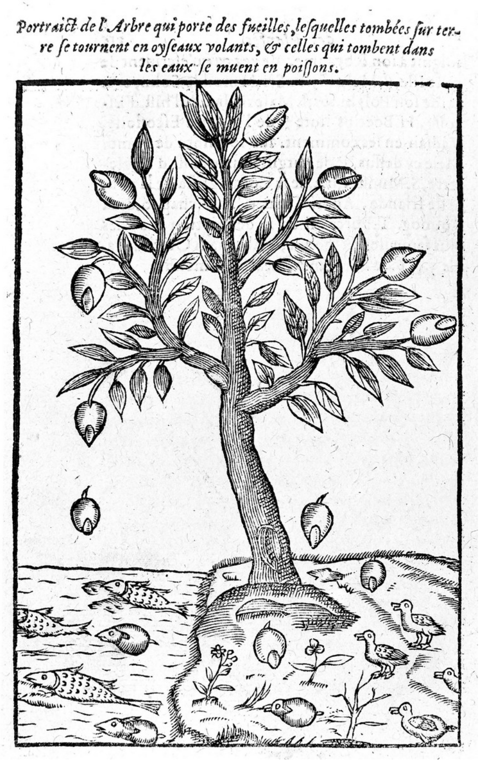
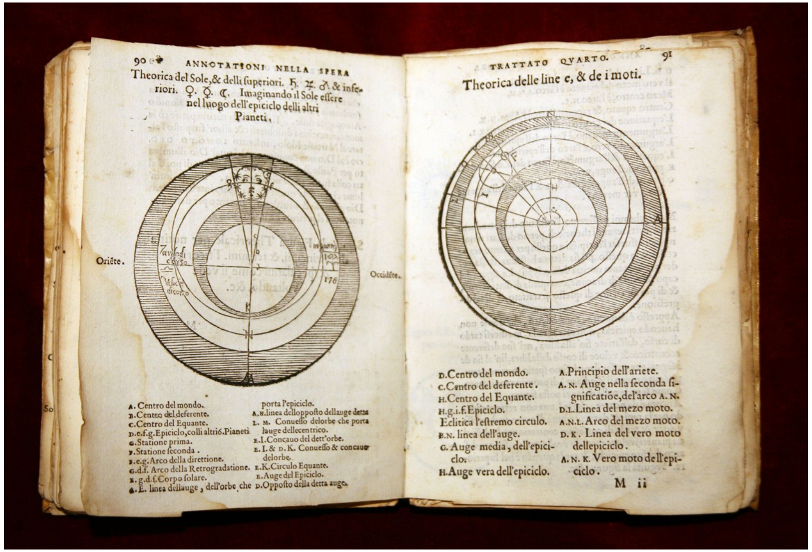
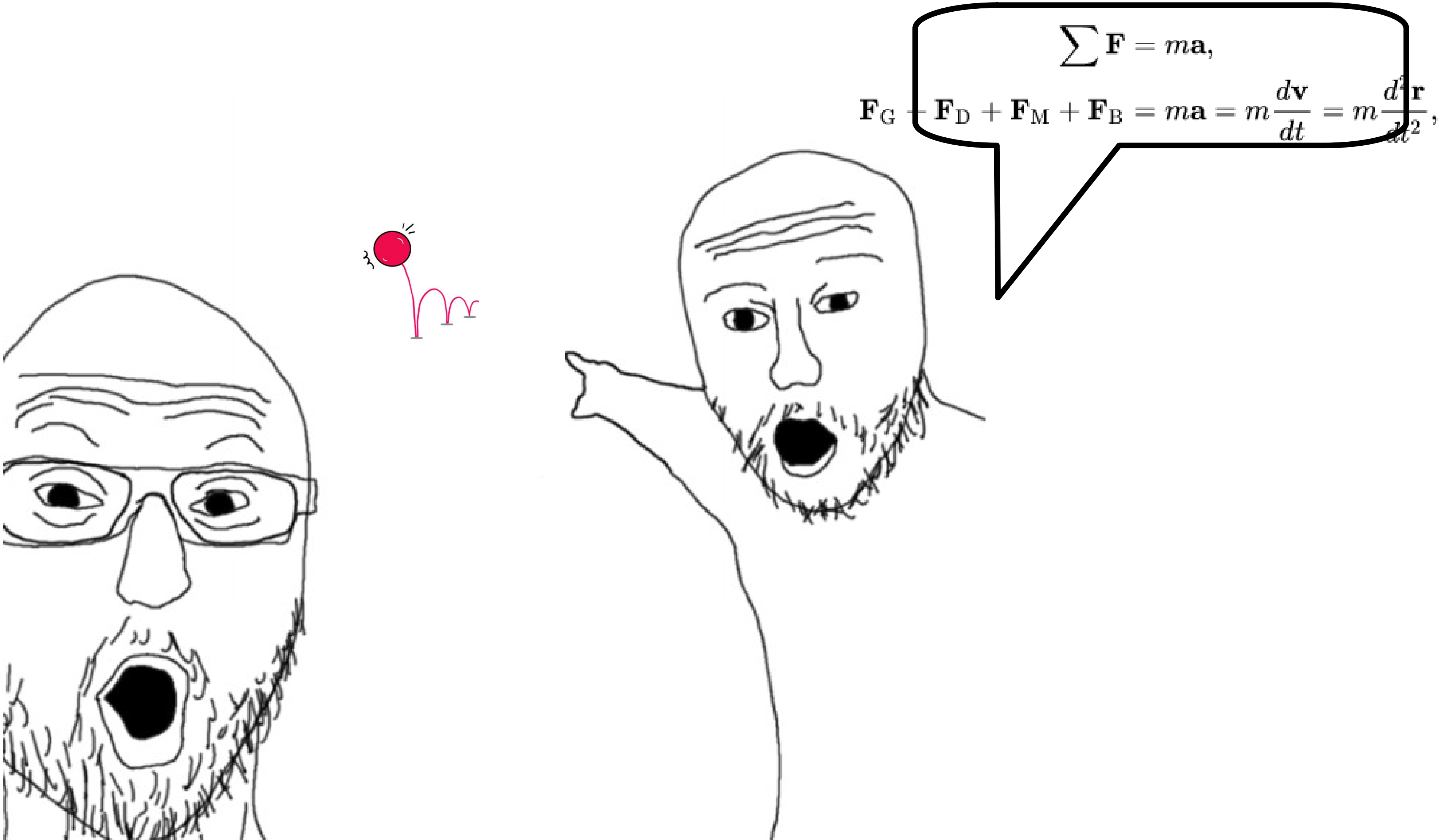
# Why is Computer Science a Science?

