The Probabilistic Method

Techniques

- Union bound
- Argument from expectation
- Alterations
- The second moment method
- The (Lovasz) Local Lemma

And much more

- Alon and Spencer, "The Probabilistic Method"
- Bolobas, "Random Graphs"

Outline

The Union Bound Technique: Main Idea

- A: event our structure exists, want $\text{Prob}[A] > 0$ or $\text{Prob}[\bar{A}] < 1$

The Union Bound Technique: Main Idea

- A: event our structure exists, want Prob$[A] > 0$ or Prob$[\bar{A}] < 1$
- Suppose $\bar{A}$ implies one of $B_1, \cdots, B_n$ must hold

The Union Bound Technique: Main Idea

- A: event our structure exists, want Prob$[A] > 0$ or Prob$[\bar{A}] < 1$
- Suppose $\bar{A}$ implies one of $B_1, \cdots, B_n$ must hold
- Then, by the union bound

$$\text{Prob}\left[\bar{A}\right] \leq \text{Prob}\left[\bigcup_i B_i\right] \leq \sum_i \text{Prob}[B_i]$$

The Union Bound Technique: Main Idea

- A: event our structure exists, want $\text{Prob}[A] > 0$ or $\text{Prob}[\bar{A}] < 1$
- Suppose $\bar{A}$ implies one of $B_1, \cdots, B_n$ must hold
- Then, by the union bound

$$\text{Prob}\left[\bar{A}\right] \leq \text{Prob}\left[\bigcup_i B_i\right] \leq \sum_i \text{Prob}[B_i]$$

- Thus, as long as

$$\sum_i \text{Prob}[B_i] < 1$$

our structure exists!

The Union Bound Technique: Main Idea

- A: event our structure exists, want Prob$[A] > 0$ or Prob$[\bar{A}] < 1$
- Suppose $\bar{A}$ implies one of $B_1, \cdots, B_n$ must hold
- Then, by the union bound

$$\text{Prob}\left[\bar{A}\right] \leq \text{Prob}\left[\bigcup_i B_i\right] \leq \sum_i \text{Prob}[B_i]$$

- Thus, as long as

$$\sum_i \text{Prob}[B_i] < 1$$

  our structure exists!

We have seen this used in Ramsey number, magical graph, d-disjunct matrix examples.

Example 1: Nice Tournaments

- A tournament is an orientation G of K_n
- Think of $u \to v$ as *player* u *beats player* v
- Fix integer k, G is nice if for every k-subset S of players there is another v who beats all of S

Example 1: Nice Tournaments

- A tournament is an orientation G of K_n
- Think of $u \to v$ as *player* u *beats player* v
- Fix integer k, G is nice if for every k-subset S of players there is another v who beats all of S
- Intuitively, nice tournaments may exist for large n

Existence of Nice Tournaments (Erdős, 1963)

- For every $\{u, v\}$, let $u \to v$ with probability $1/2$
- A: event that a random G is nice

Existence of Nice Tournaments (Erdős, 1963)

- For every $\{u, v\}$, let $u \to v$ with probability $1/2$
- A: event that a random G is nice
- $\bar{A}$ implies $\displaystyle\bigcup_{|S|=k} B_S$ where $B_S =$ "S is not beaten by **any** $v \notin S$"

Existence of Nice Tournaments (Erdős, 1963)

- For every $\{u, v\}$, let $u \to v$ with probability $1/2$
- A: event that a random G is nice
- $\bar{A}$ implies $\bigcup_{|S|=k} B_S$ where $B_S =$ "S is not beaten by **any** $v \notin S$"

$$\text{Prob}[B_S] = \left(1 - \frac{1}{2^k}\right)^{n-k}$$

- Hence, nice tournaments exist as long as $\binom{n}{k}\left(1 - \frac{1}{2^k}\right)^{n-k} < 1$

Existence of Nice Tournaments (Erdős, 1963)

- For every $\{u, v\}$, let $u \to v$ with probability $1/2$
- A: event that a random G is nice
- $\bar{A}$ implies $\bigcup_{|S|=k} B_S$ where $B_S =$ "S is not beaten by **any** $v \notin S$"

$$\text{Prob}[B_S] = \left(1 - \frac{1}{2^k}\right)^{n-k}$$

- Hence, nice tournaments exist as long as $\binom{n}{k}\left(1 - \frac{1}{2^k}\right)^{n-k} < 1$
- What's the order of n for which this holds?

$$\text{use } \binom{n}{k} \leq \left(\frac{ne}{k}\right)^k \text{ and } \left(1 - \frac{1}{2^k}\right)^{n-k} < e^{-\frac{n-k}{2^k}}$$

Existence of Nice Tournaments (Erdős, 1963)

- For every $\{u, v\}$, let $u \to v$ with probability $1/2$
- A: event that a random G is nice
- $\bar{A}$ implies $\bigcup_{|S|=k} B_S$ where $B_S =$ "S is not beaten by **any** $v \notin S$"

$$\text{Prob}[B_S] = \left(1 - \frac{1}{2^k}\right)^{n-k}$$

- Hence, nice tournaments exist as long as $\binom{n}{k}\left(1 - \frac{1}{2^k}\right)^{n-k} < 1$
- What's the order of n for which this holds?

$$\text{use } \binom{n}{k} \leq \left(\frac{ne}{k}\right)^k \text{ and } \left(1 - \frac{1}{2^k}\right)^{n-k} < e^{-\frac{n-k}{2^k}}$$

- Nice tournaments exist as long as $\left(\frac{ne}{k}\right)^k e^{-\frac{n-k}{2^k}} < 1$.

