CS4102 Algorithm

youtube.com
Exact instructions Challenge - THIS is why my kids want to kill me. | Josh Darnit

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

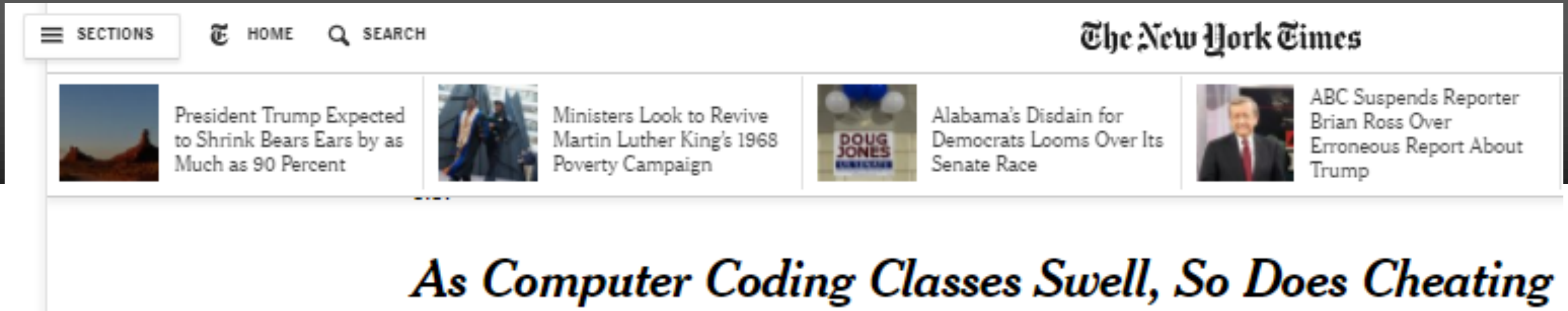
CLRS Readings

Homeworks

- 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



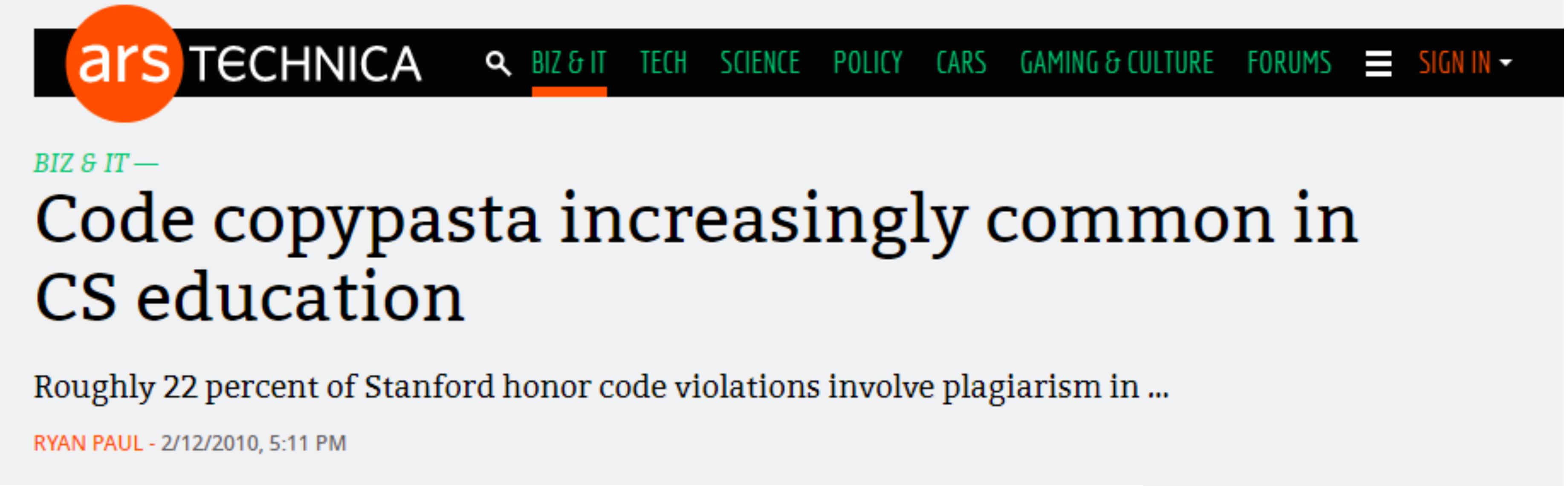
President Trump Expected to Shrink Bears Ears by as Much as 90 Percent

