Erdős covering systems

Robert Morris
IMPA, Rio de Janeiro

(Based on joint work with Paul Balister, Béla Bollobás, Julian Sahasrabudhe and Marius Tiba)

University of Oxford, March 31st, 2020

What is a covering system?

What is a covering system?

Definition (Erdős, 1950)

A *covering system* is a finite collection $A_1, \ldots, A_k$ of arithmetic progressions that cover the integers, that is, $A_1 \cup \cdots \cup A_k = \mathbb{Z}$.

What is a covering system?

Definition (Erdős, 1950)

A *covering system* is a finite collection $A_1, \ldots, A_k$ of arithmetic progressions that cover the integers, that is, $A_1 \cup \cdots \cup A_k = \mathbb{Z}$.

Erdős was interested in covering systems with *distinct* moduli.

What is a covering system?

Definition (Erdős, 1950)

A *covering system* is a finite collection $A_1, \ldots, A_k$ of arithmetic progressions that cover the integers, that is, $A_1 \cup \cdots \cup A_k = \mathbb{Z}$.

Erdős was interested in covering systems with *distinct* moduli.

For example:

$$\{0 \pmod 2\}, \; \{0 \pmod 3\}, \; \{1 \pmod 4\}, \; \{5 \pmod 6\}, \; \{7 \pmod{12}\}.$$

What is a covering system?

Definition (Erdős, 1950)

A *covering system* is a finite collection $A_1, \ldots, A_k$ of arithmetic progressions that cover the integers, that is, $A_1 \cup \cdots \cup A_k = \mathbb{Z}$.

Erdős was interested in covering systems with *distinct* moduli.

For example:

$$\{0 \pmod 2\}, \{0 \pmod 3\}, \{1 \pmod 4\}, \{5 \pmod 6\}, \{7 \pmod{12}\}.$$

8	5	2	11
4	1	10	7
0	9	6	3

What is a covering system?

Definition (Erdős, 1950)

A *covering system* is a finite collection $A_1, \ldots, A_k$ of arithmetic progressions that cover the integers, that is, $A_1 \cup \cdots \cup A_k = \mathbb{Z}$.

Erdős was interested in covering systems with *distinct* moduli.

For example:

$$\{0 \pmod 2\},\ \{0 \pmod 3\},\ \{1 \pmod 4\},\ \{5 \pmod 6\},\ \{7 \pmod{12}\}.$$

●	5	●	11
●	1	●	7
●	9	●	3

What is a covering system?

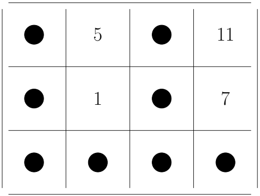
Definition (Erdős, 1950)

A *covering system* is a finite collection $A_1, \ldots, A_k$ of arithmetic progressions that cover the integers, that is, $A_1 \cup \cdots \cup A_k = \mathbb{Z}$.

Erdős was interested in covering systems with *distinct* moduli.

For example:

$\{0 \pmod 2\}$, $\{0 \pmod 3\}$, $\{1 \pmod 4\}$, $\{5 \pmod 6\}$, $\{7 \pmod{12}\}$.



What is a covering system?

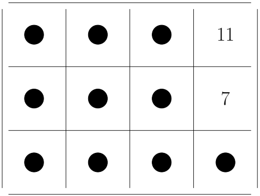
Definition (Erdős, 1950)

A *covering system* is a finite collection $A_1, \dots, A_k$ of arithmetic progressions that cover the integers, that is, $A_1 \cup \cdots \cup A_k = \mathbb{Z}$.

Erdős was interested in covering systems with *distinct* moduli.

For example:

$$\{0 \pmod{2}\}, \{0 \pmod{3}\}, \{1 \pmod{4}\}, \{5 \pmod{6}\}, \{7 \pmod{12}\}.$$



What is a covering system?

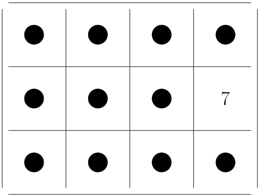
Definition (Erdős, 1950)

A *covering system* is a finite collection $A_1, \ldots, A_k$ of arithmetic progressions that cover the integers, that is, $A_1 \cup \cdots \cup A_k = \mathbb{Z}$.

Erdős was interested in covering systems with *distinct* moduli.

For example:

$$\{0 \pmod 2\},\ \{0 \pmod 3\},\ \{1 \pmod 4\},\ \{5 \pmod 6\},\ \{7 \pmod{12}\}.$$



What is a covering system?

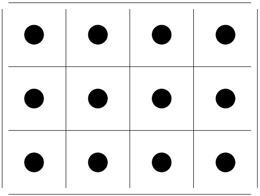
Definition (Erdős, 1950)

A *covering system* is a finite collection $A_1, \ldots, A_k$ of arithmetic progressions that cover the integers, that is, $A_1 \cup \cdots \cup A_k = \mathbb{Z}$.

Erdős was interested in covering systems with *distinct* moduli.

For example:

$$\{0 \pmod 2\},\ \{0 \pmod 3\},\ \{1 \pmod 4\},\ \{5 \pmod 6\},\ \{7 \pmod{12}\}.$$



What is a covering system?

Definition (Erdős, 1950)

A *covering system* is a finite collection $A_1, \ldots, A_k$ of arithmetic progressions that cover the integers, that is, $A_1 \cup \cdots \cup A_k = \mathbb{Z}$.

Erdős was interested in covering systems with *distinct* moduli.

For example:

$$\{0 \pmod{2}\}, \{0 \pmod{3}\}, \{1 \pmod{4}\}, \{5 \pmod{6}\}, \{7 \pmod{12}\}.$$

Erdős used a similarly simple covering system to answer a question of Romanoff (and refute a conjecture of de Polignac), by showing that not all odd numbers are of the form $2^k + p$, where p is either 1 or prime.

Some questions about covering systems

Some questions about covering systems

The minimum modulus problem (Erdős, 1950)

Do there exist covering systems with distinct moduli such that the minimum modulus is arbitrarily large?

Some questions about covering systems

The minimum modulus problem (Erdős, 1950)

Do there exist covering systems with distinct moduli such that the minimum modulus is arbitrarily large?

Question (Erdős, 1952)

How many minimal covering systems of size n *are there?*

Some questions about covering systems

The minimum modulus problem (Erdős, 1950)

Do there exist covering systems with distinct moduli such that the minimum modulus is arbitrarily large?

Question (Erdős, 1952)

How many minimal covering systems of size n are there?

Conjecture (Erdős and Graham, 1980)

If the moduli of a system of arithmetic progressions are distinct and lie in the interval $[n, Cn]$, where $n \geqslant n_0(C)$ is sufficiently large, then the uncovered set has density at least δ for some $\delta = \delta(C) > 0$.

The number of minimal covering systems

Question (Erdős, 1952)

How many minimal covering systems of size n are there?

The number of minimal covering systems

Question (Erdős, 1952)

How many minimal covering systems of size n are there?

Erdős gave a simple proof that there are only finitely many minimal covering systems of size n.

The number of minimal covering systems

Question (Erdős, 1952)

How many minimal covering systems of size n are there?

Erdős gave a simple proof that there are only finitely many minimal covering systems of size n. His bound was doubly exponential.

The number of minimal covering systems

Question (Erdős, 1952)

How many minimal covering systems of size n are there?

Erdős gave a simple proof that there are only finitely many minimal covering systems of size n. His bound was doubly exponential.

(Note that there are infinitely many covering systems of size 2, since we can take $\mathcal{A} = \{\mathbb{Z}, A\}$ for any arithmetic progression A.)

The number of minimal covering systems

Question (Erdős, 1952)

How many minimal covering systems of size n are there?

Erdős gave a simple proof that there are only finitely many minimal covering systems of size n. His bound was doubly exponential.

