Probability space

Definition (Probability space): *Probability space* is a triple (Ω, Σ, P), where Ω is a set, $\Sigma \subseteq 2^\Omega$ is a σ-algebra ($\emptyset \in \Sigma$; if $A \in \Sigma \Rightarrow \Omega \setminus A \in \Sigma$, if $A_1, A_2 \ldots \in \Sigma$, then $\bigcup_{i=1}^\infty A_i \in \Sigma$), and $P : M \to [0,1]$ is a probability measure ($P[\emptyset] = 0, P[\Omega] = 1$, if $A_1, A_2 \ldots$ are pairwise disjoint elements of Σ then $P[\bigcup_{i=1}^\infty A_i] = \sum_{i=1}^\infty P[A_i]$). Elements of Σ are called *events*, elements of Ω are *elementary events*, $P[A]$ is the *probability* of the event A.

Examples

Finite probability space: (Ω – finite, $\Sigma = 2^\Omega$, then P is uniquely determined by a function $\Sigma \to [0,1]$, s.t. $\sum_{\omega \in \Omega} p(\omega) = 1$, then $P[A] = \sum_{\omega \in A} p(A)$). More specific version, uniformly determined: $p(\omega) = \frac{1}{|\Omega|}$

Random Graphs: The probability space $G(n,p)$ of random graphs on n vertices with edge probability $p \in [0,1]$ is given by Ω – graphs on fixed n number and Σ – 2^Ω. For G on n vertices $p(G) = p^n(1-p)^{\binom{n}{k-n}}$ where n is the number of edges of G

Random point in a square: $\Omega = [0,1]^2$, Σ – lebesgue measurable subset of $[0,1]^2$ For $A \in \Sigma$: $P[A] := \lambda(A)$ – lebesgue measure = generalization of an area

Lemma (Union bound) Let (Ω, Σ, P) be a prob. space and let $A_1, \ldots, A_n \in \Sigma$ then $P\left[\bigcup_{i=1}^n A_i\right] \leq \sum_{i=1}^n P[A_i]$

Proof Let $B_i = A_i \setminus (A_1 \cup \ldots \cup A_{i-1})$. Then $B_i \subseteq A_i, \bigcup_i^n = 1B_i = \bigcup_{i=1}^n A_i$, B_i are pairwise disjoint. $P[\bigcup_{i=1}^n A_i] = P[\bigcup_{i=1}^n B_i] = \sum_{i=1}^n P[B_i] \leq \sum_{i=1}^n P[A_i]$ (since $B \subseteq A \Rightarrow P[B] \leq P[A]$) $P[A] = P[(A \setminus B) \cup B] = P[A \setminus B] + P[B] \geq P[B]$

Definition (independent events):

Let (Ω, Σ, P) be a prob. space then two events $A, B \in \Sigma$ are *independent* if $P[A, B] = P[A]P[B]$

If $A_1, \ldots, A_n \in \Sigma$, then they are *independent* if for every $I \subseteq [n] : P[\bigcap_{i \in I} A_i] = \prod_{i \in I} P[A_i]$

Definition (conditional probability): let (Ω, Σ, P) be an prob. space and $B \in \Sigma$ s.t. $P[B] > 0$ then the *conditional probability* of A, given that B occured is defined $P[A|B] = \frac{P[A \cup B]}{P[B]}$

Remark $P[A|B] = P[A]$ if A, B are independent.

Estimates

Fractional:

- $\left(\frac{n}{2}\right)^{\frac{n}{2}} \leq n! \leq n^n$
- $\left(\frac{n}{e}\right)^n \leq n! \leq en\left(\frac{n}{e}\right)^n$
- stirling formula n! is aprox, lim ... = 0

Binomial coefficients:

- $\left(\frac{n}{k}\right)^k \leq \frac{n(n-1)\ldots(n-k+1)}{k(k-1)\ldots 1} = \binom{n}{k} \leq \frac{n^k}{k!} \leq n^k$
- $\binom{n}{k} \leq \left(\frac{en}{k}\right)^k$
- $\frac{2^{2m}}{2\sqrt{m}} \leq \binom{2m}{m} \leq \frac{2^{2m}}{\sqrt{2m}}$

