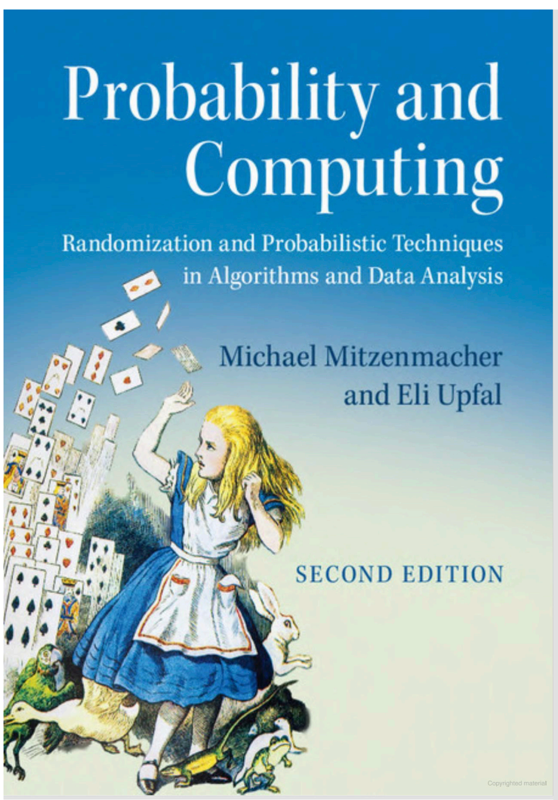
• Theorist's Toolkit:

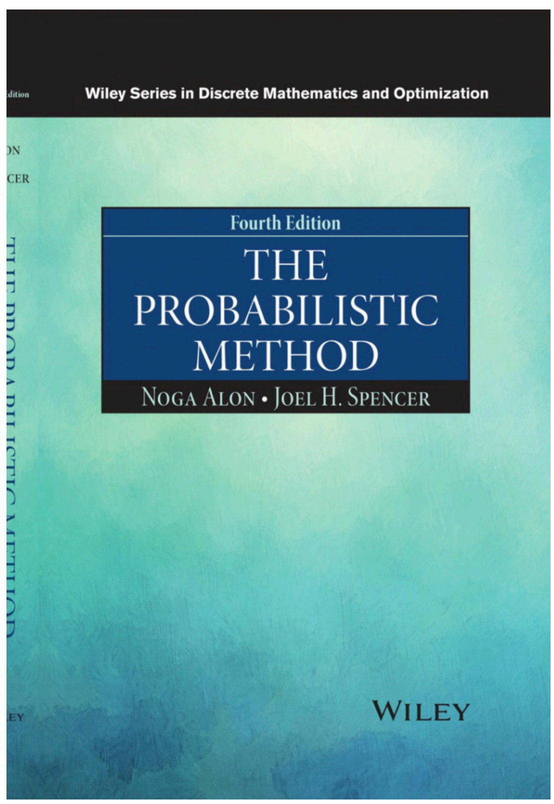
① Probabilistic methods (~3 weeks)
② Information theory (~2 weeks)
③ Streaming algorithms (~2 weeks)
④ Linear algebraic methods (~3 weeks)
⑤ Boolean analysis (~1 weeks)
⑥ Multiplicative weights update (~1 week)
⑦ Misc. topics (~2 weeks)

* Homepage: coming soon.

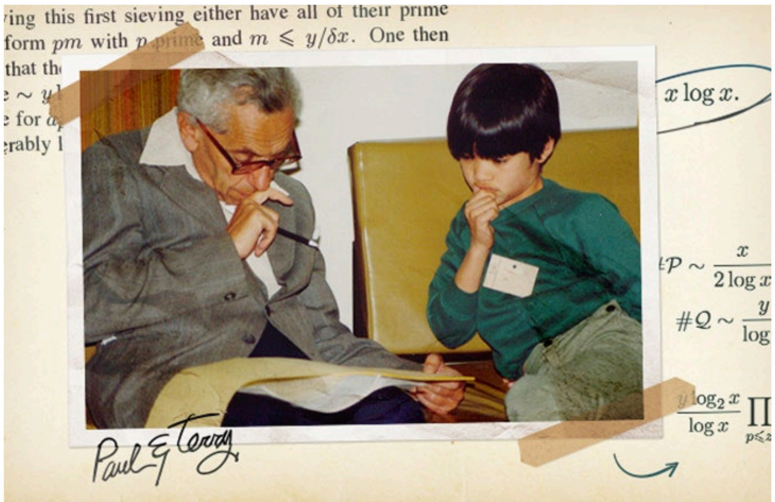
• PROBABILISTIC METHODS:

→ a powerful tool in combinatorics
→ rapid development due to the important role of randomness in TCS and stat. physics.

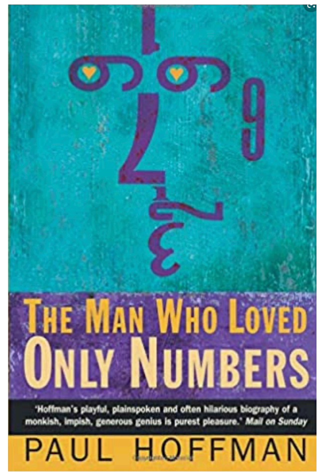




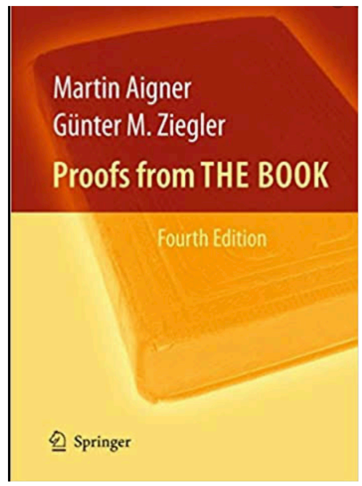
- Initiated by Paul Erdős.



Paul Erdős, left, and Terence Tao discussing math in 1985. This past August, Tao and four other mathematicians proved an old Erdős conjecture, marking the first major advance in 76 years in understanding how far apart prime numbers can be. OLENA SHMAHALO / QUANTA MAGAZINE; ORIGINAL COURTESY OF TERENCE TAO



"I am not qualified to say whether or not God exists. I kind of doubt He does. Nevertheless I'm always saying that the SF(The SF is the supreme Fascist, the Number-One guy up there) has this transfinite book-transfinite being a concept in mathematics that is larger than infinite-that contains the best proofs of all mathematical theorems, proofs that are elegant and perfect."
— Paul Erdős



Highlevel idea:

To prove: a structure with certain desired properties exists,

Do: one defines appropriate probability space of structures, and

show: $\Pr$[desired properties hold in these structures] > 0

→ existence is not proved by showing an explicit example, but rather by a nonconstructive way.

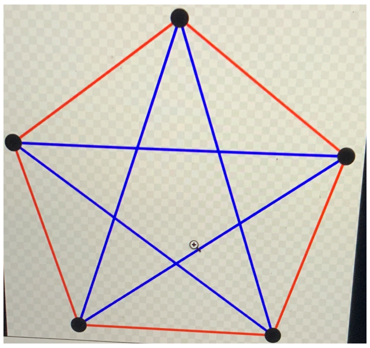
§ 1.1. An application in Ramsey Theory.

