Complexity Class Review

Definition: P is the class of decision problems which can be solved in polynomial time, i.e. time $O(n^k)$ for some $k \in \mathbb{N}$.

Definition: EXP is the class of decision problems which can be solved in exponential time, i.e. time $O(2^{n^k})$ for some $k \in \mathbb{N}$.

Definition: NP is the class of decision problems for which every "yes" instance has a short justification which can be checked in polynomial time.

Definition: Co-NP is the class of decision problems for which every "no" instance has a short justification which can be checked in polynomial time.

All Problems in NP can be brute forced

Theorem: NP $\subseteq$ EXP

The Million Dollar Question: $P = NP$?

Millennium Problems

Yang–Mills and Mass Gap

Experiment and computer simulations suggest the existence of a "mass gap" in the solution to the quantum versions of the Yang-Mills equations. But no proof of this property is known.

Riemann Hypothesis

The prime number theorem determines the average distribution of the primes. The Riemann hypothesis tells us about the deviation from the average. Formulated in Riemann's 1859 paper, it asserts that all the 'non-obvious' zeros of the zeta function are complex numbers with real part 1/2.

P vs NP Problem

If it is easy to check that a solution to a problem is correct, is it also easy to solve the problem? This is the essence of the P vs NP question. Typical of the NP problems is that of the Hamiltonian Path Problem: given N cities to visit, how can one do this without visiting a city twice? If you give me a solution, I can easily check that it is correct. But I cannot so easily find a solution.

Navier–Stokes Equation

Most computer scientists believe $P \neq NP$, but it's very difficult to prove.

	P≠NP	P=NP
2002	61 (61%)	9 (9%)
2012	126 (83%)	12 (9%)
2019	109 (88%)	15 (12%)

NP Completeness

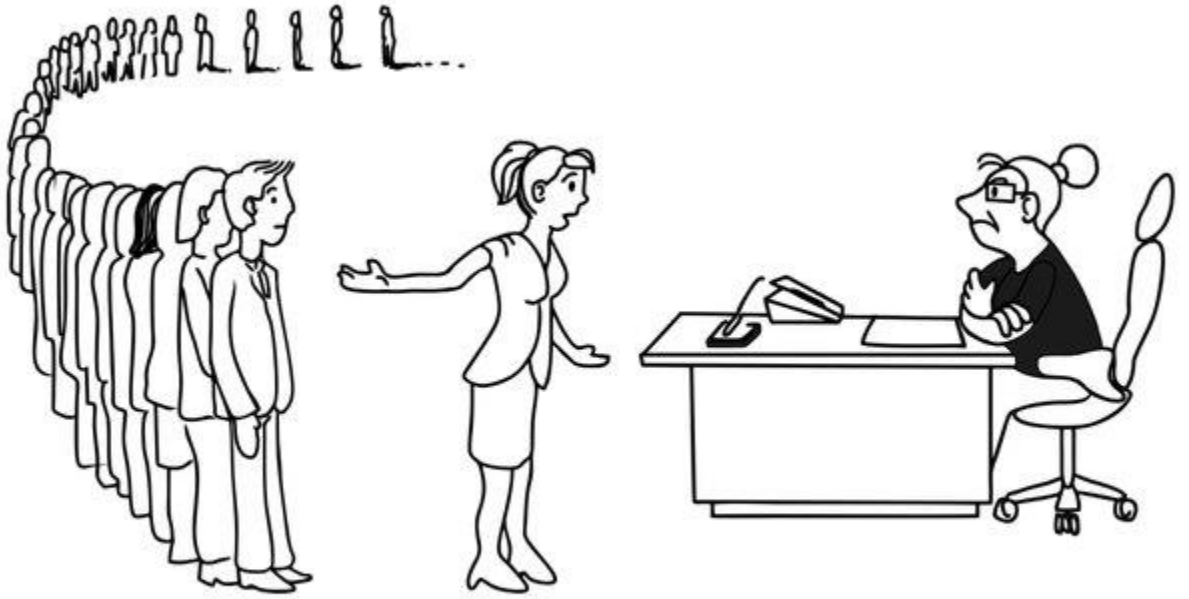
- We can't prove that a problem in NP requires exponential time.
- But we can still find evidence that certain problems in NP are hard

Definition: A problem Q is called *NP-complete* if

$$Q \in \mathrm{P} \Rightarrow \mathrm{NP} \subseteq \mathrm{P}$$

Theorem (Cook-Levin): CIRCUIT-SAT is NP-Complete

All of the NP problems we've discussed on the previous slides are NP-complete



"I can't find an efficient algorithm, but neither can all these famous people."

Reductions: How to show NP-completeness

Theorem: CLIQUE is NP-Complete ⇒ INDEPENDENT-SET is NP-Complete

Good enough to show INDEPENDENT-SET ∈ P ⇒ CLIQUE ∈ P

Learning Objectives

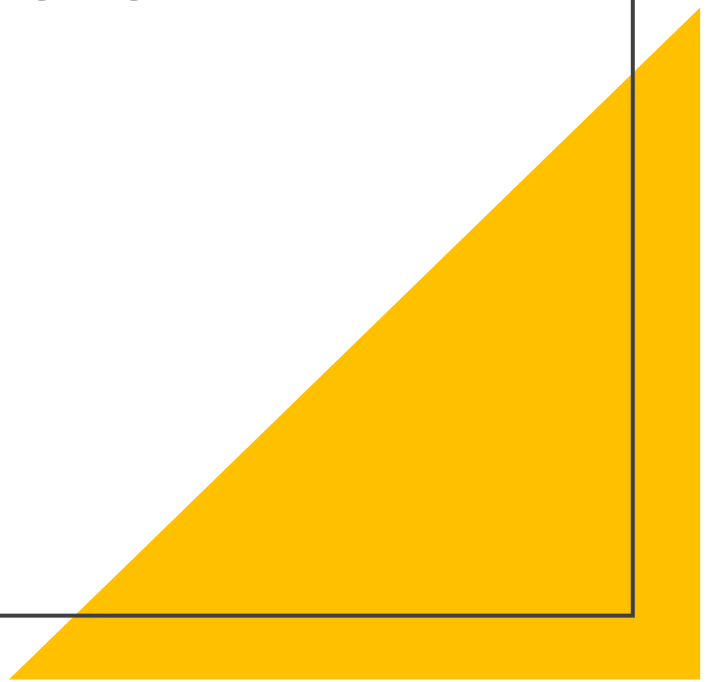
- Understand the definitions of P, NP, co-NP, and EXP
- Know some problems in each of these complexity classes
- Understand the concept of NP-completeness and why it matters

Contradiction

CS 173

Summer 2022

Calvin Beideman



Learning Objectives

- Understand how to construct a proof by contradiction

Proof by Contradiction

$$p \equiv F \vee p \equiv \neg T \vee p \equiv T \rightarrow p \equiv \neg p \rightarrow F$$

A proof by contradiction proves a proposition p by showing $\neg p \rightarrow F$, where F is a logical contradiction (anything we know to be false).

Proof Outline:

Suppose not. That is, suppose $\neg p$.
[Reach a contradiction]
Because assuming $\neg p$ led to a contradiction, it must be the case that p is true.

Example

There are infinitely many prime numbers.

Another Example

$\sqrt{3}$ is irrational

A graph example

Let $G = (V, E)$ be a graph with n vertices. Show that if every vertex in G has degree at least $n/2$, then G is connected.

Another irrationality proof

Show that $\frac{2\sqrt{3}+1}{3\sqrt{3}+2}$ is irrational

Learning Objectives

- Understand how to construct a proof by contradiction