Covering systems of congruences and the Lovász Local Lemma

Bob Hough

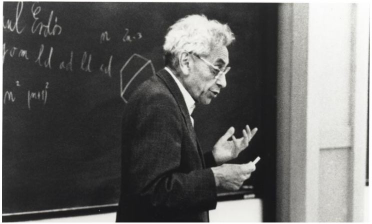
Institute for Advanced Study, Princeton

4 February, 2016

Outline

Lovász, Erdős

(a) Lászlo Lovász



(b) Paul Erdős

Basic tool: Lovász Local Lemma

The Lovász Local Lemma is a powerful combinatorial tool for handling dependent probability in the case where the dependence is local. It applies in a somewhat narrow set of circumstances with surprising results.

Basic tool: Lovász Local Lemma

Lemma (Lovász Local Lemma)

Let $A_1, A_2, ..., A_n$ be events in a probability space and $G = ([n], E)$ a dependency graph, such that, for each $1 \leq i \leq n$, event A_i is independent of the sigma-algebra generated by the events $\{A_j : (i,j) \notin E\}$. Suppose there is $0 < p < 1$ such that $\mathbf{P}(A_i) \leq p$ and that the degree of G is at most d. If

$$ep(d+1) \leq 1$$

then $\mathbf{P}\left(\bigcap_{i=1}^n \overline{A_i}\right) > 0$.

Separable coverings

Let $k \geq 1$. Say that a collection $\mathscr{C}$ of open unit balls of $\mathbb{R}^3$ is a k-covering if every point of $\mathbb{R}^3$ belongs to at least k balls. We say that $\mathscr{C}$ is *separable* if there exists a red-blue coloring of the balls such that both the red and blue balls are 1-covering.

Separable coverings

Theorem (Mani-Levitska-Pach)

Let $k \geq 1$ and let $\mathscr{C}$ be a k-covering of $\mathbb{R}^3$ such that no point of $\mathbb{R}^3$ is covered more than t times. If

$$t^3 \leq \frac{2^{k-19}}{e}$$

then the covering is decomposable.
Also, an upper bound on t is necessary.

Separable coverings

The proof that an upper bound on the multiplicity of covering is necessary is a difficult geometric-combinatorial construction, but the existence of a coloring in the case t is bounded has a beautiful and easy probabilistic proof.

Separable coverings

Proof sketch.

Consider only the part of $\mathbb{R}^3$ within a fixed box $\mathscr{B}$ – the case of $\mathbb{R}^3$ follows from a compactness argument. Say two points $x, y \in \mathscr{B}$ are equivalent if they are covered by the same set of balls. Color the balls red/blue independently, with equal probability. Let A_x be the event that x is covered by balls of only one color. We aim to show

$$\mathbf{P}\left(\bigcap_{x \in \mathscr{B}} \overline{A_x}\right) > 0.$$

Separable coverings

Proof sketch.

Recall A_x is the event that x is covered by balls of only one color.

- $\mathbf{P}(A_x) \leq 2 \times 2^{-k}$
- A_x is independent of all A_y for which $|x - y| > 3$. A dependency graph has vertices indexed by classes of points, with edges between points at distance < 3.
- The degree of the graph is bounded by $O(t^3)$

For $t = O\left(2^{\frac{k}{3}}\right)$ LLL applies to give the positive probability. $\square$

Lacunary rotations

Erdős posed the following two problems. Katznelson showed that the first can be reduced to the second, which has a positive answer.

Problem

Let $\{n_j\}$ be a lacunary sequence of positive integers, that is, there is $\epsilon > 0$ such that $\frac{n_{j+1}}{n_j} \geq 1 + \epsilon$. Let G be the Cayley graph of $\mathbb{Z}$ with this sequence, so i and j are connected if and only if $|i - j| = n_k$ for some k. Is the chromatic number of G finite?

