

# CS5314

## Randomized Algorithms

Lecture 8: Moments and Deviations  
(Common Variance, Chebyshev Inequality)

# Objectives

- Variances of  $\text{Bin}(n,p)$  and  $\text{Geo}(p)$
- Chebyshev's Inequality

# Variance of Binomial RV

Lemma: Let  $X$  be a binomial random variable with parameters  $n$  and  $p$ . Then,

$$\text{Var}[X] = np(1-p)$$

How do we get that?

$$\begin{aligned}\text{Recall: } \text{Var}[X] &= E[(X - E[X])^2] \\ &= E[X^2] - (E[X])^2\end{aligned}$$

# First Proof (computing $E[X^2]$ )

$$\begin{aligned} E[X^2] &= \sum_{0 \leq j \leq n} j^2 \Pr(X=j) \\ &= \sum_{0 \leq j \leq n} j^2 C_j^n p^j (1-p)^{n-j} \\ &= \sum_{0 \leq j \leq n} (j(j-1)+j) C_j^n p^j (1-p)^{n-j} \\ &= \sum_{2 \leq j \leq n} j(j-1) C_j^n p^j (1-p)^{n-j} \\ &\quad + \sum_{1 \leq j \leq n} j C_j^n p^j (1-p)^{n-j} \end{aligned}$$

By expanding  $C_j^n$  term, we get:

# First Proof (computing $E[X^2]$ )

$$E[X^2]$$

$$= n(n-1)p^2 \sum_{2 \leq j \leq n} C_{j-2}^{n-2} p^{j-2} (1-p)^{n-j}$$

$$+ np \sum_{1 \leq j \leq n} C_{j-1}^{n-1} p^{j-1} (1-p)^{n-j}$$

$$= n(n-1)p^2 (p + (1-p))^{n-2} + np (p + (1-p))^{n-1}$$

$$= n(n-1)p^2 + np$$

# First Proof (computing $E[X^2]$ )

Since  $\text{Var}[X] = E[X^2] - (E[X])^2$ , we have:

$$\begin{aligned}\text{Var}[X] &= n(n-1)p^2 + np - (np)^2 \\ &= n^2p^2 - np^2 + np - n^2p^2 \\ &= np - np^2 \\ &= np(1-p)\end{aligned}$$

## Second Proof (using indicator)

Binomial r.v.  $X = \text{Bin}(n, p)$  can be written as the sum of  $n$  independent indicator,  $X_1, X_2, \dots, X_n$ , each succeeds with probability  $p$

$$\text{That is, } X = X_1 + X_2 + \dots + X_n$$

$$\begin{aligned} \text{So, } \text{Var}[X] &= \text{Var}[X_1] + \text{Var}[X_2] + \dots + \text{Var}[X_n] \\ &= n \text{Var}[X_1] \end{aligned}$$

## Second Proof (using indicator)

$$\begin{aligned}\text{Var}[X_1] &= E[(X_1 - E[X_1])^2] \\ &= (1-p)^2 \Pr(X_1=1) + (0-p)^2 \Pr(X_1=0) \\ &= (1-p)^2 p + p^2(1-p) \\ &= p(1-p)(1-p + p) = p(1-p)\end{aligned}$$

Thus,

$$\text{Var}[X] = n \text{Var}[X_1] = np(1-p)$$



# Variance of Geometric RV

Lemma: Let  $X$  be a geometric random variable with parameter  $p$ . Then,

$$\text{Var}[X] = (1-p)/p^2$$

How do we get that?

# First Proof (computing $E[X^2]$ )

$$\begin{aligned} E[X^2] &= \sum_{j \geq 0} j^2 \Pr(X = j) \\ &= \sum_{j \geq 0} j^2 p (1-p)^{j-1} \\ &= [p/(1-p)] \times \sum_{j \geq 0} j^2 (1-p)^j \end{aligned}$$

To get  $E[X^2]$ , it remains to compute the value of  $\sum_{j \geq 1} j^2 (1-p)^j$

Before that, let's look at some equalities

# First Proof (computing $E[X^2]$ )

For  $|x| < 1$ ,

(a) 
$$1/(1-x) = \sum_{j \geq 0} x^j$$

(b) By differentiating (a), we get

$$1/(1-x)^2 = \sum_{j \geq 0} j x^{j-1}$$

(c) By differentiating (b), we get

$$2/(1-x)^3 = \sum_{j \geq 0} j(j-1) x^{j-2}$$

# First Proof (computing $E[X^2]$ )

Using the previous equalities,

$$\begin{aligned} & \sum_{j \geq 0} j^2 x^j \\ &= \sum_{j \geq 0} j(j-1) x^j + \sum_{j \geq 0} j x^j \\ &= 2x^2/(1-x)^3 + x/(1-x)^2 \\ &= (2x^2 + x(1-x)) / (1-x)^3 \\ &= (x^2 + x) / (1-x)^3 \end{aligned}$$