• Ramsey Number:

$R(k, \ell)$ is the smallest integer n s.t. in any edge coloring of K_n by red & blue, either there is a red K_k or blue K_ℓ.

Ramsey (1929): $R(k,\ell) < \infty$ for fixed k, ℓ.

Consider $k = 3$, $\ell = 3$, $n = 5$.



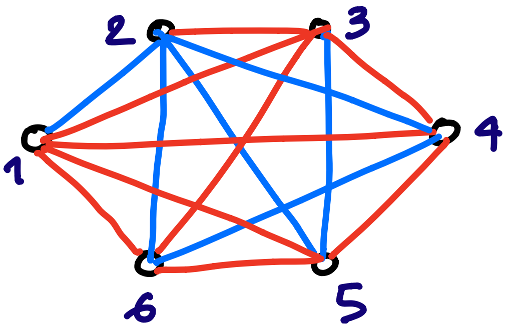
← No monochromatic K_3 (triangle). So, $R(3,3) > 5$.

• One can show: $R(3,3) = 6$.

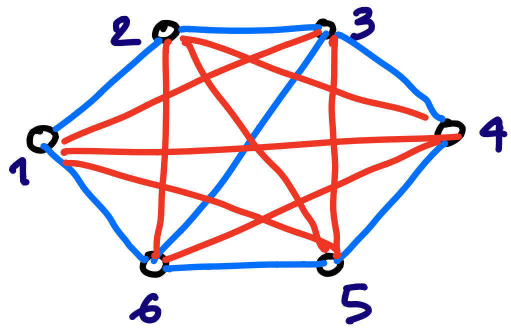
• Theorem on friends & strangers:

In any party of six people ($n = 6$), either at least 3 are pairwise mutual stranger ($k = 3$) or at least 3 are pairwise mutual acquaintances ($\ell = 3$).

friend: Blue edge, stranger: Red edge.

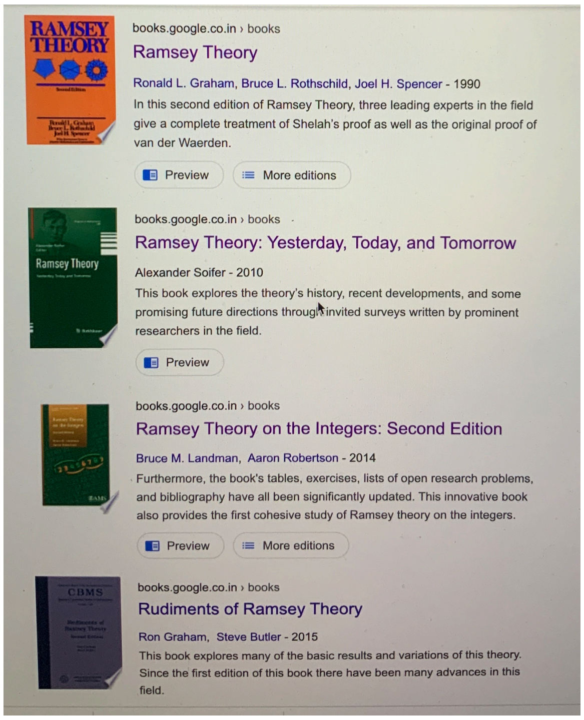


$\Delta 136$, $\Delta 246$



no blue Δ, red $\Delta 135$

- Big branch of combinatorics:

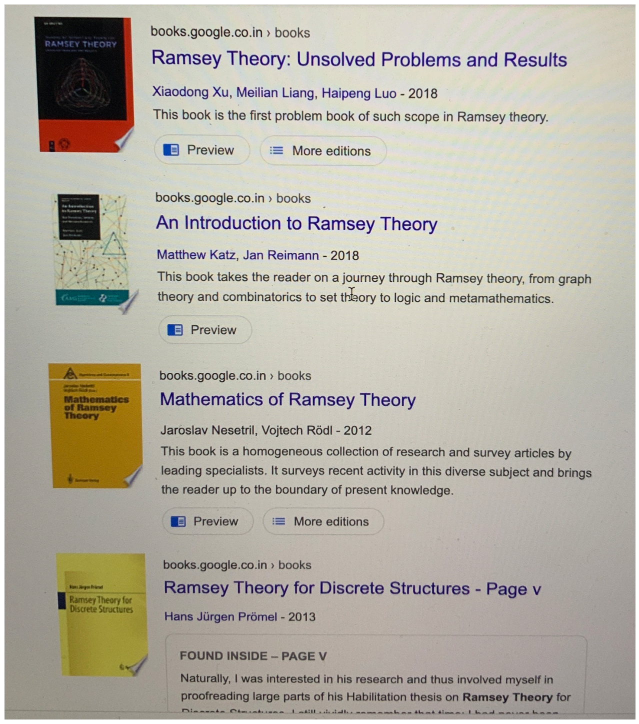


books.google.co.in › books
Ramsey Theory
Ronald L. Graham, Bruce L. Rothschild, Joel H. Spencer - 1990
In this second edition of Ramsey Theory, three leading experts in the field give a complete treatment of Shelah's proof as well as the original proof of van der Waerden.
Preview | More editions

books.google.co.in › books
Ramsey Theory: Yesterday, Today, and Tomorrow
Alexander Soifer - 2010
This book explores the theory's history, recent developments, and some promising future directions through invited surveys written by prominent researchers in the field.
Preview

books.google.co.in › books
Ramsey Theory on the Integers: Second Edition
Bruce M. Landman, Aaron Robertson - 2014
Furthermore, the book's tables, exercises, lists of open research problems, and bibliography have all been significantly updated. This innovative book also provides the first cohesive study of Ramsey theory on the integers.
Preview | More editions

books.google.co.in › books
Rudiments of Ramsey Theory
Ron Graham, Steve Butler - 2015
This book explores many of the basic results and variations of this theory. Since the first edition of this book there have been many advances in this field.



books.google.co.in › books
Ramsey Theory: Unsolved Problems and Results
Xiaodong Xu, Meilian Liang, Haipeng Luo - 2018
This book is the first problem book of such scope in Ramsey theory.
Preview | More editions

books.google.co.in › books
An Introduction to Ramsey Theory
Matthew Katz, Jan Reimann - 2018
This book takes the reader on a journey through Ramsey theory, from graph theory and combinatorics to set theory to logic and metamathematics.
Preview

books.google.co.in › books
Mathematics of Ramsey Theory
Jaroslav Nesetril, Vojtech Rödl - 2012
This book is a homogeneous collection of research and survey articles by leading specialists. It surveys recent activity in this diverse subject and brings the reader up to the boundary of present knowledge.
Preview | More editions

books.google.co.in › books
Ramsey Theory for Discrete Structures - Page v
Hans Jürgen Prömel - 2013
FOUND INSIDE – PAGE V
Naturally, I was interested in his research and thus involved myself in proofreading large parts of his Habilitation thesis on **Ramsey Theory** for

Values / known bounding ranges for Ramsey numbers $R(r, s)$ (sequence A212954 in the OEIS)

r \ s	1	2	3	4	5	6	7	8	9	10
1	1	1	1	1	1	1	1	1	1	1
2		2	3	4	5	6	7	8	9	10
3			6	9	14	18	23	28	36	40–42
4				18	25[7]	36–41	49–61	59[13]–84	73–115	92–149
5					43–48	58–87	80–143	101–216	133–316	149[13]–442
6						102–165	115[13]–298	134[13]–495	183–780	204–1171
7							205–540	217–1031	252–1713	292–2826
8								282–1870	329–3583	343–6090
9									565–6588	581–12677
10										798–23556

Erdős asks us to imagine an alien force, vastly more powerful than us, landing on Earth and demanding the value of $R(5, 5)$ or they will destroy our planet. In that case, he claims, we should marshal all our computers and all our mathematicians and attempt to find the value. But suppose, instead, that they ask for $R(6, 6)$. In that case, he believes, we should attempt to destroy the aliens.

