USING UNCERTAINTY TO ESTABLISH CERTAINTY

Po-Shen Loh, Princeton University

IPAM Fall 2009

Combinatorics:

Methods and Applications in

Mathematics and Computer Science

Sociology

Observation (S. Szalai, sociologist)

Every group of about 20 children contains a set of 4 children, any two of which are friends, or a set of 4 children, no two of which are friends.

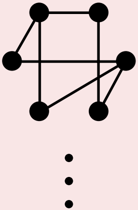
Sociology . . . or Ramsey Theory?

Observation (S. Szalai, sociologist)

Every group of about 20 children contains a set of 4 children, any two of which are friends, or a set of 4 children, no two of which are friends.

. . . but after discussion with Hungarian mathematicians Erdős, Turán, and Sós:

Ramsey number $R(4, 4)$



Draw 18 points, and connect some pairs of them by lines. No matter how this is done, there will always exist either:

- a set of 4 points, with all pairs connected, or
- a set of 4 points, with no pairs connected.

Definition

Let $R(r, s)$ be the smallest integer such that every graph with $R(r, s)$ vertices contains either a clique of size r or an independent set of size s.

Upper bounds for Ramsey numbers

Definition

Let $R(r,s)$ be the smallest integer such that every graph with $R(r,s)$ vertices contains either a clique of size r or an independent set of size s.

Erdős-Szekeres (1935)

Every graph G with $\binom{r+s-2}{r-1}$ vertices contains either a clique of size r or an independent set of size s, i.e., $R(r,s) \leq \binom{r+s-2}{r-1}$.

Upper bounds for Ramsey numbers

Definition

Let $R(r,s)$ be the smallest integer such that every graph with $R(r,s)$ vertices contains either a clique of size r or an independent set of size s.

Erdős-Szekeres (1935)

Every graph G with $\binom{r+s-2}{r-1}$ vertices contains either a clique of size r or an independent set of size s, i.e., $R(r,s) \leq \binom{r+s-2}{r-1}$.

Proof. Induction on $r+s$. Let $u_{r,s} = \binom{r+s-2}{r-1}$.
Since $u_{r,s} = u_{r-1,s} + u_{r,s-1}$, any vertex $v \in G$ has either:

- at least $u_{r-1,s}$ neighbors, or
- at least $u_{r,s-1}$ non-nbrs.

Upper bounds for Ramsey numbers

Definition

Let $R(r,s)$ be the smallest integer such that every graph with $R(r,s)$ vertices contains either a clique of size r or an independent set of size s.

Erdős-Szekeres (1935)

Every graph G with $\binom{r+s-2}{r-1}$ vertices contains either a clique of size r or an independent set of size s, i.e., $R(r,s) \leq \binom{r+s-2}{r-1}$.

Proof. Induction on $r+s$. Let $u_{r,s} = \binom{r+s-2}{r-1}$.

Since $u_{r,s} = u_{r-1,s} + u_{r,s-1}$, any vertex $v \in G$ has either:

- at least $u_{r-1,s}$ neighbors $\Rightarrow$ clique of size $r-1$
- at least $u_{r,s-1}$ non-nbrs.

Upper bounds for Ramsey numbers

Definition

Let $R(r,s)$ be the smallest integer such that every graph with $R(r,s)$ vertices contains either a clique of size r or an independent set of size s.

Erdős-Szekeres (1935)

Every graph G with $\binom{r+s-2}{r-1}$ vertices contains either a clique of size r or an independent set of size s, i.e., $R(r,s) \le \binom{r+s-2}{r-1}$.

Proof. Induction on $r+s$. Let $u_{r,s} = \binom{r+s-2}{r-1}$.
Since $u_{r,s} = u_{r-1,s} + u_{r,s-1}$, any vertex $v \in G$ has either:

- at least $u_{r-1,s}$ neighbors $\Rightarrow$ clique of size $r-1$
- at least $u_{r,s-1}$ non-nbrs. $\Rightarrow$ independent set of size $s-1$. $\square$

Upper bounds for Ramsey numbers

Erdős-Szekeres (1935)

Every graph G with $\binom{r+s-2}{r-1}$ vertices contains either a clique of size r or an independent set of size s, i.e., $R(r,s) \leq \binom{r+s-2}{r-1}$.

Erdős-Szekeres (1935)

Every graph G with $\binom{r+s-2}{r-1}$ vertices contains either a clique of size r or an independent set of size s, i.e., $R(r,s) \leq \binom{r+s-2}{r-1}$.

Upper bounds for Ramsey numbers

Erdős-Szekeres (1935)

Every graph G with $\binom{r+s-2}{r-1}$ vertices contains either a clique of size r or an independent set of size s, i.e., $R(r,s) \le \binom{r+s-2}{r-1}$.

Erdős-Szekeres (1935)

Every graph G with $\binom{r+s-2}{r-1}$ vertices contains either a clique of size r or an independent set of size s, i.e., $R(r,s) \leq \binom{r+s-2}{r-1}$.

Upper bounds for Ramsey numbers

Erdős-Szekeres (1935)

Every graph G with $\binom{r+s-2}{r-1}$ vertices contains either a clique of size r or an independent set of size s, i.e., $R(r,s) \leq \binom{r+s-2}{r-1}$.

Erdős-Szekeres (1935)

Every graph G with $\binom{r+s-2}{r-1}$ vertices contains either a clique of size r or an independent set of size s, i.e., $R(r,s) \leq \binom{r+s-2}{r-1}$.

Upper bounds for Ramsey numbers

Erdős-Szekeres (1935)

Every graph G with $\binom{r+s-2}{r-1}$ vertices contains either a clique of size r or an independent set of size s, i.e., $R(r,s) \leq \binom{r+s-2}{r-1}$.

Upper bounds for Ramsey numbers

Erdős-Szekeres (1935)

Every graph G with $\binom{r+s-2}{r-1}$ vertices contains either a clique of size r or an independent set of size s, i.e., $R(r,s) \leq \binom{r+s-2}{r-1}$.

Erdős-Szekeres (1935)

Every graph G with $\binom{r+s-2}{r-1}$ vertices contains either a clique of size r or an independent set of size s, i.e., $R(r,s) \le \binom{r+s-2}{r-1}$.

Upper bounds for Ramsey numbers

Erdős-Szekeres (1935)

Every graph G with $\binom{r+s-2}{r-1}$ vertices contains either a clique of size r or an independent set of size s, i.e., $R(r,s) \leq \binom{r+s-2}{r-1}$.

Bounds for Ramsey numbers

Erdős-Szekeres (1935)

Every graph G with $\binom{r+s-2}{r-1}$ vertices contains either a clique of size r or an independent set of size s, i.e., $R(r,s) \le \binom{r+s-2}{r-1}$.

- The diagonal bound is $R(r,r) \le \binom{2r-2}{r-1} \approx 2^{2r}$.
- To lower-bound $R(r,r)$, one must construct a large graph with all cliques and independent sets smaller than r.
- For years, the best construction was only polynomial in r.

Erdős-Szekeres (1935)

Every graph G with $\binom{r+s-2}{r-1}$ vertices contains either a clique of size r or an independent set of size s, i.e., $R(r,s) \leq \binom{r+s-2}{r-1}$.

- The diagonal bound is $R(r,r) \leq \binom{2r-2}{r-1} \approx 2^{2r}$.
- To lower-bound $R(r,r)$, one must construct a large graph with all cliques and independent sets smaller than r.
- For years, the best construction was only polynomial in r.

Erdős (1947)

There exists a graph with $2^{r/2}$ vertices, but with all cliques and independent sets smaller than r.

Bounds for Ramsey numbers

Erdős (1947)

There exists a graph with $2^{r/2}$ vertices, but with all cliques and independent sets smaller than r.

Erdős (1947)

There exists a graph with $2^{r/2}$ vertices, but with all cliques and independent sets smaller than r.

Erdős (1947)

There exists a graph with $2^{r/2}$ vertices, but with all cliques and independent sets smaller than r.

Bounds for Ramsey numbers

Erdős (1947)

There exists a graph with $2^{r/2}$ vertices, but with all cliques and independent sets smaller than r.

ERDŐS (1947)

There exists a graph with $2^{r/2}$ vertices, but with all cliques and independent sets smaller than r.

