Zero Knowledge Proofs

Plan for today

- ~~One project presentation~~
- Feedback on the semester
- Course evaluations
- Interviewing for SE jobs tips and tricks
- Zero knowledge proofs

Semester in Review

I’d like to get some feedback from you guys about this course so I can improve it in the future.

Things we did this semester

- In class activities
  - groupthink (phone exercise)
  - pair programming (movie scripts)
- Outside speakers
  - naturalness of programming languages
  - databases to answer why and how questions
  - software architecture in practice
  - semantic code search
- Paper presentations
- Homework and projects

LET'S VOTE

Homework

A. Five too many
B. Five too few
C. Five is just right

Homework

A. The homework assignments clear

B. The homework assignments were ambiguous

C. What homework assignments?

Thoughts on the project?

- 521 students didn’t *have* to do projects

A. good idea?

B. bad idea?

Paper presentations

A. Paper reading and presenting was interesting

B. Paper reading and presenting was boring

   we would rather watch Yuriy lecture, he's so funny!

C. Maybe fewer presentations would be better

D. Maybe more, shorter presentations would be better

Outside speakers

A. The speakers were a great way to get exposure to current SE research

B. Having speakers is good, but don’t make them part of the class and don’t cancel lecture

C. More speakers! Less Yuriy lecturing

(he’s so boring!)

In class, group activities

- The groupthink, phone design exercise
  - worth every penny
  - it should be made into a 1 lecture activity
  - booo group work

- Pair programming (movie script writing, vehicle design)
  - it’s good to work with others and I learned something
  - I didn’t like it

Now the official evaluations

May I have a volunteer to deliver the forms to

Interviewing tips and tricks

- What is a develop job like?
  - At Google / Microsoft, you meet with 3-5 people
    - one on one
    - sometimes two on one
    - more meetings is better
  - Start ups will more often have just 1 or 2 meetings

Your goal is not to impress with what you know, but with being able to think fast, find answers, reason about problems.

What will they ask you

- Some generic about yourself questions
  - tell me about your greatest strength
  - tell me about a time you failed and how you dealt with it
  - tell me about a conflict you've had and how you coped

http://blog.simplyhired.com/2013/06/break-down-the-30-common-job-interview-questions-into-3-types-career-stories.html

- Coding questions
  - typically fairly simple, data structure questions
    - write a queue class
    - remove a node from a balanced tree
  - looking for how you think and reason about the problem

Puzzles!

- They won’t talk about goats, wolves, and cabbage.
- It’s amazing how many different puzzle problems are out there.
- Practice some beforehand
  - The key is to talk aloud while you solve them.
    They care little if you find the solution;
    They care lots how you reason about the problem.

Example puzzles: eggs

You have two identical eggs. Standing in front of a 100 floor building, you wonder what is the maximum floor number from which the egg can be dropped without breaking it. What is the minimum number of tries needed to find out the solution?

boys and girls

In a country where everyone wants a boy, each family continues having babies till they have a boy. After some time, what is the proportion of boys to girls in the country?

rings and pirates

Alice lives alone on an island. She is in love with Bob, who lives alone on his own island. Pirates, to make some money on the side, deliver mail between islands, but they steal anything that is sent that is not locked. Alice wishes to propose to Bob by sending him a ring.

Alice has an unlimited number of boxes of various sizes. Boxes can be locked with many pad locks. Alice and Bob each have an unlimited number of locks, each with its own key, but they don’t have keys to the other’s locks. Help Alice send the ring!

Zero knowledge proofs

- Millennium Prize Problems
  - – seven problems posed in 2000
  - – solve one, get $1,000,000
  - – one has been solved ($ declined)

