propositional logic
- P=>Q: False iff F=>T
- P=>Q: True if P always False
- P=>Q = ¬PvQ
- P=>Q = ¬Q=> ¬P

quantifiers
- De Morgan's
  - $\neg(P \wedge Q) \equiv (\neg P \vee Q)$
  - $\neg(P \vee Q) \equiv (\neg P \wedge \neg Q)$
- De Morgan's for Quantifiers
  - $\neg(\forall x\ P(x)) \equiv \exists x \neg P(x)$
  - $\neg(\exists x\ P(x)) \equiv \forall x \neg P(x)$

trees (T)
- iff:
  - connected + acyclic
  - connected + e = v-1
  - connected + remove edge disconnects
  - acyclic + adding edge creates cycle
- Ts with >= 2 vertices must have at least 2 leaves
- all Ts with at least 2 vertices are bipartite
- every connected component in an acyclic G is a T
- acyclic G with k CCs => e = v - k
- a graph with v+ edges contains a cycle

hamiltonian tour (HT)
- tour that visits every vertex exactly once
- every hypercube has a HT

eulerian walk (EW)
- walk that visits every edge exactly once
- undirected G has an EW iff connected and has 0 or 2 odd degree vertices
- undirected G has an EW with v.1 != v.n iff connected and has EXACTLY 2 odd degree vertices

eulerian tour (ET)
- a closed EW
- undirected G has an ET iff G is connected and even degree

planar graphs
- Euler's Formula: for every connected planar G, v+f=e+2
- for planar G with k connected components, v-e+f=k+1
- faces of at least nine sides => (nf <= 2e) => (v+(2e/n) >= e+2)
  - (n=3) => (e <= 3v-6). (n=4) => (e < = 2v-4) (planar bipartite)
- Kuratowski's Theorem: non-planar iff contains K5/K3,3
- all planar Gs is 4-colorable
- K.3,3 is bpartite and 2 colorable
- K.i is i colorable
- max deg 2 => planar

	no repeated vertices	no repeated edges	start = end
walk			
path	×	×	
tour			×
cycle	×	×	×

handshaking lemma
- sum of degrees = 2e
- there must be even number of odd degree vertices

hypercubes (HC)
- bit string definition: V = n string bit strings, E = (x,y | x and y differ in exctly one position)
- recurisve definition: n-dim HC = (n-1)-dim HC (0 subcube) + (n-1)-dim HC with edges between each pair of vertices 0x in 0 subcube and 1x in 1 subcube
- (n-dim HC) => (2^n vertices) => ($e=n*2^{(n-1)}$)
- (n vertices) = (log2(n)-dim HC) = ($e=\log_2(n) * 2^{\log_2(n)-1}$ edges)

bipartite graphs
- G where vertices are split into two groups and edges only go between groups
- V = L ∪ R, E ⊆ L X R
- always 2-colorable
- any G is bipartite iff it has no tours of odd length

stable matching
- matching is job optimal => it is also candidate pessimal
- P&R with jobs proposing => job optimal matching
- there is only ONE job/candidate optimal matching

Chinese Remainder Theorem (CRT)
- given a system of k modular congruences, x ≡ a.i (mod m.i) where m.i are all coprime (gcd = 1), there exists a unique solution for x

ex: x ≡ 1 (mod 3). x ≡ 3 (mod 7). x ≡ 4 (mod 11).

$a \equiv 1 \pmod 3$ $\quad a \equiv 0 \pmod 7$ $\quad a \equiv 0 \pmod{11}$
$b \equiv 0 \pmod 3$ $\quad b \equiv 1 \pmod 7$ $\quad b \equiv 0 \pmod{11}$
$c \equiv 0 \pmod 3$ $\quad c \equiv 0 \pmod 7$ $\quad c \equiv 1 \pmod{11}$

a: 77 $\boxed{154}$
75
2 1

b: 33 $\boxed{99}$
28 98
5 10 15
1

c: $21^{-1} \equiv 10^{-1}$
$\equiv 10 \pmod{11}$
$21 \cdot 10 = \boxed{210}$

$x = (1)a + (3)b + (4)c$
$= 1291$
$\equiv 136 \pmod{3 \cdot 7 \cdot 11}$

GCD, MI, & euclid's algorithm
- gcd(x,y) = gcd(y, x mod y)
- if gcd(x,m) = 1, the MI of x mod m exists and is unique

extended euclid's algorithm
- find a,b such that ax+by=1
- a = x mod y, b = y mod x

ex: find GCD of 17 and 39.
(17, 39) -> (17, 5) -> (5, 2) -> (2, 1) -> (1)

ex: find the MI of 17 mod 39.
(1)39 + (0)17 = 39
(0)39 + (1)17 = 17
(1)39 + (-2)17 = 5
(-3)39 + (7)17 = 2 $\quad$ 17 - (3)5
(7)39 + (-16)17 = 1 $\quad$ 5 - (2)2