Bounds for Ramsey numbers

Erdős (1947)

There exists a graph with $2^{r/2}$ vertices, but with all cliques and independent sets smaller than r.

Bounds for Ramsey numbers

Erdős (1947)

There exists a graph with $2^{r/2}$ vertices, but with all cliques and independent sets smaller than r.

Erdős (1947)

There exists a graph with $2^{r/2}$ vertices, but with all cliques and independent sets smaller than r.

ERDŐS (1947)

There exists a graph with $2^{r/2}$ vertices, but with all cliques and independent sets smaller than r.

Erdős (1947)

There exists a graph with $2^{r/2}$ vertices, but with all cliques and independent sets smaller than r.

ERDŐS (1947)

There exists a graph with $2^{r/2}$ vertices, but with all cliques and independent sets smaller than r.

Erdős (1947)

There exists a graph with $2^{r/2}$ vertices, but with all cliques and independent sets smaller than r.

Erdős (1947)

There exists a graph with $2^{r/2}$ vertices, but with all cliques and independent sets smaller than r.

Erdős (1947)

There exists a graph with $2^{r/2}$ vertices, but with all cliques and independent sets smaller than r.

Bounds for Ramsey numbers

Erdős (1947)

There exists a graph with $2^{r/2}$ vertices, but with all cliques and independent sets smaller than r.

Erdős (1947)

There exists a graph with $2^{r/2}$ vertices, but with all cliques and independent sets smaller than r.

Proof.

- Let $n = 2^{r/2}$, and let $V = \{v_1, \ldots, v_n\}$ be vertices.
- For each pair of vertices, place an edge with probability $\frac{1}{2}$.
- For every set S of r vertices, let B_S be the event that either all or none of the edges within S appear.

Erdős (1947)

There exists a graph with $2^{r/2}$ vertices, but with all cliques and independent sets smaller than r.

Proof.

- Let $n = 2^{r/2}$, and let $V = \{v_1, \ldots, v_n\}$ be vertices.
- For each pair of vertices, place an edge with probability $\frac{1}{2}$.
- For every set S of r vertices, let B_S be the event that either all or none of the edges within S appear.
- For each of the $\binom{n}{r}$ sets S, $\mathbb{P}[B_S] = 2 \cdot 2^{-\binom{r}{2}}$. So $\mathbb{P}[\text{some } B_S \text{ occurs}]$ is at most

$$\begin{aligned} \binom{n}{r} \cdot 2 \cdot 2^{-\binom{r}{2}} &\leq \frac{n^r}{r!} \cdot 2 \cdot 2^{-\frac{r^2-r}{2}} \\ &= (2^{r/2})^r / r! \cdot 2^{1-\frac{r^2-r}{2}} \\ &= 2^{1+r/2}/r! < 1. \quad \square \end{aligned}$$

ERDŐS (1947)

There exists a graph with $2^{r/2}$ vertices, but with all cliques and independent sets smaller than r.

Proof.

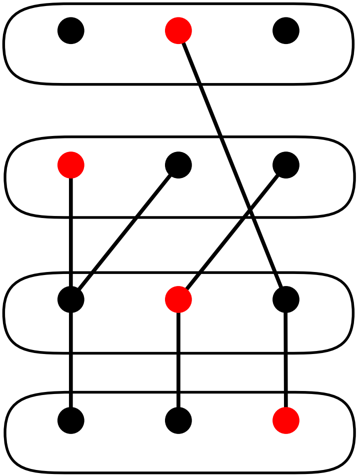
- Let $n = 2^{r/2}$, and let $V = \{v_1, \ldots, v_n\}$ be vertices.
- For each pair of vertices, place an edge with probability $\frac{1}{2}$.
- For every set S of r vertices, let B_S be the event that either all or none of the edges within S appear.
- For each of the $\binom{n}{r}$ sets S, $\mathbb{P}[B_S] = 2 \cdot 2^{-\binom{r}{2}}$. So $\mathbb{P}[\text{some } B_S \text{ occurs}]$ is at most

$$\binom{n}{r} \cdot 2 \cdot 2^{-\binom{r}{2}} \leq \frac{n^r}{r!} \cdot 2 \cdot 2^{-\frac{r^2-r}{2}}$$
$$= (2^{r/2})^r / r! \cdot 2^{1-\frac{r^2-r}{2}}$$
$$= 2^{1+r/2}/r! \rightarrow \mathbf{0.}$$

Independent transversals

Definition

An *independent transversal* has one vertex per group, with no edges between the vertices.

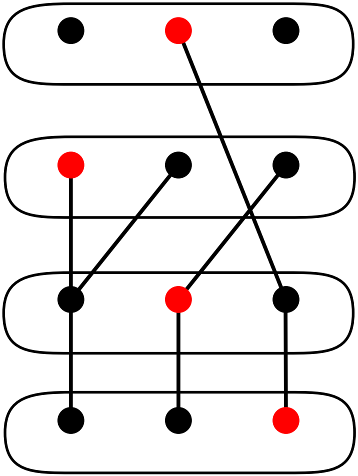


Independent transversals

Definition

An *independent transversal* has one vertex per group, with no edges between the vertices.

Let Δ be the *maximum degree* of the graph (max. number of edges incident to any vertex).



$\Delta = 3$

Independent transversals

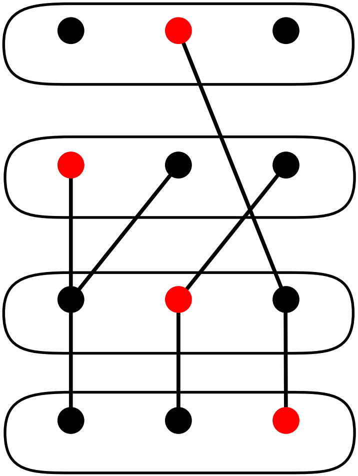
Definition

An *independent transversal* has one vertex per group, with no edges between the vertices.

Let Δ be the *maximum degree* of the graph (max. number of edges incident to any vertex).

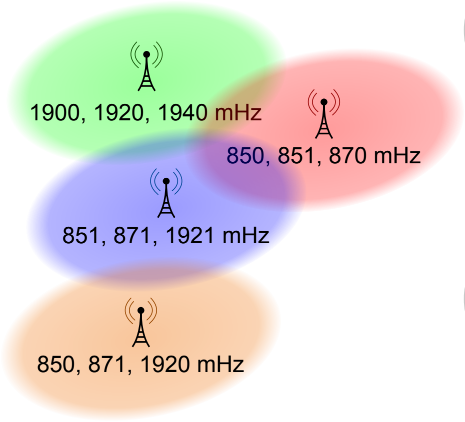
Alon (1988)

If every group has size $\geq 2e\Delta$, then indep. trans. always exists, *no matter how many groups there are.*

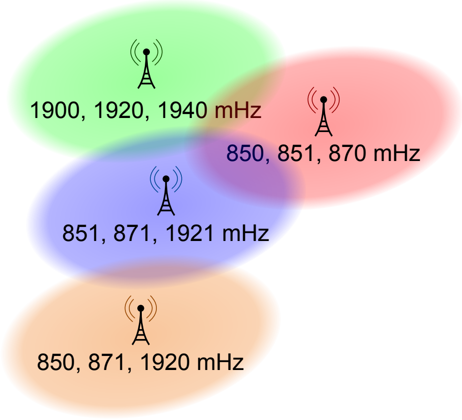


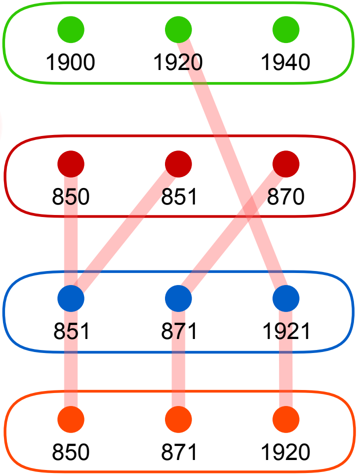
$\Delta = 3$

Independent transversals

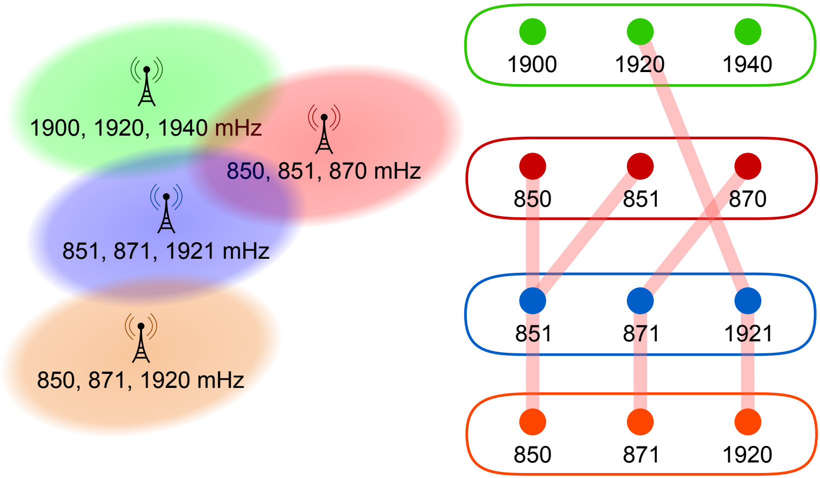


Independent transversals





Independent transversals



Remark. In this example, Δ is bounded by local geometry, but the number of towers (vertex groups) can be arbitrarily large.

