CS70: Discrete Mathematics and Probability Theory

UC Berkeley – Summer 2025 – Steve Tate

Lecture 1

What Is This Class?

Discrete Math: Math with structures with distinct objects

- Not continuous
- Not "discreet"!
- But not (necessarily) finite
- Digital? What computers work with...

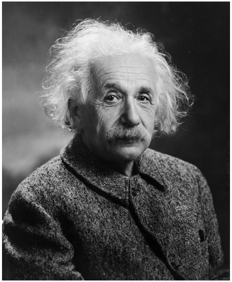
Probability Theory: Probability and properties of random events

- *Can* use continuous functions
- Basically counting....

But really this class is about: building important ideas by putting together simple concepts; careful and precise reasoning about those constructions; proofs; counting

What does Albert Einstein say about CS70?

OK, maybe not specifically CS70....



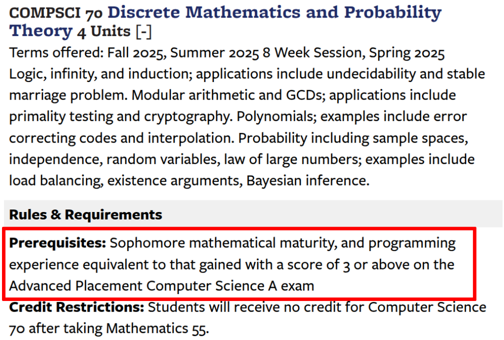
"One reason why mathematics enjoys special esteem, above all other sciences, is that its laws are absolutely certain and indisputable, while those of all other sciences are to some extent debatable and in constant danger of being overthrown by newly discovered facts."

– *Albert Einstein, 1922.*

Mathematics gives clarity and certainty (that's rare!)
$\Rightarrow$ Proofs are the "gold standard" of reasoning
$\Rightarrow$ Clarity: Order out of chaos

What does Berkeley say about this course?

What Is This Class?



COMPSCI 70 Discrete Mathematics and Probability Theory 4 Units [-]

Terms offered: Fall 2025, Summer 2025 8 Week Session, Spring 2025

Logic, infinity, and induction; applications include undecidability and stable marriage problem. Modular arithmetic and GCDs; applications include primality testing and cryptography. Polynomials; examples include error correcting codes and interpolation. Probability including sample spaces, independence, random variables, law of large numbers; examples include load balancing, existence arguments, Bayesian inference.

Rules & Requirements

Prerequisites: Sophomore mathematical maturity, and programming experience equivalent to that gained with a score of 3 or above on the Advanced Placement Computer Science A exam

Credit Restrictions: Students will receive no credit for Computer Science 70 after taking Mathematics 55.

Topics above are important and highly relevant to computer science.

⇒ *But reasoning skills are even more important...*

Background:

- "Sophomore mathematical maturity"

  ... *mostly basic (see "Note 0") – but there will be some Calculus*
- Programming background? Familiarity provides context...

Who Am I?

Instructor: Steve Tate
"Retired" Professor
Office: 676 Soda
Office Hours: Mon/Wed 2:30 – 3:30

I used to be young and nerdy
Now I'm only one of those things

Steve's Path in B.S.: Vanderbilt University
  Electrical Engineering → Computer Science → Mathematics
  In the end: Why choose?

Defining moment: Non-trivial correctness proof in data structures

Steve's Path in Ph.D.: Duke University
  Compilers → Theoretical Computer Science (*and a lot of grad Math*)

Steve's Professional Path:
  Research, Center Creation, Department Founding, ...
  And always: Love of teaching – I want you to succeed!

Who Else Should You Know?

The CS70 staff!

Outstanding quality – variety of backgrounds – your most valuable resource!

CS70: Some Administrative Details

Course Webpage: https://eecs70.org/

Read and understand policies!!! Questions about policies on HW0

Course content: CS70 is CS70 – summer or not, any instructor, ...

- ⇒ Content based on lecture notes – no book
- ⇒ Challenging in regular semester – *intense* in summer

Some administrative details:

- ⇒ Homework: Weekly, due Sat @4:00pm – 73% for full credit, 2 dropped
- ⇒ Discussions after each lecture (sign-up opens at 2:30!) – attend $\geq$ 50%
- ⇒ Mini-vitamins (due 2 hours after each lecture – highest 13 counted)
- ⇒ Office hours – optional but *very* helpful
- ⇒ Ed for class announcements, discussion, and questions (**Weekly Post**)

Exams: One midterm, final. No rescheduling or alternative times!

- ⇒ Midterm on Tuesday, July 15 (7:00pm – 9:00pm)
- ⇒ Final on Tuesday, August 12 (7:00pm – 10:00pm)
- ⇒ Recovery: Partial clobber

How to Succeed in This Class

Is this a challenging class? Yes!

