

15-251

Some
~~Great~~ Theoretical Ideas
~~in~~ Computer Science
for

Reminders

Final: Friday May 9th 8:30-11:30, McConomy.

Review session: ???

List of Lectures

1. Solving Problems, Writing Proofs and Enjoying the Pain
2. Combinatorial Games
3. Pancakes With a Problem
4. Inductive Reasoning
5. Finite Automata
6. Counting I
7. Counting II
8. Counting III
9. Unary and Binary
10. The Math of the 1950's Dating
11. Probability I: Counting in Terms of Proportions and Expectations
12. **NO CLASS**
13. Probability II: Random Walks
14. Raising a Number to a Power
15. Primes, GCD, and Continued Fractions
16. The Golden Ratio, Fibonacci, and Other Recurrences
17. Number Theory and RSA
18. Group Theory I
19. Group Theory II
20. Graphs I
21. Graphs II
22. This is the Big-Oh!
23. Grade School Revisited: How to Add and Multiply
24. Cantor's Legacy: Infinity And Diagonalization
25. Turing's Legacy: The Limits of Computation
26. Godel's Legacy: What is a Proof?
27. Efficient Reductions Between Problems
28. Complexity Theory: what is the P-versus-NP Question?

Questions About the Course?

Why theoretical ideas?
Why are algorithms important?

Some of the (many) applications

1. Error correction
 2. Optimization
 3. Zero knowledge
 4. Compression
 5. Secret sharing
 6. Sequencing the genome
 7. Cryptography
- ...

Error Correction

Want to send a sequence of integers
over a noisy channel

(1 4 23 1 17 19 -21)

Each number may get corrupted with
some (small) probability.

(1 5 23 1 17 19 21)

How do you detect errors?

How do you correct errors?

(Erasure) Error Correction

Want to send a sequence of integers
over a noisy channel

(1 4 23 1 17 19 -21)

Some of these numbers may get deleted

(1 X 23 1 17 19 X)

How do you find the missing numbers?

Clearly, we should build in some redundancy

Polynomials

Degree d polynomials:

$$P(x) = 3x + 27$$

$$P(x) = 5x^2 - 17x + 91$$

$$P(x) = 3x^{17} - 9x^3 + 1$$

$$P(x) = 2$$

$$P(x) = 0$$

A “root” is a point x such that $P(x) = 0$

Polynomials

Degree d polynomials.

A root is a point x such that $P(x) = 0$

Fact: Any degree d polynomial has at most d roots.
(if it is not zero everywhere)

Fact: If I give you $(d+1)$ points $x_0, x_1, \dots, x_d$
and values $y_0, y_1, \dots, y_d$ at these $(d+1)$ points
then there is a **unique** degree d polynomial $P(x)$
such that $P(x_k) = y_k$ for $0 \leq k \leq d$

(Erasure) Error Correction

Want to send a sequence of integers
over a noisy channel.

(1 4 23 1 17 19 -21)

Some of these numbers may get deleted

(1 X 23 1 17 19 X)

How do you find the missing numbers?

(Erasure) Error Correction

Want to send the seven numbers

(1 4 23 -1 17 19 -21)

Think of the numbers as being coefficients:

$$P(x) = 1x^6 + 4x^5 + 23x^4 - 1x^3 + 17x^2 + 19x^1 - 21$$

Evaluate this polynomial at points 0,1,2,...,15

Send the values $P(0)$, $P(1)$, $P(2)$, $P(3)$, ..., $P(15)$

As long as we receive 7 of the values sent out, can reconstruct $P(x)$, and hence get the original 7 numbers back

Some of the (many) applications

1. Error correction
 2. Optimization
 3. Zero knowledge
 4. Compression
 5. Secret sharing
 6. Sequencing the genome
 7. Cryptography
- ...

Baseball Scheduling

How do you draw up MLB's schedule?

- 30 teams
- 162 game schedule
- Many many constraints:
Cincinnati is always home on Opening Day, while Boston plays at Fenway Park each Patriots Day. The Mets have potential traffic and parking concerns when the U.S. Open tennis tournament is in town, and the Minnesota Twins share the Metrodome with the NFL's Vikings.
- Don't want things like: Texas Rangers have nine-game Detroit-to-Oakland-to-Minnesota road trip (with no day off)

Massive scheduling problem.

Use Optimization Tools

- Mike Trick in the Tepper school

<http://www.sports-scheduling.com/>



- Linear and integer programming software
- CPLEX
- Uses theoretical ideas: algorithms and geometry.
 - and sophisticated implementation.

Some of the (many) applications

1. Error correction
 2. Optimization
 3. Zero knowledge
 4. Compression
 5. Secret sharing
 6. Sequencing the genome
- ...

