CS251

Great Ideas in *Theoretical* Computer Science

Proof. Define f_{ij} as in (5). As f is symmetric, we only need to consider f_{12}.

$$\begin{aligned}
\mathbf{E}\left[f_{12}^2\right] &= \mathbf{E}_{x_3\ldots x_n}\left[\frac{1}{4}\cdot\left(f_{12}^2(00x_3\ldots x_n)+f_{12}^2(01x_3\ldots x_n)+f_{12}^2(10x_3\ldots x_n)+f_{12}^2(11x_3\ldots x_n)\right)\right]\\
&= \frac{1}{4}\mathbf{E}_{x_3\ldots x_n}\left[\left(f(00x_3\ldots x_n)-f(11x_3\ldots x_n)\right)^2+\left(f(11x_3\ldots x_n)-f(00x_3\ldots x_n)\right)^2\right]\\
&\geq \frac{1}{2}\left(\binom{n-2}{r_0-1}\cdot 2^{-(n-2)}\cdot 4+\binom{n-2}{n-r_1-1}\cdot 2^{-(n-2)}\cdot 4\right)\\
&= 8\cdot\left(\frac{(n-r_0+1)(n-r_0)}{n(n-1)}\cdot\binom{n}{r_0-1}+\frac{(n-r_1+1)(n-r_1)}{n(n-1)}\cdot\binom{n}{r_1-1}\right)2^{-n}.
\end{aligned}$$

Inequality (6) follows by applying Lemma 2.2.

In order to establish inequality (7), we show a lower bound on the principal Fourier coefficient of f:

$$\widehat{f}(\emptyset)\geq 1-2\left(\sum_{s<r_0}\binom{n}{s}+\sum_{s>n-r_1}\binom{n}{s}\right)2^{-n},$$

which implies that

$$\widehat{f}(\emptyset)^2\geq 1-4\cdot\left(\sum_{s<r_0}\binom{n}{s}+\sum_{s<r_1}\binom{n}{s}\right)2^{-n}.$$

□

Mathematical Reasoning & Proofs

What is **mathematical reasoning**?

What is a **proof**?

Is this a legit proof?

Proposition:

Start with any number.
If the number is even, divide it by 2.
If it is odd, multiply it by 3 and add 1.
If you repeat this process, it will lead you to 4, 2, 1.

Proof:

Many people have tried this.
No one came up with a counter-example. $\blacksquare$

Is this a legit proof?

~~Proposition:~~ Collatz Conjecture

Start with any number.
If the number is even, divide it by 2.
If it is odd, multiply it by 3 and add 1.
If you repeat this process, it will lead you to 4, 2, 1.

Proof:

Many people have tried this.
No one came up with a counter-example. ∎

Is this a legit proof?

Proposition:

$313(x^3 + y^3) = z^3$ has no solution for $x, y, z \in \mathbb{Z}^+$.

Proof:

Computer verified that there is no solution for numbers with < 500 digits.

$\blacksquare$

Is this a legit proof?

~~Proposition:~~

$313(x^3 + y^3) = z^3$ has no solution for $x, y, z \in \mathbb{Z}^+$.

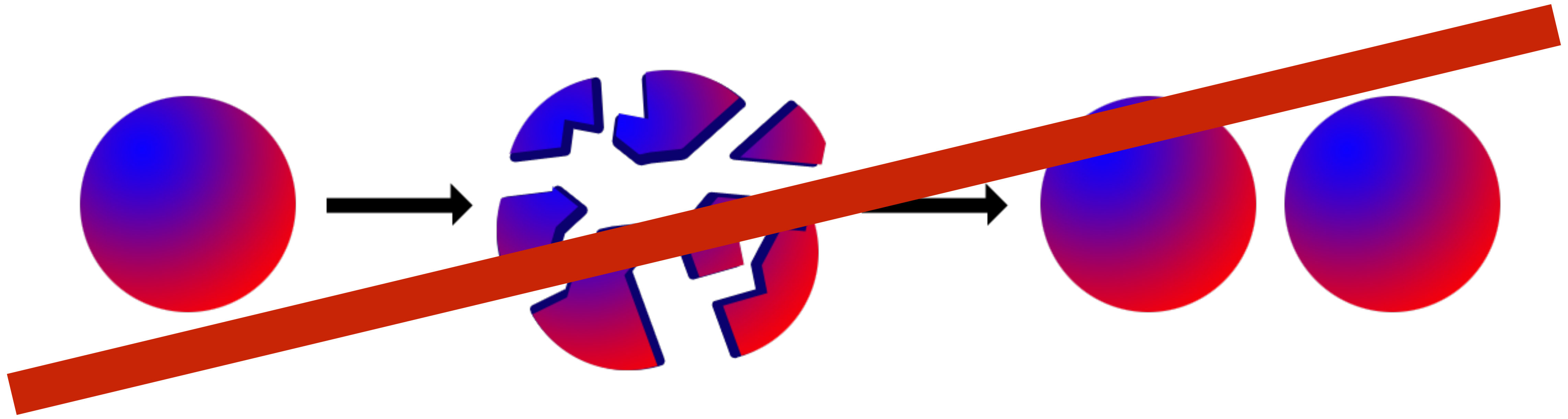
~~Proof:~~

~~Computer verified that there is no solution for numbers with $<$ 500 digits.~~ $\blacksquare$

Is this a legit proof?

Proposition:

Given a solid ball in 3d space,
there is no way to decompose it into a finite number of disjoint subsets, which can be put together to form two identical copies of the original ball.



Proof:

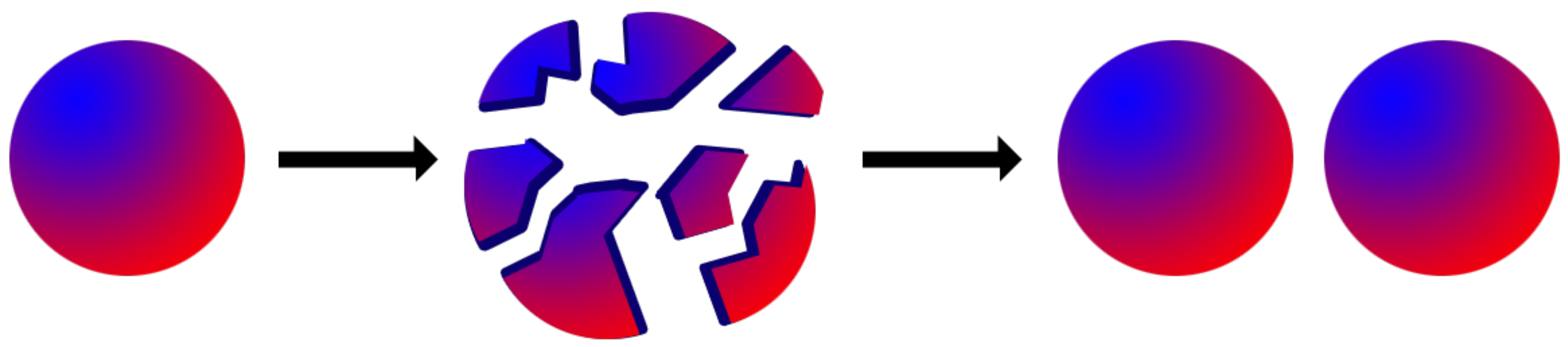
Obvious.

$\blacksquare$

Is this a legit proof?

Banach-Tarski Theorem:

Given a solid ball in 3d space,
there **is a** way to decompose it into a finite number of disjoint subsets, which can be put together to form two identical copies of the original ball.



Proof:

Uses group theory… Pieces are such weird scatterings of points that they have no meaningful "volume"…

Is this a legit proof?

Proposition:

$1 + 1 = 2.$

Proof:

This is obvious??!?

Is this a legit proof?

