The Second Moment Method

28 February 2022 08:33

Definition: For a random variable X,

$$\sigma^2 := \mathrm{Var}[X] := E[(X-\mu)^2], \text{ where}$$

variance of X $\quad \sigma = \sqrt{E[(X-\mu)^2]} \quad \mu = E[X]$.

We use σ^2 to denote variance of X. Then σ denotes the standard deviation of X.

Theorem [Chebyshev's Inequality] For any positive λ,

$$\Pr[|X-\mu| \geq \lambda\sigma] \leq \frac{1}{\lambda^2}$$

or

$$\Pr(|X-\mu| \geq \lambda) \leq \frac{\sigma^2}{\lambda^2}$$

Proof:

$$\sigma^2 = \mathrm{Var}[X]$$

$$= E[(X-\mu)^2] \geq (\lambda^2\sigma^2)\Pr[|X-\mu| \geq \lambda\sigma] + \_\_\_$$

$$\geq (\lambda^2\sigma^2)\Pr[|X-\mu| \geq \lambda\sigma]$$

Rearranging terms, we get

$$\Pr[|X-\mu| \geq \lambda\sigma] \leq \frac{1}{\lambda^2}$$

$\square$

Definition

Suppose $X = X_1 + X_2 + \cdots + X_n$

Then,

$$\mathrm{Var}[X] = \sum_{i=1}^{n} \mathrm{Var}[X_i] + \sum_{\substack{i \neq j : \\ i,j \in [n]}} \mathrm{cov}[X_i, X_j]$$

1

, where $\mathrm{cov}[Y, Z] := E[YZ] - E[Y]E[Z]$

$= E[Y]E[Z]$, when Y and Z are indep.

for any two R.V.s Y and Z. When Y and Z are independent R.V.s, then

$\mathrm{cov}(Y, Z) = 0$.

1b

* Suppose every X_i is an indicator R.V. with

$$X_i = \begin{cases} 1, & \text{with prob } p \\ 0, & \text{with prob } 1-p \end{cases}$$

Here, $\mu_i := E[X_i] = 1 \cdot p + 0 \cdot (1-p) = p$ //

Then, $\mathrm{Var}[X_i] = E\left[(X_i - \mu_i)^2\right]$, when μ_i denotes $E[X_i]$

$= E\left[(X_i - p)^2\right]$

$$= (1-p)^2 \cdot p + p^2 \cdot (1-p)$$

$$= p(1-p)\left(1-\cancel{p}+\cancel{p}\right)$$

$$= \underline{\underline{p(1-p)}}$$

So, for the indicator R.V. X_i,

$$p(1-p) = \underbrace{Var[X_i] \leq E[X_i]}_{②} = p.$$

Therefore, when $X_1, X_2, \ldots, X_n$ are indicator R.V.s, we have (from ① and ②)

$$Var[X] = \sum_{i=1}^{n} Var[X_i] + \sum_{\substack{i \neq j: \\ i,j \in [n]}} Cov[X_i, X_j]$$

$$\leq \sum_{i=1}^{n} E[X_i] + \sum_{\text{" "}} Cov[X_i, X_j]$$

$$Var[X] \leq E[X] + \sum_{\substack{i \neq j: \\ i,j \in [n]}} Cov[X_i, X_j]$$

(when $X = \sum_{i=1}^{n} X_i$, when X_i's are indicator R.V.s) ③

. ———— .

Let X be a non-negative, integral R.V. with

$\mu = E[X] < 1$. Then,

$$Pr[X>0] \le E[X].$$

$X \to 0, 1, 2, \ldots$

$$1 > E[X] = 0 \cdot Pr[X=0] + i_1 \cdot Pr[X=i_1] + i_2 \cdot Pr[X=i_2] + \cdots$$

(where $i_1, i_2, \ldots \in \mathbb{N}$)

$$\ge 1 \cdot Pr[X=i_1] + 1 \cdot Pr[X=i_2] + \cdots$$

$$= Pr[X>0].$$

Theorem 1 For any R.v. X,

$$Pr[X=0] \le \frac{Var[X]}{(E[X])^2}$$

Proof:

We know, from Chebychev's Ineq,

$$Pr[|X-\mu| \ge \lambda\sigma] \le \frac{1}{\lambda^2}$$

Putting $\lambda = \mu$ $\to E[X]$

$\to$ std. deviation $= \sqrt{E[(X-\mu)^2]}$

Putting $\lambda = \frac{\mu}{\sigma}$ $\mu \to E[X]$, $\sigma \to$ std. deviation $= \sqrt{E[(X-\mu)^2]}$

$$\Pr[X=0] \leq \Pr[|X-\mu| \geq \mu] \leq \frac{\sigma^2}{\mu^2} = \frac{\mathrm{var}[X]}{(E[X])^2}$$

$X - \mu \geq \mu$ (or $X \geq 2\mu$)

OR

$-(X-\mu) \geq \mu$

$\Downarrow$

$-X+\mu \geq \mu$

or

$X \leq 0$

$(X \geq 2\mu)$ or $(X \leq 0)$

$\square$

Corollary 2: If $\mathrm{var}[X] \in o((E[X])^2)$, then $X > 0$ almost always. (assuming X is a non-negative R.V.)

