Why CS Theory Matters

Bernard Chazelle
Princeton University
Amazing predictions
"X-rays will prove to be a hoax"

"Radio has no future."
“There is not the slightest indication that nuclear energy will ever be obtainable.
"I think there is a world market for maybe five computers."

Thomas Watson  
IBM Chairman  (1943 )
“Computing power doubles every two years.”

Moore’s Law
Moore's Law
In a few decades...

Moore's Law repealed

then what?
“There’s nothing to be discovered in physics today.”

Lord Kelvin (1824-1907)
“There’s nothing to be discovered in computer science today.”
“There’s nothing to be discovered in computer science today. ”

Lord Chazelle (2006)
“Computing will be the most disruptive scientific paradigm since quantum mechanics.”
“... and the end of Moore’s Law will make this even more obvious.”

Lord Chazelle (2006)
What is computing?

4 big ideas

- Universality
- Duality
- Self-reference
- Tractability
Alan Turing (1912-1954)

control

program data
Let 'em eat cake

Print this  Let 'em eat cake

Let 'em eat cake
Before Turing...
Before Turing...

Part of one of Babbage's Difference Engines

Courtesy IBM (www.ibm.com)

data
Fishing
Fishing manual

program
data
Fishing

Confucius

Fishing manual

program
data
needs to know how to fish
needs to know nothing about fishing
control

knows nothing

program
data
turn bits into sounds

0010101001010001000010011111010001010
display/organize email

001010100010100010011111010001010
Earth simulator
Duality
Saussure (1857-1913)

Print this

Let 'em eat cake

signifier

signified

program

data

Let 'em eat cake
Let ‘em eat cake

This is not a pipe

Magritte

Print this
Print this  

Let 'em eat cake
Self-reference
Duality: gene/protein
Self-reference: base pairs
all seem intractable

Protein folding

Scheduling

Map coloring

Andrew Wiles

Theorem proving

Traveling salesman
equivalent

Protein folding

Scheduling

Map coloring

Andrew Wiles

Theorem proving

Traveling salesman
Protein folding

E-commerce security

Map coloring

Traveling salesman

Andrew Wiles

Theorem proving

intractable ?
Two Amazing Consequences of Intractability

- Zero Knowledge
- Probabilistically Checkable Proofs
Zero Knowledge
Are you richer than me?

dunno, but I won’t tell you how much I’m worth
I won't tell you either.

So, who's richer?
There exists a dialogue...
Bob: blah blah blah
   blah blah blah
   blah blah blah
   blah blah blah

Bill: blah blah blah
   blah blah blah
   blah blah blah
   blah blah blah
at the end of which...
1. They will know who is richer
2. They will have learned nothing else

( with probability 0.99999999999 )
Zero Knowledge

I have no nukes!

Prove it!
1. No UN inspections

2. Both parties try to cheat
Who will believe me?

My Proof of Riemann’s Hypothesis

Step 1  write proof in special format

Step 2  verifier picks 5 random words
It is straightforward to check that this is a map of $\mathcal{O}$-modules. To check the injectivity of $\varphi$ suppose that $\varphi_\alpha(pD) = 0$. Then $\varphi_\alpha$ factors through $R_D/pD \cong \mathcal{O}$ and being an $\mathcal{O}$-algebra homomorphism this determines $\varphi_\alpha$. Thus $[\rho_{f,\lambda}] = [\rho_\alpha]$. If $A^{-1}\rho_\alpha A = \rho_{f,\lambda}$ then $A \mod \mathfrak{c}$ is seen to be central by Schur's lemma and so may be taken to be $I$. A simple calculation now shows that $\alpha$ is a coboundary.

To see that $\varphi$ is surjective choose

$$\Psi \in \text{Hom}_\mathcal{O}(p_D/(p_D^2, \mathcal{O}/\lambda^n)).$$

Then $\rho_\Psi: \text{Gal}(Q_\Sigma/Q) \to \text{GL}_2(R_D/(p_D^2, \ker \Psi))$ is induced by a representative of the universal deformation (chosen to equal $\rho_{f,\lambda}$ when reduced mod $p_D$) and we define a map $\alpha_\Psi: \text{Gal}(Q_\Sigma/Q) \to V_{\lambda^n}$ by

$$\alpha_\Psi(g) = \rho_\Psi(g)\rho_{f,\lambda}(g)^{-1} \in \begin{cases} 1 + p_D/(p_D^2, \ker \Psi) & p_D/(p_D^2, \ker \Psi) \\ p_D/(p_D^2, \ker \Psi) & 1 + p_D/(p_D^2, \ker \Psi) \end{cases} \subseteq V_{\lambda^n}$$

where $\rho_{f,\lambda}(g)$ is viewed in $\text{GL}_2(R_D/(p_D^2, \ker \Psi))$ via the structural map $\mathcal{O} \to R_D$ ($R_D$ being an $\mathcal{O}$-algebra and the structural map being local because of the existence of a section). The right-hand inclusion comes from

$$p_D/(p_D^2, \ker \Psi) \xrightarrow{\psi} \mathcal{O}/\lambda^n \xrightarrow{\epsilon} (\mathcal{O}/\lambda^n) \cdot \epsilon$$

$$1 \quad \mapsto \quad \epsilon.$$

Then $\alpha_\Psi$ is readily seen to be a continuous cocycle whose cohomology class lies in $H^1_{\text{ab}}(Q_\Sigma/Q, V_{\lambda^n})$. Finally $\varphi(\alpha_\Psi) = \Psi$. Moreover, the constructions are compatible with change of $n$, i.e., for $V_{\lambda^n} \hookrightarrow V_{\lambda^{n+1}}$ and $\lambda: \mathcal{O}/\lambda^n \hookrightarrow \mathcal{O}/\lambda^{n+1}$. □
There's something wrong.

I REJECT!
Verifier is correct with probability 0.99999999
There’s something wrong.

I REJECT!

If my 2000-page proof is wrong in only one step, how can verifier spot an error in 5 random words?

Verifier
Verifier

Everything looks fine.

I ACCEPT!

How does verifier know I proved Riemann’s hypothesis and not 2+2=4?

Verifier
The Algorithm
Very little does a lot

Mandelbrot Set (40 lines of code)
32
\times 17
\underline{224}
32
\underline{32}
= 544

grade school
FFT

signal processing
RSA encryption
e-commerce
PageRank

web search
Biomedical imaging

10 petabytes (~1MG)

Sloan Digital Sky Survey

10 petabytes/yr

150 petabytes/yr

10,000 times the Library of Congress
protein-protein interaction networks
Sciences of The Formula

math, physics, chemistry

\[ \oint H \cdot dl = 1 + \varepsilon \frac{d}{dt} \iiint E \cdot ds \]
Ampere's Law

\[ \oint E \cdot dl = -\mu \frac{d}{dt} \iiint H \cdot ds \]
Faraday's Law

\[ \varepsilon \iiint E \cdot ds = \iiint \iiint q_v\,dv \]
Gauss' Law

\[ \mu \iiint H \cdot ds = 0 \]
The Fourth Equation
Abu Abdullah Muhammad bin Musa al-Khwarizm (780-850)
“If Google is a religion, what is its God?

It would have to be The Algorithm.”
Thanks!

and see you at the revolution!