(Note that there are infinitely many covering systems of size 2, since we can take $\mathcal{A} = \{\mathbb{Z}, A\}$ for any arithmetic progression A.)

Simpson proved in 1985 that the largest modulus in a minimal covering system of size n is at most 2^{n-1}.

The number of minimal covering systems

Question (Erdős, 1952)

How many minimal covering systems of size n are there?

Erdős gave a simple proof that there are only finitely many minimal covering systems of size n. His bound was doubly exponential.

(Note that there are infinitely many covering systems of size 2, since we can take $\mathcal{A} = \{\mathbb{Z}, A\}$ for any arithmetic progression A.)

Simpson proved in 1985 that the largest modulus in a minimal covering system of size n is at most 2^{n-1}.

This bound is best possible, since the following system is minimal:

$$\mathcal{A} = \{2^{i-1} \pmod{2^i} : i \in [n-1]\} \cup \{0 \pmod{2^{n-1}}\}.$$

The number of minimal covering systems

Question (Erdős, 1952)

How many minimal covering systems of size n are there?

Erdős gave a simple proof that there are only finitely many minimal covering systems of size n. His bound was doubly exponential.

(Note that there are infinitely many covering systems of size 2, since we can take $\mathcal{A} = \{\mathbb{Z}, A\}$ for any arithmetic progression A.)

Simpson proved in 1985 that the largest modulus in a minimal covering system of size n is at most 2^{n-1}.

This bound is best possible, since the following system is minimal:

$$\mathcal{A} = \big\{ 2^{i-1} \pmod{2^i} : i \in [n-1] \big\} \cup \big\{ 0 \pmod{2^{n-1}} \big\}.$$

It also implies there are only $2^{O(n^2)}$ minimal covering systems of size n.

Constructing many minimal covering systems

Recall that

$$\mathcal{A} = \{2^{i-1} \pmod{2^i} : i \in [n-1]\} \cup \{0 \pmod{2^{n-1}}\}$$

is a minimal covering system.

Constructing many minimal covering systems

Recall that

$$\mathcal{A} = \{2^{i-1} \text{ (mod } 2^i) : i \in [n-1]\} \cup \{0 \text{ (mod } 2^{n-1})\}$$

is a minimal covering system. We generalise this construction as follows:

Constructing many minimal covering systems

Recall that

$$\mathcal{A} = \{2^{i-1} \pmod{2^i} : i \in [n-1]\} \cup \{0 \pmod{2^{n-1}}\}$$

is a minimal covering system. We generalise this construction as follows:

Let $p_1 < \ldots < p_k$ be the first k primes, and set $Q_k := p_1 \cdots p_k$.

Constructing many minimal covering systems

Recall that

$$\mathcal{A} = \{2^{i-1} \pmod{2^i} : i \in [n-1]\} \cup \{0 \pmod{2^{n-1}}\}$$

is a minimal covering system. We generalise this construction as follows:

Let $p_1 < \ldots < p_k$ be the first k primes, and set $Q_k := p_1 \cdots p_k$.

For each $1 \leqslant i \leqslant k$ and $1 \leqslant a \leqslant p_i - 1$, choose an arithmetic progression

$$\{a \cdot Q_{i-1} \pmod{d \cdot p_i}\} \quad \text{for some} \quad d \,\big|\, Q_{i-1}.$$

Constructing many minimal covering systems

Recall that

$$\mathcal{A} = \big\{ 2^{i-1} \pmod{2^i} : i \in [n-1] \big\} \cup \big\{ 0 \pmod{2^{n-1}} \big\}$$

is a minimal covering system. We generalise this construction as follows:

Let $p_1 < \ldots < p_k$ be the first k primes, and set $Q_k := p_1 \cdots p_k$.

For each $1 \leqslant i \leqslant k$ and $1 \leqslant a \leqslant p_i - 1$, choose an arithmetic progression

$$\big\{ a \cdot Q_{i-1} \pmod{d \cdot p_i} \big\} \quad \text{for some} \quad d \,\big|\, Q_{i-1}.$$

Together with $\big\{ 0 \pmod{Q_k} \big\}$, these cover $\mathbb{Z}$.

Constructing many minimal covering systems

Recall that

$$\mathcal{A} = \{2^{i-1} \pmod{2^i} : i \in [n-1]\} \cup \{0 \pmod{2^{n-1}}\}$$

is a minimal covering system. We generalise this construction as follows:

Let $p_1 < \ldots < p_k$ be the first k primes, and set $Q_k := p_1 \cdots p_k$.

For each $1 \leqslant i \leqslant k$ and $1 \leqslant a \leqslant p_i - 1$, choose an arithmetic progression

$$\{a \cdot Q_{i-1} \pmod{d \cdot p_i}\} \quad \text{for some} \quad d \,\big|\, Q_{i-1}.$$

Together with $\{0 \pmod{Q_k}\}$, these cover $\mathbb{Z}$.

A *frame* is a collection of arithmetic progressions as above.

An example of a frame

For each prime p we choose $p-1$ progressions of the form

$$\{a \cdot Q_{i-1} \text{ (mod } d \cdot p_i)\} \quad \text{for some} \quad d \,|\, Q_{i-1} = p_1 \cdots p_{i-1},$$

one for each $a \in \{1, \ldots, p-1\}$.

An example of a frame

For each prime p we choose $p-1$ progressions of the form

$$\{a \cdot Q_{i-1} \pmod{d \cdot p_i}\} \quad \text{for some} \quad d \,|\, Q_{i-1} = p_1 \cdots p_{i-1},$$

one for each $a \in \{1, \ldots, p-1\}$.

- $p = 2$: we take $\{1 \pmod 2\}$.

An example of a frame

For each prime p we choose $p-1$ progressions of the form

$$\{a \cdot Q_{i-1} \pmod{d \cdot p_i}\} \quad \text{for some} \quad d \,|\, Q_{i-1} = p_1 \cdots p_{i-1},$$

one for each $a \in \{1, \ldots, p-1\}$.

- $p = 2$: we take $\{1 \pmod 2\}$.
- $p = 3$: we take $\{2 \pmod 3\}$ or $\{2 \pmod 6\}$

An example of a frame

For each prime p we choose $p-1$ progressions of the form

$$\{a \cdot Q_{i-1} \pmod{d \cdot p_i}\} \quad \text{for some} \quad d \,\big|\, Q_{i-1} = p_1 \cdots p_{i-1},$$

one for each $a \in \{1, \ldots, p-1\}$.

- $p = 2$: we take $\{1 \pmod 2\}$.
- $p = 3$: we take $\{2 \pmod 3\}$ or $\{2 \pmod 6\}$
  and $\{1 \pmod 3\}$ or $\{4 \pmod 6\}$.

An example of a frame

For each prime p we choose $p-1$ progressions of the form

$$\{a \cdot Q_{i-1} \pmod{d \cdot p_i}\} \quad \text{for some} \quad d \,\big|\, Q_{i-1} = p_1 \cdots p_{i-1},$$

one for each $a \in \{1, \ldots, p-1\}$.

- $p = 2$: we take $\{1 \pmod 2\}$.
- $p = 3$: we take $\{2 \pmod 3\}$ or $\{2 \pmod 6\}$
  and $\{1 \pmod 3\}$ or $\{4 \pmod 6\}$.
- $p = 5$: we could take (for example):

$$\{1 \pmod 5\}, \{2 \pmod{10}\}, \{3 \pmod{15}\} \text{ and } \{24 \pmod{30}\}.$$

An example of a frame

For each prime p we choose $p - 1$ progressions of the form

$$\{a \cdot Q_{i-1} \pmod{d \cdot p_i}\} \quad \text{for some} \quad d \,\big|\, Q_{i-1} = p_1 \cdots p_{i-1},$$

one for each $a \in \{1, \ldots, p-1\}$.