Corollary 3: If $\mathrm{var}[X] \in o[(E[X])^2]$, then $X \to E[X]$ almost always.

Proof: For any $\varepsilon > 0$,

$$\Pr[|X-\mu| \geq \varepsilon\mu] \leq \frac{\sigma^2}{\ldots} = \frac{\mathrm{var}[X]}{\ldots}$$

$$\Pr\left[|X-\mu| \geq \varepsilon\mu\right] \leq \frac{\sigma^2}{\varepsilon^2\mu^2} = \frac{\mathrm{Var}[X]}{\varepsilon^2\cdot(E[X])^2}.$$

(by Chebyshev)

$\square$

Suppose $X = X_1 + X_2 + \cdots + X_n$, where each X_i is an indicator R.V. for the event A_i. Using Eqn ① and (1b),

$$\mathrm{Var}[X] = \sum_{i=1}^{n}\mathrm{Var}(X_i) + \sum_{\substack{i\sim j:\\ i,j\in[n]}} \underbrace{\mathrm{Cov}[X_i,X_j]}_{\text{ordered pairs}}$$

A_i is not independent of A_j.

From ②, we know that $\mathrm{Var}[X_i] \leq E[X_i]$. Applying ③,

$$\therefore\ \mathrm{Var}[X] \leq E[X] + \sum_{\substack{i\sim j:\\ i,j\in[n]}}\left(E[X_iX_j] - \cancel{E[X_i]E[X_j]}\right)$$

$$\leq E[X] + \sum_{\substack{i\sim j:\\ i,j\in[n]}} E[X_iX_j]$$

OR,

$$\mathrm{Var}[X] \leq E[X] + \Delta \quad ④$$

where

$$\mathrm{Var}[X] \leq E[X] + \Delta \quad \text{where}$$

$$\Delta = \sum_{\substack{i \sim j: \\ i, j \in [n]}} \Pr[A_i \wedge A_j]$$

2 MARCH 2022

<u>Corollary 4</u>: Let $X = X_1 + X_2 + \dots + X_n$, where every X_i is an indicator R.V. Suppose $E[X] \to \infty$ and $\Delta = o(E[X]^2)$. Then, (from Theorem 1 and Equation (4)) we can say that $X > 0$ almost always. Furthermore, $X \to E[X]$ almost always.

(by Eqn (4))

$$\text{Thm 1: } \Pr[X=0] \leq \frac{\mathrm{Var}[X]}{(E[X])^2} \leq \frac{E[X] + \Delta}{(E[X])^2} = 0 \text{ as } E[X] \to \infty$$

Corollary 3 & Eqn (4) implies $X \to E[X]$ almost always.

Application in Number Theory

Let $\nu(n)$ denote the number of distinct primes p dividing n.

Theorem [(Hardy & Ramanujan, 1920) (Turan 1934)] Let $\omega(n) \to \infty$ arbitrarily slowly. Then, the number of x in $[n]$ such that

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

$$\left| \nu(x) - \ln\ln n \right| > \omega(n) \sqrt{\ln\ln n}$$

is $o(n)$.

$\omega(n) \to n^2$

$\log n$

$\log\log\log n$

$$\left[\ln\ln n - \omega(n)\sqrt{\ln\ln n},\ \ln\ln n + \omega(n)\sqrt{\ln\ln n}\right]$$

almost all numbers in $\{1, .., n\}$ have no. of prime factors in the range.

$$f(n) = o(g(n)) \quad \text{means}$$

$$\frac{f(n)}{g(n)} = 0 \quad \text{as } n \to \infty$$

<u>Proof</u>: Choose a number x uniformly at random from $[n]$. For each prime

random from $[n]$. For each prime number $1 < p \leq n$, let

Indicator R.V.

$$X_p = \begin{cases} 1, & \text{if } p \mid x \\ 0, & \text{otherwise} \end{cases}$$

$p \mid x$ → p divides x

$$\Pr[X_p = 1] = \frac{\lfloor n/p \rfloor}{n} \leq \frac{1}{p}$$

if the random x was any of $p, 2p, 3p, 4p, \ldots$, then $X_p = 1$.