Inequality:

- $1 + x \leq e^x$
- $(1-p)^n \leq e^{-pn}$

Definition (expected value) For finite prob. space (Ω, Σ, P) a *random variable* is a function $X : \Omega \to \mathbb{R}$, *expected value* $\mathrm{E}[X]$ of a random variable is a value $\sum_{\omega \in \Omega} p(\omega)X(\omega)$, where $p(\omega) = P[\{\omega\}]$

Remark *Linearity of expected value*: $\mathrm{E}[\alpha X + \beta Y] = \alpha\mathrm{E}[X] + \beta\mathrm{E}[Y]$

Application k-satisfiability problem

Definition (Formula in conjunctive normail form – CNF) By example

Examples

$(x \vee y \vee z) \wedge (x \vee \neg y) \wedge (\neg x \vee \neg y \vee \neg z \vee t)$. Example of satisfaction $x = \mathrm{T}$, $y = \mathrm{F}$, $z = \mathrm{F}$, $t = \mathrm{F}$.

$(x \vee y) \wedge (x \vee \neg y) \wedge (\neg x \wedge y) \wedge (\neg x \vee \neg y)$. Not satisfiable.

Proposition: Let Φ be a CNF-formula s.t. every clause contains k distinct literals and with less then 2^k clauses then Φ is satisfiable.

Proof: For each variable we assign it true randomly with probability 1/2, independently of the other variables. $\Phi = C_1 \wedge C_2 \wedge \ldots \wedge C_t$, where C_i are clauses, $t < 2^k$. $P\left[C_i \mathrm{isnotsatisfied}\right] \leq \frac{1}{2^k}$ $C_i = (l_1 \vee l_2 \vee \ldots \vee)$, where l_j are literals. If $\{x, \neg x\} \subseteq C_i$, then $P = 0$, otherwise $P = \frac{1}{2^k}$. By union bound: $P[\text{some}\, C_i \,\text{is not satisfied}] \leq \frac{t}{2^k} < 1 \Rightarrow$ There exists satisfying assignment.

Maximum intersecting families

Definition (intersecting) Let X be set of n elements, $k \leq n$ we say that family $\mathcal{F} \subseteq \binom{X}{k}$ is *intersecting*, if for every $F_1, F_2 \in \mathcal{F}$ we have $F_1 \cap F_2 \neq \emptyset$.

Whenever $k > \frac{n}{2}$ max. size of int. family is $\binom{n}{k}$. If $n \geq 2k$ we can get $\binom{n-1}{k-1}$.

Theorem (Erdős-Ko-Rado) Let X be an n-element set, k be s.t. $n \geq 2k$. Then the size of any intersecting family of sets of size k is at most $\binom{n-1}{k-1}$.

Lemma Let us consider $X = \{0, 1, \ldots n-1\}$ with addition modulo n and let $A_s := \{s, s+1, \ldots s+k-1\}$ for $s \in X$ and assume $n \geq 2k$. Then the maximum intersecting family of sets A_s has size at most k.

Proof Let us assume that some A_i belongs to maximum intersecting family. Only the sets $A_{i-k+1}, A_{i-k+2}, \ldots, A_{i-1}, A_i, A_{i+1}, \ldots A_{i+k-2}, A_{i+k-1}$ may belong to the family. Furthermore only one set of each pair A_x, A_{x+k} may belong to the family $\Rightarrow$ altogether at most k sets.

Proof of Erdős-Ko-Rado WLoG $X = \{0, 1, \ldots, n-1\}$. For $s \in \{0, 1, \ldots, n-1\}, \sigma \in S_n$ (permutation) we define: $A_{s,\sigma} := \{\sigma(s), \sigma(s+1), \ldots, \sigma(s+k-1)\}$. Let $\mathcal{F}$ be the intersecting family. We want to estimate $P\left[A_{s,\sigma} \in \mathcal{F}\right]$ if s and σ are chosen uniformly at random, independently.