Problem

Let $\{n_j\}$ be lacunary as above. Is there $\theta \in (0, 1)$ such that $\{n_j\theta\}$ is not dense in $\mathbb{R}/\mathbb{Z}$?

Lacunary rotations

The reduction is as follows.

- Let $\theta \in (0,1)$ and assume there exists $0 < \delta < \frac{1}{2}$ such that
$$\inf_j \|n_j\theta\|_{\mathbb{R}/\mathbb{Z}} \geq \delta.$$
- Break $\mathbb{R}/\mathbb{Z}$ into finitely many intervals of length at most δ, and color each a different color. Then color $n \in \mathbb{Z}$ according to the color of $n\theta$.

If m, n are connected in G then $\|m\theta - n\theta\|_{\mathbb{R}/\mathbb{Z}} = \|n_j\theta\|_{\mathbb{R}/\mathbb{Z}} \geq \delta$, and hence m and n receive a different color.

Lacunary rotations

Theorem (Peres-Schlag)

Let $0 < \epsilon < \frac{1}{4}$. Let $\{n_j\}_{j=1}^{\infty}$ be a sequence of integers satisfying

$$\forall j \geq 1, \qquad \frac{n_{j+1}}{n_j} \geq 1 + \epsilon.$$

There is $\theta \in \mathbb{R}/\mathbb{Z}$ and $c > 0$ such that

$$\inf_{j \geq 1} \|n_j \theta\|_{\mathbb{R}/\mathbb{Z}} \geq c\epsilon |\log \epsilon|^{-1}.$$

Lacunary rotations

(a) Yizzy Katznelson

(b) Yuval Peres

(c) Wilhelm Schlag

Lacunary rotations

The proof uses an LLL variant.

Lemma

Let $A_1, \ldots, A_n$ be events in a probability space. Suppose for each $1 \leq i \leq n$ there is $0 \leq x_i < 1$ and integer $m_i \geq 1$ such that

$$\mathbf{P}\left(A_i \middle| \bigcap_{j < i - m_i} \overline{A_j}\right) \leq x_i \prod_{j = i - m_i}^{i-1} (1 - x_j).$$

Then

$$\mathbf{P}\left(\bigcap_{j=1}^{n} \overline{A_j}\right) \geq \prod_{j=1}^{n} (1 - x_j).$$

Lacunary rotations

Proof sketch.

It suffices to consider finite lacunary sequences by compactness. Let $0 < \delta < \frac{1}{4}$. Choose m_j minimal such that $2^{m_j} > \frac{n_j}{\delta}$. Let A_j be the union of those dyadic intervals $\left[\frac{\ell}{2^{m_j}}, \frac{\ell+1}{2^{m_j}}\right)$ intersecting

$$\{\theta : \|n_j\theta\|_{\mathbb{R}/\mathbb{Z}} < \delta\}.$$

To within constants, A_j has the same intersection with all dyadic intervals of length $\gg \frac{1}{n_j}$. Since for $i < j - O(\epsilon^{-1}|\log \delta|)$, A_i is determined on such intervals, the Lovász condition holds for $\delta = O\left(\frac{\epsilon}{|\log \epsilon|}\right)$ and $\operatorname{meas}\left(\bigcap_{j=1}^n \overline{A_j}\right) > 0$. $\square$

Outline

Covering systems

A distinct covering system of congruences

$$(a_i \bmod m_i), \qquad 1 < m_1 < m_2 < \ldots < m_k$$

is a collection of arithmetic progressions such that

$$\mathbb{Z} = (a_1 \bmod m_1) \cup (a_2 \bmod m_2) \cup \ldots \cup (a_k \bmod m_k).$$

History

Romanoff (1934) showed that integers of the form $2^k + p$, p prime, have a positive density. This is surprising because the number of (k, p) such that $2^k + p \leq x$ is of order x.

Erdős (1950), answering a question of Romanoff, found an arithmetic progression of odd integers, none of which is of the form $2^k + p$. His proof uses the following covering system.

