Covering systems

Paul Balister

University of Memphis, USA

Recent Advances in Extremal Combinatorics
University of Oxford, December 4, 2018

Joint work with Béla Bollobás, Rob Morris,
Julian Sahasrabudhe, and Marius Tiba.

Covering Systems

A **covering system** is a finite collection of arithmetic progressions

$$(a_i \bmod d_i) := a_i + d_i\mathbb{Z}, \qquad i = 1, \dots, k,$$

that cover $\mathbb{Z}$:

$$\bigcup_{i=1}^{k} (a_i \bmod d_i) = \mathbb{Z}.$$

A **covering system** is a finite collection of arithmetic progressions

$$(a_i \bmod d_i) := a_i + d_i\mathbb{Z}, \qquad i = 1, \dots, k,$$

that cover $\mathbb{Z}$:

$$\bigcup_{i=1}^{k} (a_i \bmod d_i) = \mathbb{Z}.$$

Trivial example:

$$\begin{gathered}(0 \bmod d)\\(1 \bmod d)\\\vdots\\(d-1 \bmod d)\end{gathered}$$

Covering Systems

A **covering system** is a finite collection of arithmetic progressions

$$(a_i \bmod d_i) := a_i + d_i\mathbb{Z}, \qquad i = 1, \dots, k,$$

that cover $\mathbb{Z}$:

$$\bigcup_{i=1}^{k} (a_i \bmod d_i) = \mathbb{Z}.$$

Trivial example:

$$\begin{gathered} (0 \bmod d) \\ (1 \bmod d) \\ \vdots \\ (d-1 \bmod d) \end{gathered}$$

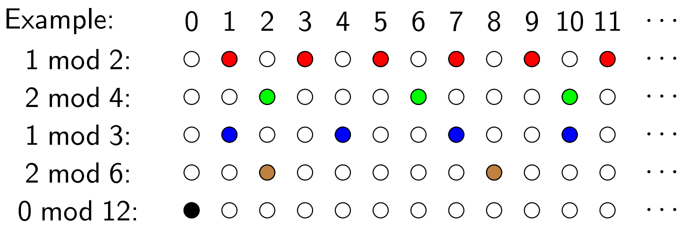
We are interested in the case when the moduli d_i are **distinct**, say

$$1 < d_1 < d_2 < \cdots < d_k.$$

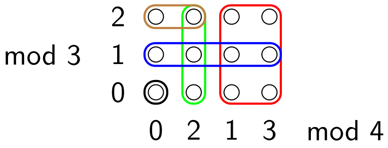
Covering Systems

Example:	0	1	2	3	4	5	6	7	8	9	10	11	···
1 mod 2:	○	●	○	●	○	●	○	●	○	●	○	●	···
2 mod 4:	○	○	●	○	○	○	●	○	○	○	●	○	···
1 mod 3:	○	●	○	○	●	○	○	●	○	○	●	○	···
2 mod 6:	○	○	●	○	○	○	○	○	●	○	○	○	···
0 mod 12:	●	○	○	○	○	○	○	○	○	○	○	○	···

Covering Systems



Or using the CRT: $\mathbb{Z}_{12} \cong \mathbb{Z}_4 \times \mathbb{Z}_3$



Some Questions

Question (Erdős, 1950)

If all the moduli d_i are distinct, can the smallest one $d_1 = \min d_i$ be arbitrarily large?

Some Questions

Question (Erdős, 1950)

If all the moduli d_i are distinct, can the smallest one $d_1 = \min d_i$ be arbitrarily large?

Question (Erdős–Selfridge, 1973)

Is there always at least one moduli d_i that is even?

Some Questions

Question (Erdős, 1950)

If all the moduli d_i are distinct, can the smallest one $d_1 = \min d_i$ be arbitrarily large?

Question (Erdős–Selfridge, 1973)

Is there always at least one moduli d_i that is even?

Question (Schinzel, 1967)

Is there always a pair of moduli d_i, d_j, $i \neq j$, with $d_i \mid d_j$?

Some Questions

Question (Erdős, 1950)

If all the moduli d_i are distinct, can the smallest one $d_1 = \min d_i$ be arbitrarily large?

Question (Erdős–Selfridge, 1973)

Is there always at least one moduli d_i that is even?

Question (Schinzel, 1967)

Is there always a pair of moduli d_i, d_j, $i \neq j$, with $d_i \mid d_j$?

Question (Erdős–Graham, 1980)

If all $d_i \in [n, Cn]$, is the density of the uncovered set $> f(C) > 0$ for all sufficiently large n?

Minimum Modulus

Question (Erdős, 1950)

If all the moduli d_i are distinct, can the smallest one d_1 be arbitrarily large?

Minimum Modulus

Question (Erdős, 1950)

If all the moduli d_i are distinct, can the smallest one d_1 be arbitrarily large?

Current record: $\exists$ covering system with $d_1 = 42$ (Tyler Owens, 2014).

Minimum Modulus

Question (Erdős, 1950)

If all the moduli d_i are distinct, can the smallest one d_1 be arbitrarily large?

Current record: $\exists$ covering system with $d_1 = 42$ (Tyler Owens, 2014).