— Joel Spencer[10]

Knowing lower & upper bounds are important questions.

Theorem: If $\binom{n}{k} \cdot 2^{1-\binom{k}{2}} < 1$, then $R(k,k) > n$.

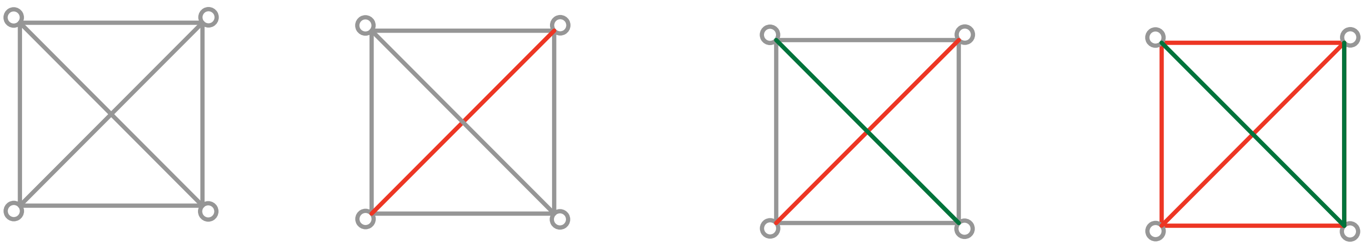
Thus, $R(k,k) > \lfloor 2^{k/2} \rfloor$ for all $k \geq 3$.

[$R(3,3) > \lfloor 2^{3/2} \rfloor \approx 2$. $R(10,10) > \lfloor 2^5 \rfloor \approx 32$]. $R(20,20) > 2^{10} > 1000$.

[Thm 6.1 in M.U, Prop 1.1.1 in A.S]

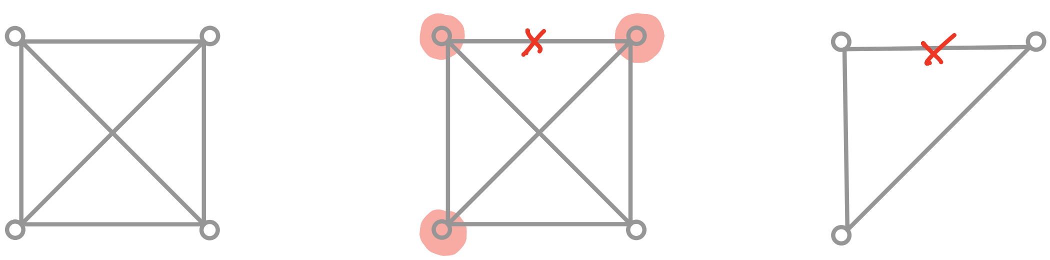
Proof:

- Do random two-coloring of edges: i.e. for each edge $e \in E$, w.p. $\frac{1}{2}$ color it red, w.p. $\frac{1}{2}$ color blue.



- For any fixed set R of k vertices, A_R be event that $K_n[R]$ is monochromatic

($K_n[R]$ is induced subgraph of K_n on R, i.e. formed with R as vertex set & all of the edges connecting pairs of vertices in R)



- Claim: $\Pr[A_R] = 2/2^{\binom{k}{2}} = 2^{1-\binom{k}{2}}$.

- Number of possible choices of R: $\binom{n}{k}$.

- Taking union bound, Pr that at least one of the events A_R occur is at most

$$\binom{n}{k} 2^{1-\binom{k}{2}} < 1. \quad \text{[By assumption]}.$$

Hence, Pr [No A_R happens] > 0.

Therefore, there is a two-coloring of K_n without any monochromatic K_k.

$\Rightarrow \boxed{R(k,k) > n.}$

Note if $k \overset{*}{\geq} 3$, $n \overset{\bullet}{=} \lfloor 2^{k/2} \rfloor$, then

$$\binom{n}{k} 2^{1-\binom{k}{2}} < \left(\frac{n^k}{k!}\right) \cdot 2^{1-k(k-1)/2}$$

$$\overset{\bullet}{\leq} \frac{2^{k^2/2+1-k^2/2+k/2}}{k!} \leq \frac{2^{k/2+1}}{k!} = \frac{2.2\ldots2}{2.3\ldots(k/2+2)\ldots k} \overset{*}{<} 1.$$

$k \geq 4 \Rightarrow$

$k \geq k/2+2$

$k=3,\ \frac{2^{2.5}}{6} < 1.$

Hence, $R(k,k) > \lfloor 2^{k/2} \rfloor$ for all $k \geq 3$. ∎

- Can we use this non-constructive proof to design an efficient algorithm to construct such coloring?

→ General approach: We need two things.

1. We can efficiently sample a coloring from the sample space.
(In this case, random coloring suffice)

2. How many samples we must generate to satisfy our requirements?
Say we sample independently at each trial and Pr[obtaining a sample with desired property] = p.

Then the number of samples needed before finding a "good" sample is a geometric random variable with expectation $1/p$.

So for efficient algorithms we need $1/p$ to be polynomial in input size

- If $p = 1 - o(1)$, then sampling once gives Monte Carlo constructive algorithm that is incorrect w.p. $o(1)$.

(Monte Carlo: Randomized Algo whose output can be wrong w certain probability)

- For example a random coloring of K_{1024} has no monochromatic K_{20} is at most $2^{20/2+1}/20! < 10^{-15}$.

→ very small probability of failure.

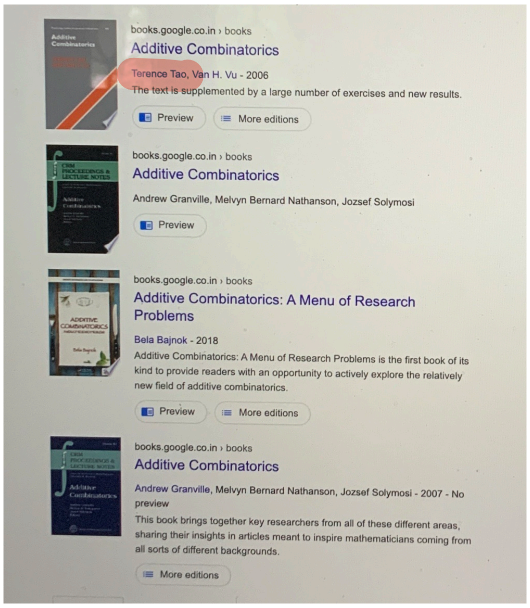
Practice: A random coloring of K_n is very likely not to contain a monochromatic $K_{2\log n}$.