Ministers Look to Revive Martin Luther King's 1968 Poverty Campaign

Alabama's Disdain for Democrats Looms Over Its Senate Race

ABC Suspends Reporter Brian Ross Over Erroneous Report About Trump

As Computer Coding Classes Swell, So Does Cheating

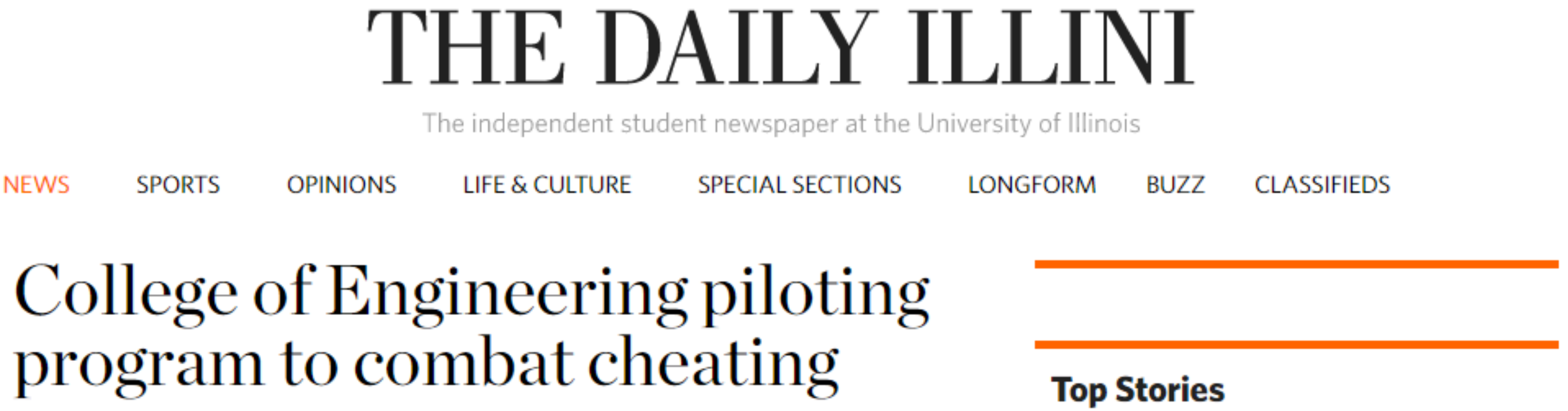


BIZ & IT —

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



College of Engineering piloting program to combat cheating

Top Stories

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 ($\geq 50\%$) 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

Gauss vs. Büttner

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

$P = NP$

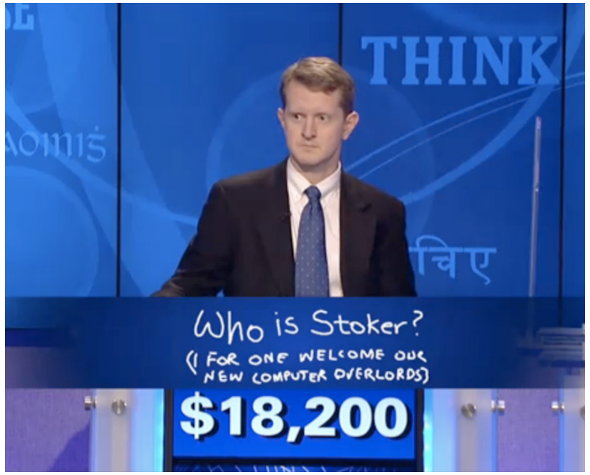
- NP problems solvable efficiently
- Gauss can quickly find the solution to Büttner's problem
- Gauss is not embarrassed

Advantages:

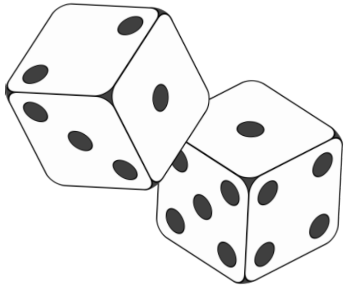
- VLSI Design
- Strong AI
- Cure for cancer?

Disadvantages:

- No privacy
- Computers take over



Heuristica



$P \neq NP$ in worst case, $P = NP$ on average

- Time to come up with a problem ≈ time to solve it
- Büttner can give hard problems, but it's hard to find them
- Gauss is not embarrassed

Advantages:

- Maybe similar to Algorithmica
- Depends on real-world distributions

Disadvantages:

- Bad real world distributions could make things hard to solve

Pessiland

$P \neq NP$ 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

Minicrypt

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

Cryptomania

Public Key Crypto Exists

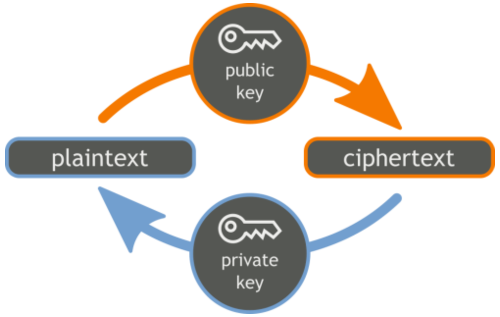
- Büttner can come up with problems and solutions, then share the solution with all other students
- Gauss is very embarrassed

Advantages:

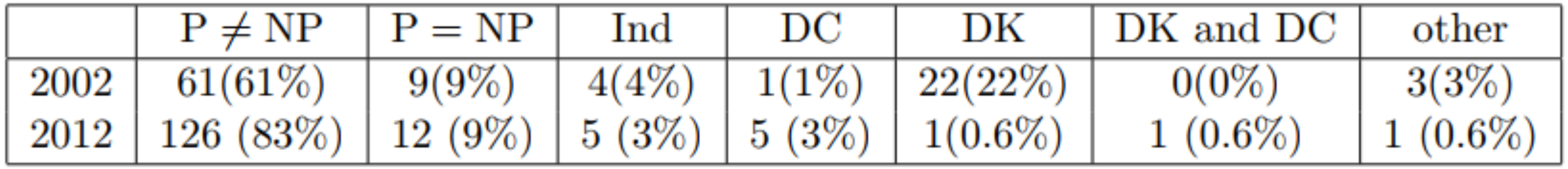
- Secure computation
- Signatures
- Bitcoin, etc.

Disadvantages:

- Algorithmic progress will be slow

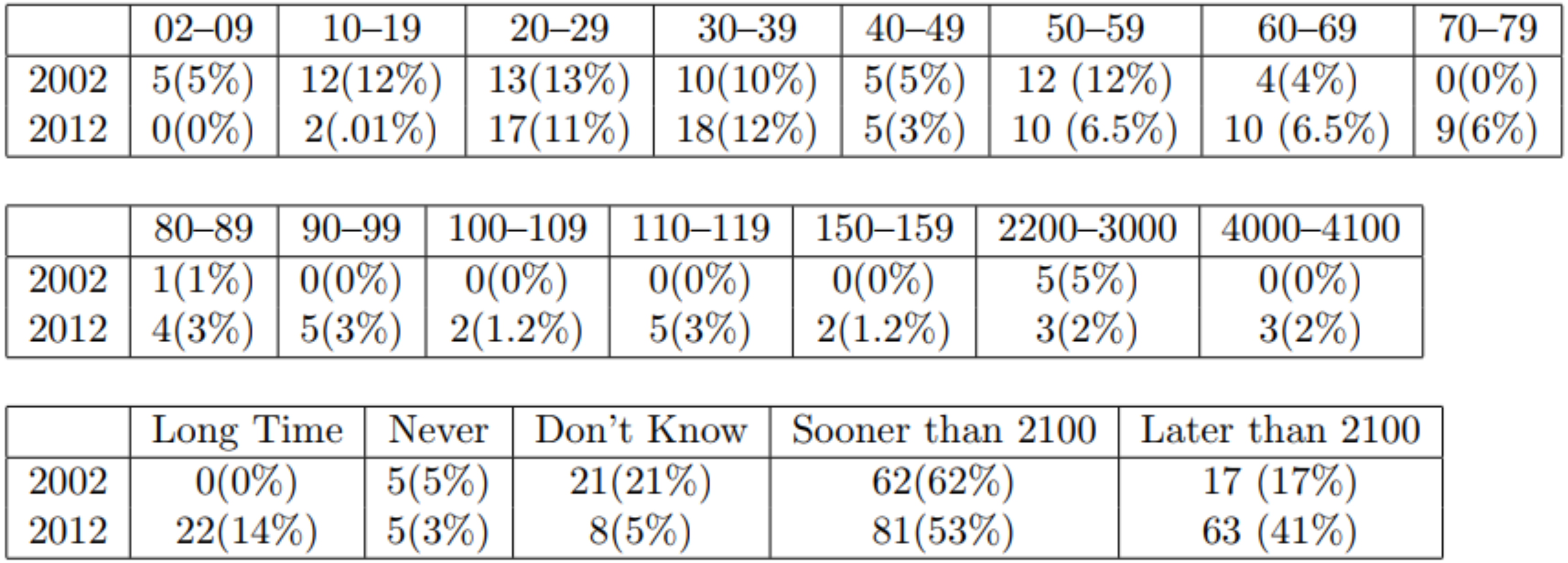


Does P=NP?



