Statement: $3=5$

Predicate: $n>3$, $n=3$

Expression: $x+y$

$A \Rightarrow B \equiv \neg A \vee B$

$\neg(A \vee B) \equiv (\neg A \wedge \neg B)$

$\forall x\,(P(x) \wedge Q(x)) \equiv \forall x\, P(x) \wedge \forall x\, Q(x)$

Sum of degrees is $2e$.

$e \leq 3v-6$ for any planar graph where $v > 2$

Average degree: $\frac{2e}{v}$

Complete graph: $\frac{n(n-1)}{2}$ edges, n = number of vertices

Tree: $n-1$ edges.

Hypercube: Rudrata Cycle: cycle that visits every node.

- 2^n vertices
- $n \cdot 2^{n-1}$ edges.

$$\forall x\, \exists y\, (P(x,y) \wedge \neg Q(x,y))$$
$$\equiv \forall x\, \exists y\, \neg(\neg P(x,y) \vee Q(x,y))$$
$$\equiv \forall x\, \exists y\, \neg(P(x,y) \Rightarrow Q(x,y))$$
$$\equiv \neg \forall y\, \exists x\, (P(x,y) \Rightarrow Q(x,y))$$

True $\Longleftrightarrow$ 1 of $x, y,$ or z are true

$$(X \wedge \neg Y \wedge \neg Z) \vee (\neg X \wedge Y \wedge \neg Z) \vee (\neg X \wedge \neg Y \wedge Z)$$

In SMZ, no man may get his favorite women

Planar Drawing

- each edge adjacent to at most 2 faces
- minimum length cycle 6, each face adjacent to ≥ 6 edges

$6f \leq 2e$

$V+F=2+E$

Contradiction – useful to prove something that DNE

Well-Ordering Principle – always a "first"

Optimal Partner – best partner in stable pairing.

Planar – drawn on plane w/out crossings

1-1: injective

onto: surjective.

FLT: For any prime p and any $a \in \{1, 2, \dots p-1\}$, we have $a^{p-1} \equiv 1 \bmod p$.

e.g. $3^{5000} \bmod 11 = (3^{10})^{500} \bmod 11$
$= 1^{500} \bmod 11 = 1$

$$\left.\begin{array}{l} n^7 \equiv n \bmod 7 \\ n^3 \equiv n \bmod 3 \\ n^2 \equiv n \bmod 2 \end{array}\right\} \rightarrow n^7 \equiv n \bmod 7\cdot3\cdot2 = n \bmod 42$$

$\exists$ Bijection if $\exists$ multiplicative inverse unique

$f: X \rightarrow Y$

onto: every $y \in Y$ has at least one $x \in X$ such that $f(x) = y$

1-1: every $y \in Y$ is mapped to from at most one $x \in X$

CRT: $x \equiv a_1 b_1 \frac{M}{m_1} + \dots + a_r b_r \frac{M}{m_r} \bmod M$

$M = m_1 \cdot m_2 \cdots m_r$

$b_i \frac{M}{m_i} \equiv 1 \bmod m_i$

If $x \equiv a \bmod p$ and $x \equiv a \bmod q$, $x \equiv a \bmod pq$.

CS70

Tree: total degrees = 2e

n vertices, n-1 edges

no cycles

connected

removal of any edge disconnects

addition of any edge creates cycle

Depth - edges to leaf.

cycle: sequence of edges where $v_1 \dots v_n$ are distinct ↳ except for last
-starts and ends at same vertex

walk: sequence of edges w/ repeated vertices

tour: walk that starts and ends at same vertex

Eulerian walk: walk that uses each edge once | 0 or 2 odd degree vertices

Eulerian tour: ↑ ends at starting point.

-iff even degree and connected

visits every edge once.