$17^{-1} \equiv -16 \equiv 23 \pmod{39}$

P&R algorithm
- improvement lemma
  - every candidate will only accept a better job as time goes on
  - every job will only propose worse candidate as time goes on
- terminates in at most (n-1)^2 + 1 days
- a candidate receives proposal on day i => they receive some proposal on every day thereafter until termination
- a candidate receives NO proposal on day i => they receive no proposal on any previous day j
- through a complete execution of the algorithm, there is at least 1 candidate who receives exactly 1 proposal

Fermat's Little Theorem
- for any prime p and any $a \in \{0,1,\ldots,N-1\}$, $a^{(p-1)} \equiv 1 \pmod p$
- tells us that exponentiation is (p-1)-periodic when modulo p

modular arithmetic rules

if $a \equiv c \pmod m$ & $b \equiv d \pmod m$
$a + b \equiv c + d \pmod m$
$a \cdot b \equiv c \cdot d \pmod m$
$a^k \equiv b^k \pmod m$

if a c (mod m):
you can divide by both sides AND m by k
ex: $2x \equiv 4 \pmod{12} \implies x \equiv 2 \pmod 6$
you can also multiply both sides by a MI
ex: $8x \equiv 9 \pmod{15} \implies x \equiv 18 \equiv 3 \pmod{15}$
$\gcd(x, y) = 1$ & $x \mid yz \implies x \mid z$

Euler's Totient Function & Theorem
- totient function: $\phi(n) = |\{i : 1 \le i \le n, \gcd(n,i) = 1\}|$
- totient theorem: $a^{\phi(n)} \equiv 1 \pmod n$
- properties:
  - $\phi(p) = p-1$ for prime p
  - $\phi(p^k) = p^k - p^{k-1} = p^k \cdot (p-1)/p$
  - $\phi(a)\phi(b) = \phi(ab)$

RSA
- variables:
  - x (mod N): message
  - y (mod N): encrypted, $\equiv x^e \pmod N$
  - $E(x) \equiv x^e \pmod N$
  - $D(y) \equiv D(x^e) \equiv x^{ed} \equiv x \pmod N$ * by FLT & CRT
  - private variables:
    - p,q: 2 large primes
    - d: private key, $\equiv e^{-1} \pmod{(p-1)(q-1)}$
  - public:
    - N: public key = pq
    - e: public key, arbitrarily chosen & is relatively prime to (p-1)(q-1)

polynomials (P)
- property 1: a non-zero P of deg d has at most d roots
- property 2: given d+1 points $(x_1,y_1),\ldots,(x_{d+1},y_{d+1})$ with all x_i distinct, there is a unique P of deg at most d that goes through those points

LaGrange Interpolation
- create Ps that go through (x ,1) and (x ,0) for all j = i
- add linear combination of subPs to get desired P

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

ex: (1, 1), (2, 2), (3, 3)

$$\Delta_1 = \frac{(x-2)(x-3)}{(1-2)(1-3)} \quad \Delta_2 = \frac{(x-1)(x-3)}{(2-1)(2-3)} \quad \Delta_3 = \frac{(x-1)(x-2)}{(3-1)(3-2)}$$

$$P = \Delta_1 + 2\Delta_2 + 3\Delta_3$$

do arithmetic mod p!!!

Berlekamp-Welch Algorithm
- $E(x) = (x-e_1)(x-e_2)\ldots(x-e_k)$: error locater P
- $Q(x) = P(x)E(x)$. $Q(i) = P(i)E(i) = r_i E(i)$

ex: received (0, 1, 4, 0, 4) w/ one error

$E(x) = x - e_0$
$Q(x)$, deg P + deg E = 2+1
$= a_3x^3 + a_2x^2 + a_1x + a_0$

do arithmetic mod p!!!

$Q(0) = 0E(0)$ $\quad a_0 = 0$
$Q(1) = 1E(1)$ $\quad a_3 + a_2 + a_1 = 1 - e$
$Q(2) = 4E(2)$ $\quad 8a_3 + 4a_2 + 2a_1 = 8 - 4e$
$Q(3) = 0E(3)$ $\quad 27a_3 + 9a_2 + 3a_1 = 0$
$Q(4) = 4E(4)$ $\quad 64a_3 + 16a_2 + 4a_1 = 16 - 4e$