- Suppose we want a Las Vegas algo: one that always gives correct soln. (runtime can vary on the input).

– simply check all $\binom{n}{k}$ cliques & make sure they are not monochromatic.

→ Not practical, if k grows with n.

§ Application in combinatorial number theory / additive combinatorics.



→ Theory of counting additive structures in sets.

[e.g. : Szemeredi's theorem on arithmetic progression, Kakeya conjecture, Erdos distance problem, ...]

Sum-free set: A subset S of an abelian group G is called sum-free if $(S+S) \cap S = \phi$

i.e., $\nexists\, a_1, a_2, a_3 \in S$ s.t. $a_1 + a_2 = a_3$.

[For example $(\mathbb{Z}, +)$ is an abelian group.

→ Closure: $a, b \in \mathbb{Z} \Rightarrow a+b \in \mathbb{Z}$

Associativity: $(a+b)+c = a+(b+c)$, $\forall\, a,b,c \in \mathbb{Z}$.

Identity: $a+0 = 0+a = a \quad \forall\, a \in \mathbb{Z}$

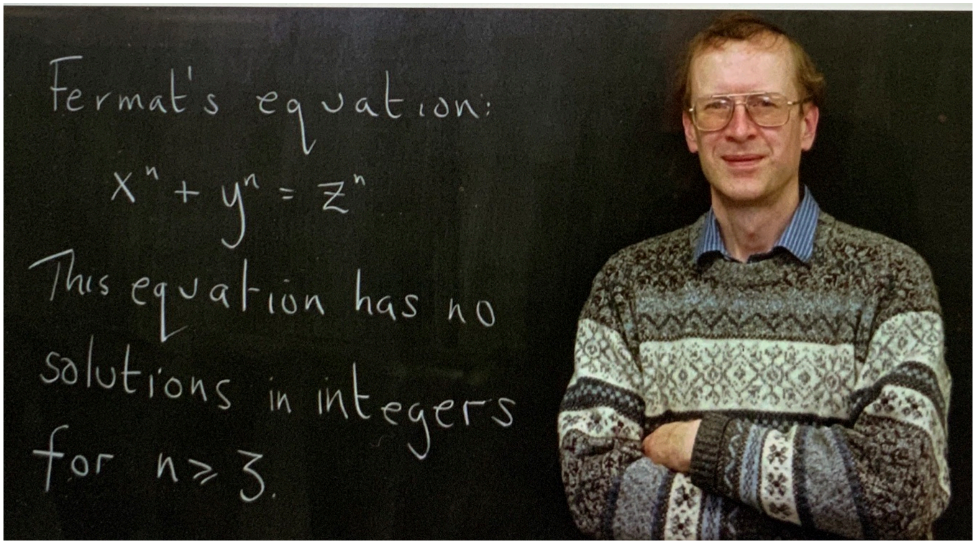
Inverse: $a+(-a) = -a+a = 0 \quad \forall\, a \in \mathbb{Z}$

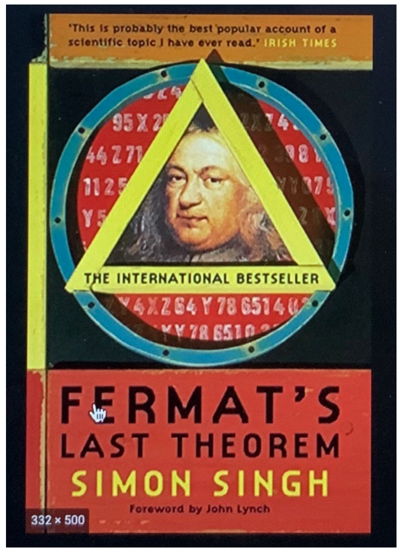
commutativity: $a+b = b+a$. $\forall\, a, b \in \mathbb{Z}$.]

set of odd numbers is sum-free.

$1, 3, 5, 7, 9, \dots$

Fermat's last theorem: For $n \in \mathbb{Z}$, $n > 2$, the set of all nonzero n^{th} powers of the integers is a sum-free subset.





• **Theorem**: [Erdős '65] Thm 1.4.1 in A-S.

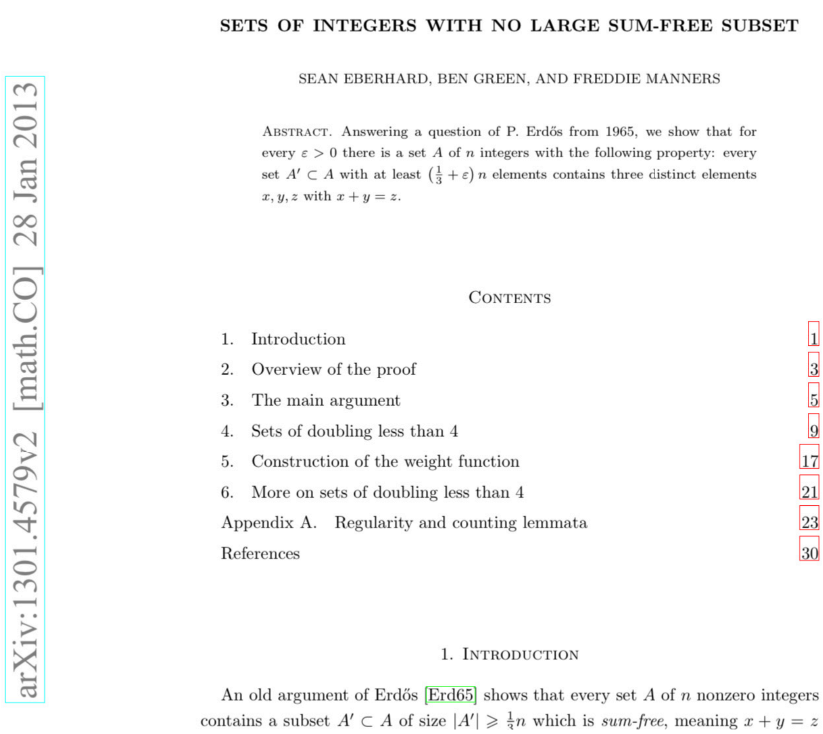
Every set $B = \{b_1, b_2, .., b_n\}$ of n nonzero integers contains a sum-free subset S of size $|S| > n/3$.

[e.g. Take $B = \{2, 3, 5, 8, 13, 21\}$ i.e., $n = 6$.
One sum-free subset is $\{2, 5, 21\}$.]

This is tight! →

say $\epsilon = 10^{-10}$, the tight result says for sufficiently large n there exists array A s.t. its any $(\frac{1}{3} + 10^{-10})n$ sized subset is not sumfree. Whereas Erdős's result says there is a $(\frac{n}{3}+1)$-sized subset which is sum-free.

