70: Discrete Math and Probability Theory

Programming + Microprocessors $\equiv$ Superpower!

What are your super powerful programs/processors doing?
  Logic and Proofs!
  Induction $\equiv$ Recursion.

What can computers do?
  Work with discrete objects.
  Discrete Math $\implies$ immense application.

Computers learn and interact with the world?
  E.g. machine learning, data analysis, robotics, ...
  Probability!

See note 1, for more discussion.

Satish Rao

18th year at Berkeley.
PhD: Long time ago, far far away.
Research: Theory (Algorithms)
Taught: 170, 174, 70, 270, 273, 294, 375, ...

Other: 1 College kid. One Cal Grad. And another College Grad.

Admin

Course Webpage: **http://www.eecs70.org/**

Explains policies, has office hours, homework, midterm dates, etc.

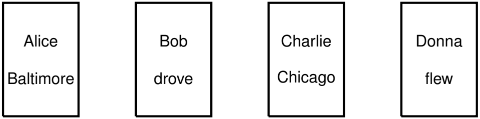
Two midterms, final.
midterm 1 before drop date.
midterm 2 late! After pass/no-pass deadline!

Questions/Announcements $\Longrightarrow$ piazza:
piazza.com/berkeley/spring2017/cs70

Wason's experiment:1

Suppose we have four cards on a table:

- 1st about Alice, 2nd about Bob, 3rd Charlie, 4th Donna.
- Card contains person's destination on one side, and mode of travel.
- Consider the theory:
  "If a person travels to Chicago, he/she flies."
- Suppose you see that Alice went to Baltimore, Bob drove, Charlie went to Chicago, and Donna flew.



- Which cards must you flip to test the theory?

Answer: Later.

CS70: Lecture 1. Outline.

Today: Note 1. Note 0 is background. Do read it.

The language of proofs!

1. Propositions.
2. Propositional Forms.
3. Implication.
4. Truth Tables
5. Quantifiers
6. More De Morgan's Laws

Propositions: Statements that are true or false.

$\sqrt{2}$ is irrational	**Proposition**	True
2+2 = 4	**Proposition**	True
2+2 = 3	**Proposition**	False
826th digit of pi is 4	**Proposition**	False
Johny Depp is a good actor	**Not a Proposition**	
All evens > 2 are sums of 2 primes	**Proposition**	False
$4 + 5$	**Not a Proposition.**	
$x + x$	**Not a Proposition.**	
Alice travelled to Chicago	**Proposition.**	False

Again: “value” of a proposition is ... True or False

Propositional Forms.

Put propositions together to make another...

Conjunction ("and"): $P \wedge Q$

"$P \wedge Q$" is True when both P and Q are True . Else False .

Disjunction ("or"): $P \vee Q$

"$P \vee Q$" is True when at least one P or Q is True . Else False .

Negation ("not"): $\neg P$

"$\neg P$" is True when P is False . Else False .

Examples:

$\neg$ "$(2+2=4)$" – a proposition that is ... False

"$2+2=3$" $\bigwedge$ "$2+2=4$" – a proposition that is ... False

"$2+2=3$" $\bigvee$ "$2+2=4$" – a proposition that is ... True

Propositional Forms: quick check!

$P =$ "$\sqrt{2}$ is rational"
$Q =$ "826th digit of pi is 2"

P is ...False .
Q is ...True .

$P \wedge Q$ ... False

$P \vee Q$ ... True

$\neg P$ ... True

Put them together..

Propositions:
P_1 - Person 1 rides the bus.
P_2 - Person 2 rides the bus.
....

But we can't have either of the following happen; That either person 1 or person 2 ride the bus and person 3 or 4 ride the bus. Or that person 2 or person 3 ride the bus and that either person 4 rides the bus or person 5 doesn't.

Propositional Form:
$\neg(((P_1 \vee P_2) \wedge (P_3 \vee P_4)) \vee ((P_2 \vee P_3) \wedge (P_4 \vee \neg P_5)))$

Can person 3 ride the bus?
Can person 3 and person 4 ride the bus together?

This seems ...complicated.

We can program!!!!

We need a way to keep track!

Truth Tables for Propositional Forms.

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

Notice: $\wedge$ and $\vee$ are commutative.

One use for truth tables: Logical Equivalence of propositional forms!

Example: $\neg(P \wedge Q)$ logically equivalent to $\neg P \vee \neg Q$

...because the two propositional forms have the same...

....Truth Table!

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

DeMorgan's Law's for Negation: distribute and flip!

$\neg(P \wedge Q) \quad \equiv \quad \neg P \vee \neg Q \qquad\qquad \neg(P \vee Q) \quad \equiv \quad \neg P \wedge \neg Q$

Distributive?

$P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$?

Simplify: $(T \wedge Q) \equiv Q$, $(F \wedge Q) \equiv F$.

Cases:

P is True .

LHS: $T \wedge (Q \vee R) \equiv (Q \vee R)$.