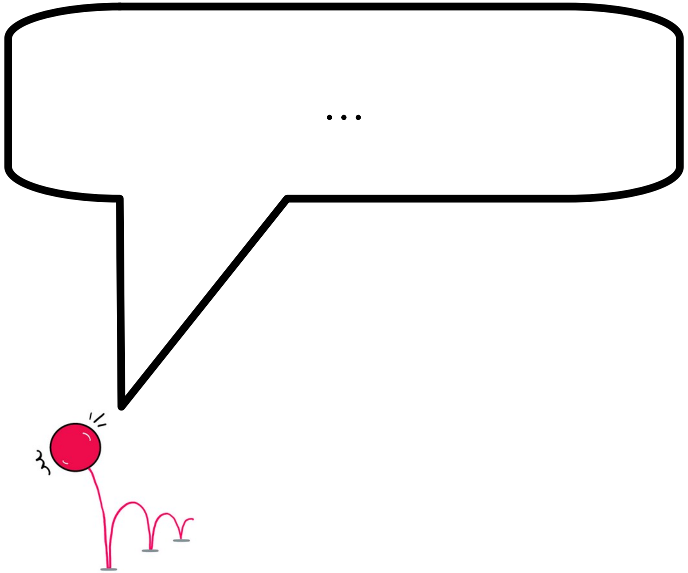
Abrahim Ladha

# Prescientific Thought




$$\sum \mathbf{F} = m\mathbf{a},$$
$$\mathbf{F}_{\mathrm{G}} + \mathbf{F}_{\mathrm{D}} + \mathbf{F}_{\mathrm{M}} + \mathbf{F}_{\mathrm{B}} = m\mathbf{a} = m\frac{d\mathbf{v}}{dt} = m\frac{d^2\mathbf{r}}{dt^2},$$



# Scientific Method

- A good scientific theory should:
- Explain all past observations
- Be used to predict future observations

Reprinted from *Communications in Pure and Applied Mathematics*, Vol. 13, No. I (February 1960). New York:
John Wiley & Sons, Inc. 

# THE UNREASONABLE EFFECTIVENSS OF MATHEMATICS IN THE NATURAL SCIENCES

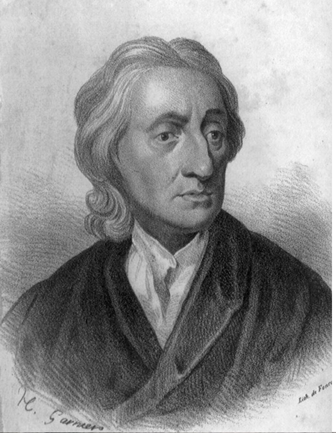
**Eugene Wigner**

- More observations can change and refine the theory
- But the theory can also predict observations
- Historically, the second has happened more

- Scientific and Mathematical Methods have had huge success in the study of materiality
- What about the immaterial?