Proposition:

$1 + 1 = 2.$

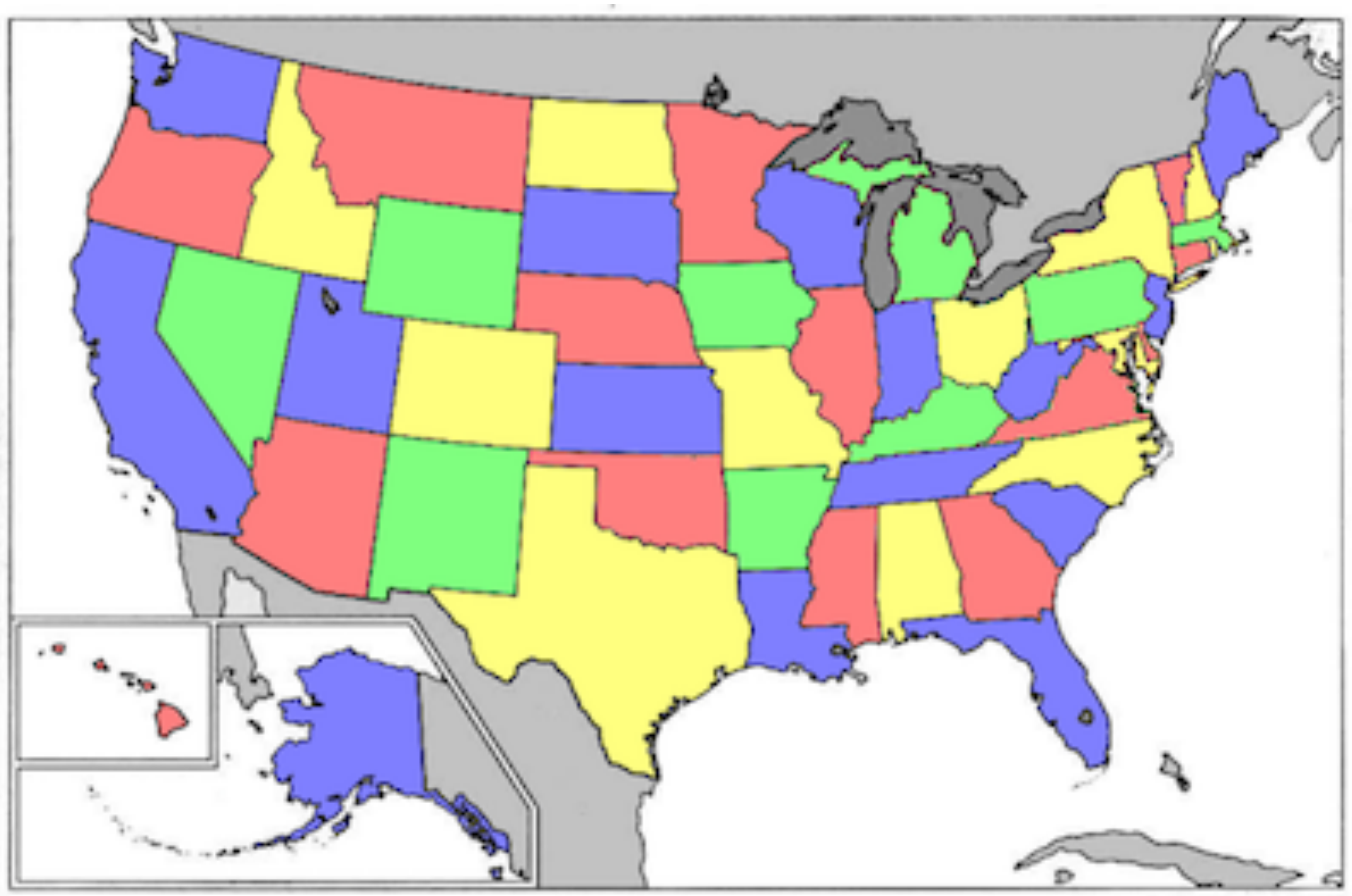
Proof:

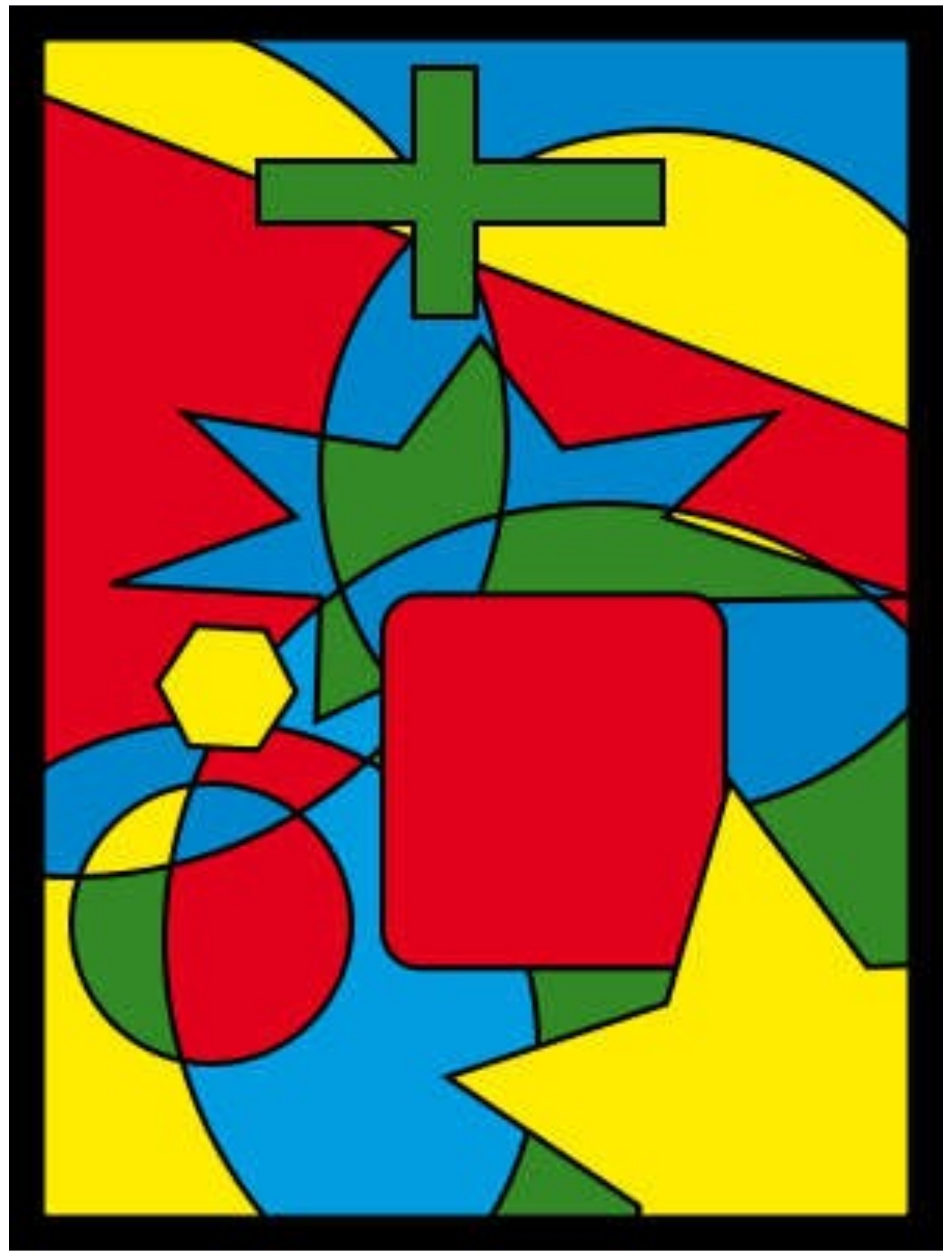
This is obvious! $\blacksquare$

The story of 4 color theorem

1852 Conjecture:

Any 2-d map of regions can be colored with 4 colors so that **no** two adjacent regions get the same color.





The story of 4 color theorem

1879: Proved by Kempe in *American Journal of Mathematics* (was widely acclaimed)

1880: Alternate proof by Tait in *Trans. Roy. Soc. Edinburgh*

1890: Heawood finds a bug in Kempe's proof

1891: Petersen finds a bug in Tait's proof

1969: Heesch showed the statement could in principle be reduced to checking a large number of cases.

1976: Appel and Haken wrote massive amount of code to compute and check 1936 cases.
(1200 hours of computer time)

The story of 4 color theorem

Much controversy at the time. Is this a proof?

The story of 4 color theorem

Much controversy at the time. Is this a proof?

