March 24

Recall. Bernolli Trials

1.	p	$\mu = p$
0.	$q = 1-p$	$\sigma^2 = pq$

Binomial Distribution

n Bernoulli Trials what's the probability of k successes?

$$P(X=k) = \binom{n}{k} p^k q^{n-k} = \binom{n}{k} p^k (1-p)^{n-k}$$

$X \sim 0, 1, 2, \cdots, n$

$E[x]$ and $Var(x)$

Let X_j represent the outcome of the j^{th} Bernoulli Trial

$P(X_j = 0) = 1-p \qquad p(X_j = 1) = p$

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

$$E[X] = E[X_1 + X_2 + \cdots + X_n]$$
$$= E[X_1] + E[X_2] + \cdots + E[X_n]$$
$$= np$$

Example consider tossing a coin with 0.3 of head and 0.7 of tail.

Assume we toss the coin 100,000 times how many heads should we expect?

$100{,}000 \times 0.3 = 30{,}000$

Variance

$$Var(X) = Var(X_1 + X_2 + \cdots + X_n)$$

Recall the variance of the sum of independent r.v. is the sum of the individual vairance

$$Var(X) = Var(X_1) + \cdots + Var(X_n) = npq$$

Geometric Distribution

A <u>Bernoulli Trial</u> with a probability p of success.

Let X be the r.v. representing the number of trials until the success occurs.

$X \sim 1, 2, \cdots, \infty$

$$P(X=k) = (1-p)^{k-1}p$$

① check if the distribution is well-defined.

$$\sum_{j=1}^{\infty} P(X=j) = \lim_{n\to\infty} \sum_{j=1}^{n} (1-p)^{j-1}p$$

$$\sum_{j=1}^{n} (1-p)^{j-1}p = (1-p)^0 p + (1-p)^1 p + (1-p)^2 p \cdots + (1-p)^n p$$

$$= \frac{p - \cancel{(1-p)^n p}\,(1-p)}{1-(1-p)} \underset{n\to\infty}{=} \frac{p-0}{p}$$

(4)

$$E[X] = \sum_{j=1}^{\infty} (1-p)^{j-1} p \cdot j$$

$$= (1-p)^0 p \cdot 1 + (1-p) p \cdot 2 + (1-p)^2 \cdot p \cdot 3 + \cdots$$

$$S = (1-p)^0 p \cdot 1 + (1-p) \cdot p \cdot 2 + (1-p)^2 p \cdot 3 + (1-p)^3 p 4 + \cdots$$

$$(1-p) S = (1-p) \cdot p \cdot 1 + (1-p)^2 p \cdot 2 + (1-p)^3 p \cdot 3 + \cdots$$

