1).*

# Coven-Meyerowitz theorem



Theorem (Coven and Meyerowitz, 1999)

*Let $A$ be a finite set of integers and*

$$S_A^* := \{p^\alpha : p^\alpha \text{ is a prime power and } \Phi_{p^\alpha}(X) | A(X)\}.$$

*Consider the following two conditions*
*(T1)* $|A| = A(1) = \prod_{s \in S_A^*} \Phi_s(1)$,
*(T2) if* $s_1, \ldots, s_k \in S_A^*$ *are powers of different primes, then* $\Phi_{s_1 \ldots s_k}(X) | A(X)$.
*Then*

- *If $A$ satisfies both (T1) and (T2) then $A$ tiles $\mathbb{Z}$.*
- *If $A$ tiles $\mathbb{Z}$ then it must satisfy (T1).*
- *If $A$ tiles $\mathbb{Z}$, and $|A|$ has at most two prime factors, then it satisfies (T2).*

# Conjecture and generalization



**Conjecture (Coven-Meyerowitz conjecture)**

*A set tiles the integers if and only if it satisfies (T1) and (T2).*

It is still open.

# Conjecture and generalization



**Conjecture (Coven-Meyerowitz conjecture)**

*A set tiles the integers if and only if it satisfies (T1) and (T2).*

It is still open. But it is known to be true in some special cases.

# Conjecture and generalization



**Conjecture (Coven-Meyerowitz conjecture)**

*A set tiles the integers if and only if it satisfies (T1) and (T2).*

It is still open. But it is known to be true in some special cases.

**Theorem (Łaba-Londner, 2025)**

*The Coven-Meyerowitz conjecture is true in $\mathbb{Z}_M$ if any of the following conditions holds.*

- $M \mid p_1^m p_2^n \prod_{i=3}^{L} p_i$,
- $M \mid p_1^2 p_2^2 p_3^2 \prod_{i=4}^{L} p_i$,

*where $p_1, p_2, p_3, p_i$'s are distinct primes.*

# A strategy to verify CM-conjecture



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

# A strategy to verify CM-conjecture



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

**Definition**

Let $A \subset \mathbb{Z}_M$, and let $\Phi_s(X) \mid A(X)$ for some $s \mid M$. We say that $\Phi_s$ is an *unsupported divisor of $A$* if:

(i) for every prime $p$ such that $p \mid s$, we have $p \mid |A|$,

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

# Questions



## Question (A)

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

# Questions



## Question (A)

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

## Question (B)

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

# Questions 

## Question (A)

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

## Question (B)

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

## Proposition

*Let $A \oplus B = \mathbb{Z}_M$ such that each prime factor of $M$ divides both $|A|$ and $|B|$.*

(i) *If the answer to Question (A) is negative for this value of $M$, then both sets $A$ and $B$ satisfy (T2).*

(ii) *If the answer to Question (B) is negative for this value of $M$, then, if (T2) holds for $A$, it must also hold for $B$.*

**Theorem**

*There exists* $M = p^n q^m$ *and a nonempty set* $A \subset \mathbb{Z}_M$ *satisfying (T1), and* $A(X)$ *has at least one unsupported cyclotomic divisor.*

### Theorem

*There exists* $M = p^n q^m$ *and a nonempty set* $A \subset \mathbb{Z}_M$ *satisfying (T1), and* $A(X)$ *has at least one unsupported cyclotomic divisor.*

### Theorem

*There exists* $M = p_1^4 p_2^4 p_3^4 p_4^4$ *and a nonempty set* $A \subset \mathbb{Z}_M$ *satisfying both (T1) and (T2), and* $A(X)$ *has at least one unsupported cyclotomic divisor.*

**Theorem**

*There exists $M = p^n q^m$ and a nonempty set $A \subset \mathbb{Z}_M$ satisfying (T1), and $A(X)$ has at least one unsupported cyclotomic divisor.*

**Theorem**

*There exists $M = p_1^4 p_2^4 p_3^4 p_4^4$ and a nonempty set $A \subset \mathbb{Z}_M$ satisfying both (T1) and (T2), and $A(X)$ has at least one unsupported cyclotomic divisor.*

However, in the 'two-prime-divisor' case we can prove the following.

