Error Correcting Code

Erasure: Use interpolation with mod.
Coefficients are just mod p. Send *n+k* packets: n packets, k lost packets. Any lower results in *p* possibilities for each point lost.

General Errors: Corrupted Packets: Need **n+2k** sent packets, **degree n+k-1**.
Use Q(x)=P(x)E(x), Q(x) degree n+k (add dropped), described by n+k coeff. E(x)=degree k, describe by k-1 coeff.
P(x)=$\frac{Q(x)}{E(x)}$ with error locater E(x).
Can claim that **n+2k** since Q(x)E(x)=Q'(x)E(x) for $1 \le x \le n + 2k$ pts, follow propr 2 they are same poly.

WOP

Assume there is some smallest elem where it doesn't hold. Then prove that it does hold. Can do either f(n) => f(n-1), or f(n-1) => f(n)

Stable Marriage:

-Alg does NOT end until all are matched
-**Improv Lemma:** If M prop to W on the kth day, every sub day she has someone she likes least as much as M
-Pairing produced is always stable
-Pairing output of TSM is male optimal
- Definition of Optimal means there's a pairing
-Pairing output of TSM is female pessimal

Counting:

Sampling with Replace, Order DNM: Think bins and balls. First and last walls are not considered, and every wall is a one. It's binlength string choose items.
1st Rule of Count→if an object can be made with successive choices, use Permutation.
2nd Rule of Count → Object made by success of choices, order doesn't matter (not labeled), Use combination. Cannot be applied if # ordered objects not same for every unordered obj
Combinatorial proofs: think committees.
THM: =Pf; Can choose k, or the complement.
THM: Pascal's Identity → =+Pf: (incl 1st obj)+(don't incl 1st obj)
THM: Pf: Obj=(1…..n). Partition on lowest obj: obj. is: include obj. 1, so n-1 choices, include 2 but not 1, so n-2 choices, include 3 but not 1 or 2, so n-3 choices, etc. Repeat to where smallest is largest, so 1.
Anagrams: $\frac{letters!}{repeats!}$ *8(labeled) balls in 24(labeled) bins:* 24^8. 8 balls 5 bins ≥1ball/bin:$\binom{7}{3}$. *30 students in pairs:* 30 labeled balls into 15 bins, 2 per bin. 15! bin combos, $\frac{30!}{2^{15}}$ ball combos, $\frac{30!}{15!2^{15}}$. Ordering 104 cards with 2 same decks same as anagrams
Counting Subsets: 2^(size of set)
Counting Cards Shuffled deck: 52!. *Flush*: $4\binom{13}{5}$. *Straight*: $9*4^5$(aces high)
Full House: $13\binom{4}{2}*12\binom{4}{3}$
3 of a kind: $13\binom{4}{3}\binom{12}{2}4^2$(incl. full house)
2 pair: $\binom{13}{2}\binom{4}{2}^2$*[11*4]last card.
5-card hand: $\binom{52}{5}$. 13*hand w/ no aces*: $\binom{48}{13}$.
13 hand *all aces:* $\binom{48}{9}$.
at least 3 cards of same value $\frac{13(4\binom{48}{2}+48)}{\binom{52}{5}} = \frac{3\ card+4\ card}{[total\ \#]}$

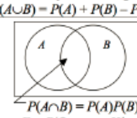
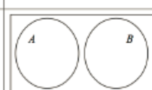
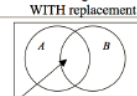
Probability Theory:

	With Replacement	Without Replacement
Order Matters	From a set of n items, where we seek to choose k. n^k	$P(n,k) = \frac{n!}{(n-k)!}$ Example: Picking a specific hand from a deck of cards
Order Doesn't Matter	$C(n+k-1,k) = \frac{(n+k-1)!}{(n-1)!k!}$ Choose k times from a set of n items with replacement. This is if we have k balls to throw into n bins.	$C(n,k) = \binom{n}{k} = \frac{n!}{(n-k)!k!}$ Example: Picking a type of hand from a deck of cards.

