Sets ①

Cardinality $[|A|]$: Size of set

Empty set $[\emptyset]$: $\{\}$

Subset $[A \subseteq B]$: elem in A in B

Proper subset $[A \subset B]$: $A \subseteq B$, but $A \neq B$

Intersection $[A \cap B]$: both A and B

Disjoint : $A \cap B = \emptyset$

Union $[A \cup B]$: either A or B

Set Difference $[B-A (B \setminus A)]$

Natural $[N]$ Rational $[Q]$

Integer $[Z]$ Complex $[C]$

Cross Product $[A \times B]$: (u, k), $u \in A, k \in B$

Power set $[P(S)]$: set of subsets

Logic ②

1) Conjunction $[P \wedge Q]$: and

2) Disjunction $[P \vee Q]$: or

3) Negation $[\neg P]$: not

4) Implication $[P \Rightarrow Q]$: implies

  a) Contrapositive $[\neg Q \Rightarrow \neg P]$

  b) Converse $[Q \Rightarrow P]$

DeMorgan's Laws :

$\neg(P \wedge Q) \equiv (\neg P \vee \neg Q)$

$\neg(P \vee Q) \equiv (\neg P \wedge \neg Q)$

Proofs ③

a | b $2 | 10 = 5$ $b = aq$

1) Direct Proof $[P \Rightarrow Q]$

2) Proof By Contraposition
  $[\neg Q \Rightarrow \neg P] \equiv [P \Rightarrow Q]$

3) Proof By Contradiction $[P]$
  $\neg P$, show $R, \neg R$, P holds

4) Proof By Cases $[P]$
  proof result in all cases

5) Induction

Pigeonhole Principle : ✱
n pigeons, K holes
if $n > K$, at least 1 hole > 1 pigeon

Induction ④

Prove for all natural #S

1) Base Case: Eq holds for initial value

2) Inductive Hypothesis: for $n = k$
  suppose $P(k)$ holds

3) Inductive Step: Assuming Inductive
  hypothesis, show $P(k+1)$

Strong Induction
  Assume holds $0 \leq n \leq k$ for $k \geq 15$

Hyper cube
$V : 2^n$ V has n degrees

$E : \frac{n}{2} 2^n$

Edge is one bit different

Stable Matching ⑤

Propose-and-Reject Algo ✱
Loop each day until no offers rejected

Morning : job proposes to most preferable candidate
who hasn't rejected

Afternoon : candidate collects offers and put most
liked on a string, reject others

Evening : Rejected job crosses candidate who rejected

- Always halts since one job must eliminate candidate
terminate at n^2

- No rogue couples

- Lemma : every subsequent day C has job offer she likes
as much as J

- Well Ordering Principle ✱
any non-empty set of natural nums has smallest num

- Propose-and-reject is job optimal, candidate pessimal

Graph Theory ⑥

Graph $[G] = (V, E)$ set of vertices and edges

Edge : $\{u, v\}$ pair of vertices, line segments

Vertices : points in a graph

Directed Graph : $G = (V, E)$ but set of Edges
are ordered arrow (u, v)

Edge e is incident on vertices u, v and u, v
are neighbors, adjacent

$degree(u) = |\{v \in V: \{u, v\} \in E\}|$

Path : sequence of edges $\{u, v_1\}\{v_2 ...\}$ distinct

Cycle (circuit) : simple path starts and ends at
same place, distinct

Walk : sequence of edges w/ repeated vertices

Tour : walk starts and ends same vertex

Connected : If has path to reach distinct vertices

Eulerian walk/tour : uses each edge exactly once
even degree graph : all vertices have even degree

Planar : drawn in place w/o crossing

Faces : regions that subdivide plane

Euler's formula : $v + f = e + 2$ for every planar

planar graphs $e \leq 3v - 6$

Non-planar graphs can pass test

Complete graphs have max num of edges

Trees : removing edge disconnects
① connected, no cycles
② connected, n-1 edges
③ connected, removal of edge disconnects
④ no cycles, addition creates cycles