**Theorem**

*Let $M = p^n q^m$. Assume that a nonempty set $A \subset \mathbb{Z}_M$ satisfies (T1) and (T2). Then $A(X)$ cannot have unsupported cyclotomic divisors.*

# Lower bound for the size of sets with given cyclotomic divisors



Let $S = \{s_1, s_2, \ldots, s_k\}$ be the divisors of $M$, and $A$ be a nonempty set in $\mathbb{Z}_M$ such that $\Phi_{s_j}(X) \mid A(X)$ $(1 \leq j \leq k)$.

**Question**

*What is the minimal size of A?*

# Lower bound for the size of sets with given cyclotomic divisors



Let $S = \{s_1, s_2, \ldots, s_k\}$ be the divisors of $M$, and $A$ be a nonempty set in $\mathbb{Z}_M$ such that $\Phi_{s_j}(X) \mid A(X)$ $(1 \leq j \leq k)$.

**Question**

*What is the minimal size of A? i.e,*

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

Motivation:

**Proposition (Lam and Leung)**

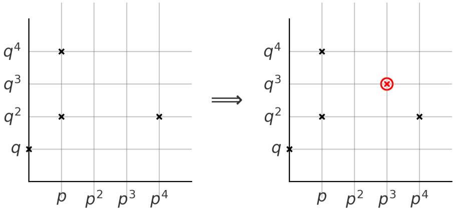
*If $\Phi_s(X)|A(X)$ for some $1 < s \in \mathbb{N}$, then*

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

# Illustration



Take some cyclomatic divisors of $M = p^4q^4$ and we add an extra divisor as below.




$S = \{q, pq^2, pq^4, p^4q^2\}$

What is the minimum size of $A$ s.t. $\Phi_q\Phi_{pq^2}\Phi_{pq^4}\Phi_{p^4q^2} \mid A(X)$?

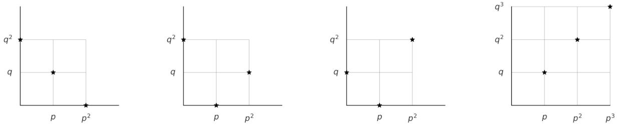
Is it smaller than the min. size of $A$ if $\Phi_{p^3q^3} \mid A(X)$ is added?

$$\text{Is MIN}(S) < \text{MIN}(S \cup \{p^3q^3\})?$$

# Examples



If $|S| = |\{s_1, s_2\}| = 2$ such that $s_i \nmid s_j$ $(i \neq j \in \{1,2\})$, then it is easy to show that $\mathrm{MIN}(S) \geq (\min(p,q))^2$.




In the first three cases we get that $\mathrm{MIN}(S) \geq pq \min(p,q)$.

In the last case $\Phi_{pq}\Phi_{p^2q^2}\Phi_{p^3q^3} \mid A(X)$ holds and we get that $\mathrm{MIN}(S) \geq (\min(p,q))^3$.

# Generalizations I.



**Proposition**

*Let* $A \in \mathcal{M}^+(\mathbb{Z}_M)$ *with* $M = p^{n_1} q^{n_2}$. *Assume that* $\Phi_{p^{m_1}} \cdots \Phi_{p^{m_r}} \Phi_{p^\alpha q^\beta} \Phi_{q^\gamma} | A$

- *for some* $1 \leq \alpha < m_1 < \cdots < m_r \leq n_1$ *and* $1 \leq \beta \neq \gamma \leq n_2$,
- *for some* $1 \leq m_1 < \cdots < m_r < \alpha \leq n_1$ *and* $1 \leq \gamma < \beta \leq n_2$.

*Then* $|A| \geq p^r q \min(p, q)$. *Hence* $\mathrm{MIN}(S) \geq p^r q \min(p, q)$.