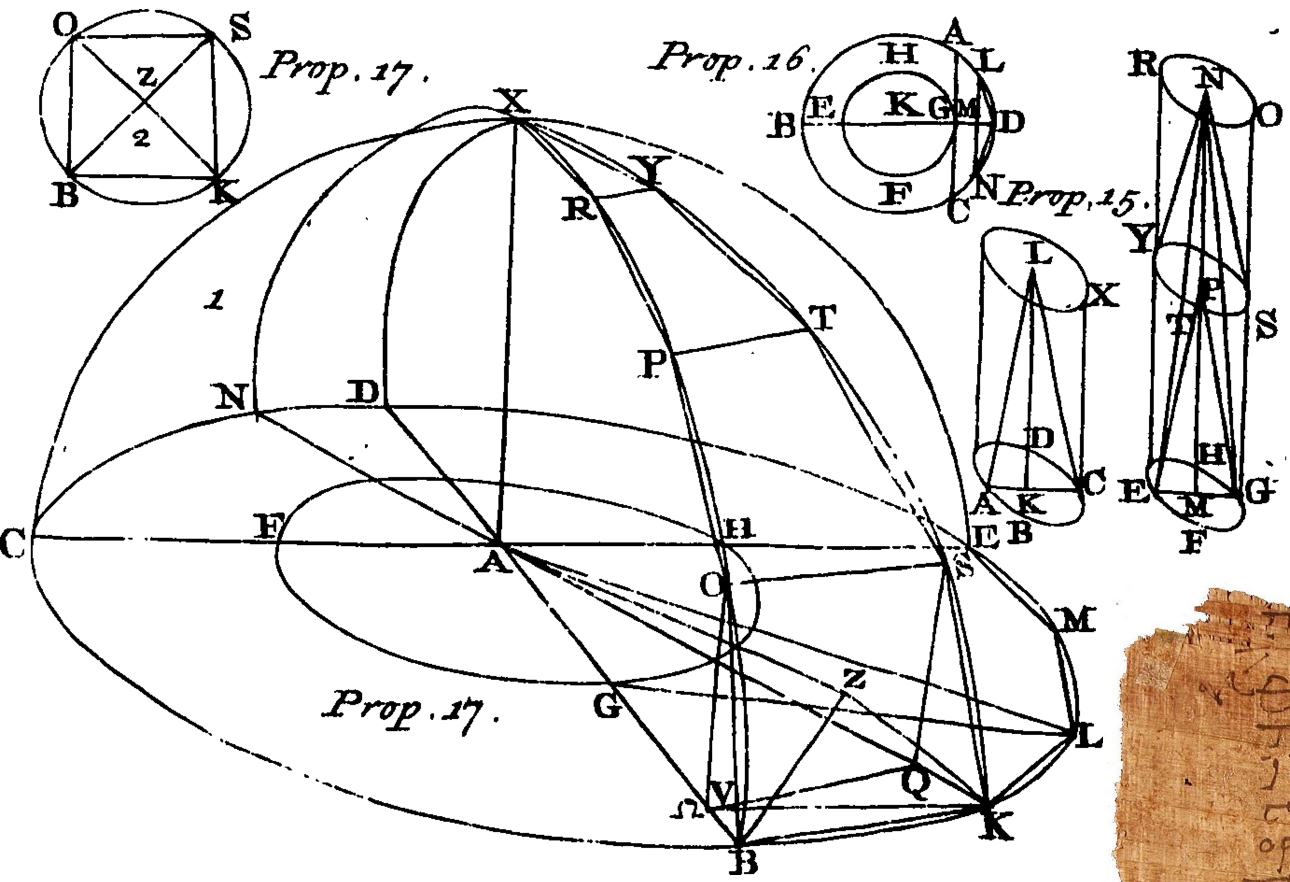
# A Few examples

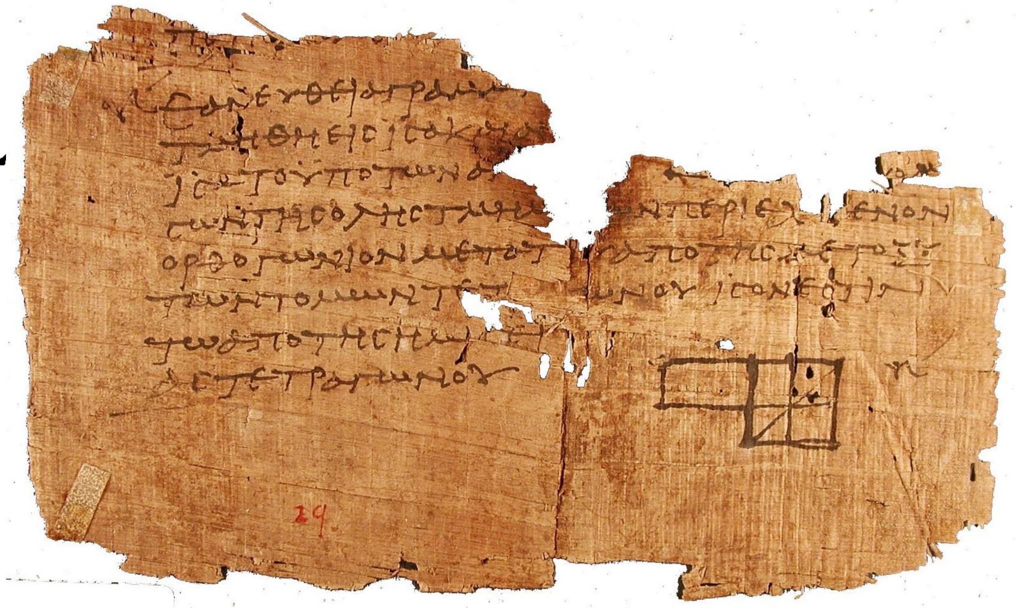
- Truth and Proof
- Computation
- Intelligence
- Knowledge
- Prediction
- Randomness vs Pseudorandomness

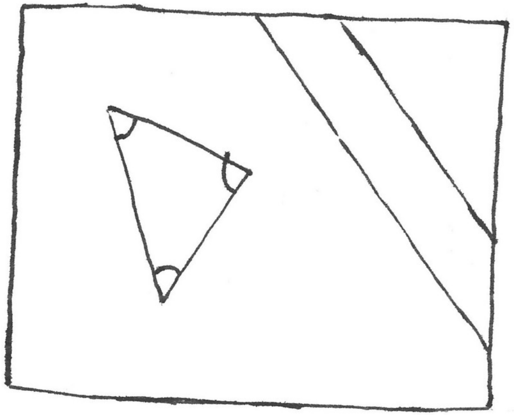


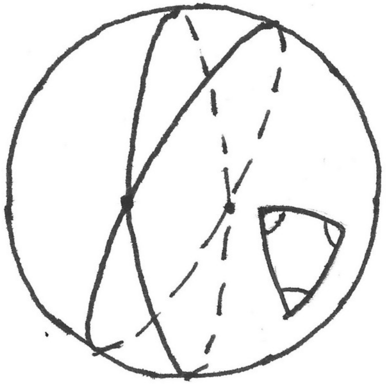

# A Priori Knowledge

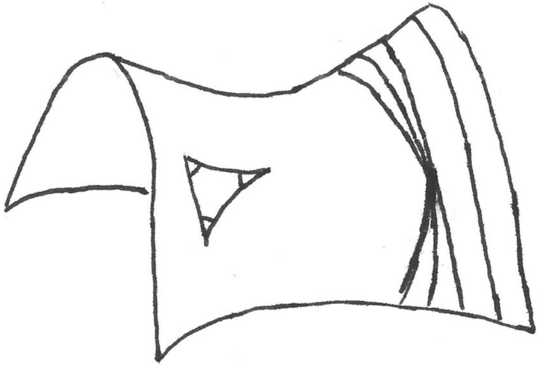
- Locke, Hume, Kant, Spinoza, and more
- Knowledge can be independent of experience and is inherent
- Knowledge is absolute
- Euclidean Geometry


Prop. 17.
Prop. 16.
Prop. 15.
Prop. 17.