Note, $10^{-10} \cdot n >> 1$.



SETS OF INTEGERS WITH NO LARGE SUM-FREE SUBSET

SEAN EBERHARD, BEN GREEN, AND FREDDIE MANNERS

ABSTRACT. Answering a question of P. Erdős from 1965, we show that for every $\varepsilon > 0$ there is a set A of n integers with the following property: every set $A' \subset A$ with at least $(\frac{1}{3} + \varepsilon)n$ elements contains three distinct elements x, y, z with $x + y = z$.

CONTENTS

1. INTRODUCTION

An old argument of Erdős [Erd65] shows that every set A of n nonzero integers contains a subset $A' \subset A$ of size $|A'| \geqslant \frac{1}{3}n$ which is *sum-free*, meaning $x + y = z$

Proof idea:

- Create a sum-free subset of large size.
- Find a 'nice' mapping (using prob. methods)

Proof: W.l.o.g. assume B is sorted & $b_n = \max_i b_i$.

- Pick prime $p > 2 \cdot b_n$ (larger than any $b_i + b_j$), s.t. $p \equiv 2 \pmod 3$, i.e. $p = 3k+2$ for some $k \in \mathbb{Z}$.

Dirichlet's theorem on arithmetic progressions

In number theory, **Dirichlet's theorem**, also called the Dirichlet prime number theorem, states that for any two positive coprime integers *a* and *d*, there are infinitely many primes of the form *a* + *nd*, where *n* is also a positive integer. In other words, there are infinitely many primes that are congruent to *a* modulo *d*. The numbers of the form *a* + *nd* form an arithmetic progression

$$a,\ a+d,\ a+2d,\ a+3d,\ \dots,$$

and Dirichlet's theorem states that this sequence contains infinitely many prime numbers. The

Such primes exists!

- Consider $C = \{k+1, k+2, \dots, 2k+1\}$.
  - C is sum-free, even modulo p.

$[(k+1)+(k+1) > 2k+1,\ (2k+1)+(2k+1) = 4k+2 \overset{\text{mod } p}{=} k < k+1]$

- $\dfrac{|C|}{p} = \dfrac{k+1}{3k+2} > 1/3$. So C is large & sum-free

- Pick x uniformly at random from $\mathbb{Z}_p^*$.

[$\mathbb{Z}_p$ is integers mod p : $\{0, 1, \dots, p-1\}$
$\mathbb{Z}_p^*$ is integers (relatively prime to p) mod p : $\{1, \dots, p-1\}$ for prime p.
i.e. for primes p : $\mathbb{Z}_p = \mathbb{Z}_p^* \cup \{0\}$.

so d_i has values $1, \dots, p-1$

- Mapping: $\forall i,\ d_i \equiv x \cdot b_i \pmod p$.

$$S_x = \{ b_i \text{ s.t. } d_i \in C \}.$$

Claim 1: $\forall x,\ S_x$ is sum-free.

From contradiction, assume $\exists b_i, b_j, b_k \in S_x$ s.t. $b_i + b_j = b_k$. $\Rightarrow b_i + b_j \equiv b_k \pmod p$

$\Rightarrow x \cdot b_i + x \cdot b_j \equiv x \cdot b_k \pmod p$

$\Rightarrow d_i + d_j \equiv d_k \pmod p$, where $d_i, d_j, d_k \in C$.

But C is sum-free. Contradiction! ■

$\{1, 2, \dots, n\}$

Fact: $\forall y \in \mathbb{Z}_p^*$, and $\forall i \in [n]$, $\exists$ exactly one $x \in \mathbb{Z}_p^*$ s.t. $y \equiv x \cdot b_i \pmod p$;

i.e. $\Pr[b_i \text{ maps to } y] = 1/(p-1)$.

→ As b_i is rel. prime to p & $b_i < p$.
$b_i \in \mathbb{Z}_p^*$, so $b_i^{-1} \in \mathbb{Z}_p^*$ (property of group).

$\therefore x = y \cdot b_i^{-1} \in \mathbb{Z}_p^*$ [as both $y, b_i^{-1} \in \mathbb{Z}_p^*$].

For contradiction, if $y = x_1 b_i = x_2 b_i \pmod p$
then $x_1 = y \cdot b_i^{-1} = x_2$. $\Rightarrow$ x is unique! ■

Claim 2: $\exists x$ s.t. $|S_x| > n/3$.

From fact, for a fixed $i \in [n]$, as x ranges over $[p-1]$, d_i ranges over all numbers in $[p-1]$.

Let us define indicator function

$$\sigma_i = \begin{cases} 1 & \text{if } x.b_i \in C \\ 0 & \text{otherwise} \end{cases}$$

Hence, $\mathbb{E}[\sigma_i] = \Pr[\sigma_i = 1] = |C|/p-1 > 1/3$.

By linearity of expectation,

$$\mathbb{E}_x[|S_x|] = \mathbb{E}_x[\sum_i \sigma_i] = \sum_i \mathbb{E}_x[\sigma_i] > \frac{n}{3}.$$

Hence, $\exists x$ s.t. $|S_x| > n/3$. ∎

Claim 1 + claim 2: S_x exists! which is large & sum-free.

$\Downarrow$

consider all n mappings & corresponding S_x

$\Downarrow$

Return the S_x w $|S_x| > n/3$.

Can be made algorithmic.

Presently $p = O(b_n)$, so may not be poly(n).

But the proof also works for any prime relatively prime to $b_1, \dots, b_n$.

Fact: Such a prime exists of value poly(n).

Using that prime we'll get an efficient algo.

§ Applications in extremal combinatorics and hypergraph theory.

Extremal Combinatorics: With Applications in Computer Science
books.google.co.in › books

This book is a concise, self-contained, up-to-date introduction to extremal combinatorics for nonspecialists.
Stasys Jukna - 2011 - Preview - More editions

Modern Methods in Extremal Combinatorics
books.google.co.in › books

In this thesis, we apply modern probabilistic and algebraic techniques to different problems in extremal combinatorics.
Lisa Sauermann - 2019 - No preview

Theory of Combinatorial Limits and Extremal Combinatorics
books.google.co.in › books

Taísa Lopes Martins - 2018 - No preview

A Course in Combinatorics
books.google.co.in › books

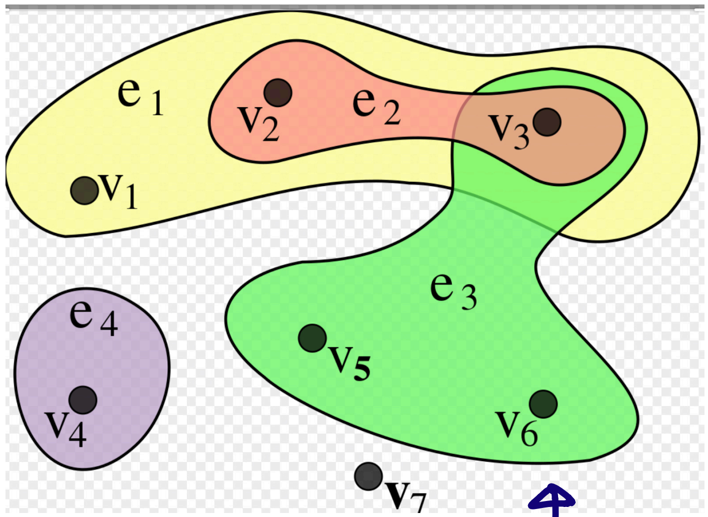
This is the second edition of a popular book on combinatorics, a subject dealing with ways of arranging and distributing objects, and which involves ideas from geometry, algebra and analysis.
J. H. van Lint, R. M. Wilson, Richard Michael Wilson - 2001 - Preview - More editions