Existence of Nice Tournaments (Erdős, 1963)

- For every $\{u, v\}$, let $u \to v$ with probability $1/2$
- A: event that a random G is nice
- $\bar{A}$ implies $\bigcup_{|S|=k} B_S$ where $B_S =$ "S is not beaten by **any** $v \notin S$"

$$\text{Prob}[B_S] = \left(1 - \frac{1}{2^k}\right)^{n-k}$$

- Hence, nice tournaments exist as long as $\binom{n}{k}\left(1 - \frac{1}{2^k}\right)^{n-k} < 1$
- What's the order of n for which this holds?

$$\text{use } \binom{n}{k} \leq \left(\frac{ne}{k}\right)^k \text{ and } \left(1 - \frac{1}{2^k}\right)^{n-k} < e^{-\frac{n-k}{2^k}}$$

- Nice tournaments exist as long as $\left(\frac{ne}{k}\right)^k e^{-\frac{n-k}{2^k}} < 1$.
- So, $n = \Omega\left(k^2 \cdot 2^k\right)$ is good!

Example 2: 2-coloring of uniform hypergraphs

- Given a k-uniform hypergraph $G = (V, E)$, i.e.
  - E is a collection of k-subsets of V
- G is 2-colorable iff each vertex in V can be assigned with red or blue such that there's no monochromatic edge

Example 2: 2-coloring of uniform hypergraphs

- Given a k-uniform hypergraph $G = (V, E)$, i.e.
  - E is a collection of k-subsets of V
- G is 2-colorable iff each vertex in V can be assigned with red or blue such that there's no monochromatic edge
- Intuitively, if $|E|$ is small then G is 2-colorable!

Example 2: 2-coloring of uniform hypergraphs

- Given a k-uniform hypergraph $G = (V, E)$, i.e.
  - E is a collection of k-subsets of V
- G is 2-colorable iff each vertex in V can be assigned with red or blue such that there's no monochromatic edge
- Intuitively, if $|E|$ is small then G is 2-colorable!
- Question is: "how small?"

Example 2: 2-coloring of uniform hypergraphs

- Given a k-uniform hypergraph $G = (V, E)$, i.e.
  - E is a collection of k-subsets of V
- G is 2-colorable iff each vertex in V can be assigned with red or blue such that there's no monochromatic edge
- Intuitively, if $|E|$ is small then G is 2-colorable!
- Question is: "how small?"
- An answer may be obtained along the line: "for n *small enough*, a random 2-coloring is good with positive probability"

Example 2: 2-coloring of uniform hypergraphs

- Given a k-uniform hypergraph $G = (V, E)$, i.e.
  - E is a collection of k-subsets of V
- G is 2-colorable iff each vertex in V can be assigned with red or blue such that there's no monochromatic edge
- Intuitively, if $|E|$ is small then G is 2-colorable!
- Question is: "how small?"
- An answer may be obtained along the line: "for n *small enough*, a random 2-coloring is good with positive probability"

Theorem (Erdős, 1963)

Every k-uniform hypergraph with $< 2^{k-1}$ edges is 2-colorable!

Outline

The Argument from Expectation: Main Idea

- X a random variable with $\mathsf{E}[X] = \mu$, then
  - There must exist a sample point ω with $X(\omega) \geq \mu$
  - There must exist a sample point ω with $X(\omega) \leq \mu$

The Argument from Expectation: Main Idea

- X a random variable with $\mathsf{E}[X] = \mu$, then
  - There must exist a sample point ω with $X(\omega) \geq \mu$
  - There must exist a sample point ω with $X(\omega) \leq \mu$
- X a random variable with $\mathsf{E}[X] \leq \mu$, then
  - There must exist a sample point ω with $X(\omega) \leq \mu$

The Argument from Expectation: Main Idea

- X a random variable with $\mathsf{E}[X] = \mu$, then
  - There must exist a sample point ω with $X(\omega) \geq \mu$
  - There must exist a sample point ω with $X(\omega) \leq \mu$
- X a random variable with $\mathsf{E}[X] \leq \mu$, then
  - There must exist a sample point ω with $X(\omega) \leq \mu$
- X a random variable with $\mathsf{E}[X] \geq \mu$, then
  - There must exist a sample point ω with $X(\omega) \geq \mu$

Have we seen this?

Example 1: Large Cuts in Graphs

Intuition & Question

Intuition: every graph must have a "sufficiently large" cut (A, B).
Question: How large?

Example 1: Large Cuts in Graphs

Intuition & Question

Intuition: every graph must have a "sufficiently large" cut (A, B).
Question: How large?

Line of thought

On average, a *random* cut has size μ, hence there must exist a cut of size $\geq \mu$.

Example 1: Large Cuts in Graphs

Intuition & Question

Intuition: every graph must have a "sufficiently large" cut (A, B).
Question: How large?

