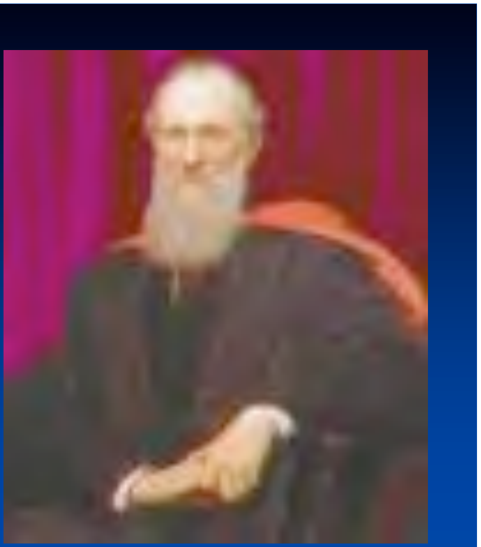
Why CS Theory Matters

Bernard Chazelle

Princeton University

Amazing predictions

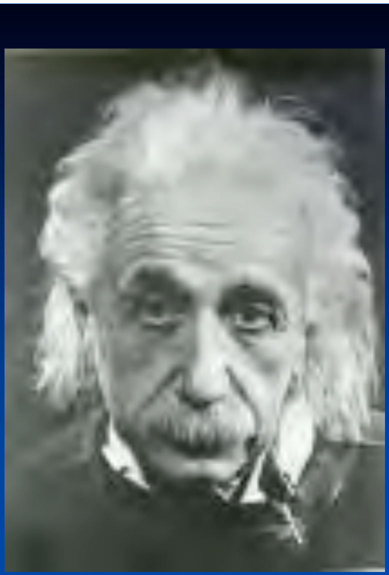
Lord Kelvin (1824-1907)



“ X-rays will prove to be a hoax"

“ Radio has no future. "

Albert Einstein (1932)



“ There is not the slightest indication
that
nuclear energy will ever be obtainable.

Thomas Watson
IBM Chairman (1943)

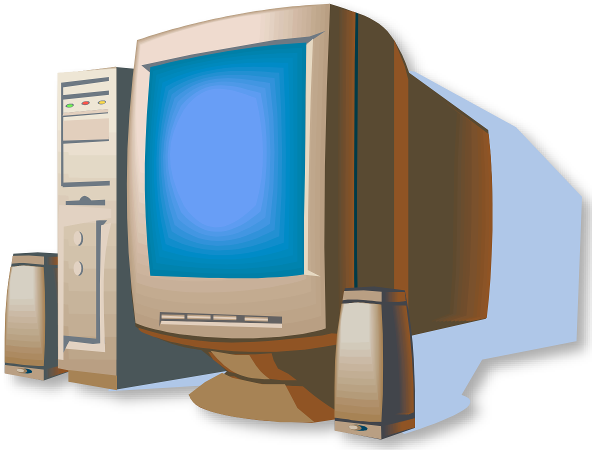
"I think there is a world market for maybe five computers."

Gordon Moore

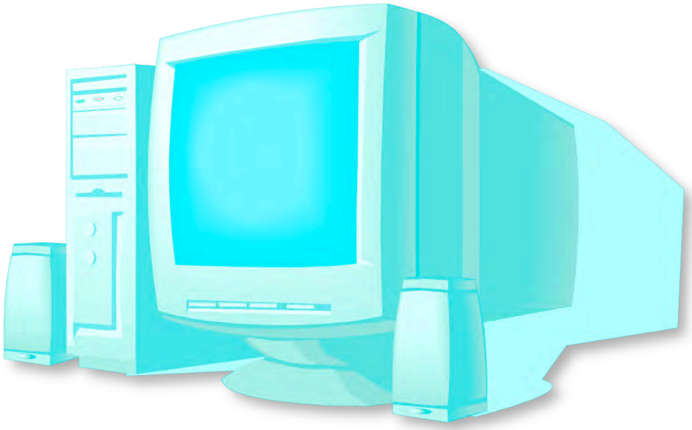
Intel Co-founder (1965)

“Computing power doubles every two years."

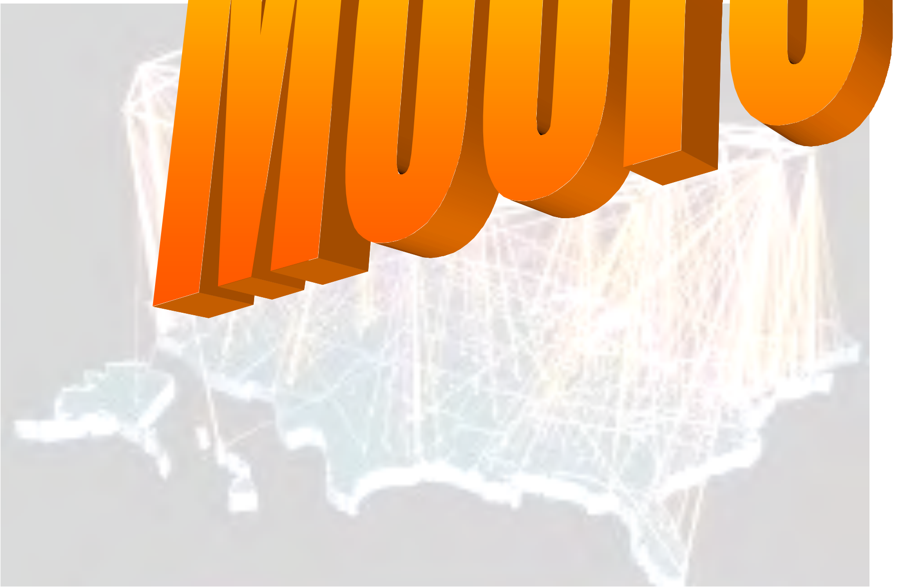
Moore's Law



iPod
Playlists
Browse
Extras
Settings
Backlight
MENU



Moore's Law

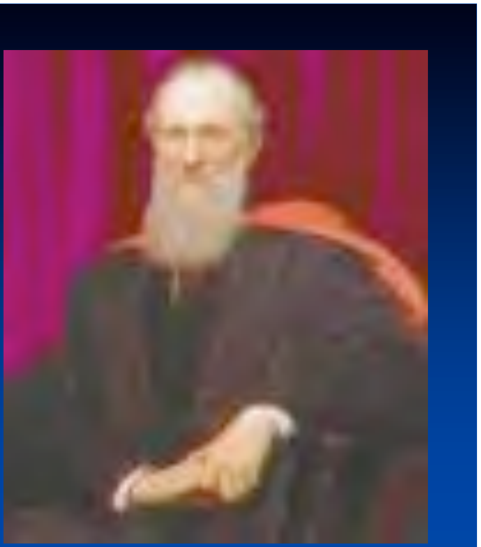


In a few decades…

Moore's Law repealed

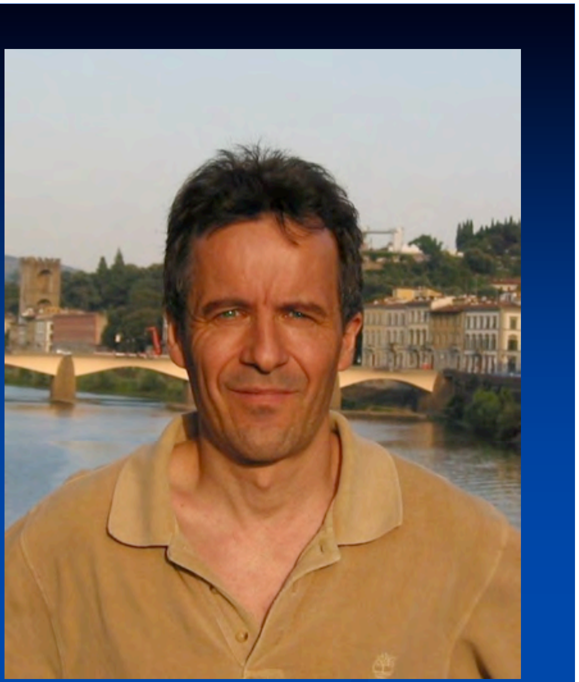
then what?

Lord Kelvin (1824-1907)



“ There’s nothing to be discovered in physics today. "

Lord Chazelle (2006)

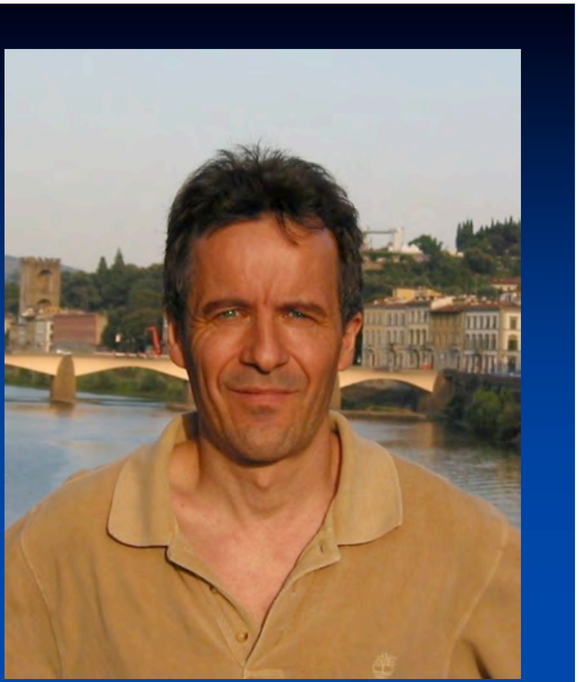


“ There’s nothing to be discovered in computer science today. "

~~*Lord Chazelle (2006)*~~

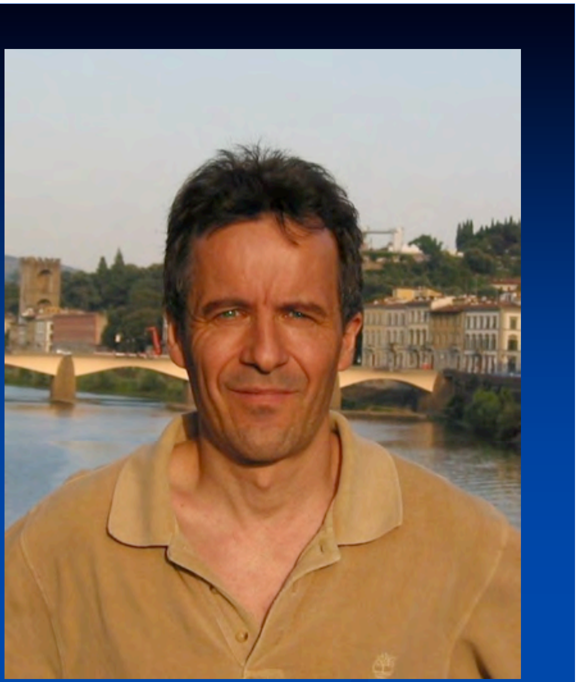
~~“ There’s nothing to be discovered in computer science today. "~~

Lord Chazelle (2006)



“ Computing will be the most disruptive scientific paradigm since quantum mechanics."

Lord Chazelle (2006)



“ … and the end of Moore’s Law will make this even more obvious."

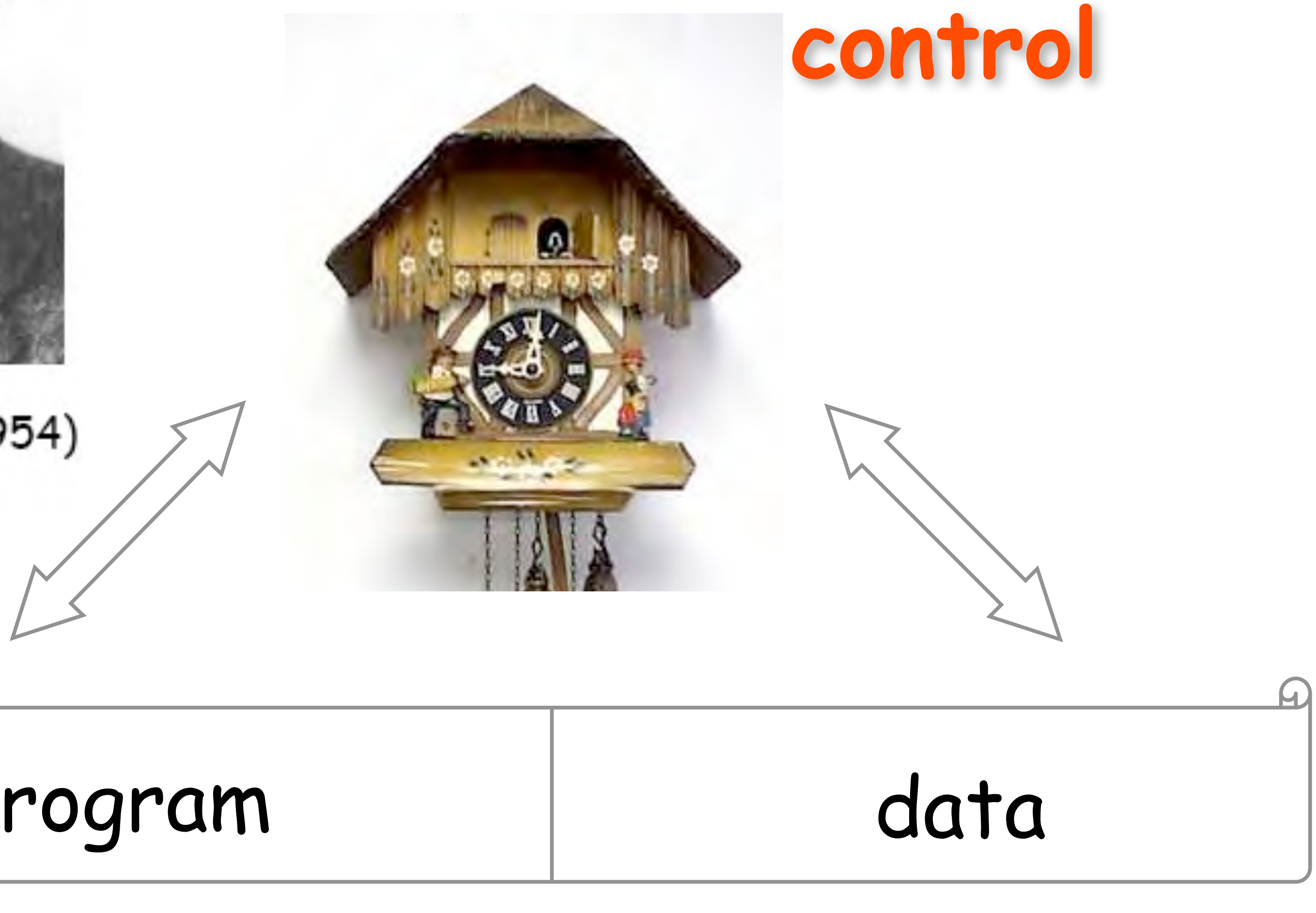
What is computing ?