Extremal Finite Set Theory
books.google.co.in › books

Intended for graduate students, instructors teaching extremal combinatorics and researchers, this book serves as a sound introduction to the theory of extremal set systems.
Daniel Gerbner, Balazs Patkos - 2018 - Preview - More editions

Extremal Combinatorial Problems and Their Applications - Page viii
books.google.co.in › books

Some information from **combinatorics** 1. 2. 3. 4. 5. Sets and operations with sets Correspondences between sets Binary functions on ordered sets **Combinatorial** schemes **Combinatorial** problems and their complexity Chapter 2. **Extremal** problems on packability of number partitions 1. Number partitions

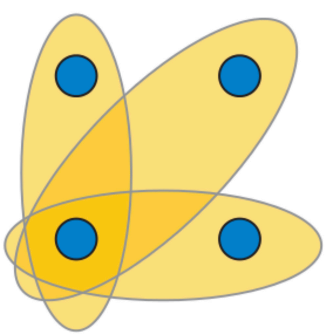


(Hypergraphs generalize graphs)

extremal combinatorics studies maximal/minimal collection of objects (sets, numbers, etc.) that can have a required property.

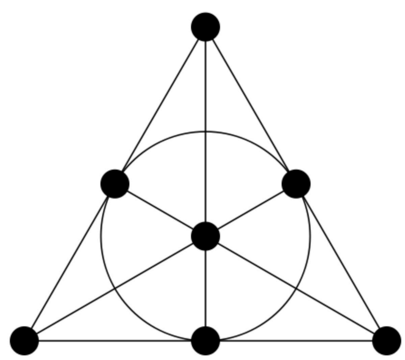
• Def: Intersecting family of sets.

A family $\mathcal{F}$ of sets is called intersecting, if $A, B \in \mathcal{F}$ implies $A \cap B \neq \phi$.



Fano plane is the finite projective plane of order 2.

Important object in projective/incidence geometries.



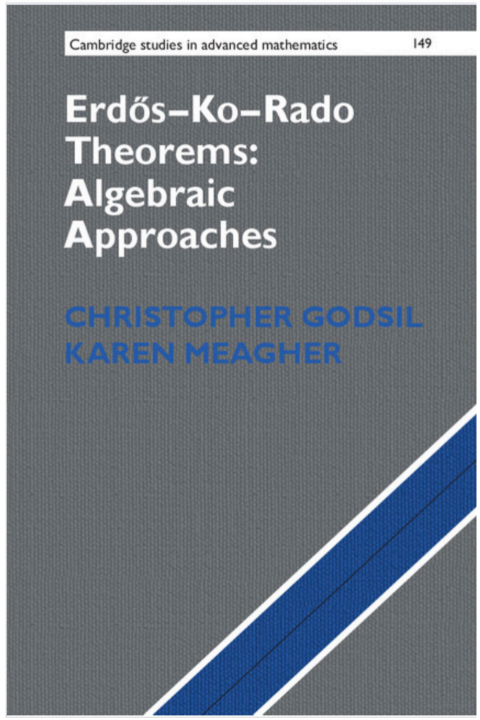
The seven points and seven lines (one drawn as a circle) of the Fano plane form a maximal intersecting family.

• Erdős-Ko-Rado theorem:

Suppose $n \geq 2k$, and $\mathcal{F}$ be an intersecting family of k-element subsets of an n-set $[n] := \{1, 2, \ldots, n\}$.

Then $\boxed{|\mathcal{F}| \leq \binom{n-1}{k-1}}$.

we need this to avoid triviality, as otherwise any two sets intersects.



(Lemma 1 in A-S)

(Ch 23 in proofs from the book)

[comment: $|\mathcal{F}| = \binom{n-1}{k-1}$, if we take the family of k-sets containing a particular element]

Claim: For $s \in [n]$, let $A_s = \{s, s+1, \ldots, s+k-1\}$, where addition is modulo n.

Then $\mathcal{F}$ can contain at most k of the sets A_s.

Pf of claim: Fix some $A_s \in \mathcal{F}$.

All other sets A_t, with $A_t \cap A_s \neq \phi$, can be partitioned into $(k-1)$ pairs:

$$\{A_{s-i}, A_{s+k-i}\}, \quad i \in [k-1].$$

A_t: $A_{s-k+1}, \ldots, A_{s+k-1}$.

Note: $A_{s-i} \cap A_{s+k-i} = \phi$.

Hence, $\mathcal{F}$ can contain at most one member of each pair; total k (including A_s). ∎

Proof of Erdős-Ko-Rado:

Let us choose $i \in [n]$ and a permutation $\sigma : [n] \to [n]$, independently & uniformly at random.

Let $A := \{\sigma(i), \sigma(i+1), \dots, \sigma(i+k-1)\}$.
[addition is again modulo n.]

Note: All k-sets are selected with the same probability in above sampling.

[Total # random choices $= \underbrace{n}_{\text{for } i} \times \underbrace{n!}_{\text{for } \sigma}$.

Fix a k-set A. How many times do we pick A?

$\to$  There are n starting positions, elements of A can be permuted $k!$ times & the rest of the items can be permuted $(n-k)!$ times.

$$\Rightarrow \frac{n \times (n-k)! \times k!}{n \times n!} = 1/\binom{n}{k}.$$

- A can be viewed as uniformly chosen over all k-sets:

Hence, $\Pr[A \in \mathcal{F}] = \dfrac{|\mathcal{F}|}{\binom{n}{k}}$. $\quad \dots (1)$

- Conditioned on any choice of σ, from above claim: $\Pr[A \in \mathcal{F} \mid \sigma] \le k/n$

$$\Rightarrow \Pr[A \in \mathcal{F}] = \sum_{\sigma} \Pr[A \in \mathcal{F} \mid \sigma] \Pr[\sigma] \le n! \cdot \frac{k}{n} \cdot \frac{1}{n!} = \frac{k}{n}$$

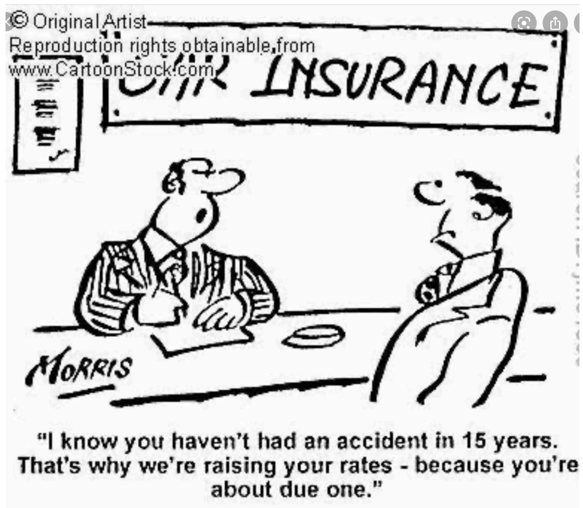
Law of total prob.