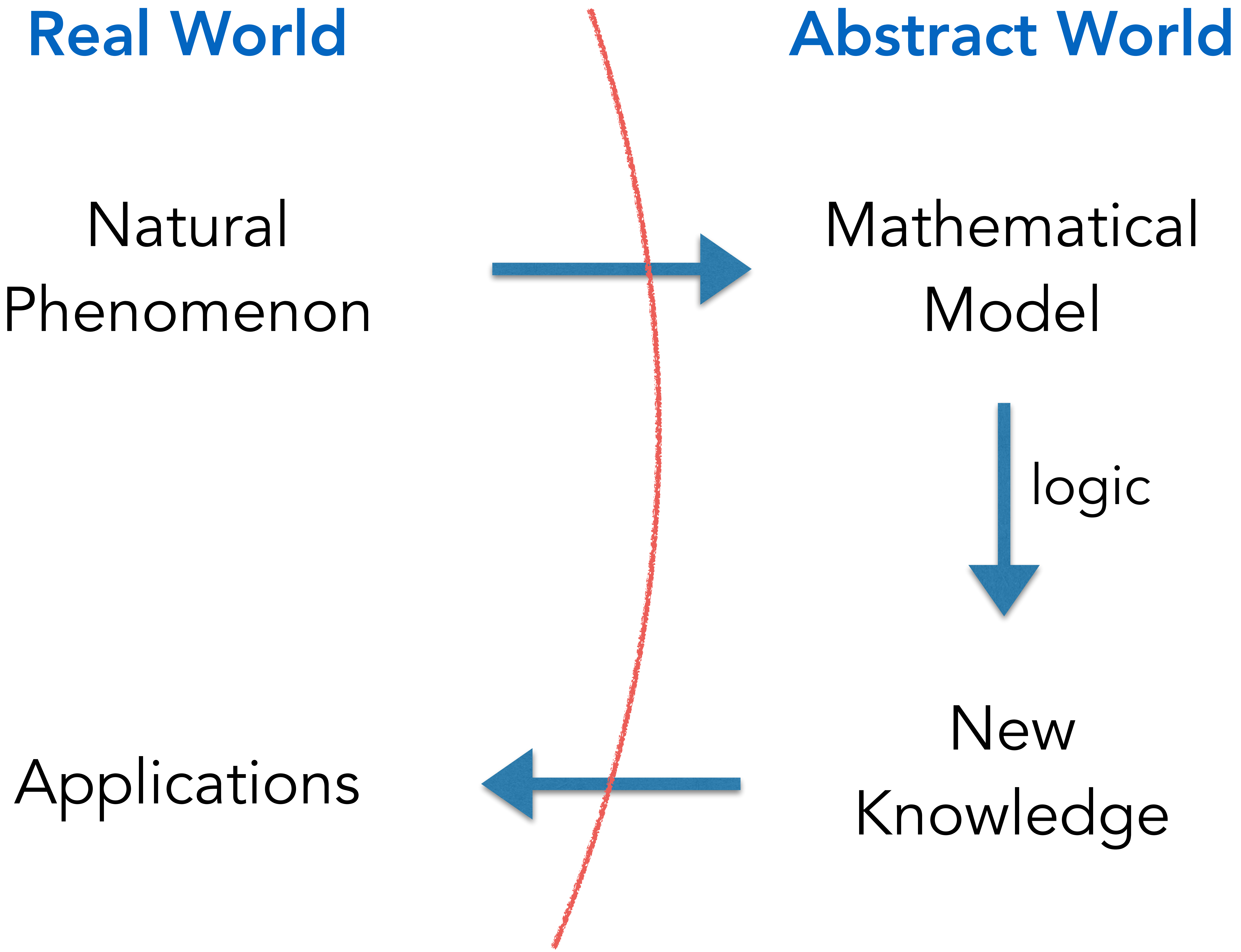
Arguments against:

- maybe there is a bug in the code
- maybe there is a bug in the compiler
- maybe there is a bug in the hardware
- no "insight" is derived

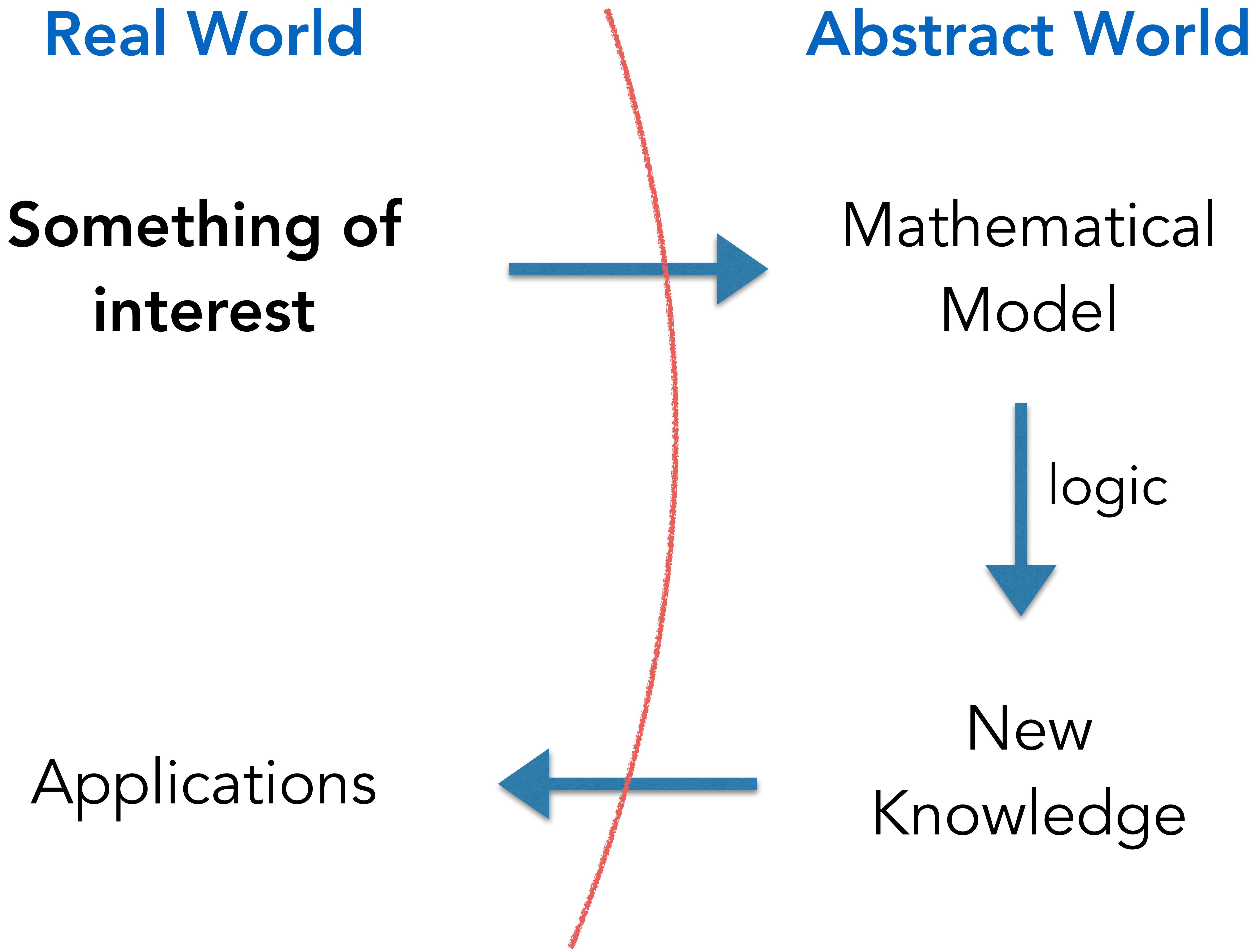
1997: Simpler computer proof by
Robertson, Sanders, Seymour, Thomas

Understanding Good Old Regular Mathematics (GORM)