In a major breakthrough, this was solved by:

Theorem (Hough, 2015)

If all the moduli d_i are distinct, $d_1 < 10^{16}$.

Minimum Modulus

Question (Erdős, 1950)

If all the moduli d_i are distinct, can the smallest one d_1 be arbitrarily large?

Current record: $\exists$ covering system with $d_1 = 42$ (Tyler Owens, 2014).

In a major breakthrough, this was solved by:

Theorem (Hough, 2015)

If all the moduli d_i are distinct, $d_1 < 10^{16}$.

We give a much simpler proof of this result, improving it to:

Theorem (BBMST, 2018)

If all the moduli d_i are distinct, $d_1 < 616000$.

Odd moduli

Question (Erdős–Selfridge, 1973)

Is there always at least one moduli d_i that is even?

Odd moduli

Question (Erdős–Selfridge, 1973)

Is there always at least one moduli d_i that is even?

Still unsolved, however:

Theorem (Hough, Nielsen, 2017)

An any covering system, there is a modulus that is divisible by 2 or 3.

Odd moduli

Question (Erdős–Selfridge, 1973)

Is there always at least one moduli d_i that is even?

Still unsolved, however:

Theorem (Hough, Nielsen, 2017)

An any covering system, there is a modulus that is divisible by 2 or 3.

The methods used are complex, and are only just enough for it to work.

Odd moduli

Question (Erdős–Selfridge, 1973)

Is there always at least one moduli d_i that is even?

Still unsolved, however:

Theorem (Hough, Nielsen, 2017)

An any covering system, there is a modulus that is divisible by 2 or 3.

The methods used are complex, and are only just enough for it to work.

Our techniques give a simple proof of this, and strengthens it to:

Theorem (BBMST, 2018)

In any covering system, $Q = \operatorname{lcm}\{d_i\}$ is divisible by 2, 9, or 15.

Odd moduli

We can also show

Theorem (BBMST, 2018+)

Any covering system with distinct **square free** *moduli must contain an even modulus.*

Odd moduli

We can also show

Theorem (BBMST, 2018+)

Any covering system with distinct **square free** *moduli must contain an even modulus.*

This last result is much harder to prove with our methods.

Schinzel's Conjecture

Question (Schinzel, 1967)

Is there always a pair of moduli d_i, d_j, $i \neq j$, with $d_i \mid d_j$?

Schinzel's Conjecture

Question (Schinzel, 1967)

Is there always a pair of moduli d_i, d_j, $i \neq j$, with $d_i \mid d_j$?

Schinzel showed that if no covering system with distinct, odd moduli exist, then this implies that for every polynomial $f(x) \in \mathbb{Z}[X]$ with $f \not\equiv 1$, $f(0) \neq 0$ and $f(1) \neq -1$, there exists an (infinite) arithmetic progression of values of $n \in \mathbb{Z}$ such that $x^n + f(x)$ is irreducible over the rationals. He also showed that this further implies that in any covering system with distinct moduli, one of the moduli divides another.

Schinzel's Conjecture

Question (Schinzel, 1967)

Is there always a pair of moduli d_i, d_j, $i \neq j$, with $d_i \mid d_j$?

Schinzel showed that if no covering system with distinct, odd moduli exist, then this implies that for every polynomial $f(x) \in \mathbb{Z}[X]$ with $f \not\equiv 1$, $f(0) \neq 0$ and $f(1) \neq -1$, there exists an (infinite) arithmetic progression of values of $n \in \mathbb{Z}$ such that $x^n + f(x)$ is irreducible over the rationals. He also showed that this further implies that in any covering system with distinct moduli, one of the moduli divides another.

Theorem (BBMST, 2018)

In any covering system with there must exists $i \neq j$ with $d_i \mid d_j$.

Erdős–Graham

Question (Erdős–Graham, 1980)

If all $d_i \in [n, Cn]$, is the density of the uncovered set $> f(C) > 0$ for all sufficiently large n?

Erdős–Graham

Question (Erdős–Graham, 1980)

If all $d_i \in [n, Cn]$, is the density of the uncovered set $> f(C) > 0$ for all sufficiently large n?

This was shown to be true (in a much stronger form) by Filaseta, Ford, Konyagin, Pomerance and Yu (2007), and was one of the first steps towards Hough's breakthrough result on the minimum modulus.

Erdős–Graham

Question (Erdős–Graham, 1980)

If all $d_i \in [n, Cn]$, is the density of the uncovered set $> f(C) > 0$ for all sufficiently large n?

This was shown to be true (in a much stronger form) by Filaseta, Ford, Konyagin, Pomerance and Yu (2007), and was one of the first steps towards Hough's breakthrough result on the minimum modulus.

They also asked:

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

Is it true that for any $C > 0$, if $d_i \geq n_0$ and $\sum \frac{1}{d_i} < C$ then the density of the uncovered set is $> f(C) > 0$ for all sufficiently large n_0?

Question (Erdős–Graham, 1980)

If all $d_i \in [n, Cn]$, is the density of the uncovered set $> f(C) > 0$ for all sufficiently large n?

This was shown to be true (in a much stronger form) by Filaseta, Ford, Konyagin, Pomerance and Yu (2007), and was one of the first steps towards Hough's breakthrough result on the minimum modulus.

