Back to work...with some review.

Probability Space: Ω, $Pr : \Omega \to [0,1]$, $\sum_{\omega \in \Omega} Pr(w) = 1$.
Random Variables: $X : \Omega \to R$.
  Associated event: $Pr[X = a] = \sum_{\omega : X(\omega) = a} Pr(\omega)$
Independent X and Y if and only if all associated events are independent.
Expectation: $E[X] = \sum_a aPr[X = a] = \sum_{\omega in \Omega} Pr(\omega)$.
  Linearity: $E[X + Y] = E[X] + E[Y]$.

Variance: $Var(X) = E[(X - E[X])^2] = E[X^2] - (E(X))^2$
  For independent X, Y, $Var(X + Y) = Var(X) + Var(Y)$.
  Also: $Var(cX) = c^2 Var(X)$ and $Var(X + b) = Var(X)$.

$X \sim P(\lambda)$ $E(X) = \lambda$, $Var(X) = \lambda$.
$X \sim B(n,p)$ $E(X) = np$, $Var(X) = np(1-p)$
$X \sim U\{1,\ldots,n\}$ $E[X] = \frac{n+1}{2}$, $Var(X) = \frac{n^2-1}{12}$.

Markov.

Markov:
 For increasing function $f(x) \to R^+$, $Pr[X \geq a] \leq \frac{E[f(X)]}{f(a)}$.

Simple Markov: Not so many can be way above average.
 For positive random variable, X, $Pr[X \geq a] \leq \frac{E[X]}{a}$.
Proof: Take $f(x) = x$ in Markov. $\square$.

Proof of Markov: Use random variable $Y = f(X)$ in Simple Markov. $\square$.

Circular!

Proof of Simple Markov:
$E[X] = \sum_x xPr[X = x] \geq \sum_{x \geq a} xPr[X = x]$
$\geq \sum_{x \geq a} aPr[X = x] = a\sum_{x \geq a} Pr[X = x] = aPr[X \geq a]$. $\square$

Markov Inequality Example: $P(\lambda)$

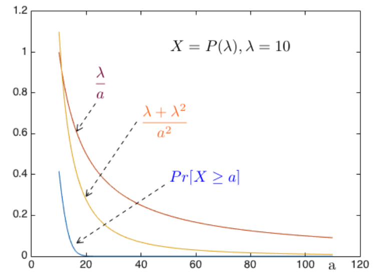
Let $X = P(\lambda)$. Recall that $E[X] = \lambda$, $Var(X) = \lambda$ and so $E[X^2] = \lambda + \lambda^2$.

Choosing $f(x) = x$, we get

$$Pr[X \geq a] \leq \frac{E[X]}{a} = \frac{\lambda}{a}.$$

Choosing $f(x) = x^2$, we get

$$Pr[X \geq a] \leq \frac{E[X^2]}{a^2} = \frac{\lambda + \lambda^2}{a^2}.$$



Chebyshev's Inequality

This is Pafnuty's inequality:
Theorem:

$$Pr[|X - E[X]| > a] \leq \frac{var[X]}{a^2}, \text{ for all } a > 0.$$

Proof: Let $Y = |X - E[X]|$ and $f(y) = y^2$. Then,

$$Pr[Y \geq a] \leq \frac{E[f(Y)]}{f(a)} = \frac{var[X]}{a^2}.$$

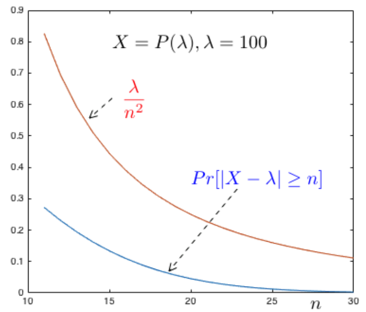
$\square$

Yes! The variance does measure the "deviations from the mean."

