Midterm 2 Review.

We have a lot of slides for your use.
But will only cover some in this lecture.
For probability, from Professor Ramchandran.
Will only review distributions since that was quick.
A bit more review of discrete math.

An important remark

► The random experiment selects one and only one outcome in $\Omega$.
► For instance, when we flip a fair coin twice
  
  * $\Omega = \{HH, TH, HT, TT\}$
  * The experiment selects one of the elements of $\Omega$.

► In this case, it's wrong to think that $\Omega = \{H, T\}$ and that the experiment selects two outcomes.

► Why? Because this would not describe how the two coin flips are related to each other.

► For instance, say we glue the coins side-by-side so that they face up the same way. Then one gets $HH$ or $TT$ with probability 50% each. This is not captured by ‘picking two outcomes.’

Probability Space.

1. A “random experiment”:
   - (a) Flip a biased coin;
   - (b) Flip two fair coins;
   - (c) Deal a poker hand.

2. A set of possible outcomes: $\Omega$.
   - (a) $\Omega = \{H, T\}$;
   - (b) $\Omega = \{HH, HT, TH, TT\}$; $|\Omega| = 4$;
   - (c) $\Omega = \{A\spadesuit, A\heartsuit, A\diamondsuit, A\clubsuit, \spadesuit, \heartsuit, \diamondsuit, \clubsuit, \ldots\}$
   - $|\Omega| = \binom{52}{5}$.

3. Assign a probability to each outcome: $Pr: \Omega \rightarrow [0, 1]$.
   - (a) $Pr[H] = p, Pr[T] = 1 - p$ for some $p \in [0, 1]$
   - (b) $Pr[HH] = Pr[HT] = Pr[TH] = Pr[TT] = \frac{1}{4}$
   - (c) $Pr[\spadesuit, \heartsuit, \diamondsuit, \clubsuit, \spadesuit, \ldots] = \frac{1}{\binom{52}{5}}$

4. Assign a probability to each outcome: $Pr: \Omega \rightarrow [0, 1]$.
   - (a) $Pr[H] = p, Pr[T] = 1 - p$ for some $p \in [0, 1]$
   - (b) $Pr[HH] = Pr[HT] = Pr[TH] = Pr[TT] = \frac{1}{4}$
   - (c) $Pr[\spadesuit, \heartsuit, \diamondsuit, \clubsuit, \spadesuit, \ldots] = \frac{1}{\binom{52}{5}}$

Probability Basics Review

Setup:

► Random Experiment.
  Flip a fair coin twice.

► Probability Space.
  
  * Sample Space: Set of outcomes, $\Omega$. $\Omega = \{HH, HT, TH, TT\}$
  (Note: Not $\Omega = \{H, T\}$ with two picks!)

  * Probability: $Pr[\omega]$ for all $\omega \in \Omega$.
    $Pr[HH] = \cdots = Pr[TT] = \frac{1}{4}$
  1. $0 \leq Pr[\omega] \leq 1$
  2. $\sum_{\omega \in \Omega} Pr[\omega] = 1$.

Probability Space: formalism.

$\Omega$ is the sample space.
$\omega \in \Omega$ is a sample point. (Also called an outcome.)
Sample point $\omega$ has a probability $Pr[\omega]$ where

- $0 \leq Pr[\omega] \leq 1$;
- $\sum_{\omega \in \Omega} Pr[\omega] = 1$.

Probability of exactly one ‘heads’ in two coin flips?

Idea: Sum the probabilities of all the different outcomes that have exactly one ‘heads’: $HT, TH$.

This leads to a definition!

Definition:

► An event, $E$, is a subset of outcomes: $E \subseteq \Omega$.
► The probability of $E$ is defined as $Pr[E] = \sum_{\omega \in E} Pr[\omega]$.

Probability of exactly one ‘heads’ in two coin flips?

Idea: Sum the probabilities of all the different outcomes that have exactly one ‘heads’: $HT, TH$.

This leads to a definition!

Definition:

► An event, $E$, is a subset of outcomes: $E \subseteq \Omega$.
► The probability of $E$ is defined as $Pr[E] = \sum_{\omega \in E} Pr[\omega]$.

Sample Space:

$\Omega = \{\omega_1, \omega_2, \ldots\}$
$Pr[\Omega] = \sum_{\omega \in \Omega} Pr[\omega]$.
Probability of exactly one heads in two coin flips?

Sample Space, \( \Omega = \{ HH, HT, TH, TT \} \).

