Tutorial 3

03 March 2022 12:00

TAIL INEQUALITIES

MARKOV'S INEQUALITY

CHEBYSHEV'S INEQUALITY

CHERNOFF'S INEQUALITY

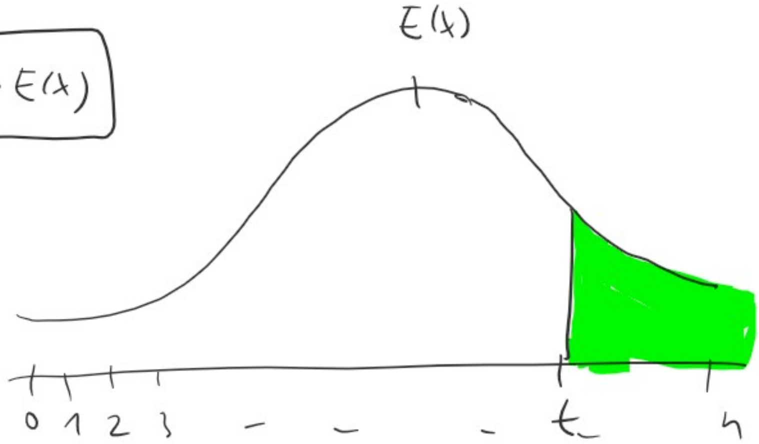
MARKOV'S INEQUALITY

X - random variable with positive values.

E(X) - expectation

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

$\boxed{t > E(X)}$



EXAMPLE

LV1 - always gives a correct answer with expected polynomial running time E(X).

LV2 - always runs in polynomial time, but can output "IDK" w.p. $0 < p < 1$ (typically $(1-p) \geq 1/2$)

Run LV1 for some time $[2E(X)+1]$ if it doesn't finish output "IDK".

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

$$\Pr\big(X_n \ge \underbrace{2E(X_n)+1}_{=\,t}\big) \le \frac{E(X_n)}{2E(X_n)+1} < 1/2 .$$

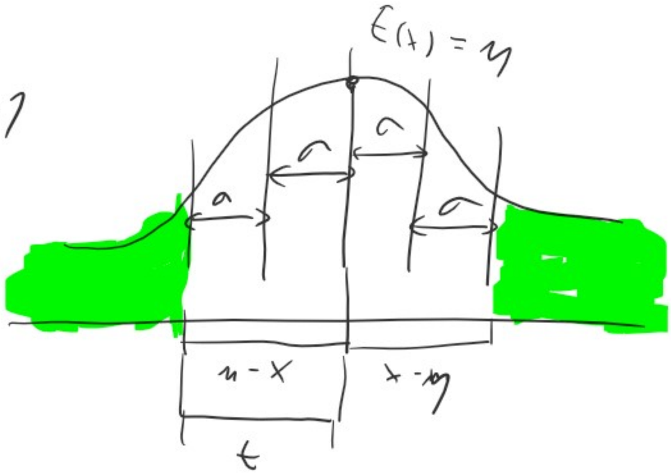
Chebyshev's inequality

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

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

$$\Pr\big(|X-\mu| \ge \overbrace{k\sigma}^{t}\big) \le \frac{1}{k^2} \Rightarrow k>1$$

$$\Pr\big(|X-\mu| \ge t\big) \le \frac{\sigma^2}{t^2}$$



Chernoff's bounds

Specific form of random variables:

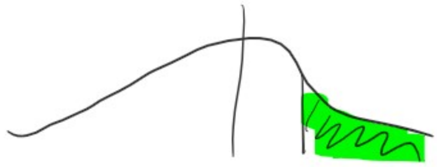
$$X = \sum_{i=1}^{n} X_i \quad , \text{ where } X_i \text{ are } \underbrace{\text{identically and independently distributed}}_{\boxed{\text{i.i.d.}}}$$

$X = \sum_{i=1} x_i$, where X_i are 'identically and independently distributed' binary variables with $Pr(X_i = 1) = p$

$E(X) = n \cdot p$

Euler's contant

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



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

Hard to use

Simpler (looser and more restricted versions)

$$Pr\left(X \le (1-\delta)\mu\right) \le e^{-\frac{\delta^2 \mu}{2}} \le e^{-\frac{\delta^2 \mu}{3}} \qquad 0 < \delta < 1$$

$$Pr\left(X \ge (1+\delta)\mu\right) \le e^{-\frac{\delta^2 \mu}{3}} \qquad 0 < \delta < 1$$

$$\Downarrow$$

$$Pr\left(|X-\mu| \ge \delta\mu\right) \le \boxed{2e^{-\frac{\delta^2 \mu}{3}}}$$

$$\parallel$$

$$Pr\left(X-\mu \ge \delta\mu\right) \vee Pr\left(\mu - X \ge \delta\mu\right)$$

$\Downarrow$ $\qquad\qquad$ $\Downarrow$

$X \ge \delta\mu + \mu$ $\qquad\qquad$ $X \le \mu - \delta\mu$

$\ge (1+\delta)\mu$ $\qquad\qquad$ $X \le (1-\delta)\mu$

$\boxed{\text{Example}}$

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

r.v. X is the number of outcomes '6'