# Generalization II.- Diagonal case



Let $s = \prod_{i=1}^{L} p_i^{\beta_i}$, then $D(s) = \frac{s}{\prod_{i=1}^{L} p_i}$

**Theorem**

*Let* $M = \prod_{i=1}^{L} p_i^{n_i}$. *Assume that* $S = \{s_1, \ldots, s_m\}$ *satisfies* $s_j \mid M$ *and*

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

*Then* $\mathrm{MIN}(S) \geq \prod_{j=1}^{m} \min_{i:p_i|s_j} p_i$

# Examples without size increase



**Proposition**

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

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

*and* $|A| = p^3q^3 = 216$*.*

**Proposition**

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

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

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

# Fibers, fibered sets



Let $N \mid M$, and let $p_i$ be a prime such that $p_i \mid N$. We define

$$F_i^N(X) = \Phi_{p_i}(X^{N/p_i}) = 1 + X^{N/p_i} + \cdots + X^{(p_i-1)N/p_i},$$

which the mask polynomial of the set
$F_i^N = \{0, N/p_i, \ldots, (p_i - 1)N/p_i\} \mod N$.

# Fibers, fibered sets



Let $N \mid M$, and let $p_i$ be a prime such that $p_i \mid N$. We define

$$F_i^N(X) = \Phi_{p_i}(X^{N/p_i}) = 1 + X^{N/p_i} + \cdots + X^{(p_i-1)N/p_i},$$

which the mask polynomial of the set
$F_i^N = \{0, N/p_i, \ldots, (p_i - 1)N/p_i\} \mod N$.

A *$p_i$-fiber on scale $N$* is a translate of $F_i^N$.

# Fibers, fibered sets



Let $N \mid M$, and let $p_i$ be a prime such that $p_i \mid N$. We define

$$F_i^N(X) = \Phi_{p_i}(X^{N/p_i}) = 1 + X^{N/p_i} + \cdots + X^{(p_i-1)N/p_i},$$

which the mask polynomial of the set
$F_i^N = \{0, N/p_i, \ldots, (p_i - 1)N/p_i\} \mod N$.

A *$p_i$-fiber on scale $N$* is a translate of $F_i^N$.

$A \subset \mathbb{Z}_M$ is *fibered* on scale $N$ if there exists a prime $p_i | N$ and there exists a polynomial $Q(X)$ with nonnegative integer coefficients such that

$$Q(X)F_i^N(X) \equiv A(X) \mod x^N - 1.$$

# de Bruin-Rédei-Schoenberg theorem



**Theorem**

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

(i) $\Phi_N(X) | A(X)$,

(ii) *A mod N is a linear combination of N-fibers, so that*

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

*where $P_i(X)$ have integer coefficients.*

**Proposition (de Bruin, Lam-Leung)**

*Let $A \in \mathcal{M}^+(\mathbb{Z}_M)$. Assume that $\Phi_N | A$, where $N$ has two distinct prime factors $p_1, p_2$. Then*

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

*where $P_1, P_2$ are polynomials with nonnegative coefficients.*

# Long fibers



**Definition**

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

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

We refer to $p_i^\alpha$-fibers with $\alpha > 1$ as *long fibers* in the $i$ direction.

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

# Generalization of de Bruin-Rédei-Schoenberg theorem



### Proposition

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

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

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

# Truncation I.



The truncation procedure allows us to reduce proving lower bounds on MIN($S$) to proving similar bounds with $S$ replaced by a simpler set.

In order to discuss the statement we need the following definition.

**Definition**

Let $S$ be the subset of the div. of $M$ and $1 \leq i \leq K$ the number of prim div. of $M$, we define

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

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

$$\mathrm{EXP}_i(S) := \{\alpha_{i,1}, \cdots, \alpha_{i,E_i}\}, \quad 1 \leq \alpha_{i,1} < \cdots < \alpha_{i,E_i}.$$

# Truncation II.



**Proposition (Truncations)**

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

(i) $A'(1) = A(1)$.