Uniform probability space: 
\[
\Pr[HH] = \Pr[HT] = \Pr[TH] = \Pr[TT] = \frac{1}{4}.
\]

Event, \( E \), “exactly one heads”: \( \{ TH, HT \} \).

\[
\Pr[E] = \sum_{\omega \in E} \Pr[\omega] = \frac{|E|}{|\Omega|} = \frac{1}{2}.
\]

Consequences of Additivity

Theorem

(a) \( \Pr[A \cup B] = \Pr[A] + \Pr[B] - \Pr[A \cap B] \); 
(inclusion-exclusion property)

(b) \( \Pr[A_1 \cup \cdots \cup A_n] \leq \Pr[A_1] + \cdots + \Pr[A_n] \); 
(union bound)

(c) If \( A_1, \ldots, A_N \) are a partition of \( \Omega \), i.e., pairwise disjoint and \( \bigcup_{n=1}^{N} A_n = \Omega \), then 
\[
\Pr[B] = \Pr[B \cap A_1] + \cdots + \Pr[B \cap A_N].
\]
(law of total probability)

Total probability

Assume that \( \Omega \) is the union of the disjoint sets \( A_1, \ldots, A_N \).

Then,
\[
\Pr[B] = \Pr[A_1 \cap B] + \cdots + \Pr[A_N \cap B].
\]
Indeed, \( B \) is the union of the disjoint sets \( A_n \cap B \) for \( n = 1, \ldots, N \).

In “math”: \( a \in B \) is in exactly one of \( A_n \cap B \). 
Adding up probability of them, get \( \Pr[\alpha] \) in sum.

Conditional Probability.

Toss a red and a blue die, sum is 7, 
what is probability that red is 1?

\[
\Pr[B|A] = \frac{|B \cap A|}{|A|} = \frac{1}{6}.
\]

Yet more fun with conditional probability.

Toss a red and a blue die, sum is 7, 
what is probability that red is 1?

\[
\Pr[B|A] = \frac{|B \cap A|}{|A|} = \frac{1}{6}.
\]

Observing \( A \) does not change your mind about the likelihood of \( B \).

Product Rule

Recall the definition:
\[
\Pr[B|A] = \frac{\Pr[A \cap B]}{\Pr[A]}.
\]

Hence,
\[
\Pr[A \cap B] = \Pr[A] \Pr[B|A].
\]

Consequently, 
\[
\Pr[A \cap B \cap C] = \Pr[(A \cap B) \cap C] = \Pr[A \cap B] \Pr[C|A \cap B] = \Pr[A] \Pr[B|A] \Pr[C|A \cap B].
\]
Theorem Product Rule
Let $A_1, A_2, \ldots, A_n$ be events. Then

\[ P[A_1 \cap \cdots \cap A_n] = P[A_1]P[A_2|A_1] \cdots P[A_n|A_1 \cap \cdots \cap A_{n-1}] \]

Proof: By induction.
Assume the result is true for $n$ (It holds for $n = 2$.) Then,

\[
\begin{align*}
P[A_1 \cap \cdots \cap A_n] &= P[A_1 \cap \cdots \cap A_{n-1}]P[A_n|A_1 \cap \cdots \cap A_{n-1}] \\
&= P[A_1]P[A_2|A_1] \cdots P[A_n|A_1 \cap \cdots \cap A_{n-1}] \\
&= P[A_1]P[A_2|A_1] \cdots P[A_n|A_1 \cap \cdots \cap A_{n-1}],
\end{align*}
\]

so that the result holds for $n + 1$. \qed

Is your coin loaded?

A picture:

<table>
<thead>
<tr>
<th>Fair coin</th>
<th>( \frac{1}{2} ) ( \frac{1}{2} ) ( 0.6 ) ( 0.4 ) ( 0.2 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loaded coin</td>
<td>( \frac{1}{2} ) ( \frac{1}{2} ) ( \frac{1}{2} ) ( \frac{1}{2} ) ( \frac{1}{2} )</td>
</tr>
</tbody>
</table>

Definition: Two events $A$ and $B$ are independent if

\[ P[A \cap B] = P[A]P[B]. \]

Examples:

- When rolling two dice, $A =$ sum is 7 and $B =$ red die is 1 are independent;
- When rolling two dice, $A =$ sum is 3 and $B =$ red die is 1 are not independent;
- When flipping coins, $A =$ coin 1 yields heads and $B =$ coin 2 yields tails are independent;
- When throwing 3 balls into 3 bins, $A =$ bin 1 is empty and $B =$ bin 2 is empty are not independent;

Fact: Two events $A$ and $B$ are independent if and only if

\[ P[A|B] = P[A]. \]

Indeed: $P[A|B] = \frac{P[A \cap B]}{P[B]}$; so that

Bayes Rule

Another picture: We imagine that there are $N$ possible causes $A_1, \ldots, A_N$.