History

$$\ldots, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14,$$
$$15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, \ldots$$

History

$(0 \bmod 2)$

$$\ldots,\underline{0}, 1, \underline{2}, 3, \underline{4}, 5, \underline{6}, 7, \underline{8}, 9, \underline{10}, 11, \underline{12}, 13, \underline{14},$$
$$15, \underline{16}, 17, \underline{18}, 19, \underline{20}, 21, \underline{22}, 23, \underline{24}, 25, \underline{26}, 27, \underline{28}, 29, \ldots$$

History

$$(0 \bmod 2) \cup (0 \bmod 3)$$

$$\ldots, \underline{0}, 1, \underline{2}, \underline{3}, \underline{4}, 5, \underline{6}, 7, \underline{8}, \underline{9}, \underline{10}, 11, \underline{12}, 13, \underline{14},$$
$$\underline{15}, \underline{16}, 17, \underline{18}, 19, \underline{20}, \underline{21}, \underline{22}, 23, \underline{24}, 25, \underline{26}, \underline{27}, \underline{28}, 29, \ldots$$

History

$$(0 \bmod 2) \cup (0 \bmod 3) \cup (1 \bmod 4)$$

$$\ldots, \underline{0}, \underline{\textcolor{red}{1}}, \underline{2}, \underline{3}, \underline{4}, \underline{\textcolor{red}{5}}, \underline{6}, 7, \underline{8}, \underline{\textcolor{red}{9}}, \underline{10}, 11, \underline{12}, \underline{\textcolor{red}{13}}, \underline{14},$$
$$\underline{15}, \underline{16}, \underline{\textcolor{red}{17}}, \underline{18}, 19, \underline{20}, \underline{\textcolor{red}{21}}, \underline{22}, 23, \underline{24}, \underline{\textcolor{red}{25}}, \underline{26}, \underline{27}, \underline{28}, \underline{\textcolor{red}{29}}, \ldots$$

History

$$(0 \bmod 2) \cup (0 \bmod 3) \cup (1 \bmod 4) \cup (3 \bmod 8)$$

$$\ldots, \underline{0}, \underline{1}, \underline{2}, \underline{\textcolor{red}{3}}, \underline{4}, \underline{5}, \underline{6}, 7, \underline{8}, \underline{9}, \underline{10}, \underline{\textcolor{red}{11}}, \underline{12}, \underline{13}, \underline{14},$$
$$\underline{15}, \underline{16}, \underline{17}, \underline{18}, \underline{\textcolor{red}{19}}, \underline{20}, \underline{21}, \underline{22}, 23, \underline{24}, \underline{25}, \underline{26}, \underline{\textcolor{red}{27}}, \underline{28}, \underline{29}, \ldots$$

History

$$(0 \bmod 2) \cup (0 \bmod 3) \cup (1 \bmod 4) \cup (3 \bmod 8)$$
$$\cup\, (7 \bmod 12)$$

$$\ldots, \underline{0}, \underline{1}, \underline{2}, \underline{3}, \underline{4}, \underline{5}, \underline{6}, \underline{7}, \underline{8}, \underline{9}, \underline{10}, \underline{11}, \underline{12}, \underline{13}, \underline{14},$$
$$\underline{15}, \underline{16}, \underline{17}, \underline{18}, \underline{19}, \underline{20}, \underline{21}, \underline{22}, 23, \underline{24}, \underline{25}, \underline{26}, \underline{27}, \underline{28}, \underline{29}, \ldots$$

History

$$(0 \bmod 2) \cup (0 \bmod 3) \cup (1 \bmod 4) \cup (3 \bmod 8)$$
$$\cup\, (7 \bmod 12) \cup (23 \bmod 24)$$

$$\ldots, \underline{0}, \underline{1}, \underline{2}, \underline{3}, \underline{4}, \underline{5}, \underline{6}, \underline{7}, \underline{8}, \underline{9}, \underline{10}, \underline{11}, \underline{12}, \underline{13}, \underline{14},$$
$$\underline{15}, \underline{16}, \underline{17}, \underline{18}, \underline{19}, \underline{20}, \underline{21}, \underline{22}, \underline{23}, \underline{24}, \underline{25}, \underline{26}, \underline{27}, \underline{28}, \underline{29}, \ldots$$

