

Lecture 28: Discrete Math Review

Or Is It Discreet Math?

Announcements

No homework parties this week! Our reservations got cancelled :(

Discussion sections will be OH / topic reviews
See weekly post for full details

HW Review is **4-6** in **320 Soda** this week

Please fill out the course evaluation survey! There's a point of extra credit in it for you :)

Rough Outline

Today: review of first half of class

- ▶ Propositional Logic
- ▶ Proofs
- ▶ Graphs
- ▶ Modular Arithmetic
- ▶ Cryptography
- ▶ Polynomials
- ▶ Error Correcting Codes
- ▶ Countability
- ▶ Computability

Propositional Logic

Propositions are basic building blocks of logic
Allow simplification of complex statements

Propositional Logic

Propositions are basic building blocks of logic
Allow simplification of complex statements

Examples?

- ▶ ~~“Pizza is a legitimate breakfast food.”~~
- ▶ “Every integer is either even or odd.” ✓
- ▶ ~~“ $x + 3 = 7$.”~~

Propositional Logic

Propositions are basic building blocks of logic
Allow simplification of complex statements

Examples?

- ▶ “Pizza is a legitimate breakfast food.” X
- ▶ “Every integer is either even or odd.” ✓
- ▶ “ $x + 3 = 7$.” X

Make formulae w/operators: $\wedge, \vee, \neg, \implies$, etc

$$(P \vee Q) \implies P$$

$$((\neg P) \iff Q) \wedge R$$

Truth Tables

Formulae are really just functions!

Input: T/F values to propositions

Output: value of formula

Truth Tables

Formulae are really just functions!

Input: T/F values to propositions

Output: value of formula

P	Q	$(\neg P) \vee (\neg Q)$	$\neg((\neg P) \vee (\neg Q))$	$P \wedge Q$
F	F	T	F	F
F	T	T	F	F
T	F	T	F	F
T	T	F	T	T

Proofs

Many ways to argue correctness of a statement

Proofs

Many ways to argue correctness of a statement

Direct proof ($P \implies Q$):

- ▶ Start from P , logically deduce Q

Proofs

Many ways to argue correctness of a statement

Direct proof ($P \implies Q$):

- ▶ Start from P , logically deduce Q

Proof by contraposition ($P \implies Q$):

- ▶ Directly prove $(\neg Q) \implies (\neg P)$

Proofs

Many ways to argue correctness of a statement

Direct proof ($P \implies Q$):

- ▶ Start from P , logically deduce Q

$$P \implies Q$$

Proof by contraposition ($P \implies Q$):

- ▶ Directly prove $(\neg Q) \implies (\neg P)$

$$\neg P \vee Q$$

Proof by contradiction (P):

- ▶ Start with $\neg P$, reach contradiction

$$P \wedge \neg Q$$

Proofs

Many ways to argue correctness of a statement

Direct proof ($P \implies Q$):

- ▶ Start from P , logically deduce Q

Proof by contraposition ($P \implies Q$):

- ▶ Directly prove $(\neg Q) \implies (\neg P)$

Proof by contradiction (P):

- ▶ Start with $\neg P$, reach contradiction

Proof by induction ($\forall n \in \mathbb{N} P(n)$):

- ▶ Prove $P(0)$ and $P(k) \implies P(k+1)$

Proof Poll

Do an example proof live! Poll for which one:

1. If $m|a$ and $n|b$, then $mn|ab$. (Direct)
2. Let $x \in \mathbb{Z}$. If $x^2 + 6x + 5$ is even, x is odd. (Contraposition)
3. Let r be rational and x be irrational. Then $r + x$ is irrational. (Contradiction)
4. Let $x \in \mathbb{R}$ and $n \in \mathbb{N}$. Then $(1 + x)^n \geq 1 + nx$. (Induction)

Direct Example

If $m|a$ and $n|b$, then $mn|ab$.

Direct Example

If $m|a$ and $n|b$, then $mn|ab$.

