$P \Rightarrow Q \equiv \neg P \vee Q$ $\quad$ $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$

$P \Rightarrow Q \equiv \neg Q \Rightarrow \neg P$ $\quad$ $P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$

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

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

$P \vee \neg P$ is always true, $P \wedge \neg P$ is never true

$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$, $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$

MATH PROPERTIES

Repeated Squaring:

$x^n = \begin{cases} x(x^2)^{\frac{n-1}{2}} & \text{if } n \text{ is odd} \\ (x^2)^{n/2} & \text{if } n \text{ is even} \end{cases}$

$\sum_{k=0}^{\infty} ar^k = \frac{a}{1-r}$

$\int x e^x \, dx = e^x(x-1) + C$

PROOFS
- odd $\Rightarrow 2k+1$
- even $\Rightarrow 2k$
- rational $\Rightarrow q = \frac{a}{b}$
- $a \mid b$, $\exists q \in \mathbb{Z}$ $b = aq$
  - if $a \mid b$ and $a \mid c$, $a \mid (b+c)$
  - if $a \mid d$ and $b \mid d$, $\frac{ab}{d}$
  - the prime factorization of b contains a: $(\forall n \in \mathbb{Z}^+)(\exists \prod_i p_i = n)$

INDUCTION
- prove base case
- state inductive hypothesis, $n=k$ or $n \leq k$
- prove inductive step

pigeonhole principle:
- $n+m$ balls in n bins $\Rightarrow \geq 1$ bin has ≥ 2 balls

GRAPHS

	no repeat edges	no repeat vertices	start = end	visits every edge at least once	visits every vertex once
simple path	X	X			
cycle	X	X	X		
walk					
eulerian walk	X			X	
eulerian tour	X		X	X	
hamiltonian walk	X	X			X
hamiltonian tour	X	X	X		X

- eulerian walk has at most two odd-degree vertices, you start and end at these vertices
- eulerian tour is connected and every vertex has an even degree
- hamiltonian walks have $|V|-1$ edges
- All hypercubes have a hamiltonian tour, $|V|$ edges
- simple graphs: any two vertices share at most 1 edge, no loops/multiple edges to vertex

PLANARITY
- no edges cross each other
- $e \leq 3v-6$ or $v+f=e+2$
- does not contain $K_{3,3}$ or K_5

$K_{3,3}$

K_5

BIPARTITE
- two colorable
- no odd length cycles
- can be split into left/right
- $e \leq 2v-4$ if planar

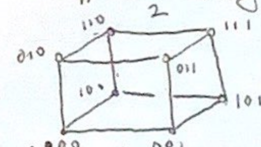
total degree: $\sum_{i=1}^{f} s_i = 2e = \sum_{v \in V} \deg(v)$

- $s_i \geq 3$, $3f \leq 2e$
- can be colored w/ ≤ 4 colors

$K_n = \frac{n(n-1)}{2}$ edges

Connectivity
- path b/w any two vertices
- connected components = 1

HYPERCUBES
- n = dimensions
- $|V| = 2^n$
- $|E| = n2^{n-1}$
- made up of 2 (n-1) hypercubes
- bipartite for $n \geq 1$
- to remove/disconnect d vertices, remove $d2^{d-1}$



TREES
- connected and acyclic
- $|V| = |E| + 1$
- disconnects if edge is deleted, connected components increases by 1
- adding an edge makes a graph
- depth: longest path from root to leaf
- always planar

STABLE MATCHING (n jobs, n candidates)
- ensures everyone is happy

Scheme
- Morning: job makes offer to most preferred candidate who has yet to reject the job
- Afternoon: each candidate will reject all offers, and consider only the top offer
- Evening: each rejected job crosses off that candidate from the list

Facts:
- will always halt, at most n^2 days
- always terminates w/ a matching
- always stable
  - → rogue couple: a job and a candidate prefer each other over their matched pair $\Rightarrow$ unstable
- Improvement lemma: over time, the job on the candidates string can only get better. The job can only get worse candidates.
- well-ordering principle: if $S \subseteq \mathbb{N}$ and $S \neq \emptyset$, then S has a smallest item
- optimality: the highest pairing for each respective group
  - ↳ stable matching is job/employer optimal
  - ↳ one stable matching: job optimal/pessimal and cand optimal/pessimal