Mod Arithmetic ⑦

range $\{0, 1, ..., N-1\}$ $x \mod m$ remainder r

Bijections : $b \in B$ unique preimage $a \in A$ $f(a) = b$
1) onto (surjective) : every $b \in B$ has a $a \in A$ preimage
2) 1-to-1 (injective) : B can't have many A

Inverse : $xy \equiv 1$ $\gcd(m, x) = 1 \Rightarrow x$

$d = \gcd(m, x) = am + bx$ b is multiplicative inverse of
x mod m

CRT

unique x that satisfies $x \equiv a_1 \pmod{n_1} ... x \equiv a_i \pmod{n_i}$

$x = \sum_{i=1}^{n} a_i b_i \mod N$ where $b_i = \frac{N}{n_i} \left(\frac{N}{n_i}\right)^{-1}$

$N = \prod_{i=1}^{n} n_i$ $\left(\frac{N}{n_i}\right)^{-1}_{n_i}$ inverse $\pmod{n_i}$ of $\frac{N}{n_i}$

RSA ⑧

p, q large primes , $N = pq$ mod N

e is relatively prime to $(p-1)(q-1)$

public key : (N, e)

private key : $d =$ inverse e mod $(p-1)(q-1)$

Encryption : message X   (compute $E(x) = x^e \mod N$

Decryption : $y = E(x)$ $D(y) = y^d \mod N = x$

Fermat's Little Theorem ✱

for prime p and any $a \in \{1, 2, ..., p-1\}$ we have
$a^{p-1} \equiv 1 \mod p$

Polynomials ⑨

1) Non-zero polynomial degree d has at most d roots

2) Given d+1 pairs with x_i distinct, unique
polynomial $P(x)$ degree at most d st
$p(x_i) = y_i$ for $1 \leq i \leq d+1$

Lagrange Interpolation ✱

$$\Delta_i(x) = \frac{\prod_{j \neq i}(x - x_j)}{\prod_{j \neq i}(x_i - x_j)}$$

$$p(x) = \sum_{i=1}^{d+1} y_i \Delta_i(x)$$

$p(x) = q'(x) q(x) + r(x)$

working in $GF(m)$

polynomial degree 2 in $GF(m)$ total?

m^3 bc each coefficient can take m values

Secret Sharing

1) Any group k can figure out

2) No group $< k-1$ have any info

code = s   q is prime larger than n and s
n officials

$P(x)$ degree k-1 where $P(0) = S$ and $P(1)$
to first official, $P(2)$ to second...

1) Any k officials use lagrange interpolation to find P

2) Group k-1 cannot reconstruct

Graph Theory

max edges for vertex $\frac{n(n+1)}{2}$

Bipartite planar graph : $e = 2v - 4$ not enough to prove

bipartite : two disjoint sets, no 2 vertices of same
set are adjacent

We assume $3f \leq 2e$ for face at least 3 sides
can change $5f = 2e$

removing edge for cycle, still connected

Not Planar

$K_{3,3}$ K_5 4D cube

Stable Matching

$(n-1)^2 + 1$ at most rejections

$n(n-1)+1$ at most proposals

companies get worse candidates over time

candidates get better job offers

Proofs (Examples)

1) Sum of digits of n divisible by $9 \Rightarrow 9 | n$ (Direct)

Let n be written as $n = abc$ $n = 100a + 10b + c$

$a+b+c = 9k$ $\Rightarrow 100a + 10b + c = 9(k+11a+b)$

2) $\sqrt{2}$ is irrational (Contradiction)

Use if a^2 is even $\Rightarrow a$ is even

Must be $\sqrt{2} = a/b \Rightarrow 2 = \frac{a^2}{b^2}$ must be some $a = 2c$

Since $a^2 = 2b^2$ state a,b share no common factors

prove a,b even

3) Every $n \in \mathbb{N}$ $n \geq 12$, $n = 4x + 5y$ $x,y \in \mathbb{N}$ (Induction)