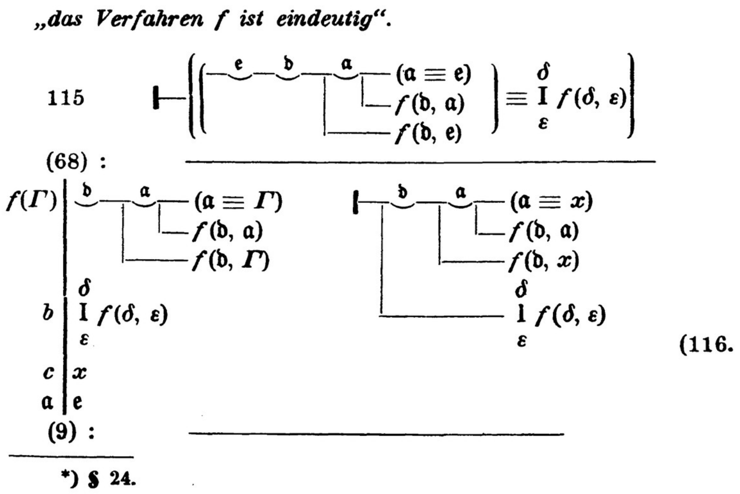
# A Priori Knowledge

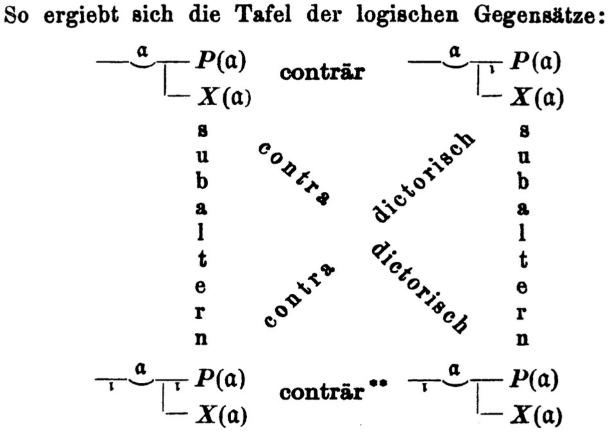
- Locke, Hume, Kant, Spinoza, and more ARE WRONG
- Knowledge is relative (to a set of axioms).

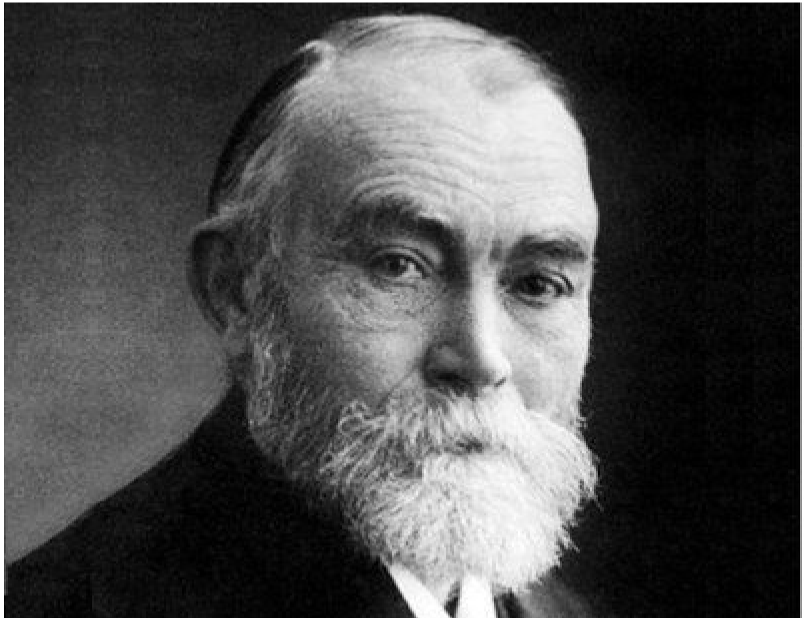
# THOUGHT

- "It is obvious that if we could find characters or signs suited for expressing all our thoughts as clearly and as exactly as arithmetic expresses numbers or geometry expresses lines, we could do in all matters insofar as they are subject to reasoning all that we can do in arithmetic and geometry. For all investigations which depend on reasoning would be carried out by transposing these characters and by a species of calculus."

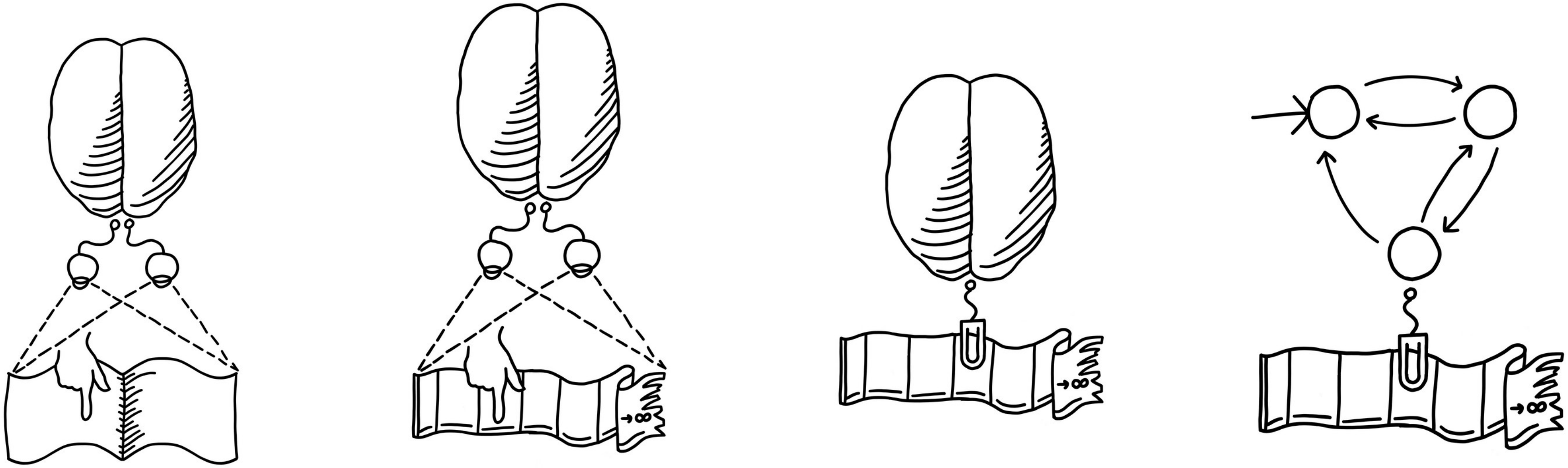
- Proto-propositional Logic
- P => Q
- etc