![Bayes Rule Diagram]

Why do you have a fever?

Using Bayes’ rule, we find

$$
\Pr[\text{Flu}|\text{High Fever}] = \frac{0.15 \times 0.80}{0.15 \times 0.80 + 10^{-8} \times 1 + 0.85 \times 0.1} \approx 0.58
$$

These are the posterior probabilities. One says that ‘Flu’ is the Most Likely a Posteriori (MAP) cause of the high fever.

Summary

Events, Conditional Probability, Independence, Bayes’ Rule

Key Ideas:
- Conditional Probability:
  \( \Pr[A|B] = \frac{\Pr[A \cap B]}{\Pr[B]} \)
- Independence: \( \Pr[A \cap B] = \Pr[A] \Pr[B] \).
- Bayes’ Rule:
  \( \Pr[A|B] = \frac{\Pr[A] \Pr[B|A]}{\sum \Pr[A_i] \Pr[B|A_i]} \)

Balls in bins

One throws $m$ balls into $n > m$ bins.

![Balls in bins Diagram]

**Theorem:**

\( \Pr[\text{no collision}] = \exp\left(-\frac{m^2}{2n}\right) \), for large enough $n$.

In particular, $\Pr[\text{no collision}] \approx 1/2$ for $m^2/2n \approx \ln(2)$, i.e.,

$$
m \approx \sqrt{2\ln(2)n} \approx 1.2\sqrt{n}.
$$

E.g., $1.2\sqrt{20} \approx 5.4$.

Roughly, $\Pr[\text{collision}] \approx 1/2$ for $m = \sqrt{n}$. ($e^{-0.5} \approx 0.6.$)

The Calculation.

- $A_i$ = no collision when $i$th ball is placed in a bin.
- $\Pr[A_1 \cap \cdots \cap A_n] = (1 - \frac{m}{n})^n$.
- $\Pr[\text{no collision}] = A_1 \cap \cdots \cap A_n$.

**Product rule:**

$$
\Pr[A_1 \cap \cdots \cap A_n] = \Pr[A_1] \Pr[A_2|A_1] \cdots \Pr[A_n|A_1 \cap \cdots \cap A_{n-1}]
$$

Hence,

$$
\ln(\Pr[\text{no collision}]) = \sum_{k=1}^{m-1} \ln\left(1 - \frac{k}{n}\right) \approx \sum_{k=1}^{m-1} \left(-\frac{k}{n}\right).
$$

(1) We used $\ln(1 - \varepsilon) = -\varepsilon$ for $|\varepsilon| \ll 1$.

(2) $1 + 2 + \cdots + m - 1 = (m-1)m/2$. 

Key Ideas:
- Conditional Probability:
  \( \Pr[A|B] = \frac{\Pr[A \cap B]}{\Pr[B]} \)
- Independence: \( \Pr[A \cap B] = \Pr[A] \Pr[B] \).
- Bayes’ Rule:
  \( \Pr[A|B] = \frac{\Pr[A] \Pr[B|A]}{\sum \Pr[A_i] \Pr[B|A_i]} \)

These are the posterior probabilities. One says that ‘Flu’ is the Most Likely a Posteriori (MAP) cause of the high fever.
Today's your birthday, it's my birthday too.

Probability that \( m \) people all have different birthdays?
With \( n = 365 \), one finds
\[
Pr[\text{collision}] \approx \frac{1}{2} \text{ if } m \approx 1.2 \sqrt{365} \approx 23.
\]

If \( m = 60 \), we find that
\[
Pr[\text{no collision}] \approx \exp\left\{ -\frac{m^2}{2n} \right\} = \exp\left\{ -\frac{60^2}{2 \times 365} \right\} \approx 0.007.
\]

If \( m = 366 \), then \( Pr[\text{no collision}] = 0 \). (No approximation here!)

Random Variables.

A random variable, \( X \), for an experiment with sample space \( \Omega \) is a function \( X : \Omega \to \mathbb{R} \).

Thus, \( X(\cdot) \) assigns a real number \( X(\omega) \) to each \( \omega \in \Omega \).