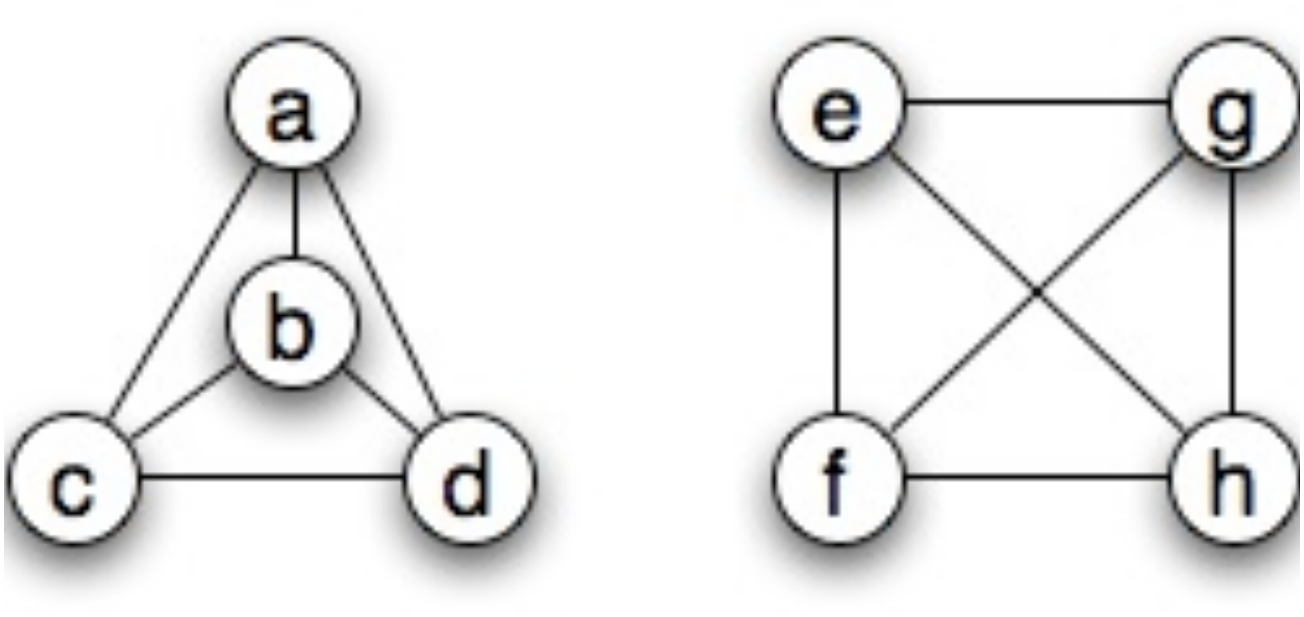
Grigori Perelman

- Suppose I solved the P vs. NP problem

for simplicity, let's assume I developed a polynomial-time algorithm for identifying if two graphs are isomorphic. (Not quite NP-complete, but close.)

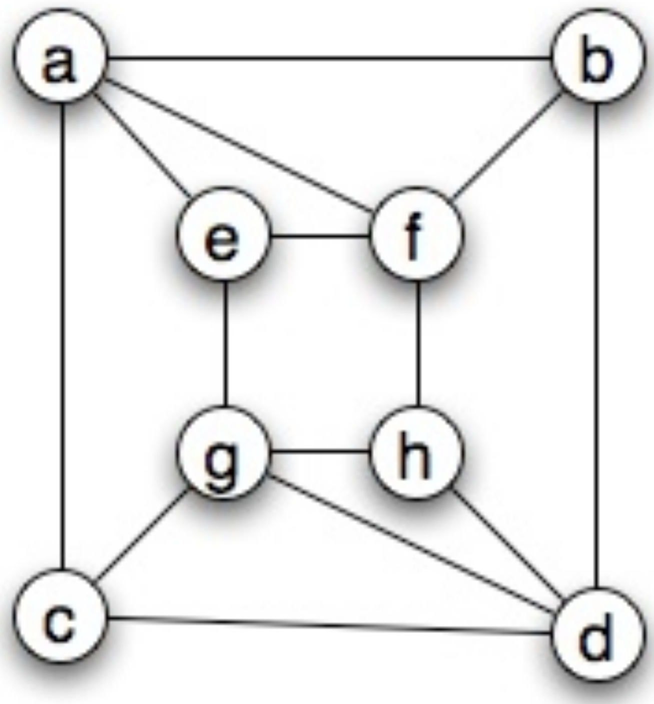
How can I prove to you that I have the algorithm, but without giving it away?

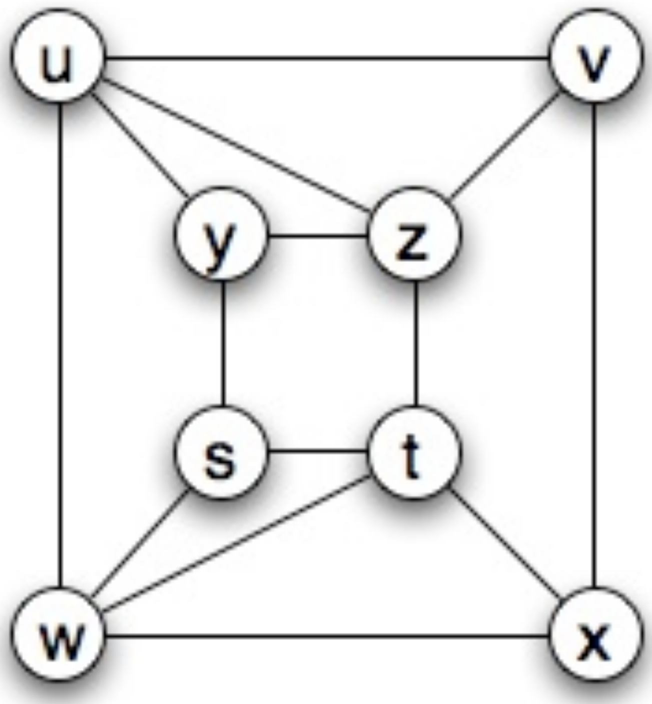
Are these graphs isomorphic?



Can you rearrange the vertices in one to look like the other?

What about these?





Can you rearrange the vertices in one to look like the other?

So let’s say I have an algorithm

- My algorithm:
- input: 2 graphs
- output: YES they are isomorphic, or

  NO they are not isomorphic.
- What can I do to prove to you that I have this algorithm?

Solve my isomorphic problem for you

- I could give you two graphs and tell you if they’re isomorphic

- Does this convince you?

Solve your isomorphic problem for you

- You could give me two graphs and tell you if they're isomorphic

- Does this convince you?

Solve your isomorphic problem for you

- You could give me two graphs and tell you if they’re isomorphic
- Does this convince you?

what are the odds that I guessed right?

Can we build on that last solution?