Line of thought

On average, a *random* cut has size μ, hence there must exist a cut of size $\geq \mu$.

- Put a vertex in either A or B with probability $1/2$
- Expected number of edges X with one end point in each is

Example 1: Large Cuts in Graphs

Intuition & Question

Intuition: every graph must have a "sufficiently large" cut (A, B).
Question: How large?

Line of thought

On average, a *random* cut has size μ, hence there must exist a cut of size $\geq \mu$.

- Put a vertex in either A or B with probability $1/2$
- Expected number of edges X with one end point in each is

$$\mathsf{E}[X] = \mathsf{E}\left[\sum_e X_e\right] = \sum_e \mathsf{Prob}[X_e] = |E|/2$$

Example 1: Large Cuts in Graphs

Intuition & Question

Intuition: every graph must have a "sufficiently large" cut (A, B).
Question: How large?

Line of thought

On average, a *random* cut has size μ, hence there must exist a cut of size $\geq \mu$.

- Put a vertex in either A or B with probability $1/2$
- Expected number of edges X with one end point in each is

$$\mathsf{E}[X] = \mathsf{E}\left[\sum_e X_e\right] = \sum_e \mathsf{Prob}[X_e] = |E|/2$$

Theorem

For every graph $G = (V, E)$, there must be a cut with $\geq |E|/2$ edges

Example 2: ± 1 Linear Combinations of Unit Vectors

Theorem

Let $\mathbf{v}_1, \cdots, \mathbf{v}_n$ *be* n *unit vectors in* $\mathbb{R}^n$.
There exist $\alpha_1, \cdots, \alpha_n \in \{-1, 1\}$ *such that*

$$|\alpha_1 \mathbf{v}_1 + \cdots + \alpha_n \mathbf{v}_n| \leq \sqrt{n}$$

and, there exist $\alpha_1, \cdots, \alpha_n \in \{-1, 1\}$ *such that*

$$|\alpha_1 \mathbf{v}_1 + \cdots + \alpha_n \mathbf{v}_n| \geq \sqrt{n}$$

Example 2: ± 1 Linear Combinations of Unit Vectors

Theorem

Let $\mathbf{v}_1, \cdots, \mathbf{v}_n$ *be* n *unit vectors in* $\mathbb{R}^n$*.*
There exist $\alpha_1, \cdots, \alpha_n \in \{-1, 1\}$ *such that*

$$|\alpha_1 \mathbf{v}_1 + \cdots + \alpha_n \mathbf{v}_n| \leq \sqrt{n}$$

and, there exist $\alpha_1, \cdots, \alpha_n \in \{-1, 1\}$ *such that*

$$|\alpha_1 \mathbf{v}_1 + \cdots + \alpha_n \mathbf{v}_n| \geq \sqrt{n}$$

Simply because on average these combinations have length $\sqrt{n}$.

Example 2: ± 1 Linear Combinations of Unit Vectors

Theorem

Let $\mathbf{v}_1, \cdots, \mathbf{v}_n$ *be* n *unit vectors in* $\mathbb{R}^n$.
There exist $\alpha_1, \cdots, \alpha_n \in \{-1, 1\}$ *such that*

$$|\alpha_1 \mathbf{v}_1 + \cdots + \alpha_n \mathbf{v}_n| \leq \sqrt{n}$$

and, there exist $\alpha_1, \cdots, \alpha_n \in \{-1, 1\}$ *such that*

$$|\alpha_1 \mathbf{v}_1 + \cdots + \alpha_n \mathbf{v}_n| \geq \sqrt{n}$$

Simply because on average these combinations have length $\sqrt{n}$.
Specifically, choose $\alpha_i \in \{-1, 1\}$ independently with prob. $1/2$

$$\mathsf{E}\left[|\alpha_1 \mathbf{v}_1 + \cdots + \alpha_n \mathbf{v}_n|^2\right] = \sum_{i,j} \mathbf{v}_i \cdot \mathbf{v}_j \mathsf{E}[\alpha_i \alpha_j] = \sum_i \mathbf{v}_i^2 = n.$$

Example 3: Unbalancing Lights

Theorem

For $1 \le i, j \le n$, we are given $a_{ij} \in \{-1, 1\}$. Then, there exist $\alpha_i, \beta_j \in \{-1, 1\}$ such that

$$\sum_i \sum_j a_{ij} \alpha_i \beta_j \ge \left(\sqrt{\frac{2}{\pi}} + o(1) \right) n^{3/2}$$

Example 3: Unbalancing Lights

Theorem

For $1 \le i, j \le n$, we are given $a_{ij} \in \{-1, 1\}$. Then, there exist $\alpha_i, \beta_j \in \{-1, 1\}$ such that

$$\sum_i \sum_j a_{ij} \alpha_i \beta_j \ge \left(\sqrt{\frac{2}{\pi}} + o(1) \right) n^{3/2}$$

- Choose $\beta_j \in \{-1, 1\}$ independently with prob. $1/2$.
- $R_i = \sum_j a_{ij} \beta_j$, then

$$\mathsf{E}[|R_i|] = 2 \frac{n \binom{n-1}{\lfloor (n-1)/2 \rfloor}}{2^n} \approx \left(\sqrt{\frac{2}{\pi}} + o(1) \right) n^{1/2}$$