It’s a skills-based class – not a lot of “new facts”

Consider becoming a jazz improvisation musician. Can you imagine saying?

- “I read all about it”
- “Twice!”
- “I watched YouTube videos”
- “I repeated the same thing you did over and over”

This needs a different way of thinking for many of you – embrace it!

How to Succeed in This Class

What *do* you need to do?

- Read about it. Multiple times. (Read + Mini-Vitamin + Lecture + Discussion + HW)
- Keep up – no time to recover if you fall behind in summer
- Practice - but don't blindly repeat
  - Always question: Why? Why? Why?
  - Always go back to the definitions – be precise!
  - Question all conditions (they're stated for a reason)
  - Be exploratory and playful – adjust things and see what happens

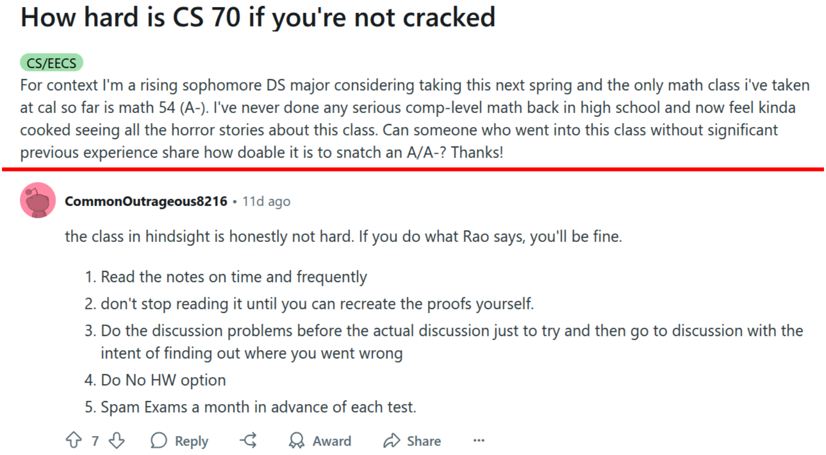
    ⇒ Jiggle the pieces until they fit – order from chaos!
  - Expect to make mistakes – appreciate what you learn from them!
  - Expect to be uncomfortable – "feel the burn!"

I believe...

- You *can* do this!
- You will be a far better computer scientist if you develop these skills

Reddit Wisdom

A post and comment from earlier this month (from June 10):



How hard is CS 70 if you're not cracked

CS/EECS

For context I'm a rising sophomore DS major considering taking this next spring and the only math class i've taken at cal so far is math 54 (A-). I've never done any serious comp-level math back in high school and now feel kinda cooked seeing all the horror stories about this class. Can someone who went into this class without significant previous experience share how doable it is to snatch an A/A-? Thanks!

CommonOutrageous8216 • 11d ago

the class in hindsight is honestly not hard. If you do what Rao says, you'll be fine.

1. Read the notes on time and frequently
2. don't stop reading it until you can recreate the proofs yourself.
3. Do the discussion problems before the actual discussion just to try and then go to discussion with the intent of finding out where you went wrong
4. Do No HW option
5. Spam Exams a month in advance of each test.

#4 doesn't apply this term (and `s/Rao/Tate/`), but otherwise good advice!

CS70: Note 1 / Lecture 1

Logic

Logic is the language of proofs and reasoning

Topics for today:

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

Propositions: Statements that are true or false

One of the two main "P"s of logic

A **proposition** is a self-contained statement that is either true or false.

Statement	*Proposition?*	*True?*
$\sqrt{2}$ is irrational	**Proposition**	True
2+2 = 4	**Proposition**	True
2+2 = 3	**Proposition**	False
826th digit of π is 4	**Proposition**	False
LeBron James is a good basketball player	**Not a Proposition**	
Every even $n > 2$ is the sum of 2 primes	**Proposition**	Maybe?
$4+5$	**Not a Proposition**	
$x+3=7$	**Not a Proposition**	

This statement is false

The last one is the "Liar's Paradox"

Similar to Russell's Paradox – gratuitous plug: see Jeffrey Kaplan's video!

Propositional Forms

Combine propositions to make new propositions

Conjunction (“and”): $P \wedge Q$

“$P \wedge Q$” is True when both P and Q are True ; otherwise False

Disjunction (“or”): $P \vee Q$

“$P \vee Q$” is True when at least one P or Q is True ; otherwise False

Note: In logic, “or” is inclusive – not exclusive “this or that” that English sometimes implies

Negation (“not”): $\neg P$

“$\neg P$” is True when P is False ; otherwise 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"

$Q =$ "$\sqrt{31} < 6$"

P is False

Q is True

$P \wedge Q$ is False

$P \vee Q$ is True

$\neg P$ is True

Propositional forms: Combinations of combinations...