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

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

# Truncation- An example



Suppose that $\Phi_s | A$ for all $s \in S$, where

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

Then, $\mathrm{EXP}_1(S) = \{3, 10\}$ and $\mathrm{EXP}_2(S) = \{2, 4, 10\}$ so that $M' := p_1^{E_1} p_2^{E_2} = p_1^2 p_2^3$.

Then the truncation procedure furnishes a multiset $A' \in \mathcal{M}(\mathbb{Z}_{p_1^2 p_2^3})$ such that $A'(1) = A(1)$ and $\Phi_s | A'$ for all $s \in S' := \{p_1, p_2, p_2^2, p_1 p_2^2, p_1^2, p_2^3 p_1^2 p_2^3\}$.

The exponent sets associated to $A'$ are $\{1, 2\}$ and $\{1, 2, 3\}$, with no gaps.

# The cyclotomic divisors of $A$ and $A'$



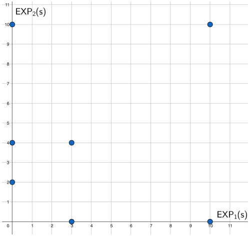



Figure: The cyclotomic divisors of $A$

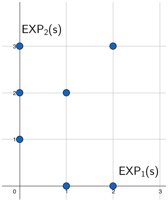



Figure: The cyclotomic divisors of $A'$

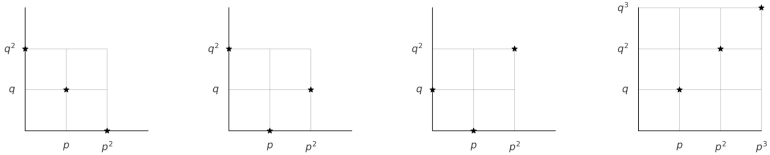
## Theorem

*Let $M = p^{n_1} q^{n_2}$, and let $S = \{s_1, s_2, s_3\}$ and $s_i \mid s_j$ for $i \neq j \in \{1, 2, 3\}$. Then*

$$\mathrm{MIN}(S) \geq (\min(p, q))^3$$

.

**Sketch of proof.** By the truncation procedure and further reduction, we can assume that all of the exponents are at most 2 or we have the diagonal case. So we get the following four cases (up to symmetry):



In our example $M = p^n q^m$ with $n \geq 9$ and $m \geq 6$, and $p = 2, q = 3$

First we define a multiset $B \in \mathcal{M}^+(\mathbb{Z}_{pq})$ $(p = 2, q = 3)$.

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

Each column sum is divisible by 27 and each row sum by 8.

In our example $M = p^n q^m$ with $n \geq 9$ and $m \geq 6$, and $p = 2, q = 3$

First we define a multiset $B \in \mathcal{M}^+(\mathbb{Z}_{pq})$ $(p = 2, q = 3)$.

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

Each column sum is divisible by 27 and each row sum by 8.

$B$ is a sum of $p$- and $q$-fibers.

Now we construct a set $A \subset \mathbb{Z}_M$ such that $A \equiv B \mod pq$.

As we have $\Phi_{p^n}\Phi_{p^{n-1}}\Phi_{p^{n-2}} \mid A(X)$, $A \mod p^n$ must be the union of long $p^3$-fibers on scale $M$. $A$ has to be a set, which is guaranteed if they are disjoint.

If $n \geq 9$, then we have enough space for that.

$\Phi_{q^m}\Phi_{q^{m-1}}\Phi_{q^{m-2}} \mid A(X)$ implies that $A \mod q^m$ has to be the union of (disjoint) long $q^3$-fibers.

If $m \geq 6$, then they can be taken to be disjoint.

# $\Phi_p \Phi_{p^2} \Phi_{p^3} \Phi_q \Phi_{q^2} \Phi_M \mid A(X)$ and $|A| = p^3 q^2 = 72$

Now $M = p^4 q^4$, $p = 2, q = 3$.