# COMPUTATION



- Any Intutive Algorithm has an Equivalent Formal Turing Machine

$$
\begin{tikzcd}
\text{Intutive Algorithm} \arrow[r, Leftrightarrow] & \text{Formal Turing Machine} \arrow[d, Leftrightarrow] \\
 & \text{Theorems}
\end{tikzcd}
$$

Formal Theorems can
implicate the intuitive concept

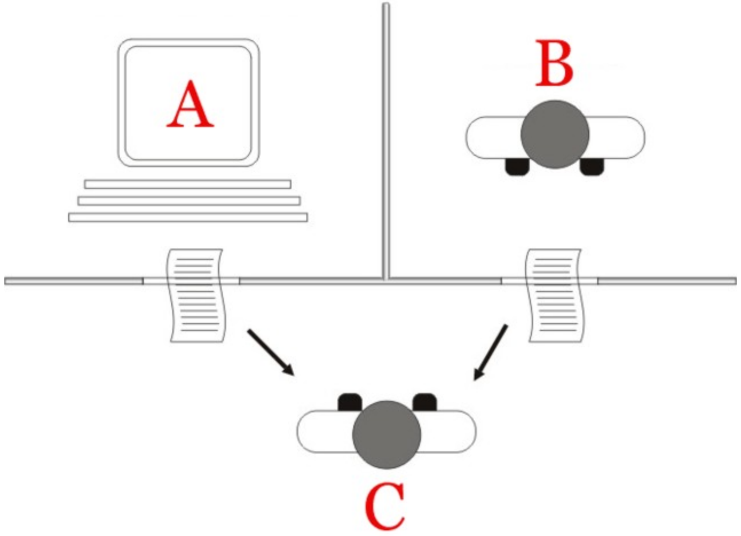
# INTELLIGENCE

# Intelligence to a Philosopher

- Incredibly debated and ancient question
- Easy to get stuck into many unrelated questions
- Sentience. Is a monkey intelligent? Is a lobster? Celery? Rock?
- Human Exceptionalism

# Turing Test

- Something is intelligent if it looks intelligent



- Diogenes and Plato
- “Axiomitization” of Man
- How to resolve?

# PREDICTION

Inductive reasoning dates back at least to the Greek philosopher of science Epicurus (342?–270? BC), who proposed the following approach:

> **Principle of Multiple Explanations.** If more than one theory is consistent with the observations, keep all theories.

The second and more sophisticated principle is the celebrated Occam's razor principle commonly attributed to William of Ockham (1290?–1349?). This was formulated about fifteen hundred years after Epicurus. In sharp contrast to the principle of multiple explanations, it states:

> **Occam's Razor Principle.** Entities should not be multiplied beyond necessity.

According to Bertrand Russell, the actual phrase used by William of Ockham was, "It is vain to do with more what can be done with fewer." This is generally interpreted as, 'among the theories that are consistent with the observed phenomena, one should select the simplest theory.' Isaac Newton (1642–1727) states the principle as rule 1 for natural philosophy in the *Principia*:

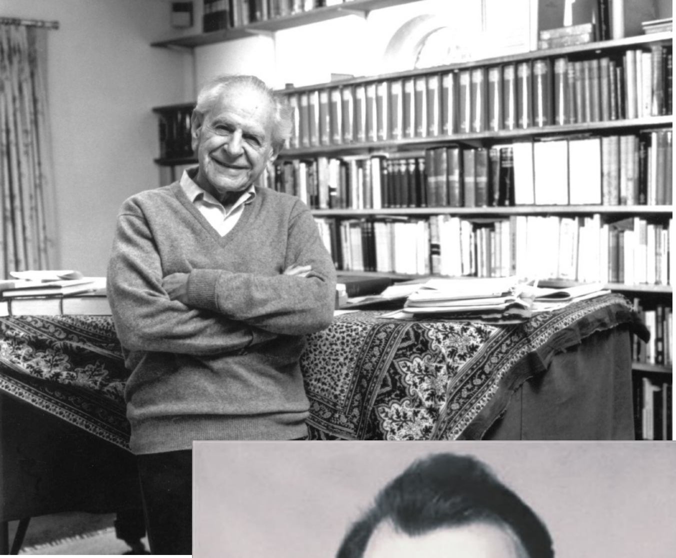
"We are to admit no more causes of natural things than such as are both true and sufficient to explain the appearances. To this purpose the philosophers say that Nature does nothing in vain, and more is in vain when less will serve; for Nature is pleased with simplicity, and affects not the pomp of superfluous causes." [Newton]

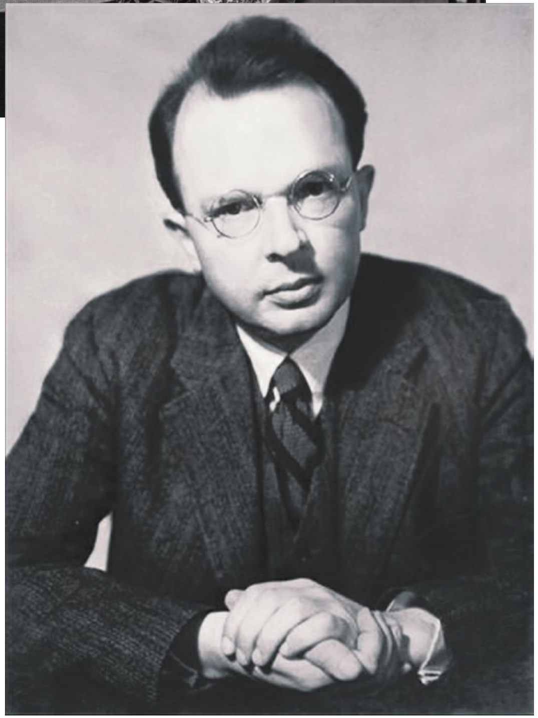
# Problem of Induction

- Induction – Make an observation and infer truth (perhaps with probability)
  - If 5 people order the soup, the salad might be bad
  - The soup might be good
- Deduction – Given premises, deduce truth
  - All men are mortal, Socrates is a man, Socrates is mortal