Example 3: Unbalancing Lights

Theorem

For $1 \le i, j \le n$, *we are given* $a_{ij} \in \{-1, 1\}$. *Then, there exist* $\alpha_i, \beta_j \in \{-1, 1\}$ *such that*

$$\sum_i \sum_j a_{ij}\alpha_i\beta_j \ge \left(\sqrt{\frac{2}{\pi}} + o(1)\right) n^{3/2}$$

- Choose $\beta_j \in \{-1, 1\}$ independently with prob. $1/2$.
- $R_i = \sum_j a_{ij}\beta_j$, then

$$\mathsf{E}[|R_i|] = 2\frac{n\binom{n-1}{\lfloor (n-1)/2 \rfloor}}{2^n} \approx \left(\sqrt{\frac{2}{\pi}} + o(1)\right) n^{1/2}$$

- Choose α_i with the same sign as R_i, for all i

Outline

Alteration Technique: Main Idea

- A randomly chosen object may not satisfy the property we want
- So, after choosing it we modify the object a little
- In non-elementary situations, the modification itself may be probabilistic
- Or, there might be more than one modification step

Example 1: Independent Set

- $\alpha(G)$ denotes the maximum size of an independent set in G
- Say G has n vertices and m edges
- Intuition: $\alpha(G)$ is proportional to n and inversely proportional to m
- Line of thought: on average a randomly chosen independent set has size μ (proportional to n and inversely proportional to m)
- Problem: random subset of vertices may not be an independent set!!!

- Choose a random subset X of vertices where Prob$[v \in X] = p$ (to be determined)
- Remove one end point from each edge in X
- Let Y be the set of edges in X
- Left with at least $|X| - |Y|$ vertices which are independent

$$\mathsf{E}[|X| - |Y|] = np - mp^2 = -m\left(p - \frac{n}{2m}\right)^2 + \frac{n^2}{4m}$$

Theorem

For any graph with n vertices and m edges, there must be an independent set of size at least $n^2/(4m)$.

Example 2: Dominating Set

- Given $G = (V, E)$, $S \subset V$ is a dominating set iff every vertex either is in S or has a neighbor in S
- Intuition: graphs with high vertex degrees should have small dominating set
- Line of thought: a randomly chosen dominating set has mean size μ

A Randomized Algorithm based on Alteration Technique

- Include a vertex in X with probability p
- Let Y = set of vertices in $V - X$ with no neighbor in X
- Output $X \cup Y$

$$\text{Prob}[u \notin X \text{ and no neighbor in } X] = (1-p)^{\deg(u)+1} \leq (1-p)^{\delta+1}$$

where $\deg(u)$ is the degree of u and δ is the minimum degree.

$$\mathsf{E}[|X| + |Y|] \leq n\left(p + (1-p)^{\delta+1}\right) \leq n\left(p + e^{-p(\delta+1)}\right)$$

To minimize the RHS, choose $p = \frac{\ln(\delta+1)}{\delta+1}$

Theorem

There exists a dominating set of size at most $n\frac{1+\ln(\delta+1)}{\delta+1}$

Example 3: 2-coloring of k-uniform Hypergraphs

- $G = (V, E)$ a k-uniform hypergraph.
- Intuition: if $|E|$ is relatively small, G is 2-colorable
- We've shown: $|E| \le 2^{k-1}$ is sufficient, but the bound is too small

Why is the bound too small?

Random coloring disregards the structure of the graph.
Need some modification of the random coloring to improve the bound.

A Randomized Algorithm

1. Order V randomly. For $v \in V$, flip 2 coins:
   - Prob$[C_1(v) = \text{HEAD}] = 1/2$;
   - Prob$[C_2(v) = \text{HEAD}] = p$
2. Color v red if $C_1(v) = \text{HEAD}$, blue otherwise
3. $D = \{v \mid v \text{ lies in some monochromatic } e \in E\}$
4. For each $v \in D$ in the random ordering
   - **If** v is still in some monochromatic e in the first coloring and no vertex in e has changed its color, **then** change v's color if $C_2(v) = \text{HEAD}$
   - **Else** do nothing!

Analysis

$$
\begin{aligned}
\text{Prob[Coloring is bad]} &\leq \sum_{e \in E} \text{Prob}[e \text{ is monochromatic}] \\
&= 2 \sum_{e \in E} \text{Prob}[e \text{ is red}] \\
&\leq 2 \sum_{e \in E} \Bigg(\text{Prob}[\underbrace{e \text{ was red and remains red}}_{A_e}] \\
&\quad + \text{Prob}[\underbrace{e \text{ wasn't red and turns red}}_{C_e}] \Bigg)
\end{aligned}
$$

$$
\text{Prob}[A_e] = \frac{1}{2^k}(1-p)^k.
$$

The Event C_e

Let v be the last vertex of e to turn blue $\rightarrow$ red

- $v \in f \in E$ and f was blue (in 1st coloring) when v is considered
- $e \cap f = \{v\}$