$d \mid x \rightarrow x = ld,\ l \in \mathbb{Z}$ || $d \mid a \wedge d \mid b \Rightarrow d \mid a-b$

rational $\rightarrow r = \frac{a}{b},\ a,b \in \mathbb{Z}$

even: $a = 2k$, odd: $a = 2k+1$

Simple Path: Sequence of edges where vertices are distinct

- # edges removed to disconnect hypercube ≥ # vertices in smaller side, post removal

Hamiltonian Path: path that visits each vertex exactly once

Simple path between every pair of vertices

→ connected

→ acyclic (no cycle)

-w/ cycle, at least two simple paths X

→ connected, acyclic = tree.

There exists pairings in which where more than one man is matched to his least favorite partner is unstable

-max number of solutions for x in range $\{0, N-1\}$ for equation $ax \equiv b \pmod N$ is d, $\gcd(a, N) = d$.

-crossing edges → remove edge.

$13x = 5 \pmod{46}$

$\gcd(46, 13)$ $46 = 3 \cdot 13 + 7$ $7 = 46 - 3 \cdot 13$

$\gcd(13, 7)$ $13 = 1 \cdot 7 + 6$ $6 = 13 - 1 \cdot 7$

$\gcd(7, 6)$ $7 = 1 \cdot 6 + 1$ $1 = 7 - 1 \cdot 6$

$\gcd(6, 1)$ $6 = 6 \cdot 1 + 0$

$\gcd(1, 0)$

$1 = 7 - 1(13 - 1 \cdot 7)$

$= 2 \cdot 7 - 1 \cdot 13$

$1 = 2(46 - 3 \cdot 13) - 1 \cdot 13$

$1 = 2 \cdot 46 - 7 \cdot 13$

$x \equiv y \pmod m$

$\Leftrightarrow m \mid (x - y)$

$\Leftrightarrow x, y$ have same remainder wrt m

$\Leftrightarrow \boxed{x = y + km}$ for $k \in \mathbb{Z}$

Mod - isolate x by multiplying by multiplicative inverse

$4x = 5 \pmod 7$ | ∃ mi only if x, m are relatively prime.

$2 \cdot 4x = 2 \cdot 5 \mod 7$

$8x = 10 \mod 7$

$x = 3 \mod 7$

1-1 - unique input for each output

onto - size of domain / codomain are the same

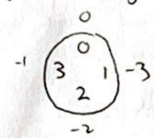
Euclid's Algorithm

$\gcd(x, y) = \gcd(y, \operatorname{mod}(x, y))$

$\gcd = 2, \rightarrow \gcd(2, 0)$

Bijection - $\gcd(a, m) = 1$

$-3 \mod 4 = 1$



Compute mod: $a = b\left(\frac{a}{b}\right) + r$

$x = r$

Euclid's Algorithm

$\gcd(16, 10)$

$16 = 10 \cdot 1 + 6 \rightarrow 6 = 16 - 10 \cdot 1$

$10 = 6 \cdot 1 + 4$ $4 = 10 - 6 \cdot 1$

$6 = 4 \cdot 1 + 2$

$4 = 2 \cdot 2 + 0 \rightarrow 2 = 6 - 4 \cdot 1$

$2 = \cancel{16 - 10 \cdot 1}\ 6 - (10 - 6 \cdot 1) \cdot 1$

$= -10 + 6 \cdot 2$

$2 = -10 + (16 - 10 \cdot 1) \cdot 2$

$= 2 \cdot 16 - 10 \cdot 3$

$2x - 3y$

$x = 2, y = -3$

$\gcd(8, 22)$ $22 = 2 \cdot 8 + 6$

$\gcd(8, 6)$ $8 = 1 \cdot 6 + 2$

$\gcd(6, 2)$ $6 = 2 \cdot 3 + 0$

$\gcd(2, 0)$ $a_i = q_i \cdot b_i + r_i$

$\gcd(x, y) = ax + by$

$x \mod n$

$1 = \gcd(n, x) = an + bx$

$bx \equiv 1 \mod n$, b is MI

$a^{(p-1)(q-1)} = 1 \mod pq$

uncorrelated.