They also asked:

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

Is it true that for any $C > 0$, if $d_i \geq n_0$ and $\sum \frac{1}{d_i} < C$ then the density of the uncovered set is $> f(C) > 0$ for all sufficiently large n_0?

Clearly the uncovered set can be made to have density $\leq \prod(1 - \frac{1}{d_i})$ by choosing the a_i greedily, so $\sum \frac{1}{d_i} < C$ is a necessary condition.

Extensions of Erdős–Graham

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

Is it true that for any $C > 0$, if $d_i \geq n_0$ and $\sum \frac{1}{d_i} < C$ then the density of the uncovered set is $> f(C) > 0$ for all sufficiently large n_0?

Unfortunately it is not sufficient:

Theorem (BBMST, 2018)

For any $\varepsilon > 0$, $n_0 > 0$, there exists a system of APs with distinct moduli d_i, $\sum \frac{1}{d_i} < 1$ and $d_i \geq n_0$, with the density of the uncovered set $< \varepsilon$.

Proof: explicit construction.

Extensions of Erdős–Graham

As $\sum \frac{1}{d_i} < C$ is not enough to give a large uncovered set, perhaps we should change the function $\frac{1}{d_i}$ to something a bit larger.

Extensions of Erdős–Graham

As $\sum \frac{1}{d_i} < C$ is not enough to give a large uncovered set, perhaps we should change the function $\frac{1}{d_i}$ to something a bit larger.

Theorem (BBMST, 2018)

If $\mu(d)$ is the multiplicative function defined by $\mu(p^e) = 1 + \frac{1}{p}(\log p)^{3+\varepsilon}$, then there exists $n_0 > 0$ such that for any C and any system of APs with distinct moduli d_i with $\sum \frac{\mu(d_i)}{d_i} < C$, $d_i \geq n_0$, the density of the uncovered set is $> e^{-4C}/2$.

Extensions of Erdős–Graham

As $\sum \frac{1}{d_i} < C$ is not enough to give a large uncovered set, perhaps we should change the function $\frac{1}{d_i}$ to something a bit larger.

Theorem (BBMST, 2018)

If $\mu(d)$ is the multiplicative function defined by $\mu(p^e) = 1 + \frac{1}{p}(\log p)^{3+\varepsilon}$, then there exists $n_0 > 0$ such that for any C and any system of APs with distinct moduli d_i with $\sum \frac{\mu(d_i)}{d_i} < C$, $d_i \geq n_0$, the density of the uncovered set is $> e^{-4C}/2$.

Note that n_0 is independent of C.

Extensions of Erdős–Graham

As $\sum \frac{1}{d_i} < C$ is not enough to give a large uncovered set, perhaps we should change the function $\frac{1}{d_i}$ to something a bit larger.

Theorem (BBMST, 2018)

If $\mu(d)$ is the multiplicative function defined by $\mu(p^e) = 1 + \frac{1}{p}(\log p)^{3+\varepsilon}$, then there exists $n_0 > 0$ such that for any C and any system of APs with distinct moduli d_i with $\sum \frac{\mu(d_i)}{d_i} < C$, $d_i \geq n_0$, the density of the uncovered set is $> e^{-4C}/2$.

Note that n_0 is independent of C.

This immediately implies Hough's result, that the minimum modulus in a covering system is bounded.

Extensions of Erdős–Graham

As $\sum \frac{1}{d_i} < C$ is not enough to give a large uncovered set, perhaps we should change the function $\frac{1}{d_i}$ to something a bit larger.

Theorem (BBMST, 2018)

If $\mu(d)$ is the multiplicative function defined by $\mu(p^e) = 1 + \frac{1}{p}(\log p)^{3+\varepsilon}$, then there exists $n_0 > 0$ such that for any C and any system of APs with distinct moduli d_i with $\sum \frac{\mu(d_i)}{d_i} < C$, $d_i \geq n_0$, the density of the uncovered set is $> e^{-4C}/2$.

Note that n_0 is independent of C.

This immediately implies Hough's result, that the minimum modulus in a covering system is bounded.

It also implies the original Erdős–Graham conjecture.

Extensions of Erdős–Graham

We also show that this result is close to best possible.

Theorem (BBMST, 2018)

For any $\lambda > 0$, if $\mu(d)$ is the multiplicative function defined by $\mu(p^e) = 1 + \frac{\lambda}{p}$, then for any $n_0 > 0$, $\varepsilon > 0$, $C > 0$, there exists a system of APs with distinct moduli such that $\sum \frac{\mu(d_i)}{d_i} < C$, $d_i \geq n_0$, and the density of the uncovered set is $< \varepsilon$.

Extensions of Erdős–Graham

We also show that this result is close to best possible.

Theorem (BBMST, 2018)

For any $\lambda > 0$, if $\mu(d)$ is the multiplicative function defined by $\mu(p^e) = 1 + \frac{\lambda}{p}$, then for any $n_0 > 0$, $\varepsilon > 0$, $C > 0$, there exists a system of APs with distinct moduli such that $\sum \frac{\mu(d_i)}{d_i} < C$, $d_i \geq n_0$, and the density of the uncovered set is $< \varepsilon$.

