Tutorial 3

08 March 2023 13:57

TAIL INEQUALITIES AND THEIR APPLICATION IN PROBABILITY AMPLIFICATION & ARGUMENTS

MARKOV'S INEQUALITY

CHEBYSHEV'S INEQUALITY

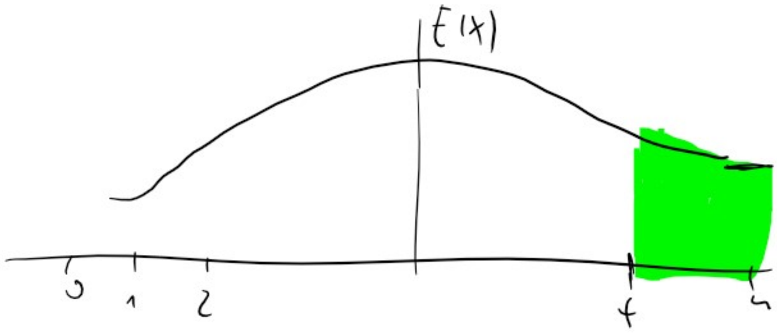
CHERNOFF INEQUALITY

MARKOV'S INEQUALITY

X - random variable with positive values.

$E(X)$ - expectation

$$\Pr(X \geq t) \leq \frac{E(X)}{t}$$



EXAMPLE

LV1 - always gives a correct answer with expected running time $E(\text{running time}) < \text{poly}(n)$

LV2 - always runs in poly(n) time but can output "IDK" w.p. $0 < p < 1$

(typically $(1-p) \geq 1/2$)

LV1 $\Rightarrow$ LV2

Run LV1 for time $\lceil 2E(X)+1 \rceil$ if it does not finish output "IDK".

X_n - number of steps needed for LV1 on input of size n.

$E(X_n)$ - poly n

$$\Pr\Big(X_n \geq \underbrace{2E(X_n)+1}_{t}\Big) \leq \frac{E(X_n)}{2E(X_n)+1} < 1/2 .$$

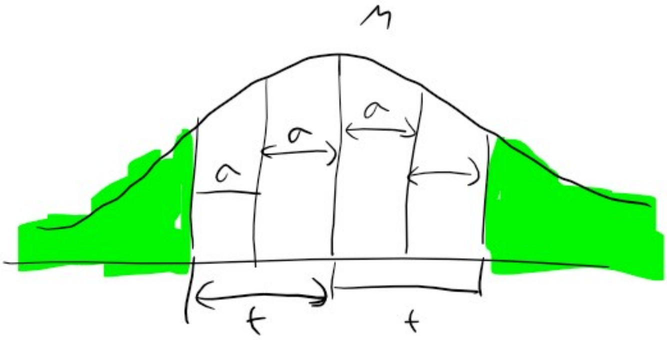
Chebyshev's inequality

X has finite mean $E(X) = \mu$

$Var(X) = \sigma^2$ $\quad\sigma$ - standard deviation

$$\Pr\Big(|X-\mu| \geq \overbrace{k\sigma}^{t}\Big) \leq \frac{1}{k^2}$$

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



Chernoff's bound

Specific form or r.v.

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

, where X_i are $\overline{\text{identically and independently distributed}}^{\text{i.i.d.}}$ binary variables with $\Pr(X_i = 1) = p$

$E(X) = n \cdot p$

↗ Exercise

$$E(X) = n \cdot p$$

Eulerise

$$Pr(X > (1+\delta)\mu) < \frac{e^{\delta}}{(1+\delta)^{(1+\delta)}}$$

$$Pr(X < (1-\delta)\mu) < \frac{e^{-\delta}}{(1-\delta)^{(1-\delta)}}$$

if $0 < \delta < 1$

$$Pr(X \leq (1-\delta)\mu) \leq e^{\frac{-\delta^2 \mu}{2}} \leq e^{\frac{-\delta^2 \mu}{3}}$$

$$Pr(X \geq (1+\delta)\mu) \leq e^{\frac{-\delta^2 \mu}{3}}$$

$$Pr(|X-\mu| \geq \delta\mu) \leq 2e^{\frac{-\delta^2 \mu}{3}}$$

$\boxed{\text{Example}}$

In the experiment we roll a six-sided die n-times

X is the number of outcomes "6"

Calculate $Pr\left(X \geq \frac{n}{4}\right) = \sum_{i=\frac{n}{4}}^{n} \binom{n}{i} \left(\frac{1}{6}\right)^{i} \left(\frac{5}{6}\right)^{n-i}$

Markov's Inequality

$E(X) = \frac{n}{6}$

$$Pr\left(X \geq \frac{n}{4}\right) \leq \frac{E(X)}{\frac{n}{4}} = \frac{n/6}{n/4} = 2/3$$

Chebyshev's Inequality

$$\mathrm{Var}(X) = \sigma^2 = n \cdot p \cdot (1-p) = n \cdot \frac{1}{6} \cdot \frac{5}{6} = \frac{5n}{36}$$