$E[X_p] \leq \frac{1}{p}$.

Let $X = \sum_{p:\, p \text{ is a prime btwn } 1 \,\&\, n} X_p$ → denotes # of prime divisors of x. That is $X = \nu(x)$.

Then,

$$E[X] = \sum_{p:\, p \text{ is a prime btwn } 1 \,\&\, n} E[X_p]$$

by lin of exp.

$$\leq \sum_{p:\, p \text{ is a prime btwn } 1 \,\&\, n} \frac{1}{p}$$

$$E[X] \leq \ln \ln n \quad \text{(standard result)} \quad ①$$

Suppose you're wrong.

Markov: $\Pr[X > a] < \frac{E[X]}{a}$

$\Pr[X > a \ln\ln n] < \frac{1}{a}$

$Var[X] = \sum Var[X_p] + 2 \sum [\ldots]$

$$\mathrm{Var}[X] = \underbrace{\sum_{\substack{p:\ p \text{ is} \\ \text{a prime less} \\ \text{than } n}} \mathrm{Var}[X_p]}_{①} + \sum_{\substack{p,q:\ p \text{ and} \\ q \text{ are distinct} \\ \text{primes btwn } 1 \& n}} \mathrm{Cov}[X_p, X_q]$$

$$\le E[X] + \underbrace{\sum \mathrm{Cov}[X_p, X_q]}_{②}$$

nums. which both p & q divide are pq, 2pq, 3pq, 4pq, ...

Now,

$$\mathrm{Cov}[X_p, X_q] = E[X_p X_q] - E[X_p]E[X_q]$$

$$\le \frac{\lfloor n/pq \rfloor}{n} - \frac{\left(\frac{n}{p}-1\right)}{n}\frac{\left(\frac{n}{q}-1\right)}{n}$$

$$\le \frac{1}{pq} - \left(\frac{1}{p}-\frac{1}{n}\right)\left(\frac{1}{q}-\frac{1}{n}\right)$$

$$= \frac{1}{n}\left(\frac{1}{p}+\frac{1}{q}\right) - \frac{1}{n^2}$$

$$\le \frac{1}{n}\left(\frac{1}{p}+\frac{1}{q}\right)$$

$$\therefore \sum_{\substack{p,q:\ p \text{ and} \\ q \text{ are distinct} \\ \text{primes btwn}}} \mathrm{Cov}(X_p, X_q) \le \sum \frac{1}{n}\left(\frac{1}{p}+\frac{1}{q}\right)$$

$< \ln\ln n$

q are distinct primes b/w 1 & n

$$\leq \frac{2}{n}\left(\#\text{ primes b/w } 1\ \&\ n\right) \sum_{\substack{p:\, p \text{ is a prime}\\ \text{b/w } 1\ \&\ n}} \frac{1}{p}$$

$\leq n$ $\qquad \leq \ln\ln n$

$$\leq \underline{\underline{2\ln\ln n}} \quad \text{--- } ③$$

from ①, ②, & ③

$$\sigma^2 = Var[X] \leq 3\ln\ln n$$

$$\therefore \sigma = \sqrt{3\ln\ln n}$$

Let $\omega(n) \to \infty$ arbitrarily slowly.

Using Chebychev's Inequality,

no. of prime divisors of n.

$$Pr\left[\,|X - \underbrace{\ln\ln n}_{E(X)}| \geq \omega(n)\underbrace{\sqrt{3\ln\ln n}}_{\sigma}\,\right] \leq \frac{1}{(\omega(n))^2}$$

That is,

$$Pr\left[\,|X - \ln\ln n| \geq \omega(n)\sqrt{\ln\ln n}\,\right] \leq \frac{3}{(\omega(n))^2}$$

$\therefore$ almost every number in $[n]$ has "very close to" $\ln\ln n$ prime factors