This leaves the exact threshold of $\mu(p^e)$ open. We know the threshold must lie between

$$1 + \frac{\Omega(1)}{p} \qquad \text{and} \qquad 1 + \frac{(\log p)^{3+o(1)}}{p}.$$

Setup for the proofs

Write $Q = \mathrm{lcm}\{d_i\} = p_1^{e_1} \dots p_n^{e_n}$. We can think of a covering system as a cover of the hypercuboid

$$\mathbb{Z}_Q = \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_n^{e_n}}.$$

Setup for the proofs

Write $Q = \mathrm{lcm}\{d_i\} = p_1^{e_1} \dots p_n^{e_n}$. We can think of a covering system as a cover of the hypercuboid

$$\mathbb{Z}_Q = \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_n^{e_n}}.$$

Let

$$Q_i = p_1^{e_1} \dots p_i^{e_i},$$

Setup for the proofs

Write $Q = \operatorname{lcm}\{d_i\} = p_1^{e_1} \dots p_n^{e_n}$. We can think of a covering system as a cover of the hypercuboid

$$\mathbb{Z}_Q = \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_n^{e_n}}.$$

Let

$$Q_i = p_1^{e_1} \dots p_i^{e_i},$$

We identify subsets

$$S \subseteq \mathbb{Z}_{Q_i} = \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_i^{e_i}}$$

with the subset

$$S \times \mathbb{Z}_{p_{i+1}^{e_{i+1}}} \subseteq \mathbb{Z}_{Q_{i+1}}$$

or

$$S \times \mathbb{Z}_{p_{i+1}^{e_{i+1}}} \times \dots \mathbb{Z}_{p_i^{e_i}} \subseteq \mathbb{Z}_Q$$

and we identify arithmetic progressions $(a_j \bmod d_j)$, $d_j \mid Q_i$, with the corresponding subset of $\mathbb{Z}_{Q_i}$.

Setup for the proofs

We 'reveal' the APs prime by prime, so all $d_j \mid Q_1$ in stage 1, all $d_j \mid Q_2$ in stage 2, etc.

Setup for the proofs

We 'reveal' the APs prime by prime, so all $d_j \mid Q_1$ in stage 1, all $d_j \mid Q_2$ in stage 2, etc.

Let

$D_i = \{d_j : d_j \mid Q_i\}$ be the set of all moduli revealed by stage i.

Setup for the proofs

We 'reveal' the APs prime by prime, so all $d_j \mid Q_1$ in stage 1, all $d_j \mid Q_2$ in stage 2, etc.

Let

$D_i = \{d_j : d_j \mid Q_i\}$ be the set of all moduli revealed by stage i.

$N_i = D_i \setminus D_{i-1}$ is the set of moduli newly revealed at stage i.

Setup for the proofs

We 'reveal' the APs prime by prime, so all $d_j \mid Q_1$ in stage 1, all $d_j \mid Q_2$ in stage 2, etc.

Let

$D_i = \{d_j : d_j \mid Q_i\}$ be the set of all moduli revealed by stage i.

$N_i = D_i \setminus D_{i-1}$ is the set of moduli newly revealed at stage i.

$B_i = \bigcup_{d_j \in N_i} (a_j \bmod d_j)$ be the subset of $\mathbb{Z}_Q$ removed at stage i.

Setup for the proofs

We 'reveal' the APs prime by prime, so all $d_j \mid Q_1$ in stage 1, all $d_j \mid Q_2$ in stage 2, etc.

Let

$D_i = \{d_j : d_j \mid Q_i\}$ be the set of all moduli revealed by stage i.

$N_i = D_i \setminus D_{i-1}$ is the set of moduli newly revealed at stage i.

$B_i = \bigcup_{d_j \in N_i} (a_j \bmod d_j)$ be the subset of $\mathbb{Z}_Q$ removed at stage i.

$R_i = \mathbb{Z}_Q \setminus \bigcup_{d_j \in D_i} (a_j \bmod d_j) = R_{i-1} \setminus B_i$
be the subset of $\mathbb{Z}_Q$ remaining after stage i.

Setup for the proofs

We construct a sequence of probability measures $\mathbb{P}_i$ on $\mathbb{Z}_Q = \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_n^{e_n}}$ which is uniform on each fibre of $x \in \mathbb{Z}_{Q_i}$, i.e., it is a product of a (non-trivial) measure on $\mathbb{Z}_{Q_i}$ (which we also call $\mathbb{P}_i$) with the uniform measure on $\mathbb{Z}_{Q/Q_i}$.

Setup for the proofs

We construct a sequence of probability measures $\mathbb{P}_i$ on $\mathbb{Z}_Q = \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_n^{e_n}}$ which is uniform on each fibre of $x \in \mathbb{Z}_{Q_i}$, i.e., it is a product of a (non-trivial) measure on $\mathbb{Z}_{Q_i}$ (which we also call $\mathbb{P}_i$) with the uniform measure on $\mathbb{Z}_{Q/Q_i}$.