RHS: $(T \wedge Q) \vee (T \wedge R) \equiv (Q \vee R)$.

P is False .

LHS: $F \wedge (Q \vee R) \equiv F$.

RHS: $(F \wedge Q) \vee (F \wedge R) \equiv (F \vee F) \equiv F$.

$P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$?

Simplify: $T \vee Q \equiv T$, $F \vee Q \equiv Q$.

Foil 1:

$(A \vee B) \wedge (C \vee D) \equiv (A \wedge C) \vee (A \wedge D) \vee (B \wedge C) \vee (B \wedge D)$?

Foil 2:

$(A \wedge B) \vee (C \wedge D) \equiv (A \vee C) \wedge (A \vee D) \wedge (B \vee C) \wedge (B \vee D)$?

Implication.

$P \implies Q$ interpreted as

If P, then Q.

True Statements: P, $P \implies Q$.
Conclude: Q is true.

Examples:

Statement: If you stand in the rain, then you'll get wet.
P = "you stand in the rain"
Q = "you will get wet"
Statement: "Stand in the rain"
Can conclude: "you'll get wet."

Statement: If a right triangle has sidelengths $a \le b \le c$, then $a^2 + b^2 = c^2$.

P = "a right triangle has sidelengths $a \le b \le c$",
Q = "$a^2 + b^2 = c^2$".

Non-Consequences/consequences of Implication

The statement "$P \implies Q$"

only is False if P is True and Q is False .

False implies nothing
P False means Q can be True or False
Anything implies true.
P can be True or False when Q is True

If chemical plant pollutes river, fish die.
If fish die, did chemical plant pollute river?

Not necessarily.

$P \implies Q$ and Q are True does not mean P is True

Be careful!

Instead we have:
$P \implies Q$ and P are True *does* mean Q is True .

The chemical plant pollutes river. Can we conclude fish die?

Some Fun: use propositional formulas to describe implication?
$((P \implies Q) \wedge P) \implies Q$.

Implication and English.

$P \implies Q$

- If P, then Q.
- Q if P.
  Just reversing the order.
- P only if Q.
  Remember if P is true then Q must be true.
  this suggests that P can only be true if Q is true.
  since if Q is false P must have been false.
- P is sufficient for Q.
  This means that proving P allows you
  to conclude that Q is true.
- Q is necessary for P.
  For P to be true it is necessary that Q is true.
  Or if Q is false then we know that P is false.

Truth Table: implication.

P	Q	$P \implies Q$
T	T	T
T	F	F
F	T	T
F	F	T

P	Q	$\neg P \vee Q$
T	T	T
T	F	F
F	T	T
F	F	T

$\neg P \vee Q \quad \equiv P \implies Q.$

These two propositional forms are logically equivalent!

Contrapositive, Converse

- Contrapositive of $P \implies Q$ is $\neg Q \implies \neg P$.
  - If the plant pollutes, fish die.
  - If the fish don't die, the plant does not pollute. (contrapositive)

  - If you stand in the rain, you get wet.
  - If you did not stand in the rain, you did not get wet. (not contrapositive!) converse!
  - If you did not get wet, you did not stand in the rain. (contrapositive.)

  Logically equivalent! Notation: $\equiv$.
  $P \implies Q \equiv \neg P \vee Q \equiv \neg(\neg Q) \vee \neg P \equiv \neg Q \implies \neg P$.
- Converse of $P \implies Q$ is $Q \implies P$.

  If fish die the plant pollutes.

  Not logically equivalent!
- **Definition:** If $P \implies Q$ and $Q \implies P$ is P if and only if Q or $P \iff Q$.
  (Logically Equivalent: $\iff$.)

Variables.

Propositions?

- $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.
- $x > 2$
- n is even and the sum of two primes

No. They have a free variable.

We call them predicates, e.g., $Q(x) =$ "x is even"
Same as boolean valued functions from 61A or 61AS!

- $P(n) =$ "$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$."
- $R(x) =$ "$x > 2$"
- $G(n) =$ "n is even and the sum of two primes"
- Remember Wason's experiment!
  $F(x) =$ "Person x flew."
  $C(x) =$ "Person x went to Chicago
- $C(x) \implies F(x)$. Theory from Wason's.
  If person x goes to Chicago then person x flew.

Next: Statements about boolean valued functions!!

Quantifiers..

There exists quantifier:

$(\exists x \in S)(P(x))$ means "There exists an x in S where $P(x)$ is true."

For example:

$$(\exists x \in \mathbb{N})(x = x^2)$$

Equivalent to "$(0 = 0) \vee (1 = 1) \vee (2 = 4) \vee \ldots$"

Much shorter to use a quantifier!

For all quantifier;
$(\forall x \in S)\ (P(x))$. means "For all x in S, we have $P(x)$ is True ."