Wouldn't it be great

If you could “prove” (beyond reasonable doubt)
to someone
that statement A is true.

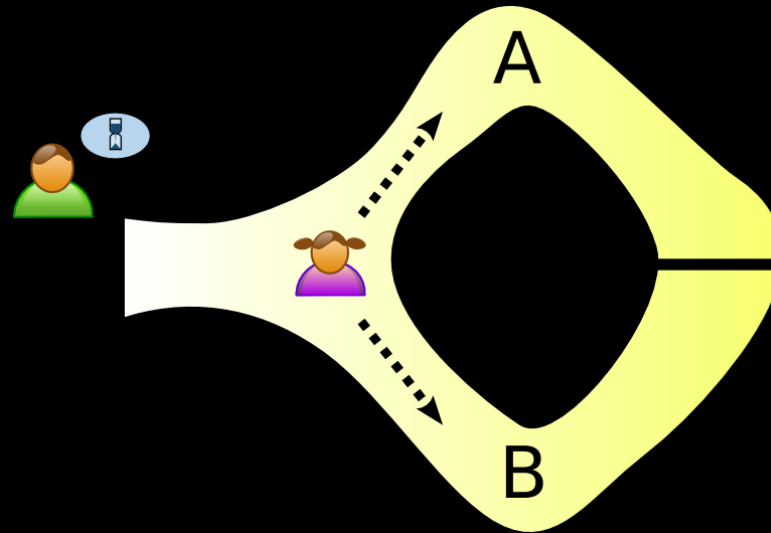
they become thoroughly convinced

But they don't learn anything
apart from the fact
that A is true.

Example “Zero-Knowledge” Proof

Alice, Bob, Cave, Magic door, secret password

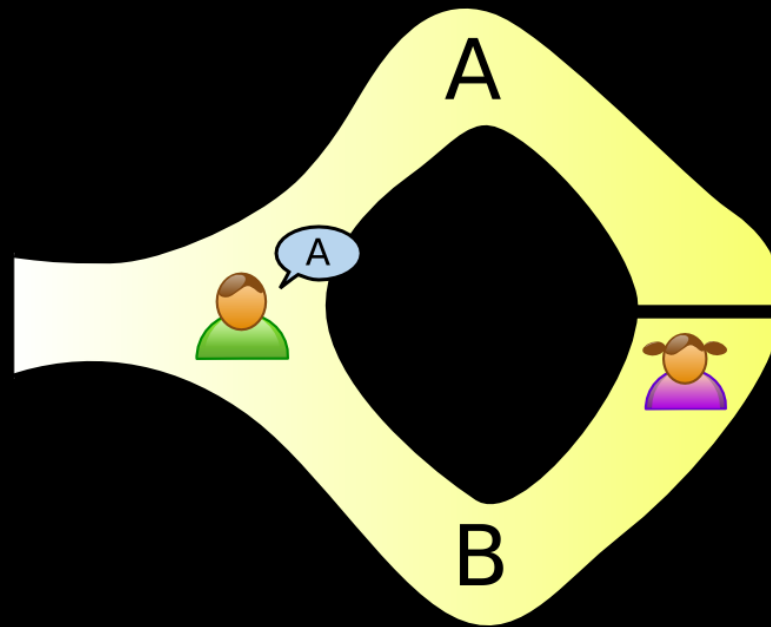
Alice claims she knows the secret password.



Alice chooses direction to enter into cave
any way she wants

Bob Calls

Bob stands at mouth of cave, asks her to come out from one of the two sides (randomly chosen)



Alice Must Comply

If Alice knows the password, she can come out on that side.

If she doesn't, she either fails or is lucky to be on the side that Bob called.

} 50% chance of failure



Repeat 100 times:
if Alice succeeds every time,
either she knows password,
or got lucky 100 times (chance is 1 in 2^{100})

Some of the (many) applications

1. Error correction
 2. Optimization
 3. Zero knowledge
 4. Compression
 5. Secret sharing
 6. Sequencing the genome
 7. Cryptography
- ...

Contest

First person to finish their cupcake gets
1% on the final.

By participating in this competition, you
agree to the following:

I understand that eating cupcakes can be a dangerous activity and that, by doing so, I am taking a risk that I may be injured.

I hereby assume all the risk described above, even if Luis von Ahn, his TAs or agents, through negligence or otherwise, otherwise be deemed liable. I hereby release, waive, discharge covenant not to sue Luis von Ahn, his TAs or any agents, participants, sponsoring agencies, sponsors, or others associated with the event, and, if applicable, owners of premises used to conduct the cupcake eating event, from any and all liability arising out of my participation, even if the liability arises out of negligence that may not be foreseeable at this time.

Please don't choke yourself...



Thanks, and
Good Luck on the Exam!