- $p = 2$: we take $\{1 \pmod{2}\}$.
- $p = 3$: we take $\{2 \pmod{3}\}$ or $\{2 \pmod{6}\}$
  and $\{1 \pmod{3}\}$ or $\{4 \pmod{6}\}$.
- $p = 5$: we could take (for example):

$$\{1 \pmod{5}\}, \{2 \pmod{10}\}, \{3 \pmod{15}\} \text{ and } \{24 \pmod{30}\}.$$

- $p = 7$: we could take (for example):

$$\{2 \pmod{7}\} \qquad \{4 \pmod{14}\} \qquad \{6 \pmod{21}\}$$

$$\{15 \pmod{35}\} \qquad \{24 \pmod{42}\} \qquad \{40 \pmod{70}\}.$$

An example of a frame

For each prime p we choose $p-1$ progressions of the form

$$\{a \cdot Q_{i-1} \pmod{d \cdot p_i}\} \quad \text{for some} \quad d \,\big|\, Q_{i-1} = p_1 \cdots p_{i-1},$$

one for each $a \in \{1, \ldots, p-1\}$.

- $p = 2$: we take $\{1 \pmod 2\}$.
- $p = 3$: we take $\{2 \pmod 3\}$ or $\{2 \pmod 6\}$
  and $\{1 \pmod 3\}$ or $\{4 \pmod 6\}$.
- $p = 5$: we could take (for example):

$$\{1 \pmod 5\}, \{2 \pmod{10}\}, \{3 \pmod{15}\} \text{ and } \{24 \pmod{30}\}.$$

- $p = 7$: we could take (for example):

$$\{2 \pmod 7\} \qquad \{4 \pmod{14}\} \qquad \{6 \pmod{21}\}$$

$$\{15 \pmod{35}\} \qquad \{24 \pmod{42}\} \qquad \{40 \pmod{70}\}.$$

- and so on...

Counting the frames

Proposition

There are at least

$$\exp\left(\frac{\Omega(n^{3/2})}{(\log n)^{1/2}}\right)$$

minimal covering systems of $\mathbb{Z}$ of size n.

Proof.

□

Counting the frames

Proposition

There are at least

$$\exp\left(\frac{\Omega(n^{3/2})}{(\log n)^{1/2}}\right)$$

minimal covering systems of $\mathbb{Z}$ *of size* n.

Proof.

Each frame has size $n = \sum_{i=1}^{k}(p_i - 1) + 1 \approx k^2 \log k$.

□

Counting the frames

Proposition

There are at least

$$\exp\left(\frac{\Omega(n^{3/2})}{(\log n)^{1/2}}\right)$$

minimal covering systems of $\mathbb{Z}$ *of size* n.

Proof.

Each frame has size $n = \sum_{i=1}^{k}(p_i - 1) + 1 \approx k^2 \log k$.

We have 2^{i-1} choices for the progression $\{a \cdot Q_{i-1} \pmod{d \cdot p_i}\}$ for each $1 \leqslant i \leqslant k$ and $1 \leqslant a \leqslant p_i - 1$

□

Counting the frames

Proposition

There are at least

$$\exp\left(\frac{\Omega(n^{3/2})}{(\log n)^{1/2}}\right)$$

minimal covering systems of $\mathbb{Z}$ of size n.

Proof.

Each frame has size $n = \sum_{i=1}^{k}(p_i - 1) + 1 \approx k^2 \log k$.

We have 2^{i-1} choices for the progression $\{a \cdot Q_{i-1} \pmod{d \cdot p_i}\}$ for each $1 \leqslant i \leqslant k$ and $1 \leqslant a \leqslant p_i - 1$, so this implies that there are at least

$$\prod_{i=1}^{k} 2^{(i-1)(p_i-1)}$$

minimal covering systems of $\mathbb{Z}$ of size n. □

Counting the frames

Proposition

There are at least

$$\exp\left(\frac{\Omega(n^{3/2})}{(\log n)^{1/2}}\right)$$

minimal covering systems of $\mathbb{Z}$ *of size* n.

Proof.

Each frame has size $n = \sum_{i=1}^{k}(p_i - 1) + 1 \approx k^2 \log k$.

We have 2^{i-1} choices for the progression $\{a \cdot Q_{i-1} \pmod{d \cdot p_i}\}$ for each $1 \leqslant i \leqslant k$ and $1 \leqslant a \leqslant p_i - 1$, so this implies that there are at least

$$\prod_{i=1}^{k} 2^{(i-1)(p_i-1)} = \exp\Big(\Omega\big(k^3 \log k\big)\Big)$$

minimal covering systems of $\mathbb{Z}$ of size n. □

Counting the frames

Proposition

There are at least

$$\exp\left(\frac{\Omega(n^{3/2})}{(\log n)^{1/2}}\right)$$

minimal covering systems of $\mathbb{Z}$ *of size* n*.*

Proof.

Each frame has size $n = \sum_{i=1}^{k}(p_i - 1) + 1 \approx k^2 \log k$.

We have 2^{i-1} choices for the progression $\{a \cdot Q_{i-1} \pmod{d \cdot p_i}\}$ for each $1 \leqslant i \leqslant k$ and $1 \leqslant a \leqslant p_i - 1$, so this implies that there are at least

$$\prod_{i=1}^{k} 2^{(i-1)(p_i-1)} \;=\; \exp\Big(\Omega\big(k^3 \log k\big)\Big) \;=\; \exp\left(\frac{\Omega(n^{3/2})}{(\log n)^{1/2}}\right)$$

minimal covering systems of $\mathbb{Z}$ of size n. □

The number of minimal covering systems

Question (Erdős, 1952)

How many minimal covering systems of size n are there?

The number of minimal covering systems

Question (Erdős, 1952)

How many minimal covering systems of size n are there?

Theorem (Balister, Bollobás, M., Sahasrabudhe and Tiba, 2020+)

The number of minimal covering systems of $\mathbb{Z}$ of size n is

$$\exp\left(\left(\frac{4\sqrt{\tau}}{3} + o(1)\right)\frac{n^{3/2}}{(\log n)^{1/2}}\right)$$

as $n \to \infty$, where

$$\tau = \sum_{t=1}^{\infty}\left(\log\frac{t+1}{t}\right)^2.$$

The number of minimal covering systems

Question (Erdős, 1952)

How many minimal covering systems of size n are there?

Theorem (Balister, Bollobás, M., Sahasrabudhe and Tiba, 2020+)

The number of minimal covering systems of $\mathbb{Z}$ of size n is

$$\exp\left(\left(\frac{4\sqrt{\tau}}{3} + o(1)\right)\frac{n^{3/2}}{(\log n)^{1/2}}\right)$$

as $n \to \infty$, where

$$\tau = \sum_{t=1}^{\infty}\left(\log\frac{t+1}{t}\right)^2.$$

To prove this result, we needed to study the 'rough typical structure' of a minimal covering system of size n.

The minimum modulus problem

The minimum modulus problem (Erdős, 1950)

Do there exist covering systems with distinct moduli such that the minimum modulus is arbitrarily large?

The minimum modulus problem

The minimum modulus problem (Erdős, 1950)

Do there exist covering systems with distinct moduli such that the minimum modulus is arbitrarily large?

There exists a system with minimum modulus 9 (Churchhouse, 1968)

The minimum modulus problem

The minimum modulus problem (Erdős, 1950)

Do there exist covering systems with distinct moduli such that the minimum modulus is arbitrarily large?

There exists a system with minimum modulus 18 (Krukenberg, 1971)

The minimum modulus problem

The minimum modulus problem (Erdős, 1950)

Do there exist covering systems with distinct moduli such that the minimum modulus is arbitrarily large?

There exists a system with minimum modulus 20 (Choi, 1971)

The minimum modulus problem

The minimum modulus problem (Erdős, 1950)

Do there exist covering systems with distinct moduli such that the minimum modulus is arbitrarily large?