$\Pr[A|B] = \frac{\Pr[A \cap B]}{\Pr[B]}$
If **Independent**: $\Pr[A|B] = \frac{\Pr[A]\Pr[B]}{\Pr[B]}$
Bayes: $\Pr[A|B] = \frac{\Pr[B|A]\Pr[A]}{\Pr[B]}$
$\Pr[B] = \Pr[A \cap B] + \Pr[-A \cap B] = \Pr[B|A]\Pr[A] + \Pr[B|-A](1 - P[A])$

$\Pr[\cap_{i=1}^{n-1} A_i] = \Pr[A_1] \times \Pr[A_2|A_1] \times \ldots \times \Pr[A_n| \cap_{i=1}^{n-1} A_i]$
Unions:
Disjoint = $\Pr[\cup_{i=1}^{n} A_i] = \sum_{i=1}^{n} \Pr[A_i]$. Otherwise: *Inclusion Exclusion*: Pr[A1∪A2…]=$\sum \Pr[Ai]$-$\sum \Pr[AiAj]$+$\sum \Pr[AiAjAk]$, etc
PF: Base: n=2. $\Pr[A_1 \cup A_2] = \Pr[A_1] + \Pr[A_2] - \Pr[A_1 \cap A_2]$. Hyp: $\Pr[\cup_{i=1}^{n} A_i] = \sum_{i=1}^{n} \Pr[A_i] + etcetc + (-1)^{(n-1)}\Pr[\cap_{i=1}^{n} A_i]$.
Step: $\Pr[\cup_{i=1}^{n+1} A_i] = \Pr[\cup_{i=1}^{n} A_i \cup A_{n+1}] = \Pr[\cup_{i=1}^{n} A_i] + \Pr[A_{n+1}] - \Pr[\cup_{i=1}^{n} A_i \cap A_{n+1}]\ from\ base$. Apply Induct Hyp on the third term. Taking $\Pr[\cup_{i=1}^{n} A_i]$ expansion into account, there are intersections between expand of $\Pr[\cup_{i=1}^{n+1} A_i]$. Seen as $(-1)^{s(intersec)-1}\sum_{i\in I'} \Pr[\cap_{i\in I'} A_i]$, where I' is [1…n+1]. Last term is finally $(-1)^n \Pr[\cap_{i=1}^{n+1} A_i]$, proving the inclusion exclusion.
-------Thm: if A, B are indep, then ~A,~B are. Can prove independence of ~A, B, then repeat for ~A ~B.
Pr[B]=Pr[B|A]Pr[A]+Pr[B|~A]Pr[~A]=Pr[B]Pr[A]+Pr[B|~A]Pr[~A] by independence. Pr[B](1-Pr[A])=Pr[B|~A]Pr[~A]. Pr[B]=Pr[B|~A].
Union Bound: Adding up all probabilities will only overshoot or equal the union of them all.
MISC: Monty Hall: group tgthr. 2/3 chance of winning if switch.
Balls and Bins: Pr[k bins empty]=$\left(\frac{n-k}{n}\right)^m = \left(1 - \frac{k}{n}\right)^m$.
REMEMBER YOU CAN MOD BEFORE OR AFTER
If it's
Order matters (labeled bins and balls): use standard (balls)^(bins).
Unlabeled balls, labeled bins: use stars and bars

Independent vs Disjoint

		Disjoint: **Yes** **If $P(A\cap B) = 0$** *Mutually Exclusive *No Overlap in Venn Diagram $P(A\cup B) = P(A) + P(B)$	Disjoint: **No** **If $P(A\cap B) \ne 0$** *Can Occur Together *Overlap in Venn Diagram $P(A\cup B) = P(A) + P(B) - P(A\cap B)$
Independent	**Yes** **If $P(B) = P(B\|A)$** *Knowing that A has occurred does NOT affect the probability that B occurs $P(A\cap B) = P(A)P(B)$	**Impossible** $P(A\cap B) = 0$ if disjoint, but $P(A)P(B) \ne 0$ because neither $P(A)$ nor $P(B) = 0$	 $P(A\cap B) = P(A)P(B)$ Ex. P(Queen ∩ King) when drawing TWO cards WITH replacement
Independent	**No** **If $P(B) \ne P(B\|A)$** *Knowing that A has occurred DOES affect the probability that B occurs $P(A\cap B) = P(A)P(B\|A)$	 $P(A\cap B) = 0$ Ex. P(Queen ∩ King) when drawing ONE card	 $P(A\cap B) \ne P(A)P(B)$ Ex. P(Queen ∩ King) when drawing TWO cards withOUT replacement

Random Variables:
$X = \sum X_i$
Binomial Distribution:
Use this when you need to count # of something
$\Pr[X = i] = \binom{n}{i}p^i(1-p)^{n-i}$
$\Pr[X \ge n] = \sum_{i=n}^{n+k}\binom{n+k}{i}(1-p)^i p^{n+k-i}$
$E[X] = np$
$Var(X) = np(1-p)$
Expectation:
$E[X] = \sum_{a\in A} a \times \Pr[X = a]$
Linearity of Expectation:
$E[X + Y] = E[X] + E[Y]$
$E[cX] = cE[X]$
If X and Y are independent: $E[XY] = E[X]E[Y]$
$Var(X) = E[X^2] - E[X]^2$
$E[X^2] = E[(\sum_{i=1}^{n} X_i)^2] = E[\sum_{i=1}^{n} X^2 + \sum_{i\ne j} X_i X_j]$
Basically care about Var(x)=E((X-mean)^2)
For **Independent Random Vars**:
$Var[cX] = c^2Var[X]$ for ANY
$Var[X + Y] = Var[X] + Var[Y]$
Covariance of X and Y: $E(XY) - E(X)E(Y)$
If two discrete independent random vars are added together, joint densities are summed and mul together.
Poiss(X+Y=z)=f(X+Y=z)=$\sum_{i=0}^{z} f(X = i)f(Y = i)$
Chebyshev:
$\Pr[|X - \mu| \ge \alpha] \le \frac{Var(X)}{\alpha^2}$