Picture of Physics



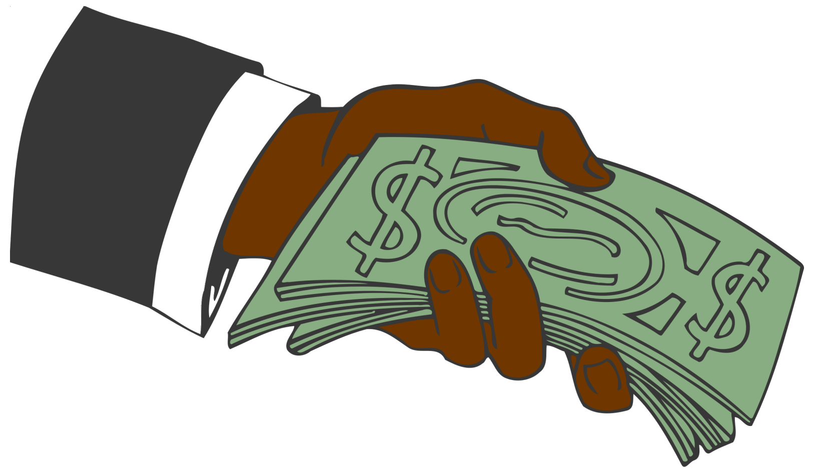
GORM: Good Old Regular Mathematics



GORM: Good Old Regular Mathematics

Real World

Exchanging goods



Applications

Abstract World

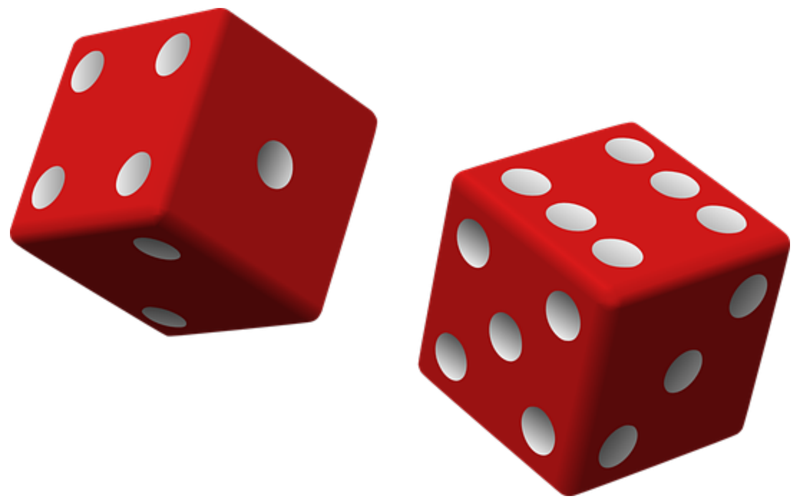
Numbers, Arithmetic

New Knowledge

GORM: Good Old Regular Mathematics

Real World

Gambling



Applications

Abstract World

Probability Theory

New Knowledge

GORM: Good Old Regular Mathematics

Real World

Abstract World

Farming

Plane Geometry

New Knowledge

Applications

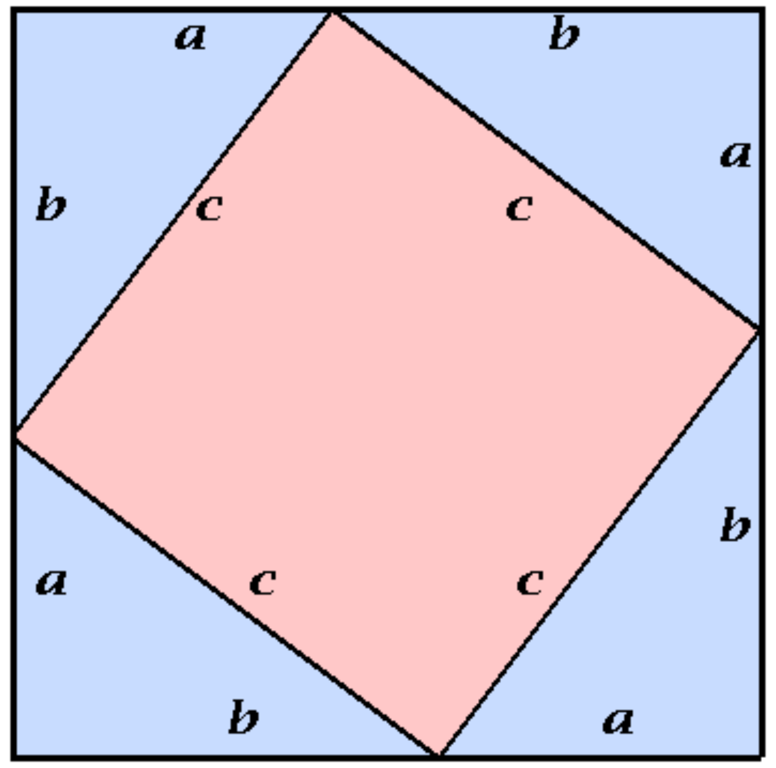
Spectrum of GORM

informal reasoning with real objects

start reasoning with mathematical objects

"formal" definitions and reasoning

"Every person is mortal.
Aristotle is a person.
Therefore,
Aristotle is mortal."



highschool

professional mathematicians

Spectrum of GORM

informal reasoning with real objects	start reasoning with mathematical objects	"formal" definitions and reasoning

Mathematical reasoning:

assumed truths —*logical deductions*→ new/deduced truths

"obvious" truths

Spectrum of GORM

informal reasoning with real objects

start reasoning with mathematical objects

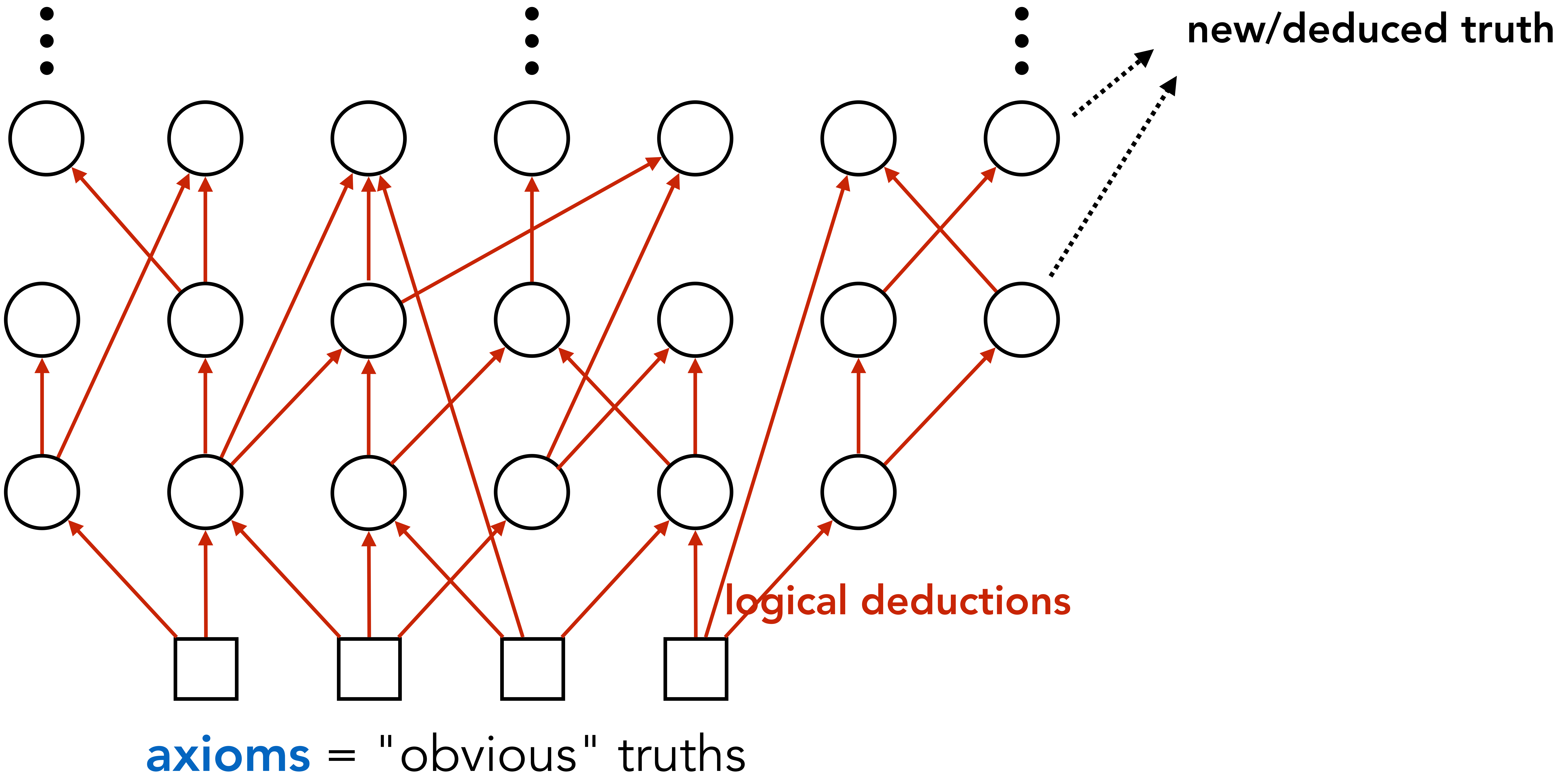
"formal" definitions and reasoning

Mathematical reasoning:

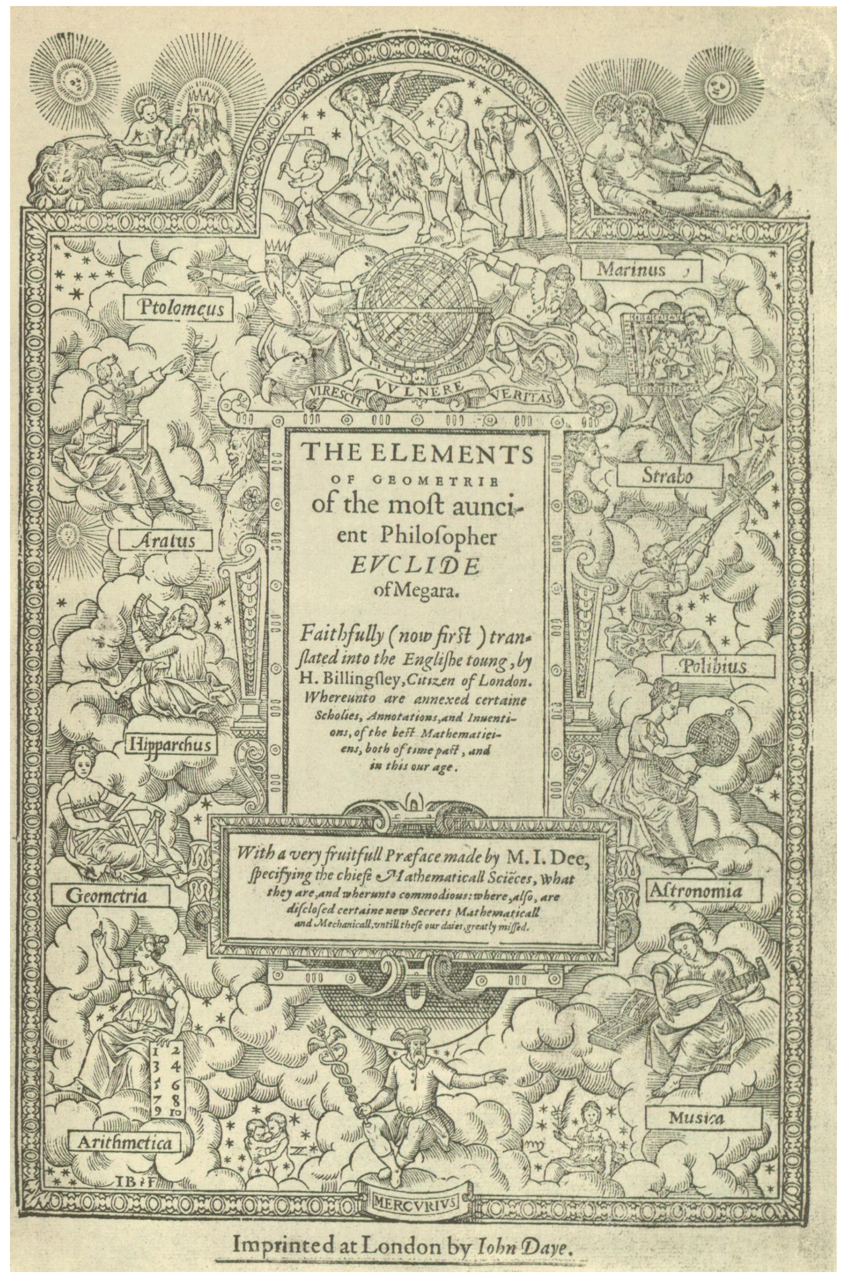
assumed truths —*logical deductions*→ new/deduced truths