	P ≠ NP	P = NP	Ind	DC	DK	DK and DC	other
2002	61(61%)	9(9%)	4(4%)	1(1%)	22(22%)	0(0%)	3(3%)
2012	126 (83%)	12 (9%)	5 (3%)	5 (3%)	1(0.6%)	1 (0.6%)	1 (0.6%)

When Will P=NP be resolved?

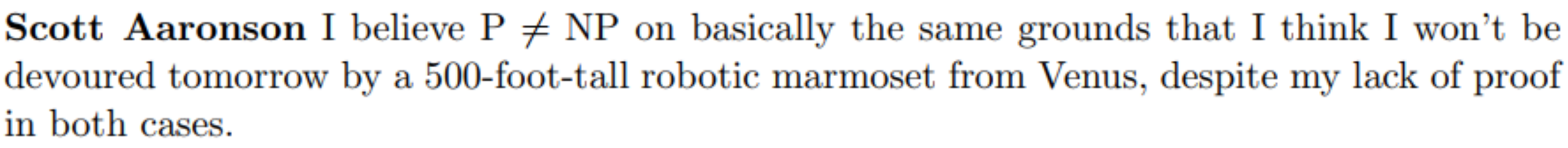


	02–09	10–19	20–29	30–39	40–49	50–59	60–69	70–79
2002	5(5%)	12(12%)	13(13%)	10(10%)	5(5%)	12 (12%)	4(4%)	0(0%)
2012	0(0%)	2(.01%)	17(11%)	18(12%)	5(3%)	10 (6.5%)	10 (6.5%)	9(6%)

	80–89	90–99	100–109	110–119	150–159	2200–3000	4000–4100
2002	1(1%)	0(0%)	0(0%)	0(0%)	0(0%)	5(5%)	0(0%)
2012	4(3%)	5(3%)	2(1.2%)	5(3%)	2(1.2%)	3(2%)	3(2%)

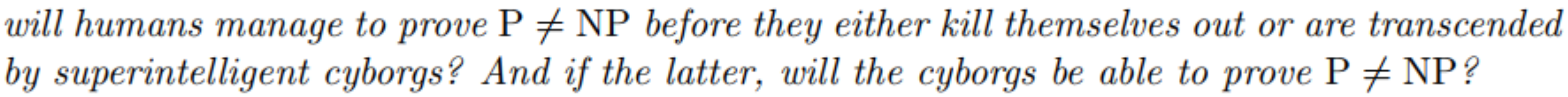
	Long Time	Never	Don't Know	Sooner than 2100	Later than 2100
2002	0(0%)	5(5%)	21(21%)	62(62%)	17 (17%)
2012	22(14%)	5(3%)	8(5%)	81(53%)	63 (41%)

Notable Statements on P vs NP

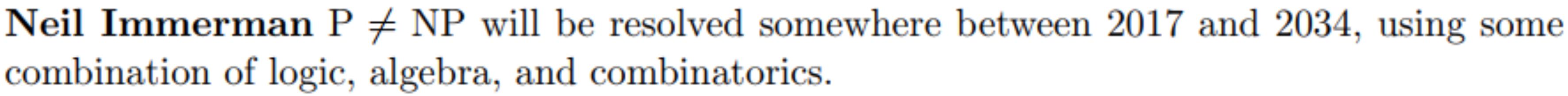


Scott Aaronson I believe $P \neq NP$ on basically the same grounds that I think I won't be devoured tomorrow by a 500-foot-tall robotic marmoset from Venus, despite my lack of proof in both cases.

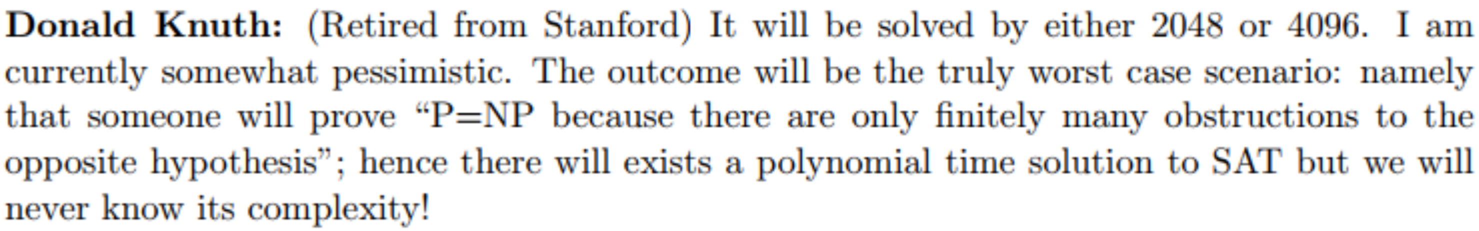
Suggested rephrased question:



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!