Base Case: $n = 12, 13, 14, 15$

Induction Hypo: Assume holds for all $12 \leq n \leq k$ $k \geq 15$

Prove for $n = k+1 \geq 16$ $k+1-4 \geq 4x+5y$ $x = x'+1$ $y = y'$

4) Improvement Lemma (Induction)

If job J makes offer to candidate C on kth day

every subsequent day C has job she likes as much as J

Proof: induction on i $i \geq k$

Base $(i = k)$: recieves offer, have J or better

Induction step: prove $i+1$ had offer from job J' on a

string she likes as much as J. J' proposes again $i+1$,

will either have J' or another better

5) Matching is always stable (Direct)

No job can be in a rogue couple. Consider couple

(J,C) Suppose J prefers C^* to C, C^* prefers current

job to J, (J,C^*) not rogue. made offer to C^* but C^*

likes current more. No job J in a rogue couple.

6) Matching is job/employer optimal (Contradiction)

Exists day job got rejected from optimal candidate

J rejected by C^* for J^* in $T: \{ (J,C^*), ... (J^*, C') \}$,

(J^*, C^*) is rogue C^* prefers J^* J^* made offer to C^*

7) Euler's formula: For every connected planar graph, (Induction)

$v + f = e + 2$

Induction on e Base: $e = 0$ $v = f = 1$

If tree) $f = 1$ $e = v-1$

Not tree) in cycle, take cycle delete edge reduce e and f

by 1 not changing v

8) Let m,x be $+\mathbb{Z}$ $\gcd(m,x)=1$, x has multiplicative inverse mod m (Direct)

and unique

$0, x, 2x, (m-1)x$ distinct mod m so $ax \equiv 1$ mod m for one a

Suppose $ax \equiv bx \pmod m$ then $(a-b)x \equiv 0$ $(a-b)x \equiv km$ but x,m relatively prime

$a-b$ must be integer multiple of m $a-b$ range 1 to $(m-1)$

* Need $\gcd(m,x) \equiv 1$ for inverse

9) CRT (Direct)

$\left(\frac{N}{n_i}\right)^{-1}_{n_i}$ exists $\frac{N}{n_i} = \Pi_{j \neq i}$ integer coprime n_i, inverse exists

$x \mod n_i = \left(\sum_{i=1}^{k} a_i b_i \right) \mod N$ mod n_i

$= a_i b_i \mod n_i$

$= a_i \mod n_i$

10) FLT p any $a \in \{1,2,...p-1\}$ $a^{p-1} \equiv 1 \mod p$

$S = \{1, 2, ... p-1\}$ $a, 2a, 3a, .. (p-1)a$ if $\gcd(p,a)=1$ are distinct

none of them zero $p-1$ of them $S' = \{a \mod p, 2a \mod p, .. (p-1)a \mod p\}$

$(p-1)! \mod p$ $a^{p-1}(p-1)! \mod p$ product of nums

$(p-1)! \mod p \equiv a^{p-1}(p-1)! \mod p$ $a^{p-1} \equiv 1$

p is prime every int has inverse

11) RSA $(x^e)^d = x \mod N$ $x \in \{0,1, ... N-1\}$ (Direct Cases)

$ed \equiv 1 \mod (p-1)(q-1)$ $ed = 1 + k(p-1)(q-1)$

$x^{ed} - x = x^{1+k(p-1)(q-1)} - 1 = x(x^{k(p-1)(q-1)} - 1)$ show $\equiv 0 \mod N$

1) Not multiple of p 2) multiple of p

$x \neq 0 \mod p$ FLT, $x^{p-1} \equiv 1 \mod p$ $x(x^{k(p-1)} ...)$ divisible by p