MODULAR ARITHMETIC
- $x \pmod m \equiv r$, $x = mq + r$ where $0 \leq r \leq m+1$
- $x + y \pmod m = x \pmod m + y \pmod m$
- $x - y \pmod m = x \pmod m - y \pmod m$
- $xy \pmod m = (x \pmod m)(y \pmod m)$
- $x \equiv y \pmod m \iff m \mid (x-y)$
- if $a \equiv c \pmod m$ & $b \equiv d \pmod m$, $a+b \equiv c+d \pmod m$, $ab \equiv cd \pmod m$
- $a \equiv b^c \pmod m \equiv (b \pmod m)^c \pmod m$
- $d = \gcd(x, y) = \gcd(y, x \pmod y)$ $= \exists a, b : ax + by$ for $x \geq y > 0$
- x^{-1} exists iff $\gcd(x, m) = 1$
  - ↳ $ax \equiv 1 \pmod m$
  - ↳ bijection exists
- only m possible values

FLT
- $\forall p$ and any $a \in \{1, 2, \ldots, p-1\}$ we have $a^{p-1} \equiv 1 \pmod p$, $\gcd(a, p) = 1$

COMMON QUESTION
- How many values $\{0, \ldots, p^k - 1\}$ are relatively prime to p
- $p^k - p^{k-1}$ bc all p^{k-1} numbers are divisible by p

xtended euclid example

x	y	$\lfloor x/y \rfloor$	a	b
35	12	2	$\boxed{-1}$	$\boxed{3}$
12	11	1	1	-1
11	1	11	$\boxed{0}$	$\boxed{1}$
$\boxed{1}$	0		start	

gcd

- new a = old b
- new $b = a - b\lfloor \frac{x}{y} \rfloor$
- if $\gcd(x,y)=1$,
  $a = x^{-1} \pmod{y}$
  $b = y^{-1} \pmod{x}$

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

$\phi(n) = |\{i : 1 \le i \le n, \gcd(n,i)=1\}|$

CRT example

$x \equiv 2 \pmod 3$ $x \equiv 2 \pmod 4$ $x \equiv 1 \pmod 5$ * all mods relatively prime

	mod 3		mod 4		mod 5
$x =$	$4 \cdot 5$	+	$3 \cdot 5$	+	$3 \cdot 4$

$x = 74$

- solution is unique
- modding x by one of the mods yields only that column

ERROR CORRECTING CODES (ALL IN GF(q))

ERASURE: k packets lost from message of length n

↳ send n+k packets and make a polynomial of n−1

- the k extra points is made from P(x) — send points
- use lagrange interpolation for the successful packets to make a new Q(x)
- recover the two packets

General: k packets corrupted, send n+2k packets

Berlekamp Welch

- make polynomial to make the 2k new points
- the message is sent where $\ge n+k$ are correct
- make $E(x) = (x-e_1)\dots(x-k)$
- For all i's, solve $Q(i) = r_i E(i)$ — polynomial w/ unknown coefficients and deg(Q) — received
- use system of linear eqs to solve for coefficients deg $\le n-1+k$
- solve $P(x) = \frac{Q(x)}{E(x)}$

RSA

- receiver sends key (N, e): public key — relatively prime to $(p-1)(q-1)$; pq ← distinct odd primes unknown
- private key: $d = e^{-1} \pmod{(p-1)(q-1)}$
- encryption $E(x) = x^e \pmod N$
- decryption: $x = (E(x))^d \pmod N$
- $D(E(x)) \equiv x \pmod N$ for every possible message $x \in \{0,1,\dots,N-1\}$
- $|S| = 24 = (7-1)(5-1)$ ← prime factors of 35
  $S = \{x : x \in \{1,\dots,34\}$ and $\gcd(x,35)=1$

Counting

	order matters	order doesn't matter
w/o replacement	$\frac{n!}{(n-k)!}$	$\binom{n}{k} = \frac{n!}{k!(n-k)!}$
w/ replacement	n^k	$\binom{n+k-1}{n} = \binom{n+k-1}{k-1}$

- multiply # of ways for each choice
- count ordered arrangements, divide by # of ways to order to get unordered
  - distinguisable, order matters
  - indistinguishable, order doesn't matter
  - one ball in each bin, w/o replacement
  - multiple balls in each bin, w/ replacement

- bijection b/w A and B
  ↳ $|A| = |B|$

Combinatorial Proofs

- $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$
- $\binom{n}{k+1} = \binom{n-1}{k} + \binom{n-2}{k} + \dots + \binom{k}{k}$
  ↳ $\binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{n} = 2^n$
  → # of ways of choosing subset X w/ k+1 elements from $|S| = n$
- $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$