The function \( X(\cdot) \) is not random, not a variable!
What varies at random (from experiment to experiment)? The outcome!

Number of pips in two dice.

"What is the likelihood of getting \( n \) pips?"

\[
Pr[X = 10] = \frac{3}{36} = Pr[X - 1(10)]; \quad Pr[X = 8] = \frac{5}{36} = Pr[X^{-1}(8)].
\]

Named Distributions.

Some distributions come up over and over again.
...like "choose" or "stars and bars"....

Let's cover one for this review.
The binomial distribution.

Flip \( n \) coins with heads probability \( p \).

Random variable: number of heads.

**Binomial Distribution:**

\[ \Pr[X = i] \text{, for each } i. \]

How many sample points in event \( \omega \) if \( \omega \) has \( i \) heads?

\( i \) heads out of \( n \) coin flips \( \Rightarrow \binom{n}{i} \)

What is the probability of \( \omega \) if \( \omega \) has \( i \) heads?

Probability of heads in any position is \( p \).

Probability of tails in any position is \( (1 - p) \).

So, we get

\[ \Pr[\omega] = p^i (1-p)^{n-i}. \]

Probability of \( X = i \) is sum of \( \Pr[\omega] \), \( \omega \in \{ X = i \} \).

\[ \Pr[X = i] = \binom{n}{i} p^i (1-p)^{n-i}, i = 0, 1, \ldots, n : \text{B(n,p) distribution} \]

Summary

**Random Variables**

- A random variable \( X \) is a function \( X : \Omega \rightarrow \mathbb{R} \).
- \( \Pr[X = a] =: \Pr[X^{-1}(a)] = \Pr[\{ \omega \mid X(\omega) = a \}] \).
- \( \Pr[X \in A] =: \Pr[X^{-1}(A)] \).
- The distribution of \( X \) is the list of possible values and their probability: \( \{(a, \Pr[X = a]) \mid a \in A \} \).

Non-recursive extended gcd.

Example: \( p = 7, q = 11 \).

\( N = 77 \).

\((p-1)(q-1) = 60\)

Choose \( e = 7 \), since \( \gcd(7,60) = 1 \).

\( \text{egcd}(7,60) \).

\[
\begin{align*}
7(0) + 60(1) &= 60  \\
7(1) + 60(0) &= 7  \\
7(-8) + 60(1) &= 4  \\
7(9) + 60(-1) &= 3  \\
7(-17) + 60(2) &= 1
\end{align*}
\]

Confirm: \(-119 + 120 = 1\)

\( d = e^{-1} = -17 = 43 \equiv 1 \pmod{60} \)
Fermat from Bijection.

**Fermat’s Little Theorem:** For prime \( p \), and \( a \neq 0 \pmod{p} \),
\[
a^{p-1} = 1 \pmod{p}.
\]

**Proof:** Consider \( T = \{a \ 1 \pmod{p}, \ldots, a \ (p-1) \pmod{p}\} \).
\( T \) is range of function \( f(x) = ax \pmod{p} \) for set \( S = \{1, \ldots, p-1\} \).
Invertible function: one-to-one.
\( T \subset S \) since \( 0 \not\in T \).
\( p \) is prime.
\( \Rightarrow \ T \sim S \).
Product of elts of \( T = \text{Product of elts of } S \).
\( (a \ 1 \cdot (a \ 2) \cdots (a \ (p-1)) = 1 \ 2 \cdots (p-1) \pmod{p} \).
Since multiplication is commutative.
\( a^{p-1}(1 \cdots (p-1)) = (1 \cdots (p-1)) \pmod{p} \).
Each of \( 2 \cdots (p-1) \) has an inverse modulo \( p \),
multiply by inverses to get...
\( a^{p-1} = 1 \pmod{p} \).

Simple Chinese Remainder Theorem.

My love is won. Zero and One. Nothing and nothing done.
Find \( x = a \pmod{m} \) and \( x = b \pmod{n} \) where \( \gcd(m,n)=1 \).