The probability measure $\mathbb{P}_i$ on $\mathbb{Z}_{Q_i}$ is defined so that

Setup for the proofs

We construct a sequence of probability measures $\mathbb{P}_i$ on $\mathbb{Z}_Q = \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_n^{e_n}}$ which is uniform on each fibre of $x \in \mathbb{Z}_{Q_i}$, i.e., it is a product of a (non-trivial) measure on $\mathbb{Z}_{Q_i}$ (which we also call $\mathbb{P}_i$) with the uniform measure on $\mathbb{Z}_{Q/Q_i}$.

The probability measure $\mathbb{P}_i$ on $\mathbb{Z}_{Q_i}$ is defined so that

$\mathbb{P}_i(x) = \mathbb{P}_{i-1}(x)$ for each $x \in \mathbb{Z}_{Q_{i-1}}$

Setup for the proofs

We construct a sequence of probability measures $\mathbb{P}_i$ on $\mathbb{Z}_Q = \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_n^{e_n}}$ which is uniform on each fibre of $x \in \mathbb{Z}_{Q_i}$, i.e., it is a product of a (non-trivial) measure on $\mathbb{Z}_{Q_i}$ (which we also call $\mathbb{P}_i$) with the uniform measure on $\mathbb{Z}_{Q/Q_i}$.

The probability measure $\mathbb{P}_i$ on $\mathbb{Z}_{Q_i}$ is defined so that

$\mathbb{P}_i(x) = \mathbb{P}_{i-1}(x)$ for each $x \in \mathbb{Z}_{Q_{i-1}}$

$\mathbb{P}_i(x, y) \leq \frac{1}{1-\delta_i}\mathbb{P}_{i-1}(x, y)$ for each $(x, y) \in \mathbb{Z}_{Q_i} = \mathbb{Z}_{Q_{i-1}} \times \mathbb{Z}_{p_i^{e_i}}$, where $\delta_i \in (0, \frac{1}{2}]$ is an appropriately chosen constant.

Setup for the proofs

We construct a sequence of probability measures $\mathbb{P}_i$ on $\mathbb{Z}_Q = \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_n^{e_n}}$ which is uniform on each fibre of $x \in \mathbb{Z}_{Q_i}$, i.e., it is a product of a (non-trivial) measure on $\mathbb{Z}_{Q_i}$ (which we also call $\mathbb{P}_i$) with the uniform measure on $\mathbb{Z}_{Q/Q_i}$.

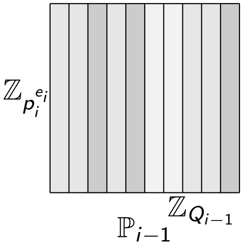
The probability measure $\mathbb{P}_i$ on $\mathbb{Z}_{Q_i}$ is defined so that

$\mathbb{P}_i(x) = \mathbb{P}_{i-1}(x)$ for each $x \in \mathbb{Z}_{Q_{i-1}}$

$\mathbb{P}_i(x, y) \leq \frac{1}{1-\delta_i}\mathbb{P}_{i-1}(x, y)$ for each $(x, y) \in \mathbb{Z}_{Q_i} = \mathbb{Z}_{Q_{i-1}} \times \mathbb{Z}_{p_i^{e_i}}$, where $\delta_i \in (0, \frac{1}{2}]$ is an appropriately chosen constant.

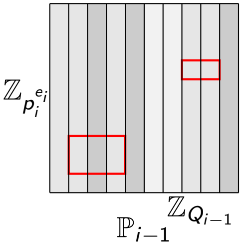
$\mathbb{P}_i(x, y)$ is as small as possible on the removed set B_i.

Setup for the proofs



$\mathbb{P}_{i-1}$ is defined on $\mathbb{Z}_{Q_{i-1}}$ and extended uniformly on each fibre $\{x\} \times \mathbb{Z}_{p_i^{e_i}} \subseteq \mathbb{Z}_{Q_{i-1}} \times \mathbb{Z}_{p_i^{e_i}} = \mathbb{Z}_{Q_i}$.

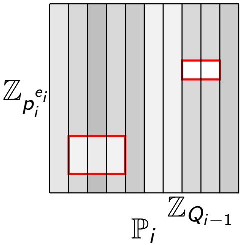
Setup for the proofs



$\mathbb{P}_{i-1}$ is defined on $\mathbb{Z}_{Q_{i-1}}$ and extended uniformly on each fibre $\{x\} \times \mathbb{Z}_{p_i^{e_i}} \subseteq \mathbb{Z}_{Q_{i-1}} \times \mathbb{Z}_{p_i^{e_i}} = \mathbb{Z}_{Q_i}$.

B_i is the region corresponding to the new APs.

Setup for the proofs

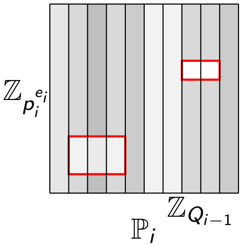


$\mathbb{P}_{i-1}$ is defined on $\mathbb{Z}_{Q_{i-1}}$ and extended uniformly on each fibre $\{x\} \times \mathbb{Z}_{p_i^{e_i}} \subseteq \mathbb{Z}_{Q_{i-1}} \times \mathbb{Z}_{p_i^{e_i}} = \mathbb{Z}_{Q_i}$.