Chebyshev and Poisson

Let $X = P(\lambda)$. Then, $E[X] = \lambda$ and $var[X] = \lambda$. Thus,

$$Pr[|X - \lambda| \geq n] \leq \frac{var[X]}{n^2} = \frac{\lambda}{n^2}.$$



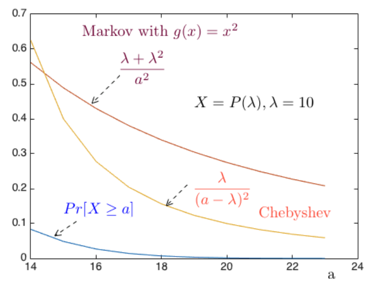
Chebyshev and Poisson (continued)

Let $X = P(\lambda)$. Then, $E[X] = \lambda$ and $var[X] = \lambda$. By Markov's inequality,

$$Pr[X \geq a] \leq \frac{E[X^2]}{a^2} = \frac{\lambda + \lambda^2}{a^2}.$$

Also, if $a > \lambda$, then $X \geq a \Rightarrow X - \lambda \geq a - \lambda > 0 \Rightarrow |X - \lambda| \geq a - \lambda$.

Hence, for $a > \lambda$, $Pr[X \geq a] \leq Pr[|X - \lambda| \geq a - \lambda] \leq \frac{\lambda}{(a-\lambda)^2}$.



Fraction of H's

Here is a classical application of Chebyshev's inequality.

How likely is it that the fraction of H's differs from 50%?

Let $X_m = 1$ if the m-th flip of a fair coin is H and $X_m = 0$ otherwise.

Define

$$Y_n = \frac{X_1 + \cdots + X_n}{n}, \text{ for } n \geq 1.$$

We want to estimate

$$Pr[|Y_n - 0.5| \geq 0.1] = Pr[Y_n \leq 0.4 \text{ or } Y_n \geq 0.6].$$

By Chebyshev,

$$Pr[|Y_n - 0.5| \geq 0.1] \leq \frac{var[Y_n]}{(0.1)^2} = 100 var[Y_n].$$

Now,

$$var[Y_n] = \frac{1}{n^2}(var[X_1] + \cdots + var[X_n]) = \frac{1}{n} var[X_1] \leq \frac{1}{4n}.$$

$Var(X_i) = p(1 - lp) \leq (.5)(.5) = \frac{1}{4}$

Fraction of H's

$$Y_n = \frac{X_1 + \cdots + X_n}{n}, \text{ for } n \geq 1.$$

$$Pr[|Y_n - 0.5| \geq 0.1] \leq \frac{25}{n}.$$

For $n = 1,000$, we find that this probability is less than 2.5%.

As $n \to \infty$, this probability goes to zero.

In fact, for any $\varepsilon > 0$, as $n \to \infty$, the probability that the fraction of Hs is within $\varepsilon > 0$ of 50% approaches 1:

$$Pr[|Y_n - 0.5| \leq \varepsilon] \to 1.$$

This is an example of the Law of Large Numbers.

We look at a calculation of this next.

Weak Law of Large Numbers

Theorem Weak Law of Large Numbers

Let $X_1, X_2, \ldots$ be pairwise independent with the same distribution and mean μ. Then, for all $\varepsilon > 0$,

$$Pr[|\frac{X_1 + \cdots + X_n}{n} - \mu| \geq \varepsilon] \to 0, \text{ as } n \to \infty.$$

Proof:
Let $Y_n = \frac{X_1 + \cdots + X_n}{n}$. Then

$$\begin{aligned} Pr[|Y_n - \mu| \geq \varepsilon] &\leq \frac{var[Y_n]}{\varepsilon^2} = \frac{var[X_1 + \cdots + X_n]}{n^2\varepsilon^2} \\ &= \frac{nvar[X_1]}{n^2\varepsilon^2} = \frac{var[X_1]}{n\varepsilon^2} \to 0, \text{ as } n \to \infty. \end{aligned}$$

□

Summary

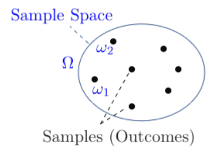
$\boxed{\text{Variance; Inequalities; WLLN}}$

- Variance: $var[X] := E[(X - E[X])^2] = E[X^2] - E[X]^2$
- Fact: $var[aX + b] = a^2 var[X]$
- Sum: X, Y, Z pairwise ind. $\Rightarrow var[X + Y + Z] = \cdots$
- Markov: $Pr[X \geq a] \leq E[f(X)]/f(a)$ where ...
- Chebyshev: $Pr[|X - E[X]| \geq a] \leq var[X]/a^2$
- WLLN: X_m i.i.d. $\Rightarrow \frac{X_1 + \cdots + X_n}{n} \approx E[X]$

Probability: Midterm 2 Review.