For any $e \neq f$ with $|e \cap f| = \{v\}$, let B_{ef} be the event that

- f was blue in first coloring, e is red in the final coloring
- v is the last of e to change color
- when v changes color, f is still blue

$$\text{Prob}[C_e] \leq \sum_{f:|f\cap e|=1} \text{Prob}[B_{ef}]$$

The Event B_{ef}

- The random ordering of V induces a random ordering σ of $e \cup f$
- i_σ = number of vertices in e coming before v in σ
- j_σ = number of vertices in f coming before v in σ

$$\text{Prob}\left[B_{ef} \mid \sigma\right] = \frac{1}{2^k} p \frac{1}{2^{n-1-i_\sigma}} (1-p)^{j_\sigma} \left(\frac{1+p}{2}\right)^{i_\sigma}$$

$$\begin{aligned}
\text{Prob}\left[B_{ef}\right] &= \sum_\sigma \text{Prob}\left[B_{ef} \mid \sigma\right] \text{Prob}[\sigma] \\
&= \frac{p}{2^{2k-1}} \mathsf{E}_\sigma\left[(1-p)^{i_\sigma}(1+p)^{j_\sigma}\right] \\
&\leq \frac{p}{2^{2k-1}}
\end{aligned}$$

Putting it All Together

Let $m = |E|$ and $x = m/2^{k-1}$

$$\begin{aligned}
\text{Prob}[\text{Coloring is bad}] &\leq 2\sum_e (\text{Prob}[A_e] + \text{Prob}[C_e]) \\
&< 2m\frac{1}{2^k}(1-p)^k + 2m^2\frac{p}{2^{2k-1}} \\
&= x(1-p)^k + x^2 p \\
&\leq 1
\end{aligned}$$

as long as

$$m = \Omega\left(2^k\sqrt{\frac{k}{\ln k}}\right)$$

Outline

Second Moment Method: Main Idea

Use Chebyshev's Inequality.

Example 1: Distinct Subset Sums

- A set $A = \{a_1, \cdots, a_k\}$ of positive integers has distinct subset sums if the sums of all subsets of A are distinct

Example 1: Distinct Subset Sums

- A set $A = \{a_1, \cdots, a_k\}$ of positive integers has distinct subset sums if the sums of all subsets of A are distinct
- $f(n) =$ maximum k for which there's a k-subset of $[n]$ having distinct subset sums

Example 1: Distinct Subset Sums

- A set $A = \{a_1, \cdots, a_k\}$ of positive integers has distinct subset sums if the sums of all subsets of A are distinct
- $f(n) =$ maximum k for which there's a k-subset of $[n]$ having distinct subset sums
- Example: $A = \{2^i \mid 0 \leq i \leq \lg n\}$

$$f(n) \geq \lfloor \lg n \rfloor + 1$$

Example 1: Distinct Subset Sums

- A set $A = \{a_1, \cdots, a_k\}$ of positive integers has distinct subset sums if the sums of all subsets of A are distinct
- $f(n)$ = maximum k for which there's a k-subset of $[n]$ having distinct subset sums
- Example: $A = \{2^i \mid 0 \leq i \leq \lg n\}$

$$f(n) \geq \lfloor \lg n \rfloor + 1$$

- Open Problem: (Erdős offered 500usd)

$$f(n) \leq \log_2 n + c?$$

Example 1: Distinct Subset Sums

- A set $A = \{a_1, \cdots, a_k\}$ of positive integers has distinct subset sums if the sums of all subsets of A are distinct
- $f(n) =$ maximum k for which there's a k-subset of $[n]$ having distinct subset sums
- Example: $A = \{2^i \mid 0 \leq i \leq \lg n\}$

$$f(n) \geq \lfloor \lg n \rfloor + 1$$

- Open Problem: (Erdős offered 500usd)

$$f(n) \leq \log_2 n + c?$$

- Simple information bound:

$$2^k \leq nk \;\Rightarrow\; k < \lg n + \lg\lg n + O(1).$$

A Bound for $f(n)$ Using Second Moment Method

Line of thought

- Fix n and k-subset $A = \{a_1, \cdots, a_k\}$ with distinct subset sums
- X = sum of random subset of A, $\mu = \mathsf{E}[X], \sigma^2 = \mathsf{Var}[X]$
- For any integer i,

$$\mathsf{Prob}[X = i] \in \left\{0, \frac{1}{2^k}\right\}$$

A Bound for $f(n)$ Using Second Moment Method

Line of thought

- Fix n and k-subset $A = \{a_1, \cdots, a_k\}$ with distinct subset sums
- X = sum of random subset of A, $\mu = \mathsf{E}[X], \sigma^2 = \mathsf{Var}[X]$
- For any integer i,

$$\mathsf{Prob}[X = i] \in \left\{0, \frac{1}{2^k}\right\}$$

- By Chebyshev, for any $\alpha > 1$

$$\mathsf{Prob}[|X - \mu| \geq \alpha\sigma] \leq \frac{1}{\alpha^2} \Rightarrow \mathsf{Prob}[|X - \mu| < \alpha\sigma] \geq 1 - \frac{1}{\alpha^2}$$

