Warm up:
Pick up a slip of paper from the front
Take out a coin
(Pennies up front if you need one)
(please return them at end)
Think of embarrassing yes/no questions to ask me
Today’s Keywords

• Differential Privacy
• NP-Completeness
• HW9 due tonight at 11pm
  – Reductions, Graphs
  – Written (LaTeX)

• HW10C due tonight at 11pm
  – Implement a problem from HW9
  – No late submissions
Final Exam

• Monday, December 9, 7pm in Maury 209 (our section)
  – Practice exam out! Solutions coming tomorrow!
  – Review session Saturday, 1pm, in Olsson 120
  – SDAC: please schedule for some time on Monday 12/9
As Computer Coding Classes Swell, So Does Cheating

BIZ & IT —

Code copypasta increasingly common in CS education

Roughly 22 percent of Stanford honor code violations involve plagiarism in ...

RYAN PAUL - 2/12/2010, 5:11 PM

THE DAILY ILLINI

The independent student newspaper at the University of Illinois

College of Engineering piloting program to combat cheating
Differential Privacy

• Gives a way to probabilistically answer questions about data without giving away its content
• You can get statistical certainty on the answer
• We’re going to use a simple example
Scheme

• Flip a coin:
  – If Heads, respond “yes”
  – If Tails, truthfully answer an embarrassing question:

• Questions
How does it work

• Assume everyone participates honestly
• We know 50% of “yes” answers were from the coin landing heads
  – If 100 people participate, eliminate 50 “yes” responses
  – Proportion of “yes” answers given by remaining “yes” answers
• Consider a person who answers “no”
  – We know this person didn’t cheat
• Consider a person who answers “yes”
  – Most people (≥ 50%) who answered “yes” only did so because the coin landed heads
  – It’s still more likely that this person did not cheat
How many people have streaked the lawn?

Your Turn!

• Flip a coin:
  – If Heads, respond “yes”
  – If Tails, truthfully answer an embarrassing question:
    • **Have you ever streaked the lawn?**
      – Write “yes” or “no”
      – Pass the slip to your left
• At the end, tally total “yes” and total “no” and pass totals forward
Impagliazzo’s 5 Worlds

Describes what computer science might look like depending on how certain open questions are answered.

• Algorithmica
• Heuristica
• Pessiland
• Minicrypt
• Cryptomania
Büttner’s goal: embarrass Gauss

- Come up with a problem which Gauss finds difficult but Büttner can solve quickly
  1. Come up with a graph and a Vertex Cover together
  2. Give the graph to Gauss
  3. When Gauss is stumped show the Vertex Cover
Algorithmica

\[ P = NP \]

- NP problems solvable efficiently
- Gauss can quickly find the solution to Büttner’s problem
- Gauss is not embarrassed

Advantages:
- VLSI Design
- Strong AI
- Cure for cancer?

Disadvantages:
- No privacy
- Computers take over
Advantages:
• Maybe similar to Algorithmica
• Depends on real-world distributions

Disadvantages:
• Bad real world distributions could make things hard to solve

$P \neq NP$ in worst case, $P = NP$ on average
• Time to come up with a problem $\approx$ time to solve it
• Büttner can give hard problems, but it’s hard to find them
• Gauss is not embarrassed
$P \neq NP$ on average, one-way functions don’t exist

- Hard problems easy to find, but *solved* hard problems difficult to find
- Gauss can be stumped, but Büttner does no better

**Advantages:**
- Universal Compression
- Reverse Engineering
- Derandomization

**Disadvantages:**
- No crypto
- No algorithmic advantages
- Progress is slow
One-way functions exist, no public key cryptography

- Büttner can give hard problems to Gauss and also know their solutions
- Gauss is embarrassed

Advantages:
- Private key crypto
- Can prove identity

Disadvantages:
- No electronic currencies
Public Key Crypto Exists
• Büttner can come up with problems and solutions, then share the solution with all other students
• Gauss is very embarrassed

Advantages:
• Secure computation
• Signatures
• Bitcoin, etc.

Disadvantages:
• Algorithmic progress will be slow
Does P=NP?

<table>
<thead>
<tr>
<th>Year</th>
<th>P ≠ NP</th>
<th>P = NP</th>
<th>Ind</th>
<th>DC</th>
<th>DK</th>
<th>DK and DC</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>2002</td>
<td>61 (61%)</td>
<td>9 (9%)</td>
<td>4 (4%)</td>
<td>1 (1%)</td>
<td>22 (22%)</td>
<td>0 (0%)</td>
<td>3 (3%)</td>
</tr>
<tr>
<td>2012</td>
<td>126 (83%)</td>
<td>12 (9%)</td>
<td>5 (3%)</td>
<td>5 (3%)</td>
<td>1 (0.6%)</td>
<td>1 (0.6%)</td>
<td>1 (0.6%)</td>
</tr>
</tbody>
</table>
When Will P=NP be resolved?

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2002</td>
<td>5(5%)</td>
<td>12(12%)</td>
<td>13(13%)</td>
<td>10(10%)</td>
<td>5(5%)</td>
<td>12(12%)</td>
<td>4(4%)</td>
<td>0(0%)</td>
</tr>
<tr>
<td>2012</td>
<td>0(0%)</td>
<td>2(.01%)</td>
<td>17(11%)</td>
<td>18(12%)</td>
<td>5(3%)</td>
<td>10(6.5%)</td>
<td>10(6.5%)</td>
<td>9(6%)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2002</td>
<td>1(1%)</td>
<td>0(0%)</td>
<td>0(0%)</td>
<td>0(0%)</td>
<td>0(0%)</td>
<td>5(5%)</td>
<td>0(0%)</td>
</tr>
<tr>
<td>2012</td>
<td>4(3%)</td>
<td>5(3%)</td>
<td>2(1.2%)</td>
<td>5(3%)</td>
<td>2(1.2%)</td>
<td>3(2%)</td>
<td>3(2%)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Long Time</th>
<th>Never</th>
<th>Don’t Know</th>
<th>Sooner than 2100</th>
<th>Later than 2100</th>
</tr>
</thead>
<tbody>
<tr>
<td>2002</td>
<td>0(0%)</td>
<td>5(5%)</td>
<td>21(21%)</td>
<td>62(62%)</td>
<td>17 (17%)</td>
</tr>
<tr>
<td>2012</td>
<td>22(14%)</td>
<td>5(3%)</td>
<td>8(5%)</td>
<td>81(53%)</td>
<td>63 (41%)</td>
</tr>
</tbody>
</table>
Scott Aaronson I believe $P \neq NP$ on basically the same grounds that I think I won’t be devoured tomorrow by a 500-foot-tall robotic marmoset from Venus, despite my lack of proof in both cases.

Suggested rephrased question:

*will humans manage to prove $P \neq NP$ before they either kill themselves out or are transcended by superintelligent cyborgs? And if the latter, will the cyborgs be able to prove $P \neq NP$?*

Neil Immerman $P \neq NP$ will be resolved somewhere between 2017 and 2034, using some combination of logic, algebra, and combinatorics.

Donald Knuth: (Retired from Stanford) It will be solved by either 2048 or 4096. I am currently somewhat pessimistic. The outcome will be the truly worst case scenario: namely that someone will prove “$P=NP$ because there are only finitely many obstructions to the opposite hypothesis”; hence there will exists a polynomial time solution to SAT but we will never know its complexity!