Lecture 21: Midterm 2 Review.
Professor Walrand:
Wrapping up his lectures for other course this week.
Will take over lectures next week.
Rao will continue co-teaching.
Office hours.
See you on Piazza.
By email.

Midterm Prep. Notes 7-12.
Modular Arithmetic.
RSA/Cryptography.
Polynomials.
Secret Sharing.
Erasure Resistant Encoding.
Error Correction.
Counting.
Countability.
Computability.

### Modular Arithmetic Inverses and GCD

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

$N = 77$.

$(p − 1)(q − 1) = 60$

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

$egcd(7, 60)$.

| $7(0)$ | $60(1)$ | $60$ |
| $7(1)$ | $60(0)$ | $7$ |
| $7(−8)$ | $60(1)$ | $4$ |
| $7(9)$ | $60(−1)$ | $3$ |
| $7(−17)$ | $60(2)$ | $1$ |

Confirm: $−119 + 120 = 1$

$d = e^{-1} = −17 = 43 = ( mod 60)$

$d = e^{-1}$ has inverse modulo $mod p$.

### RSA

**RSA:**

$N = p, q$

$e$ with $\gcd(e, (p − 1)(q − 1)) = 1$.

$d = e^{-1} (mod (p − 1)(q − 1))$.

Theorem: $x^{ed} = x (mod N)$

Proof:

$x^{ed} − x ≡ (x^{e(p−1)(q−1)−1} − 1)$

If $x$ is divisible by $p$, the product is.

Otherwise $(x^{e(p−1)(q−1)})p−1 − 1$ divisible by $p$.

Similarly for $q$.

### RSA, Public Key, and Signatures.

**RSA:**

$N = p, q$

$e$ with $\gcd(e, (p − 1)(q − 1))$.

$d = e^{-1} (mod (p − 1)(q − 1))$.

Public Key Cryptography:

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

Signature scheme:

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

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

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

$E(D(C, K)) = (C^d)^d = C (mod N)$
Polynomials

Property 1: Any degree d polynomial over a field has at most d roots.
Proof Idea: Any polynomial with roots \( r_1, \ldots, r_d \), written as \((x - r_1) \cdots (x - r_d)Q(x)\), 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 \( d + 1 \) roots: \((x, y_1), \ldots, (x, y_{d+1})\) with \( x \) distinct.
Proof Ideas: Lagrange Interpolation gives existence. Properly 1 gives uniqueness.

Applications.

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

Example: visualize.

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

\[ \cdots \Delta \cdots \]

3 card Poker deals: \( 52 \times 51 \times 50 = \frac{52!}{3!} \). First rule.
Poker hands: \( \Delta ? \).
Hand: \( Q \ K \ A \).
Deals: \( Q \ K \ A, Q \ A \ K, Q \ K \ A, Q \ K \ A, Q \ A \ K, Q \ K \ A, Q \ K \ A \).
\( \Delta = 3 \times 2 \times 1 \) First rule again.
Total: \( \frac{52!}{3!} \). Second Rule!
Choose \( k \) out of \( n \).
Ordered set: \( \frac{n!}{k!(n-k)!} \).
What is \( \Delta \) ? \( k! \) First rule again.
\( \Rightarrow \frac{n!}{k!(n-k)!} \) Second rule.

Welsh-Berlekamp

Idea: Error locator polynomial of degree \( k \) with zeros at errors.
For all points: \( i = 1, \ldots, n + 2k \), \( P(i)E(i) = R(i)E(i) \mod p \)
since \( E(i) = 0 \) at points where there are errors.

Let \( Q(x) = P(x)E(x) \).
\( Q(x) = \Delta_{n-k-1}x^{n-k-1} + \cdots + \Delta_0 \).
\( E(x) = x^k + b_{k-1}x^{k-1} + \cdots + b_0 \).

Gives system of \( n + 2k \) linear equations.
\( \Delta_{n-k-1} + \cdots + \Delta_0 = R(1)(1 + b_{k-1} \cdots + b_0) \mod p \)
\( \Delta_{n-k-2} + \cdots + \Delta_0 = R(2)((2)^k + b_{k-1}(2)^{k-1} + \cdots + b_0) \mod p \)
\( \vdots \)
\( \Delta_{0-k-1} + \cdots + \Delta_0 = R(m)((m)^k + b_{k-1}(m)^{k-1} + \cdots + b_0) \mod p \)
\( \cdots \) 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: \( n_1 \times n_2 \cdots \times n_d \). Product Rule.
Second rule: when order doesn’t matter divide...when possible.

\[ \cdots \Delta \cdots \]