"obvious" & deduced truths

Mathematical reasoning:



Early example: Euclidean geometry



5 AXIOMS

1. Any two points can be joined by exactly one line segment.

2. Any line segment can be extended into one line.

3. Given any point P and length r, there is a circle of radius r and center P.

4. Any two right angles are congruent.

5. If a line L intersects two lines M and N, and if the interior angles on one side of L add up to less than two right angles, then M and N intersect on that side of L.

(Through a point not on a given straight line, at most one line can be drawn that never meets the given line.)

Spectrum of GORM

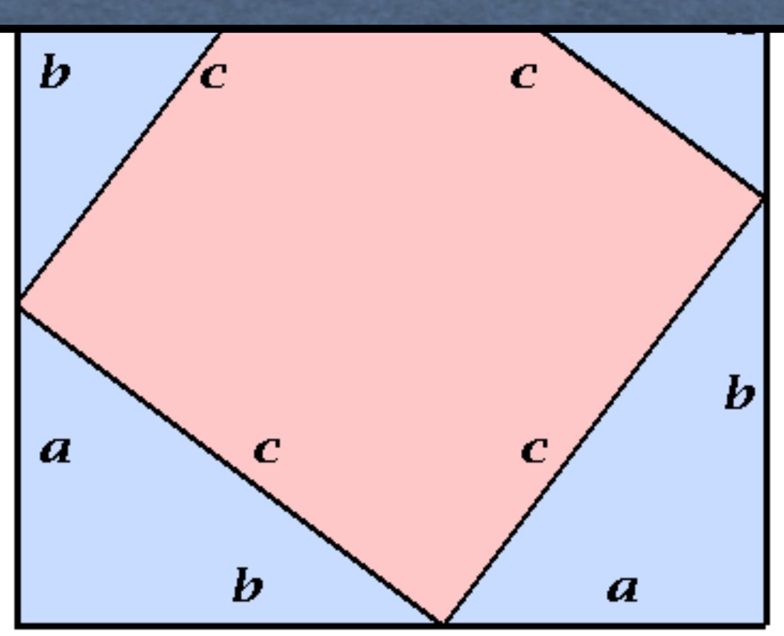
informal reasoning
with real objects

start reasoning with
mathematical objects

"formal" definitions
and reasoning

Over time serious issues emerged,
and a foundational crisis began…

"Every person is mortal.
Aristotle is a person.
Therefore,
Aristotle is mortal."



highschool

professional
mathematicians

Problems with GORM

Problem 1: What is "obvious" truth?

Can we agree on a set of axioms
that all mathematical reasoning can build on?

Problem 1: What is "obvious" truth?

The square root of 2 is irrational.

1. Suppose $\sqrt{2}$ is rational.
   Then we can find $a, b \in \mathbb{N}$ such that $\sqrt{2} = a/b$.
2. So $\sqrt{2} = r/s$, where r and s are **not** both even.
3. Then $2 = r^2/s^2$, and therefore $2s^2 = r^2$.
4. Given this, we have r^2 is even, which means r is even.
5. We can thus write $r = 2t$ for some $t \in \mathbb{N}$.
6. If $2s^2 = r^2$ and $r = 2t$, then $2s^2 = 4t^2$,
   and so $s^2 = 2t^2$.
7. Therefore s^2 is even, which means s is even.
8. Contradiction is reached.

Problem 1: What is "obvious" truth?

The square root of 2 is irrational.

1. Suppose $\sqrt{2}$ is rational.
   Then we can find $a, b \in \mathbb{N}$ such that $\sqrt{2} = a/b$.
2. So $\sqrt{2} = r/s$, where r and s are **not** both even.
3. Then $2 = r^2/s^2$, and therefore $2s^2 = r^2$.
4. Given this, we have r^2 is even, which means r is even.
5. We can thus write $r = 2t$ for some $t \in \mathbb{N}$.
6. If $2s^2 = r^2$ and $r = 2t$, then $2s^2 = 4t^2$,
   and so $s^2 = 2t^2$.
7. Therefore s^2 is even, which means s is even.
8. Contradiction is reached.

Problem 1: What is "obvious" truth?

If the square of a number is even, then that number is also even.

4a. r^2 is even. Suppose r is odd.

4b. $\boxed{\text{So there is a number } t \text{ such that } r = 2t + 1.}$

4c. So $r^2 = (2t+1)^2 = 4t^2 + 4t + 1$.

4d. $4t^2 + 4t + 1 = 2(2t^2 + 2t) + 1$, which is odd.

4e. So r^2 is odd.

4f. Contradiction is reached.

Problem 1: What is "obvious" truth?

Every number is a multiple of 2 or one more than a multiple of 2.

4b1. Call a number r good if $r = 2t$ or $r = 2t + 1$.

If $r = 2t$, $r + 1 = 2t + 1$.

If $r = 2t + 1$, $r + 1 = 2t + 2 = 2(t + 1)$.

Either way, $r + 1$ is also good.

4b2. 1 is good since $1 = 0 + 1 = (0 \cdot 2) + 1$.

4b3. $\boxed{\text{Applying 4b1 repeatedly, } 2{,}3{,}4{,}\ldots \text{ are all good.}}$

Problem 1: What is "obvious" truth?

Axiom of induction

Suppose that for every positive integer n, there is a statement $S(n)$.

If $S(1)$ is true and for all n, $S(n) \implies S(n+1)$,

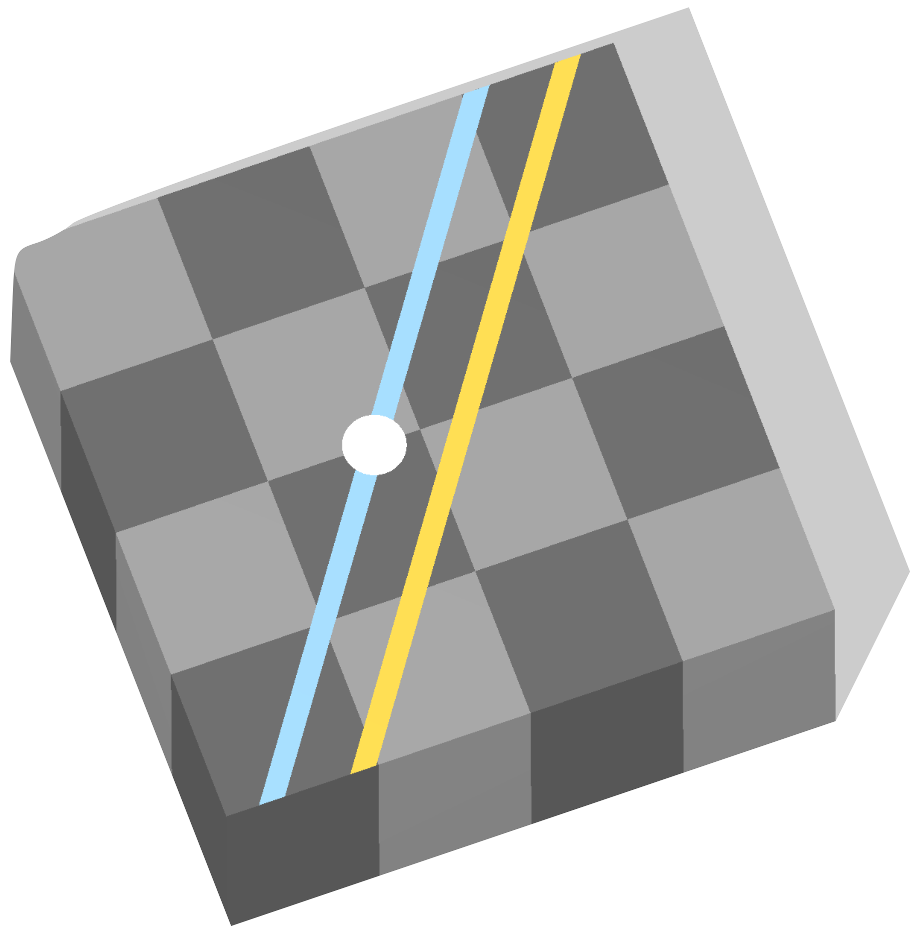
then $S(n)$ is true for all $n \geq 1$.