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

Markov's Inequality

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

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

Chebyshev's Inequality

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

$$\Pr\left(X \geq \frac{n}{4}\right) <$$

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

$$\shortparallel$$

$$\Pr\left(X - E(X) \geq t\right) \vee \Pr\left(E(X) - X \geq t\right)$$

$$\geq$$

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

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

$E(X)+t = n/4$

$$t = \frac{n}{4} - \frac{n}{6} = \frac{n}{12} \qquad \leq \frac{Var(X)}{t^2} = \frac{\frac{5n}{36}}{\frac{n^2}{144}} = \frac{20}{n}$$

Chernoff's bound

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

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

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

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

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

$$Pr\left[X \geq \left\{(1+1/2)\cdot\frac{n}{6}\right)\right] \leq e^{\frac{-\left(\frac{1}{2}\right)^2 \cdot \frac{n}{6}}{3}} = e^{-\frac{n}{72}}$$

Amplification of probabilities for 2MC algorithms

BPP – Probability of a correct result $\geq \boxed{1/2 + \varepsilon}$

PP – Probability of a correct result $> 1/2 \quad [1/2 + \varepsilon(n)]$

Probability of amplification = run the algorithm k times and use majority voting #YES > #NO output YES

Otherwise NO

... majority voting if ... ≥ ... output YES

Otherwise NO

$\boxed{\text{Chernoff's bound}}$

X_i - characterizes i^{th} run

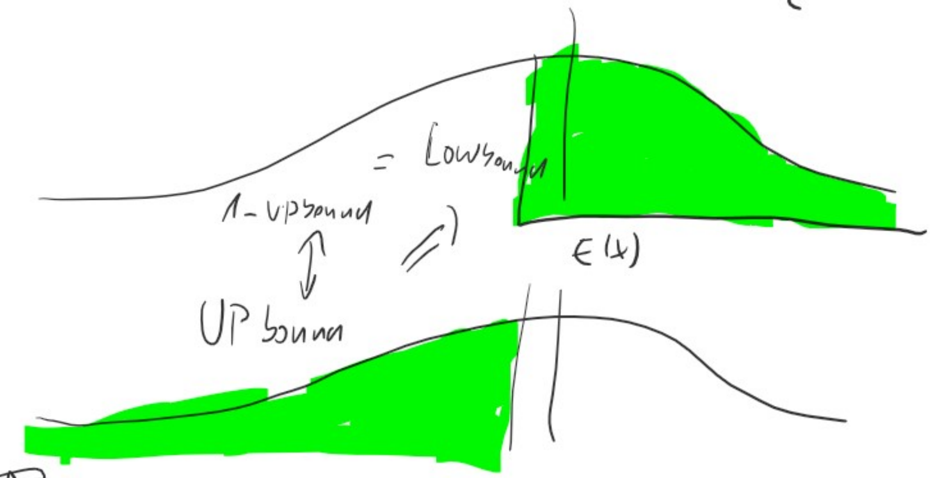
$X_i = 1$ if the correct answer is given

$X_i = 0$ if the incorrect answer is given

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

$E(X) = k \cdot (1/2 + \varepsilon)$ $\quad p = 1/2 + \varepsilon = Pr(X_i = 1)$ $\quad E(X) = \frac{k}{2} + \frac{\varepsilon}{2}$

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



$\vee|$

$1 - Pr(X \leq \frac{k}{2})$

$\shortparallel$

$1 - Pr(X \leq (1-\delta) \cdot \mu)$ $\quad (1-\delta) \cdot \mu = \frac{k}{2}$

$\shortparallel$ $\quad \delta = \frac{\varepsilon}{1/2 + \varepsilon} = \frac{\varepsilon}{p}$

$1 - Pr(X \leq (1 - \frac{\varepsilon}{p}) \cdot \overbrace{k \cdot p}^{\mu}) > 1 - e^{-\left(\frac{\varepsilon^2}{p^2}\right) \cdot \overbrace{kp}^{\mu}} \ldots \quad 1 - e^{-\frac{k \cdot \varepsilon^2}{1+2\varepsilon}}$

$$1 - P_r\left(X \leq \left(1 - \frac{\varepsilon}{p}\right) \cdot \overset{\sim 1}{\widetilde{k \cdot p}}\right) \geq 1 - e^{-\frac{\left(\frac{\varepsilon^2}{p^2}\right) \cdot \widetilde{k p}^{\,\sim 1}}{2}} = \cdots = 1 - e^{-\frac{k \cdot \varepsilon^2}{1+2\varepsilon}}$$

chosen small error

$$e^{\frac{-k \varepsilon^2}{1+2\varepsilon}} \leq \alpha \qquad / \ln$$

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

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

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

let n be the size of the input.

assume ε depends on n

and call it $\varepsilon(n)$.

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

then the number of repetitions to achieve error alpha also depends on n $(k(n))$.

for $\varepsilon(n) = \frac{1}{\text{poly}(n)}$, $k(n) = \text{poly}(n)$

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

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