# Problem of Induction

- Hume Argues there is no non-circular way to justify inductive inferences
- Why should the future resemble the past?
- “The man who has fed the chicken every day throughout its life at last wrings its neck instead, showing that more refined views as to the uniformity of nature would have been useful to the chicken.”
- The only possible induction is deduction

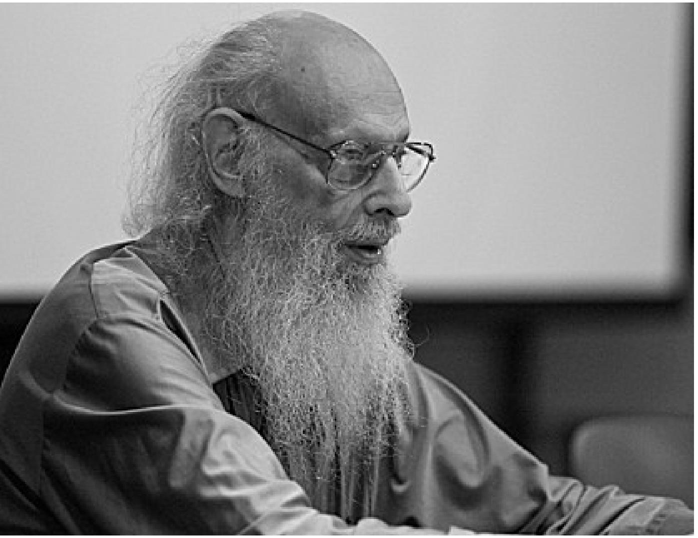




# Philosophical Failure

- Popper, Carnap attempted to resolve this
- With just philosophy, no solution had both Occam's razor and Epicurius' Principle

# Computer Science Wins



- Solmonoff Theory of Prediction solves this problem perfectly!
- Has both Occam's Razor and Epicurius Principle
- Its just Kolmogorov Complexity!

# Solmonoff Theory of Prediction

- Nature is an infinite binary string $\omega = 011011\ldots$
- preliminary data of the investigator, the hypotheses proposed, the experimental setup designed, the trials performed, the outcomes obtained, the new hypotheses formulated.

# Solmonoff Theory of Prediction

- Nature is an infinite binary string $\omega = 011011\ldots$
- Investigator learns larger and larger prefixes of $\omega$ by performing experiments on nature
- Candidate theories are programs to print prefixes
- Assign probabilities to the theories according to the lengths of the programs

# KNOWLEDGE

# Knowledge to a Philosopher

- All Knowledge is Information
- But not all Information is Knowledge
- Wiki page for philosophical definitons of knowledge has 80 sources
- Incredibly subjective if any one definition is good

# Knowledge to a Computer Scientist

- Knowledge is a witness to an NP-complete problem! (under unproved complexity assumptions)
- An answer to a hard to solve problem
- $\sqrt{125}$ is not “knowledge”
- Prover can convince verifier they have knowledge without revealing it
- Other definitions in other domains
- (Definition of common knowledge in distributed systems)

# RANDOMNESS

# Pseudorandomness

- Kolmogorov Definition works for true randomness
- Pseudorandom strings by definition have low Kolmogorov complexity
- But they look random! How to resolve?

# Pseudorandomness

## 1. Introduction.

**1.1. Randomness and complexity theory.** We introduce a new method of generating sequences of pseudo-random bits. Any such method implies, directly or indirectly, a definition of randomness.

Much effort has been devoted in the second half of this century to make precise the notion of randomness. Let us informally recall Kolmogorov's influential definition [18]:

> A sequence of bits $A = a_1, a_2, \cdots, a_k$ is random if the length of the minimal program outputting $A$ is at least $k$.

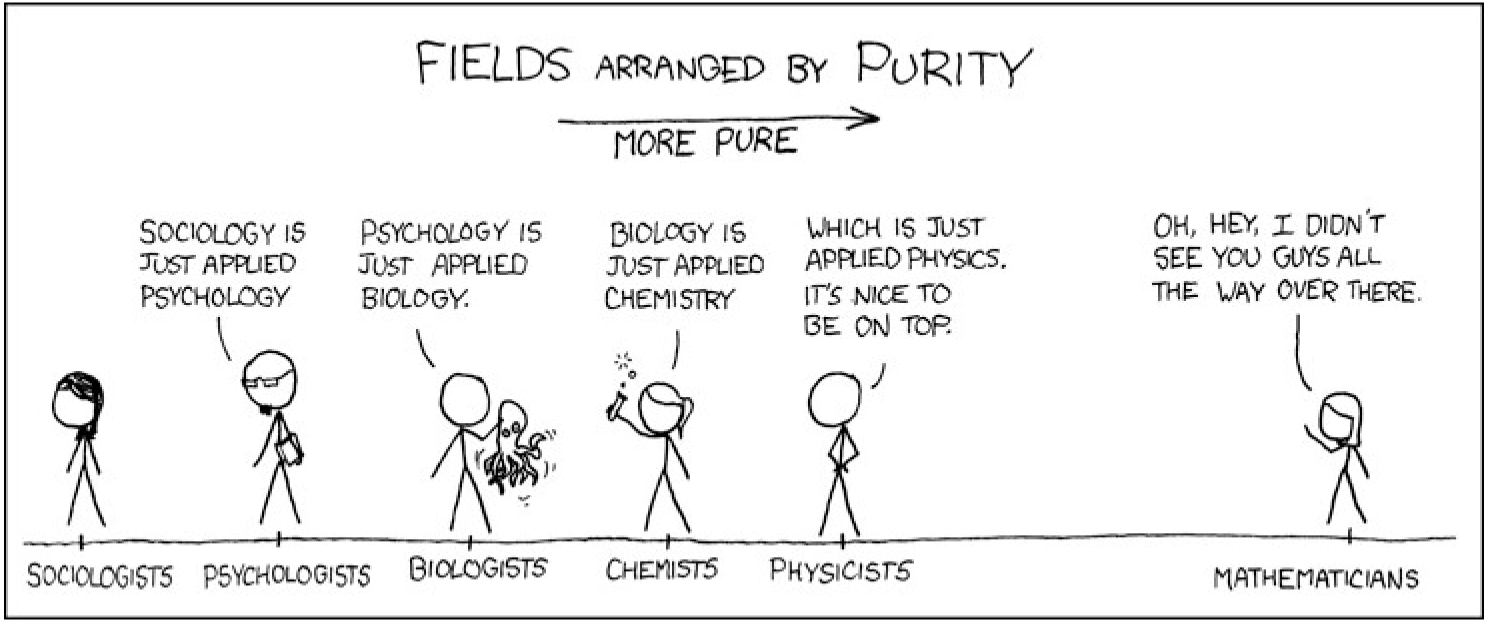
We remark that the length of a program, from a computational complexity point of view, is a rather unnatural measure. We want to investigate a more operative definition of randomness in the light of complexity theory.