If X and Y are independent, $cov(X,Y) = 0$

$E[(X-E(X))(Y-E(Y))]$

$cov(X,Y) = E(XY) - E(X)E(Y)$ If terms independent, cov = 0.

$E(XY) = \sum_{x,y} xy \Pr(X=x, Y=y)$

↳ all possible combinations

$L(Y|X) = E(Y) + \frac{cov(X,Y)}{var(X)}(X - E(X)) = E(Y)?$

Projection Property: $E[(Y-L(Y|X))X] = 0$

$E(Y - L(Y|X)) = 0$

$L(Y|X) = a + bx$ is projection of Y on $\mathcal{L}(X)$

if $Y - L(Y|X) \perp$ every linear function of X, i.e.

$E((Y-a-bX)(c+dX)) = 0, \forall c, d \in \mathbb{R}$

$E(Y) = a + bE(X)$, $E((Y-a-bX)X) = 0$

$E(X|Y) = \sum_x x \Pr(X=x|Y)$ | $\Pr(X=x|Y=y) = \frac{\Pr(X=x, Y=y)}{\Pr(Y=y)}$

Counting

Anagram: $\frac{\text{total \# letters}}{r_1! r_2! \ldots r_w!}$ e.g. Anaconda $\frac{8!}{3!2!}$

Order matters: $n_1 \cdot n_2 \cdot n_3 \cdot \ldots \cdot n_k$ || w/ replacement, $n_1 = n_2 = n_k$ ∴ n^k

Order doesn't: $\binom{n}{k}$ ~~[illegible]~~? -less

cards - consider suits/values differently

~~Dart/unit circle~~

Halting

Wrapper(P) → program used to solve question

TestHalt → program that tests halting on P(x)

Wrapper(TestHalt)

equally likely to be fair or biased ... flip twice + get 2 T's
$\Pr(H) = 0.7$.

e.g. F: # additional flips

$E(F|e) = E(F|e, fair)P(fair|e) + E(F|e, biased)P(biased|e)$

Bayes... $\Pr(fair|e) = \frac{\Pr(e|fair)\Pr(fair)}{\Pr(e|fair)\Pr(fair) + \Pr(e|biased)\Pr(biased)}$

$= \frac{\frac{1}{4}(\frac{1}{2})}{\frac{1}{4}(\frac{1}{2}) + (\frac{3}{10})^2(\frac{1}{2})}$

$\Pr(biased|e) = 1 - \uparrow$

By memoryless property, $E(F|e, fair) = E(F|fair)$

geometric distribution...

$E(F|e) = 2(\frac{25}{34}) + \frac{10}{7}(\frac{9}{34})$

Conditional Expectation

$E(Y|X=x) = \sum_y y \cdot P(Y=y|X=x)$

$E(Y|X)$ is function of X, $E(Y|X=x)$ is specific value.

$E[a_1 Y_1 + a_2 Y_2 | X] = a_1 E_1(Y_1|X) + a_2 E(Y_2|X)$

$E(h(X) \cdot Y | X) = h(X) \times E[Y|X]$

X, Y independent $\Rightarrow E(Y|X) = E(Y)$

$E(Y) = \sum_x E(Y|X=x) = E(E(Y|X))$

$MSE = E((Y-g(X))^2) = \sum_{x,y} (y - g(x))^2 P(X=x, Y=y)$

Covariance

$cov(X,X) = E(X^2) - E^2(X) = Var(X)$

$cov(X, aY+b) = a \cdot cov(X,Y)$

$cov(X, Y+Z) = cov(X,Y) + cov(X,Z)$

$Var(X+Y) = cov(X+Y, X+Y) = var(X) + var(Y) + 2cov(X,Y)$

Markov Chains

irreducible - there exists some path between every pair of states
- always has unique invariant distribution

aperiodic - length of all paths starting at X_i and ending at X_i has GCD 1.

periodicity - what period occurrence of state has
e.g. period 2: can be on even/odd, but not both

invariant - $\pi_n = \pi_0, \forall n \geq 0$ (stationary) $\pi P = \pi$

balance equations:

$\pi(1), \pi(2), \pi(3) \ldots, \pi(n) = \pi(1) \ldots \pi(n) \begin{bmatrix} \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{bmatrix}$

e.g.