$x^{k(p-1)(q-1)} - 1 \leq 0 \mod p$

must also be divisible by q so divide by product N

12) Prime Number Theorem $\pi(n)$: primes $\leq n$ for $n \geq 17$ $\pi(n) \geq \frac{n}{\ln n}$

13) deg d poly has unique polynomial (Contradiction)

Suppose another $q(x)$ $q(x_i) = y_i$ then $r(x) = p(x) - q(x)$

r is at most degree d $r(x_i) = p(x_i) - q(x_i) = 0$ at $d+1$ points so

$r(x)$ at least $d+1$ roots

14) Euler's Totient Theorem

n and a are coprime $a^{\phi(n)} \equiv 1 \pmod n$ $\phi(n)$: # $\geq^* \leq n$ coprime to n

FLT model $\{m_1, m_2, ... m_\phi n\} = \phi(n)$ set $\{am_1, am_2, ... am_{\phi(n)}\}$

m_i and a coprime to n. Suppose shared factor p $p | n$ or $p | m_i$

Injective: $f(x) = f(y)$ $ax \equiv ay$ a has inverse

Surjective: take y prime n $f^{-1}(a^{-1}y) \equiv y \pmod n$ $f(x) = y$ $a^{-1}y$ prime n

General

Use variable to suppose things

Sets: Demorgans $\forall \exists$

$\neg(\forall(x)P(x)) \equiv \exists x (\neg P(x))$

10 Error Correcting Codes

Erasure Errors: n packets, k packets lost
   Need n+k to retrieve

① Polynomial P(x) degree n-1,
② mod q. Send P(i)=m , n+k ≤ q
③ Recover w/ any n points

Use Lagrange interpolation:
   points → Polynomial

General Errors: n packets, k packets corrupted
   Need n+2k to retrieve. Berlekamp-Welch Alg

① Polynomial P(x) degree n-1, $\in GF(q)$
② Error Locator Polynomial $E(x)=(x-e_1)(x-e_2)...(x-e_k)$
   Plug in $Q(i)=r_i E(i)$ $1 \le i \le n+2k$ where $Q(i)=P(i)E(i)$
③ Solve for error correcting E(x) errors $e_1, e_2...$
   and $P(x)=\frac{Q(x)}{E(x)}$ use long division

Distance Properties Reed-Solomon Codes
Hamming distance: positions where strings differ
$$d(\vec{s}, \vec{r}) = \sum_{i=1}^{L} 1(r_i \ne s_i) \quad \text{1 if true}$$

Min distance of two codes   d
At d/2, can impersonate two codes equally

11 Counting

First Rule Counting: succession of k choices where
   n_1 ways first choice, then for every first choice n_2 second choice
Total choices: $n_1 \times n_2 \times ... \times n_k$

Second Rule Counting: succession choices order does not matter
   Ways of choosing k elements from S in n total elements
Total: $\binom{n}{k} = \frac{n!}{n-k! \, k!}$

Ex Select multiset size k with set size n, use binary strings w/ 1 for bin edge can model $\binom{n+k-1}{k}$ k fruits

Zeroth Rule of Counting: if set A bijection set B,
   |A|=|B|

Combinatorial Proofs: Proofs by stories told from multiple points of view

Permutations: rearrangement, n! distinct ways
Derangement: Permutation w/ no fixed points

Inclusion Exclusion:
Disjoint: $|A_1 \cup A_2| = |A_1| + |A_2|$, since $|A_1 \cap A_2| = 0$
$|A_1 \cup ... \cup A_n| = \sum_{i=1}^{n} (-1)^{k-1} \sum_{S \subseteq \{1,...n\}, |S|=k} |\cap_{i \in S} A_i|$

Stirling's Approx: $n! \approx \sqrt{2\pi n} \left(\frac{n}{e}\right)^n$
   Simple: $\left(\frac{n}{e}\right)^n$