**CRT Thm:** Unique solution \( \pmod{mn} \).

**Proof:**
Consider \( u = m(n^{-1}) \pmod{m} \).
\( u = 0 \pmod{n} \) \( \Rightarrow \ u = 1 \pmod{m} \).
Consider \( v = m(n^{-1}) \pmod{n} \),
\( v = 1 \pmod{n} \) \( \Rightarrow \ v = 0 \pmod{m} \).
Let \( x = au + bv \).
\( x = a \pmod{m} \) since \( bv = 0 \pmod{m} \) and \( au = a \pmod{m} \)
\( x = b \pmod{n} \) since \( au = 0 \pmod{n} \) and \( bv = b \pmod{n} \)

Only solution? If not, two solutions, \( x \) and \( y \).
\( (x \ y) = 0 \pmod{m} \) and \( (x \ y) = 0 \pmod{n} \).
\( \Rightarrow \ (x \ y) \) is multiple of \( n \) and since \( \gcd(m,n)=1 \).
\( \Rightarrow \ x = y = mn \Rightarrow \ x \ y \notin \{0, \ldots, mn-1\} \).
Thus, only one solution modulo \( mn \).

Chinese Remainder Theorem.

**Theorem:** There is a unique solution modulo \( \Pi/N \), to the system
\[
x = a_1 \pmod{n_1} \text{ and } \gcd(n_1, n_2) = 1.
\]
For \( x = 5 \pmod{7} \), \( x = 2 \pmod{11} \), \( x = 1 \pmod{3} \).
\[
x = 5 \cdot (11) \cdot (11) \cdot (11) \cdot (7) \cdot (3) \cdot (3) \cdot (7) \cdot (11) = 2\cdot 7 \cdot 4 \cdot 3 \cdot 7 \cdot 3 \cdot 11 \cdot 11 \cdot (mod 3)
\]
This is all modulo \( 11 \cdot 7 \cdot 3 = 231 \).
For each modulus \( n_i \),
multiply all other moduli by the inverses \( \pmod{n_i} \)
and scale by \( a_i \).

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 \( (x-r_1) \cdots (x-r_k) \Omega(x) \),
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.

RSA

**RSA:**
\[
N = p \cdot q
\]
e with \( \gcd(e, (p - 1)(q - 1)) = 1 \).
\[
d = e^{-1} \pmod{(p - 1)(q - 1)}.
\]
**Theorem:** \( x^ed = x \pmod{n} \)

**Proof:**
\[
x^ed - x = x^{(p-1)(q-1)+1} - x = x((x^{(q-1)})^{p-1} - 1)
\]
If \( x \) is divisible by \( p \), the product is.
Otherwise \( (x^{(q-1)})^{p-1} = 1 \pmod{p} \) by Fermat.
\( \Rightarrow \ (x^{(q-1)})^{p-1} - 1 \) divisible by \( p \).
Similarly for \( q \).

RSA, Public Key, and Signatures.

**RSA:**
\[
N = p \cdot q
\]
e with \( \gcd(e, (p - 1)(q - 1)) = 1 \).
\[
d = e^{-1} \pmod{(p - 1)(q - 1)}.
\]
**Public Key Cryptography:**
\[
D(E(m, K), K) = (m^d)^{-1} \pmod{N}.
\]
**Signature scheme:**
\[
S(C) = D(C).
\]
Announce \( (C, S(C)) \)
**Verify:** Check \( C = E(C) \).
\[
E(D(C, K), K) = (C^d)^{-1} \pmod{N}.
\]
Applications.

Property 2: There is exactly 1 polynomial of degree \( \leq d \) with arithmetic modulo prime \( p \) that contains any \( d+1 \) points: \((x_i, y_i), \ldots, (x_{d+1}, y_{d+1})\) 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: \( (0, P(0)), \ldots, (n-1, P(n-1)) \).
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 \( i = 1, \ldots, n+2kP(i) \).give \( E(i) = R(i)E(i) \) (mod \( p \)) since \( E(i) = 0 \) at points where there are errors.
Let \( Q(x) = P(x)E(x) \).
\[ Q(x) = a_{b_1-k}x^{b_1-k-1} + \cdots + a_0. \]
\[ E(x) = x^k + b_{k-1}x^{k-1} + \cdots + b_0. \]
Gives system of \( n+2k \) linear equations.
\[ a_{b_1-k} + \cdots + a_0 = R(1)(1 + b_{k-1} \cdots b_0) \pmod{p} \]
\[ a_{b_{i+1}-1}(2)^{i+k-1} + \cdots + a_0 = R(2)(2^k + b_{k-1}(2^{k-1}) \cdots b_0) \pmod{p} \]
\[ \vdots \]
\[ a_{b_{i+1}-1}(n)^{i+k-1} + \cdots + a_0 = R(n)((n^k + b_{k-1}(n^{k-1}) \cdots b_0) \pmod{p} \]
and \( n+2k \) unknown coefficients of \( Q(x) \) and \( E(x) \).
Solve for coefficients of \( Q(x) \) and \( E(x) \).
Find \( P(x) = Q(x)/E(x) \).

