CS70 – Spring 2026

Lecture 1: Jan. 20

CS70 Main Staff

- Prof. Alistair Sinclair (OH Mo11-12 & Th 2:30-3:30 in 677 Soda)

  First half (discrete math)

- Prof. Yun Song (OH Mo1-2 & Th 5:30-6:30 in 629 Soda)

  Second half (counting/probability)

- Head TAs:

  Erica Liu

  Sam Poder

  Gavin Zhang

CS70 Brief Overview

- Logic & proofs
- Graphs
- Modular arithmetic & applications to cryptography, secret sharing, error-correcting codes
- Self-reference, undecidability & uncomputability
- Counting and probability
- Probabilistic algorithms: load-balancing, hashing, estimation, inference…

Killer apps: Examples

- Can we design a “stable” algorithm for matching applicants to college slots?
- Can we share a secret code among a group of generals so that any set of four of them can recover the code but any smaller set has no information about it?
- If 6000 requests are allocated randomly among 1000 servers, what’s the (likely) maximum load on any server?
- We receive a corrupted message along a noisy channel. What is our best guess at the original message? Can we protect against such errors via coding and/or redundancy?
- Can we state a mathematical problem that even the most powerful computers can never solve?

CS70 Policies

- Course web page: www.eecs70.org/
  All course materials are on this page.
  Visit it daily and **read these policies today!**

- Ed: One-stop shop for all Q&A and announcements:
  read policies online for **etiquette**! Visit it daily.

- Email: sp26@eecs70.org (instructors & Head TAs)
  Use only for **private** administrative matters!

- Materials: No book. Lecture notes on web page.
  Read lecture notes **before & after** each lecture!

- Enrollment: Limit is **510** students. Room size is **481**.
  If you don't have a seat, please watch the **webcast!**
  [We may stop recording if #students ≤ 481.]
  Waitlist is processed by staff: Please **DO NOT** email us!

CS70 Policies (cont.)

- Assessment:
  Discussion: 5% [13x for full credit]
  Mini-Vitamins: 5% [due before lecture; top 13 only]
  Homework: 15%
  Midterm: 30% [Thu. 3/12, 7-9pm]
  Final: 45% [Thu. 5/14, 3-6pm]

- Final exam conflicts **cannot** be accommodated!
  Midterm conflicts (e.g., with other exams): you must notify us at least 2 weeks in advance

- Homeworks: weekly (due Saturdays 4pm)
  Lowest three HW scores dropped but…
  …**no late homeworks or excuses accepted!**
  All homeworks equally weighted; max credit will be given for 73/100 (no extra credit)
  No "No-HW" option

CS70 Policies (cont.)

- Resources
  - Lectures + Lecture Notes
  - Homeworks
  - Discussions [2 per week; go to any section; popular times fill up so choose another time; **not** mini lectures]
  - Office hours [go to any; prepare in advance!]

- Collaboration vs Cheating
  We strongly encourage collaboration but…
  … **all your work must be composed only by you!**
  Zero tolerance for cheating!

- Discussions start **Thu/Fri Jan 22/23**
  Office hours/HW parties start **Mon Jan 27**

CS70 FAQs

- This is a Math class but I'm a CS student; why do I have to take it?

  (1) You may be designing AI (e.g.) for critical medical decisions

  (2) Somebody has to check if ChatGPT is giving good answers!

- Is it just about proofs?

  No! Unlike many DiscMath/Prob classes, CS70 is based around "killer apps"

- I didn't do competition Math; will I be able to keep up?

  This is not competition Math; no special background is assumed

- Do I need to spend way more than 10 hours a week on CS70?

  No! If so, please talk to us about making your study habits more effective

- I've been to lecture and read the notes once; how come I still don't get it?

  Math needs to be closely read several times before you get it

CS70 Survival Tips

- Don’t fall behind: can’t cram this class in the last week
- Read the lecture notes before class (high-level skim) and after class (in depth, more than once!)
- Take the homeworks seriously and start early
- Make use of office hours
- Participate actively in discussion sections
- Form study groups (2-3 people)
- ChatGPT can be your friend—or your worst enemy!