$$pS = \underline{(1-p)^0 p + (1-p) \cdot p + (1-p)^2 p + (1-p)^3 p}$$

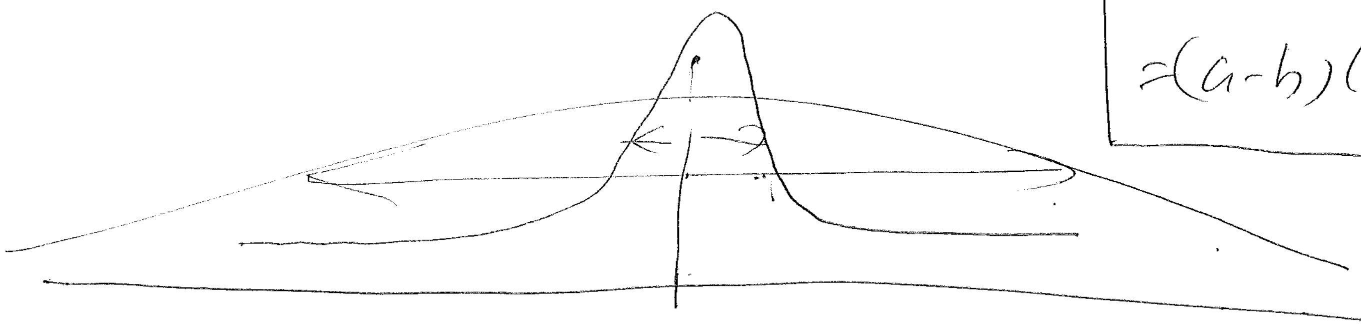
$$= 1$$

$$S = \frac{1}{p} \qquad E[X] = \frac{1}{p}$$

Example: consider a coin with probability 0.2 of H

$$Var(X) = E[X^2] - (E[X])^2$$

$$\boxed{\begin{aligned} &a^2 - b^2 \\ &= (a-b)(a+b) \end{aligned}}$$



$E[X]$ / μ

$$\boxed{\begin{aligned} &(a+1)^2 - a^2 \\ &= \cancel{((a+1)-a)}(a+1+a) \\ &= 2a+1 \end{aligned}}$$

$$E[X^2] = \sum_{j=1}^{\infty} (1-p)^{j-1} p \cdot j^2$$

$$S = (1-p)^0 p \cdot 1^2 + (1-p)^1 \cdot p \cdot 2^2 + (1-p)^2 \cdot p \cdot 3^2 + (1-p)^4 \cdot p \cdot 4^2 + \cdots$$

$$(1-p)S = \qquad (1-p)^1 \cdot p \cdot 1^2 + (1-p)^2 \cdot p \cdot 2^2 + (1-p)^3 \cdot p \cdot 3^2 + \cdots$$

$$pS = (1-p)^0 \cdot p \cdot \overset{(2\cdot 0+1)}{1} + (1-p)^1 \cdot p \cdot (2\cdot 1+1) + (1-p)^2 p (2\cdot 2+1) +$$
$$(1-p)^3 \cdot p (2\cdot 3+1) + \cdots$$

$$= \cancel{\sum_{k=1}^{\infty} (1-p) p \cdot (2\cdot k+1)}$$

$$= (1-p)^0 \cdot p + (1-p)^1 \cdot p + (1-p)^2 \cdot p + (1-p)^3 p + \cdots$$
$$(1-p)^1 \cdot p \cdot 2 \cdot 1 + (1-p)^2 \cdot p \cdot 2 \cdot 2 + (1-p)^3 p \cdot 2 \cdot 3 \cdots$$

$$= \sum_{j=1}^{\infty} (1-p)^{j-1} p$$

$$+ 2 \sum_{j=1}^{\infty} (1-p)^{j} \cdot p \cdot j$$

$$= \sum_{j=1}^{\infty} (1-p)^{j-1} p + 2(1-p) \sum_{j=1}^{\infty} (1-p)^{j-1} \cdot p \cdot j$$