On one hand: $P\left[A_{s,\sigma} \in \mathcal{F}\right] = \frac{|\mathcal{F}|}{\binom{n}{k}}$ (first choose s, then σ, uniformly chosen subset).

On the other hand: $P\left[A_{s,\sigma} \in \mathcal{F}\right] \leq \frac{k}{n}$ (first choose σ, then s; by previous lemma).

Altogether $\frac{|\mathcal{F}|}{\binom{n}{k}} = P\left[A_{s,\sigma} \in \mathcal{F}\right] \leq \frac{k}{n} \rightarrow |\mathcal{F}| \leq \frac{k}{n}\binom{n}{k} = \binom{n-1}{k-1}$.

Expected values

Definition (random variable) let (Ω, Σ, P) be a probability space. A *random variable* is any P-measurable function $X : \Omega \rightarrow \mathbb{R}$. In finite case any function is P-measurable.

Definition (expected value): The *expected value* of random variable X is the value $E[X] := \int_\Omega X dP$. In finite case $E[X] = \sum_{\omega \in \Omega} p(\omega) X(\omega)$ where $p(\omega) = P(\{\omega\})$ Equivalently $E[X] = \sum_{a \in X(\Omega)} a P[X = a]$.

Definition (independence of random variables): Two random variables X, Y are *independent* if $\forall A, B \in \Sigma : P[(X \in A) \wedge (Y \in B)] = P[X \in A] P[Y \in B]$

Lemma For probability space (Ω, Σ, P) and random variables X, Y and $\alpha, \beta \in \mathbb{R}$:

(i) $E[\alpha X + \beta Y] = \alpha E[X] + \beta E[Y]$
(ii) $E[XY] = E[X]E[Y]$ if X and Y are independent.

Proof (finite case)

(i)

$$E[\alpha X+\beta Y]=\sum_{\omega\in\Omega}p(\omega)(\alpha X+\beta Y)(\omega)=\sum_{\omega\in\Omega}p(\omega)\alpha X(\omega)+p(\omega)\beta Y(\omega)=\alpha E[X]+\beta E[Y]$$

(ii)

$$E[XY]=\sum_{c\in XY(\Omega)}cP[XY=c]=\sum_{\substack{a\in X(\Omega)\\ b\in Y(\Omega)}}abP[(X=a)\wedge(Y=b)]\overset{\text{ind.}}{=}$$

$$\overset{\text{ind.}}{=}\sum_{\substack{a\in X(\Omega)\\ b\in Y(\Omega)}}abP[X=a]P[Y=b]=\left(\sum_{a\in X(\Omega)}aP[X=a]\right)\left(\sum_{b\in Y(\Omega)}bP[Y=b]\right)=E[X]E[Y]$$

Definition (indicator): For probability space (Ω,Σ,P) and an event $A\in\Sigma$, the *indicator of A* is the random variable $I_A:\Omega\to\mathbb{R}$ defined as: $I_A(\omega)=0$ if $\omega\notin A$, 1 otherwise.

Lemma $E[I_A]=P[A]$

Proof (finite case) $E[I_A]=\sum_{\omega\in\Omega}p(\omega)I_A(\omega)=\sum_{\omega\in A}p(\omega)=P[A]$

Proof (general case) $E[I_A]=\int_{\omega\in\Omega}I_A(\omega)dP(\omega)=\int_{\omega\in A}dP=P[A]$

Application The expected value of fixed points in a random permutation. For permutation σ of $\{1,2,\ldots,n\}$, a fixed point is $i\in\{1,2,\ldots,n\}$ s.t. $\sigma(i)=i$.

Proposition: Expected number of fixed points in a permutation on $\{1,\ldots,n\}$ is 1.

Proof For $i\in\{1,\ldots,n\}$ $A_i\ldots i$ is a fixed point. $P[A_i]=E[I_{A_i}]=\frac{1}{n}$. Expected number of fixed points $E[\sum_i I_{A_i}]=n\cdot\frac{1}{n}=1$.

Definition (Tournament) A *tournament* is a complete directed graph. (Interpretation is that everybody plays with everybody and the direction means the winner.)