History

Erdős' proof:
Let x belong to the progression

$$x \in (2^0 \bmod 3) \cap (2^1 \bmod 5) \cap (2^0 \bmod 7) \cap (2^7 \bmod 13) \\ \cap (2^3 \bmod 17) \cap (2^{23} \bmod 241)$$

Then for any k, $x - 2^k$ is divisible by one of $3, 5, 7, 13, 17, 241$. To make sure that $x - 2^k$ is never equal to one of these primes, further restrict x to a residue class modulo a large enough power of 2.

Exact covering systems

A covering system is exact if $\frac{1}{m_1} + \cdots + \frac{1}{m_k} = 1$.

Theorem (Newman)

Every exact covering system has a repeated modulus.

Proof.

Suppose that $\mathbb{Z} = \bigsqcup_{i=1}^{k} (a_i \bmod m_i)$ with each $m_i > 1$ and for each i, $0 \leq a_i < m_i$. Then

$$\frac{1}{1-z} = \sum_{i=1}^{k} \frac{z^{a_i}}{1-z^{m_i}}.$$

In order for the poles on left and right to match, it is necessary that the largest modulus appears with multiplicity > 1. $\square$

Two well-known problems

1. From the 1950 paper, Erdős: For each $M > 1$, is there a cover with
$$M < m_1 < m_2 < \ldots < m_k \qquad ?$$
2. Erdős, Selfridge: Is there a cover with
$$1 < m_1 < m_2 < \ldots < m_k$$
all odd?

Past results

Some records for the minimum modulus:

$9, 18, 20$	Churchhouse, Krukenberg, Choi	1968-71
24	Morikawa	1980s
25	Gibson	2006
40	Nielsen	2009

Past results

Filaseta, Ford, Konyagin, Pomerance, Yu (2007):
As $M \to \infty$, if $M < m_1 < m_2 < \ldots < m_k$ are covering moduli then

$$\sum \frac{1}{m_i} \to \infty$$

as a function of M.

Main theorem

Theorem (H. 2015)

Any distinct covering system has $m_1 < 10^{16}$.

Theorem (H., Nielsen 2015 (in progress))

Any distinct covering system has a modulus divisible by either 2 or 3.

Builds on work of FFKPY '07.

Ideas in the argument

$M = 10^{16}$ (a large fixed constant).
Assume that $\mathscr{M} \subset \{m \in \mathbb{Z}, m > M\}$ is a finite set of moduli. For each $m \in \mathscr{M}$ let congruence $a_m \bmod m$ be given.
Let the unsifted set be

$$R = \left(\bigcup_{m \in \mathscr{M}} (a_m \bmod m) \right)^c.$$

We show that the density of R is > 0.

Ideas in the argument

Let $Q = \mathrm{LCM}(m : m \in \mathscr{M})$. The density of the unsifted set

$$R = \left(\bigcup_{m \in \mathscr{M}} (a_m \bmod m)\right)^c \subset \mathbb{Z}/Q\mathbb{Z}$$

is estimated in stages.

Set $1 < P_0 < P_1 < P_2 < \ldots$, $P_i \to \infty$ thresholds, and

$$Q_i = \prod_{p < P_i, p^j \| Q} p^j.$$

Let $R_0 \supset R_1 \supset R_2 \supset \ldots$

$$R_i = \left(\bigcup_{m \in \mathscr{M} : m | Q_i} (a_m \bmod m)\right)^c$$

$R = R_i$ eventually.