4 big ideas

- Universality
- Duality
- Self-reference
- Tractability

Universality

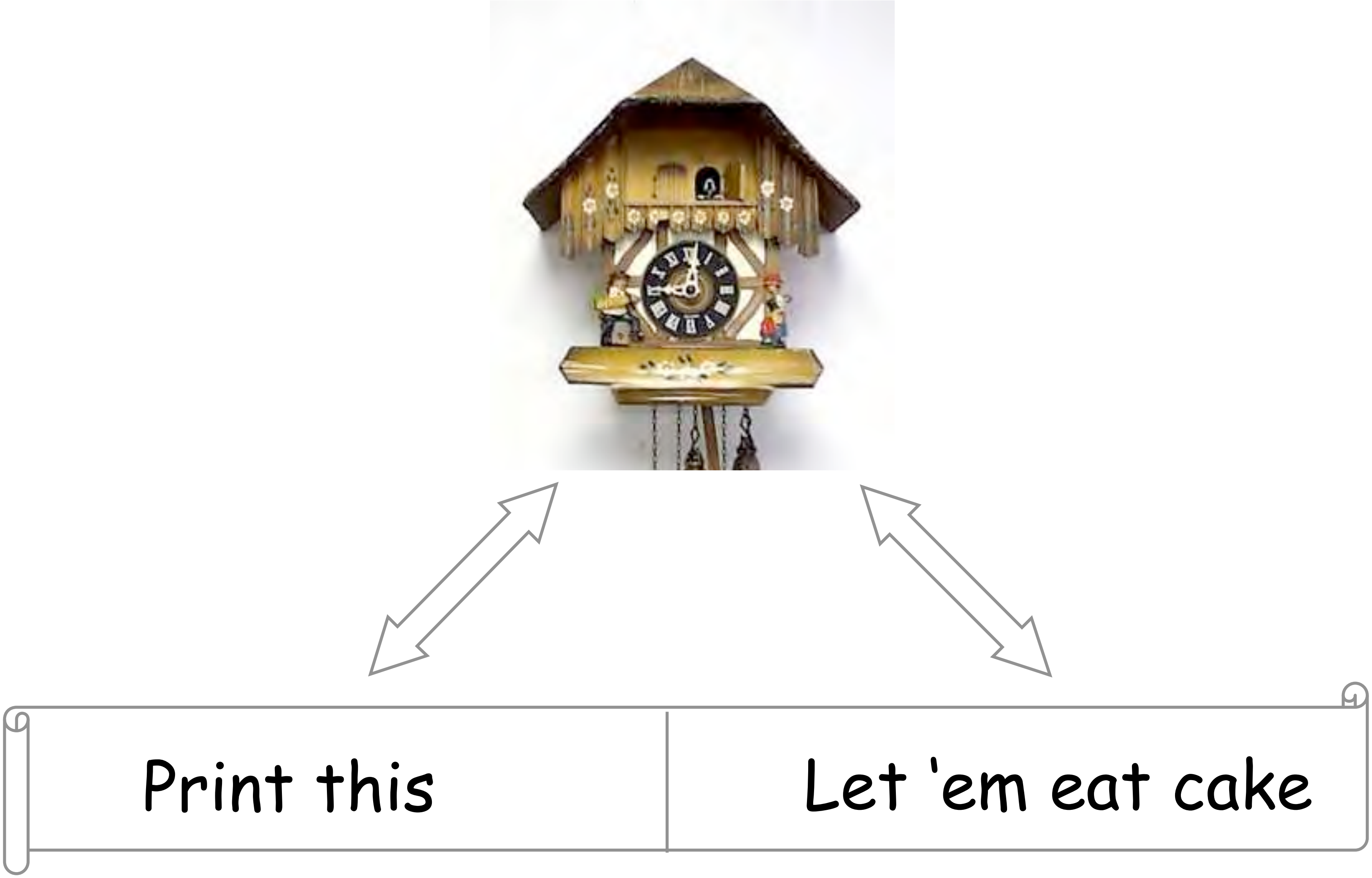
Alan Turing (1912-1954)



control

program

data

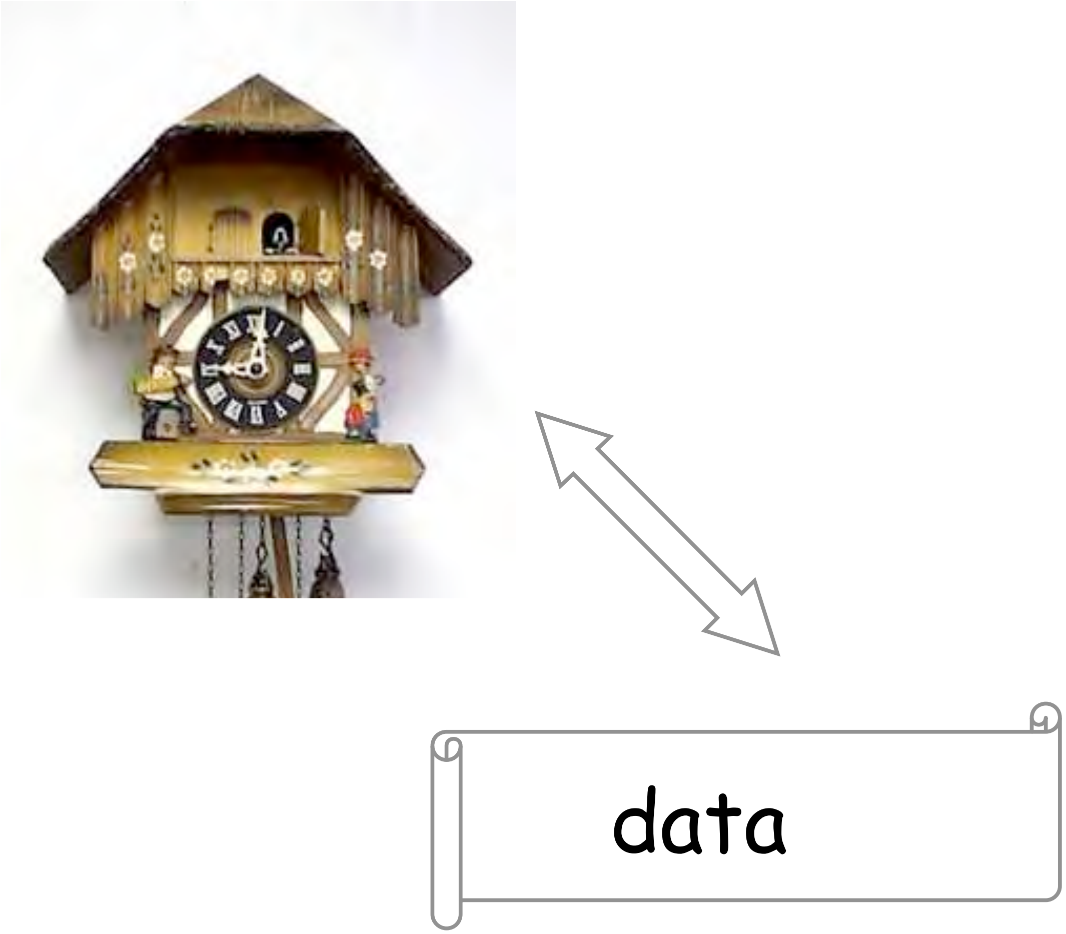


Print this

Let 'em eat cake

Let 'em eat cake

Before Turing…

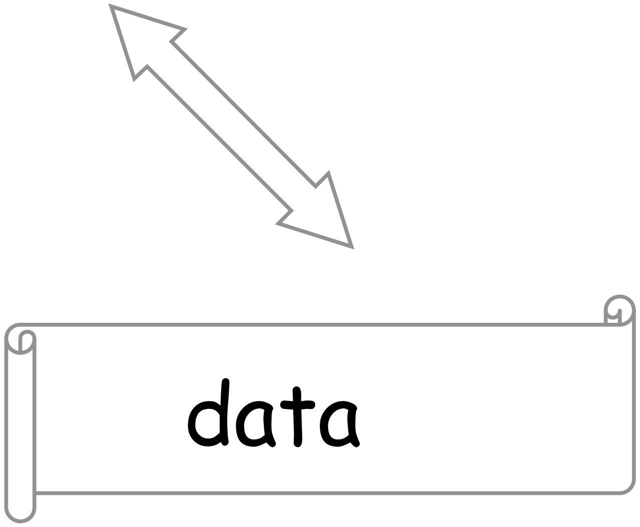


data

Before Turing…

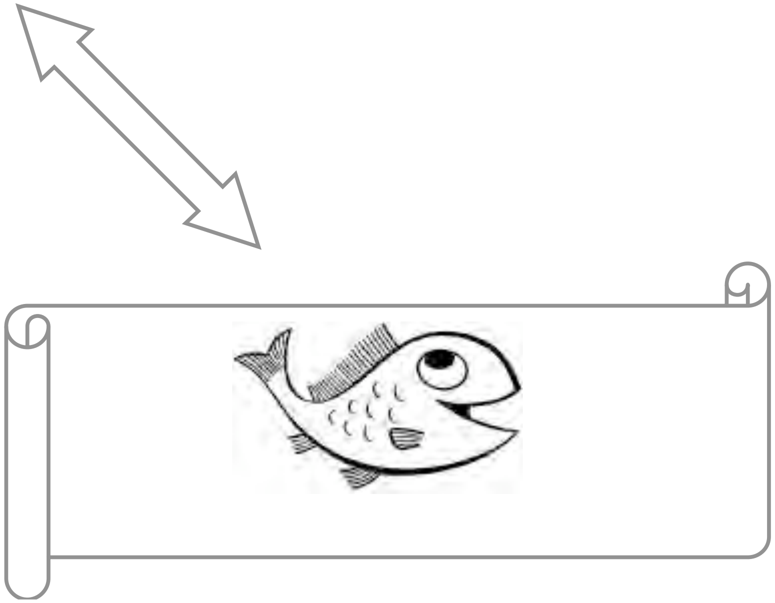
Courtesy IBM (www.ibm.com)