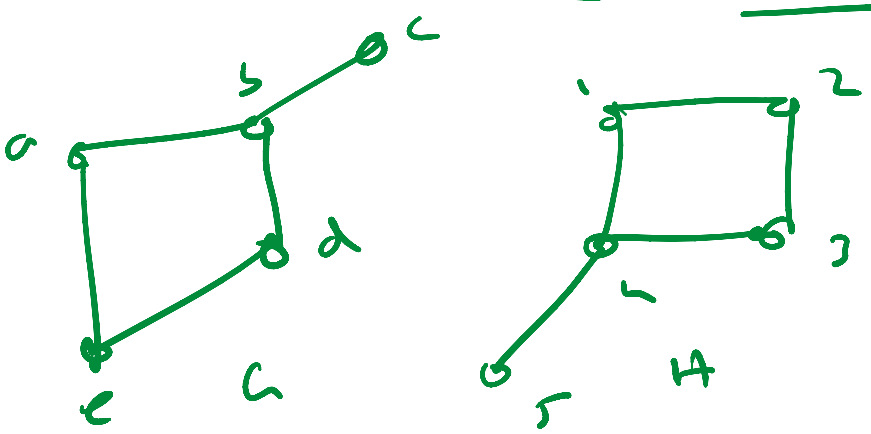
$\square$

Application in random graphs

independence number.   *monotone property.*   *clique no. of G. OR size of a largest clique in G.*

Consider a graph property. For example, a graph G satisfies Property P if $\omega(G) \geq 4$.

$\alpha(G) \geq 4$



Defn. A property of graphs is a family of graphs closed under isomorphism.

$f(c) = 5$

$f(b) = 4$

$f(a) = 1$

$f(e) = 2$

$f(d) = 3$

G is isomorphic to H.

$\frac{p(n)}{r(n)} = 0$ when $n \to \infty$ OR $p(n) = o(r(n))$

$\frac{r(n)}{p(n)} = 0$ as $n \to \infty$ OR $p = p(n) = \omega(r(n))$

$G(n, p)$

$\mathcal{G}(n,p)$ $\quad p = p(n) = \omega(r\ldots)$

A function $r(n)$ is a threshold function for some property P, if whenever $p = p(n) \ll r(n)$ then $\mathcal{G}(n,p)$ does not satisfy property P almost always, and whenever $p \gg r(n)$ then $\mathcal{G}(n,p)$ satisfies property P almost always.

Theorem: The property $\omega(G) \geq 4$ has threshold function $n^{-2/3}$.

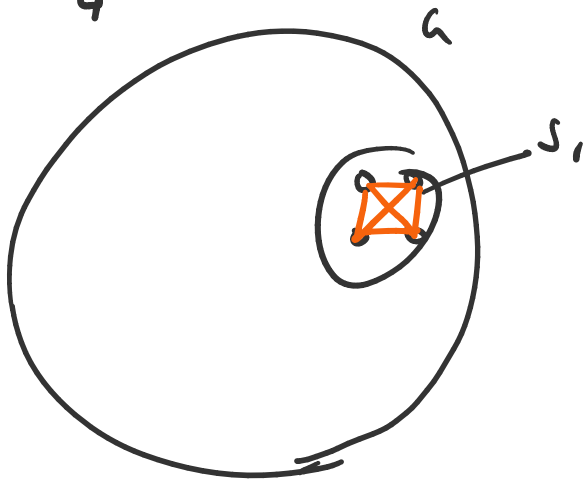
Proof: Let $G \in \mathcal{G}(n,p)$.
Let $S_1 \subseteq V(G)$ with $|S_1| = 4$. Then, we define an indicator R.V.

$$X_1 = \begin{cases} 1, & \text{if } S_1 \text{ is a } K_4 \\ 0, & \text{otherwise} \end{cases}$$

clique on 4 vertices

$$\Pr[X_1 = 1] = p^6 .$$

$$E[X_1] = p^6 \quad (1)$$



clique on 4 vertices

Let X be the R.V. that denotes the no. of distinct K_4's in G.

clique on 4 vertices

Then, $X = X_1 + X_2 + \cdots + X_{\binom{n}{4}}$, where $S_1, S_2, \ldots, S_{\binom{n}{4}}$ $\rightarrow$ collection of all 4-sized subsets of $[n]$.

when $X_i = \begin{cases} 1, & \text{if set } S_i \text{ is a } K_4 \\ 0, & \text{o/w} \end{cases}$

$$E[X] = E\left[X_1 + X_2 + \cdots + X_{\binom{n}{4}}\right]$$

$$= \sum_{i=1}^{\binom{n}{4}} E[X_i] \qquad \text{(by linearity of expectation)}$$

$$= \binom{n}{4} p^6 \qquad \text{(from (1))}$$

$$\leq n^4 p^6 \text{ ——— (1A)}$$

Observation

Note that when $p = n^{-2/3}$

then $E[X] = \binom{n}{4} p^6 \leq n^4 \cdot \frac{1}{(n^{2/3+\varepsilon})^6} = \frac{n^4}{n^{4+\varepsilon}} = 1 \quad o(1)$.