Definition (Hamiltonian paht over directed graphs) Path over all vertices that follows direction of edges.

Remark Each tournament has at least one Hamiltonian path.

Theorem (Szele) For every integer n there is a tournament with at least $\frac{n!}{2^{n-1}}$ Hamiltonian paths.

Proof Set $\{1,2,\ldots,n\}$ to be the set of the vertices of the tournament. Direct each edge (independently of others) with probability of $\frac{1}{2}$ in one direction and $\frac{1}{2}$ in the second one. Consider a permutation $\sigma\in S_n$ and let X_σ be a random variable indicating the event that $\sigma(1),\sigma(2),\ldots,\sigma(n)$ forms a Hamiltonian path in this order. $E[X_\sigma]=\frac{1}{2^{n-1}}$ (there are $(n-1)$ edges in the path, all of them need to be in correct direction). Let X be number of Hamiltonian paths, then $E[X]=\sum_{\sigma\in S_n}E[X_\sigma]=\frac{n!}{2^{n-1}}$, thus there exists an tournament with such number of Hamiltonian paths.

Application (MaxSAT) Let Φ be a formula in conjunctive normal form with m clauses and k distinct literals in each clause. Find assignment tat satisfies as many clauses as possible.

Proposition There is an assignment for which at least $\frac{2^k-1}{2^k}m$ are satisfied.

Proof Choose a random assignment: for clause C let A_C be an event that C is satisfied in the assignment. $E[I_{A_C}]=P[A_C]\geq\frac{2^k-1}{2^k}$. $E[\text{number of satisfied clauses}]=\sum_{C\text{ is clause}}E[I_{A_C}]\geq m\frac{2^k-1}{2_k}$.

Application (MaxCut) We are given a graph $G=(V,E)$. The task is to find splitting $V=A\dot{\cup}B$ so that the number of edges on the cut between A and B is as large as possible.

Proposition For every G we can get cut of size $\frac{m}{2}$ where $m=|E|$.

Proof For each vertex v, it will be in A with probability $\frac{1}{2}$ and in B with probability $\frac{1}{2}$ independently of other vertices. For $e\in E$ let A_e : e belongs to the AB-cut. $P[A_e]=\frac{1}{2}$. $E[\text{edges in cut}]=\sum E[I_{A_e}]=\frac{m}{2}$.

Derandomization of MaxCut

1. Choose an edge e of E, put one vertex of e into A and one into B.
2. Pick remaining vertices one by one, add them either into A or B, so that at least $\frac{1}{2}$ of the edges coming to $A \cup B$ will go into the cut.

In each step we put at least as many edges into the cut as outside. Therefore we have at least $\frac{m}{2}$ edges in final cut.

Derandomization of MaxSAT (sketch) Let us consider formula $(x \vee y \vee z) \wedge (x \vee \neg y \vee \neg z) \wedge (\neg x \vee z \vee t)$. Pick variables one by one. Fix each variable to "better" value w.r.t. computed expected number of satisfied clauses in random assignment of remaining variables.

- x to true: expected value is $1 + 1 + \frac{3}{4}$
- x to false: expected value is $\frac{3}{4} + \frac{3}{4} + 1$

"better" approach is to choose $x =$ true. This works because $E[I_A] = \frac{1}{2}E[I_{A|B}] + \frac{1}{2}E[I_{A|B^C}]$ if $P[B] = \frac{1}{2}$.

Proposition (Balancing vectors) Let $v_i, \ldots, v_n \in \mathbb{R}^n$ be such that $||v_i|| = 1$ for every $i \in \{1, 2, \ldots, n\}$. Then there are $\varepsilon \in \{-1, 1\}$ such that $||\varepsilon_1 v_1 + \varepsilon_2 v_2 + \ldots + \varepsilon_n v_n|| \leq \sqrt{n}$. Also there are $\varepsilon \in \{-1, 1\}$ such that $||\varepsilon_1 v_1 + \varepsilon_2 v_2 + \ldots + \varepsilon_n v_n|| \geq \sqrt{n}$. Furthermore the these bounds are tight (can be proven via diagonal and its norm).