The following table represents a multiset $B \in \mathcal{M}^+(\mathbb{Z}_{72})$, where the cyclic group $\mathbb{Z}_{72}$ is written as $\mathbb{Z}_8 \oplus \mathbb{Z}_9$

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 5 | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 2 |
| 3 | 4 | 0 | 0 | 0 | 2 | 0 | 0 | 0 |
| 0 | 0 | 5 | 2 | 0 | 0 | 0 | 0 | 2 |
| 0 | 0 | 3 | 2 | 0 | 0 | 0 | 4 | 0 |
| 0 | 0 | 0 | 0 | 5 | 2 | 0 | 0 | 2 |
| 0 | 4 | 0 | 0 | 3 | 2 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 5 | 2 | 2 |
| 0 | 0 | 0 | 4 | 0 | 0 | 3 | 2 | 0 |

The entries in each column add up to 8, and the entries in each row add up to 9. This guarantees that

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

Now we construct a set $A \subset \mathbb{Z}_M$ such that $B \equiv A \bmod p^3 q^2$ and $\Phi_M \mid A$.

Each positive entry (2, 3, 4, 5) in the table is a nonnegative integer coefficient linear combination of 2 and 3. Hence, we may define $A$ is each $\mathbb{Z}_{pq^2}$ coset to be either just a single 2-fiber, or a single 3-fiber, or two 2-fibers, or a 3-fiber and a 2-fiber, where each fiber is on scale $M$.

If there is two fibers in one $\mathbb{Z}_{pq^2}$ coset, we place them in different $\mathbb{Z}_{pq}$ cosets of it, guaranteeing that they do not overlap.

Hence $A$ is a set satisfying the requirements.

# Possible generalization



The previous construction can be extended to any primes $p \neq q$.

**Theorem**

*Let $p, q$ be any two distinct primes. We can choose $a, b, n, m \in \mathbb{N}$ ($a << n, b << m$) large enough so that there is a set $A$ of size $|A| = p^a q^b$ that satisfies*

$$\Phi_p \Phi_{p^2} \cdots \Phi_{p^a} \Phi_q \Phi_{q^2} \cdots \Phi_{q^b} \Phi_{p^n q^m} \mid A.$$

# Further generalization



Two natural directions of generalization.

- *simultaneous divisibility* by a block of the form

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

  where $L_0 = p^\alpha q^\beta \mid M = p^n q^m$ by replacing the single $p$- and $q$-fibers with long $p^{n-\alpha+1}$- and $q^{m-\beta+1}$-fibers.
- The construction can also be extended inductively to the case of *arbitrary finite sets of primes* $\{p_1, \ldots, p_r\}$, provided that the parameters involved are chosen sufficiently large.

# (T2) lower bound



**Theorem**

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

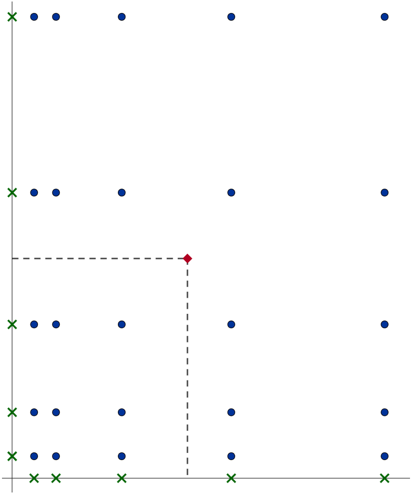
$$A(1) > \prod_{s \in S_A^*} \Phi_s(1), \tag{2}$$

*where $S_A^*$ is the set of prime powers $p^\alpha$ such that $\Phi_{p^\alpha}(X) \mid A(X)$*

In other words, if $A \in \mathcal{M}^+(\mathbb{Z}_{p^m q^n})$ satisfies $(T2)$ and also has an unsupported divisor $\Phi_N(X) \mid A(X)$. Then $A$ has the size increase given in (2).