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?

Is it even possible to meet all conditions?

⇒ This is the "Satisfiability" problem – a *very* important problem in computer science!

We need a way to keep track of truth values!

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: Test logical equivalence of propositional forms!

Example: Are $\neg(P \wedge Q)$ and $\neg P \vee \neg Q$ logically equivalent?

...enumerate all truth values...

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

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

De Morgan's Law's for Negation: distribute and flip the operator!

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

Reasoning By Cases

Question: Is $P \wedge (Q \vee R)$ equivalent to $(P \wedge Q) \vee (P \wedge R)$?

Could write out truth tables – how many rows?

Or think through cases:

Case 1: P is True

LHS: $P \wedge (Q \vee R)$ becomes $\mathit{True} \wedge (Q \vee R) \equiv Q \vee R$

RHS: $(\mathit{True} \wedge Q) \vee (\mathit{True} \wedge R) \equiv Q \vee R$ ✓

Case 2: P is False

LHS: $P \wedge (Q \vee R)$ becomes $\mathit{False} \wedge (Q \vee R) \equiv \mathit{False}$

RHS: $(\mathit{False} \wedge Q) \vee (\mathit{False} \wedge R) \equiv \mathit{False} \vee \mathit{False} \equiv \mathit{False}$ ✓

Cases let us remove one variable and have easy-to-perform reasoning

Implication

English: “If P then Q”

Logically written: $P \implies Q$

Caution: Proposition if/then is *not* a programming if/then

It’s a statement about the relation between P and Q — it’s not causal!

Better (Perhaps) English: “Whenever P is True , Q must be True ”

Example: If you stand in the rain, then you’ll get wet.

P = “you stand in the rain”
Q = “you will get wet”

Hypothesis (or antecedent): “you stand in the rain”
Conclusion (or consequent): “you’ll get wet”

Truth (Validity) of Implication

"$P \implies Q$" is itself a proposition – not just talking *about* propositions!

Warning: This confuses some students, who want to treat implication as an *action* and not a *statement* that can be true of false (i.e., a proposition).

As a first step, use the English term "OK" or "invalid"
What makes $P \implies Q$ invalid (or wrong)?
Only when P is True and Q is False !

I claim $P \implies Q$ and there is a case where

- P is True and Q is False — *invalid!* (proposition is False)
- P is True and Q is True — *OK* (proposition is True)
- P is False and Q is ... anything? — *OK* (proposition is True)

As a proposition, $P \implies Q$ is True when it's "OK"; False when "invalid"

Truth (Validity) of Implication

I claim $P \implies Q$ and there is a case where

- P is True and Q is False — *invalid!* (proposition is False)
- P is True and Q is True — *OK* (proposition is True)
- P is False and Q is ... anything? — *OK* (proposition is True)

$P \implies Q$ is a proposition, so let's make a truth table:

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

Truth (Validity) of Implication

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

Understanding "special cases":

- P is False – "$P \implies Q$" is always true ("vacuously true")
  "If pigs fly then horses can read"
  Is it *invalid*? No!
  Is it *useful*? No!
- Q is True – "$P \implies Q$" is always true ("trivially true")
  "If p is prime, then $2p$ is even"
  Is it *invalid*? No!
  Is it *useful*? No! (Remember: *not causal!*)

Implication and English

English has a lot of ways to express the same logical implication:

- If P, then Q

  If I stand in the rain, then I get wet

- Q if P

  I get wet if I stand in the rain

- P only if Q

  I stand in the rain only if I get wet (confusing? use “could be standing” in the first part)

- P is sufficient for Q

  standing in the rain is sufficient for getting wet

- Q is necessary for P

  getting wet is necessary for standing in the rain

- Sometimes English simply *implies* the logic:

  Standing in the rain, I get wet

Roles of P and Q are not interchangeable! (Try some!)

Implications: Equivalent Proposition...

Recall truth table:

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

Note: 1 "F" and 3 "T"
Just like "OR"...
Except on wrong line

Consider $\neg P$ with "OR":

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

They're the same now! So:

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

Contrapositive

If $\underbrace{\text{chemical plant pollutes river}}_{P}$, then $\underbrace{\text{fish die}}_{Q}$

Logic: $P \implies Q$

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

Says: *If fish didn't die, then the chemical plant didn't pollute the river*
Is it (necessarily) true?

Yes! Logically:

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

and

$$\neg Q \implies \neg P \quad \equiv \quad \neg(\neg Q) \vee \neg P \quad \equiv \quad Q \vee \neg P \quad \equiv \quad \neg P \vee Q$$

The contrapositive is equivalent to the original implication!