	1	2	3
1	0	1	0
2	2/3	0	1/3
3	0	1	0

$\pi(1) = \frac{2}{3}\pi(2)$

$\pi(2) = \pi(1) + \pi(3)$

$\pi(3) = \frac{1}{3}\pi(2)$

Long term fraction - solve $\pi(n)$

$\rightarrow \pi(1) + \ldots + \pi(n) = 1$

expected time = hitting time

Hitting time - Probability of going to everything that you can transition to from x.

$E(X_n)$ - calculate

$= E(X_n | X_{n-1}) \overset{K}{\sum}$ possible values of $X_n \cdot \Pr(\text{value})$

Replace k w/ X_{n-1}

↳ $E(X_n | X_{n-1}) = f(X_{n-1})$

↳ $E(E(X_n|X_{n-1})) = E(X_n) = E(f(X_{n-1}))$

Plug in X_1, X_2, X_3 (find for each)

Find pattern

Continous

$F(x)$ is integral of $f(x)$

cdf: F

$\underbrace{Pr(a < x < b)}_{\text{cdf}} = \int_a^b \underbrace{f(x)}_{\text{pdf}} \, dx$

cdf is Pr.

CDF - probability for expo.

PDF: 1) non-negative on its domain; $0 < x < a$

2) Integral of PDF = 1

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

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

Tail Sum: X - Continous, non-negative

$E(X) = \int_0^\infty P(X > x) \, dx$

Joint PDF: $f_{X,Y}(x,y) : \mathbb{R}^2 \to \mathbb{R}$

- $\forall x,y \;\; f(X,Y)(x,y) > 0$
- $\int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f_{X,Y}(x,y) \, dy \, dx = 1$

$P(a \le X \le b, c \le Y \le d) = \int_a^b \int_c^d f_{X,Y}(x,y) \, dy \, dx$

Independence:

$P(a \le x \le b, c \le Y \le d) = P(a \le X \le b) \, P(c \le Y \le d)$

$f_{X,Y}(x,y) = f_X(x) f_Y(y)$

Dart/unit circle - $2x \, 1\{0 \le x \le 1\}$

$f_X(x) = 2x$

CLT: $A_n' = \dfrac{\sum_{i=1}^n X_i - n\mu}{\sigma\sqrt{n}}$ ← mean from one Bernoulli variable

SD

50% of mass within 0.67σ on either side of mean

99.7% within 3σ

height: $x = \mu$, $\frac{1}{\sqrt{2\pi\sigma^2}} \approx \frac{0.4}{\sigma}$

Uniform $U(a,b)$

$f(x) = \frac{1}{b-a}, \quad a \le x \le b$

$F(x) = 0, \quad x < a$

$\frac{x-a}{b-a}, \quad a < x < b$

$1, \quad x > b$

$E(X) = \frac{a+b}{2}$

$Var(X) = \frac{1}{12}(b-a)^2$

Expo.

min of Exp(λ) var

$= \exp(\Sigma_i \lambda)$

$E(T) = \int_0^\infty 1 - F_T(t) \, dt$

Expo(λ)

. memoryless

$f(x) = \lambda \cdot e^{-\lambda x}$

$F(x) = 1 - e^{-\lambda x}$

$E(X) = \frac{1}{\lambda}$

λ = rate of occurence

$Var(X) = \frac{1}{\lambda^2}$

Gaussian/Normal $N(\mu, \sigma^2)$

- any unspecified distribution will converge to Gaussian

Mean: μ, Var: σ^2

$f(x|\mu,\sigma^2) = \frac{1}{\sigma\sqrt{2\pi}} e^{\frac{-(x-\mu)^2}{2\sigma^2}}$