Results

Alon (1988)

If every group has size $\geq 2e\Delta$, then an independent transversal always exists, *no matter how many groups there are*.

Progress:

- Sizes $\geq 2\Delta$ suffice (Haxell, 2001)

Results

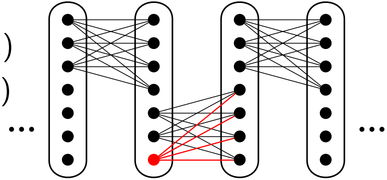
Alon (1988)

If every group has size $\geq 2e\Delta$, then an independent transversal always exists, *no matter how many groups there are*.

Progress:

- Sizes $\geq 2\Delta$ suffice (Haxell, 2001)
- 2Δ is tight (Szabó-Tardos, 2006)

  Construction with sizes exactly $2\Delta - 1$, *but no indep. trans.*



Results

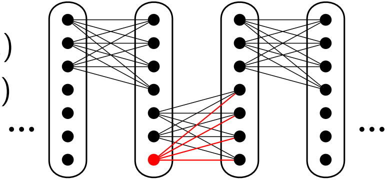
Alon (1988)

If every group has size $\geq 2e\Delta$, then an independent transversal always exists, *no matter how many groups there are.*

Progress:

- Sizes $\geq 2\Delta$ suffice (Haxell, 2001)
- 2Δ is tight (Szabó-Tardos, 2006)

  Construction with sizes exactly $2\Delta - 1$, *but no indep. trans.*



- But if degrees are not concentrated,* then sizes $\geq (1 + o(1))\Delta$ suffice. (L.-Sudakov, 2007)

  * *i.e., if each vertex sends only $o(\Delta)$ edges into each other part*

Question

Let $B_1, \dots, B_n$ be "bad" events in a probability space. How can one show that with positive probability, none of the B_i occur?

Observations:

- For the Ramsey lower bound, the union bound $\mathbb{P}[\text{some } B_i] \leq \sum \mathbb{P}[B_i]$ was already below 1.

Question

Let $B_1, \ldots, B_n$ be "bad" events in a probability space. How can one show that with positive probability, none of the B_i occur?

Observations:

- For the Ramsey lower bound, the union bound $\mathbb{P}[\text{some } B_i] \leq \sum \mathbb{P}[B_i]$ was already below 1.
- Consider flipping 2000 fair coins, and let B_i be the event that the i-th coin is heads.
- The union bound only gives $\mathbb{P}[\text{some } B_i] \leq \sum \mathbb{P}[B_i] = 1000$.

Question

Let $B_1, \ldots, B_n$ be "bad" events in a probability space. How can one show that with positive probability, none of the B_i occur?

Observations:

- For the Ramsey lower bound, the union bound $\mathbb{P}[\text{some } B_i] \leq \sum \mathbb{P}[B_i]$ was already below 1.

- Consider flipping 2000 fair coins, and let B_i be the event that the i-th coin is heads.
- The union bound only gives $\mathbb{P}[\text{some } B_i] \leq \sum \mathbb{P}[B_i] = 1000$.
- Yet no matter how many *independent* coins we flip, it is possible (although unlikely) that all are tails.

Erdős-Lovász (1975)

Let $B_1, \ldots, B_n$ be "bad" events, such that for some p, d:

- Every $\mathbb{P}[B_i] \leq p$.
- Each B_i is independent of all but $\leq d$ of the other B_j.
- $ep(d+1) \leq 1$, where $e \approx 2.718$.

Then with positive probability, none of the B_i occur.

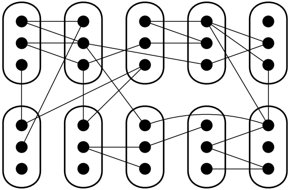
ERDŐS-LOVÁSZ (1975)

Let $B_1, \ldots, B_n$ be "bad" events, such that for some p, d:

- Every $\mathbb{P}[B_i] \leq p$.
- Each B_i is independent of all but $\leq d$ of the other B_j.
- $ep(d+1) \leq 1$, where $e \approx 2.718$.

Then with positive probability, none of the B_i occur.

Proof that sizes $= 2e\Delta$ guarantee an indep. transversal.



ERDŐS-LOVÁSZ (1975)

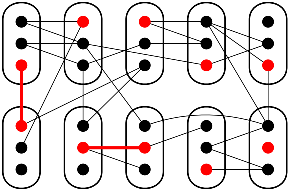
Let $B_1, \ldots, B_n$ be "bad" events, such that for some p, d:

- Every $\mathbb{P}[B_i] \leq p$.
- Each B_i is independent of all but $\leq d$ of the other B_j.
- $ep(d+1) \leq 1$, where $e \approx 2.718$.

Then with positive probability, none of the B_i occur.

Proof that sizes $= 2e\Delta$ guarantee an indep. transversal.

- Randomly pick one vertex per group.



ERDŐS-LOVÁSZ (1975)

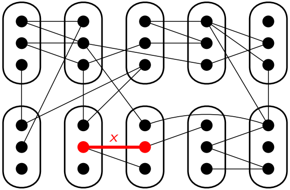
Let $B_1, \ldots, B_n$ be "bad" events, such that for some p, d:

- Every $\mathbb{P}[B_i] \leq p$.
- Each B_i is independent of all but $\leq d$ of the other B_j.
- $ep(d+1) \leq 1$, where $e \approx 2.718$.

Then with positive probability, none of the B_i occur.

Proof that sizes $= 2e\Delta$ guarantee an indep. transversal.

- Randomly pick one vertex per group.
- For each edge x, let B_x be the event that both endpoints of x were picked.
- Let $p = \mathbb{P}[B_x] = \frac{1}{(2e\Delta)^2}$.



The Local Lemma

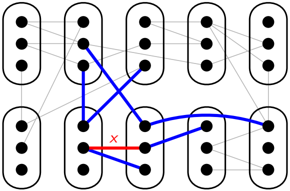
Erdős-Lovász (1975)

Let $B_1, \ldots, B_n$ be "bad" events, such that for some p, d:

- Every $\mathbb{P}[B_i] \leq p$.
- Each B_i is independent of all but $\leq d$ of the other B_j.
- $ep(d+1) \leq 1$, where $e \approx 2.718$.

Then with positive probability, none of the B_i occur.

Proof that sizes $= 2e\Delta$ guarantee an indep. transversal.



- Randomly pick one vertex per group.
- For each edge x, let B_x be the event that both endpoints of x were picked.
- Let $p = \mathbb{P}[B_x] = \frac{1}{(2e\Delta)^2}$.
- Let $d = 2 \cdot (2e\Delta) \cdot \Delta - 2$.
- Then $ep(d+1) < 1$, so there is an outcome when none of the B_x occur, i.e., an independent transversal exists. $\square$

Sperner's Theorem

Sperner (1928)

Let $\mathcal{F}$ be a family of subsets of $\{1, \ldots, n\}$ that is an *antichain*, i.e., no $A, B \in F$ satisfy $A \subset B$. Then $|\mathcal{F}| \leq \binom{n}{\lfloor n/2 \rfloor}$.