$$= 1 + 2(1-p)\frac{1}{p}$$

$$= 1 + \frac{2}{p} - 2 = \cancel{\frac{2}{p^2} - 1} \ \frac{2}{p} - 1$$

$$E[X^2] = \frac{2}{p^2} - \frac{1}{p} \qquad E[X] = \frac{1}{p}$$

$$Var(X) = E[X^2] - (E[X])^2$$

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

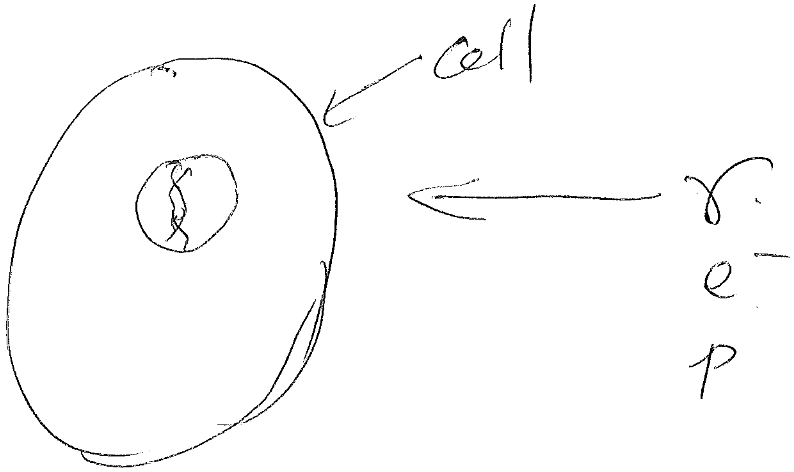
$$= \frac{1}{p^2} - \frac{1}{p}$$

Poisson Distribution

A r.v. X is subject to the Poisson Distribution

if $P(X=k) = \dfrac{\lambda^k e^{-\lambda}}{k!}$ $\quad X=0,1,\ldots$

$0! = 1$



$\longrightarrow H_2O \longrightarrow HO\cdot H$

$-\quad HO\cdot \quad H\cdot$

$$P(X=k) = \frac{\lambda^k e^{-\lambda}}{k!}$$

① is it well-defined?

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} = e^{-\lambda} \sum_{k=0}^{\infty} \frac{\lambda^k}{k!} = e^{-\lambda} \cdot e^{\lambda} = 1$$

② $$E[X] = \sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot k$$

$$= \sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{(k-1)!} = \lambda \sum_{k=0}^{\infty} \frac{\lambda^{k-1} e^{-\lambda}}{(k-1)!} = \lambda$$

$$= \cancel{\frac{\lambda^0 e^{-\lambda}}{0!} \cdot 0} + \frac{\lambda^1 \cdot e^{-\lambda}}{1!} \cdot 1 + \frac{\lambda^2 e^{-\lambda}}{2!} \cdot 2$$

$$+ \frac{\lambda^3 e^{-\lambda}}{3!} \cdot 3 + \cdots$$

$$= \frac{\lambda^1 \cdot e^{-\lambda}}{0!} + \frac{\lambda^2 e^{-\lambda}}{1!} + \frac{\lambda^3 e^{-\lambda}}{2!} + \frac{\lambda^4 e^{-\lambda}}{3!} + \cdots$$

$$= \lambda \left(\frac{\lambda^0 e^{-\lambda}}{0!} + \frac{\lambda^1 e^{-\lambda}}{1!} + \frac{\lambda^2 e^{-\lambda}}{2!} + \frac{\lambda^3 e^{-\lambda}}{3!} + \cdots \right)$$

$$= \lambda$$

3

$$Var(X) = E[X^2] - (E(X))^2$$

$$E[X^2] = \sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot k^2$$

$$= \sum \frac{\lambda^k e^{-\lambda}}{(k-1)!} \left(\left(k-1\right)+1\right)$$

$$= \sum \frac{\lambda^k e^{-\lambda}}{(k-1)!}(k-1) + \sum \frac{\lambda^k e^{-\lambda}}{(k-1)!}$$

$$= \lambda \underbrace{\sum \frac{\lambda^{k-1} e^{-\lambda}}{(k-1)!}(k-1)} + \lambda \sum \frac{\lambda^{k-1} e^{-\lambda}}{(k-1)!}$$

$$= \lambda \cdot \lambda + \lambda = \lambda^2 + \lambda$$

$$Var(X) = (\lambda^2 + \lambda) - \lambda^2 = \lambda$$

Randomized Algorithm : an algorithm that make random choices during its execution.
It assume the on-demand availability of uniform random bits

Generally speaking : Two types.

Las Vegas Algorithm : guarantees correctness
No guarantee of running time

Monte Carlo Algorithm :

guarantees running time
No guarantee of correctness
usually with a success probability of $\propto p < 1$

applications:

(1) Beating the adversary ✓

(2) Random Sampling

(3) Hashing ✓

(4) Existence Proof

$$X_{n+1} = (aX_n + c) \bmod m \quad 2^{32}$$

$X_0 \leftarrow$ seed