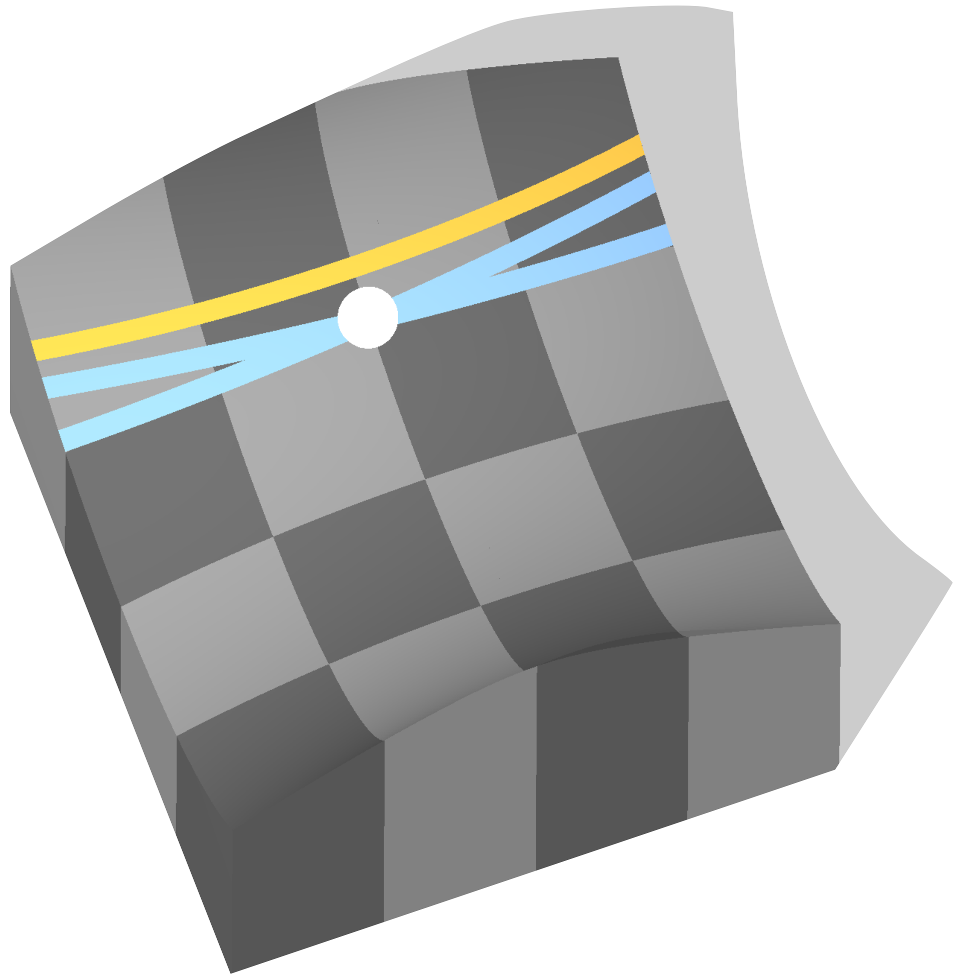
? Can every mathematical theorem be **derived** from a set of agreed upon **axioms**?

Problem 1: What is "obvious" truth?

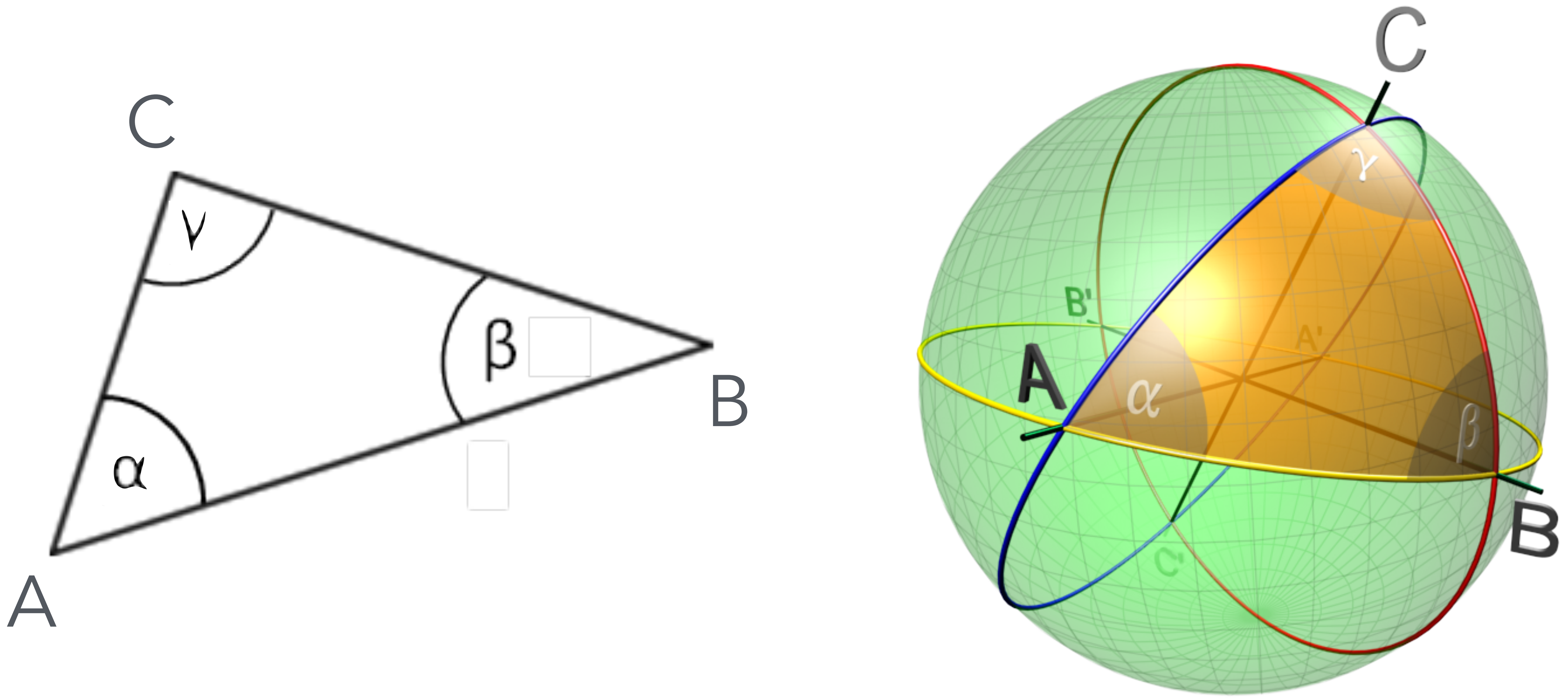
Back to Euclid

Axiom 5: Through a point not on a given straight line, at most one line can be drawn that never meets the given line.