Sperner's Theorem

Sperner (1928)

Let $\mathcal{F}$ be a family of subsets of $\{1, \ldots, n\}$ that is an *antichain*, i.e., no $A, B \in F$ satisfy $A \subset B$. Then $|\mathcal{F}| \leq \binom{n}{\lfloor n/2 \rfloor}$.

Proof that $\displaystyle \sum_{\mathbf{A} \in \mathcal{F}} \frac{\mathbf{1}}{\binom{\mathbf{n}}{|\mathbf{A}|}} \leq \mathbf{1}.$

Sperner (1928)

Let $\mathcal{F}$ be a family of subsets of $\{1, \ldots, n\}$ that is an *antichain*, i.e., no $A, B \in F$ satisfy $A \subset B$. Then $|\mathcal{F}| \leq \binom{n}{\lfloor n/2 \rfloor}$.

Proof that $\displaystyle \sum_{A \in \mathcal{F}} \frac{1}{\binom{n}{|A|}} \leq 1.$

- Let $(x_1, x_2, \ldots, x_n)$ be a random permutation of $\{1, \ldots n\}$.
- For each $A \in \mathcal{F}$, let E_A be the event that $\{x_1, \ldots, x_{|A|}\} = A$.

Sperner (1928)

Let $\mathcal{F}$ be a family of subsets of $\{1,\dots,n\}$ that is an *antichain*, i.e., no $A, B \in F$ satisfy $A \subset B$. Then $|\mathcal{F}| \le \binom{n}{\lfloor n/2 \rfloor}$.

Proof that $\displaystyle\sum_{A\in\mathcal{F}} \frac{1}{\binom{n}{|A|}} \le 1$**.**

- Let $(x_1, x_2, \dots, x_n)$ be a random permutation of $\{1, \dots n\}$.
- For each $A \in \mathcal{F}$, let E_A be the event that $\{x_1, \dots, x_{|A|}\} = A$.
- The E_A are mutually exclusive since $\mathcal{F}$ is an antichain, so:

$$\sum_{A\in\mathcal{F}} \mathbb{P}[E_A] \;=\; \mathbb{P}[\text{some } E_A \text{ occurs}] \;\le\; 1.$$

SPERNER (1928)

Let $\mathcal{F}$ be a family of subsets of $\{1, \ldots, n\}$ that is an *antichain*, i.e., no $A, B \in F$ satisfy $A \subset B$. Then $|\mathcal{F}| \leq \binom{n}{\lfloor n/2 \rfloor}$.

Proof that $\displaystyle\sum_{A \in \mathcal{F}} \frac{1}{\binom{n}{|A|}} \leq 1$.

- Let $(x_1, x_2, \ldots, x_n)$ be a random permutation of $\{1, \ldots n\}$.
- For each $A \in \mathcal{F}$, let E_A be the event that $\{x_1, \ldots, x_{|A|}\} = A$.
- The E_A are mutually exclusive since $\mathcal{F}$ is an antichain, so:

$$\sum_{A \in \mathcal{F}} \frac{1}{\binom{n}{|A|}} = \sum_{A \in \mathcal{F}} \mathbb{P}[E_A] = \mathbb{P}[\text{some } E_A \text{ occurs}] \leq 1.$$

$\square$

Erdős (1945)

Let $x_1, \ldots, x_n$ be real numbers greater than 1. Let S be a collection of sums of distinct x_i, such that any $s, s' \in S$ satisfy $|s - s'| \leq 1$. Then $|S| \leq \binom{n}{\lfloor n/2 \rfloor}$.

Erdős (1945)

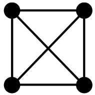
Let $x_1, \ldots, x_n$ be real numbers greater than 1. Let S be a collection of sums of distinct x_i, such that any $s, s' \in S$ satisfy $|s - s'| \leq 1$. Then $|S| \leq \binom{n}{\lfloor n/2 \rfloor}$.

Proof.

- For each element $s \in S$, we may define a set $A_s \subset \{1, \ldots, n\}$ such that $s = \sum_{i \in A_s} x_i$.
- Let $\mathcal{F}$ be the collection of all such A_s.
- Every $A_s \not\subset A_{s'}$ because all $x_i > 1$.
- Sperner's Theorem implies that $|\mathcal{F}| \leq \binom{n}{\lfloor n/2 \rfloor}$. □

Definition

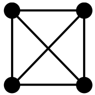
A graph is *planar* if it can be drawn with no crossing edges.



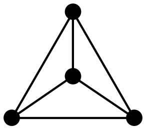
K_4

Definition

A graph is *planar* if it can be drawn with no crossing edges.



K_4

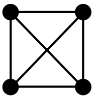


K_4, planar drawing

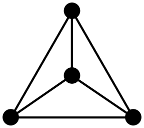
Planarity

Definition

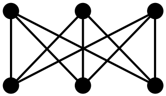
A graph is *planar* if it can be drawn with no crossing edges.



K_4



K_4, planar drawing

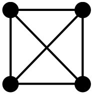


$K_{3,3}$ is never planar

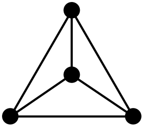
PLANARITY

DEFINITION

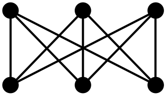
A graph is *planar* if it can be drawn with no crossing edges.



K_4



K_4, planar drawing



$K_{3,3}$ is never planar

Famous theorems:

- The vertices of any planar graph can be colored with only 4 colors, s.t. no pair of adjacent vertices gets the same color.
- Kuratowski: A graph is planar iff it does not contain a topological copy of $K_{3,3}$ or K_5.
- Euler formula: $Vertices - Edges + Faces = 2$.

Crossing number

Definition

The *crossing number* $\mathrm{cr}(G)$ of a graph G is the minimum number of pairs of edges that cross in a drawing.

Crossing number

Definition

The *crossing number* $\mathrm{cr}(G)$ of a graph G is the minimum number of pairs of edges that cross in a drawing.

Ajtai-Chvátal-Newborn-Szemerédi and Leighton (1982)

Any graph with V vertices and $E \geq 4V$ edges has $\mathrm{cr} \geq \frac{E^3}{64V^2}$.

Definition

The *crossing number* $\mathrm{cr}(G)$ of a graph G is the minimum number of pairs of edges that cross in a drawing.

Ajtai-Chvátal-Newborn-Szemerédi and Leighton (1982)

Any graph with V vertices and $E \geq 4V$ edges has $\mathrm{cr} \geq \frac{E^3}{64V^2}$.

First show: $E \leq 3V - 6$ for planar graphs.

- $2E =$ sum of perimeters of faces $\geq 3F$.

Definition

The *crossing number* $\mathrm{cr}(G)$ of a graph G is the minimum number of pairs of edges that cross in a drawing.

Ajtai-Chvátal-Newborn-Szemerédi and Leighton (1982)

Any graph with V vertices and $E \geq 4V$ edges has $\mathrm{cr} \geq \frac{E^3}{64V^2}$.

First show: $E \leq 3V - 6$ for planar graphs.

- $2E$ = sum of perimeters of faces $\geq 3F$.
- Substitute $F \leq \frac{2}{3}E$ into Euler formula $V - E + F = 2$:

$$2 \;=\; V - E + F \;\leq\; V - \frac{1}{3}E. \qquad \square$$

Crossing number

Definition

The *crossing number* $\mathrm{cr}(G)$ of a graph G is the minimum number of pairs of edges that cross in a drawing.

Ajtai-Chvátal-Newborn-Szemerédi and Leighton (1982)

Any graph with V vertices and $E \geq 4V$ edges has $\mathrm{cr} \geq \frac{E^3}{64V^2}$.

First show: $E \leq 3V - 6$ for planar graphs.

- $2E =$ sum of perimeters of faces $\geq 3F$.
- Substitute $F \leq \frac{2}{3}E$ into Euler formula $V - E + F = 2$:

$$2 \quad = \quad V - E + F \quad \leq \quad V - \frac{1}{3}E. \qquad \square$$

Corollary: $E - \mathrm{cr} \leq 3V - 6$

Crossing number

Definition

The *crossing number* $\mathrm{cr}(G)$ of a graph G is the minimum number of pairs of edges that cross in a drawing.