$P(X \ge m) = \int_m^\infty \lambda e^{-\lambda x} dx = e^{-\lambda m}$

$P(X \le m) = \int_0^m \lambda e^{-\lambda x} dx = 1 - e^{-\lambda m}$

X_1, X_2 independent

$\to P(X_1 > a, X_2 > b) = P(X_1 > a) \, P(X_2 > b)$

$E(X) = \int x f_X(x) \, dx$

Minimum of two independent Exp(λ) $= \text{Exp}(2\lambda)$

$G_1(X) = 1 - F(X) = e^{-x}$

Memoryless Property:

$Pr(X > t+s \mid X > s)$

$= \frac{Pr(X > t+s, X > s)}{Pr(X > s)}$

$= \frac{Pr(X > t+s)}{Pr(X > s)}$

$= \frac{e^{-(t+s)}}{e^{-s}}$

$= e^{-t} = Pr(X > t)$

For any indicator, expectation = probability.

CLT: 95% confidence within 2 SD of mean | for large n, mean μ, & Var $\frac{\sigma^2}{n}$ | height @ $\mu = \frac{1}{\sqrt{2\pi\sigma^2}}$

50% within 0.67σ

99.7% 3σ

RSA

$E(x) = x^e \bmod N$, $N = pq$

$D(x) = x^d \bmod N$, e relatively prime $(p-1)(q-1)$

$d = MI$, $e \bmod (p-1)(q-1)$

$ed = 1$

$D(E(x)) = x \bmod N$

$\hookrightarrow (x^e)^d = x \bmod N$

$ed = 1 \bmod (p-1)(q-1)$

$x^{ed} - x = x^{1+k(p-1)(q-1)} - x$

$= x(x^{k(p-1)(q-1)} - 1) = 0 \bmod N$

$N = pq \rightarrow$ show divisible by p and q

Case 1: $p \mid x$, $q \mid x$

Case 2: $x^{p-1} \equiv 1 \bmod p$

$(x^{p-1})^{k(q-1)} \equiv 1^{k(q-1)}$

$\Rightarrow x^{k(p-1)(q-1)} - 1 \equiv 0 \bmod p.$

FLT $a^{(p-1)(q-1)} \equiv 1 \bmod pq$ if (a, pq) coprime

$x^{p-1} = 1 \bmod p$. if x coprime p

$x^p = 1 \bmod p$

$x^{(p-1)(q-1)} = 1 \bmod p \cdot q$

Secret Sharing:

$\geq k$ people can figure out

$\deg = k-1$

Watch out for $GF(7)$

e.g. $\frac{(x-4)(x-5)}{2} = 4(x-4)(x-5) \bmod 7.$

$2 \cdot 4 = 1$ MI

$\frac{1}{(4)} \bmod 7 = 2.$

$\hookrightarrow x$ what $= 1 \bmod GF$

Interpolation:

$p(x) = P(1)\Delta_1 + P(2)\Delta_2 + \ldots$

Errors Erasure: n = send, k = lost

use polynomial deg $n-1$

$n+k$ packets

$q > n+k$ $GF(q)$

General

$P(x) = \frac{Q(x)}{E(x)}$

$E(x) = (x-e_1)\ldots(x-e_k)$ position of errors.

$Q(x) = r_x E(x)$

received value.

of degree $1 + \deg P(x)$

Set S is countable iff bijection between S and $\mathbb{N}$

	F	F	I
inf	C.I.	f	F

$\overset{F}{\overline{}}$ inf $\mid$ C.I. $\quad$ f $\mid$ F $\quad$ I $\mid$ I

---

pq Set $\{0 \ldots pq-1\}$

q numbers divisible by p

p numbers divisible by q

Deg n polynomial defined by $n+1$ pts.