Proof Pick each ε_i to be equal to -1 with probability $\frac{1}{2}$ and 1 with probability $\frac{1}{2}$ independently of others. Let $X = ||\varepsilon_1 v_i + \ldots + \varepsilon_n v_n||^2$. $E[X] = E[\sum_{i,j=1}^{n} \varepsilon_i \varepsilon_j \langle v_i, v_j \rangle] \overset{\text{lin.}}{=} \sum_{i,j=1}^{n} E[\varepsilon_i \varepsilon_j] \langle v_i, v_j \rangle$. Since $E[\varepsilon_i \varepsilon_i] = 1$ and $E[\varepsilon_i \varepsilon_j] = 0$ for $i \neq j$ it holds: $E[X] = \sum_{i=1}^{n} \langle v_i, v_i \rangle = \sum_{i=1}^{n} ||v_i||^2 = n$.

Alterations

Proposition (weak form of Turán's theorem) Let $G = (V, E)$ be a graph with n vertices and m edges and let $d = \frac{2m}{n}$ denotes the average degree. Then $\alpha(G) \geq \frac{n}{2d}$.

Remark Full version on Turán's theorem gives $\alpha(G) \geq \frac{n}{d+1}$

Proof (of weak Turán's theorem) Consider $p \in [0, 1]$. Pick a random subset $S \subseteq V$ s.t. each vertex belongs to S with probability p, independently of others. Consider two random variables $X = |S|$ and $Y = |E(G[S])|$. $E[X] = pn$. $E[Y] = p^2 m$. $E[X - Y] = p(n - pm) = p(n - \frac{dn}{2}) = pn(1 - p\frac{d}{2})$. Choose $p = \frac{1}{d}$, then: $E[X - Y] = \frac{n}{2d}$. Remove the vertex from each edge, then we get independent set of size at least $\frac{n}{2d}$.

Lemma (Markov's inequality) Let X be a nin-negative random variable, let $a > 0$. Then $P[X \geq a] \leq \frac{E[X]}{a}$.

Proof $E[X] \geq aP[X \geq a]$

Definition (proper k-coloring) Let $G = (V, E)$ be a graph. Then *proper k-coloring* of G is a function $c : V \to \{1, 2, \ldots k\}$ such that $c(u) \neq c(v)$ for any $uv \in E$.

Definition (chromatic number) *Chromatic number* of G is the minimum $k \in \mathbb{N}$ s.t. G admits proper k-coloring.

Definition (Girth) A *girth* of G, $g(G)$ is the length of the shortest cycle in G. If G is forest let $g(G) = \infty$.

Theorem (Erdős) For every $k, l > 0$ there is a graph G such that $g(G) > l, \chi(G) > k$.

Proof WLoG $k, \ell \geq 3$. We set $\varepsilon = \frac{1}{2\ell}, p = n^{\varepsilon - 1}$. Consider $G(n, p)$. For $i \in \{3, \ldots, \ell\}$ the cycles of size i on K_n: $\binom{n}{i}\frac{(n-1)!}{2} \leq n^i$. Let X be a random variable of the number of cycles of length at most ℓ.

$$E[X] \leq \sum_{i=3}^{\ell} n^i p^i = \sum_{i=3}^{\ell} n^{i\varepsilon} \leq \ell n^{\frac{1}{2\ell}\ell} = \ell n^{\frac{1}{2}} = o(n)$$

Thus for n large enough: $E[X] < \frac{n}{4}$. By Markov's inequality: $P[X > \frac{n}{2}] < \frac{\frac{n}{4}}{\frac{n}{2}} = \frac{1}{2}$.