There exists a system with minimum modulus 24 (Morikawa, 1981)

The minimum modulus problem

The minimum modulus problem (Erdős, 1950)

Do there exist covering systems with distinct moduli such that the minimum modulus is arbitrarily large?

There exists a system with minimum modulus 25 (Gibson, 2006)

The minimum modulus problem

The minimum modulus problem (Erdős, 1950)

Do there exist covering systems with distinct moduli such that the minimum modulus is arbitrarily large?

There exists a system with minimum modulus 40 (Nielsen, 2009)

The minimum modulus problem

The minimum modulus problem (Erdős, 1950)

Do there exist covering systems with distinct moduli such that the minimum modulus is arbitrarily large?

There exists a system with minimum modulus 42 (Owens, 2014).

The minimum modulus problem

The minimum modulus problem (Erdős, 1950)

Do there exist covering systems with distinct moduli such that the minimum modulus is arbitrarily large?

There exists a system with minimum modulus 42 (Owens, 2014).

The first significant progress in the other direction was made in 2007 by Filaseta, Ford, Konyagin, Pomerance and Yu:

The minimum modulus problem

The minimum modulus problem (Erdős, 1950)

Do there exist covering systems with distinct moduli such that the minimum modulus is arbitrarily large?

There exists a system with minimum modulus 42 (Owens, 2014).

The first significant progress in the other direction was made in 2007 by Filaseta, Ford, Konyagin, Pomerance and Yu:

Theorem (Filaseta, Ford, Konyagin, Pomerance and Yu, 2007)

Let $\mathcal{A}$ be a covering system with distinct moduli $d_1, \ldots, d_k \geqslant M$. Then

$$\sum_{i=1}^{k} \frac{1}{d_i} \geqslant \frac{\log M \log\log\log M}{4 \log\log M}.$$

The minimum modulus problem

The minimum modulus problem (Erdős, 1950)

Do there exist covering systems with distinct moduli such that the minimum modulus is arbitrarily large?

There exists a system with minimum modulus 42 (Owens, 2014).

The first significant progress in the other direction was made in 2007 by Filaseta, Ford, Konyagin, Pomerance and Yu:

Theorem (Filaseta, Ford, Konyagin, Pomerance and Yu, 2007)

Let $\mathcal{A}$ be a covering system with distinct moduli $d_1, \ldots, d_k \geqslant M$. Then

$$\sum_{i=1}^{k} \frac{1}{d_i} \geqslant \frac{\log M \log\log\log M}{4 \log\log M}.$$

They also proved the conjecture of Erdős and Graham.

The minimum modulus problem

Building on their work, Hough resolved the minimum modulus problem:

Theorem (Hough, 2015)

Every covering system with distinct moduli has minimum modulus $\leqslant 10^{16}$.

The minimum modulus problem

Building on their work, Hough resolved the minimum modulus problem:

Theorem (Hough, 2015)

Every covering system with distinct moduli has minimum modulus $\leqslant 10^{16}$.

Sketch of the proof.

□

The minimum modulus problem

Building on their work, Hough resolved the minimum modulus problem:

Theorem (Hough, 2015)

Every covering system with distinct moduli has minimum modulus $\leqslant 10^{16}$.

Sketch of the proof.

'Reveal' the arithmetic progressions 'prime by prime', and 'track' the evolution of the uncovered set.

□

The minimum modulus problem

Building on their work, Hough resolved the minimum modulus problem:

Theorem (Hough, 2015)

Every covering system with distinct moduli has minimum modulus $\leqslant 10^{16}$.

Sketch of the proof.

'Reveal' the arithmetic progressions 'prime by prime', and 'track' the evolution of the uncovered set. The key idea is to define a probability measure that distorts the space,

□

The minimum modulus problem

Building on their work, Hough resolved the minimum modulus problem:

Theorem (Hough, 2015)

Every covering system with distinct moduli has minimum modulus $\leqslant 10^{16}$.

Sketch of the proof.

'Reveal' the arithmetic progressions 'prime by prime', and 'track' the evolution of the uncovered set. The key idea is to define a probability measure that distorts the space, blowing up the uncovered set, but without increasing the measure of any single point too much. □

The minimum modulus problem

Building on their work, Hough resolved the minimum modulus problem:

Theorem (Hough, 2015)

Every covering system with distinct moduli has minimum modulus $\leqslant 10^{16}$.

Sketch of the proof.

'Reveal' the arithmetic progressions 'prime by prime', and 'track' the evolution of the uncovered set. The key idea is to define a probability measure that distorts the space, blowing up the uncovered set, but without increasing the measure of any single point too much.

We bound the (distorted) measure of the set covered when revealing the prime p,

□

The minimum modulus problem

Building on their work, Hough resolved the minimum modulus problem:

Theorem (Hough, 2015)

Every covering system with distinct moduli has minimum modulus $\leqslant 10^{16}$.

Sketch of the proof.

'Reveal' the arithmetic progressions 'prime by prime', and 'track' the evolution of the uncovered set. The key idea is to define a probability measure that distorts the space, blowing up the uncovered set, but without increasing the measure of any single point too much.

We bound the (distorted) measure of the set covered when revealing the prime p, and show that if the minimum modulus is sufficiently large, then the total (distorted) measure removed can be made arbitrarily small. □

A geometric setting

Let $S_1, \ldots, S_n$ be finite sets with at least two elements, and set

$$Q_k = S_1 \times \cdots \times S_k$$

for each $1 \leqslant k \leqslant n$.

A geometric setting

Let $S_1, \ldots, S_n$ be finite sets with at least two elements, and set

$$Q_k = S_1 \times \cdots \times S_k$$

for each $1 \leqslant k \leqslant n$.

A *hyperplane* in Q_n is a set

$$A = Y_1 \times \cdots \times Y_n \subset Q_n,$$

with each Y_i either equal to S_i or a singleton element of S_i.

A geometric setting

Let $S_1, \ldots, S_n$ be finite sets with at least two elements, and set

$$Q_k = S_1 \times \cdots \times S_k$$

for each $1 \leqslant k \leqslant n$.

A *hyperplane* in Q_n is a set

$$A = Y_1 \times \cdots \times Y_n \subset Q_n,$$

with each Y_i either equal to S_i or a singleton element of S_i.

The set of *fixed coordinates* of A is

$$F(A) := \{k : Y_k \neq S_k\}.$$

A geometric setting

Let $S_1, \ldots, S_n$ be finite sets with at least two elements, and set

$$Q_k = S_1 \times \cdots \times S_k$$

for each $1 \leqslant k \leqslant n$.

A *hyperplane* in Q_n is a set

$$A = Y_1 \times \cdots \times Y_n \subset Q_n,$$

with each Y_i either equal to S_i or a singleton element of S_i.

The set of *fixed coordinates* of A is

$$F(A) := \{k : Y_k \neq S_k\}.$$

We say that two hyperplanes A and A' are *parallel* if $F(A) = F(A')$.

A geometric theorem

The set of *fixed coordinates* of a hyperplane $A = Y_1 \times \cdots \times Y_n$ is

$$F(A) := \{k : Y_k \neq S_k\},$$

and two hyperplanes A and A' are *parallel* if $F(A) = F(A')$.

A geometric theorem

The set of *fixed coordinates* of a hyperplane $A = Y_1 \times \cdots \times Y_n$ is

$$F(A) := \{k : Y_k \neq S_k\},$$

and two hyperplanes A and A' are *parallel* if $F(A) = F(A')$.

Theorem (Balister, Bollobás, M., Sahasrabudhe and Tiba, 2020+)

If $|S_k| \geqslant 4k$ for all sufficiently large k, then there exists a constant C such that the following holds. Let $\mathcal{A}$ be a collection of hyperplanes that cover $Q_n = S_1 \times \cdots \times S_n$. Then either two of the hyperplanes are parallel, or there exists a hyperplane $A \in \mathcal{A}$ with $F(A) \subset \{1, \ldots, C\}$.