2-sided: Pr[|X-E[X]|≥a]≤ $\frac{Var(X)}{a^2}$, from here we get Pr [|X-E[X]|≥Bσ]=$\frac{1}{B^2}$, plug in a=Bσ. Pf: Using Markov, Pr[Var(X)≥ a^2]≤ $\frac{E(Var(X))}{a^2}$=$\frac{Var(X)}{a^2}$■
Markov: $\Pr[X \ge \alpha] \le \frac{E[X]}{\alpha}$
Markov's ineq: 1-sided: if X is nonneg, Pr[X≥a]≤ $\frac{E[X]}{a}$.Pf:want to show E[X]≥aPr[X≥a],
E[X]=$\sum_{i<a} iPr$[X=i]+$\sum_{i\ge a} Pr$[X=i])≥0+$\sum_{i\ge a} aPr$[X=i]rounding down≥a$\sum_{i\ge a}$ Pr[X=i]=aPr[X≥a]■
Discrete Distributions
$\Pr[X \ge i] = \sum_{i}^{\infty} \Pr[X = i]$
$E[X] = \sum_{i=1}^{\infty} i \times \Pr[X \ge i]$ if X nonneg rv
Geometric: Used when finding things until the final
Ex – coin flips until 1st heads, wait # days before end condition
$\Pr[X = i] = (1-p)^{i-1}p$
$\Pr[X \ge i] = (1-p)^{i-1}$
$E[X] = \Pr[X \ge i] = \sum_{i=1}^{\infty}(1-p)^{i-1}p = \frac{a_1}{1-r} = \frac{1}{p}$
$Var(X) = \frac{p}{(1-p)^2}$
Poisson: Used with rare events
Ex – Geiger, misconnect phone calls, cases of disease, births per hour. Occurances happen randomly with some const density in contiunuous region
$\Pr[X = i] = e^{-\lambda}\frac{\lambda^i}{i!}$. Has parameter λ
$E[X] = \sum_{i=1}^{\infty} i \times \Pr[X \ge i] = \lambda$
$Var(X) = \lambda$. Use algebra and regular x^2 E{X^2}
Remember: $\sum_{i=0}^{\infty}\frac{\lambda^i}{i!} = e^\lambda$
Continuous Probability:
Probability Density Function(pdf):
$\Pr[a \le X \le b] = \int_a^b f(x)xdx$
$E[X] = \int_{\infty}^{\infty} xf(x)dx$
$Var(X) = \int_{-\infty}^{\infty} x^2f(x)dx - \left(\int_{-\infty}^{\infty} xf(x)dx\right)^2$
Joint Distribution: f(x,y), if indep, f(x)f(y)
Continuous Distributions:
Uniform: on interval [0, *l*]
With Discrete: Var(x)=$\frac{n^2-1}{12}$, E[X] = average
Pdf = 1/length
$E[X] = \int_0^l x\frac{1}{l}\,dx = \frac{l}{2}$, or the Average
Var(X) = $\frac{(b-a)^2}{12}$
Pr[a<X<b]=$\frac{length\ of\ [a,b]}{total\ length}$=$\frac{b-a}{l}$
Exponential:
Pdf = $\lambda e^{-\lambda x}$
$\Pr[X > t] = \int_t^{\infty} \lambda e^{-\lambda x}dx = e^{-\lambda t}$
$E[X] = \frac{1}{\lambda}$
$Var(X) = \frac{1}{\lambda^2}$
Normal:
Pdf = $\frac{1}{\sqrt{2\pi\sigma^2}}e^{-\frac{(x-\mu)^2}{2\sigma^2}}$
In a standard, E[X]=0, Var(X)=1
$\Pr[X \le a] = \Pr[Y \le \frac{(a-\mu)}{\sigma}]$
$\Pr[a \le Y \le b] = \frac{1}{\sqrt{2\pi}}\int_{\sigma a+\mu}^{\sigma b+\mu} e^{-\frac{(x-\mu)^2}{2\sigma^2}}$
$0 = E(Y) = E\left(\frac{(X-\mu)}{\sigma}\right) = \frac{E(X)-\mu}{\sigma}$
$1 = Var(Y) = Var\left(\frac{(X-\mu)}{\sigma}\right) = \frac{Var(X)}{\sigma^2}$
Central Limit Theorem:
$A'_n = \frac{(A_n-\mu)\sqrt{n}}{\sigma} = \sum_{i=1}^{n}\frac{X_i - n\mu}{\sigma\sqrt{n}}$
$\Pr[A'_n \le \alpha] \to \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\alpha} e^{-\frac{x^2}{2}}dx$
Modular Arithmetic:
-if x, y relatively prime, gcd(x, y)=1
ITS ONLY INVERTIBLE IF RELATIVELY PRIME
- d=gcd(x,y)=ax+by
-gcd(a+b, b)=gcd(a, b)
->gcd(a+b,b)=gcd(b, a+b mod b)=gcd(b,a)
RSA:
Function: $E(x) = x^e mod\ N$, N =pq ad 3 relatively prime to (p-1)(q-1)
Inverse: $D(x) = x^d mod\ N$, d is inverse e mod (p-1)(q-1)
Fermat's Little Theorm:

For any prime p, and $a \in \{1, \dots, p-1\}, a^{p-1} = 1 \ mod\ p$

Euclid:

Let $x \geq y$ and let q, r be natural numbers such x=yq+r and r < y. Then gcd(x, y)=gcd(r, y).

If gcd(x,y)=1, then there exists a,b in Z st ax+by=d

Pqr relatively prime, so pairs have only factor of 1, and themselves.

Polynomials:

Prop 1: Non zero poly of deg d has at most d roots. If line not x-axis, then it intersects at most d points

Prop 2: Given d+1 pairs, with all x distinct, unique poly p(x) of degree at most d.

Messing with points is exactly error correcting codes

Miss 1 point, p possible points (given mod p)

Miss all points, p^d+1 possible points

ECC:

Send additional packets to make up for the errors

Erasure Errors:

1) By prop 2 of poly, reconstruct P(x) from values at any n dinstinct points since it has deg n-1. If we lose k packets, send **n+k** packets over

General Errors:

- Send over **n+2k** packets. With k packets corrupted.
- Compute poly Q(X) and E(X), where Q is $a_{n+k-1}x^{n+k-1} + \cdots + a_1x + a_0$ and E(X) is $x^k + b_{(k-1)x}x^{k-1} + \cdots + b_1x + b_0$

General Steps:

1) Suppose k chars are expect to corrupt.
2) Establish E(x)
3) Establish Q(x)
4) Use System of Linear Eqs plug in x vals wth finite field, and set equal to r_xE(x)
5) solve systems
6) Solve for P(x)=Q(x)/E(x)

Graphs:

Definitions: Path – sequence of edges from on pt to another

Walk – path with repeated vertices

Cycle – start and end on same node

Tour – walk that starts and ends on same vertices

Connected – has a pth between any two vertices

Euler Walks/Tours:

Walk – walk each edge exact once

Tour – Tour that uses each edge exact once

THM: undirected graph G=(V,E) has euler tour iff graph is connected and even degree for each nodes.

Claims: 1) even degree, walk from u can only get stuck at u. 2) remove a tour from even deg = even deg graph 3) If A doesn't contain all edges, then there is a vertex that A passes through that does not contain edge v.

--

Directed graph G=(V,E) has euler tour iff graph is connected and has indegree equal to outdegree

Euler path only if out degree greater than indegree.

Euler undir path only if two vertex odd degree

De Brujin:

A 2^n bit circular sequence such that every string of length n occurs as a contiguous substring of the sequence exactly once. (finit state?)

Hypercubes:

n-dimensional hypercube has 2 n-1 dimensional hypercubes. Each node has degree n.

Every node adjacent has 1 bit difference

|E_S|>=|S|

Total edges is $n2^{n-1}$

Coupon Collector/Baseball Card:

n types of coupons, X=# of boxes until have ≥1 of every coupon. X=$X_1 + \cdots + X_n$, $X_i$is # of boxes after see (i-1)th new coupon until see ith coupon. $X_i = geom\left(\frac{n-(i-1)}{n}\right)$, $\text{E}[X_i] = \frac{n}{n-(i-1)}$, E[X]=$\sum E[X_i] \leq n(1+\ln(n)) \approx n ln(n)$

Memoryless/Cumulative Distr Func:

GEOM and EXP distr are memoryless:

$$\Pr[X > m + n | X > m] = \Pr[X > n]$$

The cumulative Distr Funct F(a) := $\Pr[X \leq a]$. Shows the same thing as the distribution.