Ajtai-Chvátal-Newborn-Szemerédi and Leighton (1982)

Any graph with V vertices and $E \geq 4V$ edges has $\mathrm{cr} \geq \frac{E^3}{64V^2}$.

First show: $E \leq 3V - 6$ for planar graphs.

- $2E =$ sum of perimeters of faces $\geq 3F$.
- Substitute $F \leq \frac{2}{3}E$ into Euler formula $V - E + F = 2$:

$$2 = V - E + F \leq V - \frac{1}{3}E. \qquad \square$$

Corollary: $E - \mathrm{cr} \leq 3V - 6 \implies \mathrm{cr} \geq E - 3V$.

$$\text{cr} \geq E \quad - 3V$$

$$\mathrm{cr} \geq E - 3V$$

Crossing number

$$\text{cr} \geq E \; - 3V$$

Crossing number

$$\mathrm{cr} \geq E \; - 3V$$

Crossing number

$$\text{cr} \geq E \;\; - 3V$$

Crossing number

$$\text{cr} \geq E \ - 3V$$

Crossing number

$$\mathrm{cr} \geq E \quad - 3V$$

Crossing number

$$\text{cr} \geq E - 3V$$

Crossing number

$$\text{cr} \geq E \; - 3V$$

$$\mathrm{cr} \geq E \;\; - 3V$$

Crossing number

$$\text{cr} \geq E - 3V$$

Crossing number

$$\text{cr} \geq E \;\; - 3V$$

Crossing number

$$\text{cr} \geq E \; - 3V$$

Crossing number

$$\text{cr} \geq E - 3V$$

Crossing number

$\text{cr} \geq E \; - 3V$

Crossing number

$$\mathrm{cr} \geq E - 3V$$

Crossing number

$$\text{cr} \geq E \; - 3V$$

$$\text{cr} \geq E - 3V$$

Crossing number

$\text{cr} \geq E - 3V$

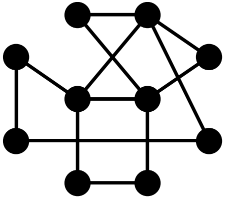
Proof that $\mathbf{cr(G) \geq \frac{E^3}{64V^2}}$ whenever $\mathbf{E \geq 4V}$.

$\text{cr} \geq E \;\; - 3V$

Proof that $\mathbf{cr(G) \geq \frac{E^3}{64V^2}}$ whenever $\mathbf{E \geq 4V}$.

- Fix a drawing of G, and let $X = \#$crossings.
- Randomly keep each vertex with probability $p = \frac{4V}{E}$.

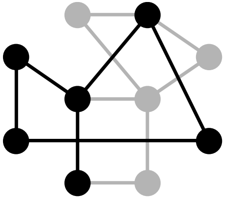
$\text{cr} \geq E \; - 3V$



Proof that $\mathbf{cr(G) \geq \frac{E^3}{64V^2}}$ whenever $\mathbf{E \geq 4V}$.

- Fix a drawing of G, and let $X = \#$crossings.
- Randomly keep each vertex with probability $p = \frac{4V}{E}$.

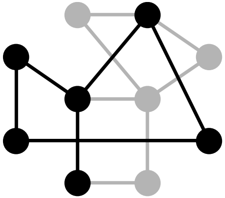
$\text{cr} \geq E \; - 3V$



Proof that $\mathbf{cr(G) \geq \frac{E^3}{64V^2}}$ whenever $\mathbf{E \geq 4V}$.

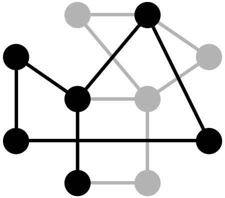
- Fix a drawing of G, and let $X = \#$crossings.
- Randomly keep each vertex with probability $p = \frac{4V}{E}$.
- Let V', E', X' be numbers of vertices, edges, crossings left.

$\text{cr} \geq E \ - 3V$



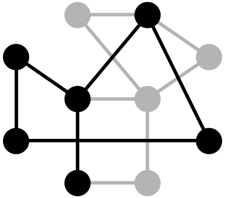
Proof that $\mathbf{cr(G) \geq \frac{E^3}{64V^2}}$ whenever $\mathbf{E \geq 4V}$.

- Fix a drawing of G, and let $X = \#\text{crossings}$.
- Randomly keep each vertex with probability $p = \frac{4V}{E}$.
- Let V', E', X' be numbers of vertices, edges, crossings left.
- $X' \geq E' - 3V'$



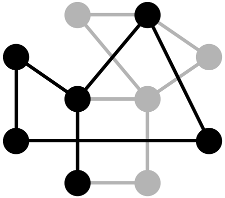
Proof that $\mathrm{cr}(G) \geq \frac{E^3}{64V^2}$ whenever $E \geq 4V$.

- Fix a drawing of G, and let $X = \#\text{crossings}$.
- Randomly keep each vertex with probability $p = \frac{4V}{E}$.
- Let V', E', X' be numbers of vertices, edges, crossings left.
- $X' \geq E' - 3V'$, so $\mathbb{E}[X'] \geq \mathbb{E}[E'] - 3\mathbb{E}[V']$.



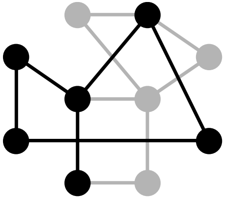
Proof that $\mathbf{cr(G) \geq \frac{E^3}{64V^2}}$ whenever $\mathbf{E \geq 4V}$.

- Fix a drawing of G, and let $X = \#$crossings.
- Randomly keep each vertex with probability $p = \frac{4V}{E}$.
- Let V', E', X' be numbers of vertices, edges, crossings left.
- $X' \geq E' - 3V'$, so $\mathbb{E}[X'] \geq \mathbb{E}[E'] - 3\mathbb{E}[V']$.
- $\mathbb{E}[X'] = Xp^4$, $\mathbb{E}[E'] = Ep^2$, and $\mathbb{E}[V'] = Vp$.



Proof that $\mathbf{cr(G) \geq \frac{E^3}{64V^2}}$ whenever $\mathbf{E \geq 4V}$.

- Fix a drawing of G, and let $X = \#$crossings.
- Randomly keep each vertex with probability $p = \frac{4V}{E}$.
- Let V', E', X' be numbers of vertices, edges, crossings left.
- $X' \geq E' - 3V'$, so $\mathbb{E}[X'] \geq \mathbb{E}[E'] - 3\mathbb{E}[V']$.
- $\mathbb{E}[X'] = Xp^4$, $\mathbb{E}[E'] = Ep^2$, and $\mathbb{E}[V'] = Vp$, so:



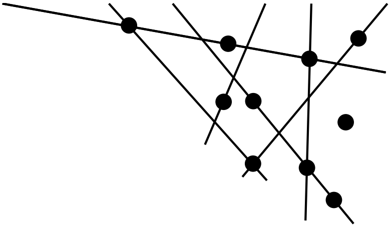
$$\begin{aligned} Xp^4 &\geq Ep^2 - 3Vp \\ X &\geq p^{-2} \cdot (E - 3Vp^{-1}) \\ &= \left(\frac{E}{4V}\right)^2 \cdot \frac{E}{4}. \end{aligned}$$

□

Point-line incidences

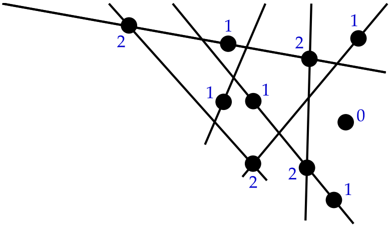
Szemerédi-Trotter (1983)

Let P be a set of n points, and L be a set of m lines. Then only $I \leq 4(m^{2/3}n^{2/3} + m + n)$ pairs $(p, \ell) \in P \times L$ have p lying on ℓ.



Szemerédi-Trotter (1983)

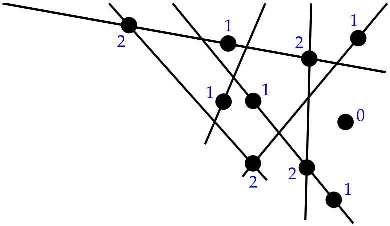
Let P be a set of n points, and L be a set of m lines. Then only $I \leq 4(m^{2/3}n^{2/3} + m + n)$ pairs $(p, \ell) \in P \times L$ have p lying on ℓ.