Bound for chromatic number by independence number. Let $a = \lceil \frac{3}{p} \log n \rceil + 1$. Then $\frac{3}{p} \log n \leq a - 1 \leq \frac{4}{p} \log n$ (from n large enough). Let α be random variable denoting independence number of G.

$$P\left[\alpha \geq a\right] \leq \binom{n}{a}(1-p)^{\binom{a}{2}} \leq n^a \ell^{-p\binom{a}{2}} = \exp\left(a\left(\log n - p\frac{a-1}{2}\right)\right) \leq \exp\left(a\left(\log n - \frac{p}{2}\frac{3\log n}{p}\right)\right) =$$

$$= \exp\left(a\left(-\frac{1}{2}\log n\right)\right) \overset{n\to\infty}{\to} 0$$

For n large enough $P[\alpha \geq a] < \frac{1}{2}$. By union bound there is G with: n vertices, has at most $\frac{n}{2}$ cycles of length ℓ, $\alpha(G) < a$. Finally let us obtain G' be removing vertex from each cycle of G. Then G' has at least $\frac{n}{2}$ vertices, $g(G') > \ell$, $\alpha(G') < a$, $\chi(G') \geq \frac{\frac{n}{2}}{a-1} \geq \frac{p}{4\log n}\frac{n}{2} = \frac{n^\varepsilon}{8\log n} \to \infty$. For n large enough $\chi(G') > k$ as we wanted.

Theorem (Bayes theorem) Let $A, B_1, B_2, \ldots, B_n \subseteq \Omega$ be events s.t. $B_1, B_2, \ldots, B_n$ are pairwise disjoint cover Ω, $P[B_i] > 0$. Then $P[B_i|A] = \frac{P[A|B_i]P[B_i]}{\sum_{j=1}^n P[A|B_j]P[B_j]}$

Observation: $P[A] = \sum_{j=1}^n \underbrace{P[A|B_j]P[B_j]}_{P[A\cap B_j]}$.

Proof (Bayes theorem) $P[B_i|A] = \frac{P[A\cap B_i]}{P[A]} = \frac{P[A|B_i]P[B_i]}{P[A]}$ we finish by the observation.

Problem (Matrix multiplication testing) Let A, B, C be $n \times n$ matrices. We would like to test whether $AB = C$.

One method is to compute AB – currently in time approximately $O(n^{2.37})$. Our goal is to get test in time close to $O(n^2)$.

Algorithm (Freivalds' algorithm) For parameter $k \in \mathbb{N}$ run in time $O(kn^2)$ will answer correctly with probability at least $1 - 2^k$.

Generate a random $0,1$ vector (generates each entry with probability $\frac{1}{2}$ independently of others) r with n entries. Test whether $A(Br) - Cr = 0$.

If $AB = C$ then $ABr = Cr \to ABr - Cr = 0$ In this case algorithm always answers yes.

If $AB \neq C$, aim is that we can answer no with probability $\frac{1}{2}$. Let $D = AB - C$, then D has a non-zero entry $d_{i,j}$. Let $Dr = v$, then $v_i = \sum_{k=1}^n d_{i,k}r_k = d_{i,j}r_j + y$. Then $P[v_i = 0] = P[v_i = 0|y = 0]P[y = 0] + P[v_i = 0|y \neq 0]P[y \neq 0]$

$$\begin{aligned} P[v_i = 0] &= P[v_i = 0|y = 0]P[y = 0] + P[v_i = 0|y \neq 0]P[y \neq 0] \\ &= \tfrac{1}{2}P[y = 0] + P[v_i = 0|y \neq 0]P[y \neq 0] \\ &\leq \tfrac{1}{2}P[y = 0] + \tfrac{1}{2}P[y \neq 0] \\ &= \tfrac{1}{2} \end{aligned}$$

…and check if $P[y = 0] = 0$ or $P[y \neq 0] = 0$.

Problem (small triangles in a square) Consider a set $T \subseteq [0,1]^2$ (finite). We set $S(T)$ be the smallest area of a triangle determined by points of T.

Question: If $|T| = n$ how big can $S(T)$ be? We will see: There is T with $S(T) \geq \frac{1}{100n^2}$ (reachable $\Omega\left(\frac{\log n}{n^2}\right)$).