12 Countability and Computability

Bijections: f:A→B every a∈A unique image b∈f(a) b∈B preimage f(a)=b
injection(1-to-1): distinct input to distinct output
   $x \ne y \Rightarrow f(x) \ne f(y)$
surjective(onto): every element in range has preimage
   $(\forall y \exists x)(f(x)=y)$
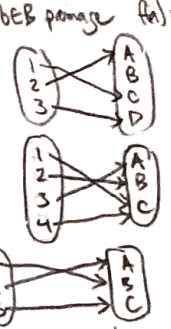
Bijection: injection and surjective

Countable set S if bijection between S and N or ⊆ N
   N, Z, Q have same cardinality
R is not using Cantor's diagonalization
Ex Enumerate real nums in infinite list diagonal = r,
we find r and 1 to every digit, must be real but is 1 num off from nth digit

No program can test if in infinite loop, self reference, cannot separate programs from data

13 Discrete Probability

Probability Space: Sample space Ω, probability P[ω]
   1) Non-negative: $0 \le P[\omega] \le 1$ for $\omega \in \Omega$
   2) Total 1: $\sum_{\omega \in \Omega} P[\omega] = 1$

Event A is subset sample space $A \subseteq \Omega$
$P[A] = \sum_{\omega \in A} P[\omega]$
Event $\bar{A}$ is complement of A $\bar{A} = 1 - A$ $A^c \cup A = \Omega$
                                                          $A \cap A^c = \emptyset$
Throw m balls into n bins n^m sample space
1) What is sample space? (experiment, possible outcomes)
2) What is probability of each outcome? (sample point)
3) Event we are interested in? (what subset of sample space)
4) Add up probabilities of sample points in it.

14 Conditional Probability, Independence, Combination

Conditional Probability of A given B, events $A, B \subseteq \Omega$
$$P[A|B] = \frac{P[A \cap B]}{P[B]}$$

Bayes Rule: Flip $P[A|B]$ $P[B|A]$ General
$$P[A|B] = \frac{P[A \cap B]}{P[B]} = \frac{P[B|A]P[A]}{P[B]} = \frac{P[B|A]P[A]}{\sum_{i=1}^{} P[B|A_i]P[A_i]}$$

Total Probability Rule
$$P[B] = P[A \cap B] + P[\bar{A} \cap B] = P[B|A]P[A] + P[B|\bar{A}]P[\bar{A}]$$
$$P[A|B] = \frac{P[B|A]P[A]}{P[B|A]P[A] + P[B|\bar{A}](1-P[A])}$$

Where H is partitioned $A_1 \cup A_2 \cup ... \cup A_n$
   Total Prob Rule: $P[B] = \sum_{i=1}^{} P[B|A_i]P[A_i]$

Independent: $P[A \cap B] = P[A] \cdot P[B]$
$P[A|B] = \frac{P[A \cap B]}{P[B]} = P[A]$

Mutual Independence: Events $A_1, \ldots, A_n$ $B_i \in \{A_i, \bar{A}_i\}_{i=1-n}$

$$P[B_1 \cap \ldots \cap B_n] = \prod_{i=1}^{n} P[B_i]$$

Pairwise Independence: each pair is independent

Mutual Independence $\underset{\Leftarrow}{\Rightarrow}$ Pairwise Independence

Product Rule (not Mutually independent)

$$P[\cap_{i=1}^{n} A_i] = P[A_1] \cdot P[A_2 | A_1] \times \ldots \times P[A_n | \cap_{i=1}^{n-1} A_i]$$

Principle Inclusion-Exclusion: $A_1, \ldots, A_n$ probability space

$$P[A_1 \cup \ldots \cup A_n] = \sum_{k=1}^{n} (-1)^{k-1} \sum_{S \subseteq \{1, \ldots, n\} : |S|=k} P[\cap_{i \in S} A_i]$$

$$P[\cup_{i=1}^{n} A_i] = \sum_{i=1}^{n} P[A_i] - \sum_{i<j} P[A_i \cap A_j] + \sum_{i<j<k} P[A_i \cap A_j \cap A_k] + (-1)^{n-1} P[\cap A_i]$$