# First Proof (computing $E[X^2]$ )

So,

$$\begin{aligned} E[X^2] &= \left[ \frac{p}{1-p} \right] \times \sum_{j \geq 0} j^2 (1-p)^j \\ &= \left[ \frac{p}{1-p} \right] \times \left( (1-p)^2 + (1-p) \right) / \left( 1 - (1-p) \right)^3 \\ &= \left[ \frac{p}{1-p} \right] \times \left( (1-p)(2-p) \right) / p^3 \\ &= (2-p)/p^2 \end{aligned}$$

Then,

$$\begin{aligned} \text{Var}[X] &= E[X^2] - (E[X])^2 \\ &= (2-p)/p^2 - (1/p)^2 = (1-p)/p^2 \end{aligned}$$

## Second Proof (by memory-less property)

Let  $Y$  be a random variable such that

$Y=1$  if the first trial succeeds, and

$Y=0$  if the first trial fails

Then,

$$\begin{aligned} E[X^2] &= \Pr(Y=1) E[X^2|Y=1] \\ &\quad + \Pr(Y=0) E[X^2|Y=0] \\ &= p E[X^2|Y=1] + (1-p) E[X^2|Y=0] \\ &= p + (1-p) E[X^2|Y=0] \end{aligned}$$

## Second Proof (by memory-less property)

We want to get  $E[X^2|Y=0]$  ...

Let  $Z$  = #remaining trials until first success

In this case ( $Y=0$ ), we have  $X = Z + 1$

So,  $E[X^2|Y=0] = E[(Z+1)^2]$  ... [why?]

$$= E[Z^2 + 2Z + 1] = E[Z^2] + 2E[Z] + 1$$

But from the memory-less property,

$$E[Z^2] = E[X^2] \quad \text{and} \quad E[Z] = E[X]$$

## Second Proof (by memory-less property)

$$\begin{aligned}\text{So, } E[X^2] &= p + (1-p) E[X^2 | Y=0] \\ &= p + (1-p) (E[X^2] + 2E[X] + 1) \\ &= p + (1-p) (E[X^2] + 2/p + 1)\end{aligned}$$

Rearranging terms,

$$\begin{aligned}p E[X^2] &= p + 2(1-p)/p + (1-p) \\ &= 1 + (2-2p)/p = (2-p)/p\end{aligned}$$

$$\text{Again, } E[X^2] = (2-p)/p^2$$

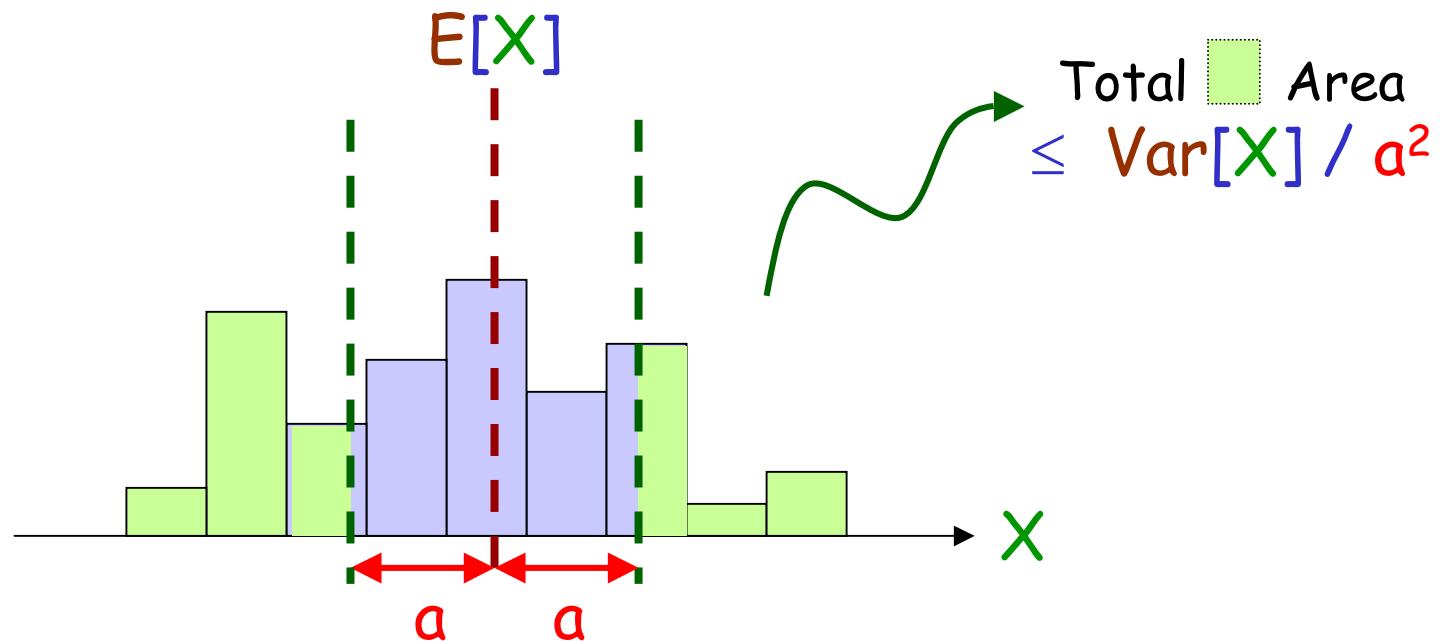
$$\rightarrow \text{Var}[X] = (1-p)/p^2 \text{ as before}$$