Proof Preliminary computations: Consider three random points P, Q, R uniformly chosen, independently. Let $\lambda(PQR)$ denote the area of PQR triangle First aim: bound $P[\lambda(PQR) \leq \varepsilon]$.

$$W := \mathrm{dist}(P, Q),\ \Delta > 0 \text{ (real parameter)}, i \in \mathbb{N}$$

$$P[\underbrace{W \in [(i-1)\Delta, i\Delta]}_{B_i}] \leq \pi(i^2\Delta^2 - (i-1)^2\Delta^2) = \pi(2i-1)\Delta^2$$

$$P[\lambda(PQR) \leq \varepsilon] = \sum_{i=1}^{\lfloor \frac{\sqrt{2}}{\Delta} \rfloor + 1} P[\lambda(PQR) \leq \varepsilon | B_i] P[B_i]$$

$$P[\lambda(PQR) \leq \varepsilon | B_i] \leq \frac{\sqrt{2} \cdot 4\varepsilon}{(1-i)\Delta}$$

$$P[\lambda(PQR) \leq \varepsilon] = P[\lambda(PQR) \leq \varepsilon | B_1] P[B_1] + \sum_{i=2}^{\lfloor \frac{\sqrt{2}}{\Delta} \rfloor + 1} P[\lambda(PQR) \leq \varepsilon | B_i] P[B_i] \leq$$

$$\leq 1\pi\Delta^2 + \sum_{i=2}^{\lfloor \frac{\sqrt{2}}{\Delta} \rfloor + 1} \frac{4\varepsilon}{(i-1)\Delta} \sqrt(2)\pi(2i-1)\Delta^2 =$$

$$= \pi\Delta^2 + \sum_{i=2}^{\lfloor \frac{\sqrt{2}}{\Delta} \rfloor + 1} 4\sqrt{2}\pi\varepsilon \frac{2i-1}{i-1} \Delta$$

Take $\Delta \to 0$ The aim is:

$$P[\lambda \leq \varepsilon] \leq 4\sqrt{2}\pi\varepsilon 2\sqrt{2} = 16\pi\varepsilon$$

(requires one more limit pass, we shall skip) Easier one is:

$$P[\lambda \leq \varepsilon] \leq 4\sqrt{2}\pi\varepsilon 3\sqrt{2}$$

By ineq. $2 + \frac{1}{i-2} \leq 3$

Consider $2n$ random points in $[0,1]^2$ (chosen uniformly, independently). Let X be a number of triangles with area at most $\frac{1}{100n^2}$.

$$E[X] \leq \binom{2n}{3} 16\pi \frac{1}{100n^2} \leq \frac{8n^3}{6} \cdot \frac{16\pi}{100n^2} < \frac{600n^3}{600n^2} < n$$

Thus there is S with at most n triangles with area at most $\frac{1}{100n^2}$. Let us remove one point from each such triangle.

2^{nd} moment method

Definition (Variance) Let X be a random variable. Then the *variance* of X is defined as: $\text{var}[X] = E[(X - E[X])^2] = E[X^2] - (E[X])^2$

Definition (Standard deviation) $\sigma = \sqrt{\text{var}[X]}$ Equivalently: $E[|X - E[X]|]$ (but this is much harder to work with).

Definition (Covariance) Let X, Y be random variables, then *covariance* of X and Y is defined as $\text{Cov}[X,Y] = E[(X - E[X])(Y - E[Y])] = E[XY] - E[X]E[Y]$

Remark If X, Y are independent then $\text{Cov}[X,Y] = 0$.

Lemma Let $X_1, X_2, \ldots, X_n$ be random variables. Then

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

Proof

$$\text{Var}\left[\sum_{i=1}^n X_i\right] = E\left[\left(\sum_{i=1}^n X_i\right)\left(\sum_{j=1}^n X_j\right)\right] - \left(\sum_{i=1}^n E[X_i]\right)\left(\sum_{j=1}^n E[X_j]\right) =$$

$$= E\left[\sum_{i=1}^{n} X_i^2\right] + E\left[\sum_{i\neq j} X_i X_j\right] - \sum_{i=1}^{n}(E[X_i])^2 - \sum_{i\neq j} E[X_i]E[X_j] = \sum_{i=1}^{n}\mathrm{Var}[X_i] + \sum_{i\neq j}\mathrm{Cov}[X_i, X_j]$$

Lemma (Chebyshev inequality) Let X be a random variable with finite variance and $t > 0$. Then $P[|X - E[X]| \geq t] \leq \frac{\mathrm{Var}[X]}{t^2}$.