A geometric theorem

The set of *fixed coordinates* of a hyperplane $A = Y_1 \times \cdots \times Y_n$ is

$$F(A) := \{k : Y_k \neq S_k\},$$

and two hyperplanes A and A' are *parallel* if $F(A) = F(A')$.

Theorem (Balister, Bollobás, M., Sahasrabudhe and Tiba, 2020+)

If $|S_k| \geqslant 4k$ for all sufficiently large k, then there exists a constant C such that the following holds. Let $\mathcal{A}$ be a collection of hyperplanes that cover $Q_n = S_1 \times \cdots \times S_n$. Then either two of the hyperplanes are parallel, or there exists a hyperplane $A \in \mathcal{A}$ with $F(A) \subset \{1, \ldots, C\}$.

This implies Hough's theorem in the case of square-free moduli.

A geometric theorem

The set of *fixed coordinates* of a hyperplane $A = Y_1 \times \cdots \times Y_n$ is

$$F(A) := \{k : Y_k \neq S_k\},$$

and two hyperplanes A and A' are *parallel* if $F(A) = F(A')$.

Theorem (Balister, Bollobás, M., Sahasrabudhe and Tiba, 2020+)

If $|S_k| \geqslant 4k$ for all sufficiently large k, then there exists a constant C such that the following holds. Let $\mathcal{A}$ be a collection of hyperplanes that cover $Q_n = S_1 \times \cdots \times S_n$. Then either two of the hyperplanes are parallel, or there exists a hyperplane $A \in \mathcal{A}$ with $F(A) \subset \{1, \ldots, C\}$.

This implies Hough's theorem in the case of square-free moduli.

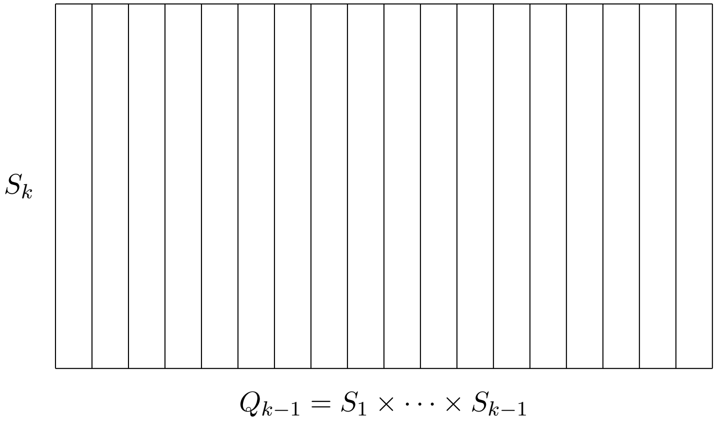
(Proof: Set $S_k = \{1, \ldots, p_k\}$, where p_k is the kth prime, and use the Chinese Remainder Theorem to map progressions to hyperplanes.)

A picture of the geometric setting

Let $S_1, \ldots, S_n$ be finite sets with at least two elements, and set

$$Q_k = S_1 \times \cdots \times S_k$$

for each $1 \leqslant k \leqslant n$.

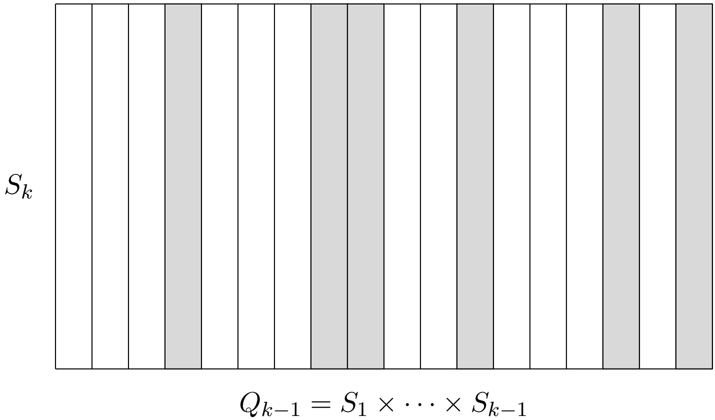


A picture of the geometric setting

Let $S_1, \ldots, S_n$ be finite sets with at least two elements, and set

$$Q_k = S_1 \times \cdots \times S_k$$

for each $1 \leqslant k \leqslant n$.

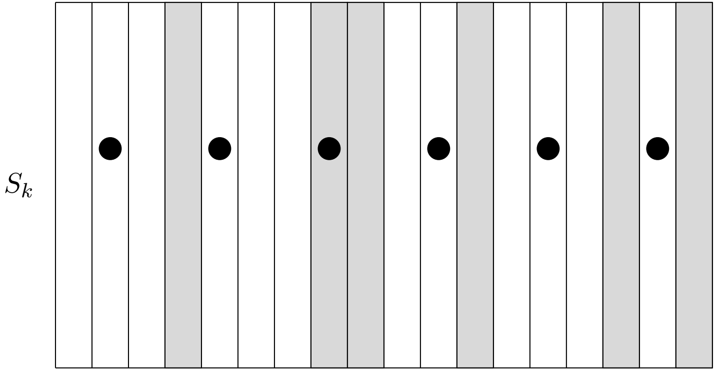


A picture of the geometric setting

Let $S_1, \ldots, S_n$ be finite sets with at least two elements, and set

$$Q_k = S_1 \times \cdots \times S_k$$

for each $1 \leqslant k \leqslant n$.



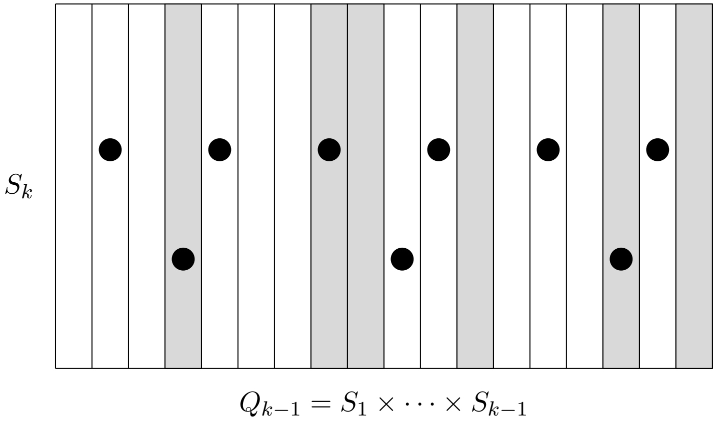
$$Q_{k-1} = S_1 \times \cdots \times S_{k-1}$$

A picture of the geometric setting

Let $S_1, \dots, S_n$ be finite sets with at least two elements, and set

$$Q_k = S_1 \times \cdots \times S_k$$

for each $1 \leqslant k \leqslant n$.

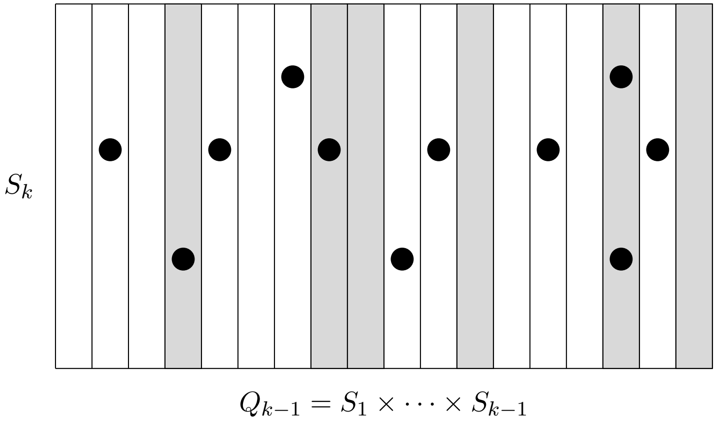


A picture of the geometric setting

Let $S_1, \ldots, S_n$ be finite sets with at least two elements, and set

$$Q_k = S_1 \times \cdots \times S_k$$

for each $1 \leqslant k \leqslant n$.