Sample Space - pool of outcomes

Events - one event in sample space

Bayes $P(A \mid B) = \frac{P(A \cap B)}{P(B)}$ MLE: $B \mid A_n$, max A_n; MAP: $A_n \mid B$

$P(A \cap B) = P(A)P(B \mid A)$

$= P(B) \cdot P(A \mid B)$

$P(A \mid B) = \frac{P(B \mid A)P(A)}{P(B)}$

+ correlation: $Pr(A \cap B) > Pr(A)Pr(B)$

− correlation: $Pr(A \cap B) < Pr(A)Pr(B)$

Total: $P(B) = P(A \cap B) + P(\bar{A} \cap B)$

$= P(B \mid A) \cdot P(A) + P(B \mid \bar{A})(1 - P(A))$

$= P(A) \cdot P(B \mid A) + P(\bar{A}) \cdot P(B \mid \bar{A})$

Bayes $Pr(A \mid B) = \frac{Pr(B \mid A)Pr(A)}{1 + Pr(B \mid \bar{A})}$ $Pr(\bar{A})$

Independence: $P(A) = P(A \mid B)$

$P(A \cap B) = P(A) \cdot P(B)$

Write down all known probabilities

Product Rule for sequence of choices.

$Pr(\cap_{i=1}^n A_i) = Pr(A_1) \cdot Pr(A_2 \mid A_1) \cdot Pr(A_3 \mid A_1 \cap A_2) \cdots Pr(A_n \mid \cap_{i=1}^{n-1} A_i)$

$Pr(\cup_{i=1}^n A_i) = \sum_{i=1}^n Pr(A_i) - \sum_{(i,j)} Pr(A_i \cap A_j) + \sum_{(i,j,k)} Pr(A_i \cap A_j \cap A_k) \ldots$

e.g. $Pr(A_1 \cup A_2 \cup A_3) = Pr(A_1) + Pr(A_2) + Pr(A_3)$
$- Pr(A_1 \cap A_2) - Pr(A_1 \cap A_3)$
$- Pr(A_2 \cap A_3) + Pr(A_1 \cap A_2 \cap A_3)$

Disjoint: (mutually exclusive): $P(A \cap B) = 0$

$Pr(\cup_{i=1}^n A_i) = \sum_{i=1}^n Pr(A_i)$

Union Bound $Pr(\cup_{i=1}^n A_i) \leq \sum_{i=1}^n Pr(A_i)$

e.g. no collisions

Find all possible pairs, enumerate.

m keys, n location

$k = \binom{m}{2} = \frac{m(m-1)}{2}$ possible pairs

$Pr(A_i)$ (collision) $= \frac{1}{n}$.

$Pr(\bar{A}) \leq \sum_{i=1}^k Pr(A_i) = k \cdot \frac{1}{n} = \frac{m(m-1)}{2n}$

Mutually Independent: All are independent of each other.

$Pr(\cap_{i \in I} A_i) = \prod_{i \in I} Pr(A_i)$

Mutual Independence $\Rightarrow$ pairwise independence.

$\hookrightarrow$ only pairs.

$A \Rightarrow B$

$Pr(A \cap B) = Pr(A)$

If $Pr(A \mid B) > Pr(A)$, $Pr(B \mid A) > Pr(B)$

$E[X^2 - X] \geq -1$

If $Pr(A) > Pr(\bar{A})$, $Pr(A \mid B) \geq Pr(\bar{A} \mid B)$ False.

k indistinguishable items among n slots

Balls/bins $\rightarrow$ Stars/bars. n bins, k balls $\binom{n+k-1}{n-1}$

$\binom{n}{k} = \frac{n!}{k!(n-k)!}$

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

$= E(X^2) - (E(X))^2$

$Var(X+Y) = var(X) + var(Y) + 2cov(X,Y)$

$E(X^2) = \sum_{i=1}^{n} E(X_i^2) + \sum_{i \neq j} E(X_i X_j)$

$E(X_i^2) = Pr(X_i = 1)$ = Probability X_i is as desired

$Var(cX) = c^2 Var(X)$

Independent R.V.

