Applied Stochastics With Applications in Security and Privacy - Excercises, part 2

Mateusz Jachniak

03.04.2020

Exercise 1. Prove theorem:

Let $X_1, \ldots, X_n$ be independent Bernoulli random P variables s.t. $X_i \sim Ber(p, i)$ for $1 \leq i \leq n$. Let $X \sum_{i=1}^{n} X_i$ and denote $\mu = E[X] = \sum_{i=1}^{n} p_i$. Then, for any $0 < \Delta < 1$:

$$Pr[X \leq (1-\Delta)\mu] \leq \Big(\frac{e^{-\Delta}}{(1-\Delta)^{(1-\Delta)}}\Big)^{\mu} \tag{1}$$

$$Pr[X \leq (1-\Delta)\mu] \leq e^{-\mu\Delta^2/2} \tag{2}$$

Solution:

Applying Markov inequality:

$$Pr[X \leq a] \geq \frac{E[X]}{a} \tag{3}$$

and later using fact: $E[e^{tX}] = M_x(t) = e^{\mu(e^t-1)}$.

For all $t < 0$ we get:

$$Pr[X \leq (1-\Delta)\mu] = Pr[e^{tX} \geq e^{t(1-\Delta)\mu}) \leq \frac{E[e^{tX}]}{e^{t(1-\Delta)\mu}} = \frac{e^{\mu(e^t-1)}}{e^{t(1-\Delta)\mu}}$$

Chosing $0 < \Delta < 1$, we set $t = ln(1-\Delta) < 0$ and we have (1):

$$Pr[X \leq (1-\Delta)\mu] \leq \Big(\frac{e^{-\Delta}}{(1-\Delta)^{(1-\Delta)}}\Big)^{\mu}$$

Now it has to be provided, that for $0 < \Delta < 1$ that:

$$Pr[X \leq (1-\Delta)\mu] \leq e^{-\mu\Delta^2/2}$$

For $0 < \Delta < 1$ this is equivalent. Taking the natural logarithm of both sides we obtain:

$$-\Delta - (1-\Delta)ln(1-\Delta) \leq -\frac{\Delta^2}{2} \equiv -\Delta - (1-\Delta)ln(1-\Delta) + \frac{\Delta^2}{2} \leq 0$$

For $0 < \Delta < 1$ we can denote $f(\Delta)$ s.t. :

$$f(\Delta) = -\Delta - (1-\Delta)ln(1-\Delta) + \frac{\Delta^2}{2}$$

Lets see, what we got, by calculating both derivatives:

$$f'(\Delta) = ln(1-\Delta) + \Delta \quad \text{ and } \quad f''(\Delta) = -\frac{1}{1-\Delta} + 1$$

Since $f''(\Delta) < 0$ in the range $(0, 1)$ and since $f'(0) = 0$, we have $f'(\Delta) \leq 0$ in the range $[0, 1)$. Therefore, $f(\Delta)$ is non increasing in that interval. Since $f(0) = 0$, it follows that $f(\Delta) \leq 0$ when $0 < \Delta < 1$ as required it's equivalent to (2).