Part of one of Babbage's Difference Engines

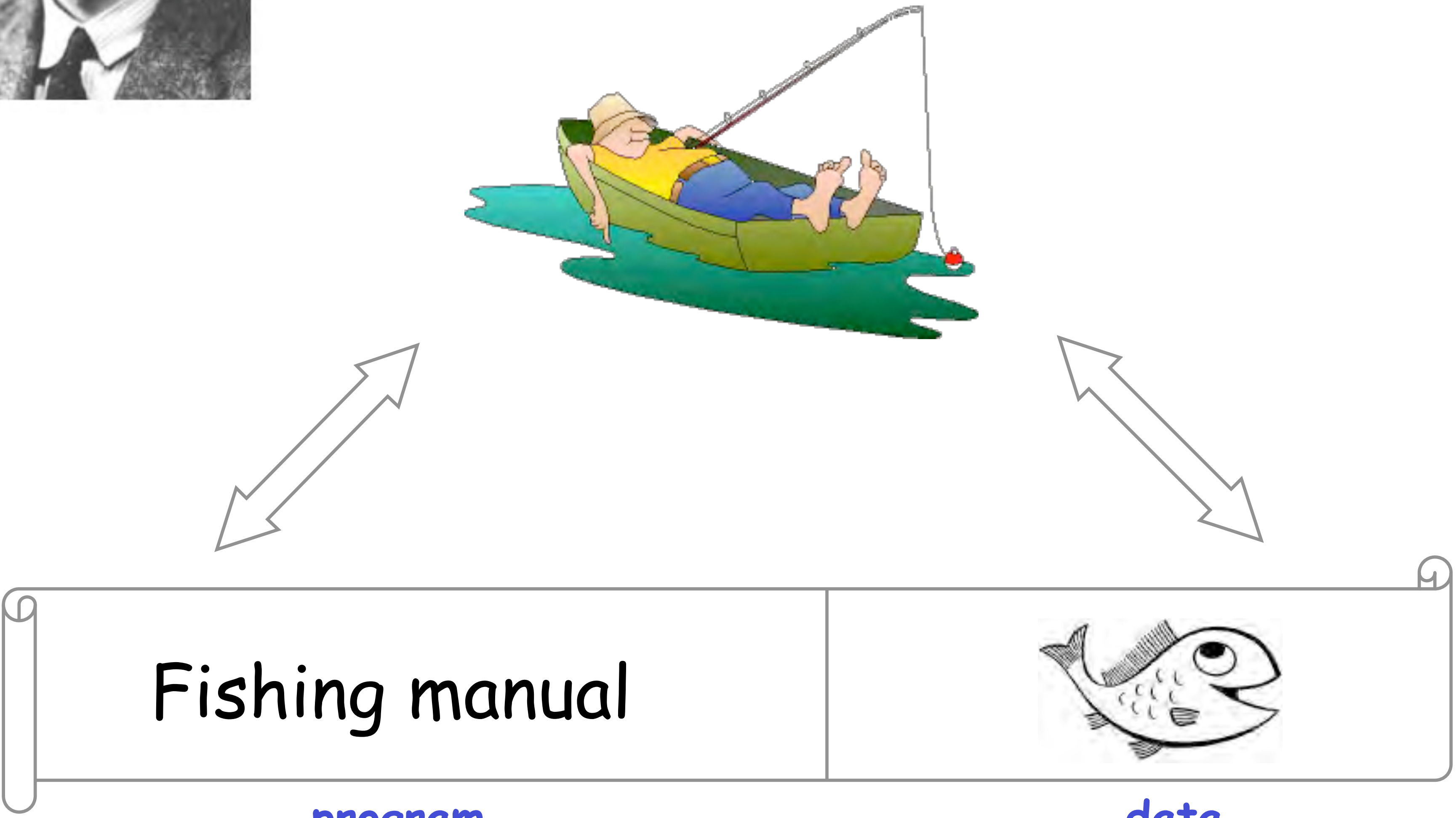


data

Fishing …



Fishing …



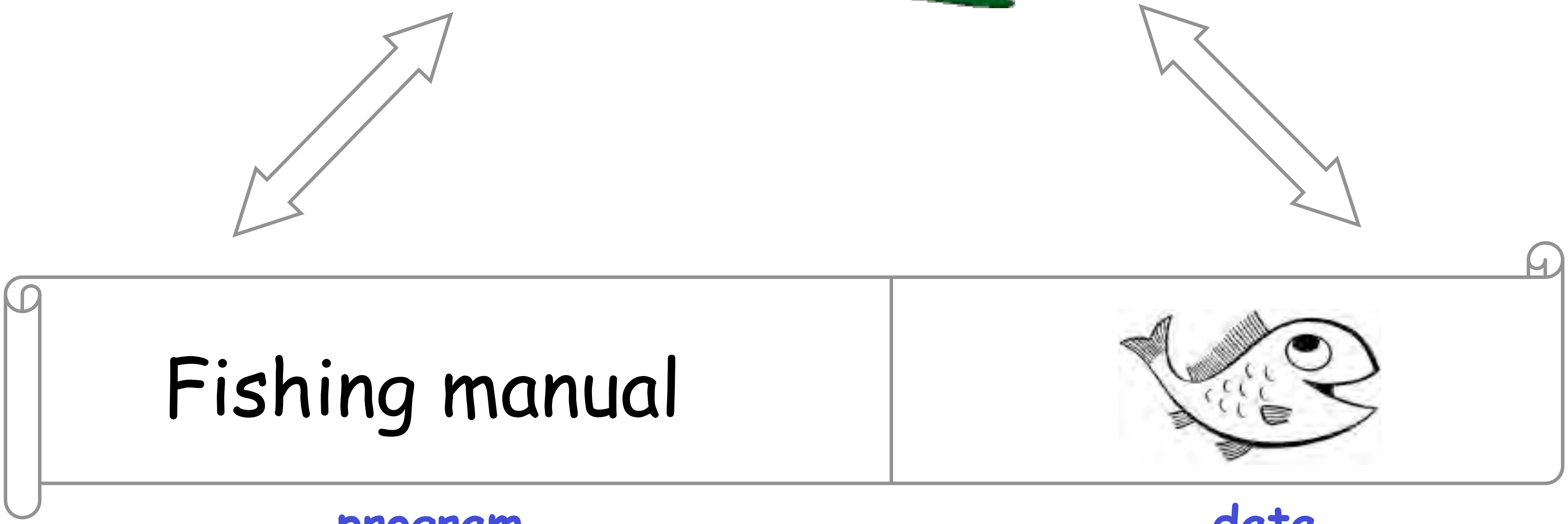
Fishing manual

program

data

Fishing …

Confucius

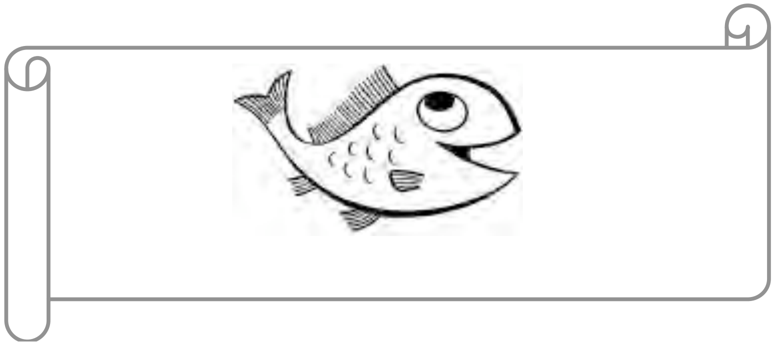


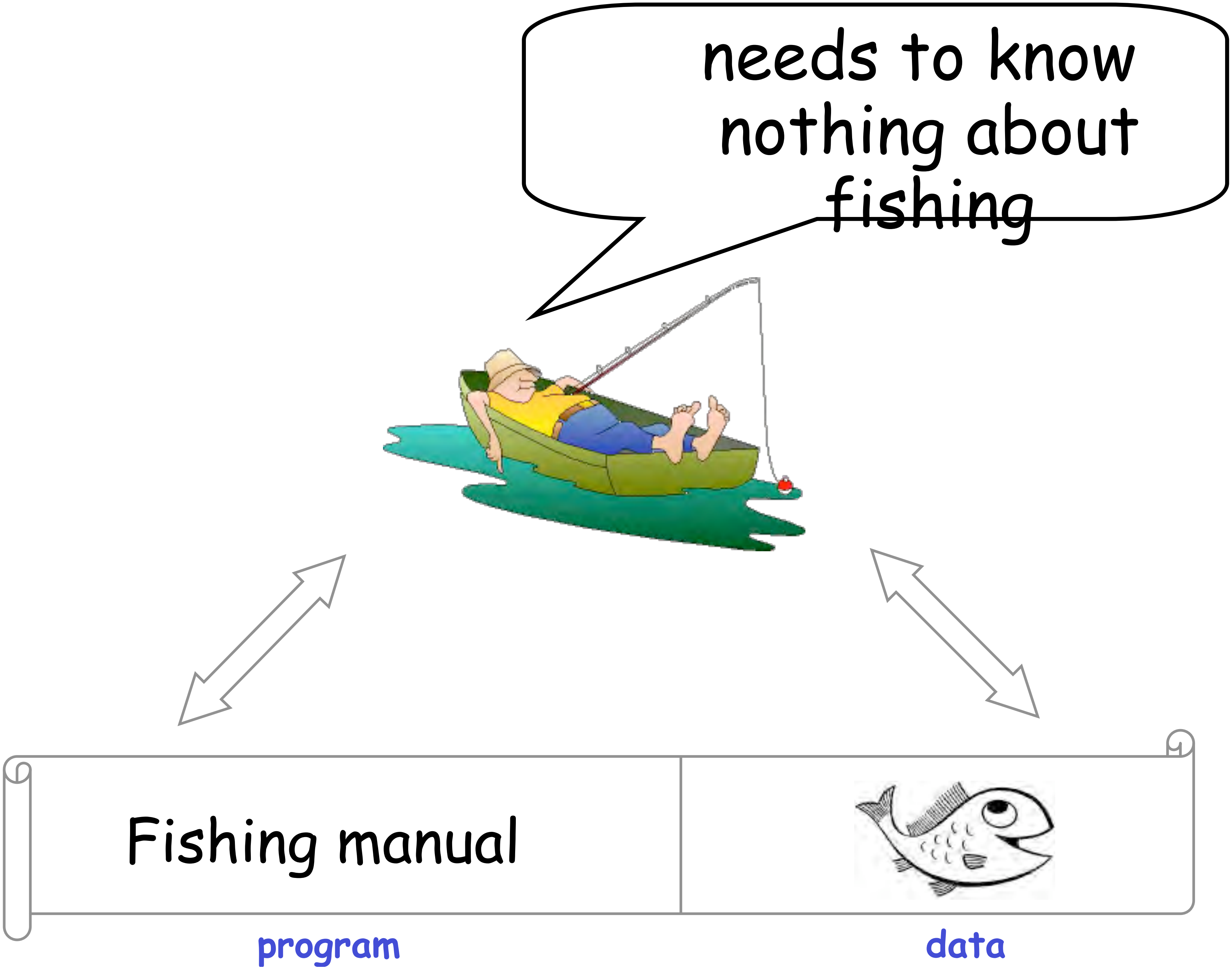
Fishing manual

program

data

needs to know how to fish



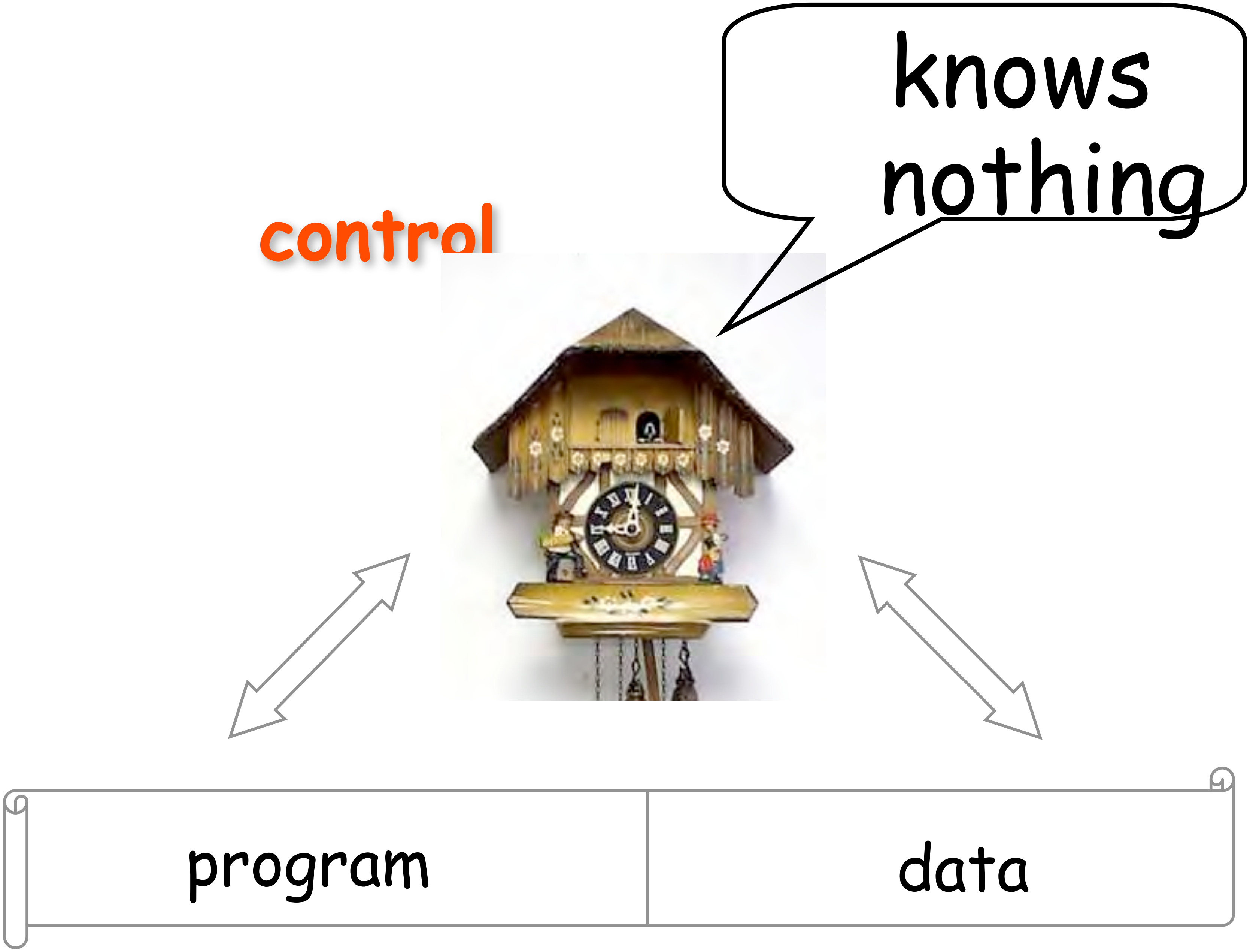


needs to know nothing about fishing