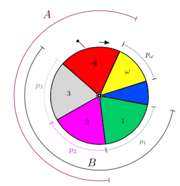
- Framework:
  - Probability Space
  - Conditional Probability & Bayes' Rule
  - Independence
  - Mutual Independence

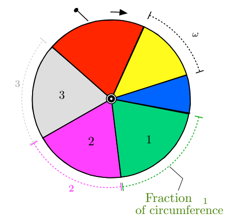
Review: Probability Space



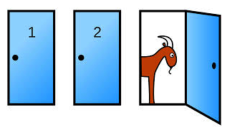
$0 \leq Pr[\omega] \leq 1$

$\sum_\omega Pr[\omega] = 1$



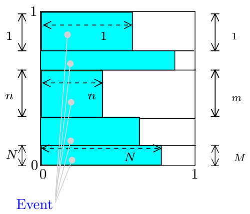


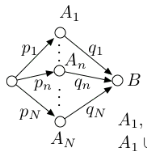
$Pr[A|B] = Pr[A \cap B]/Pr[B]$.
$Pr[A \cap B \cap C]$
$= Pr[A]Pr[B|A]Pr[C|A \cap B]$.



Review: Bayes' Rule

- Priors: $Pr[A_n] = p_n, n = 1, \ldots, M$
- Conditional Probabilities: $Pr[B|A_n] = q_n, n = 1, \ldots, N$
- $\Rightarrow$ Posteriors: $Pr[A_n|B] = \frac{p_n q_n}{p_1 q_1 + \cdots + p_N q_N}$





$p_n = Pr[A_n]$
$q_n = Pr[B|A_n]$

$A_1, \ldots, A_N$ disjoint
$A_1 \cup \cdots \cup A_N = \Omega$

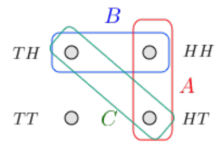
Bayes' Rule: Examples

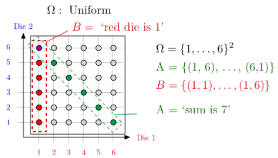
Let $p'_n = Pr[A_n|B]$ be the posterior probabilities.
Thus, $p'_n = p_n q_n / (p_1 q_1 + \cdots + p_N q_N)$.

Questions: Is it true that

- if $q_n > q_k$, then $p'_n > p'_k$? Not necessarily.
- if $p_n > p_k$, then $p'_n > p'_k$? Not necessarily.
- if $p_n > p_k$ and $q_n > q_k$, then $p'_n > p'_k$? Yes.
- if $q_n = 1$, then $p'_n > 0$? Not necessarily.
- if $p_n = 1/N$ for all n, then MLE = MAP? Yes.

Review: Independence





"First coin yields 1" and "Sum is 7" are independent

Pairwise, but not mutually

If $\{A_j, i \in J\}$ are mutually independent, then $[A_1 \cap \bar{A}_2] \Delta A_3$ and $A_4 \setminus A_5$ are independent.

Our intuitive meaning of "independent events" is mutual independence.

Review: Independence

Recall

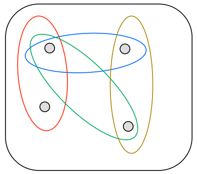
- A and B are independent if $Pr[A \cap B] = Pr[A]Pr[B]$.
- $\{A_j, j \in J\}$ are mutually independent if
  $Pr[\cap_{j \in K} A_j] = \Pi_{j \in K} Pr[A_j], \forall$ finite $K \subset J$.