Polynomials

- a nonzero polynomial of degree d has at most d roots
- given d+1 pairs (x_i, y_i) where x_i is distinct, there is a unique polynomial p(x) of degree at most d such that $p(x_i) = y_i$ for $1 \le i \le d+1$

Lagrange Interpolation

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

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

max degree

- $f+g$: max(deg f, deg g)
- $f \cdot g$: $f+g$
- $\frac{f}{g}$: $f-g$

min degree

0 for all

COUNTABILITY/COMPUTABILITY

	countable	uncountable
FINITE	if it is finite then it is automatically countable	~~R[0,1] → diagonalizable~~
INFINITE	bijection b/w a set S an $\mathbb{N}$; cantor-bernstein $f: \mathbb{Q} \to \mathbb{N}$; enumerate i.e strings	$\mathbb{R}[0,1]$ → diagonalization; cantor set; infinite length bits/sequences

- $A \subseteq B$ and B is countable ⟹ A is countable
- $A \supseteq B$ and A is uncountable ⟹ B is uncountable

Halting Problem

- given P, x, and testHalt(P, x), you can't know if it doesn't halt because it will never provide an answer
- Infinite recursion

FINITE FIELDS

- GF(m), m is prime
- allows for +, −, ×, ÷ any non zero number (mod m)
- # of polynomials of $2 \ge d$ are there (mod m) ⟹ m^3, m^{d+1}

Secret Sharing

- ~~x~~ is the secret P(0)
- P(1), …, P(n) is given to the decoders
- P(x) of degree k−1, k people are needed
- scheme that requires x_i from n groups of people
  ↳ create n polynomials of $x_i - 1$ and use the secrets to make an n+1th polynomial of degree n−1

PROBABILITY

$\Omega \sim$ Sample Space $\quad P[A] = 1 - P[\bar{A}] \quad$ · comma (,) = and ($\cap$)

$0 \le P[\omega] \le 1$

$\sum_{\omega \in \Omega} P[\omega] = 1 \quad P[A] = \sum_{\omega \in A} P(\omega)$

eg. Coin Toss, $P[H] = \frac{2}{3}$

$P[HHHH] = \left(\frac{2}{3}\right)^4$

$P[HHTT] = \left(\frac{2}{3}\right)^4 \left(\frac{1}{3}\right)^2$

~ All four same

$P[A] = P[HHHH] + P[TTTT]$

$= \left(\frac{2}{3}\right)^4 + \left(\frac{1}{3}\right)^4 = \frac{17}{81}$

~ exactly n items w/ prob p

$P[C] = \binom{K}{n} p^n (1-p)^{K-n}$

↳ K is total trials

uniform – $P[A_1] = P[A_2] = \dots = P[A_K]$

$P[A] = \frac{|A|}{|\Omega|}$

~ Poker hands (Flush)

$P[A] = \frac{4 \times \binom{13}{5}}{\binom{52}{5}}$

~ Bin 1 is empty

$P[A] = \left(\frac{n-1}{n}\right)^m$

m = # of trials

CONDITIONAL PROBABILITY

· $P[\omega \mid B] = \frac{P(\omega)}{P(B)}$ for $\omega \in B$

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

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

· Independence

↳ $P[A \cap B] = P(A) P(B)$

↳ $P(A \mid B) = P(A)$

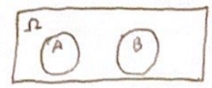
↳ $P(B \mid A) = P(B)$

Union Bound

· $P\left(\bigcup_{i=1}^{n} A_i\right) \le \sum_{i=1}^{n} P(A_i)$

MUTUALLY EXCLUSIVE/Disjoint

· $P[A \cap B] = 0$



$P[B] = P[A \cap B] + P[\bar{A} \cap B]$

$= P[B \mid A] P[A] + P[B \mid \bar{A}] P[\bar{A}]$

↳ total probability rule/law

· pairwise independence ≠ mutual independence

↳ $P[A_i \mid \bigcap_{j \in I} A_j] = P[A_i]$

↳ for every subset $I \subseteq \{1, \dots, n\}$ w/ size $|I| \ge 2$

$P[\bigcap_{i \in I} A_i] = \prod_{i \in I} P[A_i]$

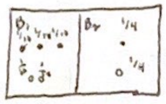
└ for all $B_i \in \{A_i, \bar{A_i}\}$

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

CONDITIONAL PROBABILITY EXAMPLES

~ card dealing, second is an ace given first is an ace

$P[A \cap B] = \frac{4}{52} \cdot \frac{3}{51} \quad P[B] = \frac{4}{52} \quad P[A \mid B] = \frac{3}{51}$