Mutually Exclusive: $A_1, \ldots, A_n$ $(A_i \cap A_j = \emptyset$ all $i,j)$

$$P[\hat{\cup}_{i=1}^{n} A_i] = \hat{\sum}_{i=1}^{n} P[A_i]$$

Union Bound: $A_1, \ldots, A_n$ all $n \in \mathbb{Z}^+$

$$P[\hat{\cup}_{i=1}^{n} A_i] \leq \hat{\sum}_{i=1}^{n} P[A_i]$$

⑮ Random Variables

Random variable: depends on outcome of probabilistic experiment

X in Ω for $X: \Omega \to \mathbb{R}$ $X(\omega)$ for all $\omega \in \Omega$

Distribution of X is collection of values $\{(a, P[X=a]) : a \in A\}$

The collection of events form partition

Bernoulli Distribution: take s in $\{0,1\}$

$$P[X=i] = \begin{cases} p & \text{if } i=1 \\ 1-p & \text{if } i=0 \end{cases} \qquad X \sim \text{Bernoulli}(p)$$

Binomial Distribution: values of X, prob of $X=i$ sum of sample pts

$$\binom{n}{i} \text{ and } p^i(1-p)^{n-i}$$

$$P[X=i] = \binom{n}{i} p^i (1-p)^{n-i} \qquad X \sim \text{Bin}(n, p)$$

Hypergeometric Distribution: sample w/o replacement, not independent

$$P[Y=k] = \binom{n}{k} \frac{\frac{B!}{(B-k)!} \cdot \frac{(N-B)!}{(N-B-(n-k))!}}{\frac{N!}{(N-n)!}} = \frac{\binom{B}{k}\binom{N-B}{n-k}}{\binom{N}{n}}$$

$N = B+W$ balls sample $n \leq N$ $\qquad Y \sim \text{Hypergeometric}(N, B, n)$

Joint Distribution X and Y $\{((a,b), P[X=a, Y=b]) : a \in A, b \in B\}$

marginal distribution $P[X=a] = \sum_{b \in B} P[X=a, Y=b]$

RV X and Y independent: $P[X=a, Y=b] = P[X=a] P[Y=b]$

Indicator RV $I_1, \ldots, I_n$ mutually independent

Summarize distribution w/ Expectation

Expectation discrete RV X sum over all possible values "typical" value

$$E[X] = \sum_{a \in A} a \times P[X=a]$$

Linearity of Expectation: $E[X+Y] = E[X] + E[Y]$

$$E[cX] = cE[X]$$

Geometric Distribution: how long before event happens

$$P[X=i] = (1-p)^{i-1} p \qquad X \sim \text{Geometric}(p)$$

General

- Binary String to Solve balls bins
- Inclusion Exclusion to flip and find $P[A \cap B \cap C]$
- del powers determine d degree polynomial
- $E(x) = x - e_1$ where e_1 is x val of corrupted packet
- Not all polynomials have d roots
- Use symmetry when you can