Proof Let us define random variable $Y = (X - E[X])^2$. Then

$$P[|X - E[X]| \geq t] = P[Y \geq t^2] \overset{\text{Markov}}{\leq} \frac{E[Y]}{t^2} = \frac{\mathrm{Var}[X]}{t^2}$$

Problem Consider random graph $G(n, p)$, estimate probability that $G(n, p)$ contains a triangle.

Expectation: if p is very small than the probability is almost 0, if p is very large than the probability is almost 1.

Let X be the number of triangles in $G(n, p)$, than $E[X] = \binom{n}{3}p^3$ If p is function of n and in $o(\frac{1}{n})$, then $E[X] \overset{n\to\infty}{\to} 0$. It holds: $P[G(n, p) \text{ contains } \triangle] \overset{\text{Markov}}{\leq} E[X]$ thus $P[G(n, p) \text{ contains } \triangle] \to 0$.

We would like to know whether if $p = \omega(\frac{1}{n})$ then $P[G(n, p) \text{ contains } \triangle] \to 1$ We know that $E[X] \to \infty$

Definition (Monotone property) A graph property A is *monotone*, if for every two graphs G, H with $V(G) = V(H)$, $E(H) \subseteq E(G)$, we get if H has A, then G has A.

Definition (Threshold function) A function $r : \mathbb{N} \to \mathbb{R}$ is a *threshold function* for property A if for every function $p : \mathbb{N} \to [0, 1]$ we get:

$$\lim_{n\to\infty} P[G(n, p(n)) \text{ has } A] = \begin{cases} 0 & p(n) = o(r(n)) \\ 1 & \omega(r(n) \Leftrightarrow r(n) = o(p(n)) \end{cases}$$

Problem (cont.)

Theorem The function $\frac{1}{n}$ is a threshold function for the property “G contains a triangle”.

Lemma Let $X_1, X_2, \ldots$ be non-negative random variables such that $\lim_{n\to\infty} \frac{\mathrm{Var}[X_n]}{(E[X_n])^2} = 0$, then $\lim_{n\to\infty} P[X_n > 0] = 1$.

Proof It holds that $P[|X - E[X]| \geq E[X_n]] \leq \frac{\mathrm{Var}[X_n]}{(E[X_n])^2}$ and $P[X_n > 0] = 1 - P[X_n = 0] \geq 1 - \frac{\mathrm{Var}[X_n]}{(E[X_n])^2}$. Then it follows $P[X_n > 0] = 1 - 0 = 1$

Proof of the theorem Case $p(n) = o(\frac{1}{n})$ we already concluded. Now let us consider $p(n) = \omega(\frac{1}{n})$.

Let T = number of triangles in $G(n, p(n)) = G(n, p)$ and let T_i be indicators of individual triangles (thus $T = \sum T - i$). Now we have $E[T] = \binom{n}{3}p^3$

$$\mathrm{Var}[T] = \mathrm{Var}\left[\sum_i T_i\right] = \sum_i \mathrm{Var}[T_i] + \sum_{i\neq j}\mathrm{Cov}[T_i, T_j]$$

$$\mathrm{Var}[T_i] \leq E[T_i^2] = E[T_i] = p^3$$

$$\mathrm{Cov}[T_i, T_j] \begin{cases} \leq E[T_i T_j] = p^5 & T_i, T_j \text{ share an edge} \\ \overset{T_i T_j \text{ ind.}}{=} 0 & T_i, T_j \text{ edge disjoint} \end{cases}$$

$$\frac{\mathrm{Var}[T]}{(E[T])^2} \leq \frac{\binom{n}{3}p^3 + \binom{n}{2}(n-2)(n-3)p^5}{\left(\binom{n}{3}p^3\right)^2} = O\left(\frac{1}{n^3p^3} + \frac{1}{n^2p}\right) \overset{\text{if } p=\omega(\frac{1}{n})}{\to} 0$$

Concluded by lemma.