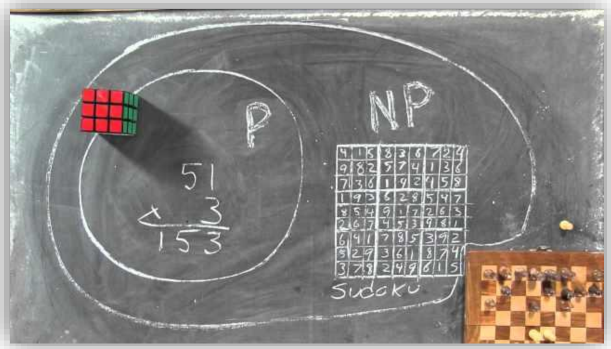
intro to the theory of computation

Instructor: Prof. James R. Lee

TA: Yiqing Ai

CSE 431
Winter 2018

Course web page:
http://www.cs.washington.edu/cse431
Sign up for the mailing list!



Textbook:
Primary: *Introduction to the Theory of Computation* (Sipser)
Secondary readings provided or optional

Evaluation and grading (approx):
Weekly homeworks 50%, Midterm 15%, Final 35%

First homework will be out on Tuesday (9-Jan);
due (electronic turn-in) before class 16-Jan

course content

Fundamentally, we ask the questions:

What can a computer do? What can it do efficiently?

What can't it do?

Why are compilers so bad at catching bugs?

Why can't they optimize my code better? Parallelize it?

Why does proving theorems seem hard?

Why can't they solve chess? Go?

Why does AI seem hard?

Is there a mathematical basis for the "singularity"?

Is there secure cryptography?

Is it safe against quantum computers?

What about side-channel attacks? (uh oh…)

aliens who play chess

Suppose an alien came to earth and claimed it could play perfect chess.

Before admitting defeat as the inferior species, is there any way we could test his/her/its claim?

Yes. In complexity theory, this is the theorem that $\mathrm{IP} = \mathrm{PSPACE}$.

We wouldn't need to spend billions of years playing against the alien over and over. Instead, we would engage in a short conversation about the sums of certain polynomials over a finite field.

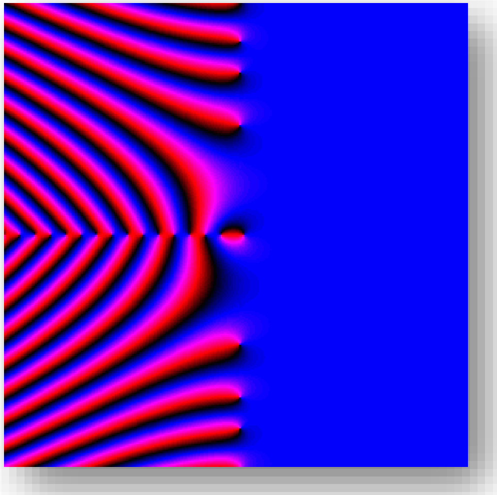
proofs and computational problems

The Riemann hypothesis

(A conjecture about the zeros of the Riemann zeta function.)

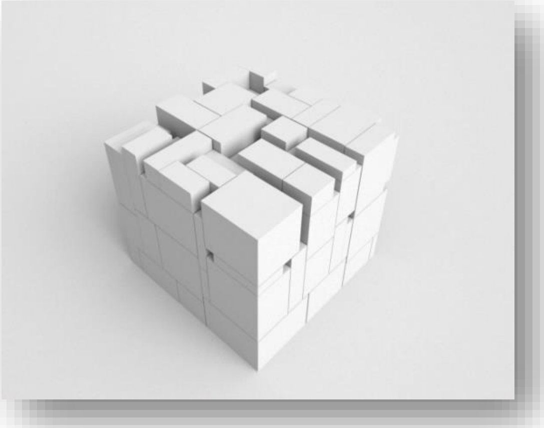
This is considered by some to be the most important unsolved problem in mathematics.

($1M Clay Math prize)



3D Bin Packing is NP-complete

There is a finite set of (a billion, say) of rectangular boxes of different sizes such that if you knew how to pack these boxes into the trunk of your car, you would also know a proof of the Riemann hypothesis.