The distortion method (Hough, 2015)

The distortion method (Hough, 2015)

We will reveal the hyperplanes in n rounds, and define a sequence of probability measures $\mathbb{P}_0, \ldots, \mathbb{P}_n$ on Q_n that gradually distort the space.

The distortion method (Hough, 2015)

We will reveal the hyperplanes in n rounds, and define a sequence of probability measures $\mathbb{P}_0, \ldots, \mathbb{P}_n$ on Q_n that gradually distort the space.

The measure $\mathbb{P}_k$ will depend on the hyperplanes with $\max(F(A)) \leqslant k$, i.e., those that were revealed in the first k rounds.

The distortion method (Hough, 2015)

We will reveal the hyperplanes in n rounds, and define a sequence of probability measures $\mathbb{P}_0, \ldots, \mathbb{P}_n$ on Q_n that gradually distort the space.

The measure $\mathbb{P}_k$ will depend on the hyperplanes with $\max(F(A)) \leqslant k$, i.e., those that were revealed in the first k rounds. It will be chosen so that the $\mathbb{P}_k$-measure of the set covered in the kth round is small.

The distortion method (Hough, 2015)

We will reveal the hyperplanes in n rounds, and define a sequence of probability measures $\mathbb{P}_0, \ldots, \mathbb{P}_n$ on Q_n that gradually distort the space.

The measure $\mathbb{P}_k$ will depend on the hyperplanes with $\max(F(A)) \leqslant k$, i.e., those that were revealed in the first k rounds. It will be chosen so that the $\mathbb{P}_k$-measure of the set covered in the kth round is small.

However, it will be important that:

The distortion method (Hough, 2015)

We will reveal the hyperplanes in n rounds, and define a sequence of probability measures $\mathbb{P}_0, \ldots, \mathbb{P}_n$ on Q_n that gradually distort the space.

The measure $\mathbb{P}_k$ will depend on the hyperplanes with $\max(F(A)) \leqslant k$, i.e., those that were revealed in the first k rounds. It will be chosen so that the $\mathbb{P}_k$-measure of the set covered in the kth round is small.

However, it will be important that:

- we do not change the measure of the set of already-covered points;

The distortion method (Hough, 2015)

We will reveal the hyperplanes in n rounds, and define a sequence of probability measures $\mathbb{P}_0, \ldots, \mathbb{P}_n$ on Q_n that gradually distort the space.

The measure $\mathbb{P}_k$ will depend on the hyperplanes with $\max(F(A)) \leqslant k$, i.e., those that were revealed in the first k rounds. It will be chosen so that the $\mathbb{P}_k$-measure of the set covered in the kth round is small.

However, it will be important that:

- we do not change the measure of the set of already-covered points;
- we do not increase the measure of any set too much.

The distortion method (Hough, 2015)

We will reveal the hyperplanes in n rounds, and define a sequence of probability measures $\mathbb{P}_0, \ldots, \mathbb{P}_n$ on Q_n that gradually distort the space.

The measure $\mathbb{P}_k$ will depend on the hyperplanes with $\max(F(A)) \leqslant k$, i.e., those that were revealed in the first k rounds. It will be chosen so that the $\mathbb{P}_k$-measure of the set covered in the kth round is small.

However, it will be important that:

- we do not change the measure of the set of already-covered points;
- we do not increase the measure of any set too much.

Let $\mathbb{P}_{k-1}$ be a probability measure on Q_{k-1}.

The distortion method (Hough, 2015)

We will reveal the hyperplanes in n rounds, and define a sequence of probability measures $\mathbb{P}_0, \ldots, \mathbb{P}_n$ on Q_n that gradually distort the space.

The measure $\mathbb{P}_k$ will depend on the hyperplanes with $\max(F(A)) \leqslant k$, i.e., those that were revealed in the first k rounds. It will be chosen so that the $\mathbb{P}_k$-measure of the set covered in the kth round is small.

However, it will be important that:

- we do not change the measure of the set of already-covered points;
- we do not increase the measure of any set too much.

Let $\mathbb{P}_{k-1}$ be a probability measure on Q_{k-1}. A natural way to define the measure $\mathbb{P}_k$ on Q_k would be to define $\mathbb{P}_k(x) = 0$ if x is covered in step k,

The distortion method (Hough, 2015)

We will reveal the hyperplanes in n rounds, and define a sequence of probability measures $\mathbb{P}_0, \ldots, \mathbb{P}_n$ on Q_n that gradually distort the space.

The measure $\mathbb{P}_k$ will depend on the hyperplanes with $\max(F(A)) \leqslant k$, i.e., those that were revealed in the first k rounds. It will be chosen so that the $\mathbb{P}_k$-measure of the set covered in the kth round is small.

However, it will be important that:

- we do not change the measure of the set of already-covered points;
- we do not increase the measure of any set too much.

Let $\mathbb{P}_{k-1}$ be a probability measure on Q_{k-1}. A natural way to define the measure $\mathbb{P}_k$ on Q_k would be to define $\mathbb{P}_k(x) = 0$ if x is covered in step k, and redistribute the removed measure over the remaining elements (taking care not to change the measure of any Q_{k-1}-measurable set).

The distortion method (Hough, 2015)

We will reveal the hyperplanes in n rounds, and define a sequence of probability measures $\mathbb{P}_0, \ldots, \mathbb{P}_n$ on Q_n that gradually distort the space.

The measure $\mathbb{P}_k$ will depend on the hyperplanes with $\max(F(A)) \leqslant k$, i.e., those that were revealed in the first k rounds. It will be chosen so that the $\mathbb{P}_k$-measure of the set covered in the kth round is small.

However, it will be important that:

- we do not change the measure of the set of already-covered points;
- we do not increase the measure of any set too much.

Let $\mathbb{P}_{k-1}$ be a probability measure on Q_{k-1}. A natural way to define the measure $\mathbb{P}_k$ on Q_k would be to define $\mathbb{P}_k(x) = 0$ if x is covered in step k, and redistribute the removed measure over the remaining elements (taking care not to change the measure of any Q_{k-1}-measurable set).

However, it turns out to be simpler to do something more complicated!

The distortion method (BBMST version)

Recall that $Q_k = Q_{k-1} \times S_k$, and for each $x \in Q_{k-1}$ define

$$\alpha_k(x) := \frac{\big|\{y \in S_k : (x,y) \in B_k\}\big|}{|S_k|},$$

where B_k is the set covered by the hyperplanes with $\max(F(A)) = k$.

The distortion method (BBMST version)

Recall that $Q_k = Q_{k-1} \times S_k$, and for each $x \in Q_{k-1}$ define

$$\alpha_k(x) := \frac{\big|\{y \in S_k : (x,y) \in B_k\}\big|}{|S_k|},$$

where B_k is the set covered by the hyperplanes with $\max(F(A)) = k$.

In words, $\alpha_k(x)$ is the proportion of the 'fibre'

$$F_x := \big\{(x,y) : y \in S_k\big\} \subset Q_k$$

that is covered in round k.

The distortion method (BBMST version)

Recall that $Q_k = Q_{k-1} \times S_k$, and for each $x \in Q_{k-1}$ define

$$\alpha_k(x) := \frac{\big|\{y \in S_k : (x,y) \in B_k\}\big|}{|S_k|},$$

where B_k is the set covered by the hyperplanes with $\max(F(A)) = k$.