16 Variance and Covariance

Variance: For RV X w/ $E[X] = \mu$,

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

Standard Deviation

$$\sigma(X) := \sqrt{Var(X)}$$

Independent RV $X = X_1 + X_2 + \ldots + X_n$ if $X_i = X_j$

$$Var(X) = \sum_{i=1}^{n} Var(X_i) = n\,Var(X_i)$$

$$\sigma(X) = \sqrt{n} \cdot \sigma(X_i)$$

$$E[X] = n\,E[X_i]$$

For RV X,Y

$$E[XY] = E[X]E[Y] \quad Var(X+Y) = Var(X) + Var(Y)$$

Covariance

$$Cov(X,Y) = E[XY] - E[X]\cdot E[Y]$$

$$Var(X+Y) = Var(X) + Var(Y) + 2Cov(X,Y)$$

19 Geometric, Poisson Distributions

Geometric: tossing tails for i-1 before heads with

$$P[X=i] = (1-p)^{i-1} p \qquad X \sim Geometric(p)$$

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

Poisson: avg num λ per time or space determines prob func

$$P[X=i] = \frac{\lambda^i}{i!} e^{-\lambda} \qquad X \sim Poisson(\lambda)$$

$$E[X] = \lambda \qquad\qquad Var(X) = \lambda$$

Independent Poisson RV

Let $X \sim Poisson(\lambda)$ and $Y \sim Poisson(\mu)$

$$X+Y \sim Poisson(\lambda + \mu)$$

Similar to $Binomial(n, \frac{\lambda}{n})$

17 Concentration Inequalities & Law of Large Nums

Markov's Inequality

For nonnegative RV X $X(\omega) \geq 0$ ∀ $\omega \in \Omega$, c constant

$$P[X \geq c] \leq \frac{E[X]}{c}$$

Chebyshev's Inequality   iid

RV X w/ finite expectation $E[X] = \mu$ constant c

$$P[|X - \mu| \geq c] \leq \frac{Var(X)}{c^2}$$

$$P[|X-\mu| \geq k\sigma] \leq \frac{1}{k^2} \qquad \text{where} \qquad \sigma = \sqrt{Var(X)}$$

Law of Large Numbers

for iid $X_1, X_2, X \ldots$ $S_n = X_1 + X_2 + \ldots + X_n$ $E[X_i] = \mu$

$$P[|\tfrac{1}{n}S_n - \mu| < \varepsilon] \to 1 \qquad n \to \infty$$

20 Continuous Probability Distributions

No longer probability points, but intervals

Probability Density Function (pdf)   "probability per unit length"

For RV X is func $f: R \to R$

1. f is nonnegative. $f(x) \geq 0$ for all $x \in R$
2. The total integral of f is equal to 1: $\int_{-\infty}^{\infty} f(x)\,dx = 1$

$$P[a \leq X \leq b] = \int_a^b f(x)\,dx \quad \text{for all} \quad a < b$$

Cumulative Distribution Function (cdf)

$$F(x) = P[X \leq x] = \int_{-\infty}^{x} f(z)\,dz$$

$$pdf: f(x) = \frac{dF(x)}{dx}$$

$$E[X] = \int_{-\infty}^{\infty} x f(x)\,dx$$

$$Var(X) = E[X^2] - E[X]^2 = \int_{-\infty}^{\infty} x^2 f(x)\,dx - \left(\int_{-\infty}^{\infty} x f(x)\,dx\right)^2$$

Joint Distribution   "probability per unit area"

2 RV X,Y is func $f: R^2 \to R$

1. f is nonnegative $f(x,y) \geq 0$
2. total integral equals 1: $\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f(x,y)\,dx\,dy = 1$

$$P[a \leq X \leq b, c \leq Y \leq d] = \int_c^d \int_a^b f(x,y)\,dx\,dy$$

Independence

$$P[a \leq X \leq b, c \leq Y \leq d] = P[a \leq X \leq b]\,P[c \leq Y \leq d]$$

Marginal Dist   Conditional

$$f_X(x) = \int_{-\infty}^{\infty} f(x,y)\,dy \qquad\qquad f_{Y|X}(y|x) = \frac{f(x,y)}{f_X(x)}$$

Exponential Distribution

Continuous version of geometric

$$f(x) = \begin{cases} \lambda e^{-\lambda x} & \text{if } x \geq 0 \\ 0 & \text{ow} \end{cases} \qquad X \sim Exp(\lambda)$$

$$E[X] = \frac{1}{\lambda} \qquad\qquad Var(X) = \frac{1}{\lambda^2}$$

Normal Distribution

for any $\mu \in \mathbb{R}$ and $\sigma > 0$, cont RV X

$$f(x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-(x-\mu)^2/(2\sigma^2)} \qquad X \sim N(\mu, \sigma^2)$$