Szemerédi-Trotter (1983)

Let P be a set of n points, and L be a set of m lines. Then only $I \leq 4(m^{2/3}n^{2/3} + m + n)$ pairs $(p, \ell) \in P \times L$ have p lying on ℓ.

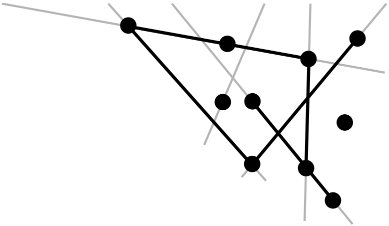
Proof. Let G be defined by the drawing of P and L.



Szemerédi-Trotter (1983)

Let P be a set of n points, and L be a set of m lines. Then only $I \leq 4(m^{2/3}n^{2/3} + m + n)$ pairs $(p, \ell) \in P \times L$ have p lying on ℓ.

Proof. Let G be defined by the drawing of P and L.

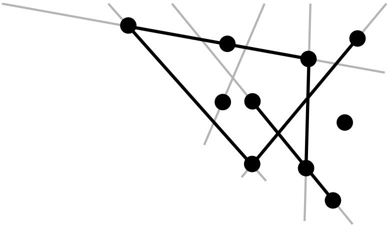


SZEMERÉDI-TROTTER (1983)

Let P be a set of n points, and L be a set of m lines. Then only $I \leq 4(m^{2/3}n^{2/3} + m + n)$ pairs $(p, \ell) \in P \times L$ have p lying on ℓ.

Proof. Let G be defined by the drawing of P and L. Then:

- $V = n$
- $\mathrm{cr}(G) \leq \binom{m}{2} \leq \frac{m^2}{2}$

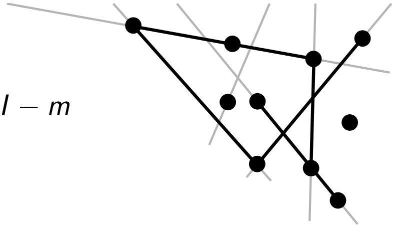


SZEMERÉDI-TROTTER (1983)

Let P be a set of n points, and L be a set of m lines. Then only $I \leq 4(m^{2/3}n^{2/3} + m + n)$ pairs $(p, \ell) \in P \times L$ have p lying on ℓ.

Proof. Let G be defined by the drawing of P and L. Then:

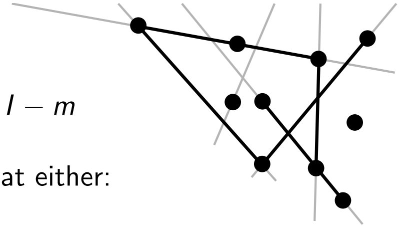
- $V = n$
- $\mathrm{cr}(G) \leq \binom{m}{2} \leq \frac{m^2}{2}$
- $E \geq \sum_{\ell \in L} (\#\{p \in \ell\} - 1) = I - m$



Szemerédi-Trotter (1983)

Let P be a set of n points, and L be a set of m lines. Then only $I \leq 4(m^{2/3}n^{2/3} + m + n)$ pairs $(p, \ell) \in P \times L$ have p lying on ℓ.

Proof. Let G be defined by the drawing of P and L. Then:



- $V = n$
- $\mathrm{cr}(G) \leq \binom{m}{2} \leq \frac{m^2}{2}$
- $E \geq \sum_{\ell \in L} (\#\{p \in \ell\} - 1) = I - m$

The Crossing Lemma showed that either:

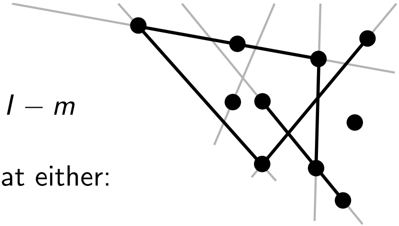
- $E < 4V$, or
- $\mathrm{cr}(G) \geq \frac{E^3}{64V^2}$.

Szemerédi-Trotter (1983)

Let P be a set of n points, and L be a set of m lines. Then only $I \leq 4(m^{2/3}n^{2/3} + m + n)$ pairs $(p, \ell) \in P \times L$ have p lying on ℓ.

Proof. Let G be defined by the drawing of P and L. Then:

- $V = n$
- $\mathrm{cr}(G) \leq \binom{m}{2} \leq \frac{m^2}{2}$
- $E \geq \sum_{\ell \in L} (\#\{p \in \ell\} - 1) = I - m$



The Crossing Lemma showed that either:

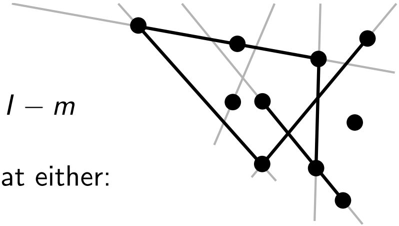
- $E < 4V \quad \Rightarrow \quad I - m < 4n$
- $\mathrm{cr}(G) \geq \frac{E^3}{64V^2}$.

SZEMERÉDI-TROTTER (1983)

Let P be a set of n points, and L be a set of m lines. Then only $I \leq 4(m^{2/3}n^{2/3} + m + n)$ pairs $(p, \ell) \in P \times L$ have p lying on ℓ.

Proof. Let G be defined by the drawing of P and L. Then:

- $V = n$
- $\text{cr}(G) \leq \binom{m}{2} \leq \frac{m^2}{2}$
- $E \geq \sum_{\ell \in L} (\#\{p \in \ell\} - 1) = I - m$



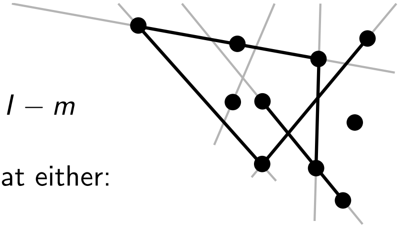
The Crossing Lemma showed that either:

- $E < 4V \quad \Rightarrow \quad I - m < 4n$
- $\text{cr}(G) \geq \frac{E^3}{64V^2} \quad \Rightarrow \quad \frac{m^2}{2} \geq \frac{(I-m)^3}{64n^2}$

SZEMERÉDI-TROTTER (1983)

Let P be a set of n points, and L be a set of m lines. Then only $I \leq 4(m^{2/3}n^{2/3} + m + n)$ pairs $(p, \ell) \in P \times L$ have p lying on ℓ.

Proof. Let G be defined by the drawing of P and L. Then:



- $V = n$
- $\mathrm{cr}(G) \leq \binom{m}{2} \leq \frac{m^2}{2}$
- $E \geq \sum_{\ell \in L} (\#\{p \in \ell\} - 1) = I - m$

The Crossing Lemma showed that either:

- $E < 4V \quad \Rightarrow \quad I - m < 4n$
- $\mathrm{cr}(G) \geq \frac{E^3}{64V^2} \quad \Rightarrow \quad \frac{m^2}{2} \geq \frac{(I-m)^3}{64n^2} \quad \Rightarrow \quad (I - m)^3 \leq 32m^2n^2.$

Both cases give $I - m \leq 4(m^{2/3}n^{2/3} + n)$. □

Definition

For $A \subset \mathbb{R}$, let $A + A = \{a + b : a, b \in A\}$, $A \cdot A = \{ab : a, b \in A\}$.

Question

Must one of $A + A$ or $A \cdot A$ always be substantially larger than A?

Definition

For $A \subset \mathbb{R}$, let $A + A = \{a + b : a, b \in A\}$, $A \cdot A = \{ab : a, b \in A\}$.

Question

Must one of $A + A$ or $A \cdot A$ always be substantially larger than A?

- If $A = \{2^1, 2^2, \ldots, 2^n\}$, then $A \cdot A = \{2^2, 2^3, \ldots, 2^{2n}\}$ has size $\approx 2|A|$, but $|A + A| = \binom{n}{2} \approx \frac{1}{2}|A|^2$.

Definition

For $A \subset \mathbb{R}$, let $A + A = \{a + b : a, b \in A\}$, $A \cdot A = \{ab : a, b \in A\}$.

Question

Must one of $A + A$ or $A \cdot A$ always be substantially larger than A?