Thus, A, B, C, D are mutually independent if there are

- independent 2 by 2:
  $Pr[A \cap B] = Pr[A]Pr[B], \ldots, Pr[C \cap D] = Pr[C]Pr[D]$
- by 3: $Pr[A \cap B \cap C] = Pr[A]Pr[B]Pr[C], \ldots, Pr[B \cap C \cap D] = Pr[B]Pr[C]Pr[D]$
- by 4: $Pr[A \cap B \cap C \cap D] = Pr[A]Pr[B]Pr[C]Pr[D]$.

Independence: Question

Consider the uniform probability space and the events A, B, C, D.



Which maximal collections of events among A, B, C, D are pairwise independent?

$\{A, B, C\}$, and $\{B, C, D\}$

Can you find three events among A, B, C, D that are mutually independent?

No: We would need an outcome with probability $1/8$.

Review: Collisions & Collecting

Collisions:

$$Pr[\text{no collision}] \approx e^{-m^2/2n}$$

Collecting:

$$Pr[\text{miss Wilson}] \approx e^{-m/n}$$

$$Pr[\text{miss at least one}] \leq ne^{-m/n}$$

Review: Math Tricks

Approximations:

$$\ln(1-\varepsilon) \approx -\varepsilon$$
$$\exp\{-\varepsilon\} \approx 1-\varepsilon$$

Sums:

$$(a+b)^n = \sum_{m=0}^{n} \binom{n}{m} a^m b^{n-m}$$
$$1+2+\cdots+n = \frac{n(n+1)}{2};$$

Math Tricks, continued

Symmetry: E.g., if we pick balls from a bag, with no replacement,

$$Pr[\text{ball 5 is red}] = Pr[\text{ball 1 is red}]$$

Order of balls = permutation.

All permutations have same probability.
Union Bound:

$$Pr[A \cup B \cup C] \le Pr[A] + Pr[B] + Pr[C]$$

Inclusion/Exclusion:

$$Pr[A \cup B] = Pr[A] + Pr[B] - Pr[A \cap B]$$

Total Probability:

$$Pr[B] = Pr[A_1]Pr[B|A_1] + \cdots + Pr[A_n]Pr[B|A_n]$$

An L^2-bounded martingale converges almost surely. Just kidding!

A mini-quizz

True or False:

- $Pr[A \cup B] = Pr[A] + Pr[B]$. False True iff disjoint.
- $Pr[A \cap B] = Pr[A]Pr[B]$. False True iff independent.
- $A \cap B = \emptyset \Rightarrow A, B$ independent. False
- For all A, B, one has $Pr[A|B] \ge Pr[A]$. False
- $Pr[A \cap B \cap C] = Pr[A]Pr[B|A]Pr[C|B]$. False

A mini-quizz; part 2

- $\Omega = \{1,2,3,4\}$, uniform. Find events A, B, C that are pairwise independent, not mutually.

  $A = \{1,2\}, B = \{1,3\}, C = \{1,4\}$.
- A, B, C pairwise independent. Is it true that $(A \cap B)$ and C are independent?

  No. In example above, $Pr[A \cap B \cap C] \ne Pr[A \cap B]Pr[C]$.
- Assume $Pr[C|A] > Pr[C|B]$.

  Is it true that $Pr[A|C] > Pr[B|C]$?

  No.
- Deal two cards from a 52-card deck. What is the probability that the value of the first card is strictly larger than that of the second?

  $Pr[\text{same}] = \frac{3}{51}$. $Pr[\text{different}] = \frac{48}{51}$. $Pr[\text{first} > \text{second}] = \frac{24}{51}$.

Discrete Math:Review

Modular Arithmetic Inverses and GCD

x has inverse modulo m if and only if $gcd(x,m) = 1$.

Group structures more generally.

Proof Idea:
$\{0x, \ldots, (m-1)x\}$ are distinct modulo m if and only if $gcd(x,m) = 1$.

Finding gcd.
$gcd(x,y) = gcd(y, x-y) = gcd(y, x \pmod y)$.

