ADFOCS 2006 Saarbrücken

ERDŐS MAGIC

Joel Spencer

Courant Institute

Der Zauberer von Budapest

Erdős 1947: If $\binom{n}{k}2^{1-\binom{k}{2}} < 1$ there **exists** a two coloring of the edges of K_n with no monochromatic K_k.

Proof: Color Randomly!

Calculation: $n = \frac{k}{e\sqrt{2}}\sqrt{2}^k(1 + o(1))$

Working with Paul Erdős was like taking a walk in the hills. Every time when I thought that we had achieved our goal and deserved a rest, Paul pointed to the top of another hill and off we would go.

– Fan Chung

Removing the Blemishes

G with n vertices, $\frac{nd}{2}$ edges, $d \geq 1$

Thm: There exists independent S^*

$$|S^*| \geq \frac{n}{2d}$$

Put $v \in S$ with probability p (parameter!)

If edge $\{v, w\}$ with $v, w \in S$ delete v

Left with independent S^*

Expectation:

S has pn vertices, $\frac{nd}{2}p^2$ edges

S^* has $\geq f(p) := pn - \frac{nd}{2}p^2$ vertices

Calculus: Set $p = \frac{1}{d}$

Erdős Magic: Exists S^* with

$$|S^*| \geq E[|S^*|] \geq f(p) = \frac{n}{2d}$$

Theorem (Turán). Any graph G has an independent set S with

$$|S| \geq \sum_{v \in G} \frac{1}{d_v + 1}$$

Randomized Algorithm

- Order Vertices Randomly.
- Place v in S greedily.

If v comes before its neighbors *then* it goes into S.

$$\Pr[v \in S] \geq \frac{1}{d_v + 1}$$

Linearity of Expectation:

$$E[|S|] = \sum_{v \in G} \Pr[v \in S] \geq \sum_{v \in G} \frac{1}{d_v + 1}$$

Erdős Magic: Such S **MUST** exist.

Erdős Magic (CS version!)

- Suppose a randomized algorithm creates a structure with desired properties with positive probability. Then such a structure *must* exist

- Suppose a randomized algorithm creates a structure S whose expected size is α. Then there *must* exist structures S of size $\geq \alpha$. (And also $\leq \alpha$.)

Derandomization?? Sometimes!!

Discrepancy

$n \times n$ $A = [a_{ij}]$, all $|a_{ij}| \le 1$

Theorem: There exist $\epsilon_1, \ldots, \epsilon_n \in \{-1, +1\}$

$$\left| \sum_{j=1}^{n} a_{ij} \epsilon_j \right| \le \sqrt{2n \ln n}, 1 \le i \le n$$

Probability Fact: $b_1, \ldots, b_n \in [-1, +1]$, $\epsilon_1, \ldots, \epsilon_n \in \{-1, +1\}$ uniform i.i.d., $E := \sum_{j=1}^{n} \epsilon_j b_j$:

$$\Pr[|E| > \alpha\sqrt{n}] < 2e^{-\alpha^2/2}$$

Intuition: E Gaussian, $\sigma \le \sqrt{n}$

Proof of Theorem: Take ϵ_i randomly!

$\Pr[\text{FAIL}] < n \cdot n^{-1} = 1$

Derandomization: Yes!

Thm (JS): Can get all $|\cdot| \le 6\sqrt{n}$

But no algorithm known!

$|A_i| = n$, $1 \le i \le m = 2^{n-1}k$

Seek Red/Blue χ with no A_i monochromatic

Erdős [1963]: $k < 1 \Rightarrow \exists\chi$

Beck [1978]: $k < cn^{1/3} \Rightarrow \exists\chi$

Radhakrishnan-Srinivasan[2000]

$$k < c[n/\ln n]^{1/2} \Rightarrow \exists\chi$$

Erdős [1964]: There exists family with $k = cn^2$ with no χ

Coloring Algorithm(s)

1. Color Randomly

2. Order Vertices Randomly.

3. Consider sequentially. If v "still dangerous" switch $\chi(v)$ with probability p

Still Dangerous: $v \in A_i$ which has *always* been monochromatic

FAIL: Some A_i monochromatic at end

Erdős Magic: If Pr[FAIL] < 1 χ **MUST** exist

Two Failure Modes

FAILI: A_i was "Red" and stayed Red

FAILII: A_i wasn't Red and became Red

$$\Pr[\text{FAILI}(A_i)] = 2^{1-n}(1-p)^n$$

$$\Pr[\text{FAILI}] \leq (2^{n-1}k)(2^{1-n}(1-p)^n) = k(1-p)^n$$

A_i *blames* A_j if

- $A_i \cap A_j = \{v\}$
- A_j Blue at start
- A_i Red at end
- v **LAST** point of A_i to change
- When v reached A_j all Blue

Theorem: If FAILII then some A_i blames some A_j

Corollary:

$$\Pr[\text{FAILII}] \leq \sum_{i \neq j} \Pr[A_i \text{ blames } A_j]$$

Bounding Pr[A_i blames A_j]

Fix ordering.