Examples:

"Adding 1 makes a bigger number."

$$(\forall x \in \mathbb{N})\ (x + 1 > x)$$

"the square of a number is always non-negative"

$$(\forall x \in \mathbb{N})(x^2 >= 0)$$

Wait! What is $\mathbb{N}$?

Quantifiers: universes.

Proposition: "For all natural numbers n, $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$."

Proposition has **universe**: "the natural numbers".

Universe examples include..

- $\mathbb{N} = \{0, 1, \ldots\}$ (natural numbers).
- $\mathbb{Z} = \{\ldots, -1, 0, \ldots\}$ (integers)
- $\mathbb{Z}^+$ (positive integers)
- $\mathbb{R}$ (real numbers)
- Any set: $S = \{Alice, Bob, Charlie, Donna\}$.
- See note 0 for more!

Back to: Wason's experiment:1

Theory: "If a person travels to Chicago, he/she flies."

Suppose you see that Alice went to Baltimore, Bob drove, Charlie went to Chicago, and Donna flew.

Which cards do you need to flip to test the theory?

$P(x)$ = "Person x went to Chicago." $Q(x)$ = "Person x flew"

Statement/theory: $\forall x \in \{A, B, C, D\}, P(x) \implies Q(x)$

$P(A)$ = False . Do we care about $Q(A)$?
No. $P(A) \implies Q(A)$, when $P(A)$ is False , $Q(A)$ can be anything.

$Q(B)$ = False . Do we care about $P(B)$?
Yes. $P(B) \implies Q(B) \equiv \neg Q(B) \implies \neg P(B)$.
So $P(Bob)$ must be False .

$P(C)$ = True . Do we care about $Q(C)$?
Yes. $P(C) \implies Q(C)$ means $Q(C)$ must be true.

$Q(D)$ = True . Do we care about $P(D)$?
No. $P(D) \implies Q(D)$ holds whatever $P(D)$ is when $Q(D)$ is true.

Only have to turn over cards for Bob and Charlie.

More for all quantifiers examples.

- "doubling a number always makes it larger"

$$(\forall x \in N)\ (2x > x) \quad \textbf{False} \quad \textbf{Consider } x = 0$$

Can fix statement...

$$(\forall x \in N)\ (2x \geq x) \quad \textbf{True}$$

- "Square of any natural number greater than 5 is greater than 25."

$$(\forall x \in N)(x > 5 \implies x^2 > 25).$$

Idea alert: Restrict domain using implication.

Note that we may omit universe if clear from context.

Quantifiers..not commutative.

- In English: “there is a natural number that is the square of every natural number”.

$$(\exists y \in N)\ (\forall x \in N)\ (y = x^2) \quad \text{False}$$

- In English: “the square of every natural number is a natural number.”

$$(\forall x \in N)(\exists y \in N)\ (y = x^2) \quad \text{True}$$

Quantifiers....negation...DeMorgan again.

Consider

$$\neg(\forall x \in S)(P(x)),$$

English: there is an x in S where $P(x)$ does not hold.

That is,

$$\neg(\forall x \in S)(P(x)) \iff \exists(x \in S)(\neg P(x)).$$

What we do in this course! We consider claims.

Claim: $(\forall x)\ P(x)$ "For all inputs x the program works."
For False , find x, where $\neg P(x)$.
Counterexample.
Bad input.
Case that illustrates bug.
For True : prove claim. Next lectures...

Negation of exists.

Consider

$$\neg(\exists x \in S)(P(x))$$

English: means that for all x in S , $P(x)$ does not hold.

That is,

$$\neg(\exists x \in S)(P(x)) \iff \forall(x \in S)\neg P(x).$$

Which Theorem?

Theorem: $(\forall n \in N)\, \neg(\exists a, b, c \in N)\, (n \geq 3 \implies a^n + b^n = c^n)$

Which Theorem?

Fermat's Last Theorem!

Remember Special Triangles: for $n = 2$, we have 3,4,5 and 5,7, 12 and ...

1637: Proof doesn't fit in the margins.

1993: Wiles ...(based in part on Ribet's Theorem)

DeMorgan Restatement:
Theorem: $\neg(\exists n \in N)\, (\exists a, b, c \in N)\, (n \geq 3 \implies a^n + b^n = c^n)$

Summary.

Propositions are statements that are true or false.

Proprositional forms use $\wedge, \vee, \neg$.

Propositional forms correspond to truth tables.

Logical equivalence of forms means same truth tables.

Implication: $P \implies Q \iff \neg P \vee Q$.

Contrapositive: $\neg Q \implies \neg P$
Converse: $Q \implies P$

Predicates: Statements with “free” variables.

Quantifiers: $\forall x\ P(x)$, $\exists y\ Q(y)$

Now can state theorems! And disprove false ones!

DeMorgans Laws: “Flip and Distribute negation”

$$\neg(P \vee Q) \iff (\neg P \wedge \neg Q)$$
$$\neg \forall x\ P(x) \iff \exists x\ \neg P(x).$$

Next Time: proofs!