

70: Discrete Math and Probability Theory

Programming + Data Structures/Algorithms + Microprocessors
≡ Superpower! (almost)

What are our super powerful programs/processors doing?

Logic and Proofs!

Induction ≡ Recursion.

What can computers do?

Work with discrete objects.

Discrete Math \implies immense application.

Computers learn and interact with the world?

E.g. AI/machine learning, cyber-physical systems/robotics,
networking/wireless communications, ...

Probability!

Instructors

Instructor: Sanjit Seshia.

Professor of EECS (office: 566 Cory)

19th year on the faculty at Berkeley!

Ph.D.: in Computer Science, from Carnegie Mellon University.

Research: Formal Methods (a.k.a. Computational Proof Methods)

applied to cyber-physical systems/robotics (e.g. “is this self-driving car safe”), computer security (e.g., “can this program leak my private data?”), ...

Taught: CS 70, EECS 149/249A, CS 172, EECS 144/244, EECS 219C, EECS149.1x on edX, ...

Instructors

- Alistair Sinclair
- Professor of CS (office 677 Soda)

- @ Berkeley since pre-history (1994)
- Originally from the UK: undergrad @ Cambridge, PhD @ Edinburgh

- Research: CS Theory, esp. algorithms, randomness, statistical physics, stochastic processes...
- Teaching: CS70, CS170, CS172, CS174 + various grad classes

Admin

Course Webpage: <http://eecs70.org/>

Explains policies, has office hours, schedule, homework, exam dates, etc.

One midterm, final.

midterm on March 6

final on May 10

Questions/Announcements \implies Ed Discussion

Grading – see course webpage

homework/no-homework option continues

Learning and Teaching

Variety of Background Knowledge on the Topics of CS70
“mini-vitamins” before lecture can help

Variety of Learning Styles
take “notes” during lecture?

Variety of Teaching Styles
slides vs. no slides

Learn by Doing (Mathematical Modeling/Problem Solving)

CS70: Lecture 1. Outline.

Today: Note 1. (Note 0 is background. Do read/skim it.)

The language of proofs! Mathematical Logic!

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

$$2+2 = 4$$

$$2+2 = 3$$

826th digit of pi is 4

Stephen Curry is a good basketball player

All evens > 2 are unique sums of 2 primes

$$4 + 5$$

$$x + x$$

Proposition True

Proposition True

Proposition False

Proposition False

Not a Proposition

Proposition False

Not a Proposition.

Not a Proposition.

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

“ $2 + 2 = 3$ ” \wedge “ $2 + 2 = 4$ ” – a proposition that is ... False

“ $2 + 2 = 3$ ” \vee “ $2 + 2 = 4$ ” – a proposition that is ... True

Propositional Forms: quick check!

$P = \text{“}\sqrt{2} \text{ is rational”}$

$Q = \text{“}826\text{th digit of pi is } 2\text{”}$

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.

....

Suppose 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 ride the bus or person 5 doesn't.

Propositional Form:

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

Who can ride the bus?

What combinations of people can ride the bus?

This seems ...**complicated**.

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

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

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

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

Implication.

$P \implies Q$ interpreted as

If P , then Q .

True Statements: $P, P \implies Q$.

Conclude: Q is true.

Example: 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."

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 polluted river?

Not necessarily.

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

Instead we have:

$P \implies Q$ and P are **True** does mean Q is **True** .

Be careful out there!

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 .
- ▶ P only if Q .
- ▶ P is sufficient for Q .
- ▶ Q is necessary for P .

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

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

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., $Q(x) = \text{“}x \text{ is even”}$

Same as boolean valued functions from 61A!

- ▶ $P(n) = \text{“}\sum_{i=1}^n i = \frac{n(n+1)}{2}\text{.”}$
- ▶ $R(x) = \text{“}x > 2\text{”}$
- ▶ $G(n) = \text{“}n \text{ is even and the sum of two primes”}$

Next: Statements about boolean valued functions!!

Quantifiers..

There exists quantifier:

$(\exists x \in S)(P(x))$ means "P(x) is true for some x in S"

Wait! What is S?

S is the **universe**: "the type of x".

Universe examples include..

- ▶ $N = \{0, 1, 2, \dots\}$ (natural numbers).
- ▶ $Z = \{\dots, -1, 0, 1, \dots\}$ (integers)
- ▶ Z^+ (positive integers)
- ▶ See note 0 for more!

Quantifiers..

There exists quantifier:

$(\exists x \in S)(P(x))$ means "P(x) is true for some x in S"

For example:

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

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

Much shorter to use a quantifier!

For all quantifier;

$(\forall x \in S)(P(x))$. means "For all x in S 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"

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

Quantifiers are not commutative.

- ▶ Consider this English statement: "there is a natural number that is the square of every natural number", i.e the square of every natural number is the same number!

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

- ▶ Consider this one: "the square of every natural number is a natural number"...

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

Quantifiers...negation...DeMorgan again.

Consider

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

By DeMorgan's law,

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

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

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

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

Equivalent to:

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

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

Which Theorem?

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

Which Theorem?

Fermat's Last Theorem!

Remember Right-Angled Triangles: for $n = 2$, we have (3, 4, 5) and (5, 12, 13), and ... (Pythagorean triples)

1637: Fermat: Proof doesn't fit in the margins.

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

DeMorgan Restatement:

Theorem: $\neg(\exists n \in \mathbb{N} \exists a, b, c \in \mathbb{N} (n \geq 3 \wedge a^n + b^n = c^n))$

Summary.

Propositions are statements that are true or false.

Propositional forms use \wedge, \vee, \neg .

The meaning of a propositional form is given by its truth table.

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!