Give recursive Algorithm! Base Case? $gcd(x,0) = x$.

Extended-gcd(x,y) returns (d,a,b)
$d = gcd(x,y)$ and $d = ax + by$

Multiplicative inverse of (x,m).
egcd$(x,m) = (1,a,b)$
a is inverse! $1 = ax + bm = ax \pmod m$.

Idea: egcd.
gcd produces 1
by adding and subtracting multiples of x and y

Example: $p = 7$, $q = 11$.

$N = 77$.
$(p-1)(q-1) = 60$
Choose $e = 7$, since $\gcd(7,60) = 1$.
egcd(7,60).

$$\begin{aligned} 7(0)+60(1) &= 60 \\ 7(1)+60(0) &= 7 \\ 7(-8)+60(1) &= 4 \\ 7(9)+60(-1) &= 3 \\ 7(-17)+60(2) &= 1 \end{aligned}$$

Confirm: $-119+120 = 1$

$d = e^{-1} = -17 = 43 = \pmod{60}$

Fermat from Bijection.

Fermat's Little Theorem: For prime p, and $a \not\equiv 0 \pmod{p}$,

$a^{p-1} \equiv 1 \pmod{p}$.

Proof: Consider $T = \{a \cdot 1 \pmod{p}, \ldots, a \cdot (p-1) \pmod{p}\}$.

T is range of function $f(x) = ax \mod (p)$ for set $S = \{1, \ldots, p-1\}$.
Invertible function: one-to-one.
$T \subseteq S$ since $0 \notin T$.
p is prime.
$\implies T = S$.
Product of elts of T = Product of elts of S.

$$(a \cdot 1) \cdot (a \cdot 2) \cdots (a \cdot (p-1)) \equiv 1 \cdot 2 \cdots (p-1) \mod p,$$

Since multiplication is commutative.

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

Each of $2, \ldots (p-1)$ has an inverse modulo p,
mulitply by inverses to get...

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

□

RSA

RSA:
$N = p, q$
e with $\gcd(e, (p-1)(q-1)) = 1$.
$d = e^{-1} \pmod{(p-1)(q-1)}$.

Theorem: $x^{ed} = x \pmod{N}$

Proof:
$x^{ed} - x$ is divisible by p and $q \implies$ theorem!

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

If x is divisible by p, the product is.
Otherwise $(x^{k(q-1)})^{p-1} = 1 \pmod{p}$ by Fermat.
$\implies (x^{k(q-1)})^{p-1} - 1$ divisible by p.

Similarly for q.

□

RSA, Public Key, and Signatures.

RSA:
$N = p, q$
e with $\gcd(e, (p-1)(q-1))$.
$d = e^{-1} \pmod{(p-1)(q-1)}$.

Public Key Cryptography:

$D(E(m,K),k) = (m^e)^d \mod N = m$.

Signature scheme:

$S(C) = D(C)$.
Announce $(C, S(C))$

Verify: Check $C = E(C)$.

$E(D(C,k),K) = (C^d)^e = C \pmod{N}$

Polynomials

Property 1: Any degree d polynomial over a field has at most d roots.

Proof Idea:
Any polynomial with roots $r_1, \ldots, r_k$.
written as $(x-r_1)\cdots(x-r_k)Q(x)$.
using polynomial division.
Degree at least the number of roots.

□

Property 2: There is exactly 1 polynomial of degree $\leq d$ with arithmetic modulo prime p that contains any $d+1$:
$(x_1, y_1), \ldots, (x_{d+1}, y_{d+1})$ with x_i distinct.

Proof Ideas:
Lagrange Interpolation gives existence.
Property 1 gives uniqueness.

□

Applications.

Property 2: There is exactly 1 polynomial of degree $\leq d$ with arithmetic modulo prime p that contains any $d+1$ points:
$(x_1, y_1), \ldots, (x_{d+1}, y_{d+1})$ with x_i distinct.

