Problem Session 4

Solving Instances Vs. Solving Problems

How to Market Your P=NP Solution

Telling What a Program Does

- Suppose I write a program to sort integers.
- Can't I feed it a list of integers and see whether they come out sorted?
  - Or a million lists and check them all?
- Yes, but maybe your program will fail to sort the 1,000,001th list you try.

Solving Instances Vs. Solving Problems

- Instances of a problem are not problems.
- Suppose TM M accepts language L, and w is a string.
  - One TM M_{yes} ignores its input and accepts.
  - Another TM M_{no} ignores its input and rejects.
- One answers the question “is w in L?”
- But I can’t tell which.

Polytime Algorithms for Part of an NP-complete problem

- Suppose I have a polytime algorithm that works correctly on all tested instances of an NP-complete problem.
- Could I sell that solution?
  - Could I keep it secret so only I could solve NP-complete problems in polytime?

Zero-Knowledge Proofs

- Developed by Shafi Goldwasser, Silvio Micali, and Charles Rackoff in 1985.
  - An early idea in cryptographic protocols.
- Let's you prove that you know something without revealing how you know it.
  - Hypothetical polytime algorithm for an NP-complete problem was key motivation.

Polytime Algorithm for Instances of a Problem

- It is possible to find polytime algorithms that solve instances of NP-complete problems.
  - Or even a million instances.
- But as for the analogous matter of decidability, it doesn't help us.

Testing Polytime Solutions

- What about a polytime "solution" to SAT that we test on 1,000,000 inputs and it gives the correct answer each time.
- How do you know it is correct?
- If a satisfying assignment exists, we could expect the tester to show us one.
  - Which we could then check.

Testing Polytime Solutions – (2)

- But what if the algorithm says “no”?
- We can’t even check that it is correct in less than exponential time.
- But if the expression has many satisfying assignments, we could try a few at random.
- Alas, expressions with one satisfying assignment exist.
  - Consider Cook’s construction applied to a DTM.

Thanks

- Thanks for being part of this course.
- Good luck on the final exam.