- If $A = \{2^1, 2^2, \ldots, 2^n\}$, then $A \cdot A = \{2^2, 2^3, \ldots, 2^{2n}\}$ has size $\approx 2|A|$, but $|A + A| = \binom{n}{2} \approx \frac{1}{2}|A|^2$.
- If $A = \{1, 2, \ldots, n\}$, then $A + A = \{2, 3, \ldots, 2n\}$ has size $\approx 2|A|$, but $|A \cdot A| \gtrsim \frac{|A|^2}{\log |A|}$.

Combinatorial number theory

Definition

For $A \subset \mathbb{R}$, let $A + A = \{a + b : a, b \in A\}$, $A \cdot A = \{ab : a, b \in A\}$.

Question

Must one of $A + A$ or $A \cdot A$ always be substantially larger than A?

- If $A = \{2^1, 2^2, \ldots, 2^n\}$, then $A \cdot A = \{2^2, 2^3, \ldots, 2^{2n}\}$ has size $\approx 2|A|$, but $|A + A| = \binom{n}{2} \approx \frac{1}{2}|A|^2$.
- If $A = \{1, 2, \ldots, n\}$, then $A + A = \{2, 3, \ldots, 2n\}$ has size $\approx 2|A|$, but $|A \cdot A| \gtrsim \frac{|A|^2}{\log |A|}$.

Erdős-Szemerédi (1983)

There is a constant $c > 0$ such that $|A + A|$ or $|A \cdot A|$ is $\gtrsim |A|^{1+c}$.

Erdős-Szemerédi (1983)

There is a constant $c > 0$ such that $|A + A|$ or $|A \cdot A|$ is $\gtrsim |A|^{1+c}$.

Erdős-Szemerédi (1983)

There is a constant $c > 0$ such that $|A + A|$ or $|A \cdot A|$ is $\gtrsim |A|^{1+c}$.

Erdős-Szemerédi (1983)

There is a constant $c > 0$ such that $|A + A|$ or $|A \cdot A|$ is $\gtrsim |A|^{1+c}$.

Erdős-Szemerédi (1983)

There is a constant $c > 0$ such that $|A + A|$ or $|A \cdot A|$ is $\gtrsim |A|^{1+c}$.

Erdős-Szemerédi (1983)

There is a constant $c > 0$ such that $|A + A|$ or $|A \cdot A|$ is $\gtrsim |A|^{1+c}$.

Erdős-Szemerédi (1983)

There is a constant $c > 0$ such that $|A + A|$ or $|A \cdot A|$ is $\gtrsim |A|^{1+c}$.

Erdős-Szemerédi (1983)

There is a constant $c > 0$ such that $|A + A|$ or $|A \cdot A|$ is $\gtrsim |A|^{1+c}$.

Erdős-Szemerédi (1983)

There is a constant $c > 0$ such that $|A + A|$ or $|A \cdot A|$ is $\gtrsim |A|^{1+c}$.

Erdős-Szemerédi (1983)

There is a constant $c > 0$ such that $|A + A|$ or $|A \cdot A|$ is $\gtrsim |A|^{1+c}$.

Erdős-Szemerédi (1983)

There is a constant $c > 0$ such that $|A + A|$ or $|A \cdot A|$ is $\gtrsim |A|^{1+c}$.

ERDŐS-SZEMERÉDI (1983)

There is a constant $c > 0$ such that $|A + A|$ or $|A \cdot A|$ is $\gtrsim |A|^{1+c}$.

Erdős-Szemerédi (1983)

There is a constant $c > 0$ such that $|A + A|$ or $|A \cdot A|$ is $\gtrsim |A|^{1+c}$.

Erdős-Szemerédi (1983)

There is a constant $c > 0$ such that $|A + A|$ or $|A \cdot A|$ is $\gtrsim |A|^{1+c}$.

Erdős-Szemerédi (1983)

There is a constant $c > 0$ such that $|A + A|$ or $|A \cdot A|$ is $\gtrsim |A|^{1+c}$.

Erdős-Szemerédi (1983)

There is a constant $c > 0$ such that $|A + A|$ or $|A \cdot A|$ is $\gtrsim |A|^{1+c}$.

Sum-product results

Erdős-Szemerédi (1983)

There is a constant $c > 0$ such that $|A + A|$ or $|A \cdot A|$ is $\gtrsim |A|^{1+c}$.

Conjecture (Erdős-Szemerédi)

The theorem should hold for any $c < 1$.

Sum-product results

Erdős-Szemerédi (1983)

There is a constant $c > 0$ such that $|A + A|$ or $|A \cdot A|$ is $\gtrsim |A|^{1+c}$.

Conjecture (Erdős-Szemerédi)

The theorem should hold for any $c < 1$.

Progress:

- $c = \frac{1}{31}$, Nathanson (1997)
- $c = \frac{1}{15}$, Ford (1998)

Sum-product results

Erdős-Szemerédi (1983)

There is a constant $c > 0$ such that $|A + A|$ or $|A \cdot A|$ is $\gtrsim |A|^{1+c}$.

Conjecture (Erdős-Szemerédi)

The theorem should hold for any $c < 1$.

Progress:

- $c = \frac{1}{31}$, Nathanson (1997)
- $c = \frac{1}{15}$, Ford (1998)
- $c = \frac{1}{4}$, Elekes (1997)
- $c = \frac{3}{11}$, Solymosi (2005)
- $c = \frac{1}{3} - \epsilon$, Solymosi (2008)

Proof that $|A + A|$ or $|A \cdot A|$ is always $\gtrsim n^{5/4}$, when $|A| = n$.

Proof that $|\mathbf{A}+\mathbf{A}|$ or $|\mathbf{A}\cdot\mathbf{A}|$ is always $\gtrsim \mathbf{n}^{5/4}$, when $|\mathbf{A}|=\mathbf{n}$.

- Let $\ell_{a,b}$ be the line $y = a(x-b)$, and let $L = \{\ell_{a,b} : a, b \in A\}$.
- Let P be the set of points (x, y) with $x \in A+A$ and $y \in A \cdot A$.

Proof that $|\mathbf{A}+\mathbf{A}|$ or $|\mathbf{A}\cdot\mathbf{A}|$ is always $\gtrsim \mathbf{n}^{5/4}$, when $|\mathbf{A}| = \mathbf{n}$.

- Let $\ell_{a,b}$ be the line $y = a(x-b)$, and let $L = \{\ell_{a,b} : a, b \in A\}$.
- Let P be the set of points (x, y) with $x \in A+A$ and $y \in A \cdot A$.
- Each $\ell_{a,b}$ contains every point $(c+b, ac)$ with $c \in A$.
  Hence $\ell_{a,b}$ intersects $\geq |A| = n$ points of P.

Proof that $|\mathbf{A}+\mathbf{A}|$ or $|\mathbf{A}\cdot\mathbf{A}|$ is always $\gtrsim \mathbf{n}^{5/4}$, when $|\mathbf{A}| = \mathbf{n}$.

- Let $\ell_{a,b}$ be the line $y = a(x-b)$, and let $L = \{\ell_{a,b} : a, b \in A\}$.
- Let P be the set of points (x, y) with $x \in A+A$ and $y \in A \cdot A$.
- Each $\ell_{a,b}$ contains every point $(c+b, ac)$ with $c \in A$. Hence $\ell_{a,b}$ intersects $\geq |A| = n$ points of P.
- There are n^2 lines $\ell_{a,b}$, so there are $I \geq n^3$ total incidences.
- Szemerédi-Trotter implies that $I \leq 4(|L|^{2/3}|P|^{2/3} + |L| + |P|)$.

Proof that $|A+A|$ or $|A \cdot A|$ is always $\gtrsim n^{5/4}$, when $|A| = n$.

- Let $\ell_{a,b}$ be the line $y = a(x-b)$, and let $L = \{\ell_{a,b} : a, b \in A\}$.
- Let P be the set of points (x, y) with $x \in A+A$ and $y \in A \cdot A$.
- Each $\ell_{a,b}$ contains every point $(c+b, ac)$ with $c \in A$.
  Hence $\ell_{a,b}$ intersects $\geq |A| = n$ points of P.
- There are n^2 lines $\ell_{a,b}$, so there are $I \geq n^3$ total incidences.
- Szemerédi-Trotter implies that $I \leq 4(|L|^{2/3}|P|^{2/3} + |L| + |P|)$.
- $|L| = n^2 \leq |P|$

Proof that $|A + A|$ or $|A \cdot A|$ is always $\gtrsim n^{5/4}$, when $|A| = n$.