- There are at most $2\alpha\sigma + 1$ integers within $\alpha\sigma$ of μ; hence,

$$1 - \frac{1}{\alpha^2} \leq \frac{1}{2^k}(2\alpha\sigma + 1)$$

- σ is a function of n and k

More Specific Analysis

$$\sigma^2 = \frac{a_1^2 + \cdots + a_k^2}{4} \leq \frac{n^2 k}{4} \;\Rightarrow\; \sigma \leq n\sqrt{k}/2$$

There are at most $(\alpha n\sqrt{k} + 1)$ within $\alpha\sigma$ of μ

$$1 - \frac{1}{\alpha^2} \leq \frac{1}{2^k}(\alpha n\sqrt{k} + 1)$$

Equivalently,

$$n \geq \frac{2^k\left(1 - \frac{1}{\alpha^2}\right) - 1}{\alpha\sqrt{k}}$$

Recall $\alpha > 1$, we get

$$k \leq \lg n + \frac{1}{2}\lg\lg n + O(1).$$

Example 2: $\mathcal{G}(n,p)$ Model and $\omega(G) \geq 4$ Property

$\mathcal{G}(n,p)$

Space of random graphs with n vertices, each edge (u,v) is included with probability p

Also called the Erdős-Rényi Model.

Question

Does a "typical" $G \in \mathcal{G}(n,p)$ satisfy a given property?

- Is G connected?
- Does G have a 4-clique?
- Does G have a Hamiltonian cycle?

Threshold Function

- As p goes from 0 to 1, $G \in \mathcal{G}(n,p)$ goes from "typically empty" to "typically full"
- Some property may become more likely or less likely

Threshold Function

- As p goes from 0 to 1, $G \in \mathcal{G}(n,p)$ goes from "typically empty" to "typically full"
- Some property may become more likely or less likely
- The property *having a* 4*-clique* will be come more likely

Threshold Function

$f(n)$ is a threshold function for property P if

- When $p \ll f(n)$ almost all $G \in \mathcal{G}(n,p)$ do not have P
- When $p \gg f(n)$ almost all $G \in \mathcal{G}(n,p)$ do have P

- It is not clear if any property has threshold function

The $\omega(G) \geq 4$ Property

- Pick $G \in \mathcal{G}(n, p)$ at random
- $S \in \binom{V}{4}$, X_S indicates if S is a clique
- $X = \sum_S X_S$ is the number of 4-clique
- $\omega(G) \geq 4$ iff $X > 0$

The $\omega(G) \geq 4$ Property

- Pick $G \in \mathcal{G}(n, p)$ at random
- $S \in \binom{V}{4}$, X_S indicates if S is a clique
- $X = \sum_S X_S$ is the number of 4-clique
- $\omega(G) \geq 4$ iff $X > 0$

Natural line of thought:

$$\mathsf{E}[X] = \sum_S \mathsf{E}[X_S] = \binom{n}{4} p^6 \approx \frac{n^4 p^6}{24}$$

The $\omega(G) \geq 4$ Property

- Pick $G \in \mathcal{G}(n,p)$ at random
- $S \in \binom{V}{4}$, X_S indicates if S is a clique
- $X = \sum_S X_S$ is the number of 4-clique
- $\omega(G) \geq 4$ iff $X > 0$

Natural line of thought:

$$\mathsf{E}[X] = \sum_S \mathsf{E}[X_S] = \binom{n}{4} p^6 \approx \frac{n^4 p^6}{24}$$

- When $p = o\left(n^{-2/3}\right)$, we have $\mathsf{E}[X] = o(1)$; thus,

$$\text{Prob}[X > 0] \leq \mathsf{E}[X] = o(1)$$

The $\omega(G) \geq 4$ Property

More precisely

$$p = o\left(n^{-2/3}\right) \Longrightarrow \lim_{n\to\infty} \text{Prob}[X > 0] = 0$$

In English

When $p = o\left(n^{-2/3}\right)$ and n sufficiently large, almost all graphs from $\mathcal{G}(n,p)$ do not have $\omega(G) \geq 4$

The $\omega(G) \geq 4$ Property

More precisely

$$p = o\left(n^{-2/3}\right) \Longrightarrow \lim_{n\to\infty} \text{Prob}[X > 0] = 0$$

In English

When $p = o\left(n^{-2/3}\right)$ and n sufficiently large, almost all graphs from $\mathcal{G}(n,p)$ do not have $\omega(G) \geq 4$

- What about when $p = \omega\left(n^{-2/3}\right)$?

The $\omega(G) \geq 4$ Property

More precisely

$$p = o\left(n^{-2/3}\right) \Longrightarrow \lim_{n\to\infty} \text{Prob}[X > 0] = 0$$

In English

When $p = o\left(n^{-2/3}\right)$ and n sufficiently large, almost all graphs from $\mathcal{G}(n,p)$ do not have $\omega(G) \geq 4$

- What about when $p = \omega\left(n^{-2/3}\right)$?
- We know $\lim_{n\to\infty} \mathsf{E}[X] = \infty$

The $\omega(G) \geq 4$ Property

More precisely

$$p = o\left(n^{-2/3}\right) \Longrightarrow \lim_{n\to\infty} \text{Prob}[X > 0] = 0$$

In English

When $p = o\left(n^{-2/3}\right)$ and n sufficiently large, almost all graphs from $\mathcal{G}(n,p)$ do not have $\omega(G) \geq 4$