Converse

If $\underbrace{\text{chemical plant pollutes river}}_{P}$, then $\underbrace{\text{fish die}}_{Q}$

Logic: $P \implies Q$

Converse: $Q \implies P$

Says: *If fish die, then the chemical plant polluted the river*

Is it (necessarilynecessarily) true?

No! There are many reasons why fish might die...

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

The converse is not equivalent to the original implication!

It can be true though! Write "$P \iff Q$" or "P if and only if Q" or "P iff Q"

Predicates: Using Variables

The second of the two main "P"s of logic

Are these propositions?

- $x + 3 = 7$
- n is even and the sum of two primes
- $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

No. Propositions must be *self-contained* – these have free variables

We call them **predicates**, e.g., $Q(x) =$ "x is even"

Same as boolean valued functions from 61A!

- $P(x) =$ "$x + 3 = 7$"
- $G(n) =$ "n is even and the sum of two primes"
- $S(n) =$ "$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$"

Next: Statements about predicates!

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:

- $\mathbb{N} = \{0, 1, 2, \ldots\}$ (natural numbers)
- $\mathbb{Z} = \{\ldots, -1, 0, 1, \ldots\}$ (integers)
- $\mathbb{Z}^+$ (positive integers)
- $\mathbb{Q}$ (rational numbers)
- $\mathbb{R}$ (real numbers)

Quantifiers

Existential quantifier: ("there exists"):
$(\exists x \in S)(P(x))$ means "$P(x)$ is True for some x in S"

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!

Universal quantifier: ("for all"):
$(\forall x \in S)\ (P(x))$ means "For all x in S, $P(x)$ is True "

Examples:

- $(\forall x \in \mathbb{N})\ (x + 1 > x)$
  "Adding 1 to a natural number makes a bigger number"
- $(\forall x \in \mathbb{Z})\ (x^2 \geq 0)$
  "The square of an integer is always non-negative"

Quantifier Order

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!)

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

Consider this one: “The square of every natural number is a natural number”

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

Order of *alternating* quantifier (can!) make a big difference

Order of adjacent *same* quantifiers does *not* make a difference!

For example: $\exists x \exists y\, P(x,y) \ \equiv \ \exists y \exists x\, P(x,y)$

Sometimes written with a single quantier symbol: $\exists x, y\, P(x,y)$

A Helpful Visualization

Picture two-argument $P(x,y)$ as a table of T/F values

$\exists x \forall y \; P(x,y)$

$y \rightarrow$

x $\downarrow$

T	F	F	F	T	$\cdots$
F	F	T	F	T	$\cdots$
T	T	F	F	T	$\cdots$
T	T	T	T	T	$\cdots$
F	T	F	T	F	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	

One row with all T

$\forall y \exists x \; P(x,y)$

$y \rightarrow$

x $\downarrow$

T	F	F	F	T	$\cdots$
F	F	T	F	T	$\cdots$
T	T	F	F	T	$\cdots$
T	F	F	T	T	$\cdots$
F	T	F	T	F	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	

All columns have a T

Negating a Universally-Quantified Statement

Consider

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

Read: “It is not the case that for all x in S, $P(x)$ is True ”

De Morgan’s law for quantifiers (same idea: move negation in and flip op):

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

Read the second as: “There is an x in S where $P(x)$ is not True ”

Useful to *dis*-prove a claim:

Claim: $(\forall x)\ P(x)$ “For all inputs x the program works.”
Not true? Need to show $\neg(\forall x)\ P(x)$

Answer this question: *where* is it not true?
A *counterexample*
Bad input
Case that illustrates bug

Negating an Existentially-Quantified Statement

Consider

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

Read: “There does not exist an x in S such that $P(x)$ holds”

De Morgan’s law for quantifiers (same idea: move negation in and flip op):

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

Read: “For all x in S, $P(x)$ does not hold”

Example: (note how negation “inside” is handled)

$$\neg(\exists x \in \mathbb{N})(x < 0) \quad \iff \quad (\forall x \in \mathbb{N})(x \geq 0)$$

Read these out — see how they are equivalent?

Which Theorem is This?

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

Which Theorem?

Fermat's Last Theorem (FLT)!

Remember right triangles (Pythagorean triples) – when $n = 2$:

Triple $(3, 4, 5)$ since $3^2 + 4^2 = 5^2$
Triple $(5, 12, 13)$ since $5^2 + 12^2 = 13^2$

FLT says not possible for higher powers

Long and storied history:

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

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

De Morgan Restatement:

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

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

Contrapositive: $\neg Q \implies \neg P$ (equivalent to $P \implies Q$)

Converse: $Q \implies P$ (not equivalent)

Predicates: Statements with variables

Quantifiers: Universal $\forall x\ P(x)$ and existential $\exists y\ Q(y)$

Now can state theorems (provable propositions)! And disprove false ones!

De Morgan's 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!