Standard normal distribution $\mu = 0, \ \sigma^2 = 1$

If $X \sim N(\mu, \sigma^2)$, then $Y = \frac{X - \mu}{\sigma} \sim N(0,1)$ $\Longleftrightarrow$

If $Y \sim N(0,1)$ then $X = \sigma Y + \mu \sim N(\mu, \sigma^2)$

$$E[X] = \mu \qquad\qquad Var(X) = \sigma^2$$

Can relate to $N(0,1)$ by $P[X \leq a] = P[Y \leq \frac{a - \mu}{\sigma}]$

Independent Normal RV

Let $X \sim N(\mu_x, \sigma_x^2)$ and $Y \sim N(\mu_y, \sigma_y^2)$

RV $Z = aX + bY$ normally distributed

$$\mu = a\mu_x + b\mu_y \qquad \sigma^2 = a^2\sigma_x^2 + b^2\sigma_y^2$$

㉑ Central Limit Theorem

Distribution of sample avg $\frac{S_n}{n}$ for large enough n looks like normal distribution w/ mean μ var $\frac{\sigma^2}{n}$

50% of mass in width 0.67σ of either side

99.7% in interval width 3σ either side

CLT

Let X_1, X_2 be sequence of iid w/ $E[X] = \mu$ $Var = \sigma^2$

Let $S_n = \sum_{i=1}^{n} X_i$ $\frac{S_n - n\mu}{\sigma\sqrt{n}}$ conv to $N(0,1)$ as $n \to \infty$

$$P\left[\frac{S_n - n\mu}{\sigma\sqrt{n}} \leq C\right] \to \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{c} e^{-\frac{x^2}{2}} dx \qquad n \to \infty$$

Don't use for probabilities smaller then $O(\frac{1}{\sqrt{n}})$

Approx finite n

Expectation

$$E[X] = \sum_i i \cdot P[x = i]$$

$$E[X + Y] = E[X] + E[Y]$$

$$E[cX] = c E[X]$$

Variance

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

$$Var(cx) = c^2 Var(x)$$

$$Var(x + y) = Var(x) + Var(y) + 2Cov(X, Y)$$

Independent

$$P[X = a, Y = b] = P[X = a]P[Y = b]$$

$$E[XY] = E[X]E[Y]$$

$$Var(x + y) = Var(x) + Var(y)$$

$$P[A \cap B] = P[A]P[B] \qquad P[A|B] = P[A]$$

Distribution Formulas

Binomial	$X \sim Bin(n, p)$	$\binom{n}{i} p^i (1-p)^{n-i}$	$E[X] = np$	$Var(x) = np(1-p)$
Geometric	$X \sim Geometric(p)$	$p(1-p)^{i-1}$	$E[X] = \frac{1}{p}$	$Var(x) = \frac{1-p}{p^2}$
Poisson	$X \sim Poisson(\lambda)$	$\frac{\lambda^i}{i!} e^{-\lambda}$	$E[X] = \lambda$	$Var(x) = \lambda$
Bernoulli	$X \sim Bernoulli(p)$	$\begin{cases} p & \text{if } i=1 \\ 1-p & \text{if } i=0 \end{cases}$	$E[X] = p$	$Var(x) = p(1-p)$

Cont

Exponential	$X \sim Exp(\lambda)$	$f(x) = \lambda e^{-\lambda x}$ if $x \geq 0$	$E[X] = \frac{1}{\lambda}$	$Var(x) = \frac{1}{\lambda^2}$
Normal	$X \sim N(\mu, \sigma^2)$	$f(x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-(x-\mu)^2/(2\sigma^2)}$	$E[X] = \mu$	$Var(x) = \sigma^2$
Uniform	interval $[0, \ell]$	$f(x) = \frac{1}{\ell}$	$E[X] = \frac{\ell}{2}$	$Var(x) = \frac{\ell^2}{12}$