Example: visualize.

First rule: \( n_1 \times n_2 \times \cdots \times n_k \). Product Rule.
Second rule: when order doesn’t matter divide when possible.

3 card poker deals: \( 52 \times 51 \times 50 = \frac{52!}{3!} \). First rule.
Poker hands: \( \Delta \).
Hand: \( Q, K, A \).
Deals: \( Q, K, A, Q, K, A, Q, K, A, Q, K, A \).  \( \Delta = 3 \times 2 \times 1 \) First rule again.
Total: \( \frac{52!}{3!} \). Second rule!

Choose \( k \) out of \( n \).
Ordered set: \( \frac{n!}{k!(n-k)!} \). Second rule.

What is \( \Delta \)?
First rule again.
Total: \( \frac{52!}{3!} \). Second rule.

Summary.

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

Counting

- First Rule
- Second Rule
- Stars/Bars

Common Scenarios: Sampling, Balls in Bins.

- Sum Rule. Inclusion/Exclusion.
- Combinatorial Proofs.

- First Rule
- Second Rule
- Stars/Bars

Common Scenarios: Sampling, Balls in Bins.

- Sum Rule. Inclusion/Exclusion.
- Combinatorial Proofs.
Combinatorial Proofs.

Theorem: \( \binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1} \).

Proof: How many size \( k \) subsets of \( n+1 \)?

How many size \( k \) subsets of \( n \)?

Chose first element, need to choose \( k-1 \) more from remaining \( n \) elements.

\[ \begin{align*}
\binom{n}{k} &= \binom{n-1}{k} + \binom{n-1}{k-1} \\
&= \binom{n}{k} + \binom{n}{k-1} \\
\end{align*} \]

How many don't contain the first element?

Need to choose \( k \) elements from remaining \( n-1 \) elts.

\[ \binom{n-1}{k} \]

So, \( \binom{n}{k} = \binom{n}{k} + \binom{n}{k-1} \).

Cardinalities of uncountable sets?

Cardinality of \([0,1]\) smaller than all the reals?

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

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

One to one. \( x \neq y \)

If both in \([0,1/2]\), a shift \( f(x) \neq f(y) \).

If neither in \([0,1/2]\) different mult inverses \( f(x) \neq f(y) \).

If one is in \([0,1/2]\) and one isn’t, different ranges \( f(x) \neq f(y) \).

Bijection!

\([0,1]\) is same cardinality as nonnegative reals!

Countability

Isomorphism principle.

Example.

Cardinality of \([0,1]\) smaller than all the reals?

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.

Enumerable means countable.

Subset of countable set is countable.

All countably infinite sets are the same cardinality as each other.
Examples: Countable by enumeration

- \( N \times N \) - Pairs of integers.
- Square of countably infinite?
  - Enumerate: (0,0), (0,1), (0,2), ... ???
  - Never get to (1,1)!
  - Enumerate: (0,0), (1,0), (0,1), (2,0), ..., (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.

Halt and Turing.

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

1. If \( HALT(P,I) \) = "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 \( HALT \).

Can run Turing on Turing!

Does \( Turing(Turing) \) halt?

- \( Turing(Turing) \) halts
  - \( \Rightarrow \) then \( HALT(Turing, Turing) \) = halts
  - \( \Rightarrow \) \( Turing(Turing) \) loops forever.

- \( Turing(Turing) \) loops forever.
  - \( \Rightarrow \) then \( HALT(S(Turing, Turing)) \neq \) halts
  - \( \Rightarrow \) \( Turing(Turing) \) halts.

Either way is contradiction. Program \( HALT \) does not exist!

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 \( \forall i \in \mathbb{N}, \) then \( HALT(Turing, Turing) \neq \) halts

\( \Rightarrow \) \( Turing(Turing) \) halts.

Either way is contradiction. Program \( HALT \) does not exist!

Uncomputability.

- Halting problem is undecidible.
- Diagonalization.

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 \( x^2 + y^2 = 1 \) 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

- no program can take any set of integer equations and always output correct answer.
Midterm format

Time: approximately 120 minutes.
Some longer questions.
Priming: sequence of questions...
but don’t overdo this as test strategy!!!
Ideas, conceptual, more calculation.

Wrapup.

Watch Piazza for Logistics!

Other issues....
fa17@eecs70.org
Private message on piazza.