Fishing manual

program

data



control

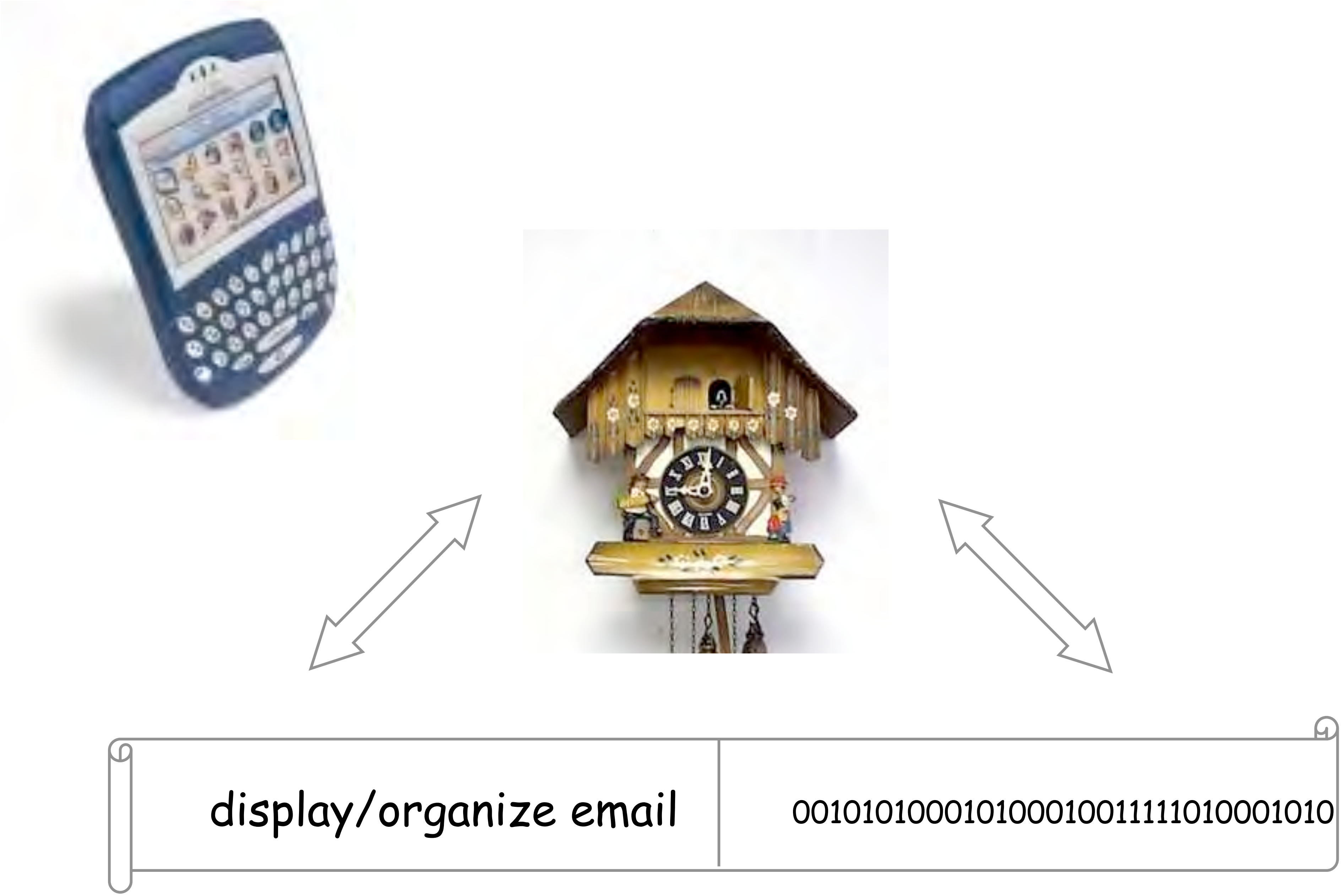
knows nothing

program

data

turn bits into sounds

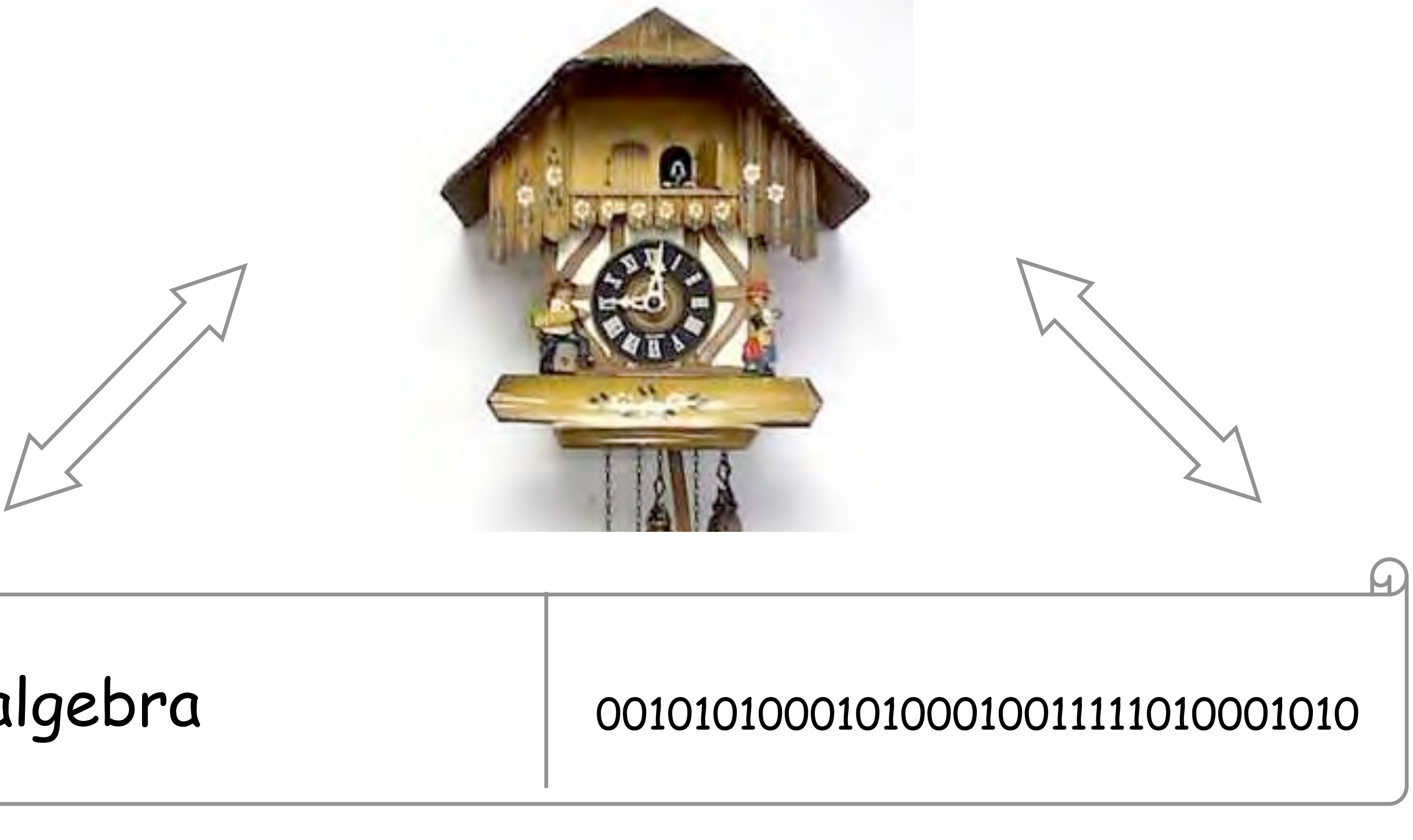
001010100010100010011111010001010



display/organize email

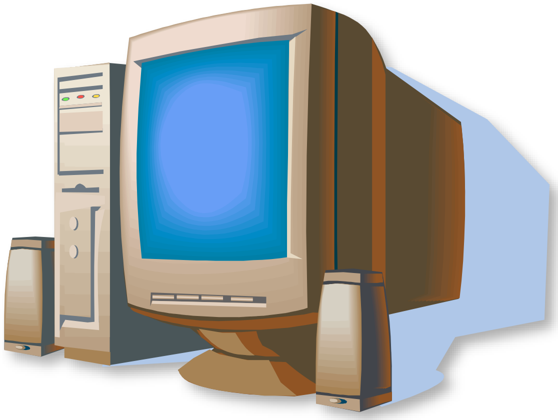
001010100010100010011111010001010

Earth simulator



algebra

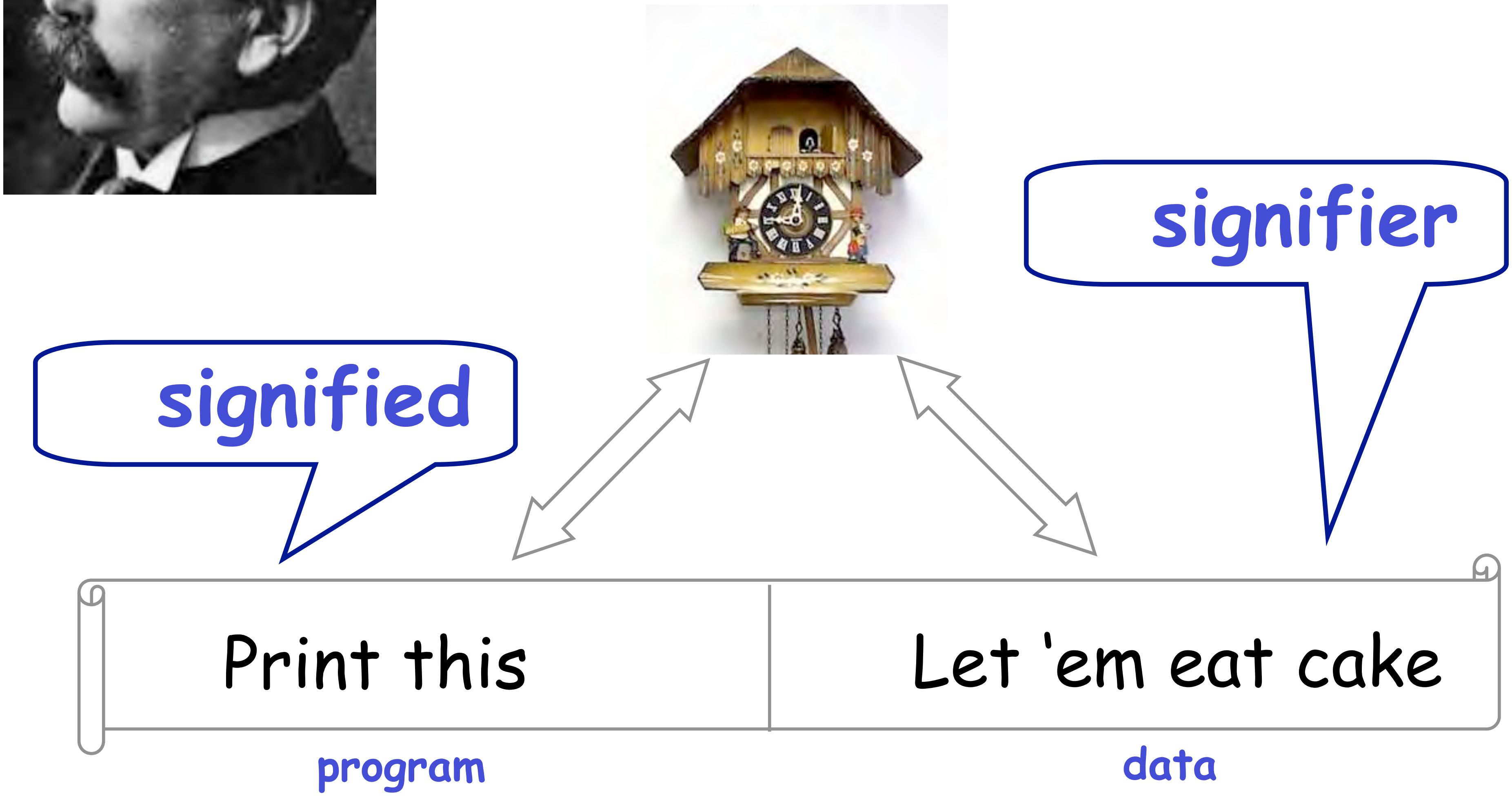
001010100010100010011111010001010



All the same !