Ideas in the argument

Recall R_i is the unsifted set after the ith stage,

$$R_i = \left(\bigcup_{m|Q_i} (a_m \bmod m) \right)^c$$

with $Q_i = \prod_{p<P_i, p^j \| Q} p^j$.

We assume that P_0 is sufficiently small as compared to the minimum modulus M so that P_0-smooth numbers larger than M are sparse. Thus the density of R_0 can be estimated with a union bound, that is, for some $0 < \delta < 1$,

$$\begin{aligned} \mathrm{dens}(R_0) &\geq 1 - \sum_{m \in \mathscr{M}, m|Q_0} \mathrm{dens}(a_m \bmod m) \\ &= 1 - \sum_{m \in \mathscr{M}, m|Q_0} \frac{1}{m} \geq 1 - \delta. \end{aligned}$$

Ideas in the argument

The proof now proceeds by induction.

- Think of $\mathbb{Z}/Q_{i+1}\mathbb{Z}$ as fibered over $\mathbb{Z}/Q_i\mathbb{Z}$, so that R_{i+1} exists in fibers over R_i.
- Estimate the density of R_{i+1} within individual fibers above R_i.

Schematic

For instance, suppose that the previous stage was determined by the congruences (0 mod 2), (0 mod 5) and (1 mod 10). ($Q_i = 10$)

$$\underline{0} \quad \underline{1} \quad \underline{2} \quad 3 \quad \underline{4} \quad \underline{5} \quad \underline{6} \quad 7 \quad \underline{8} \quad 9$$

Schematic

For instance, suppose that the previous stage was determined by the congruences (0 mod 2), (0 mod 5) and (1 mod 10). ($Q_i = 10$)

$\underline{0}$	$\underline{1}$	$\underline{2}$	3	$\underline{4}$	$\underline{5}$	$\underline{6}$	7	$\underline{8}$	9
$\underline{10}$	$\underline{11}$	$\underline{12}$	13	$\underline{14}$	$\underline{15}$	$\underline{16}$	17	$\underline{18}$	19
$\underline{20}$	$\underline{21}$	$\underline{22}$	23	$\underline{24}$	$\underline{25}$	$\underline{26}$	27	$\underline{28}$	29
$\underline{30}$	$\underline{31}$	$\underline{32}$	33	$\underline{34}$	$\underline{35}$	$\underline{36}$	37	$\underline{38}$	39
$\underline{40}$	$\underline{41}$	$\underline{42}$	43	$\underline{44}$	$\underline{45}$	$\underline{46}$	47	$\underline{48}$	49
$\underline{50}$	$\underline{51}$	$\underline{52}$	53	$\underline{54}$	$\underline{55}$	$\underline{56}$	57	$\underline{58}$	59
$\underline{60}$	$\underline{61}$	$\underline{62}$	63	$\underline{64}$	$\underline{65}$	$\underline{66}$	67	$\underline{68}$	69
$\underline{70}$	$\underline{71}$	$\underline{72}$	73	$\underline{74}$	$\underline{75}$	$\underline{76}$	77	$\underline{78}$	79
$\underline{80}$	$\underline{81}$	$\underline{82}$	83	$\underline{84}$	$\underline{85}$	$\underline{86}$	87	$\underline{88}$	89

And the next stage contains the congruences

Schematic

For instance, suppose that the previous stage was determined by the congruences (0 mod 2), (0 mod 5) and (1 mod 10). ($Q_i = 10$)

0	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47	48	49
50	51	52	53	54	55	56	57	58	59
60	61	62	63	64	65	66	67	68	69
70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89

And the next stage contains the congruences (3 mod 18)

Schematic

For instance, suppose that the previous stage was determined by the congruences (0 mod 2), (0 mod 5) and (1 mod 10). ($Q_i = 10$)

0	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27	28	29
30	31	32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47	48	49
50	51	52	53	54	55	56	57	58	59
60	61	62	63	64	65	66	67	68	69
70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89

And the next stage contains the congruences (3 mod 18) and (4 mod 15). ($Q_{i+1} = 90$)