- Factor 2 for Red/Blue symmetry
- v Blue and Flips: $p/2$
- $w \in A_j$ after v: $1/2$
- $u \in A_i$ after v: $1/2$
- $w \in A_j$ before v: $1/2 - p/2$
- $u \in A_i$ before v: $1/2 + p/2$

I: Set of $w \in A_i$ before v

J: Set of $u \in A_j$ before v

$$\Pr[A_i \text{ blames } A_j | I, J] = 2^{2-2n} p (1+p)^{|I|} (1-p)^{|J|}$$

A Bad Gamble

$n-1$ Red Cards, $n-1$ Blue Cards, Joker

Shuffle. Start with 1000$

Red: Multiply funds by $1+p$

Blue: Multiply funds by $1-p$

Joker: Cash In.

Theorem: Expectation less than initial

Corollary

$$\Pr[A_i \text{ blames } A_j] \leq 2^{2-2n}p$$

Corollary

$$\Pr[\text{FAILII}] \leq (2^{n-1}k)^2 2^{2-2n}p = k^2 p$$

Asymptotic Calculus

Pr[FAIL] $< k(1-p)^n + k^2p$

Erdős Magic: If for some $p \in [0,1]$

$$k(1-p)^n + k^2p < 1 \ (*)$$

then χ **MUST** exist.

What is max $k = k(n)$ so that (*) holds for some $p \in [0,1]$?

Answer: $k \sim c\sqrt{n/\ln n}$

Heilbronn Problem

THM: $\exists P_1, \ldots, P_n \in [0,1]^2$, all $\mu(P_iP_jP_k) \leq 10^{-3}n^{-2}$

Pf: Random $m = 2n$ points.

$\Pr[\mu(P_iP_jP_k) \leq \epsilon] \leq 10\epsilon$ (exercise!)

$E[\text{small}\Delta] \leq \binom{m}{3}10^{-2}n^{-2}$

Delete one vertex from each small triangle.

$\geq f(m) := m - \binom{m}{3}10^{-2}n^{-2} \geq n$ remain

Erdős Magic: Points *must* exist!

Liar Game

Paul seeks $x \in \{1, \ldots, 100\}$.

Ten Queries. Carole may lie once.

Theorem: Carole Wins!

Carole plays randomly

At end of game:

Pr[x possible] $= \frac{11}{1024}$

Expected number of possible $100\frac{11}{1024} > 1$

When > 1 possible Carole wins

Carole sometimes wins

Erdős Magic: Carole always wins!

Sum Free Sets

$A \subseteq Z - \{0\}$ sumfree if no $a_1 + a_2 = a_3$

THM: $B = \{b_1, \ldots, b_s\} \subset Z - \{0\}$. There exists sumfree $A \subset B$, $|A| \geq \frac{1}{3}|B|$

Pf: $p = 3k + 2$ prime, $p > 2 \max |b_i|$

$C = \{k + 1, \ldots, 2k + 1\}$ sumfree in Z_p

Random Hash: $x \in Z_p - \{0\}$ uniform

$\Psi_x : B \to Z_p - \{0\}$

$b \to xb \bmod p$

$\Psi_x^{-1}(C)$ sumfree (in Z)

$\Pr[\Psi_x(b) \in C] = \frac{k+1}{3k+1} > \frac{1}{3}$

$E[|\Psi_x^{-1}(C)|] > \frac{|B|}{3}$

Erdős Magic: There exists x

$$|\Psi_x^{-1}(C)| > \frac{|B|}{3}$$

Take $A = \Psi_x^{-1}(C)$.

It is not knowledge, but the act of learning, not possession but the act of getting there, which grants the greatest enjoyment. When I have clarified and exhausted a subject, then I turn away from it, in order to go into darkness again; the never-satisfied man is so strange - if he has completed a structure then it is not in order to dwell in it peacefully, but in order to begin another. I imagine the world conqueror must feel thus, who, after one kingdom is scarely conquered, stretches out his arms for another.
– Karl Friedrich Gauss (1808)

The universe is not only queerer than we suppose but queerer than we *can* suppose.

– J.B.S. Haldane