$P[\text{Bin } 1 \mid 0] = \frac{\overbrace{\frac{1}{10} + \frac{1}{10}}^{\text{white + bin 1}}}{\underbrace{\frac{1}{10} + \frac{1}{10} + \frac{1}{4}}_{\text{white}}}$

RANDOM VARIABLES (X)

· # of times a sample occurs

↳ Distribution: $P[X = a] = \frac{b}{\Omega}$ ← # of times $X = a$ occurs

↳ $a_1 \ne a_2$, disjoint

↳ $\left[\bigcup_{i=1}^{|\Omega|} A_i\right] = \Omega$

VARIANCE CONTINUED...

· if X_i is identically distributed, $Var(X_i) = n Var(X_i)$

· $Var(c) = 0$

· cov is bilinear $\quad Cov(aX, bY) = ab\, Cov(X, Y)$

Variance/Covariance

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

· $\sigma(X) = \sqrt{Var(X)} \quad$ · $Var(X+Y) = Var(X) + Var(Y) + 2Cov(X,Y)$

· $Var(cX) = c^2 Var(X)$ ↳ $Var(X) + Var(Y)$ if independent

· $Cov(X, Y) = E[XY] - E[X]E[Y] = E[(X - \mu_x)(Y - \mu_y)]$

· $Corr(X, Y) = \frac{Cov(X, Y)}{\sigma_x \sigma_y}$, within $[-1, 1]$

↳ $\sigma(X) > 0$ and $\sigma(Y) > 0$

↳ if $corr(X, Y) = \pm 1$, there exists a and b such that $Y = aX + b$

Joint Distributions

$\{(a, b), P[X = a, Y = b]\} \quad a \in A, b \in B\}$

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

Expectation

· mean value of the random variable

· $E[X] = \sum x_i p(x_i)$

· $E[g(X)] = \sum_{x \in \mathbb{R}} g(x) P(X = x)$ (LOTUS)

· $E[X^K] = \sum x_i^K P(x_i)$

· $E[g(X, Y)] = \sum_{x,y \in \mathbb{R}} g(x, y) P[X = x, Y = y]$

· $E[a_1 X_1 + a_2 X_2] = a_1 E[X_1] + a_2 E[X_2]$

· Conditional Expectation: $E[Y \mid X = x] = \sum_y y \Pr[Y = y \mid X = x]$

· $E[E[Y \mid X]] = E[Y] \Rightarrow$ Law of Total Expectation

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

X_i is indicator $\Rightarrow E[X_i] = 1 P[X_i] + 0 P[\bar{X_i}]$

BOUNDS

· Markov's: $P[X \ge c] \le \frac{E[X]}{c}$

↳ non-negative r.v's

↳ generalized: $P[|Y| \ge c] \le \frac{E[|Y|^r]}{c^r}$

Chebyshev's: $P[|X - \mu| \ge k\sigma] \le \frac{1}{k^2}$

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

tail sum: $E[X] = \sum_{i=1}^{\infty} P[X \ge i]$

CONFIDENCE INTERVALS

· $P(|\hat{p} - p| \ge \varepsilon) \le \frac{Var(\hat{p})}{\varepsilon^2} \le \delta \Rightarrow P(|\frac{S_n}{n} - \mu| \ge \varepsilon) \le \frac{\sigma^2}{n\varepsilon^2} = \delta$

↳ $\delta = 0.05 \Rightarrow$ 95% confidence

↳ $\hat{p}$ = proportion of success in n trials, $Var(\hat{p}) = \frac{p(1-p)}{n}$

· Law of large numbers: as $n \to \infty$, sample average of i.i.d $X_1, \dots, X_n$ tends to population mean

LINEAR REGRESSION

$y(\hat{x}) = L(Y \mid X) = E[Y] + \frac{cov(X, Y)}{Var(X)} (X - E[X])$

↳ if $E[Y \mid X]$ is a linear function, $E[Y \mid X] = L[Y \mid X]$

CONTINUOUS PROBABILITY

PDF:

$f_X(x) \ge 0$ for $x \in \mathbb{R}$

$\int_{-\infty}^{\infty} f_X(x)\,dx = 1$ $\quad P[a \le X \le b] = \int_a^b f(x)\,dx \ \ \forall a<b$

Independent if:

$P[a \le X \le b, c \le Y \le d] = P[a \le X \le b]\,P[c \le y \le d] = f_{X,Y}(x,y) = f_X(x)\,f_Y(y)$

Conditional Continuous Probability

$f_{X|A}(x) = \frac{f_X(x)}{P(A)}, \quad f_{X|Y}(x|y) = \frac{f_{XY}(x,y)}{f_Y(y)}$

$P[x \le X \le x+dx] = \int_x^{x+dx} f(z)\,dz \approx f(x)\,dx$

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

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

Central Limit Theorem (CLT)

- as $n \to \infty$, distribution becomes normal

$\frac{S_n - n\mu}{\sigma\sqrt{n}} \longrightarrow N(0,1)$ $\quad n \to \infty$

$P\left[\frac{S_n - n\mu}{\sigma\sqrt{n}} \le c\right] \to \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{c} e^{-x^2/2}\,dx$ as $n \to \infty$

CDF:

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

$f(x) = \frac{d}{dx} F(x)$

Joint Distribution

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

Marginal densities

$f_X(x) = \int f_{X,Y}(x,y)\,dy$

$f_Y(y) = \int f_{X,Y}(x,y)\,dx$

DISCRETE	Description	PMF $(P(X=k))$	CMF $(P[X \le k])$	$E[X]$	$Var[X]$
Uniform(a, b)	choosing smt in range a, b w/ equal p; $X \in [a,b]$	$\frac{1}{b-a+1}$	$\frac{k-a+1}{b-a+1}$	$\frac{a+b}{2}$	$\frac{(b-a+1)^2-1}{12}$
Bernoulli(p)	indicater r.v.'s; $X \in \{0,1\}$	$\begin{cases} p & k=1 \\ 1-p & k=0 \end{cases}$		p	$p(1-p)$
Bin(n,p)	# of successes in n independent trials w/ replacement; $X \in \{0,1,2,\dots\}$	$\binom{n}{k} p^k (1-p)^{n-k}$		np	$pn(1-p)$
Geometric(p)	How long to wait before smt happens; $X \in \{1,2,3,\dots\}$	$p(1-p)^{k-1}$	$1-(1-p)^k$	$\frac{1}{p}$	$\frac{1-p}{p^2}$
Pois(λ)	event happens w/ average; $X \in \{0,1,2,3,\dots\}$	$\frac{\lambda^k e^{-\lambda}}{k!}$		λ	λ
hypergeometric(N,K,n)	Bin w/o replacement; $X \in \{0,1,2,\dots\}$	$\frac{\binom{K}{k}\binom{N-K}{n-k}}{\binom{N}{n}}$		$n\frac{K}{N}$	$n\frac{K(N-K)(N-n)}{N^2(N-1)}$

integrate this to get probability

derive to get probability

Continuous	PDF $(f_X(x))$	CDF $(F_X(x) = P(X \le x))$	$E[X]$	$Var(X)$	Description
Uniform(a,b)	$\frac{1}{b-a}$	$\frac{x-a}{b-a}$	$\frac{a+b}{2}$	$\frac{(b-a)^2}{12}$	continuous form of uniform
Exp(λ)	$\lambda e^{-\lambda x}$	$1 - e^{-\lambda x}$	$\frac{1}{\lambda}$	$\frac{1}{\lambda^2}$	continuous form of geometric
$N(\mu, \sigma^2)$	$\frac{1}{\sqrt{2\pi\sigma^2}} e^{-(x-\mu)^2/(2\sigma^2)}$	$\int_{-\infty}^{x} \frac{1}{\sqrt{2\pi}} e^{-t^2/2}\,dt$	μ	σ^2	bell shaped curve symmetric around $x=\mu$ width by σ

- if $X \sim N(0,1)$ and $Y \sim N(0,1)$
  $Z = aX + bY \sim N(0, a^2+b^2)$
  ↳ $\mu = a\mu_x + b\mu_y$
  ↳ $\sigma^2 = a^2\sigma_x^2 + b^2\sigma_y^2$

If Given, $Y = aX + b$

↳ change bounds to be in terms of Y

↳ change p(x) to be in terms of y

- $X + Y \sim$ Binomial$(2n, p)$ if independent
- bounds for $\lceil Z \rceil \in [i, i+1]$
  $\lfloor Z \rfloor \in [i-1, i]$

$\mathbb{N} = \{0, 1, 2, \dots\}$

$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$

$\mathbb{Q} = \{$decimals w/ ending 0 or repeating sequence$\}$

rationals

Real Numbers