Ideas in the argument

When estimating $R_{i+1} \subset \mathbb{Z}/Q_{i+1}\mathbb{Z}$ in fibers above $R_i \subset \mathbb{Z}/Q_i\mathbb{Z}$,

- R_{i+1} in the fiber above $r \in R_i$ is determined by congruences to moduli m with $m|Q_{i+1}$, $m \nmid Q_i$.
- Each such m has a unique factorization as $m_0 n$ where $m_0|Q_i$ and n has all of its prime factors in the interval $(P_i, P_{i+1}]$. This set of n's we call the 'new factors' $\mathscr{N}_{i+1}$.
- We group congruences according to new factor n and fiber r

$$A_{n,r} = \{a_m \bmod n : m = m_0 n, a_m \equiv r \bmod m_0\}.$$

Thus

$$(r \bmod Q_i) \cap R_{i+1} = (r \bmod Q_i) \setminus \bigcup_{n \in \mathscr{N}_{i+1}} A_{n,r}.$$

Schematic

In the earlier example, when $r \equiv 9 \bmod 10$

$$
\begin{array}{cccccccccc}
\underline{0} & \underline{1} & \underline{2} & \underline{3} & \color{red}{\underline{4}} & \underline{5} & \underline{6} & 7 & \underline{8} & 9 \\
\underline{10} & \underline{11} & \underline{12} & 13 & \underline{14} & \underline{15} & \underline{16} & 17 & \underline{18} & \color{red}{\underline{19}} \\
\underline{20} & \underline{21} & \underline{22} & 23 & \underline{24} & \underline{25} & \underline{26} & 27 & \underline{28} & 29 \\
\underline{30} & \underline{31} & \underline{32} & 33 & \color{red}{\underline{34}} & \underline{35} & \underline{36} & 37 & \underline{38} & \underline{39} \\
\underline{40} & \underline{41} & \underline{42} & 43 & \underline{44} & \underline{45} & \underline{46} & 47 & \underline{48} & \color{red}{\underline{49}} \\
\underline{50} & \underline{51} & \underline{52} & 53 & \underline{54} & \underline{55} & \underline{56} & \underline{57} & \underline{58} & 59 \\
\underline{60} & \underline{61} & \underline{62} & 63 & \color{red}{\underline{64}} & \underline{65} & \underline{66} & 67 & \underline{68} & 69 \\
\underline{70} & \underline{71} & \underline{72} & 73 & \underline{74} & \underline{75} & \underline{76} & 77 & \underline{78} & \color{red}{\underline{79}} \\
\underline{80} & \underline{81} & \underline{82} & 83 & \underline{84} & \underline{85} & \underline{86} & 87 & \underline{88} & 89 \\
 & & & & & & & & & \uparrow \\
 & & & & & & & & & r
\end{array}
$$

the red elements above r are the set $A_{3,r}$.

Heuristic

A heuristic: the distribution of sizes $|A_{n,r} \bmod nQ_i|$ is key.

- For each $n \in \mathscr{N}_{i+1}$, when varying r in the whole set $\mathbb{Z}/Q_i\mathbb{Z}$ $|A_{n,r} \bmod nQ_i|$ has a distribution with mean $\approx \log P_i$.
- Sieving by $A_{n,r}$, is independent of any congruences defined to moduli coprime to n (Chinese Remainder Theorem).

Total independence would give a density in fiber r of

$$\prod_{n \in \mathscr{N}_{i+1}} \left(1 - \frac{|A_{n,r} \bmod nQ_i|}{n}\right) \approx \prod_{n \in \mathscr{N}_{i+1}} \left(1 - \frac{\log P_i}{n}\right) \approx P_{i+1}^{-O(1)},$$

which would allow the sieving process to continue into the next stage.

Difficulties

There are two problems with the heuristic.