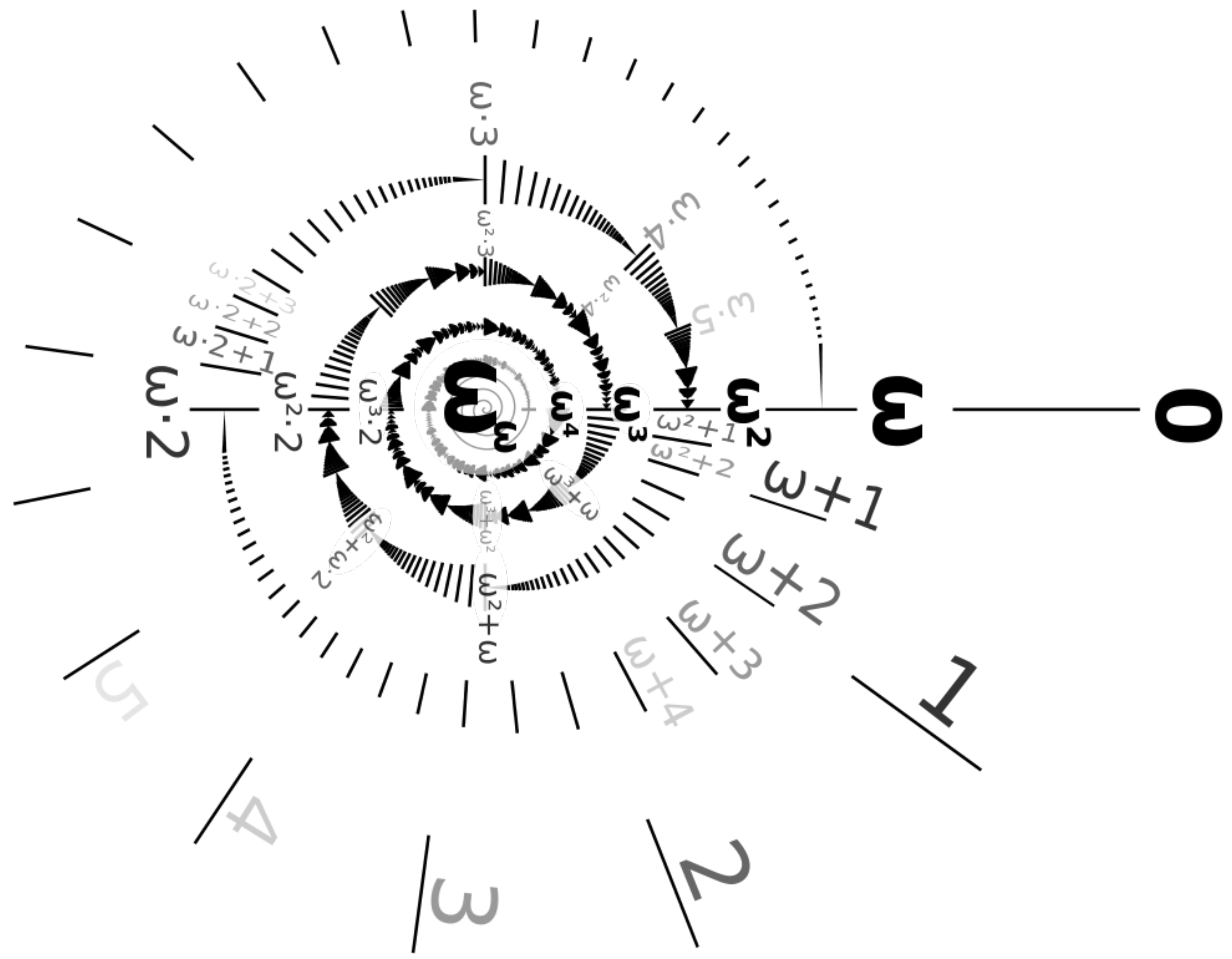
Problem 1: What is "obvious" truth?



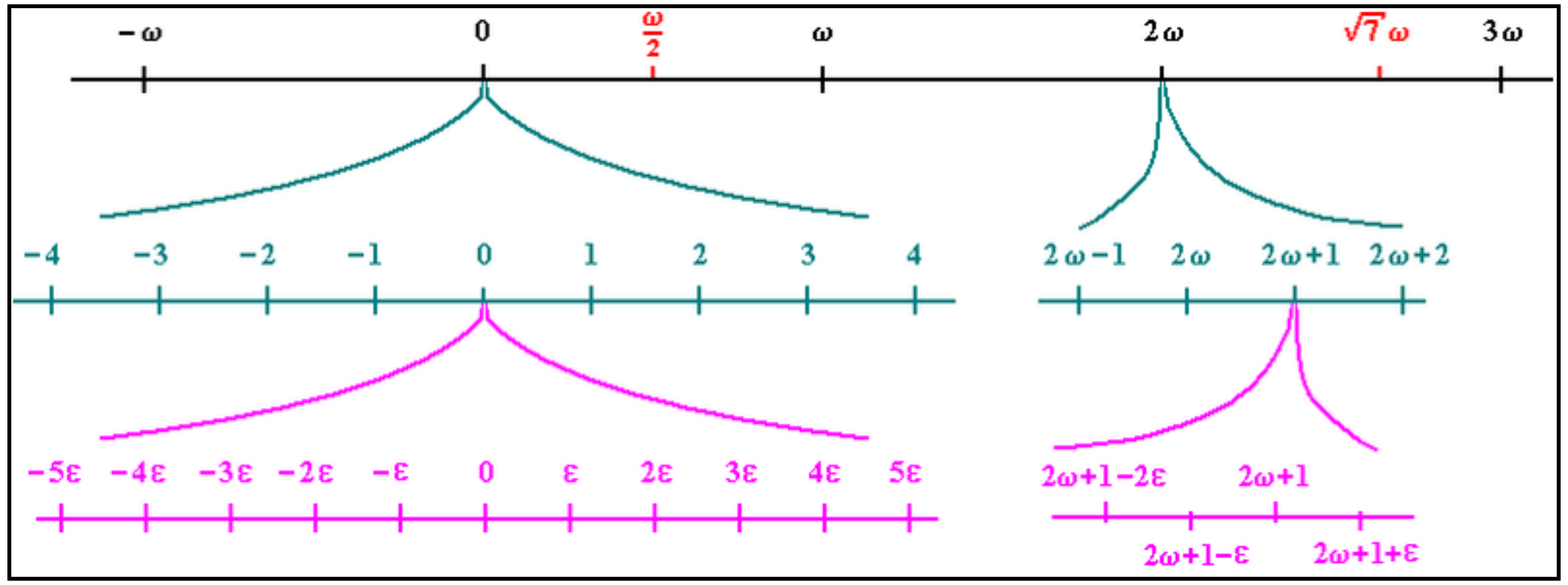
Truth is relative to your **interpretation**.

Problem 2: Infinity

Infinitely large (transfinite numbers)



Infinitely small (infinitesimals)



Problem 3: Russell's paradox

A naïve definition of a set breaks mathematics.

Problem 4: The use of human language

Not precise, ambiguous.

Serious problems! What is the solution?

Spectrum of mathematical reasoning

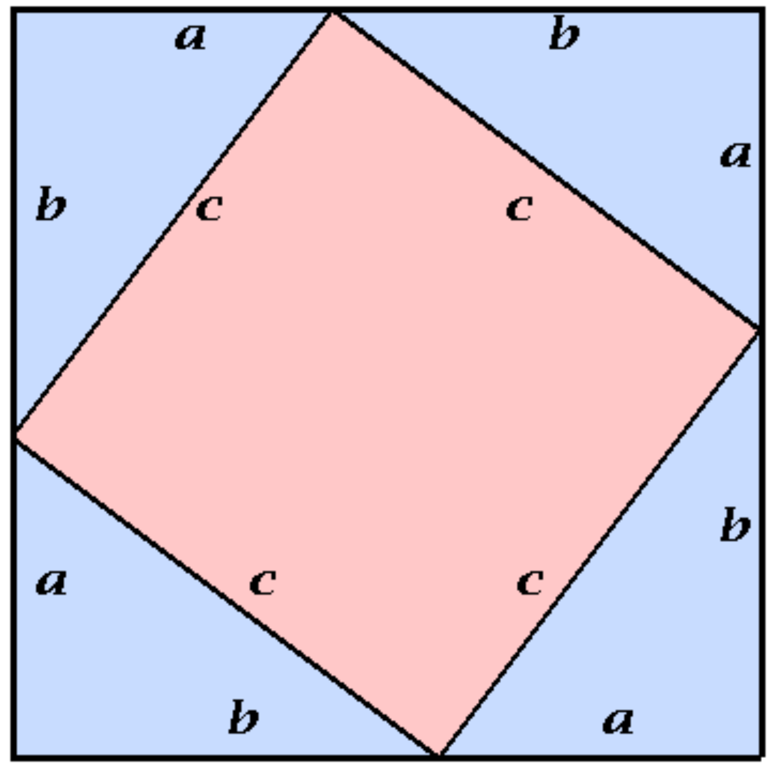
GORM territory

informal reasoning
with real objects

start reasoning with
mathematical objects

"formal" definitions
and deductions

"Every person is mortal.
Aristotle is a person.
Therefore,
Aristotle is mortal."