Galois Fields
- a finite field modulo m

# of points	# of polynomials
d+1	1
d	m
d-1	m^2
...	...
d-k	m^{k+1}
...	...
0	m^{d+1}

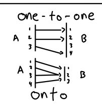
error correcting codes
- erasure errors:
  - n packets, k dropped
  - packets labelled so receipient knows exactly which packets are dropped
  - must send n+k packets, where each packet is m is a number in GF
- general error:
  - n packets, k corrupted. must send n+2k packets
  - when reconstructing, there is a unique polynomial P(x) of degree at most n-1 such that P(i)=ri for at least n+k of the received packets

counting

	permutations (ordered)	combinations (unordered)
w/o replacement	$\frac{n!}{(n-k)!}$	$\binom{n}{k} = \frac{n!}{k!(n-k)!}$
w/ replacement	n^k	$\binom{n+k-1}{k}$

countability
- set is countable if there exists a bijection between it and N
- countable: ℤ, ℚ, N x N, finite length strings from finite or infinite set of characters
- non-countable: ℝ[0,1], ℝ, infinite length strings

bijections
- f: A->B is a bijection iff it is onto and one-to-one
- one-to-one (injective): every element in A has a mapping to a distinct element in B
- onto (surjective): every element in B has a pre-image in A



Cantor's Diagonalization
- change every value along diagonal
- can apply to functions, which are uniquely defined by their outputs on each input

halting problem
- to show TestX(Q, y) which determines whether Q does some task X on input y

```
def TestHalt(P, x)
  def Q(y)
    run P(x)
    do X
  return TestX(Q, y)
```

probability and independence formulas
- conditional probability: $P[A|B] = \frac{P[A \cap B]}{P[B]}$
- total probability: $P[A] = \sum_{i=0}^{n} P[B|A_i]P[A_i]$
- Bayes Theorem: $P[A|B] = \frac{P[B|A]P[A]}{P[B]}$
- product rule: $P[A \cap B] = P[A]P[B|A]$
- pairwise independence: $P[A|B] = P[A]$
- pairwise independence: $P[A \cap B] = P[A]P[B]$
- mutual independence: $P[\bigcap_{i \in I} A_i] = \prod_{i \in I} P[A_i]$

pairwise I does not imply mutual I
- union bound: $P[\bigcup_{i=1}^{n} A_i] \le \sum_{i=1}^{n} P[A_i]$

expected value formulas
- $E[X] = \sum k \cdot P(x = k)$
- linearity of expectation:
  - $E[X+Y] = E[X] + E[Y]$
  - $E[cX] = c\,E[X]$
- LOTUS: $E[f(X)] = \sum f(k)\,P(X=k)$

Markov's Inequality
- $P(X \ge c) \le \frac{E(X)}{c}$

Chebyshev's Inequality
- $P[|X-\mu| \ge c] \le \frac{Var(X)}{c^2} = \frac{\sigma^2}{c^2} < \delta$

variance formulas
- $Var(X) = E[(X-E[X])^2]$
- $Var(X) = E[X^2] - (E[X])^2$
- $Var(X+Y) = V(X) + V(Y) + \overbrace{2Cv(X,Y)}^{=0 \text{ for I.V.}}$
- $Var(cX) = c \cdot Var(X)$
- $Cov(X,Y) = E[(X - EY)(Y - EX)]$
- $Cov(X,Y) = E[XY] - E[X]E[Y]$
- $Cov(X,X) = Var(X)$
- Independent => $Cov(X,Y) = 0$
- $Cov(X,Y) = 0 \not\Rightarrow$ Independent
- $Corr(X,Y) = \frac{Cov(X,Y)}{\sigma_X \sigma_Y}$

bernoulli distribution
- Bern(p)
- $Pr(X=0) = 1-p$
- $Pr(X=1) = p$
- $E[X] = p$
- $Var(X) = p(1-p)$

binomial distribution
- Binom(n, p)
- $Pr(X=k) = \binom{n}{k} p^k (1-p)^{n-k}$
- $E[X] = np$
- $Var(X) = np(1-p)$

geometric distribution
- Geom(p)
- $Pr(X=k) = p(1-p)^{k-1}$
- $E[X] = \frac{1}{p}$
- $Var(X) = \frac{1-p}{p^2}$

poisson distribution
- Poiss(λ)
- $Pr(X=k) = \frac{\lambda^k e^{-\lambda}}{k!}$
- $E[X] = \lambda$
- $Var(X) = \lambda$

$X \sim Pois(\lambda_1) + Y \sim Pois(\lambda_2) = Pois(\lambda_1 + \lambda_2)$

Central Limit Theorem

$c = \infty \to 1 \quad c = 0 \to \frac{1}{2}$

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

X_i has mean μ and variance σ^2 and

$S_n = \sum_{i=1}^{n} X_i$, $A_n = \frac{1}{n}\sum_{i=1}^{n} X_i$, $E[A_n] = \mu$, $Var(A_n) = \frac{\sigma^2}{n}$

as $n \to \infty$. $A_n \to N(\mu, \frac{\sigma^2}{n})$, $S_n \to N(n\mu, n\sigma^2)$