*A mental experiment.* A and B want to play head and tail in four different

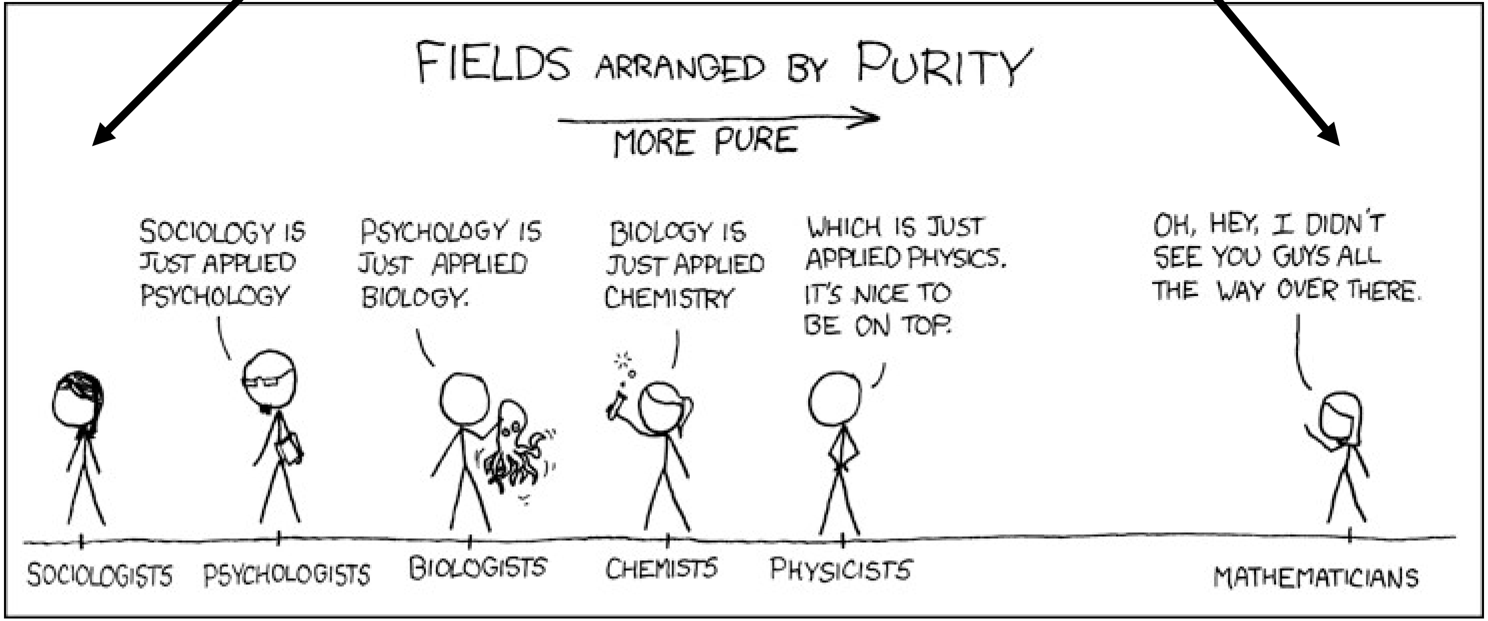
# Pseudorandomness

- An infinite sequence of bits is pseudorandom if
- Given first n bits, probability any algorithm guesses bit n+1 correctly is not greater than ½
- P[A guesses b_{n+1}] <= ½ +- e
- Brings in computational assumptions

- Computer Science has nothing to do with computers. These are just tools.
- Chemistry is not about beakers
- The computational lens is the greatest scientific and philosophical advancement in history
- We (Computer Scientists) have as big of a claim to understanding the beauty of the natural world as much as physicists or biologists do


FIELDS ARRANGED BY PURITY
MORE PURE
SOCIOLOGY IS JUST APPLIED PSYCHOLOGY
PSYCHOLOGY IS JUST APPLIED BIOLOGY.
BIOLOGY IS JUST APPLIED CHEMISTRY
WHICH IS JUST APPLIED PHYSICS. IT'S NICE TO BE ON TOP.
OH, HEY, I DIDN'T SEE YOU GUYS ALL THE WAY OVER THERE.
SOCIOLOGISTS
PSYCHOLOGISTS
BIOLOGISTS
CHEMISTS
PHYSICISTS
MATHEMATICIANS