Duality

Saussure
(1857-1913)



signified

signifier

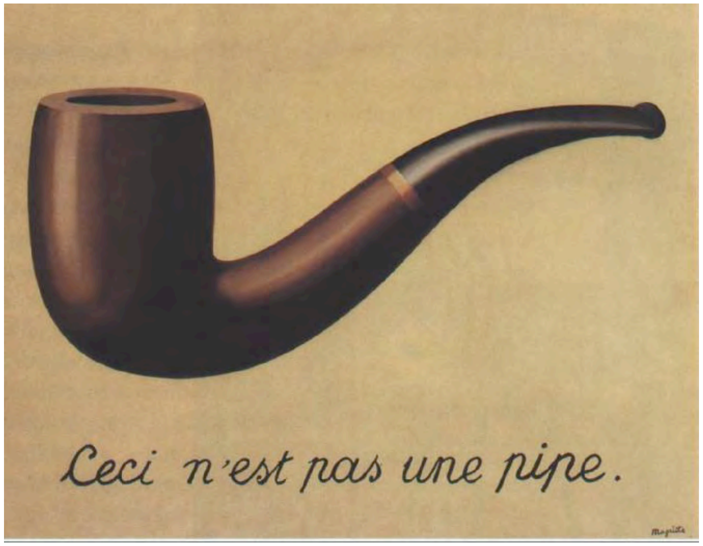
Print this

Let 'em eat cake

program

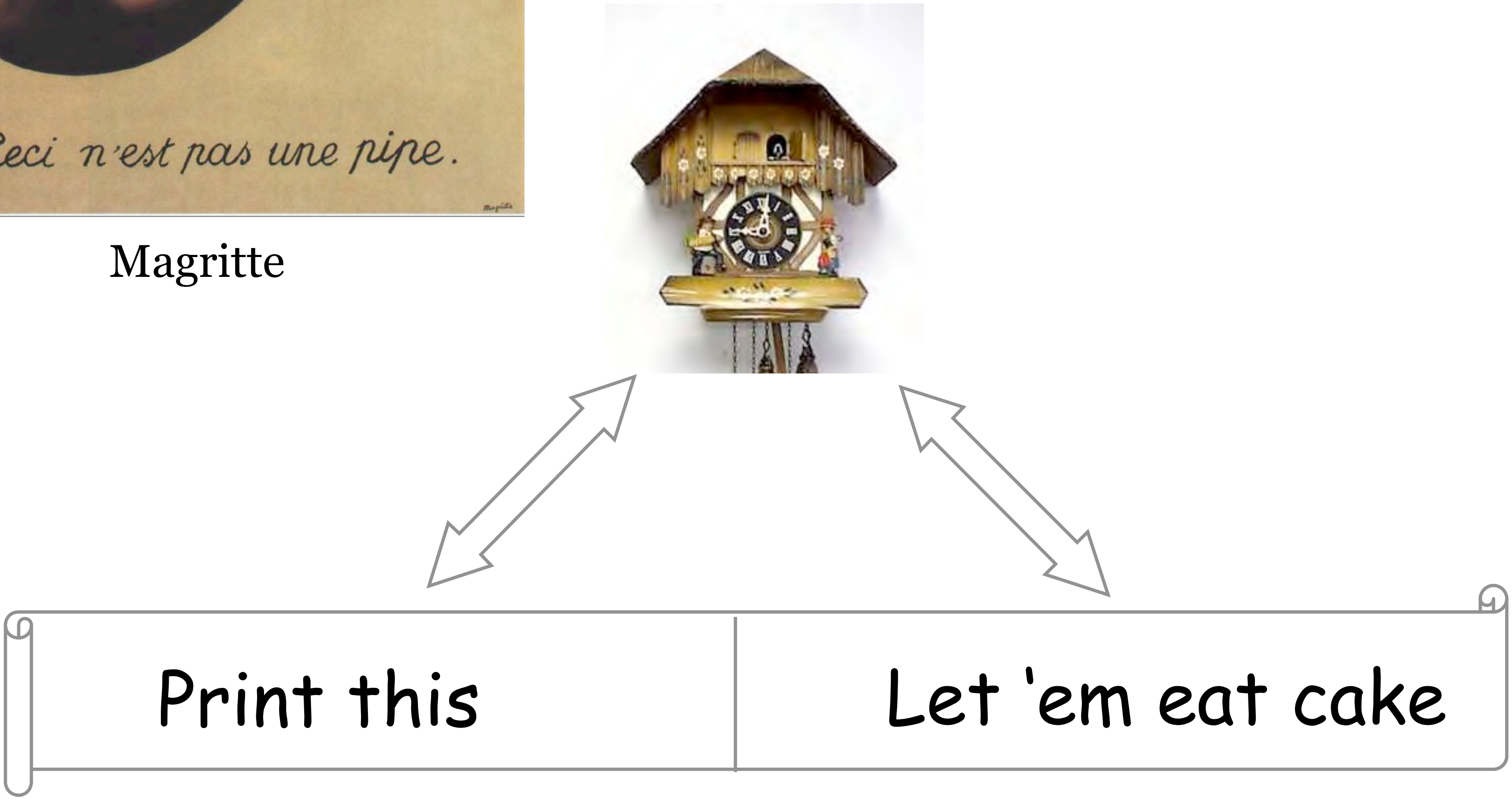
data

Let 'em eat cake



Magritte

This is not a pipe

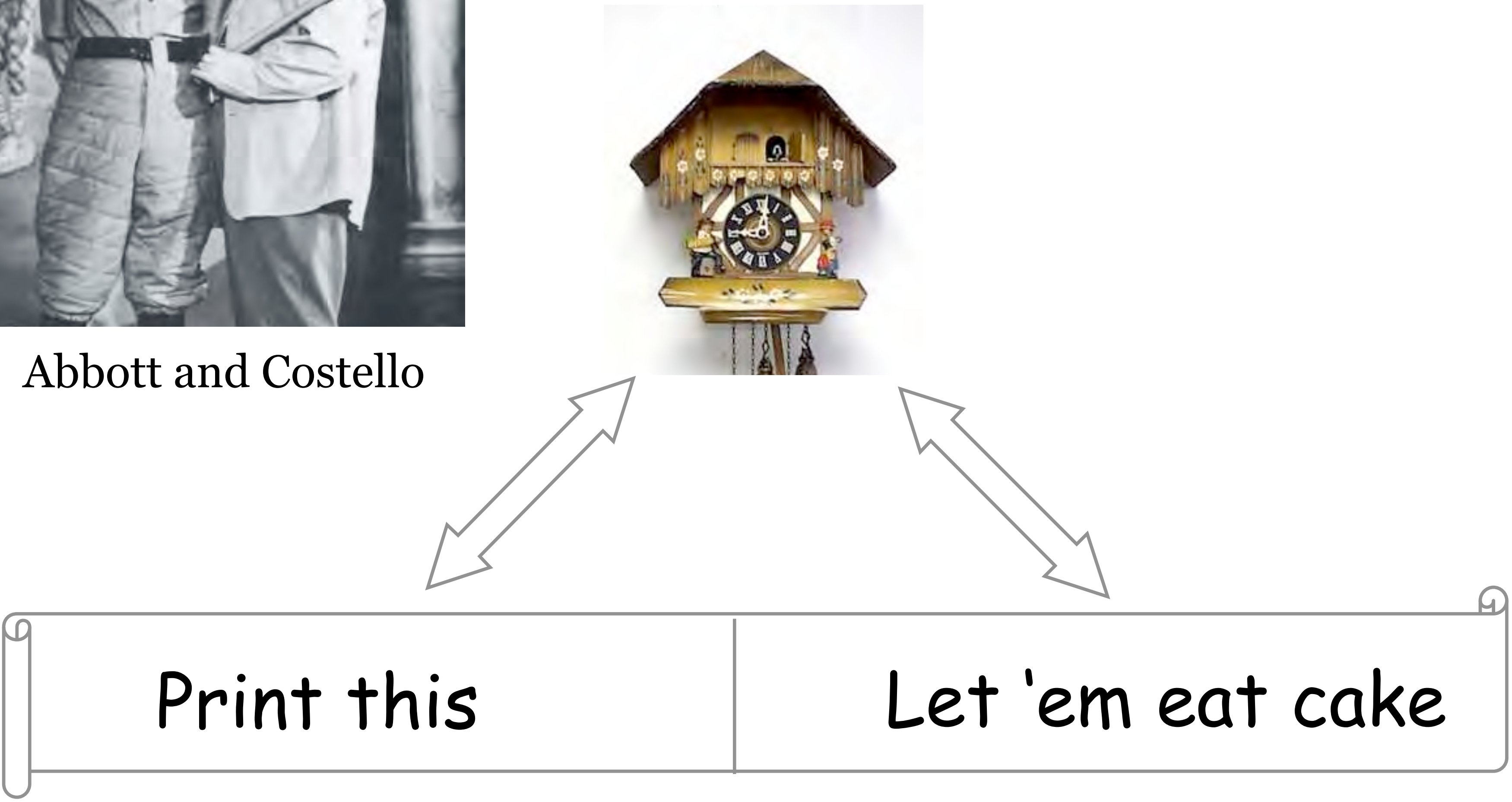


Print this

Let 'em eat cake

WHO'S ON FIRST ?

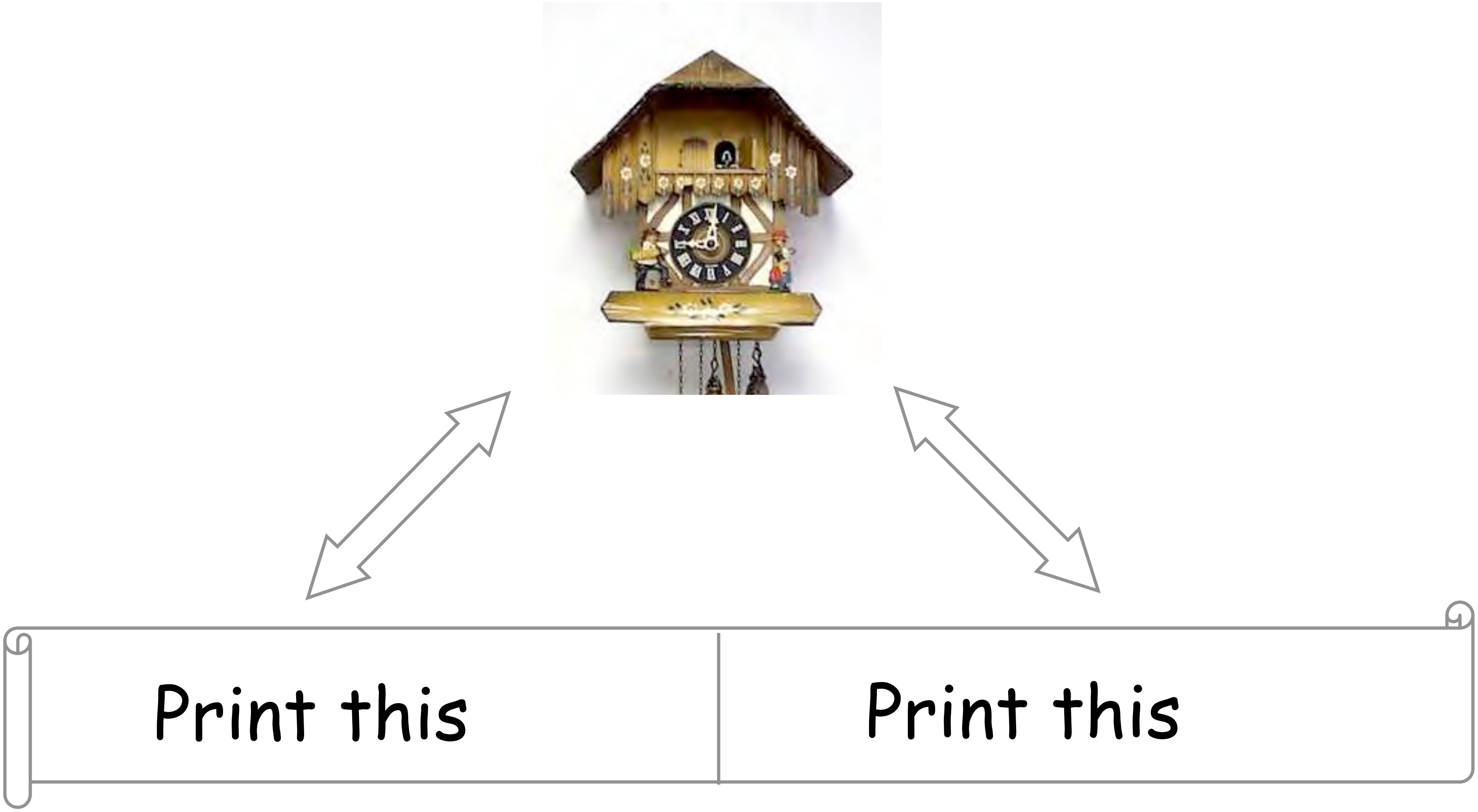
Abbott and Costello



Print this

Let 'em eat cake

Self-reference



Print this

Print this

Print this

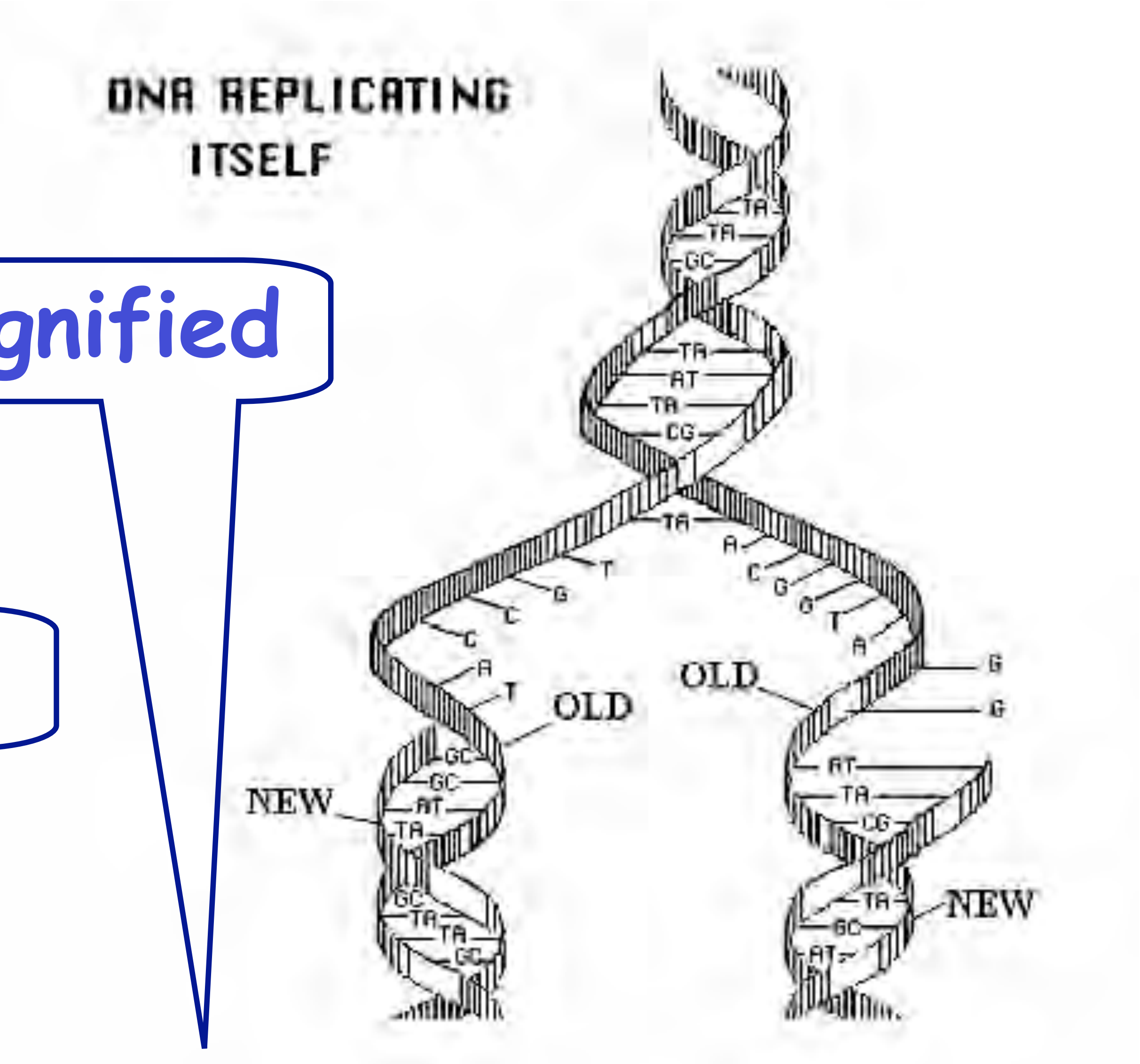
Virus !