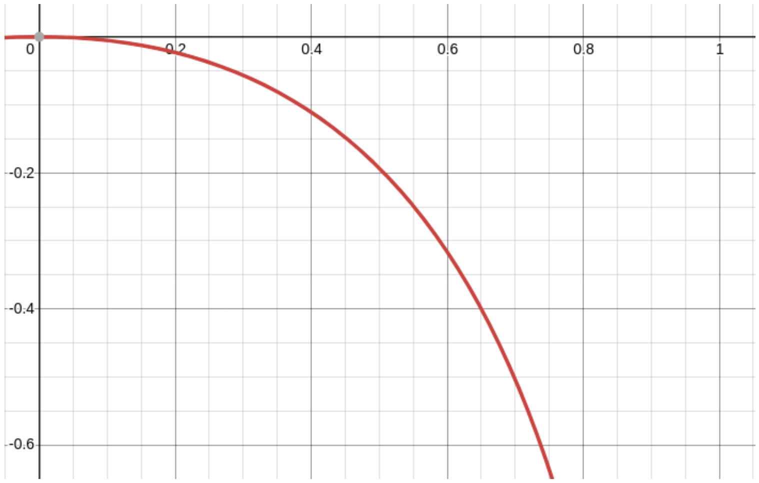

Figure 1: $f'(\Delta) = ln(1-\Delta) + \Delta$

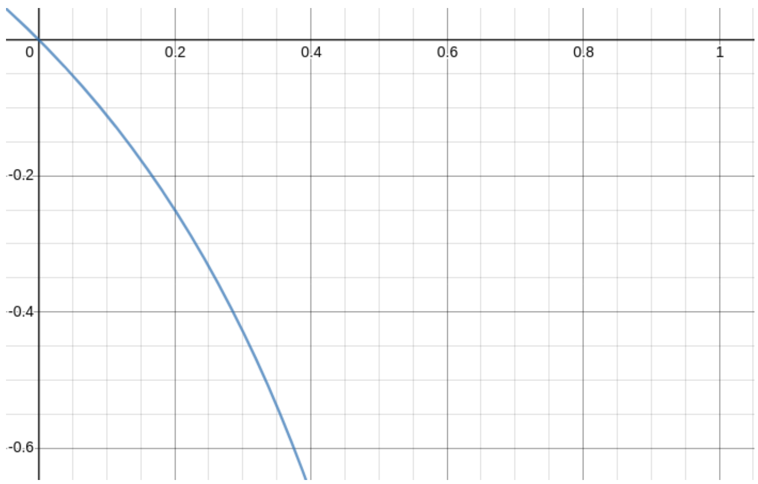

Figure 2: $f''(\Delta) = -\frac{1}{1-\Delta} + 1$

Exercise 2. Suppose we toss a fair coin n times independently. Estimate the probability of getting no more than $\frac{n}{4}$ or no less than $\frac{3n}{4}$ heads using Chernoff bound and Chebyshev's inequality. Derive the formulas as functions of n and compare them by plotting them on the same graph.

Solution:

First what we can see is that, in this case we have binomial distribution with probability of win and lose are the same, equal $\frac{1}{2}$. Let's find an upper bound the Chebyshev's inequality for probability no less than $\frac{3n}{4}$:

$$\begin{aligned}
Pr[X \geq \frac{3n}{4}] &= Pr[X - np \geq \frac{3n}{4} - np] && \text{cause E[X] for binomial is equal np} \\
&\leq Pr[|X - np| \geq \frac{3n}{4} - np \\
&\leq \frac{Var(X)}{(\frac{3n}{4} - np)^2} && \text{using Chebyshev's inequality} \\
&= \frac{p(1-p)}{n(\frac{3}{4} - p)^2} && \text{using binomial variance, which is equal np(1-p)} \\
&= \frac{4}{n} && \text{for } p = \frac{1}{2}
\end{aligned} \tag{1}$$

Calculation for probability no grater than $\frac{n}{4}$ going the same way, so the result is $Pr[X \leq \frac{n}{4}] \leq \frac{n}{4}$
Now let's think about Chernoff bound. For binomial distribution we have:

$$M_X(s) = (pe^s + q)^n$$

Thus, a Chernoff bound (for for probability no less than $\frac{3n}{4}$) can be descripted as:

$$Pr[X \geq \frac{3n}{4}] \leq \min_{s>0} e^{-sa} M_X(s) = \min_{s>0} e^{-\frac{3s}{4}} (pe^s + q)^n$$

which is the same for no grater than $\frac{n}{4}$ (and next calculations are equal). Now, to find a minimizing value of s, we have to calculate derivative:

$$\frac{\partial}{\partial s} e^{-sa} (pe^s + q)^n$$

After some calculations, we receive:

$$e^s = \frac{aq}{np(1-\frac{3}{4})}$$

Now, using s, we obtain:

$$Pr[X \geq \frac{3n}{4}] \leq \Big(\frac{1-p}{1-\frac{3}{4}}\Big)^{(1-\frac{3}{4})n} \Big(\frac{p}{\frac{3}{4}}\Big)^{\frac{3n}{4}}$$

For $p = q = \frac{1}{2}$:

$$Pr[X \geq \frac{3n}{4}] \leq (\frac{16}{27})^{\frac{n}{4}}$$

As it has been noticed before, calculations go the same way, so we obtain:

$$Pr[X \leq \frac{n}{4}] \leq (\frac{16}{27})^{\frac{n}{4}}$$

Now let's compare Chebyshev's inequality and Chernoff bound. Using simple script for $n \in [0, 100]$

```
import numpy as np
import matplotlib.pyplot as plt

n = np.arange(0, 100, 1)

plt.plot(n, 4/n, n, pow((16/27),(n/4)))
plt.show()
```

From the chart below (which is result of above code), we can make a great conlusion, that Chernoff bound is a very better way to estimate bounds than Chebyshev's or Markov's inequality. What importnant, it's for more samples the Chernoff bound is more precised, in oposite to Chebyshev's inequality.