$\dots (2)$

From (1) & (2),

$$|\mathcal{F}| \le \binom{n}{k} \cdot \frac{k}{n} = \binom{n-1}{k-1}. \quad \blacksquare$$

LECTURE 2: EXPECTATIONS/ AVERAGING ARGUMENT.



- **Linearity of expectations:**

Let $X_1, X_2, \dots, X_n$ be random variables.
If $X = c_1 X_1 + \dots + c_n X_n$, then
$$\mathbb{E}[X] = c_1 \mathbb{E}[X_1] + \dots + c_n \mathbb{E}[X_n].$$

- **Expectation Argument:**

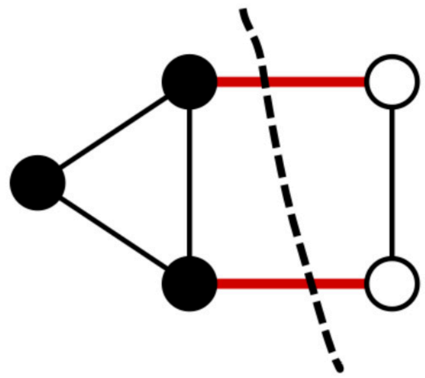
In a discrete probability space, a random variable must assume with +ve probability at least one value that is no greater than its expectation and at least one value that is not smaller than its expectation.

Lemma: (Lem 6.2 in M-U)
Let S be a probability space, and a random variable X defined on S s.t. $\mathbb{E}[X] = \mu$. Then $\Pr(X \geq \mu) > 0$, $\Pr(X \leq \mu) > 0$.

• Application: Finding Max-cut.

Given an undirected graph $G := (V, E)$ a cut $[S, V \setminus S]$ is a partition of V.

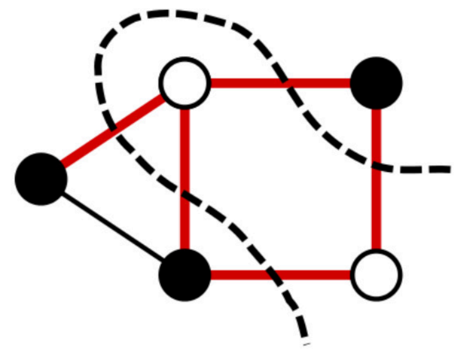
Value of cut is the number of edges with one endpoint in S, and other endpoint in $V \setminus S$.



A minimum cut. in P

Max-cut: maximum value cut

Deep connections with SDP, PCP, UGC



A maximum cut. is NP-hard

• Theorem: Always $\exists$ cut of value $\geq \frac{|E|}{2}$.
(Thm 6.3 in M-U)

Proof: For each vertex $v \in V$, uniformly at random choose $\{0, 1\}$, independently.

Define indicator random variable

$$X_i = \begin{cases} 1 & \text{if endpoints of edge } i \text{ have different value} \\ 0 & \text{.. same value.} \end{cases}$$

$\therefore \mathbb{E}[X_i] = \frac{1}{2}\cdot 1 + \frac{1}{2}\cdot 0 = \frac{1}{2}$.

Define S = vertices of value 0.
$\bar{S}$ = " " value 1.

$\therefore$ expected size of cut $[S, \bar{S}]$

$$= \mathbb{E}\Big[\sum_{i\in E} X_i\Big] = \sum_{i\in E} \mathbb{E}[X_i] = \frac{|E|}{2}. \quad \blacksquare$$

⊙ Transforming to an algorithm:

Say a random 0-1 assignment gives a cut (A, B). [A, B are 0-1 vertices, resp.]

Let $p = \Pr[\text{cut}(A,B) \geq |E|/2]$.

Now, $\frac{|E|}{2} = \mathbb{E}[\text{cut}(A,B)]$

$$= \sum_{j<|E|/2} j \Pr[\text{cut}(A,B)=j] + \sum_{j\geq |E|/2} j \Pr[\text{cut}(A,B)=j]$$

$$\leq (1-p)\left(\frac{|E|}{2} - 1\right) + p|E|.$$

$$\Rightarrow p \geq \frac{1}{(|E|/2)+1}.$$

So, expected number of samples to obtain a cut with $|E|/2$ edges is only $|E|/2 + 1$. Polynomial time!

§ Derandomization :

Let us consider vertices deterministically, one by one, $v_1, v_2, \ldots, v_n$.

Let x_i is the value assigned to v_i.

if $x_i = 0$ then $v_i \in A$

if $x_i = 1$ then $v_i \in B$.

Suppose, we have assigned values to $v_1, \ldots, v_k$.

Now we consider expected value of the cut if remaining vertices $v_{k+1}, \ldots, v_n$ are assigned 0/1 uniformly at random and independently.

→ This is conditional expectation.

$\mathbb{E}[\text{cut}(A,B) \mid v_1 = x_1, \ldots, v_k = x_k]$.

We want to inductively assign value x_{k+1} to v_{k+1} s.t.

$$\boxed{\begin{aligned}&\mathbb{E}[\text{cut}(A,B) \mid v_1 = x_1, \ldots, v_k = x_k] \\ &\quad \leq \mathbb{E}[\text{cut}(A,B) \mid v_1 = x_1, \ldots, v_k = x_k, v_{k+1} = x_{k+1}]\end{aligned}}$$

Then we will get

$$\underbrace{\mathbb{E}[\text{cut}(A,B) \mid v_1 = x_1, \ldots, v_n = x_n]}_{\text{value of our solution}} \geq \mathbb{E}[\text{cut}(A,B)].$$

$\geq |E|/2$

Base case:

$\mathbb{E}[\text{cut}(A,B) \mid v_1 = x_1] = \mathbb{E}[\text{cut}(A,B)]$.

→ holds by symmetry, as it does not matter where we place the first vertex.

Inductive step:

Consider $v_{k+1} = 1$ and 0 w.p. $1/2$.

Then, $\mathbb{E}[\text{cut}(A,B) \mid v_1 = x_1, \dots, v_k = x_k]$

$= \frac{1}{2}\underbrace{\mathbb{E}[\text{cut}(A,B) \mid v_1 = x_1, \dots, v_k = x_k, v_{k+1} = 1]}_{Q_1}$

$+ \frac{1}{2}\underbrace{\mathbb{E}[\text{cut}(A,B) \mid v_1 = x_1, \dots, v_k = x_k, v_{k+1} = 0]}_{Q_2}$

$= \frac{1}{2}(Q_1 + Q_2)$.

$\Rightarrow \max(Q_1, Q_2) \geq \frac{1}{2}(Q_1 + Q_2)$

$= \mathbb{E}[\text{cut}(A,B) \mid v_1 = x_1, \dots, v_k = x_k]$.