# Computer Science

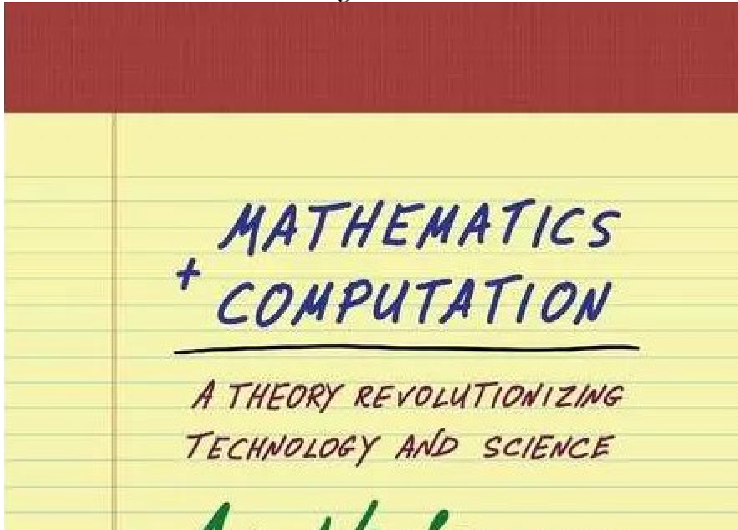


# A Recipe for All of Computer Science

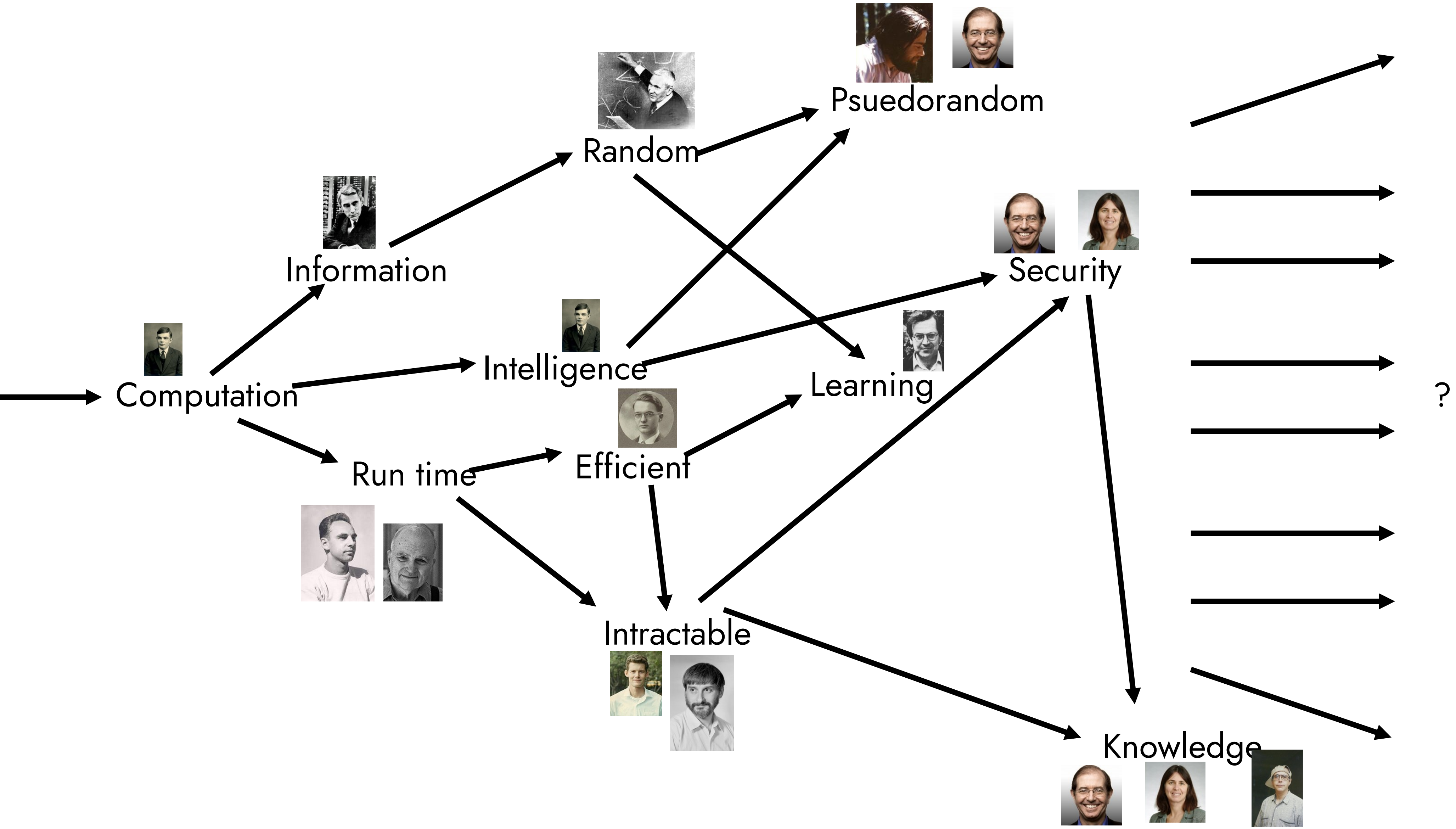
- Choose an abstract intuitive concept
- Construct a formal definition
- Argue that the intuitive concept corresponds to the formal definition
- Proofs or results involving the formal definition implicate the intuitive concept

I feel proud to belong to a field that has seriously taken on defining (sometimes redefining, sometimes in several ways) and understanding such fundamental notions that include: *collusion, coordination, conflict, entropy, equilibrium, evolution, fairness, game, induction, intelligence, interaction, knowledge, language, learning, ontology, prediction, privacy, process, proof, secret, simultaneity, strategy, synchrony, randomness, and verification.*

It is worthwhile reading this list again, slowly. I find it quite remarkable to contrast the long history, volumes of text written, and intellectual breadth that the concepts in this list represent, with the small size and the relative youthfulness of ToC, which has added so much to their understanding.



- Proof – Frege, Hillbert, Russell, Whitehead, (1900s)
- Truth – Tarski (1933)
- Computation, Algorithm – Turing (1936)
- Information, Communication, Noise – Shannon (1948)
- Intelligence – Turing (1950)
- Grammatical and Ungrammatical – Chomsky (1950s)
- Randomness – Kolmogorov (1963)
- Run-time, Complexity – Hartmanis and Stearns (1965)
- Efficient – Edmonds and Cobham(1965)
- Intractable, Difficult – Cook and Levin (1971, 1973)
- Pseudorandomness – Blum, Micali (1982)
- Secure – Goldwasser, Micali (1982)
- Learning – Valiant (1984)
- Knowledge – Babai, Goldwasser, Micali, Rackoff, Moran, (1989+)


Psuedorandom
Random
Information
Security
Intelligence
Learning
Computation
?
Efficient
Run time
Intractable
Knowledge

# The Future?

- Discrete Math is young
- The Blums’ work on conciousness
- More modeling of the brain
- Scientific revolutions