Secret Sharing: k out of n people know secret.
Scheme: degree $n-1$ polynomial, $P(x)$.
Secret: $P(0)$ **Shares:** $(1, P(1)), \ldots (n, P(n))$.
Recover Secret: Reconstruct $P(x)$ with any k points.

Erasure Coding: n packets, k losses.
Scheme: degree $n-1$ polynomial, $P(x)$. Reed-Solomon.
Message: $P(0) = m_0, P(1) = m_1, \ldots P(n-1) = m_{n-1}$
Send: $(0, P(0)), \ldots (n+k-1, P(n+k-1))$.
Recover Message: Any n packets are cool by property 2.

Corruptions Coding: n packets, k corruptions.
Scheme: degree $n-1$ polynomial, $P(x)$. Reed-Solomon.
Message: $P(0) = m_0, P(1) = m_1, \ldots P(n-1) = m_{n-1}$
Send: $(0, P(0)), \ldots (n+2k-1, P(n+2k-1))$.
Recovery: $P(x)$ is only consistent polynomial with $n+k$ points.
Property 2 and pigeonhole principle.

Welsh-Berlekamp

Idea: Error locator polynomial of degree k with zeros at errors.

For all points $i = 1, \dots, i, n+2k$, $P(i)E(i) = R(i)E(i) \pmod p$
since $E(i) = 0$ at points where there are errors.
Let $Q(x) = P(x)E(x)$.

$Q(x) = a_{n+k-1}x^{n+k-1} + \cdots a_0$.
$E(x) = x^k + b_{k-1}x^{k-1} + \cdots b_0$.
Gives system of $n+2k$ linear equations.

$$\begin{aligned}
a_{n+k-1} + \dots a_0 &\equiv R(1)(1 + b_{k-1} \cdots b_0) \pmod p \\
a_{n+k-1}(2)^{n+k-1} + \dots a_0 &\equiv R(2)((2)^k + b_{k-1}(2)^{k-1} \cdots b_0) \pmod p \\
&\vdots \\
a_{n+k-1}(m)^{n+k-1} + \dots a_0 &\equiv R(m)((m)^k + b_{k-1}(m)^{k-1} \cdots b_0) \pmod p
\end{aligned}$$

..and $n+2k$ unknown coefficients of $Q(x)$ and $E(x)$!

Solve for coefficients of $Q(x)$ and $E(x)$.

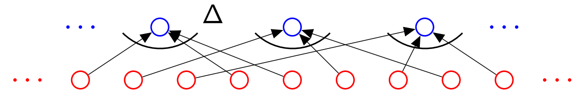
Find $P(x) = Q(x)/E(x)$.

Counting

First Rule
Second Rule
Stars/Bars
Common Scenarios: Sampling, Balls in Bins.
Sum Rule. Inclusion/Exclusion.
Combinatorial Proofs.

Example: visualize.

First rule: $n_1 \times n_2 \cdots \times n_3$. Product Rule.
Second rule: when order doesn't matter divide..when possible.

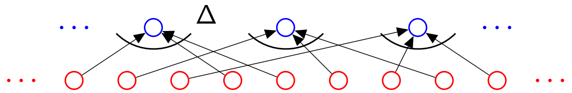


3 card Poker deals: $52 \times 51 \times 50 = \frac{52!}{49!}$. First rule.
Poker hands: Δ?
Hand: Q, K, A.
Deals: Q,K,A, Q,A,K, K,A,Q, K,A,Q, A,K,Q, A,Q,K.
$\Delta = 3 \times 2 \times 1$ First rule again.
Total: $\frac{52!}{49!3!}$ Second Rule!

Choose k out of n.
Ordered set: $\frac{n!}{(n-k)!}$
What is Δ? $k!$ First rule again.
$\implies$ Total: $\frac{n!}{(n-k)!k!}$ Second rule.

Example: visualize

First rule: $n_1 \times n_2 \cdots \times n_3$. Product Rule.
Second rule: when order doesn't matter divide..when possible.