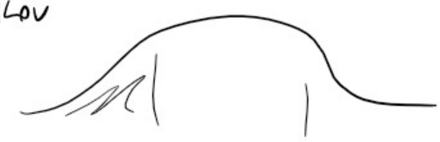
$$\Pr(\cancel{X} \geq \tfrac{n}{4})$$

$$\Pr(|X - E(X)| \geq t)$$

$$=$$

$$\Pr(X - E(X) \geq t) \cup \Pr(E(X) - X \geq t) \leq$$

Chepyshov



$$\geq$$

$$\Pr(X - E(X) \geq t)$$

$$\Pr(X \geq t + E(X))$$

$$t + E(X) = \frac{n}{4} \Rightarrow t = \frac{n}{4} - E(X)$$

$$t = \frac{n}{4} - \frac{n}{6} = \frac{n}{12}$$

$$\leq \frac{\mathrm{Var}(X)}{t^2} = \frac{\frac{5n}{36}}{\frac{n^2}{144}} = \frac{20}{n}$$

Chernoff's inequality

$$X = \sum_{i=1}^{n} X_i \qquad \Pr(X_i = 1) = \frac{1}{6}$$

$$\Pr(X \geq (1+\delta) E(X)) \leq e^{-\frac{\delta^2 E(X)}{3}}$$

$$(1+\delta) E(X) = \frac{n}{4}$$

$$(1+\delta) \frac{n}{6} = n/4$$

$\delta = 1/2 \qquad (0 < \delta < 1)$

$$\Pr\Big(X \geq (\underset{\delta}{1+1/2})\,\underset{E(X)}{\frac{n}{6}}\Big) \leq e^{-\frac{1/4 \cdot \frac{n}{6}}{3}} = e^{-\frac{n}{72}}$$

Amplification of probabilities for 2MC alorithms

BPP Probability of a corect result $\geq 3/4 \quad (1/2 + \varepsilon)$

PP ——————— " ——— $> 1/2 \quad (1/2 + \varepsilon(n))$

Probability amplification: run the algorithm k-times and use majority voting # YES > # NO output YES otherwise NO

X_i – characterizes i^{th} run

$X_i = 1$ if the correct answer is given

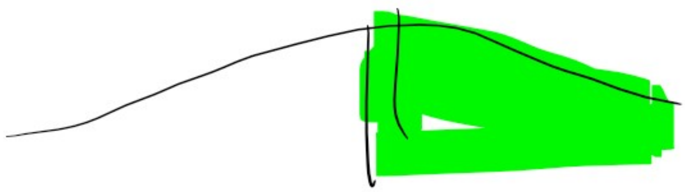
$X_i = 0$ if the incorrect answer is given

$X = \sum_{i=1}^{k} X_i$ the number of correct answers

$E(X) = k \cdot (1/2 + \varepsilon)$

$\Pr\left(X > \frac{k}{2}\right)$

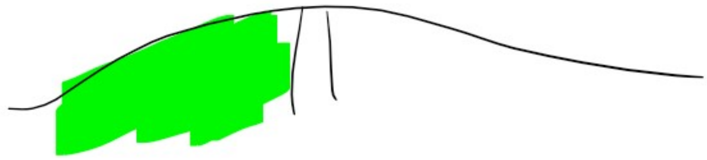
$\vee\!|$



$$1 - \Pr\left(X \le \frac{\varepsilon}{2}\right)$$

$$\shortparallel$$

$$1 - \Pr\left(X \le (1-\delta)\,\eta\right)$$



$$(1-\delta)\,\eta = \varepsilon/2$$

$$(1-\delta) = \frac{\varepsilon}{2\eta}$$

$$\delta = 1 - \frac{\varepsilon}{2kp} = 1 - \frac{1}{2p} = \dots = \frac{\varepsilon}{p}$$

$$= \frac{2p-1}{2p} = \frac{p - 1/2}{p} = \frac{\varepsilon}{p}$$

$$1 - \Pr\left(X \le \left(1 - \frac{\varepsilon}{p}\right) \cdot k \cdot p\right) \ge 1 - e^{-\frac{\left(\frac{\varepsilon^2}{p^2}\right) \cdot k \cdot p}{2}} = \dots = 1 - e^{-\frac{k \cdot \varepsilon^2}{1+2\varepsilon}}$$

$$e^{\frac{-k\varepsilon^2}{1+2\varepsilon}} \le \alpha$$ → chosen small number

$/\ln$

$$-\frac{k\varepsilon^2}{1+2\varepsilon} \le \ln \alpha$$

$$-k\varepsilon^2 \le \ln \alpha \, (1+2\varepsilon)$$

$$k \ge -\frac{\ln \alpha \, (1+2\varepsilon)}{\varepsilon^2}$$

Let n be the size of the input and assume ε depends on n call it $\varepsilon(n)$.

1.) Let $\varepsilon(n) = \frac{1}{\mathrm{poly}(n)}$

$$k(n) \ge -\frac{\ln \alpha \, (1 + 2\varepsilon(n))}{\varepsilon(n)^2}$$

$$k(n) \geq - \frac{\ln \alpha \,(1 + \varepsilon(n))}{\varepsilon(n)^2}$$

2.) $\varepsilon(n) = \frac{1}{2^n}$ (possible in PP)

$$k(n) \in O\left(\frac{1/2^n}{(1/2^n)^2}\right) = O(2^n)$$