1. For most $n_1, n_2 \in \mathscr{N}_{i+1}$, $(n_1, n_2) > 1$, so that sieving by the sets $A_{n_1,r}$ and $A_{n_2,r}$ is not independent.
2. We vary $r \in R_i$, which is a small and irregular subset of $\mathbb{Z}/Q_i\mathbb{Z}$, so the typical behavior of $|A_{n,r}|$ in the set of interest is unknown.

Basic tool: Lovász Local Lemma

Lemma (Lovász Local Lemma, relative form)

Let $A_1, A_2, \ldots, A_n$ be events in a probability space with dependency graph G. Let real numbers $x_1, x_2, \ldots, x_n$ satisfy $0 \le x_i < 1$, and for each $1 \le i \le n$,

$$\mathbf{P}(A_i) \le x_i \prod_{(i,j)\in E} (1 - x_j).$$

Then for any $1 \le m \le n$

$$\mathbf{P}\left(\bigcap_{i=1}^{n} A_i^c\right) \ge \mathbf{P}\left(\bigcap_{i=1}^{m} A_i^c\right) \cdot \prod_{j=m+1}^{n} (1 - x_j) \ge \prod_{i=1}^{n} (1 - x_i).$$

Solution ideas

In our context, for $r \in R_i$ and $n \in \mathscr{N}_{i+1}$, sieving by $A_{n,r}$ mod n is an event with probability $\frac{|A_{n,r}|}{n}$. By the Chinese Remainder Theorem, a valid dependency graph has edges between n_1 and n_2 when $(n_1, n_2) > 1$.

Solution ideas

A crucial feature of our argument is that, within the good fibers $r \in R_i$ where LLL applies, the relative form of LLL also guarantees that the set $(r \bmod Q_i) \cap R_{i+1}$ is *well-distributed* in the sense that for each $n \in \mathscr{N}_{i+1}$,

$$\max_{b \bmod n} \frac{|R_{i+1} \cap (r \bmod Q_i) \cap (b \bmod n) \bmod Q_{i+1}|}{|R_{i+1} \cap (r \bmod Q_i) \bmod Q_{i+1}|} \leq \frac{e^{O(\#\{p|n\})}}{n}.$$

This is deduced from the relative form of the Local Lemma.

Summary

Two further ingredients go into our argument.

1. Expectations are calculated with respect to a pseudo-random measure which is adjusted after each stage of the argument. This measure ensures that the residual set always appears large and well-distributed with respect to the measure.
2. The sizes of the sieving sets are controlled on average with moments, taken with respect to the pseudo-random measure.

Optimization

In ongoing joint work with Pace Nielsen optimizing aspects of the argument we've considered the following issues.

- An extremal form of the Lovász Local Lemma found by Shearer relates the lemma to the partition function of a hard-core lattice gas from statistical mechanics.
- The graph of the partition function has a natural decomposition into cliques indexed by primes.
- The logarithmic derivative of the partition function at prime variables has an expansion in primitive objects (Penrose trees) analogous to the factorization of the Riemann zeta function as a product over primes.

Optimization

- Whereas the original solution used convexity to find Lovász weights, our current formulation bounds the tree expansion in the logarithmic derivative of the partition function using a stochastic fixed point equation.
- We have been analyzing the inverse problem of determining sieving sets which are extremal for the tree expansion in order to exploit extra structure in these examples.

Outline

Open problems

Let $\alpha, \beta \in \mathbb{R}$ with $\alpha > 0$. The *Beatty sequence* $S(\alpha, \beta)$ is defined to be

$$S(\alpha, \beta) = \{\lfloor \alpha n + \beta \rfloor\}_{n=1}^{\infty}.$$

Conjecture (Fraenkel)

If $m \geq 2$ and $\{S(\alpha_i, \beta_i), i = 1, \ldots, m\}$ are Beatty sequences partitioning the positive integers then $\frac{\alpha_i}{\alpha_j} \in \mathbb{Z}$ for some $i \neq j$.