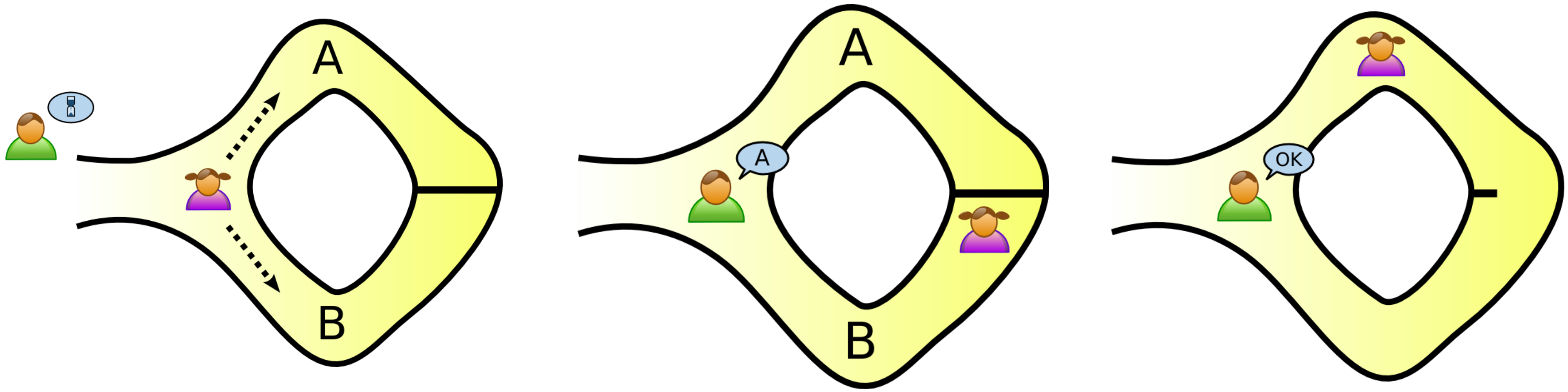
(Indeed, proofs of the Riemann hypothesis with at most a million symbols are in 1-1 correspondence with ways to pack the boxes into your car.)

zero-knowledge proofs

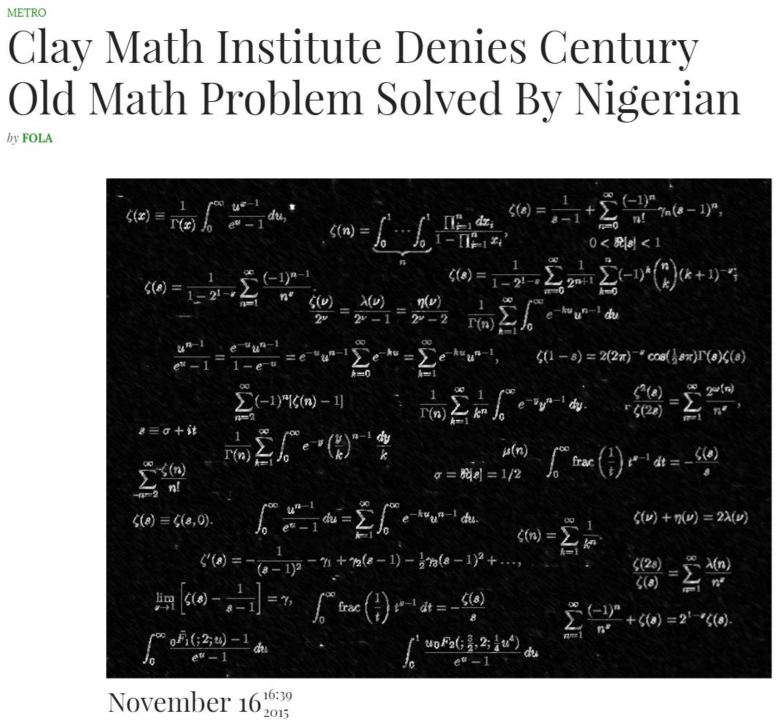
Suppose you manage to prove the Riemann Hypothesis.
(Good work. This should get you at least a B+ in the course!)

But you signed an NDA. Your company won't let you publish it. ☹
Can you still win the $1M prize?

Yes! There is a way to convince someone that you know a proof without revealing anything other than the fact that you proved it.



probabilistically checkable proofs



METRO

Clay Math Institute Denies Century Old Math Problem Solved By Nigerian

by FOLA

November 16 16:39 2015

Proof correct?

The verifier says “I agree.”

Proof wrong?

Then 99/100 times, the verifier will say “Wait! I found a bug.”

PCP Theorem: There is a way to write down the proof so that its validity can be checked by someone who picks 5 random words.

“Hello world.”

First assignment for freshman CSE students:

Write a Java program that prints “Hello world.” on the screen and then exits. Efficiency is not an issue. No partial credit.