In words, $\alpha_k(x)$ is the proportion of the 'fibre'

$$F_x := \big\{(x,y) : y \in S_k\big\} \subset Q_k$$

that is covered in round k. Fix $\delta > 0$, and define $\mathbb{P}_k$ as follows:

The distortion method (BBMST version)

Recall that $Q_k = Q_{k-1} \times S_k$, and for each $x \in Q_{k-1}$ define

$$\alpha_k(x) := \frac{\big|\{y \in S_k : (x,y) \in B_k\}\big|}{|S_k|},$$

where B_k is the set covered by the hyperplanes with $\max(F(A)) = k$.

In words, $\alpha_k(x)$ is the proportion of the 'fibre'

$$F_x := \big\{(x,y) : y \in S_k\big\} \subset Q_k$$

that is covered in round k. Fix $\delta > 0$, and define $\mathbb{P}_k$ as follows:

- If $\alpha_k(x) \leqslant \delta$, then we set $\mathbb{P}_k(x,y) = 0$ for every element of $F_x \cap B_k$, and increase the measure proportionally on the rest of F_x;

The distortion method (BBMST version)

Recall that $Q_k = Q_{k-1} \times S_k$, and for each $x \in Q_{k-1}$ define

$$\alpha_k(x) := \frac{\big|\{y \in S_k : (x,y) \in B_k\}\big|}{|S_k|},$$

where B_k is the set covered by the hyperplanes with $\max(F(A)) = k$.

In words, $\alpha_k(x)$ is the proportion of the 'fibre'

$$F_x := \big\{(x,y) : y \in S_k\big\} \subset Q_k$$

that is covered in round k. Fix $\delta > 0$, and define $\mathbb{P}_k$ as follows:

- If $\alpha_k(x) \leqslant \delta$, then we set $\mathbb{P}_k(x,y) = 0$ for every element of $F_x \cap B_k$, and increase the measure proportionally on the rest of F_x;
- If $\alpha_k(x) > \delta$, then we 'cap' the distortion by increasing the measure at each point of $F_x \setminus B_k$ by a factor of $1/(1-\delta)$, and decreasing the measure on points of $F_x \cap B_k$ by a corresponding factor.

The distortion method (key lemma)

Lemma

Let $\mathcal{A}$ be a collection of hyperplanes in $Q_n = S_1 \times \cdots \times S_n$. If

$$\frac{1}{4\delta(1-\delta)} \sum_{k=1}^{n} \mathbb{E}_{k-1}\big[\alpha_k(x)^2\big] < 1,$$

then $\mathcal{A}$ does not cover Q_n.

The distortion method (key lemma)

Lemma

Let $\mathcal{A}$ be a collection of hyperplanes in $Q_n = S_1 \times \cdots \times S_n$. If

$$\frac{1}{4\delta(1-\delta)} \sum_{k=1}^{n} \mathbb{E}_{k-1}\big[\alpha_k(x)^2\big] < 1,$$

then $\mathcal{A}$ does not cover Q_n.

Proof.

A simple calculation (using the inequality $\max\{a-b,0\} \leqslant a^2/4b$) gives

$$\mathbb{P}_k(B_k) \leqslant \frac{\mathbb{E}_{k-1}\big[\alpha_k(x)^2\big]}{4\delta(1-\delta)}.$$

□

The distortion method (key lemma)

Lemma

Let $\mathcal{A}$ be a collection of hyperplanes in $Q_n = S_1 \times \cdots \times S_n$. If

$$\frac{1}{4\delta(1-\delta)} \sum_{k=1}^{n} \mathbb{E}_{k-1}\big[\alpha_k(x)^2\big] < 1,$$

then $\mathcal{A}$ does not cover Q_n.

Proof.

A simple calculation (using the inequality $\max\{a-b,0\} \leqslant a^2/4b$) gives

$$\mathbb{P}_k(B_k) \leqslant \frac{\mathbb{E}_{k-1}\big[\alpha_k(x)^2\big]}{4\delta(1-\delta)}.$$

Hence $\sum_k \mathbb{P}_n(B_k) = \sum_k \mathbb{P}_k(B_k) < 1$, and so $\mathcal{A}$ does not cover Q_n. □

The distortion method (bounding the moments of α_k)

To deduce the theorem, it only remains to bound, for each $1 \leqslant k \leqslant n$, the second moment of $\alpha_k(x)$ with respect to the measure $\mathbb{P}_{k-1}$.

The distortion method (bounding the moments of α_k)

To deduce the theorem, it only remains to bound, for each $1 \leqslant k \leqslant n$, the second moment of $\alpha_k(x)$ with respect to the measure $\mathbb{P}_{k-1}$.

Lemma

Let $\mathcal{A}$ be a collection of hyperplanes in $Q_n = S_1 \times \cdots \times S_n$, no two of which are parallel. Then, for each $1 \leqslant k \leqslant n$,

$$\mathbb{E}_{k-1}\big[\alpha_k(x)^2\big] \leqslant \frac{1}{|S_k|^2} \prod_{j=1}^{k-1} \left(1 + \frac{3}{(1-\delta)|S_j|}\right).$$

The distortion method (bounding the moments of α_k)

To deduce the theorem, it only remains to bound, for each $1 \leqslant k \leqslant n$, the second moment of $\alpha_k(x)$ with respect to the measure $\mathbb{P}_{k-1}$.

Lemma

Let $\mathcal{A}$ be a collection of hyperplanes in $Q_n = S_1 \times \cdots \times S_n$, no two of which are parallel. Then, for each $1 \leqslant k \leqslant n$,

$$\mathbb{E}_{k-1}\big[\alpha_k(x)^2\big] \leqslant \frac{1}{|S_k|^2} \prod_{j=1}^{k-1} \left(1 + \frac{3}{(1-\delta)|S_j|}\right).$$

Proof.

A straightforward induction shows that if $F(A) \subset [k]$, then

$$\mathbb{P}_k(A) \leqslant \prod_{j \in F(A)} \frac{1}{(1-\delta)|S_j|}.$$

□

The distortion method (bounding the moments of α_k)

To deduce the theorem, it only remains to bound, for each $1 \leqslant k \leqslant n$, the second moment of $\alpha_k(x)$ with respect to the measure $\mathbb{P}_{k-1}$.

Lemma

Let $\mathcal{A}$ be a collection of hyperplanes in $Q_n = S_1 \times \cdots \times S_n$, no two of which are parallel. Then, for each $1 \leqslant k \leqslant n$,

$$\mathbb{E}_{k-1}\big[\alpha_k(x)^2\big] \leqslant \frac{1}{|S_k|^2} \prod_{j=1}^{k-1} \left(1 + \frac{3}{(1-\delta)|S_j|}\right).$$

Proof.

A straightforward induction shows that if $F(A) \subset [k]$, then

$$\mathbb{P}_k(A) \leqslant \prod_{j \in F(A)} \frac{1}{(1-\delta)|S_j|}.$$

The lemma now follows from a simple union bound. □

The distortion method (completing the proof)

Theorem (Balister, Bollobás, M., Sahasrabudhe and Tiba, 2020+)

If $|S_k| \geqslant (3+\varepsilon)k$ *for all* $k \geqslant k_0$*, then there exists* $C = C(\varepsilon, k_0)$ *such that the following holds. Let* $\mathcal{A}$ *be a collection of hyperplanes that cover* $Q_n = S_1 \times \cdots \times S_n$*. Then either two of the hyperplanes are parallel, or there exists a hyperplane* $A \in \mathcal{A}$ *with* $F(A) \subset \{1, \ldots, C\}$*.*

The distortion method (completing the proof)

Theorem (Balister, Bollobás, M., Sahasrabudhe and Tiba, 2020+)

If $|S_k| \geqslant (3+\varepsilon)k$ *for all* $k \geqslant k_0$*, then there exists* $C = C(\varepsilon, k_0)$ *such that the following holds. Let* $\mathcal{A}$ *be a collection of hyperplanes that cover* $Q_n = S_1 \times \cdots \times S_n$*. Then either two of the hyperplanes are parallel, or there exists a hyperplane* $A \in \mathcal{A}$ *with* $F(A) \subset \{1, \ldots, C\}$*.*

Proof.