Open problems

Short of resolving the odd covering problem, ruling out distinct covering systems with somewhat more restrictive conditions has applications to deciding the irreducibility of families of polynomials.

Related problems

There has recently been a spectacular contribution of probability theory to number theory, resolving the Erdős Discrepancy Problem.

Theorem (Tao, Polymath5)

Let $f : \mathbb{N} \to \{\pm 1\}$. The discrepancy is infinite:

$$\sup_{n,d\in\mathbb{N}} \left| \sum_{j=1}^{n} f(jd) \right| = \infty.$$

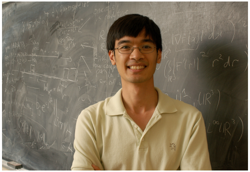


Figure : Terence Tao

Discrepancy problem

The argument considers stochastic multiplicative functions, which is an active area of current research. One hopes for further exciting contributions of probability to number theory, including more applications of the Lovász Local Lemma.

Thanks for coming!

Deducing well-distribution for good fibers

Recall that for good $r \in R_i^*$ we want the bound

$$\max_{b \bmod n} \frac{|R_{i+1} \cap (r \bmod Q_i) \cap (b \bmod n) \bmod Q_{i+1}|}{|R_{i+1} \cap (r \bmod Q_i) \bmod Q_{i+1}|} \leq \frac{e^{O(\#\{p|n\})}}{n}.$$

Applying LLL:

$$\begin{aligned}
\mathrm{LHS} &= \frac{\mathbf{P}\left((b \bmod n) \cap \bigcap_{n' \in \mathcal{N}_{i+1}} A_{n',r}^c\right)}{\mathbf{P}\left(\bigcap_{n' \in \mathcal{N}_{i+1}} A_{n',r}^c\right)} \\
&\leq \frac{\mathbf{P}\left((b \bmod n) \cap \bigcap_{n' \in \mathcal{N}_{i+1}, (n',n)=1} A_{n',r}^c\right)}{\mathbf{P}\left(\bigcap_{n' \in \mathcal{N}_{i+1}} A_{n',r}^c\right)} \\
&= \frac{1}{n} \frac{\mathbf{P}\left(\bigcap_{n' \in \mathcal{N}_{i+1}, (n',n)=1} A_{n',r}^c\right)}{\mathbf{P}\left(\bigcap_{n' \in \mathcal{N}_{i+1}} A_{n',r}^c\right)}.
\end{aligned}$$

Deducing well-distribution for good fibers

By relative LLL the ratio of probabilities

$$\frac{\mathbf{P}\left(\bigcap_{n'\in\mathscr{N}_{i+1},(n',n)=1} A_{n',r}^c\right)}{\mathbf{P}\left(\bigcap_{n'\in\mathscr{N}_{i+1}} A_{n',r}^c\right)}$$

is bounded by

$$\begin{aligned}\prod_{n'\in\mathscr{N}_{i+1},(n',n)=1}(1-x_{n'})^{-1} &\leq \prod_{p|n}\prod_{n'\in\mathscr{N}_{i+1},p|n'}(1-x_{n'})^{-1}\\ &\lesssim \prod_{p|n}\exp\left(\sum_{n'\in\mathscr{N}_{i+1},p|n'}\frac{|A_{n',r}|e^{\lambda\omega(n)}}{n'}\right)\\ &\lesssim \exp(O(\#\{p|n\})).\end{aligned}$$

Approximate covering systems

Theorem (Ford, H., unpublished)

For any $\epsilon, M > 0$ *there is a set* $\mathscr{M} \subseteq \mathbb{Z}_{>M}$ *such that* $\sum_{m \in \mathscr{M}} \frac{1}{m} < 1$, *with congruences* $\{a_m \bmod m : m \in \mathscr{M}\}$ *such that*

$$\operatorname{dens}\left(\bigcup_{m \in \mathscr{M}} (a_m \bmod m)\right) \geq 1 - \epsilon.$$