$\frac{A_n - \mu}{\sigma/\sqrt{n}} \to N(0,1)$, and $\frac{S_n - n\mu}{\sigma\sqrt{n}} \to N(0,1)$

Wald's Identity

$Y = X_1 + \dots + X_N$ N is a RV

$E[Y] = E[E[Y|N]]$

$= \sum_n E[Y|N=n]\,P(N=n)$

$= \sum_n n\,E[X_i]\,P(N=n)$

$= E[X_i]\,E[N]$

Mean Squared Error
- $E[Y - f(x)]$ where f is estimator

Ideal Estimation
- $E[Y|X=x]$

Linear Least Squares Estimate
- $LLSE(Y\ X) = \frac{Cov(X,Y)}{Var(X)}(X - E[X]) + E[Y]$

bias- variance decomposition of MSE
- $E[(X-a)^2] = E[\delta^2 + 2\delta(\mu - a) + (\mu - a)^2]$

where $\delta = X - E[X]$

$= E[\delta^2] + 2(\mu - a)E[\delta] + (\mu - a)^2$

$= Var(X) + (\mu - a)^2$

gives the **generalized Markov's inequality**

$$P(|X-a| \ge \varepsilon) \le \frac{Var(X) + (E[X] - a)^2}{\varepsilon^2}$$

Markov Chains

invariant distribution

Probability Density Function ($f_x(x)$)
- $f_x(x) > 0$ for all x
- $\int_{-\infty}^{\infty} f_x(x)dx = 1$
- $P[a \le X \le b] = \int_a^b f_x(x)dx$

Cummulative Density Function ($F_x(x)$)
- $F_x(x) = P[x \le a] = \int_{-\infty}^{a} f(x)dx$
- $f_x(x) = \frac{d}{dx} F_x(x)$

independence for continuous RVs

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

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

expected value
- $E[X] = \int_{-\infty}^{\infty} x f_x(x)dx$

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

$= E[X^2] - E[X]^2$

$= \int_{-\infty}^{\infty} x^2 f_x(x)\,dx - \left(\int_{-\infty}^{\infty} x f_x(x)\,dx\right)^2$

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

Total Probability
- $P[A] = \int_{-\infty}^{\infty} P[A|X=x]\,f_x(x)\,dt$

joint density
- $P[a \le X \le b, c \le Y \le d] = \int_c^d \int_a^b f(x,y)\,dx\,dy$
- for independent RVs $f(x,y) = f_x(x)\,f_y(y)$

marginal density
- $f_x(x) = \int_{-\infty}^{\infty} f_{x,y}(x,y)\,dx$

conditional density
- $f_{Y|X}(x,y) = \frac{f_{X,Y}(x,y)}{f_X(x)}$

uniform distribution
- Unif(a,b)
- pdf: $f_x(x) = \frac{1}{b-a}$ $[a,b]$, 0 otherwise
- cdf: $F_x(x) = \frac{x-a}{b-a}$ $[a,b]$, 0 otherwise
- $E\,X = \frac{1}{2}(a+b)$
- $Var(X) = \frac{1}{12}(b-a)^2$

normal distribution
- $N(\mu, \sigma^2)$
- pdf: $\frac{1}{\sqrt{2\pi\sigma^2}} e^{-(x-\mu)^2/(2\sigma^2)}$
- cdf: $\frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-t^2/2}\,dt$ ← for $N(0,1)$
- $E[X] = \mu$
- $Var(X) = \sigma^2$

exponential distribution
- Exp(λ)
- pdf: $f_x(x) = \lambda e^{-\lambda x}$ $x \ge 0$, 0 otherwise
- cdf: $F_x(x) = 1 - e^{-\lambda x}$ $x \ge 0$, 0 otherwise
- $E[X] = \frac{1}{\lambda}$
- $Var(X) = \frac{1}{\lambda^2}$

normal distribution properties

$X \sim N(\mu, \sigma^2) \Rightarrow \frac{X-\mu}{\sigma} \sim N(0,1)$

$\Rightarrow aX + b \sim N(a\mu + b, a^2\sigma^2)$

$aX + bY \sim N(a\mu_X + b\mu_Y,\ a^2\sigma_X^2 + b^2\sigma_Y^2)$

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

$= \sum_i E[x_i^2] + \sum_{i \ne j} E[x_i x_j] - E[n x_i]^2$

$= n\,E[x_i^2] + n(n-1)\,E[x_i x_j] - (n\,E[x_i])^2$