B_i is the region corresponding to the new APs.

$\mathbb{P}_i$ is defined to give the same mass to each fibre, but shifted away from B_i.

Setup for the proofs



$\mathbb{P}_{i-1}$ is defined on $\mathbb{Z}_{Q_{i-1}}$ and extended uniformly on each fibre $\{x\} \times \mathbb{Z}_{p_i^{e_i}} \subseteq \mathbb{Z}_{Q_{i-1}} \times \mathbb{Z}_{p_i^{e_i}} = \mathbb{Z}_{Q_i}$.

B_i is the region corresponding to the new APs.

$\mathbb{P}_i$ is defined to give the same mass to each fibre, but shifted away from B_i.

But not so much that it increases the density by more than $1/(1-\delta_i)$ anywhere. Note that if less than δ_i of the fibre is removed, then no measure is placed inside B_i in that fibre.

Setup for the proofs

Formally, for each $x \in \mathbb{Z}_{Q_{i-1}}$, define

$$\alpha_i(x) = \frac{\mathbb{P}_{i-1}\big(x \cap B_i\big)}{\mathbb{P}_{i-1}(x)} = \frac{\big|\big\{y \in \mathbb{Z}_{p_i^{e_i}} : (x, y) \in B_i\big\}\big|}{p_i^{e_i}},$$

to be the proportion of the fibre of $x \in \mathbb{Z}_{Q_{i-1}}$ in $\mathbb{Z}_{Q_i}$ that is removed at stage i.

Setup for the proofs

Formally, for each $x \in \mathbb{Z}_{Q_{i-1}}$, define

$$\alpha_i(x) = \frac{\mathbb{P}_{i-1}\big(x \cap B_i\big)}{\mathbb{P}_{i-1}(x)} = \frac{\Big|\Big\{y \in \mathbb{Z}_{p_i^{e_i}} : (x,y) \in B_i\Big\}\Big|}{p_i^{e_i}},$$

to be the proportion of the fibre of $x \in \mathbb{Z}_{Q_{i-1}}$ in $\mathbb{Z}_{Q_i}$ that is removed at stage i.

Now define

$$\mathbb{P}_i(x,y) := \begin{cases} \max\Big\{0,\ \frac{\alpha_i(x)-\delta_i}{\alpha_i(x)(1-\delta_i)}\Big\} \cdot \mathbb{P}_{i-1}(x,y), & \text{if } (x,y) \in B_i; \\ \min\Big\{\frac{1}{1-\alpha_i(x)},\ \frac{1}{1-\delta_i}\Big\} \cdot \mathbb{P}_{i-1}(x,y), & \text{if } (x,y) \notin B_i. \end{cases}$$

Measure removed

We use a 2nd moment calculation to bound the amount of measure removed at each stage:

Lemma

$$\mathbb{P}_{i-1}(R_{i-1}) - \mathbb{P}_i(R_i) = \mathbb{P}_i(B_i) \leq \frac{\mathbb{E}_{i-1}(\alpha_i(x)^2)}{4\delta_i(1-\delta_i)}$$

Measure removed

We use a 2nd moment calculation to bound the amount of measure removed at each stage:

Lemma

$$\mathbb{P}_{i-1}(R_{i-1}) - \mathbb{P}_i(R_i) = \mathbb{P}_i(B_i) \le \frac{\mathbb{E}_{i-1}(\alpha_i(x)^2)}{4\delta_i(1-\delta_i)}$$

Proof: $\mathbb{P}_i(R_{i-1}) = \mathbb{P}_{i-1}(R_{i-1})$ as R_{i-1} is a union of complete fibres. Thus the measure removed is just $\mathbb{P}_i(R_{i-1} \setminus R_i) = \mathbb{P}_i(B_i)$, the $\mathbb{P}_i$-measure remaining inside B_i. But this is exactly

$$\mathbb{P}_i(B_i) = \mathbb{E}_{i-1}\frac{\max\{\alpha_i(x) - \delta_i, 0\}}{1-\delta_i}$$

Measure removed

We use a 2nd moment calculation to bound the amount of measure removed at each stage:

Lemma

$$\mathbb{P}_{i-1}(R_{i-1}) - \mathbb{P}_i(R_i) = \mathbb{P}_i(B_i) \le \frac{\mathbb{E}_{i-1}(\alpha_i(x)^2)}{4\delta_i(1-\delta_i)}$$

Proof: $\mathbb{P}_i(R_{i-1}) = \mathbb{P}_{i-1}(R_{i-1})$ as R_{i-1} is a union of complete fibres. Thus the measure removed is just $\mathbb{P}_i(R_{i-1} \setminus R_i) = \mathbb{P}_i(B_i)$, the $\mathbb{P}_i$-measure remaining inside B_i. But this is exactly

$$\mathbb{P}_i(B_i) = \mathbb{E}_{i-1} \frac{\max\{\alpha_i(x) - \delta_i, 0\}}{1-\delta_i}$$

and we can bound $\alpha - \delta \le \alpha^2/4\delta$ for all $\alpha > 0$ by rearranging the inequality $(\alpha - 2\delta)^2 \ge 0$.