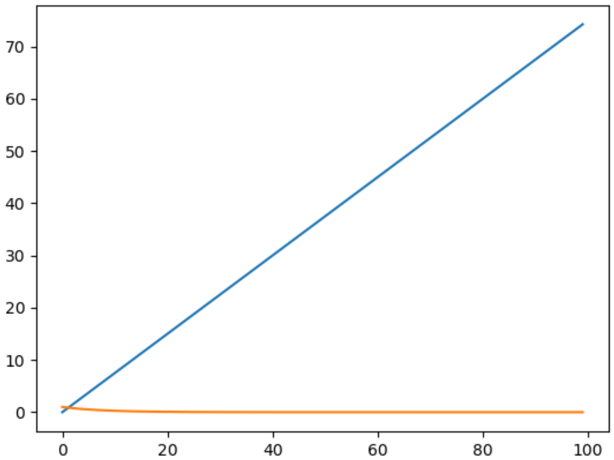

Figure 3: Blue is Chebyshev's inequality result, orange - Chernoff bound

Exercise 3. Compare Chernoff-type bounds for binomial distribution with Markov's and Chebyshev's inequalities. For $X \sim Bin(n, \frac{1}{2})$ and for $n = 100, 1000, 10000$ calculate the estimates of $Pr[X > 1\frac{1}{5}E[X]]$ and $Pr[|X - E[X]| \geq \frac{1}{10}E[X]]$ using Chernoff bounds and compare the results with the values calculated in Exercise 12 from Part I and II of the classroom notes.

Solution:

1) $\boldsymbol{Pr[X > 1\frac{1}{5}E[X]]}$

Let's determine the form of the Chernoff Bounds for the Binomial distribution. From Corollary 1.8:

$$Pr[|X - \mu| \geq \Delta\mu] \leq 2e^{-\mu\Delta^2/3}$$

for any Δ such that $0 < \Delta < 1$. $\mu = E[X]$, and using symmetry of Binomial distribution around the mean, we can say that $Pr[X > 1\frac{1}{5}E[X]] = \frac{1}{2}Pr[|X - E[X]| \geq \frac{1}{5}E[X]] - Pr[X = 1\frac{1}{5}E[X]]$. It is apparent that the value of Δ is $\frac{1}{5}$ in this case. We got:

$$\begin{aligned}
&Pr[X > 60] \equiv \frac{1}{2}Pr[X - 50 \geq 10] - Pr[X = 60] \leq\approx 5.03 \times 10^{-1} \\
&Pr[X > 600] \equiv \frac{1}{2}Pr[X - 500 \geq 100] - Pr[X = 600] \leq\approx 1.27 \times 10^{-3} \\
&Pr[X > 6000] \equiv \frac{1}{2}Pr[X - 5000 \geq 1000] - Pr[X = 6000] \leq\approx 1.11 \times 10^{-29}
\end{aligned} \tag{1}$$

To make conclusion, when n increases the Chernoff makes a better results than Chebyshev's inequality.

2) $\boldsymbol{Pr[|X - E[X]| \geq \frac{1}{10}E[X]]}$ Using the formula, we have to only plug in the next numbers ($\Delta = \frac{1}{10}$).:

$$\begin{aligned}
&Pr[|X - 50| \geq 5] \leq 1.69 \times 10^{0} \\
&Pr[|X - 500| \geq 50] \leq 3.78 \times 10^{-1} \\
&Pr[|X - 5000| \geq 500] \leq 1.16 \times 10^{-7}
\end{aligned} \tag{2}$$

To make conclusion, when n increases the Chernoff makes a better results than Chebyshev's inequality, like in previous case.