Proof:

- ▶ Since $m|a$, $a = km$ for $k \in \mathbb{Z}$
- ▶ Since $n|b$, $b = jn$ for $j \in \mathbb{Z}$
- ▶ Hence $ab = km \cdot jn = kj(mn)$

Contraposition Example

Let $x \in \mathbb{Z}$. If $x^2 + 6x + 5$ is even, x is odd.

Contraposition Example

Let $x \in \mathbb{Z}$. If $x^2 + 6x + 5$ is even, x is odd.

Proof:

- ▶ Contrapos: If x is even, $x^2 + 6x + 5$ is odd.
- ▶ Suppose $x = 2k$ for some $k \in \mathbb{Z}$
- ▶ $x^2 + 6x + 5 = 4k^2 + 12k + 5 = 2(2k^2 + 6k + 2) + 1$
- ▶ $2k^2 + 6k + 2 \in \mathbb{Z}$, so $x^2 + 6x + 5$ odd

Contradiction Example

Let $r \in \mathbb{Q}$ and x be irrational. Then $r+x$ irrational.

Assume $r+x \in \mathbb{Q}$

$$r+x = \frac{a}{b} \quad r = \frac{c}{d}$$

$$x = (r+x) - r = \frac{a}{b} - \frac{c}{d}$$

$$= \frac{ad - cb}{bd}$$

$$x \in \mathbb{Q}$$



Contradiction Example

Let $r \in \mathbb{Q}$ and x be irrational. Then $r + x$ irrational.

Proof:

- ▶ Suppose $r + x = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$
- ▶ r rational, so $r = \frac{c}{d}$ for some $c, d \in \mathbb{Z}$
- ▶ Hence $x = (r + x) - r = \frac{a}{b} - \frac{c}{d} = \frac{ad - cb}{bd}$
- ▶ So x rational, contradiction!

Induction Example

Let $x \in \mathbb{R}$ and $n \in \mathbb{N}$. Then $(1 + x)^n \geq 1 + nx$.

Induction Example

Let $x \in \mathbb{R}$ and $n \in \mathbb{N}$. Then $(1 + x)^n \geq 1 + nx$.

Proof:

- ▶ Base Case: $n = 0$, statement is $1 \geq 1$.
- ▶ Suppose $(1 + x)^k \geq 1 + kx$
- ▶ Then we have

$$\begin{aligned}(1 + x)^{k+1} &= (1 + x)^k(1 + x) \\ &\geq (1 + kx)(1 + x) \\ &= 1 + x + kx + kx^2 \\ &= 1 + (k + 1)x + kx^2 \\ &\geq 1 + (k + 1)x\end{aligned}$$

Graph Definitions

Graph is vertices + edges

Use drawings to help visualize

Graph Definitions

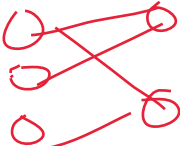
Graph is vertices + edges
Use drawings to help visualize

Special kinds of graphs:

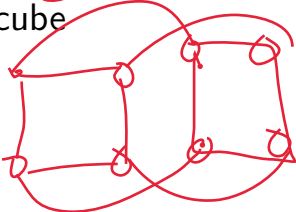
Complete



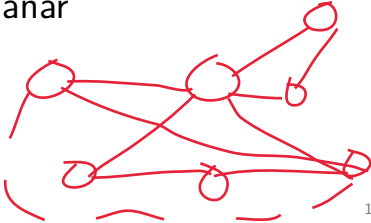
Bipartite



Hypercube



Planar



Induction on Graphs

Can induct on number of vertices, edges, etc

Be careful of build-up error!

“Shrink down, grow back” can help avoid this

Induction on Graphs

Can induct on number of vertices, edges, etc

Be careful of build-up error!