X, Y are independent iff $X=a$, $Y=b$ are independent $\forall a, b$.

$Pr(X=a, Y=b) = Pr(X=a) Pr(Y=b)$ $\forall a, b$.

$Var(X+Y) = Var(X) + Var(Y)$

I.R.V.

$E(XY) = E(X) E(Y)$

		$E(X)$	$Var(X)$
Binomial	$P(X=k) = \binom{n}{k} p^k (1-p)^{n-k}$	np	$np(1-p)$ num successes
Geometric	$P(X=k) = (1-p)^{k-1} p$	$\frac{1}{p}$	$\frac{1-p}{p^2}$ how long b4 success
Poisson	$P(X=k) = \frac{\lambda^k}{k!} e^{-\lambda}$	λ	λ averages; $=\lambda$

$p = \frac{1}{2}$ maximizes variance

Coupon Collector - collect n.

$E(X) = n(\ln n + \gamma)$, $\gamma = 0.5772$.

Linearity of Expectation.

$E(X+Y) = E(X) + E(Y)$

$E(cX) = cE(X)$

$E(c) = c$

constant

"Roll a die n times. X_n be average num rolls."

$var[X_n] = \frac{1}{n} var[X_1]$

$x_1 = 4$, $x_2 = 3$ ...

$var[X_n] = var\left(\frac{x_1 + x_2 + \ldots + x_n}{n}\right)$

Taylor Series: $e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \ldots$

$n \geq \frac{1}{4\varepsilon^2 \delta}$, ε = error, δ = confidence

Chebyshev's Inequality:

$Pr[|X-\mu| \geq \alpha] \leq \frac{Var(X)}{\alpha^2}$, $E(X) = \mu$

$Pr[|X-\mu| \geq \beta\sigma] \leq \frac{1}{\beta^2}$, $\sigma = \sqrt{Var(x)}$, $E(x) = \mu$

independent, identical R.V. variances.

Chebyshev:

$Pr[|X - E[X]| \geq a] \leq \frac{Var[X]}{a^2}$ Probability that we are more than a away from mean.

Markov:

$Pr[X \geq a] \leq \frac{E(X)}{a}$.

$Pr(|X-E(X)| < a) = 1 - Pr(|X-E(X)| \geq a)$

$\geq 1 - \frac{Var(X)}{a^2}$

$\ln(1-\varepsilon) \approx -\varepsilon$

$\exp\{-\varepsilon\} \approx 1-\varepsilon$

$(a+b)^n = \sum_{m=0}^{n} \binom{n}{m} a^m b^{n-m}$

$1 + 2 + \ldots + n = \frac{n(n+1)}{2}$

Symmetry: if we pick balls from a bag, w/out replacement

Pr(ball 5 is red) = Pr(ball 1 is red)

Order of balls - permutation

All permutations have same probability.

Random Experiment defined by set of probabilities and sample space.

If $P(X) > P(Y)$, then $P(X|Z) > P(Y|Z)$ False

If X is indep Y, $P[X] = \sum_z P(Z, X|Y)$ True.

If $P(X) > P(Y)$, then $P(XZ) \ngtr P(YZ)$ False

X and Y independent, $X = G(p)$, $Y = G(q)$

$Pr(X \leq Y) = \sum_{x=1}^{\infty} Pr(X=x, Y \geq x) = \sum_{x=1}^{\infty} (1-p)^{x-1} p (1-q)^{x-1}$

$= p \sum_{x=1}^{\infty} [(1-p)(1-q)]^x$

$= \frac{p}{1-(1-p)(1-q)}$

Halt

def Q(P)

P()

return true

Program (Q, P)

Random Variable: a real valued function of the outcome of a random experiment

There is 1 polynomial of degree $\leq d$ with modulo prime p that contains any $d+1$: $(x_1, y_1) \ldots (x_{d+1}, y_{d+1})$ w/ x_i distin

deg d polynomial has $\leq d$ solutions.