Bounding the second moment

Write
$$\nu(d) = \prod_{p_j \mid d} \frac{1}{1-\delta_j}$$

Lemma

$$\mathbb{P}_i(a \bmod d) \le \frac{1}{d} \prod_{j \le i,\, p_j \mid d} \frac{1}{1-\delta_j} = \frac{\nu(\gcd(Q_i, d))}{d}.$$

Bounding the second moment

Write

$$\nu(d) = \prod_{p_j \mid d} \frac{1}{1-\delta_j}$$

Lemma

$$\mathbb{P}_i(a \bmod d) \le \frac{1}{d} \prod_{j \le i,\, p_j \mid d} \frac{1}{1-\delta_j} = \frac{\nu(\gcd(Q_i, d))}{d}.$$

Lemma

$$\mathbb{E}_{i-1}(\alpha_i(x)^2) \le \sum_{m_1 p_i^j,\, m_2 p_i^k \in N_i} p_i^{-j-k} \frac{\nu(\mathrm{lcm}(m_1, m_2))}{\mathrm{lcm}(m_1, m_2)}$$
$$\le \frac{1}{(p_i - 1)^2} \prod_{j<i} \Big(1 + \frac{3p_j - 1}{(p_j - 1)^2 (1-\delta_j)}\Big).$$

The ultimate uncovered region

By tracking the measure removed at each stage we can bound

$$\mathbb{P}_k(R_k) \geq 1 - \eta := 1 - \sum_i \frac{\mathbb{E}_{i-1}(\alpha_i(x)^2)}{4\delta_i(1-\delta_i)}.$$

If this is positive we know that there is an uncovered region.

The ultimate uncovered region

By tracking the measure removed at each stage we can bound

$$\mathbb{P}_k(R_k) \geq 1 - \eta := 1 - \sum_i \frac{\mathbb{E}_{i-1}(\alpha_i(x)^2)}{4\delta_i(1-\delta_i)}.$$

If this is positive we know that there is an uncovered region.

However it is also possible to bound R_k in the **uniform** measure $\mathbb{P}_0$ by tracking the average logarithmic distortion $\mathbb{E}_k[\max\{\log(\mathbb{P}_k(x)/\mathbb{P}_0(x)), 0\}]$.

Lemma

$$\mathbb{P}_0(R_k) \geq (1-\eta)\exp\Big(-\frac{2}{1-\eta}\sum_{d\in D_k}\frac{\nu(d)}{d}\Big)$$

Differences from Hough's method

In Hough's method, probability measures $\mathbb{P}_i$ are also defined. However measure is removed entirely from B_i, and then renormalized on the rest of the fibre.

Differences from Hough's method

In Hough's method, probability measures $\mathbb{P}_i$ are also defined. However measure is removed entirely from B_i, and then renormalized on the rest of the fibre.

Then fibres with too much measure removed must then also be removed, otherwise the measure becomes too distorted away from the uniform measure.

Differences from Hough's method

In Hough's method, probability measures $\mathbb{P}_i$ are also defined. However measure is removed entirely from B_i, and then renormalized on the rest of the fibre.

Then fibres with too much measure removed must then also be removed, otherwise the measure becomes too distorted away from the uniform measure.

As substantial measure is removed at each stage, it is necessary to process primes in groups, so at stage i, many new primes are considered.

Differences from Hough's method

In Hough's method, probability measures $\mathbb{P}_i$ are also defined. However measure is removed entirely from B_i, and then renormalized on the rest of the fibre.

Then fibres with too much measure removed must then also be removed, otherwise the measure becomes too distorted away from the uniform measure.

As substantial measure is removed at each stage, it is necessary to process primes in groups, so at stage i, many new primes are considered.

At each stage, the Lovász Local Lemma is needed to estimate the amount of measure in B_i, as B_i is now a much more complicated set.

Differences from Hough's method

In Hough's method, probability measures $\mathbb{P}_i$ are also defined. However measure is removed entirely from B_i, and then renormalized on the rest of the fibre.

Then fibres with too much measure removed must then also be removed, otherwise the measure becomes too distorted away from the uniform measure.

As substantial measure is removed at each stage, it is necessary to process primes in groups, so at stage i, many new primes are considered.

At each stage, the Lovász Local Lemma is needed to estimate the amount of measure in B_i, as B_i is now a much more complicated set.

Fibres in which the remaining measure is not sufficiently 'pseudo-random' must also be removed, otherwise problems may occur later.

Application of the method to the Hough–Nielsen 2-3 result

As an example, assume no d_j is divisible by 2 or 3. We will prove the Hough–Nielsen result that the APs cannot cover $\mathbb{Z}$ in this case. As no d_j is divisible by 2 or 3, we start with the third prime $p_3 = 5$.

Application of the method to the Hough–Nielsen 2-3 result

As an example, assume no d_j is divisible by 2 or 3. We will prove the Hough–Nielsen result that the APs cannot cover $\mathbb{Z}$ in this case. As no d_j is divisible by 2 or 3, we start with the third prime $p_3 = 5$.