“Shrink down, grow back” can help avoid this

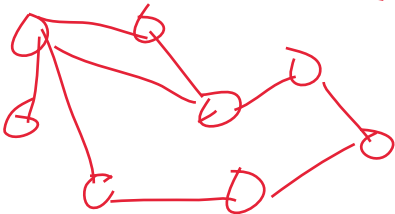
Example: proving Euler's formula $v + f = e + 2$

$B C f = 1$ $e = v - 1$ f

$e + 2 = v + 1$ \swarrow

$v' + f' = e' + 2$

$v + f = \cancel{v} = e + \cancel{1} + 2$



Euler and Coloring

Euler says planar graphs are sparse: $e \leq 6v - 12$

Means always have degree < 6 vertex!

Use to inductively prove 6-color theorem

Euler and Coloring

Euler says planar graphs are sparse: $e \leq 6v - 12$

Means always have degree < 6 vertex!

Use to inductively prove 6-color theorem

With more work, also gives 5-color theorem

Modular Arithmetic

Alternative to arithmetic on the real numbers

Define $+$ and \cdot on $\{0, 1, 2, \dots, m - 1\}$

Modular Arithmetic

Alternative to arithmetic on the real numbers

Define $+$ and \cdot on $\{0, 1, 2, \dots, m - 1\}$

Still has “properties we want” from \mathbb{R}

Allows for exact addition, multiplication, division, exponentiation, etc on computers!

$$ax \equiv 1 \pmod{m}$$

Extended GCD Algorithm

Goal: find (d, a, b) st $\gcd(x, y) = d = ax + by$
Allows us to find inverses if $\gcd(x, y) = 1$!

Recursive call on $y, x \bmod y$ to get (d', a', b')
Return $(d', b', a' - \lfloor \frac{x}{y} \rfloor b')$

$$d = 1 = ax + by \rightarrow 1 \equiv ax \pmod{y}$$
$$x' = y, \quad y' = x \bmod y = x - \lfloor \frac{x}{y} \rfloor y$$
$$d' = a'x' + b'y' = a'y + b'(x - \lfloor \frac{x}{y} \rfloor y)$$

Chinese Remainder Theorem

Given coprime n_1, n_2, \dots, n_k , \exists unique soln modulo $N = \prod_i n_i$ to system of equations $x \equiv a_i \pmod{n_i}$

Chinese Remainder Theorem

Given coprime n_1, n_2, \dots, n_k , \exists unique soln modulo $N = \prod_i n_i$ to system of equations $x \equiv a_i \pmod{n_i}$

Key is finding "basis" elements b_i st

- ▶ $b_i \equiv 1 \pmod{n_i}$
- ▶ $b_i \equiv 0 \pmod{n_j}$ for $j \neq i$

$$x = \sum_i a_i \cdot b_i$$

$$b_i = \prod_{j \neq i} n_j \cdot \prod_{j \neq i} (n_j^{-1} \pmod{n_i})$$

Private Key Cryptography



Private Key Cryptography



One-Time Pad: xor message w/random, shared pad
Perfect security – but only for one message!

Public Key Cryptography

RSA: way to avoid logistical issues of OTP

Private key: $(N = pq, d)$

Public key: $(N, e = d^{-1} \pmod{(p-1)(q-1)})$

Public Key Cryptography

RSA: way to avoid logistical issues of OTP

Private key: $(N = pq, d)$

Public key: $(N, e = d^{-1} \pmod{(p-1)(q-1)})$

Encryption: $E(m) = m^e \pmod{N}$

Decryption: $D(c) = c^d \pmod{N}$

Public Key Cryptography

RSA: way to avoid logistical issues of OTP

Private key: $(N = pq, d)$

Public key: $(N, e = d^{-1} \pmod{(p-1)(q-1)})$

Encryption: $E(m) = m^e \pmod{N}$

Decryption: $D(c) = c^d \pmod{N}$

Correctness: FLT + CRT

Security: $\neg \exists \text{ poly}$

$$m^{ed} \pmod{N} \rightarrow m^{k \frac{(p-1)(q-1)}{e}} \cdot m$$

Polynomial Representations

Two equiv representations of degree d polynomials:

- ▶ Coefficients ($c_d x^d + \dots + c_1 x + c_0$)
- ▶ Values ($(x_1, y_1), \dots, (x_{d+1}, y_{d+1})$)

Polynomial Representations

Two equiv representations of degree d polynomials:

- ▶ Coefficients ($c_d x^d + \dots + c_1 x + c_0$)
- ▶ Values ($(x_1, y_1), \dots, (x_{d+1}, y_{d+1})$)

Convert coefficients to values: evaluate polynomial

Polynomial Representations

Two equiv representations of degree d polynomials:

- ▶ Coefficients ($c_d x^d + \dots + c_1 x + c_0$)
- ▶ Values ($(x_1, y_1), \dots, (x_{d+1}, y_{d+1})$)

Convert coefficients to values: evaluate polynomial

Other direction: Lagrange interpolation

Interpolation Interpretation

Given points $(x_1, y_1), \dots, (x_{d+1}, y_{d+1})$, want degree d poly through them

Interpolation Interpretation

Given points $(x_1, y_1), \dots, (x_{d+1}, y_{d+1})$, want degree d poly through them

Key is finding “basis” polys $\Delta_i(x)$ st

- ▶ $\Delta_i(x_i) = 1$
- ▶ $\Delta_i(x_j) = 0$ for $j \neq i$

Note similarity to proof of CRT!

$$P(x) = \sum_i y_i \Delta_i(x)$$

$$\Delta_i(x) = \prod_{j \neq i} (x - x_j) / (x_i - x_j)$$

Error Correcting Codes

Application of polys: fix transmission errors

Reed-Solomon: interpolate poly through message

$$P(1) = m_1, P(2) = m_2, \dots, P(n) = m_n$$

Error Correcting Codes

Application of polys: fix transmission errors

Reed-Solomon: interpolate poly through message

$$P(1) = m_1, P(2) = m_2, \dots, P(n) = m_n$$

Recover P means recover message!

k erasures needs $n + k$ packets

k corruptions needs $n + 2k$ packets



Countability

Main idea: “same size” means “has bijection”

Use \mathbb{N} as point of comparison

eg $|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| = |\{0, 1\}^*|$

Countability

Main idea: “same size” means “has bijection”

Use \mathbb{N} as point of comparison

eg $|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| = |\{0, 1\}^*|$

To prove a set countable:

- ▶ Provide bijection with known countable set
- ▶ Provide injection (1-1) to countable set
- ▶ Provide surjection (onto) from countable set

Last two from Cantor-Schröder-Bernstein Thm

Uncountability

Not all sets are the same size as \mathbb{N} !

Uncountability

Not all sets are the same size as \mathbb{N} !

Canonical Example: $\{0, 1\}^\infty$

n	$o(n)$
0	0 0 0 0 0 ...
1	1 0 1 0 1 ...
2	1 1 1 0 1 ...
3	0 1 0 0 0 ...
\vdots	\vdots

1101...

Uncountability

Not all sets are the same size as \mathbb{N} !

Canonical Example: $\{0, 1\}^\infty$

n	$o(n)$	
0	0 0 0 0 0 ...	$s = 1101\dots$
1	1 0 1 0 1 ...	$s \neq o(n)$ for any $n!$
2	1 1 1 0 1 ...	
3	0 1 0 0 0 ...	
\vdots	\vdots	

Show set uncountable w/diagonalization or show “same size”/“bigger than” known uncountable set

Uncomputability

Computers can't do everything!

Case study: Halting Problem is impossible

You will halt!

Fine, loop!



TestHalt

I'll loop instead!

Actually, I'll halt!



Turing

Reductions

Many other problems also uncomputable!

Often easiest to prove with reduction from TestHalt



Fin

Next time: probability review (with Elizabeth)!