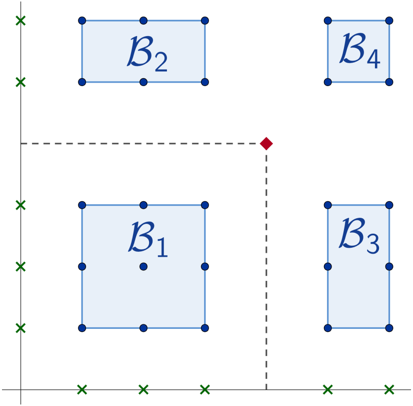
# The original setup





# The truncated version





**Corollary**

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

If $A \oplus B$ is a tile of $\mathbb{Z}_M$ for $M = p^m q^n$, and $A$ satisfies (T2), then $B$ also satisfies (T2).

**Question ('weaker' Coven-Meyerowitz conjecture)**

*Is it true that whenever* $A \oplus B$ *is a tile of a cyclic group and* $A$ *satisfies (T2), then* $B$ *also satisfies (T2)?*

# Negative results in 4D



**Theorem**

*Let* $N = p_1 p_2 p_3 p_4$ *and* $M = N^4$*, where*

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

*Then there exists a set* $A \subset \mathbb{Z}_M$ *such that:*

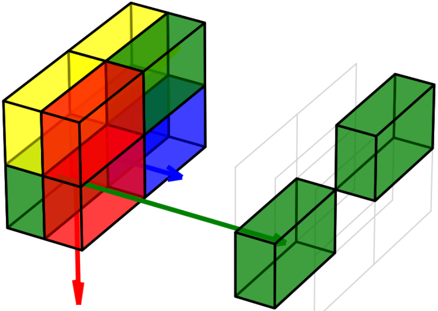
(i) *the prime power cyclotomic divisors of* $A(X)$ *are* $\Phi_{p_i^\alpha}(X)$ *for all* $i = 1, 2, 3, 4$ *and* $\alpha = 2, 3, 4$*,*

(ii) *A satisfies both (T1) and (T2), so that in particular we have* $|A| = N^3$*,*

(iii) *additionally,* $A(X)$ *has the unsupported cyclotomic divisor* $\Phi_N(X)$*.*

# Tricky 4D-fiber shift





# Properties



- Let $A'$ be a $\mathbb{Z}_N^3$ coset, hence $A' = N^3$.
- Originally, we have $\Phi_m \mid A'(X)$ for $m = p_i^k$ ($i \in \{1, 2, 3, 4\}$,$k \in \{2, 3, 4\}$), and all (T2) divisors given by them.
- The shifted set $A$ preserves this divisibility.
- We divide each side such that the shifted part in the $p_i$-direction is divisible by $p_i$, and each $\mathbb{Z}_M/p_i$ coset we shift the same number of $p_i^3$-fibers.
- Thus the set is the sum of $p_i$-fibers, hence $\Phi_N \mid A$.

# Final remarks



- The standard set (which takes one point from each $\mathbb{Z}_{N^3}$-coset) is a tiling complement but it satisfies $(T2)$.
- It can be modified such that $\Phi_s \mid B(X)$ whenever $s|N$ and $s \neq N$, and $\Phi_N \nmid B(X)$ (thus (T2) fails for the set $B$).
- However we cannot guarantee that $A$ tiles with $B$, namely we cannot ensure e.g. that $\Phi_{p_1 p_2 p_3^2 p_4^2} \mid A(X)B(X)$ holds.

# Final remarks



- The standard set (which takes one point from each $\mathbb{Z}_{N^3}$-coset) is a tiling complement but it satisfies $(T2)$.
- It can be modified such that $\Phi_s \mid B(X)$ whenever $s|N$ and $s \neq N$, and $\Phi_N \nmid B(X)$ (thus (T2) fails for the set $B$).
- However we cannot guarantee that $A$ tiles with $B$, namely we cannot ensure e.g. that $\Phi_{p_1 p_2 p_3^2 p_4^2} \mid A(X)B(X)$ holds.

**Question ('weaker' Coven-Meyerowitz conjecture)**

*Is it true that whenever $A \oplus B$ is a tile of a cyclic group and $A$ satisfies (T2), then $B$ also satisfies (T2)?*

Thank you for your kind attention.