Self-replication

Print this twice | Print this twice

Print this twice Print this twice

James Watson – Francis Crick, 1953



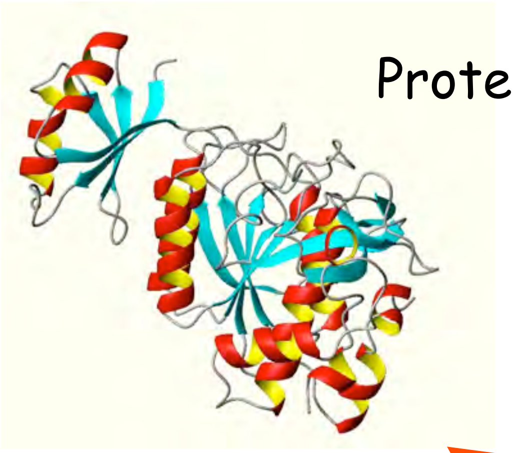
signified

signifier

Duality: gene/protein

Self-reference: base pairs

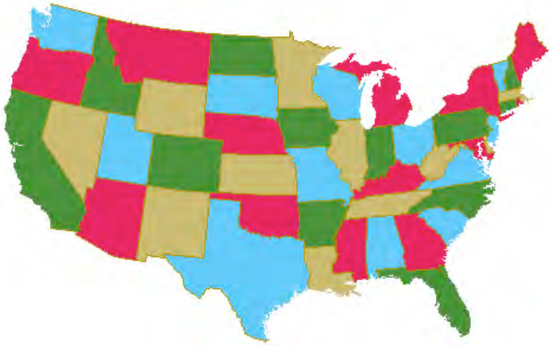
Tractability



Protein folding

Scheduling

all seem intractable

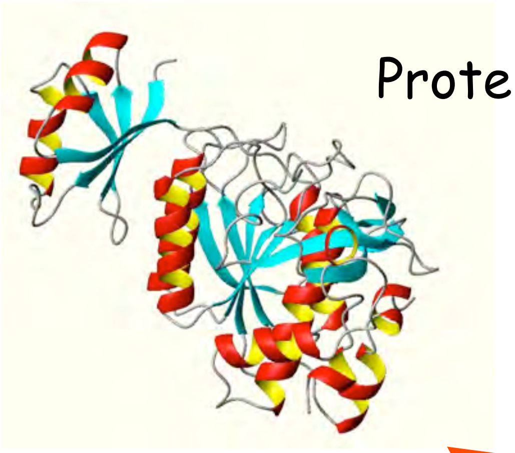


Map coloring

Andrew **Wiles**

Theorem proving

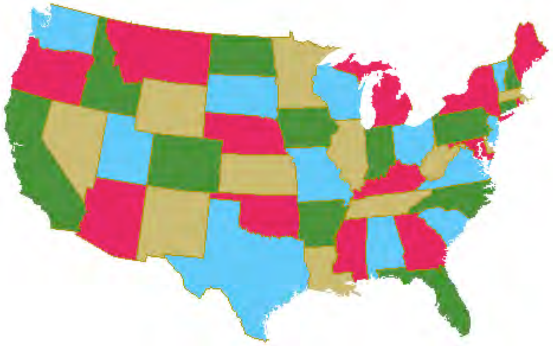
Traveling salesman



Protein folding

Scheduling

equivalent

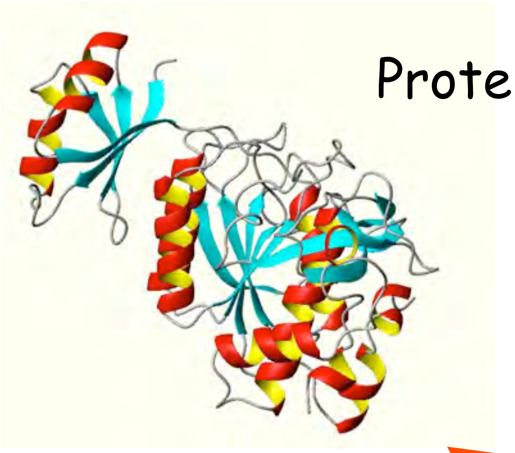


Map coloring

Andrew Wiles

Theorem proving

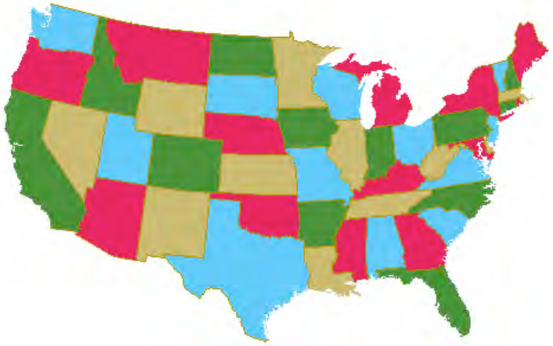
Traveling salesman



Protein folding

E-commerce
security

intractable ?



Map coloring

Andrew *Wiles*

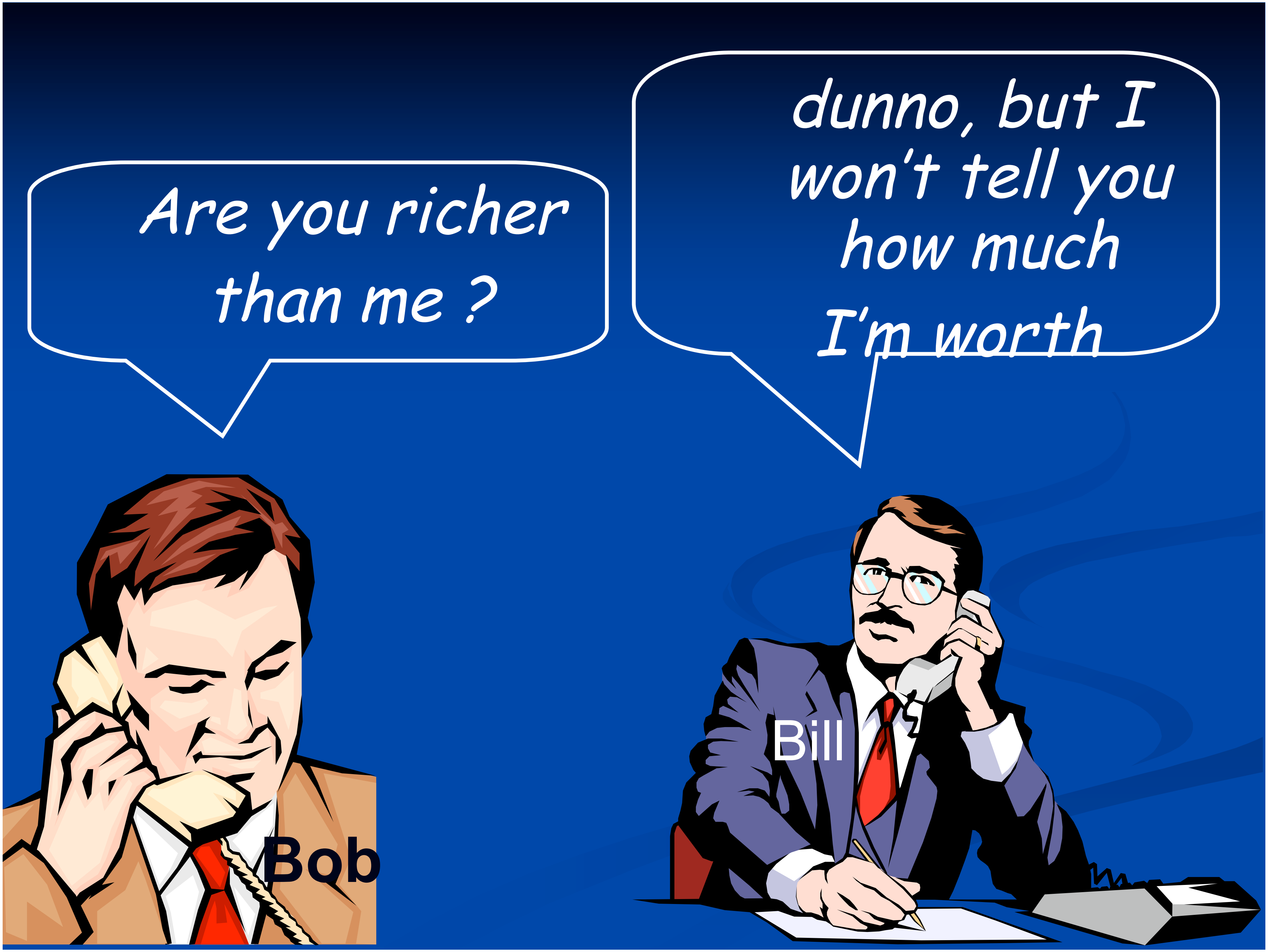
Theorem proving

Traveling salesman

Two Amazing Consequences of Intractability

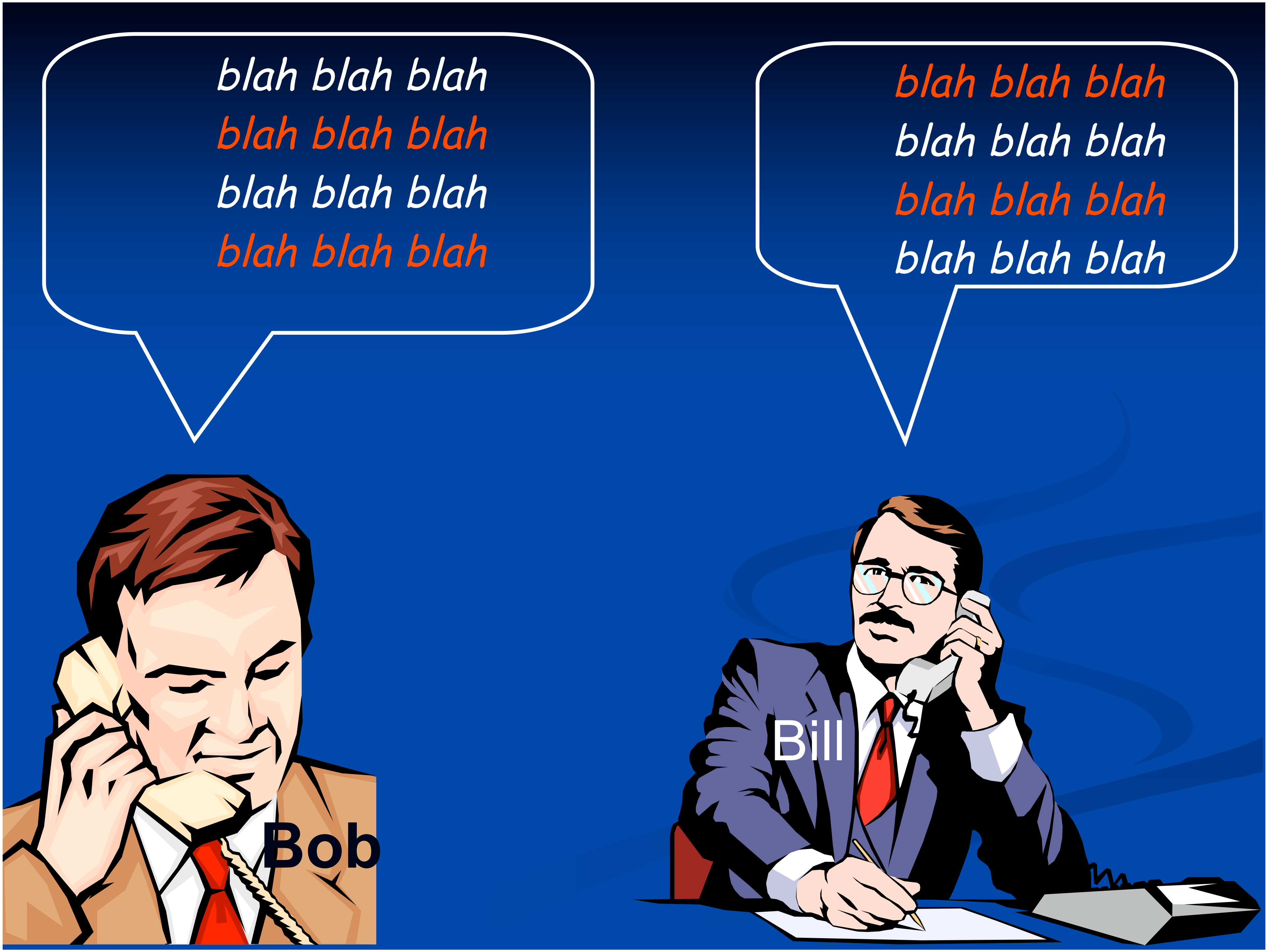
- Zero Knowledge
- Probabilistically Checkable Proofs