The previous lemma gives (via a straightforward calculation)

$$\frac{1}{4\delta(1-\delta)} \sum_{k=C}^{n} \mathbb{E}_{k-1}\big[\alpha_k(x)^2\big] \leqslant \sum_{k=C}^{n} O\big(k^{-(1+\varepsilon)}\big) < 1$$

if C is sufficiently large.

□

The distortion method (completing the proof)

Theorem (Balister, Bollobás, M., Sahasrabudhe and Tiba, 2020+)

If $|S_k| \geqslant (3+\varepsilon)k$ for all $k \geqslant k_0$, then there exists $C = C(\varepsilon, k_0)$ such that the following holds. Let $\mathcal{A}$ be a collection of hyperplanes that cover $Q_n = S_1 \times \cdots \times S_n$. Then either two of the hyperplanes are parallel, or there exists a hyperplane $A \in \mathcal{A}$ with $F(A) \subset \{1, \ldots, C\}$.

Proof.

The previous lemma gives (via a straightforward calculation)

$$\frac{1}{4\delta(1-\delta)} \sum_{k=C}^{n} \mathbb{E}_{k-1}\big[\alpha_k(x)^2\big] \leqslant \sum_{k=C}^{n} O\big(k^{-(1+\varepsilon)}\big) < 1$$

if C is sufficiently large. Moreover, if $F(A) \not\subset \{1, \ldots, C\}$ for every $A \in \mathcal{A}$, then $\alpha_k(x) = 0$ for every $1 \leqslant k \leqslant C$ and $x \in Q_{k-1}$.

□

The distortion method (completing the proof)

Theorem (Balister, Bollobás, M., Sahasrabudhe and Tiba, 2020+)

If $|S_k| \geqslant (3+\varepsilon)k$ for all $k \geqslant k_0$, then there exists $C = C(\varepsilon, k_0)$ such that the following holds. Let $\mathcal{A}$ be a collection of hyperplanes that cover $Q_n = S_1 \times \cdots \times S_n$. Then either two of the hyperplanes are parallel, or there exists a hyperplane $A \in \mathcal{A}$ with $F(A) \subset \{1, \ldots, C\}$.

Proof.

The previous lemma gives (via a straightforward calculation)

$$\frac{1}{4\delta(1-\delta)} \sum_{k=C}^{n} \mathbb{E}_{k-1}\big[\alpha_k(x)^2\big] \leqslant \sum_{k=C}^{n} O\big(k^{-(1+\varepsilon)}\big) < 1$$

if C is sufficiently large. Moreover, if $F(A) \not\subset \{1, \ldots, C\}$ for every $A \in \mathcal{A}$, then $\alpha_k(x) = 0$ for every $1 \leqslant k \leqslant C$ and $x \in Q_{k-1}$.

By the Key Lemma, it follows that $\mathcal{A}$ does not cover Q_n, as required. □

The density of the uncovered set

Theorem (Filaseta, Ford, Konyagin, Pomerance and Yu, 2007)

If $n \gg \exp\big(\log C \log\log C\big)$*, then for any system of arithmetic progressions with distinct moduli* $d_1, \ldots, d_k \subset [n, Cn]$*, the uncovered set has density at least*

$$(1 + o(1)) \prod_{i=1}^{k} \left(1 - \frac{1}{d_i}\right).$$

The density of the uncovered set

Question (Filaseta, Ford, Konyagin, Pomerance and Yu, 2007)

If a covering system has distinct moduli $d_1, \ldots, d_k$ *satisfying*

$$d_1, \ldots, d_k \geqslant M \qquad \textit{and} \qquad \sum_{i=1}^{k} \frac{1}{d_i} < C,$$

does it follow that the uncovered set has density at least $\delta = \delta(C) > 0$*?*

The density of the uncovered set

Question (Filaseta, Ford, Konyagin, Pomerance and Yu, 2007)

If a covering system has distinct moduli $d_1, \ldots, d_k$ satisfying

$$d_1, \ldots, d_k \geqslant M \qquad \text{and} \qquad \sum_{i=1}^{k} \frac{1}{d_i} < C,$$

does it follow that the uncovered set has density at least $\delta = \delta(C) > 0$?

Theorem (Balister, Bollobás, M., Sahasrabudhe and Tiba, 2020+)

For every $M > 0$ and $\delta > 0$, there exists a finite collection of arithmetic progressions with distinct moduli $d_1, \ldots, d_k \geqslant M$, such that

$$\sum_{i=1}^{k} \frac{1}{d_i} < 1$$

and the density of the uncovered set is less than δ.

The density of the uncovered set

Theorem (Balister, Bollobás, M., Sahasrabudhe and Tiba, 2020+)

Let χ *be the multiplicative function defined by*

$$\chi(p^i) = 1 + \frac{(\log p)^4}{p}$$

for all primes p *and integers* $i \geqslant 1$. *There exists* $M > 0$ *so that for any system of arithmetic progressions with distinct moduli* $d_1, \ldots, d_k \geqslant M$, *if*

$$C = \sum_{i=1}^{k} \frac{\chi(d_i)}{d_i},$$

then the density of the uncovered set is at least e^{-4C}.

The density of the uncovered set

Theorem (Balister, Bollobás, M., Sahasrabudhe and Tiba, 2020+)

Let χ *be the multiplicative function defined by*

$$\chi(p^i) = 1 + \frac{(\log p)^4}{p}$$

for all primes p *and integers* $i \geqslant 1$*. There exists* $M > 0$ *so that for any system of arithmetic progressions with distinct moduli* $d_1, \ldots, d_k \geqslant M$*, if*

$$C = \sum_{i=1}^{k} \frac{\chi(d_i)}{d_i},$$

then the density of the uncovered set is at least e^{-4C}*.*

The function χ cannot be replaced by one of the form $\chi(p^i) = 1 + O(1/p)$.

Some additional consequences

Conjecture (Schinzel, 1967)

In any covering system, one of the moduli divides another.

Some additional consequences

Theorem (Balister, Bollobás, M., Sahasrabudhe and Tiba, 2020+)

In any covering system, one of the moduli divides another.

Some additional consequences

Theorem (Balister, Bollobás, M., Sahasrabudhe and Tiba, 2020+)

In any covering system, one of the moduli divides another.

The Erdős–Selfridge problem

Does there exist a covering system with all moduli distinct and odd?

Some additional consequences

Theorem (Balister, Bollobás, M., Sahasrabudhe and Tiba, 2020+)

In any covering system, one of the moduli divides another.

The Erdős–Selfridge problem

Does there exist a covering system with all moduli distinct and odd?

Theorem (Hough and Nielsen, 2019)

In any covering system with distinct odd moduli, one of the moduli is divisible by 3.

Some additional consequences

Theorem (Balister, Bollobás, M., Sahasrabudhe and Tiba, 2020+)

In any covering system, one of the moduli divides another.

The Erdős–Selfridge problem

Does there exist a covering system with all moduli distinct and odd?

Theorem (Balister, Bollobás, M., Sahasrabudhe and Tiba, 2020+)

In any covering system with distinct odd moduli, the least common multiple of the moduli is divisible by either 9 *or* 15.

Some additional consequences

Theorem (Balister, Bollobás, M., Sahasrabudhe and Tiba, 2020+)

In any covering system, one of the moduli divides another.

The Erdős–Selfridge problem

Does there exist a covering system with all moduli distinct and odd?

Theorem (Balister, Bollobás, M., Sahasrabudhe and Tiba, 2020+)

In any covering system with distinct odd moduli, the least common multiple of the moduli is divisible by either 9 or 15.

Theorem (Balister, Bollobás, M., Sahasrabudhe and Tiba, 2020+)

No covering system exists with distinct odd square-free moduli.

Thank you!