- Let $\ell_{a,b}$ be the line $y = a(x - b)$, and let $L = \{\ell_{a,b} : a, b \in A\}$.
- Let P be the set of points (x, y) with $x \in A + A$ and $y \in A \cdot A$.
- Each $\ell_{a,b}$ contains every point $(c + b, ac)$ with $c \in A$. Hence $\ell_{a,b}$ intersects $\geq |A| = n$ points of P.
- There are n^2 lines $\ell_{a,b}$, so there are $I \geq n^3$ total incidences.
- Szemerédi-Trotter implies that $I \leq 4(|L|^{2/3}|P|^{2/3} + |L| + |P|)$.
- $|L| = n^2 \leq |P|$, and $|P| \leq |L|^{2/3}|P|^{2/3}$ since $|P| \leq n^4 = |L|^2$.

Proof that $|\mathbf{A}+\mathbf{A}|$ or $|\mathbf{A}\cdot\mathbf{A}|$ is always $\gtrsim \mathbf{n}^{5/4}$, when $|\mathbf{A}| = \mathbf{n}$.

- Let $\ell_{a,b}$ be the line $y = a(x-b)$, and let $L = \{\ell_{a,b} : a, b \in A\}$.
- Let P be the set of points (x, y) with $x \in A+A$ and $y \in A\cdot A$.
- Each $\ell_{a,b}$ contains every point $(c+b, ac)$ with $c \in A$. Hence $\ell_{a,b}$ intersects $\geq |A| = n$ points of P.
- There are n^2 lines $\ell_{a,b}$, so there are $I \geq n^3$ total incidences.
- Szemerédi-Trotter implies that $I \leq 4(|L|^{2/3}|P|^{2/3} + |L| + |P|)$.
- $|L| = n^2 \leq |P|$, and $|P| \leq |L|^{2/3}|P|^{2/3}$ since $|P| \leq n^4 = |L|^2$.

$$I \leq 4\cdot 3\cdot |L|^{2/3}|P|^{2/3}$$

Proof that $|A+A|$ or $|A \cdot A|$ is always $\gtrsim n^{5/4}$, when $|A| = n$.

- Let $\ell_{a,b}$ be the line $y = a(x-b)$, and let $L = \{\ell_{a,b} : a, b \in A\}$.
- Let P be the set of points (x, y) with $x \in A + A$ and $y \in A \cdot A$.
- Each $\ell_{a,b}$ contains every point $(c+b, ac)$ with $c \in A$.
  Hence $\ell_{a,b}$ intersects $\geq |A| = n$ points of P.
- There are n^2 lines $\ell_{a,b}$, so there are $I \geq n^3$ total incidences.
- Szemerédi-Trotter implies that $I \leq 4(|L|^{2/3}|P|^{2/3} + |L| + |P|)$.
- $|L| = n^2 \leq |P|$, and $|P| \leq |L|^{2/3}|P|^{2/3}$ since $|P| \leq n^4 = |L|^2$.

$$n^{9/3} = n^3 \leq I \leq 4 \cdot 3 \cdot |L|^{2/3}|P|^{2/3}$$

Proof that $|A+A|$ or $|A \cdot A|$ is always $\gtrsim n^{5/4}$, when $|A| = n$.

- Let $\ell_{a,b}$ be the line $y = a(x-b)$, and let $L = \{\ell_{a,b} : a, b \in A\}$.
- Let P be the set of points (x, y) with $x \in A+A$ and $y \in A \cdot A$.
- Each $\ell_{a,b}$ contains every point $(c+b, ac)$ with $c \in A$.
  Hence $\ell_{a,b}$ intersects $\geq |A| = n$ points of P.
- There are n^2 lines $\ell_{a,b}$, so there are $I \geq n^3$ total incidences.
- Szemerédi-Trotter implies that $I \leq 4(|L|^{2/3}|P|^{2/3} + |L| + |P|)$.
- $|L| = n^2 \leq |P|$, and $|P| \leq |L|^{2/3}|P|^{2/3}$ since $|P| \leq n^4 = |L|^2$.

$$n^{9/3} \quad = \quad n^3 \quad \leq \quad I \quad \leq \quad 4 \cdot 3 \cdot |L|^{2/3}|P|^{2/3} \quad = \quad 12 \cdot n^{4/3} \cdot |P|^{2/3}$$

Proof that $|A + A|$ or $|A \cdot A|$ is always $\gtrsim n^{5/4}$, when $|A| = n$.

- Let $\ell_{a,b}$ be the line $y = a(x - b)$, and let $L = \{\ell_{a,b} : a, b \in A\}$.
- Let P be the set of points (x, y) with $x \in A + A$ and $y \in A \cdot A$.
- Each $\ell_{a,b}$ contains every point $(c + b, ac)$ with $c \in A$. Hence $\ell_{a,b}$ intersects $\geq |A| = n$ points of P.
- There are n^2 lines $\ell_{a,b}$, so there are $I \geq n^3$ total incidences.
- Szemerédi-Trotter implies that $I \leq 4(|L|^{2/3}|P|^{2/3} + |L| + |P|)$.
- $|L| = n^2 \leq |P|$, and $|P| \leq |L|^{2/3}|P|^{2/3}$ since $|P| \leq n^4 = |L|^2$.

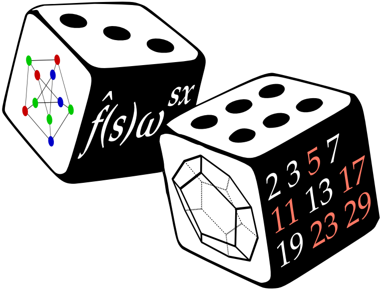
$$
\begin{aligned}
n^{9/3} = n^3 \leq I &\leq 4 \cdot 3 \cdot |L|^{2/3}|P|^{2/3} = 12 \cdot n^{4/3} \cdot |P|^{2/3} \\
\frac{1}{12} n^{5/3} &\leq |P|^{2/3} \\
0.024 n^{5/2} &\leq |P|
\end{aligned}
$$

Proof that $|A + A|$ or $|A \cdot A|$ is always $\gtrsim n^{5/4}$, when $|A| = n$.

- Let $\ell_{a,b}$ be the line $y = a(x - b)$, and let $L = \{\ell_{a,b} : a, b \in A\}$.
- Let P be the set of points (x, y) with $x \in A + A$ and $y \in A \cdot A$.
- Each $\ell_{a,b}$ contains every point $(c + b, ac)$ with $c \in A$. Hence $\ell_{a,b}$ intersects $\geq |A| = n$ points of P.
- There are n^2 lines $\ell_{a,b}$, so there are $I \geq n^3$ total incidences.
- Szemerédi-Trotter implies that $I \leq 4(|L|^{2/3}|P|^{2/3} + |L| + |P|)$.
- $|L| = n^2 \leq |P|$, and $|P| \leq |L|^{2/3}|P|^{2/3}$ since $|P| \leq n^4 = |L|^2$.

$$\begin{aligned} n^{9/3} = n^3 \leq I &\leq 4 \cdot 3 \cdot |L|^{2/3}|P|^{2/3} = 12 \cdot n^{4/3} \cdot |P|^{2/3} \\ \frac{1}{12}n^{5/3} &\leq |P|^{2/3} \\ 0.024n^{5/2} &\leq |P| = |A + A| \cdot |A \cdot A|. \end{aligned}$$

Therefore, $|A + A|$ or $|A \cdot A|$ must be $\gtrsim n^{5/4}$. $\square$



IPAM Fall 2009

Los Angeles, California

Combinatorics:

Methods and Applications in

Mathematics and Computer Science

Workshop 1. Probabilistic techniques and applications

Workshop 2. Combinatorial geometry

Workshop 3. Topics in graphs and hypergraphs

Workshop 4. Analytical methods in combinatorics, additive number theory and computer science

Organizers: *N. Alon, G. Kalai, J. Pach, V. Sós, A. Steger, B. Sudakov, T. Tao.*