Orderings of ANAGRAM?
Ordered Set: 7! First rule.
A's are the same!
What is Δ?
ANAGRAM
$A_1NA_2GRA_3M$, $A_2NA_1GRA_3M$, ...
$\Delta = 3 \times 2 \times 1 = 3!$ First rule!
$\implies \frac{7!}{3!}$ Second rule!

Summary.

k Samples with replacement from n items: n^k.
Sample without replacement: $\frac{n!}{(n-k)!}$

Sample without replacement and order doesn't matter: $\binom{n}{k} = \frac{n!}{(n-k)!k!}$.
"n choose k"
(Count using first rule and second rule.)

Sample with replacement and order doesn't matter: $\binom{k+n-1}{n-1}$.

Count with stars and bars:
how many ways to add up n numbers to get k.
Each number is number of samples of type i which adds to total, k.

Simple Inclusion/Exclusion

Sum Rule: For disjoint sets S and T, $|S \cup T| = |S| + |T|$

Example: How many permutations of n items start with 1 or 2?
$1 \times (n-1)! + 1 \times (n-1)!$

Inclusion/Exclusion Rule: For any S and T,
$|S \cup T| = |S| + |T| - |S \cap T|$.

Example: How many 10-digit phone numbers have 7 as their first or second digit?

S = phone numbers with 7 as first digit. $|S| = 10^9$

T = phone numbers with 7 as second digit. $|T| = 10^9$.

$S \cap T$ = phone numbers with 7 as first and second digit. $|S \cap T| = 10^8$.

Answer: $|S| + |T| - |S \cap T| = 10^9 + 10^9 - 10^8$.

Combinatorial Proofs.

Theorem: $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$.
Proof: How many size k subsets of $n+1$? $\binom{n+1}{k}$.

How many size k subsets of $n+1$?
How many contain the first element?
Chose first element, need to choose $k-1$ more from remaining n elements.
$\implies \binom{n}{k-1}$

How many don't contain the first element ?
Need to choose k elements from remaining n elts.
$\implies \binom{n}{k}$

So, $\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$. $\square$

Countability

Isomporphism principle.
Example.
Countability.
Diagonalization.

Isomorphism principle.

Given a function, $f : D \to R$.
One to One:
For all $\forall x, y \in D$, $x \neq y \implies f(x) \neq f(y)$.
or
$\forall x, y \in D$, $f(x) = f(y) \implies x = y$.

Onto: For all $y \in R$, $\exists x \in D, y = f(x)$.

$f(\cdot)$ is a **bijection** if it is one to one and onto.

Isomorphism principle:
If there is a bijection $f : D \to R$ then $|D| = |R|$.

Cardinalities of uncountable sets?

Cardinality of $[0,1]$ smaller than all the reals?

$f : R^+ \to [0,1]$.

$$f(x) = \begin{cases} x + \frac{1}{2} & 0 \leq x \leq 1/2 \\ \frac{1}{4x} & x > 1/2 \end{cases}$$

One to one. $x \neq y$
If both in $[0,1/2]$, a shift $\implies f(x) \neq f(y)$.
If neither in $[0,1/2]$ different mult inverses $\implies f(x) \neq f(y)$.
If one is in $[0,1/2]$ and one isn't, different ranges $\implies f(x) \neq f(y)$.
Bijection!

$[0,1]$ is same cardinality as nonnegative reals!

Countable.

Definition: S is **countable** if there is a bijection between S and some subset of N.

If the subset of N is finite, S has finite **cardinality**.

If the subset of N is infinite, S is **countably infinite**.

Bijection to or from natural numbers implies countably infinite.

Enumerable means countable.

Subset of countable set is countable.

All countably infinite sets are the same cardinality as each other.