Orderings of ANAGRAM?
Ordered Set: 7! First rule.
A’s are the same!
What is \( \Delta ? \)
ANAGRAM:
\( A_1 A_2 A_3 A_4 A_5 A_6 A_7 \).
\( \Delta = 3 \times 2 \times 1 = 6 ! \) First rule!
\( \Rightarrow \frac{7!}{3!} \) Second rule!
**Summary.**

- **Combinatorial Proofs.**
  - **Theorem:** \( \binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1} \).
  - **Proof:** How many size \( k \) subsets of \( n+1 \) elements?
    - 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.
          \( \Rightarrow \binom{n}{k-1} \)
        - How many don't contain the first element?
          - Need to choose \( k \) elements from remaining \( n \) elts.
            \( \Rightarrow \binom{n}{k} \)
    - So, \( \binom{n}{k} + \binom{n}{k} = \binom{n+1}{k} \).

- **Balls in bins.**
  - "\( k \) Balls in \( n \) bins" = "\( k \) samples from \( n \) possibilities."
  - "indistinguishable balls" = "order doesn't matter"
  - "only one ball in each bin" = "without replacement"
  - 5 balls into 10 bins
    - 5 samples from 10 possibilities with replacement
      - **Example:** 5 digit numbers.
    - 5 indistinguishable balls into 52 bins only one ball in each bin
      - **Example:** Poker hands.
    - 5 indistinguishable balls into 3 bins
      - 5 samples from 3 possibilities with replacement and no order
        - Dividing 5 dollars among Alice, Bob and Eve.

- **Countability**
  - **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 \( y \in R, \exists x \in D, y = f(x) \).
    - \( f() \) is a bijection if it is one to one and onto.
  - **Isomorphism principle:**
    - If there is a bijection \( f : D \to R \) then \( |D| = |R| \).

- **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 both digits, \( |S \cap T| = 10^8 \).
    - Answer: \( |S| + |T| - |S \cap T| = 10^9 + 10^9 - 10^8 \).

**Diagonalization.**
Cardinalities of uncountable sets?

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

- $f: R^+ \rightarrow [0,1]$.  
  \[ f(x) = \begin{cases} 
  x + \frac{1}{x} & 0 \leq x \leq 1/2 \\
  2 - x & x > 1/2 
  \end{cases} \]

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 mul 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.

For example:

- $N \times N$ - Pairs of integers.
  - Square of countably infinite?
  - Enumerate: $(0,0),(0,1),(0,2),...$ ???
  - Never get to $(1,1)!$
  - Enumerate: $(0,0),(0,1),(0,2),(1,0),(1,1),(0,2)$ ...
  - $(a,b)$ 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?
  - Enumerated: $0$, first positive, first negative, second positive...
  - Will eventually get to any rational.

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. Enumerates means countable.

Subset of countable set is countable.

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

Examples: Countable by enumeration

- Countably infinite (same cardinality as naturals)
  - $\mathbb{Z}^+$ - 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: $f(e) = e/2$.
  - $\mathbb{Z}$ - all integers.
    - Twice as big?
      - Bijection: $f(z) = 2z; -\text{sign}(z)$.
      - Enumerate: $0, -1, 1, -2, 2...$

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 $i$th set in $L$ does not contain $i$, $i \in D$.
      - Otherwise $i \notin D$.
    - $D$ is different from $i$th set in $L$ for every $i$.
      - \( D \) 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 power set of $N$.)
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: Y es! No! Y es! No! Y es! No! ...

Halt and Turing.

Proof: Assume there is a program HALT(·, ·).
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
⇒ then HALTS(Turing, Turing) = halts
⇒ Turing(Turing) loops forever.
Turing(Turing) loops forever
⇒ then HALTS(Turing, Turing) ≠ halts
⇒ Turing(Turing) halts.
Either way is contradiction. Program HALT does not exist!

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.

P1 P2 P3 · · ·
P1 H H L · · ·
P2 L L H · · ·
P3 L H H · · ·
⋯ ⋮ ⋮ ⋮ ⋮

Halt - diagonal.
Turing - is not Halt.
and is different from every Pi on the diagonal.
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
⇒ no program can take any set of integer equations and always output correct answer.

Midterm format

Time: approximately 105 minutes versus 90 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.
Printing: sequence of questions...
but don’t overdo this as test strategy!!!
Proofs, algorithms, properties.
Some calculation.

Wrapup.

Watch Piazza for Logistics!
Watch Piazza for Advice!
If you sent me email about Midterm conflicts
Other arrangements.
Should have received an email today from me.
Other issues...
satishr@cs.berkeley.edu
Private message on piazza.

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