So when $p \ll n^{-2/3}$, then $E[X] = o(1)$.

We know $\Pr[X > 0] \leq E[X]$. $\therefore$ in this case $\Pr(X > 0) = o(1)$. So $X = 0$ almost always

OR

asymptotically almost

$f(n) = o(g(n))$

$f(n) = o(g(n))$

$\frac{f(n)}{g(n)} = 0$, as $n \to \infty$

$f(n) = o(1)$, it means $\frac{f(n)}{1} = 0$, when $n \to \infty$.

asymptotically almost surely.

Suppose $p >> n^{-2/3}$. Then, $E[X] \le n^4 \cdot \frac{1}{(n^{2/3-\varepsilon})^6}$

$= \frac{n^4}{n^{4-6\varepsilon}} = \infty$, as $n \to \infty$. So $E[X] \to \infty$ as $n \to \infty$.

Let A_i, $1 \le i \le \binom{n}{4}$, be the event that $X_i = 1$. We want to show that

To show:

$\Delta = o(E[X]^2)$, where $\Delta = \sum_{\substack{i \sim j: \\ i,j \in [\binom{n}{4}]}} \Pr[A_i \wedge A_j]$.

Then, by Corollary 4, $X > 0$ almost always. This would prove the theorem.

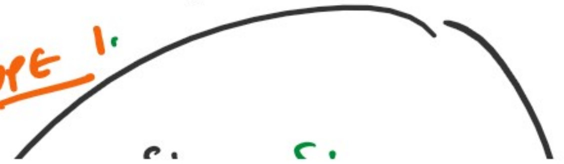
Let us compute Δ.

$$\Delta = \sum_{\substack{i \sim j: \\ i,j \in [\binom{n}{4}]}} \Pr[A_i \wedge A_j]$$

A_i is the event that S_i is a K_4.

no. of TYPE 1 event

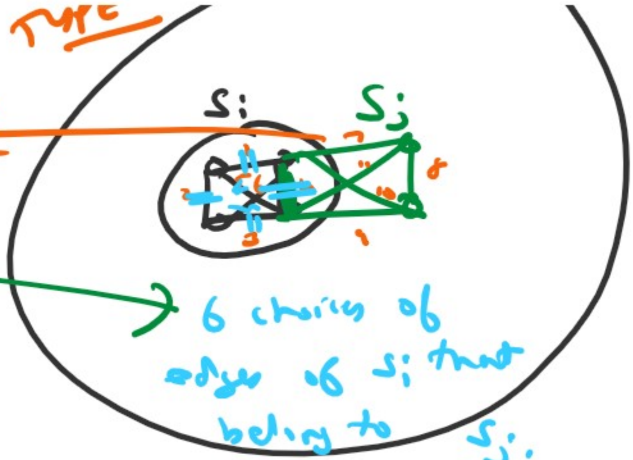
TYPE 1.



no. of dependent pairs of S_i & S_j.

$$\le 6 \cdot n^6 \cdot p^{11} + 4 \cdot n^5 p^9$$

TYPE

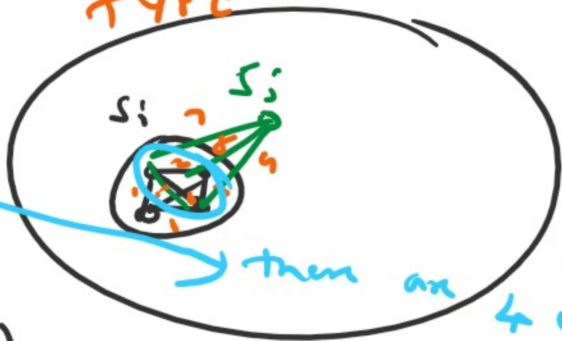


p^{11}

6 choices of edges of S_i that belong to S_j.

no. of TYPE 2 dependent pairs of S_i & S_j

TYPE 2



p^9

then are 4 choices of a triple in S_i that also belongs to S_j

K_3.

$$= O(n^6 p^{11}) + O(n^5 p^9)$$

$$= o(n^6 p^9)$$

$$= O(n^6 p^9 \cdot n^2 p^3)$$

$$= O(n^8 p^{11})$$

when $p = n^{-2/3}$

$$n^2 p^3 = \frac{n^2}{(n^{2/3})^3} = \frac{n^2}{n^2} = 1$$

So when $p >> n^{-2/3}$, clearly $n^2 p^3 \ge 1$.

We have shown that,

$$\Delta = o(n^8 p^{11})$$

OR from (1A) $\Delta = o((E[X])^2)$.

This proves the theorem.

$\square$.