So we just need to compute Q_1 & Q_2 and assign $v_{k+1} = 1$ if $Q_1 > Q_2$
and $= 0$ if $Q_1 \leq Q_2$.

Computation of Q_1 (Q_2 is analogous):

→ Conditioning gives assignment of $x_1, x_2, \dots, x_{k+1}$.

We can count the number of edges among these k+1 vertices such that their endpoints received different values. — these edges will contribute to the cut. Let this count be $|E_{k+1}|$.

Other edges contribute to cut w.p. $\frac{1}{2}$.

→ Easy to compute in $O(|E|)$ time.

idea: The larger of the two quantities is determined by whether v_{k+1} has more 0-neighbors or 1-neighbors.

Edges not having v_{k+1} as endpoint contribute the same to both Q_1, Q_2.

⊙ Simple greedy algo:
- Consider vertices in an arbitrary order.
- Put v_1 in A.
- for each successive vertex v_i
  Put v_i in A (resp. B) if v_i has more neighbors in B (resp. A).

§ Applications: Balancing vectors.

- Basic problem in discrepancy, has various applications.


polyalg.csa.iisc.ac.in

Polynomials as an Algorithmic Paradigm

HOME TALKS VISITS JOIN US

Online vector balancing

Nikhil Bansal, CWI and TU Eindhoven

13/07/2020, 21:00:00-22:00:00 Talk Recording Link

Abstract: Consider the setting where vectors in [-1,1]^n arrive online, and upon the arrival of vector v_t at time t, it must be immediately and irrevocably assigned a sign +1 or -1. The goal is to pick these signs to ensure that the norm of the signed sum of these vectors stays small.

Such online discrepancy games were originally considered by Spencer in the 70's, but have received renewed attention due to applications in online algorithms. I will give an overview of the results and techniques in the area and describe several new recent results (after the STOC 2020 paper) that obtain close to optimal bounds in many general settings such as for the online version of Komlos and Banaszczyk problems.

Based on joint works with Joel Spencer, Haotian Jiang, Raghu Meka, Sahil Singla and Makrand Sinha.

- Problem: Let $v_1, v_2, \dots, v_n \in \mathbb{R}^m$. Find signs $\epsilon_i \in \{+1, -1\}$ s.t.

$$\left\| \sum_{i=1}^{n} \epsilon_i v_i \right\|_2 \text{ is minimized.}$$

(Here, $\|\cdot\|_2$ is Euclidean norm, i.e.

$$\|x\|_2 = \sqrt{x_1^2 + \dots + x_m^2} \text{ for vector } x = (x_1, \dots, x_m).$$

- Theorem:

Let $v_i \in \mathbb{R}^m$, $\|v_i\|_2 = 1$ $\forall i \in [n]$.

Then $\exists\, \epsilon_i \in \{+1, -1\}$ for $i \in [n]$, s.t.

$$\left\| \sum_{i=1}^{n} \epsilon_i v_i \right\|_2 \le \sqrt{n}, \quad \left\| \sum_{i=1}^{n} \epsilon_i v_i \right\|_2 \ge \sqrt{n},$$

Proof: Select ϵ_i's uniformly and independently from $\{-1,+1\}$.

Let $X = \| \sum_{i=1}^{n} \epsilon_i v_i \|_2^2$

Dot product

$$= \sum_{i=1}^{n} \sum_{j=1}^{n} \epsilon_i \epsilon_j v_i \cdot v_j \qquad \left[\because \|x\|_2^2 = x \cdot x \right]$$

Thus, $\mathbb{E}[X] = \sum_{i=1}^{n} \sum_{j=1}^{n} v_i \cdot v_j \, \mathbb{E}[\epsilon_i \epsilon_j]$

(by lin. of exp.)

Now $\mathbb{E}[\epsilon_i \epsilon_j] = \mathbb{E}[\epsilon_i] \, \mathbb{E}[\epsilon_j] = 0$, for $i \neq j$.

and $\mathbb{E}[\epsilon_i \epsilon_j] = \mathbb{E}[\epsilon_i^2] = 1$ for $i = j$.

$\therefore \mathbb{E}[X] = \sum_{i=1}^{n} v_i \cdot v_i = n \cdot 1 = n$.

$\Rightarrow \exists \, \epsilon_i$'s s.t. $X \leq n$ and $X \geq n$.

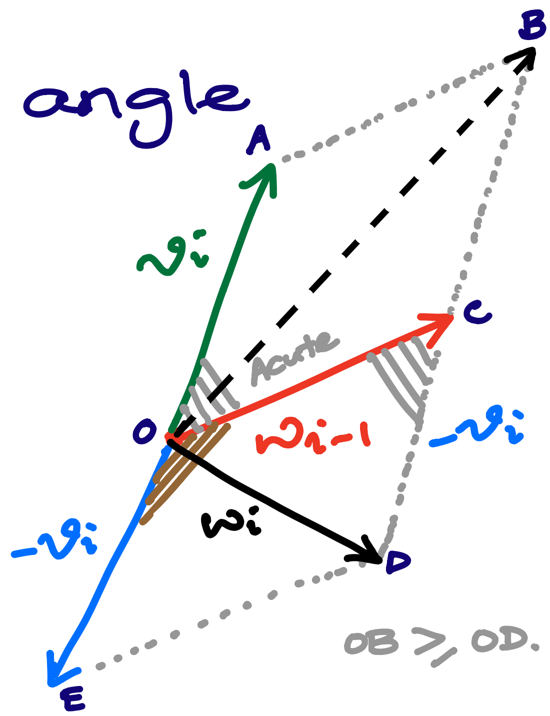
The theorem is proven, by taking square roots as $X^{\frac{1}{2}} = \| \sum_{i=1}^{n} \epsilon_i v_i \|_2$.

- Note: Using Jensen's inequality $\mathbb{E}(X^{\frac{1}{2}}) \leq \sqrt{\mathbb{E}X} = \sqrt{n}$. Now as $y = x^{1/2}$ is strictly concave and X is not constant, the inequality is not tight [e.g. see Thomas-Cover Thm 2.6.2] and $\mathbb{E}(X^{1/2}) < \sqrt{n}$ unless X is constant.

- An alternate nonprobabilistic proof.

Greedy algo.

- Initialize: $\epsilon_1 = +1$, $w_1 := v_1$.
- For $i = 2$ to n:
  - ▸ if (v_i makes acute angle with $w_{i-1} = \sum_{j=1}^{i-1} \epsilon_j v_j$) then set $\epsilon_i = -1$.
  - ▸ Else set $\epsilon_i = +1$.



⊙ Proofs follows from Pythagorus + Induction.

- Claim: $\|w_i\|_2 \leq \sqrt{i}$.

Base case: $\|w_1\|_2 = \|v_1\|_2 = 1$.

Induction:

w_{i-1} and $\epsilon_i v_i$ makes obtuse angle.

$$\therefore \|w_i\|_2^2 \leq \|w_{i-1}\|_2^2 + \|\epsilon_i v_i\|_2^2 \quad \text{(Pyth.)}$$

$$\leq (i-1) + 1 = i. \qquad \bullet$$

Therefore, $\|w_n\|_2 \leq \sqrt{n}$. ■