Examples

Countably infinite (same cardinality as naturals)

- Z^+ - positive integers
  Where's 0?
  Bijection: $f(z) = z - 1$.
  (Where's 0? 1 Where's 1? 2 ...)
- E even numbers.
  Where are the odds? Half as big?
  Bijection: $f(e) = e/2$.
- Z- all integers.
  Twice as big?
  Bijection: $f(z) = 2|z| - sign(z)$.
  Enumerate: $0, -1, 1, -2, 2...$

Examples: Countable by enumeration

- $N \times N$ - Pairs of integers.
  Square of countably infinite?
  Enumerate: $(0,0),(0,1),(0,2),\ldots$???
  Never get to $(1,1)$!
  Enumerate: $(0,0),(1,0),(0,1),(2,0),(1,1),(0,2)\ldots$
  (a,b) at position $(a+b-1)(a+b)/2+b$ in this order.
- Positive Rational numbers.
  Infinite Subset of pairs of natural numbers.
  Countably infinite.
- All rational numbers.
  Enumerate: list 0, positive and negative. How?
  Enumerate: 0, first positive, first negative, second positive..
  Will eventually get to any rational.

Diagonalization: power set of Integers.

The set of all subsets of N.

Assume is countable.

There is a listing, L, that contains all subsets of N.

Define a diagonal set, D:
If ith set in L does not contain i, $i \in D$.
otherwise $i \notin D$.

D is different from ith set in L for every i.
$\implies$ D is not in the listing.

D is a subset of N.

L does not contain all subsets of N.

Contradiction.

Theorem: The set of all subsets of N is not countable.
(The set of all subsets of S, is the **powerset** of N.)

Uncomputability.

Halting problem is undecibable.

Diagonalization.

Halt does not exist.

$HALT(P,I)$
P - program
I - input.

Determines if $P(I)$ (P run on I) halts or loops forever.

Theorem: There is no program HALT.

Proof: Yes! No! Yes! No! No! Yes! No! Yes! .. $\square$

Halt and Turing.

Proof: Assume there is a program $HALT(\cdot,\cdot)$.

Turing(P)
1. If HALT(P,P) ="halts", then go into an infinite loop.
2. Otherwise, halt immediately.

Assumption: there is a program HALT.
There is text that "is" the program HALT.
There is text that is the program Turing.
Can run Turing on Turing!

Does Turing(Turing) halt?

Turing(Turing) halts
$\implies$ then HALTS(Turing, Turing) $=$ halts
$\implies$ Turing(Turing) loops forever.

Turing(Turing) loops forever.
$\implies$ then HALTS(Turing, Turing) $\neq$ halts
$\implies$ Turing(Turing) halts.

Either way is contradiction. Program HALT does not exist! $\square$

Another view: diagonalization.

Any program is a fixed length string.
Fixed length strings are enumerable.
Program halts or not any input, which is a string.

	P_1	P_2	P_3	$\cdots$
P_1	H	H	L	$\cdots$
P_2	L	L	H	$\cdots$
P_3	L	H	H	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Halt - diagonal.
Turing - is not Halt.
and is different from every P_i on the diagonal.
Turing is not on list. Turing is not a program.
Turing can be constructed from Halt.
Halt does not exist!

Undecidable problems.

Does a program print "Hello World"?
Find exit points and add statement: **Print** "Hello World."

Can a set of notched tiles tile the infinite plane?
Proof: simulate a computer. Halts if finite.

Does a set of integer equations have a solution?
Example: Ask program if " $x^n + y^n = 1$?" has integer solutions.
Problem is undecidable.

Be careful!

Is there a solution to $x^n + y^n = 1$?
(Diophantine equation.)

The answer is yes or no. This "problem" is not undecidable.

Undecidability for Diophantine set of equations
$\implies$ no program can take any set of integer equations
and always output correct answer.

Midterm format

Time: approximately 120 minutes.

Many short answers.
Get at ideas that we study.

Know material well:	fast, correct.
Know material medium:	slower, less correct.
Know material not so well:	Uh oh.

Some longer questions.

Priming: sequence of questions...
but don't overdo this as test strategy!!!

Ideas, conceptual,
more calculation.

Wrapup.

Watch Piazza for Logistics!
Watch Piazza for Advice!

If you sent me email about Midterm conflicts
Other arrangements.
Should have recieved an email today from me.

Other issues....
satishr@cs.berkeley.edu, admin@cs70.org
Private message on piazza.

Good Studying!!!!!!!!!!!!!!!!!