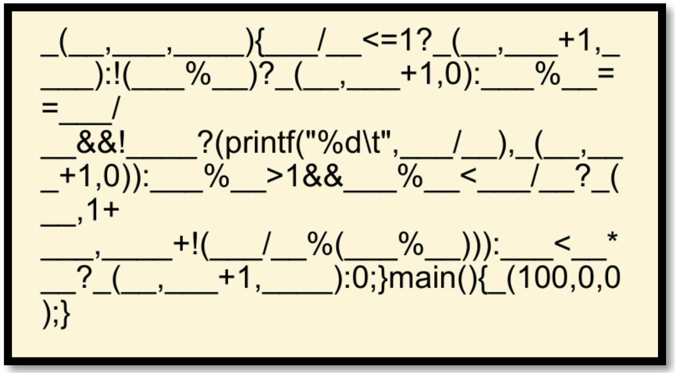
TA staff is annoyed:

OK, let’s write an **autograder** script.

If should take a Java program P as input and

- **PASS** if P prints “Hello world.” and halts
- **FAIL** otherwise

Need to handle code like this:



```
_(__,___,____){___/__<=1?_(__,___+1,_
___):!(___%__)?_(__,___+1,0):___%__=
=___/
__&&!____?(printf("%d\t",___/__),_(__,__
_+1,0)):___%__>1&&___%__<___/__?_(
__,1+
___,____+!(___/__%(___%__))):___<__*
__?_(__,___+1,____):0;}main(){_(100,0,0
);}
```

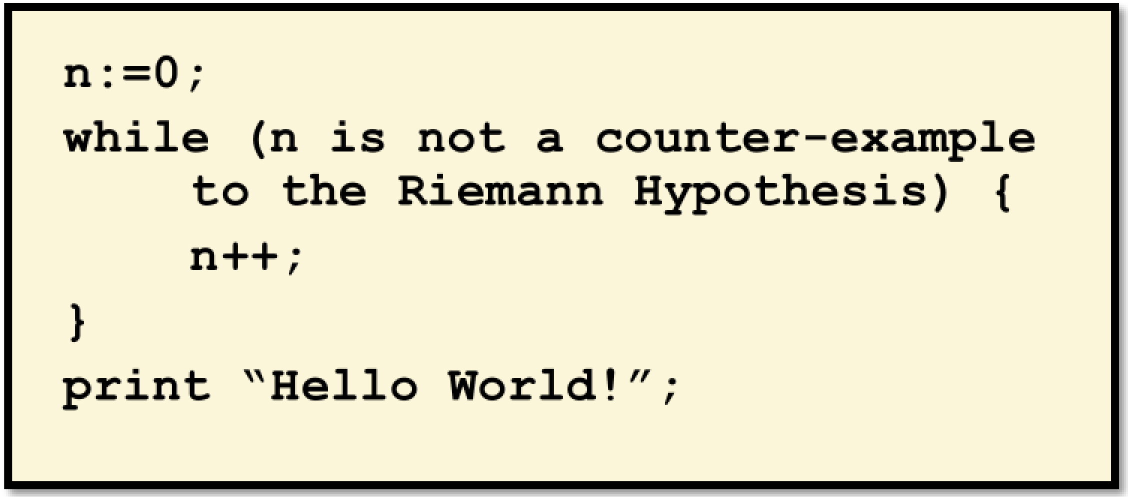
How would such a script work?

“Hello world.”

First assignment for freshman CSE students:

Write a Java program that prints “Hello world.” on the screen and then exits. Efficiency is not an issue. No partial credit.

This seems mean:



```
n:=0;
while (n is not a counter-example
      to the Riemann Hypothesis) {
      n++;
}
print “Hello World!”;
```

This program passes if and only if the Riemann Hypothesis is false.

Writing this autograder seems like a nightmare.