- What about when $p = \omega\left(n^{-2/3}\right)$?
- We know $\lim_{n\to\infty} \text{E}[X] = \infty$
- But it's not necessarily the case that $\text{Prob}[X > 0] \to 1$
- Equivalently, it's not necessarily the case that $\text{Prob}[X = 0] \to 0$
- Need more information about X

Here Comes Chebyshev

Let $\mu = \mathsf{E}[X]$, $\sigma^2 = \mathsf{Var}[X]$

$$\begin{aligned}
\mathsf{Prob}[X = 0] &= \mathsf{Prob}[X - \mu = -\mu] \\
&\leq \mathsf{Prob}\left[\{X - \mu \leq -\mu\} \cup \{X - \mu \geq \mu\}\right] \\
&= \mathsf{Prob}\left[|X - \mu| \geq \mu\right] \\
&\leq \frac{\sigma^2}{\mu^2}
\end{aligned}$$

Here Comes Chebyshev

Let $\mu = \mathsf{E}[X]$, $\sigma^2 = \mathsf{Var}[X]$

$$
\begin{aligned}
\mathsf{Prob}[X = 0] &= \mathsf{Prob}[X - \mu = -\mu] \\
&\leq \mathsf{Prob}\left[\{X - \mu \leq -\mu\} \cup \{X - \mu \geq \mu\}\right] \\
&= \mathsf{Prob}\left[|X - \mu| \geq \mu\right] \\
&\leq \frac{\sigma^2}{\mu^2}
\end{aligned}
$$

Thus, if $\sigma^2 = o\left(\mu^2\right)$ then $\mathsf{Prob}[X = 0] \to 0$ as desired!

Lemma

For any random variable X

$$\mathsf{Prob}[X = 0] \leq \frac{\mathsf{Var}[X]}{(\mathsf{E}[X])^2}$$

PTCF: Bounding the Variance

Suppose $X = \sum_{i=1}^n X_i$

$$\mathsf{Var}\left[X\right] = \sum_{i=1}^{n} \mathsf{Var}\left[X_i\right] + \sum_{i \neq j} \mathsf{Cov}\left[X_i, X_j\right]$$

If X_i is an indicator for event A_i and Prob$[X_i = 1] = p_i$, then

$$\mathsf{Var}\left[X_i\right] = p_i(1 - p_i) \leq p_i = \mathsf{E}[X_i]$$

If A_i and A_j are independent, then

$$\mathsf{Cov}\left[X_i, X_j\right] = \mathsf{E}[X_i X_j] - \mathsf{E}[X_i]\mathsf{E}[X_j] = 0$$

If A_i and A_j are not independent (denoted by $i \sim j$)

$$\mathsf{Cov}\left[X_i, X_j\right] \leq \mathsf{E}[X_i X_j] = \mathsf{Prob}[A_i \cap A_j]$$

PTCF: Bounding the Variance

Theorem

Suppose

$$X = \sum_{i=1}^{n} X_i$$

where X_i is an indicator for event A_i. Then,

$$\mathsf{Var}[X] \leq \mathsf{E}[X] + \sum_i \mathsf{Prob}[A_i] \underbrace{\sum_{j:j\sim i} \mathsf{Prob}[A_j \mid A_i]}_{\Delta_i}$$

PTCF: Bounding the Variance

Theorem

Suppose

$$X = \sum_{i=1}^{n} X_i$$

where X_i is an indicator for event A_i. Then,

$$\mathsf{Var}\left[X\right] \leq \mathsf{E}[X] + \sum_i \mathsf{Prob}[A_i] \underbrace{\sum_{j:j\sim i} \mathsf{Prob}[A_j \mid A_i]}_{\Delta_i}$$

Corollary

If $\Delta_i \leq \Delta$ for all i, then

$$\mathsf{Var}\left[X\right] \leq \mathsf{E}[X](1+\Delta)$$

Back to the $\omega(G) \geq 4$ Property

$$
\begin{aligned}
\Delta_S &= \sum_{T \sim S} \text{Prob}[A_T \mid A_S] \\
&= \sum_{|T \cap S| = 2} \text{Prob}[A_T \mid A_S] + \sum_{|T \cap S| = 3} \text{Prob}[A_T \mid A_S] \\
&= \binom{n-4}{2}\binom{4}{2} p^5 + (n-4)p^3 \;\; = \Delta
\end{aligned}
$$

Back to the $\omega(G) \geq 4$ Property

$$
\begin{aligned}
\Delta_S &= \sum_{T \sim S} \text{Prob}[A_T \mid A_S] \\
&= \sum_{|T \cap S| = 2} \text{Prob}[A_T \mid A_S] + \sum_{|T \cap S| = 3} \text{Prob}[A_T \mid A_S] \\
&= \binom{n-4}{2}\binom{4}{2} p^5 + (n-4)p^3 \;\; = \Delta
\end{aligned}
$$

So,

$$\sigma^2 \leq \mu(1 + \Delta)$$

- Recall: we wanted $\sigma^2/\mu^2 = o(1)$ – OK as long as $\Delta = o(\mu)$
- Yes! When $p = \omega\left(n^{-2/3}\right)$, certainly

$$\Delta = \binom{n-4}{2}\binom{4}{2} p^5 + (n-4)p^3 = o\left(n^4 p^6\right)$$

The $\omega(G) \geq 4$ Property: Conclusion

Theorem

$f(n) = n^{-2/3}$ is a threshold function for the $\omega(G) \geq 4$ property

With essentially the same proof, we can show the following.