We let

$$\pi_i = \prod_{3 \le j \le i} \Big(1 + \frac{3p_j - 1}{(p_j - 1)^2(1 - \delta_j)}\Big)$$

so that $\mathbb{E}_{i-1}(\alpha_i(x)^2) \le \frac{\pi_{i-1}}{(p_i - 1)^2}$.

Application of the method to the Hough–Nielsen 2-3 result

As an example, assume no d_j is divisible by 2 or 3. We will prove the Hough–Nielsen result that the APs cannot cover $\mathbb{Z}$ in this case. As no d_j is divisible by 2 or 3, we start with the third prime $p_3 = 5$.

We let
$$\pi_i = \prod_{3\le j\le i}\Big(1+\frac{3p_j-1}{(p_j-1)^2(1-\delta_j)}\Big)$$
so that $\mathbb{E}_{i-1}(\alpha_i(x)^2) \le \frac{\pi_{i-1}}{(p_i-1)^2}$.

We let $\mu_2 = 1$ and set
$$\mu_i = \mu_{i-1} - \frac{\pi_{i-1}}{4\delta_i(1-\delta_i)(p_i-1)^2}$$
so that, by induction, $\mathbb{P}_i(R_i) \ge \mu_i$.

Application of the method to the Hough–Nielsen 2-3 result

As an example, assume no d_j is divisible by 2 or 3. We will prove the Hough–Nielsen result that the APs cannot cover $\mathbb{Z}$ in this case. As no d_j is divisible by 2 or 3, we start with the third prime $p_3 = 5$.

We let

$$\pi_i = \prod_{3 \le j \le i} \Big(1 + \frac{3p_j - 1}{(p_j - 1)^2(1 - \delta_j)}\Big)$$

so that $\mathbb{E}_{i-1}(\alpha_i(x)^2) \le \frac{\pi_{i-1}}{(p_i - 1)^2}$.

We let $\mu_2 = 1$ and set

$$\mu_i = \mu_{i-1} - \frac{\pi_{i-1}}{4\delta_i(1 - \delta_i)(p_i - 1)^2}$$

so that, by induction, $\mathbb{P}_i(R_i) \ge \mu_i$.

It is enough to show that $\mu_i > 0$ for all $i \ge 3$.

Application of the method to the Hough–Nielsen 2-3 result

Rewriting in terms of $f_i := \frac{\pi_i}{\mu_i}$ we have $f_2 = 1$ and

$$f_i = f_{i-1} \cdot \frac{1 + \frac{3p_i - 1}{(p_i-1)^2(1-\delta_i)}}{1 - \frac{f_{i-1}}{4\delta_i(1-\delta_i)(p_i-1)^2}}$$

Application of the method to the Hough–Nielsen 2-3 result

Rewriting in terms of $f_i := \frac{\pi_i}{\mu_i}$ we have $f_2 = 1$ and

$$f_i = f_{i-1} \cdot \frac{1 + \frac{3p_i - 1}{(p_i-1)^2(1-\delta_i)}}{1 - \frac{f_{i-1}}{4\delta_i(1-\delta_i)(p_i-1)^2}}$$

We calculate the first few values assuming, say, $\delta_i = 0.2$.

k	p_k	f_k
3	5	2.32034632
4	7	4.371999733
5	11	6.569584328
	$\vdots$	
44	193	192.9769395
	$\vdots$	

Application of the method to the Hough–Nielsen 2-3 result

Rewriting in terms of $f_i := \frac{\pi_i}{\mu_i}$ we have $f_2 = 1$ and

$$f_i = f_{i-1} \cdot \frac{1 + \frac{3p_i - 1}{(p_i-1)^2(1-\delta_i)}}{1 - \frac{f_{i-1}}{4\delta_i(1-\delta_i)(p_i-1)^2}}$$

We calculate the first few values assuming, say, $\delta_i = 0.2$.

k	p_k	f_k
3	5	2.32034632
4	7	4.371999733
5	11	6.569584328
	$\vdots$	
44	193	192.9769395
	$\vdots$	

OK, so when do we stop?

Application of the method to the Hough–Nielsen 2-3 result

Lemma

If $k \geq 10$, $\mu_k > 0$, and $f_k \geq (\log k + \log\log k - 3)^2 k$, then the system does not cover.

Application of the method to the Hough–Nielsen 2-3 result

Lemma

If $k \geq 10$, $\mu_k > 0$, and $f_k \geq (\log k + \log\log k - 3)^2 k$, then the system does not cover.

Proof: we use the result that $p_k \geq (\log k + \log\log k - 1)k$ (Dusart, 1999) to prove by induction that this assumption on μ_k, f_k implies the same for $k + 1$.

Application of the method to the Hough–Nielsen 2-3 result

Lemma

If $k \geq 10$, $\mu_k > 0$, and $f_k \geq (\log k + \log\log k - 3)^2 k$, then the system does not cover.

Proof: we use the result that $p_k \geq (\log k + \log\log k - 1)k$ (Dusart, 1999) to prove by induction that this assumption on μ_k, f_k implies the same for $k+1$.

Now note that in the 2-3 problem, this condition holds for $p_{44} = 193$:

$$f_{44} = 192.9769395 < (\log 44 + \log\log 44 - 3)^2 \cdot 44 = 196.8258827. \qquad \square$$