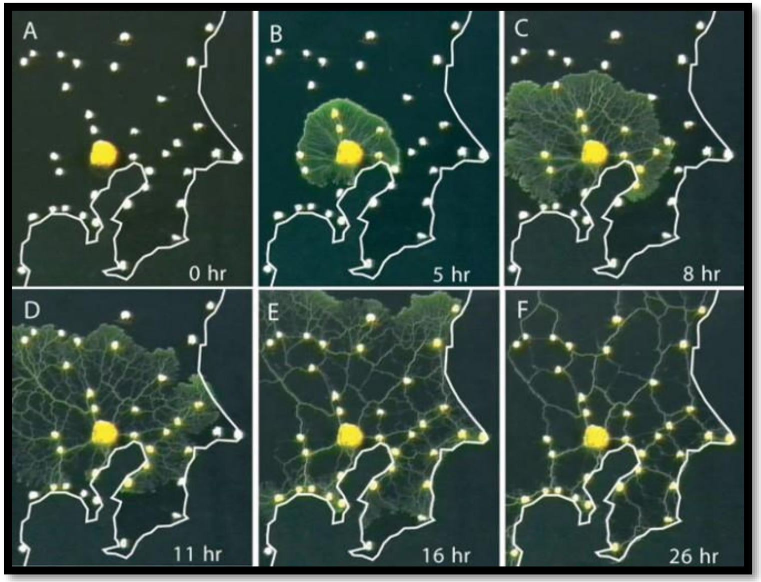
“Hello world.”

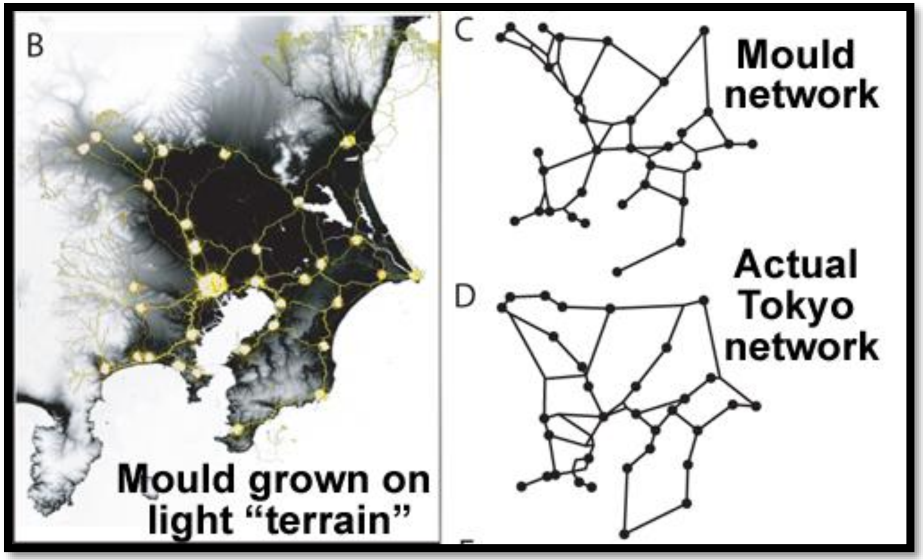
First assignment for freshman CSE students:

Write a Java program that prints “Hello world.” on the screen and then exits. Efficiency is not an issue. No partial credit.

Despite the simplicity of the assignment, there is NO COMPUTER PROGRAM that can grade it correctly.

What is a computer program? What is a computer?



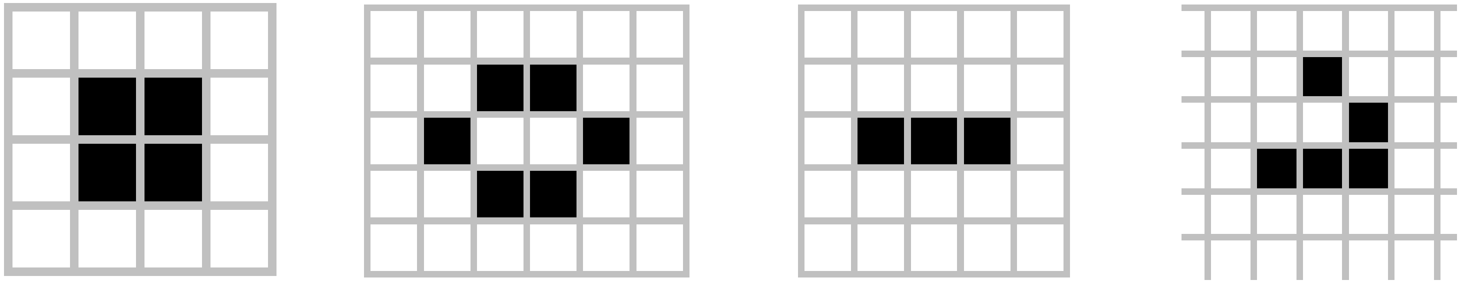


Conway's "Game of Life"