Zero Knowledge

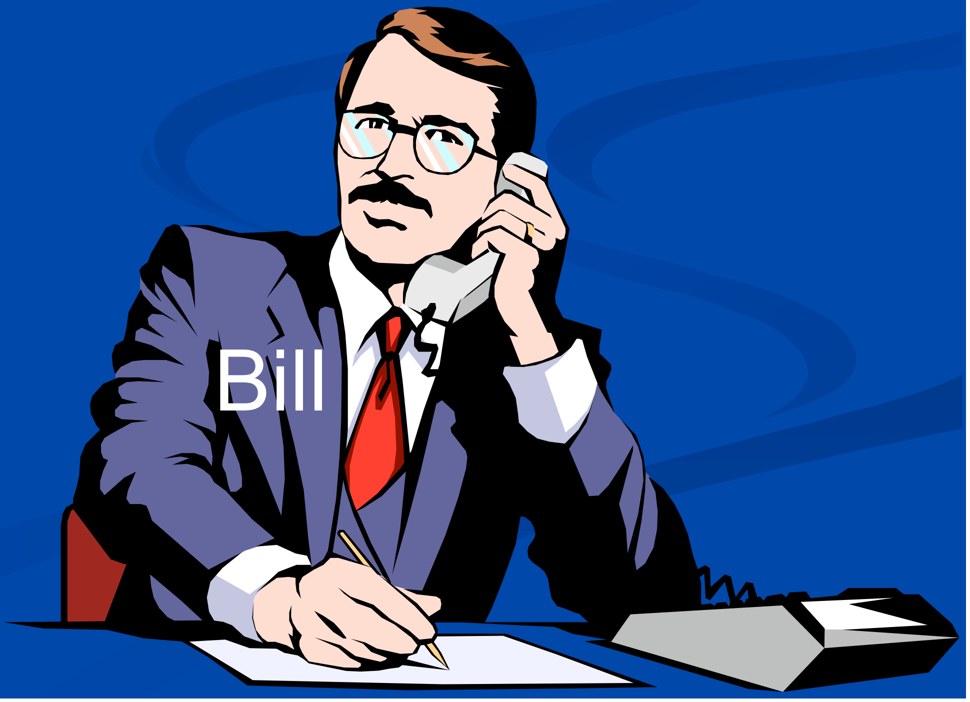

Are you richer than me ?
dunno, but I won't tell you how much I'm worth
Bob
Bill

So, who's richer ?
I won't tell you either
Bob
Bill

There exists a dialogue…

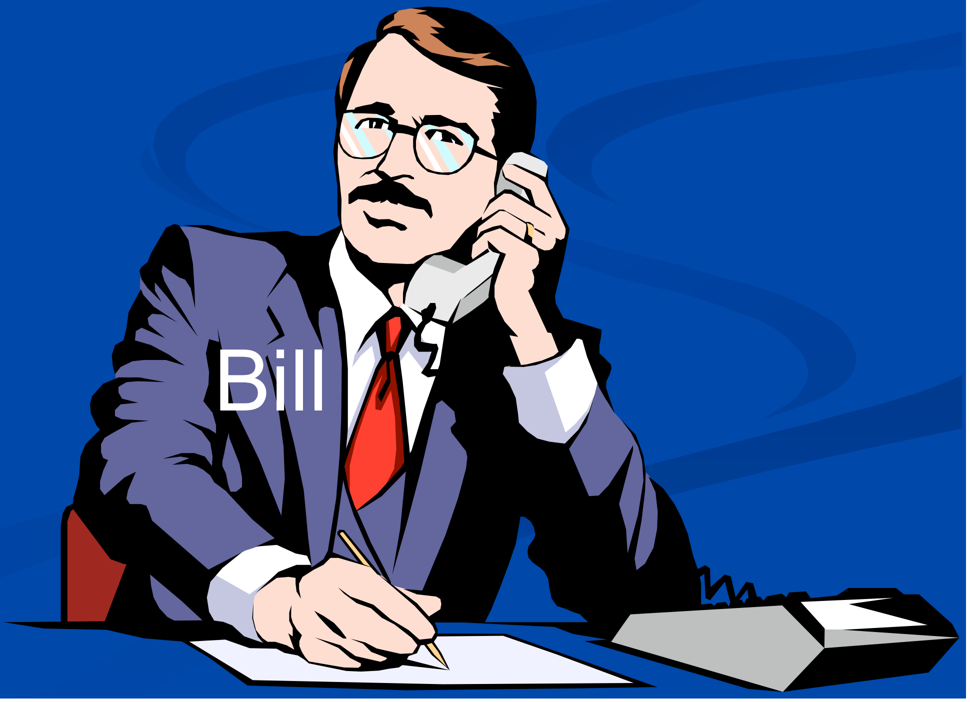

blah blah blah
blah blah blah
blah blah blah
blah blah blah
blah blah blah
blah blah blah
blah blah blah
blah blah blah
Bob
Bill

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

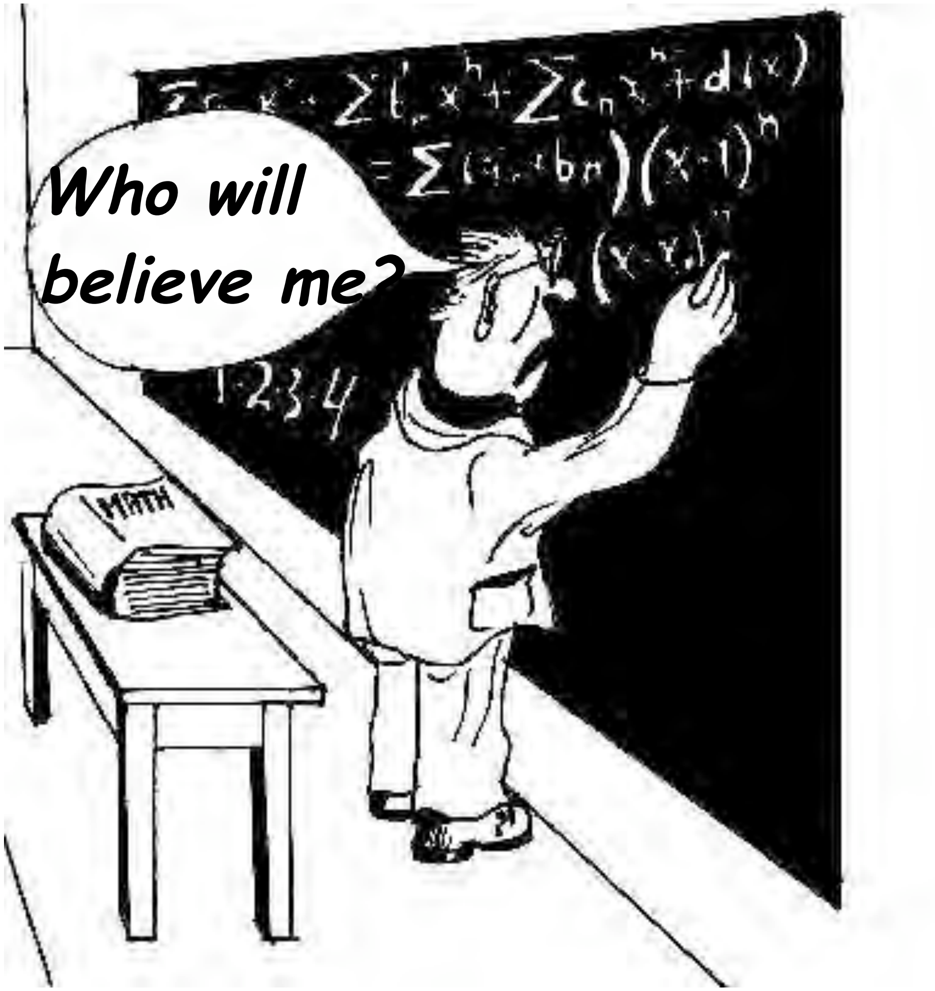
I have no nukes !

Prove it!

1. No UN inspections

2. Both parties try to cheat

PCP



Step 1 write proof in special format

Step 2 verifier picks 5 random words

My Proof of Riemann’s Hypothesis

It is straightforward to check that this is a map of $\mathcal{O}$-modules. To check the injectivity of φ suppose that $\varphi_\alpha(\mathfrak{p}_{\mathcal{D}}) = 0$. Then φ_α factors through $R_{\mathcal{D}}/\mathfrak{p}_{\mathcal{D}} \simeq \mathcal{O}$ and being an $\mathcal{O}$-algebra homomorphism this determines φ_α. Thus $[\rho_{f,\lambda}] = [\rho_\alpha]$. If $A^{-1}\rho_\alpha A = \rho_{f,\lambda}$ then $A \bmod \varepsilon$ is seen to be central by Schur's lemma and so may be taken to be I. A simple calculation now shows that α is a coboundary.

To see that φ is surjective choose

$$\Psi \in \mathrm{Hom}_{\mathcal{O}}(\mathfrak{p}_{\mathcal{D}}/\mathfrak{p}_{\mathcal{D}}^2, \mathcal{O}/\lambda^n).$$

Then ρ_Ψ: $\mathrm{Gal}(\mathbf{Q}_\Sigma/\mathbf{Q}) \to \mathrm{GL}_2(R_{\mathcal{D}}/(\mathfrak{p}_{\mathcal{D}}^2, \ker\Psi))$ is induced by a representative of the universal deformation (chosen to equal $\rho_{f,\lambda}$ when reduced mod $\mathfrak{p}_{\mathcal{D}}$) and we define a map $\alpha_\Psi : \mathrm{Gal}(\mathbf{Q}_\Sigma/\mathbf{Q}) \to V_{\lambda^n}$ by

$$\alpha_\Psi(g) = \rho_\Psi(g)\rho_{f,\lambda}(g)^{-1} \in \left\{ \begin{pmatrix} 1 + \mathfrak{p}_{\mathcal{D}}/(\mathfrak{p}_{\mathcal{D}}^2, \ker\Psi) & \mathfrak{p}_{\mathcal{D}}/(\mathfrak{p}_{\mathcal{D}}^2, \ker\Psi) \\ \mathfrak{p}_{\mathcal{D}}/(\mathfrak{p}_{\mathcal{D}}^2, \ker\Psi) & 1 + \mathfrak{p}_{\mathcal{D}}/(\mathfrak{p}_{\mathcal{D}}^2, \ker\Psi) \end{pmatrix} \right\} \subseteq V_{\lambda^n}$$

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

$$\begin{array}{ccccc} \mathfrak{p}_{\mathcal{D}}/(\mathfrak{p}_{\mathcal{D}}^2, \ker\Psi) & \overset{\Psi}{\hookrightarrow} & \mathcal{O}/\lambda^n & \xrightarrow{\sim} & (\mathcal{O}/\lambda^n)\cdot\varepsilon \\ & & 1 & \mapsto & \varepsilon. \end{array}$$

Then α_Ψ is readily seen to be a continuous cocycle whose cohomology class lies in $H^1_{\mathrm{Se}}(\mathbf{Q}_\Sigma/\mathbf{Q}, V_{\lambda^n})$. 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

Everything looks fine.

I ACCEPT !

Verifier is correct with probability 0.9999999

Verifier

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

Everything looks fine.