Topic 1 : Logic & Proofs

Goals :

1. Learn mathematical language & notation
2. Learn to write convincing arguments (e.g., to justify why your programs work as intended)

Propositional Logic

Proposition: A **statement** that is either **true** or **false**

Examples:

- $\sqrt{3}$ is irrational
- $6 - 2 = 3$
- 1 billion is a big number
- Julius Caesar was 5' 8" tall
- $3x + 17 = 42$
- $42/23$
- Julius Caesar was short

Combining Propositions

$P \wedge Q$	"AND"	} "connectives"
$P \vee Q$	"OR"	
$\neg P$	"NOT"	

Examples:

P: "3 is even" Q: "2+2 = 4"

$P \wedge Q$:

$P \vee Q$:

$\neg P$:

Truth Tables

define connectives

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

Truth Tables define connectives

P	Q	$P \wedge Q$	$P \vee Q$	$P \Rightarrow Q$
T	T	T	T	
T	F	F	T	
F	T	F	T	
F	F	F	F	

Another connective: $P \Rightarrow Q$ "IMPLIES"

Example: "If you pass the exam, you'll get into College"

Q: How can this be false?

A:

Logical Equivalences

Fact: $P \Rightarrow Q$ is equivalent to $\neg P \vee Q$

We write $(P \Rightarrow Q) \equiv \neg P \vee Q$

Why? Check the truth tables!

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

Example: "If you pass the exam you'll get into College"

$\equiv$

"Either you fail the exam or you'll get into College"

The contrapositive of $P \Rightarrow Q$ is $\neg Q \Rightarrow \neg P$

The converse of $P \Rightarrow Q$ is $Q \Rightarrow P$

Exercise: Use truth tables to check that:

- $(P \Rightarrow Q) \equiv (\neg Q \Rightarrow \neg P)$

[If you don't get into College then you didn't pass the exam]

- $(P \Rightarrow Q) \not\equiv (Q \Rightarrow P)$

[If you get into College then you passed the exam]

One more connective: $P \Leftrightarrow Q$ "IF & ONLY IF"

This is defined by: $(P \Leftrightarrow Q) \equiv (P \Rightarrow Q) \wedge (Q \Rightarrow P)$

Predicates & Quantifiers : First Order Logic

Propositions : Aristotle is a philosopher
Plato is a philosopher

↓

Predicate : Phil (Aristotle)
Phil (Plato)
} where Phil(x) denotes "x is a philosopher"

Quantifiers : (over some universe $\mathcal{U}$)

$(\forall x \in \mathcal{U})\ P(x)$ – universal "for all"

$(\exists x \in \mathcal{U})\ P(x)$ – existential "exists"

Example :

P(x) : x is divisible by 2
Q(x) : x ------- 3
R(x) : x ------- 6

} Q: How do we write: "A nat. number x is div. by 6 iff only if it's div. by both 2 and 3" ?

More examples:

"209 has a divisor larger than 17"

"$f(x) = x^2 - 4x + 3$ has exactly two distinct real roots"

"There is no largest integer"

Negation: De Morgan's Laws

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

Ex: Check using truth tables!

With quantifiers:

$$\neg(\forall x\, P(x)) \equiv \exists x\, (\neg P(x))$$
$$\neg(\exists x\, P(x)) \equiv \forall x\, (\neg P(x))$$

Example

$$\neg(\exists x \forall y \exists z\ P(x,y,z)) \equiv \forall x \exists y \forall z\, (\neg P(x,y,z))$$

Fun Example

Bob is on trial for murder.

Bob's attorney never lies.

Judge: "If Bob committed this murder, he didn't act alone"

Attorney: "That's not true!"

Q: Did the attorney help Bob?

A:

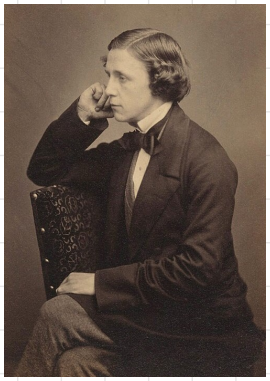
Fun Example 2

[R. Smulyan]

"A watched kettle never boils unless it is watched"

Q: true/false/undetermined ?

1. No one who is going to a party fails to brush his/her hair
2. No one looks fascinating if he/she is untidy
3. Opium-eaters have no self-command
4. Everyone who has brushed his/her hair looks fascinating
5. No one wears kid gloves unless he/she is going to a party
6. A person is untidy if she/he has no self-command



Lewis Carroll
Symbolic Logic
1897

Q : What can we say about someone who is wearing kid gloves?

Summary

- Propositions
- Connectives $\wedge$ $\vee$ $\neg$ $\Rightarrow$ $\Leftrightarrow$
- Truth tables ; logical equivalence $\equiv$
- Implications

  $P \Rightarrow Q \equiv \neg Q \Rightarrow \neg P$ (contrapositive)

  $\not\equiv Q \Rightarrow P$ (converse)
- Predicates & Quantifiers:

  $\forall x\ P(x)$ $\exists x\ P(x)$
- De Morgan's Laws:

  $\neg \forall x\ P(x) \equiv \exists x\ (\neg P(x))$ $\neg \exists x\ P(x) \equiv \forall x (\neg P(x))$