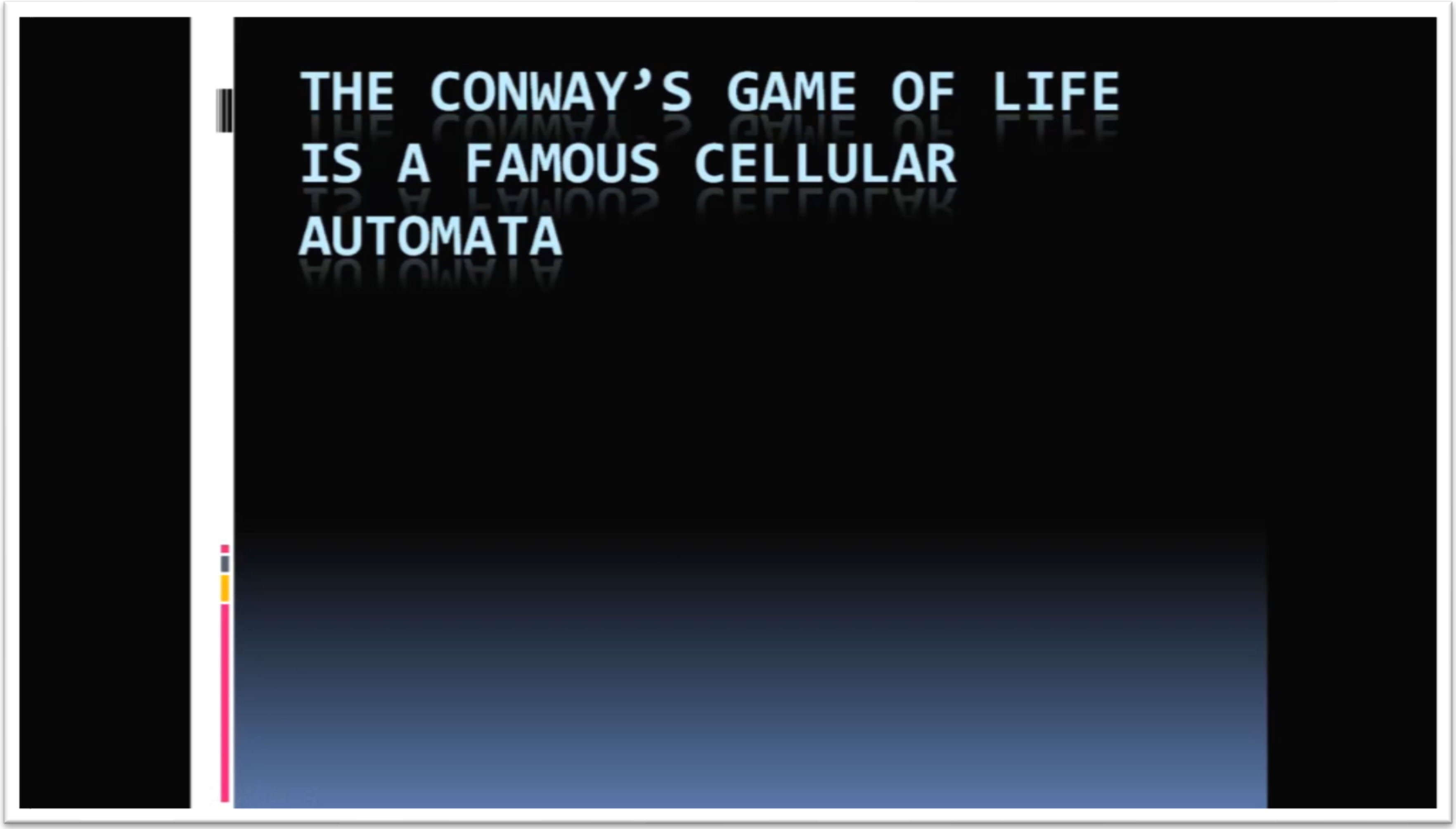
The universe of the Game of Life is an infinite two-dimensional grid of square *cells*, each of which is in one of two possible states, *alive* or *dead*.

Every cell interacts with its eight neighbors, which are the cells that are horizontally, vertically, or diagonally adjacent. At each step in time, the following transitions occur:

1. Any live cell with fewer than two live neighbors dies (under population)
2. Any live cell with two or three live neighbors lives on to the next generation.
3. Any live cell with more than three live neighbors dies (over population)
4. Any dead cell with exactly three live neighbors becomes a live cell (reproduction)



Conway's "Game of Life"



THE CONWAY'S GAME OF LIFE IS A FAMOUS CELLULAR AUTOMATA