# Chebyshev Inequality

Theorem: For any positive  $a$ ,

$$\Pr(|X - E[X]| \geq a) \leq \text{Var}[X]/a^2$$



# Proof

By using Markov Inequality!!!

$$\begin{aligned} & \Pr( |X - E[X]| \geq a ) \\ &= \Pr( (X - E[X])^2 \geq a^2 ) \\ &\leq E[(X - E[X])^2] / a^2 && \text{[by Markov inequality]} \\ &= \text{Var}[X] / a^2 \end{aligned}$$

# Chebyshev Inequality (other variations)

Corollary: For any positive  $r$ ,

$$\Pr(|X - E[X]| \geq r \sigma[X]) \leq 1/r^2$$

Corollary: For any positive  $r$ ,

$$\Pr(|X - E[X]| \geq r E[X]) \leq \text{Var}[X]/(r E[X])^2$$

# Markov vs Chebyshev

- When applying Chebyshev :
  1.  $X$  can take on negative values
  2. Need  $\text{Var}[X]$  to get the bound
  3. Often give better bounds than Markov (since it is based on more information)

# Markov vs Chebyshev

## (Example 1)

Suppose we flip a fair coin  $n$  times

**Question:** Can we bound the probability of more than  $3n/4$  heads?

Let  $X$  = number of heads. So,  $E[X] = n/2$

By Markov Inequality,

$$\begin{aligned}\Pr(X \geq 3n/4) &\leq E[X] / (3n/4) \\ &= (n/2) / (3n/4) = 2/3\end{aligned}$$

# Markov vs Chebyshev

## (Example 1)

Let's use Chebyshev Inequality instead:

Again,  $X$  = number of heads

So,  $E[X] = n/2$  and  $\text{Var}[X] = n/4$  ... [why?]

Then, we have

$$\Pr(X \geq 3n/4)$$

$$\leq \Pr(|X - E[X]| \geq n/4) \dots [\text{why?}]$$

$$\leq \text{Var}[X] / (n/4)^2$$

$$= 4/n \quad \dots \text{much better bound than } 2/3!!!$$

# Markov vs Chebyshev

## (Example 2)

Let us revisit Coupon Collector's problem:

There are a total of  $n$  different cards.  
Each time, the card we buy is chosen independently and uniformly at random from the  $n$  cards.

Let  $X$  = number of cards we need to buy  
Previously, we get  $E[X] = nH(n)$

# Markov vs Chebyshev

## (Example 2)

**Question:** Can we bound the probability of buying more than  $2nH(n)$  cards?

By Markov Inequality,

$$\begin{aligned} & \Pr(X \geq 2nH(n)) \\ & \leq E[X] / (2nH(n)) \\ & = nH(n) / (2nH(n)) \\ & = 1/2 \end{aligned}$$



# Markov vs Chebyshev

## (Example 2)

Question:

How about using Chebyshev Inequality?

To apply the inequality, we need to get  
 $\text{Var}[X]$  ... What is this value?

# Markov vs Chebyshev

## (Example 2)

Let  $X_i$  = #cards bought to get a new card after collecting exactly  $i-1$  distinct cards

$$\text{So, } X = X_1 + X_2 + \dots + X_n$$

Also, the variables  $X_i$  are all independent!

Thus,

$$\text{Var}[X] = \text{Var}[X_1] + \text{Var}[X_2] + \dots + \text{Var}[X_n]$$

# Markov vs Chebyshev (Example 2)

What is  $\text{Var}[X_k]$ ?

Recall:  $X_k$  is  $\text{Geo}(p)$  with  $p = (n-k+1)/n$

Thus,

$$\begin{aligned}\text{Var}[X_k] &= (1-p)/p^2 \\ &\leq 1/p^2 \\ &= n^2/(n-k+1)^2\end{aligned}$$

# Markov vs Chebyshev

## (Example 2)

$$\begin{aligned}\text{So, } \text{Var}[X] &= \text{Var}[X_1] + \text{Var}[X_2] + \dots + \text{Var}[X_n] \\ &\leq n^2/(n)^2 + n^2/(n-1)^2 + \dots + n^2/(1)^2 \\ &\leq 2n^2\end{aligned}$$

Now, by Chebyshev Inequality,

$$\begin{aligned}\Pr(X \geq 2nH(n)) &\leq \Pr(|X - E[X]| \geq nH(n)) \\ &\leq \text{Var}[X] / (nH(n))^2 \\ &\leq 2n^2 / (nH(n))^2 \\ &= O(1/\log^2 n) \quad \dots \text{ much better than } 1/2!!!\end{aligned}$$