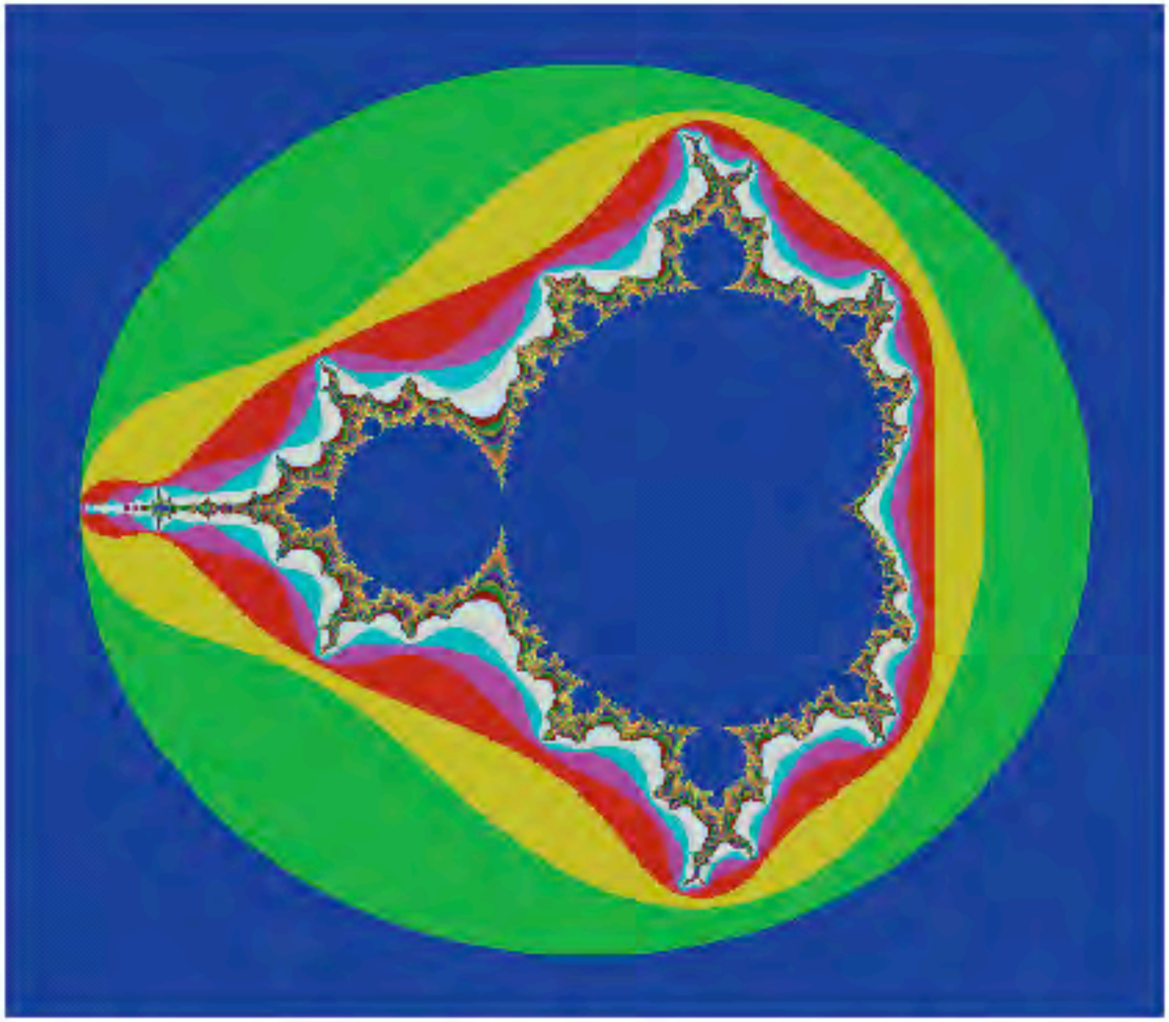
I ACCEPT !

Verifier

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

The Algorithm

Very little does a lot



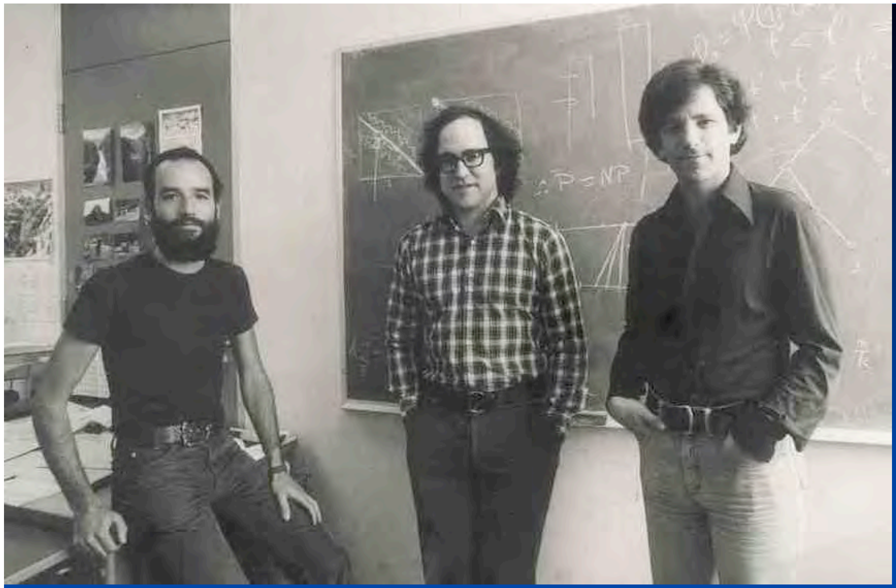
Mandelbrot Set (40 lines of code)

$$\begin{array}{r} 32 \\ \times\ 17 \\ \hline 224 \\ 32 \\ \hline =\ 544 \end{array}$$

grade school

FFT

signal processing



RSA

encryption

e-commerce

PageRank

web search

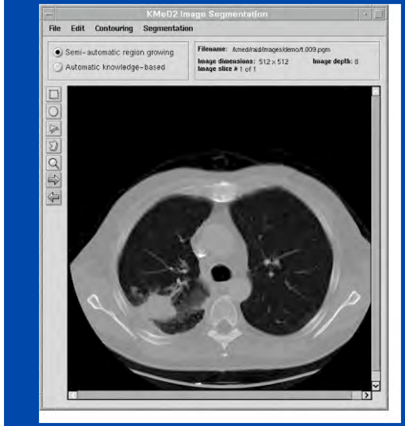
Google

10 petabytes
(~1MG)

Sloan Digital
Sky Survey

10 petabytes/yr

Biomedical imaging



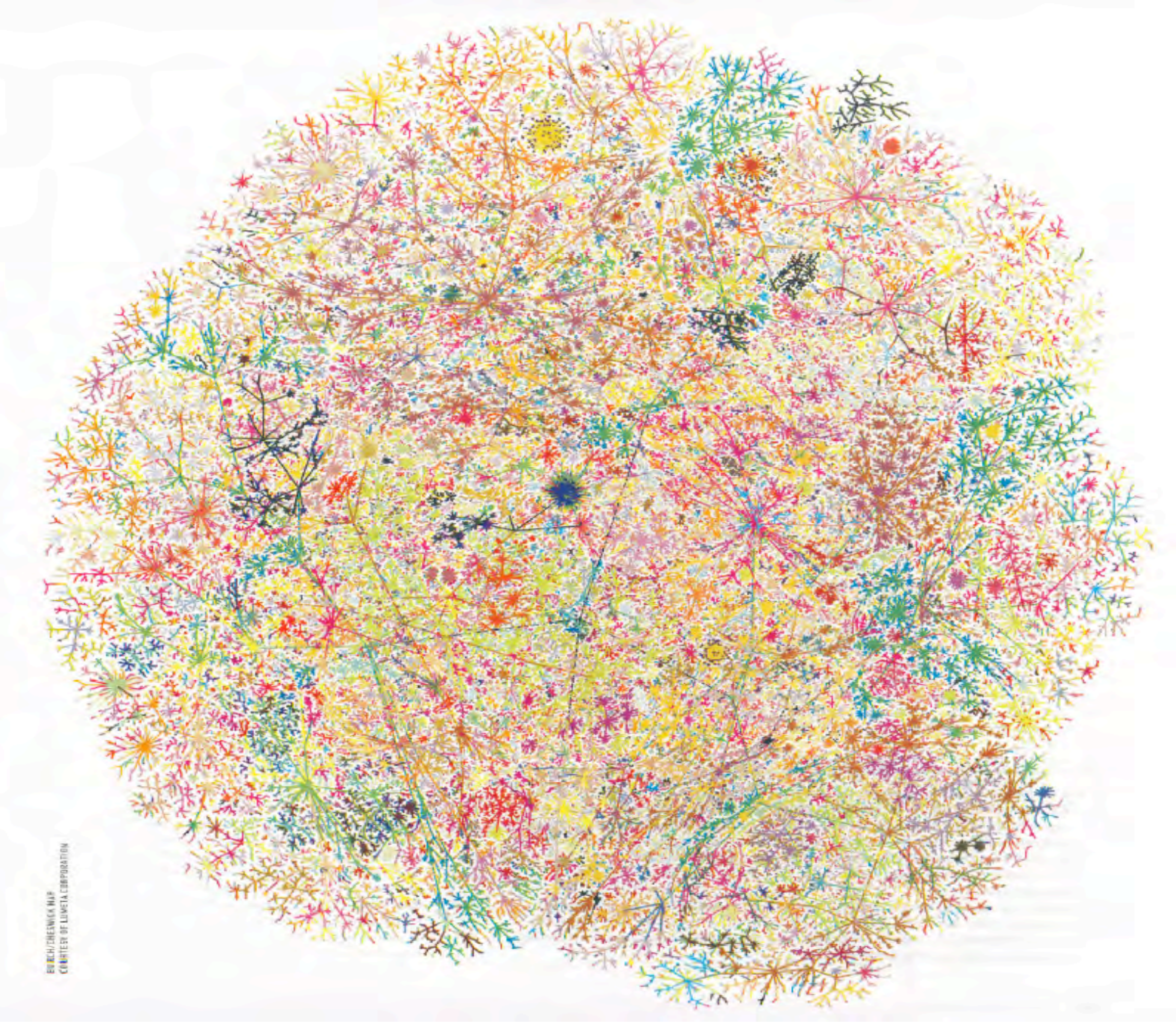
● Semi-automatic region growing
○ Automatic knowledge-based

Filename: /kmed/raid/images/demo/t.009.pgm
Image dimensions: 512 × 512
Image depth: 8
Image slice # 1 of 1

150 petabytes/yr

10,000 times the
Library of Congress

protein-protein interaction networks



BURCH/CHESWICK MAP
COURTESY OF LUMETA CORPORATION

Sciences of The Formula

math, physics, chemistry

$$\oint H \cdot dl = I + \varepsilon \frac{d}{dt}\iint E \cdot ds$$

Ampere's Law

$$\oint E \cdot dl = -\mu \frac{d}{dt}\iint H \cdot ds$$

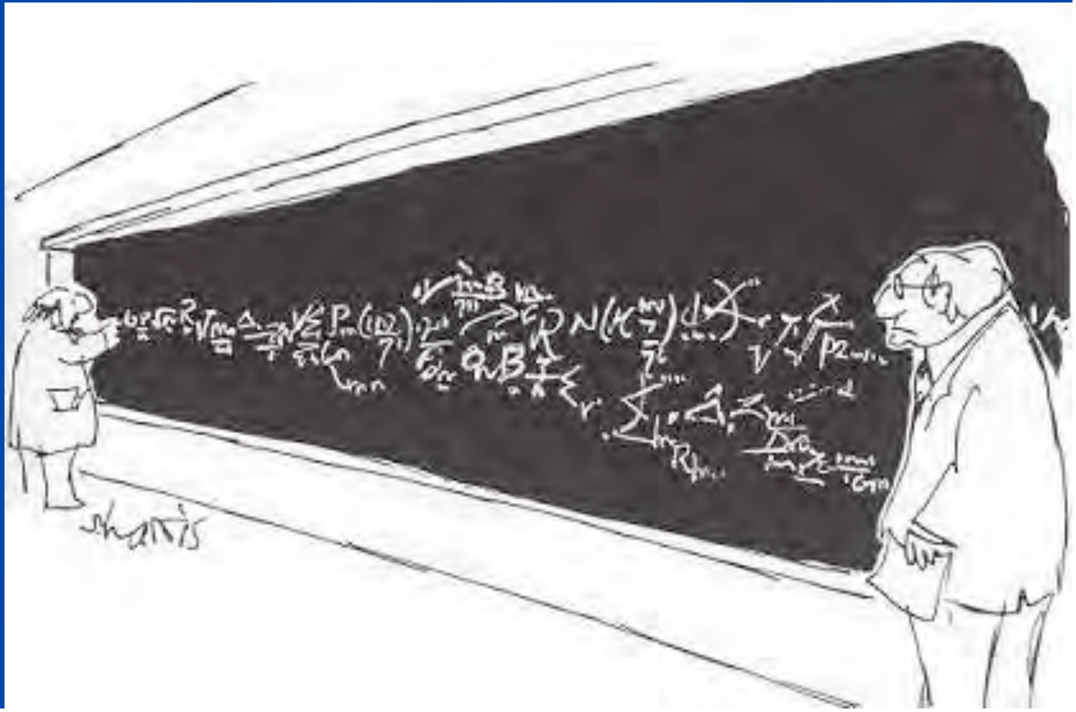
Faraday's Law

$$\varepsilon \oiint E \cdot ds = \iiint q_v dv$$

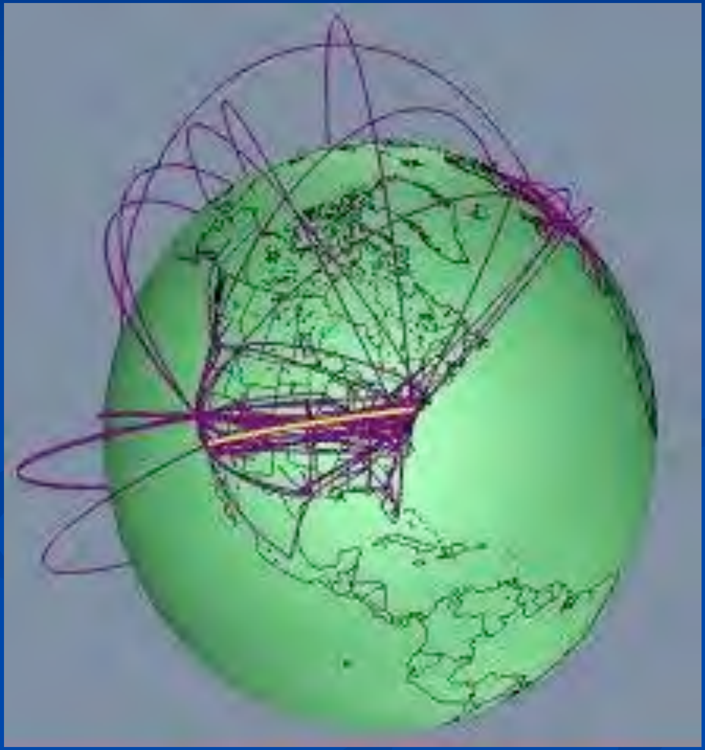
Gauss' Law

$$\mu \oiint H \cdot ds = 0$$

The Fourth Equation



Sciences of The Algorithm



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 !