Let H be a graph with v vertices and e edges. Define the *density* $\rho(H) = e/v$. Call H *balanced* if every subgraph H' has $\rho(H') \leq \rho(H)$

Theorem

The property "$G \in \mathcal{G}(n, p)$ contains a copy of H" has threshold function $f(n) = n^{-v/e}$.

What Happens when $p \approx$ Threshold?

Theorem

Suppose $p = cp^{-2/3}$*, then* X *is approximately Poisson*$(c^6/24)$
In particular, $\text{Prob}[X = 0] \to 1 - e^{-c^6/24}$

Outline

Lovasz Local Lemma: Main Idea

- Recall the union bound technique:
  - want to prove Prob$[A] > 0$
  - $\bar{A} \Rightarrow$ (or $\Leftrightarrow$) some bad events $B_1 \cup \cdots \cup B_n$
  - done as long as Prob$[B_1 \cup \cdots \cup B_n] < 1$
- Could also have tried to show

$$\text{Prob}[\bar{B}_1 \cap \cdots \cap \bar{B}_n] > 0$$

- Would be much simpler if the B_i were mutually independent, because

$$\text{Prob}[\bar{B}_1 \cap \cdots \cap \bar{B}_n] = \prod_{i=1}^{n} \text{Prob}[\bar{B}_i] > 0$$

Main Idea

Lovasz Local Lemma is a sort of generalization of this idea when the "bad" events are not mutually independent

PTCF: Mutual Independence

Definition (Recall)

A set $B_1, \dots, B_n$ of events are said to be or mutually independent (or simply independent) if and only if, for any subset $S \subseteq [n]$,

$$\text{Prob}\left[\bigcap_{i \in S} B_i\right] = \prod_{i \in S} \text{Prob}[B_i]$$

Definition (New)

An event B is mutually independent of events $B_1, \cdots, B_k$ if, for any subset $S \subseteq [k]$,

$$\text{Prob}\left[B \mid \bigcap_{i \in S} B_i\right] = \text{Prob}[B]$$

Question: can you find B, B_1, B_2, B_3 such that B is mutually independent of B_1 and B_2 but not from all three?

PTCF: Dependency Graph

Definition

Given a set of events $B_1, \cdots, B_n$, a directed graph $D = ([n], E)$ is called a dependency digraph for the events if every event B_i is independent of all events B_j for which $(i, j) \notin E$.

- What's a dependency digraph of a set of mutually independence events?
- Dependency digraph is **not unique**!

The Local Lemma

Lemma (General Case)

Let $B_1, \cdots, B_n$ *be events in some probability space. Suppose* $D = ([n], E)$ *is a dependency digraph of these events, and suppose there are real numbers* $x_1, \cdots, x_n$ *such that*

- $0 \leq x_i < 1$
- $\text{Prob}[B_i] \leq x_i \prod_{(i,j) \in E} (1 - x_j)$ *for all* $i \in [n]$

Then,

$$\text{Prob}\left[\bigcap_{i=1}^{n} \bar{B}_i\right] \geq \prod_{i=1}^{n} (1 - x_i)$$

The Local Lemma

Lemma (Symmetric Case)

Let $B_1, \cdots, B_n$ be events in some probability space. Suppose $D = ([n], E)$ is a dependency digraph of these events with maximum out-degree at most Δ. If, for all i,

$$\text{Prob}[B_i] \leq p \leq \frac{1}{e(\Delta + 1)}$$

then

$$\text{Prob}\left[\bigcap_{i=1}^{n} \bar{B}_i\right] > 0.$$

The conclusion also holds if

$$\text{Prob}[B_i] \leq p \leq \frac{1}{4\Delta}$$

Example 1: Hypergraph Coloring

- $G = (V, E)$ a hypergraph, each edge has $\geq k$ vertices
- Each edge f intersects at most Δ other edges
- Color each vertex randomly with red or blue
- B_f: event that f is monochromatic

$$\text{Prob}[B_f] = \frac{2}{2^{|f|}} \leq \frac{1}{2^{k-1}}$$

- There's a dependency digraph for the B_f with max out-degree $\leq \Delta$

Theorem

G is 2-colorable if

$$\frac{1}{2^{k-1}} \leq \frac{1}{e(\Delta + 1)}$$

Example 2: k-SAT

Theorem

In a k-CNF formula φ, if no variable appears in more than $2^{k-2}/k$ clauses, then φ is satisfiable.

Example 3: Edge-Disjoint Paths

- $\mathcal{N}$ a directed graph with n inputs and n outputs
- From input a_i to output b_i there is a set P_i of m paths
- In switching networks, we often want to find (or want to know if there exists) a set of edge-disjoint $(a_i \to b_i)$-paths

Theorem

Suppose $8nk \leq m$ and each path in P_i share an edge with at most k paths in any P_j, $j \neq i$. Then, there exists a set of edge-disjoint $(a_i \to b_i)$-paths.