highschool

professional
mathematicians

Spectrum of mathematical reasoning

GORM territory

FORM

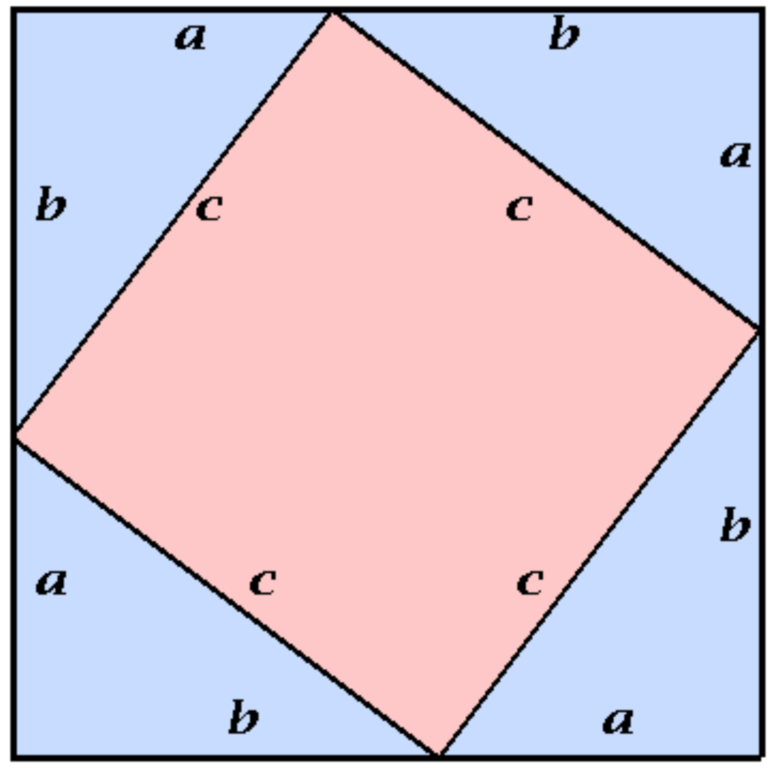
informal reasoning with real objects

start reasoning with mathematical objects

"formal" definitions and deductions

more absolute formalism

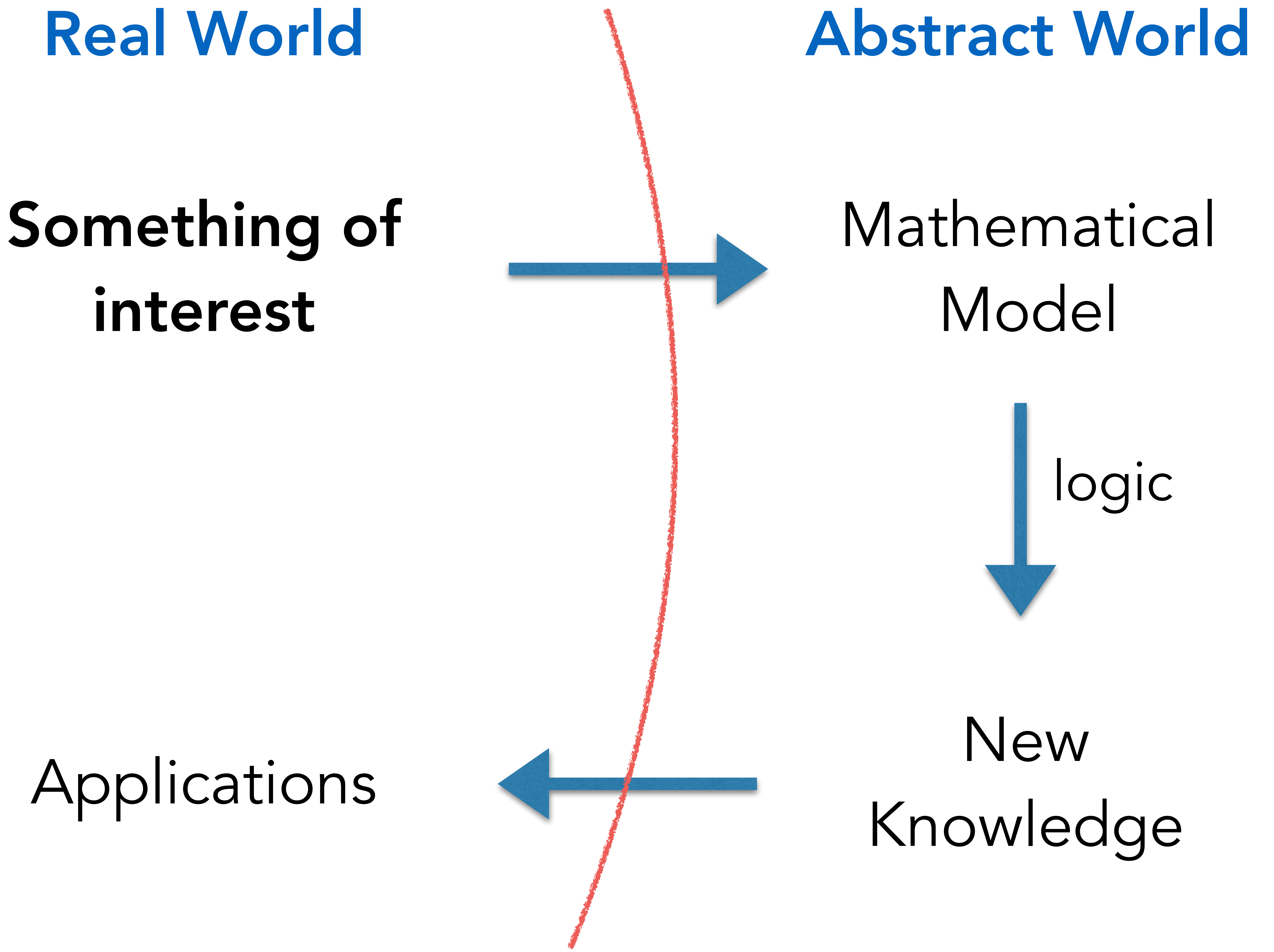
"Every person is mortal.
Aristotle is a person.
Therefore,
Aristotle is mortal."



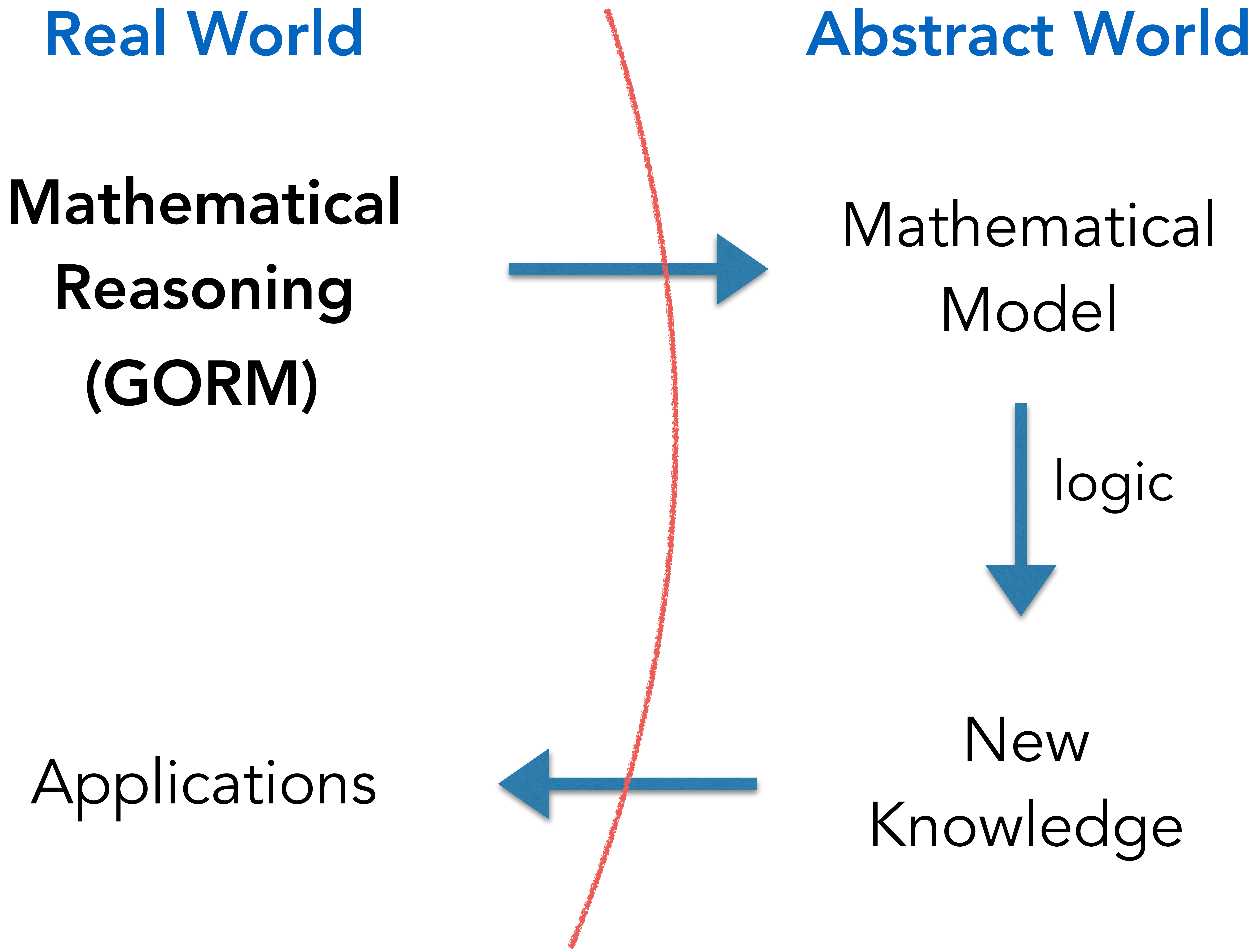
highschool

professional mathematicians

GORM: Good Old Regular Mathematics



Picture of FORM



Mathematical model for mathematical reasoning

Mathematical reasoning:

assumed truths $\xrightarrow[\textit{deductions}]{\textit{logical}}$ new/deduced truths

"obvious" & deduced truths

How do you formally represent **statements** (that may be true or false)?

Which statements are "obviously" true? (What are the **axioms**?)

Which **deduction rules** are allowed? How are they formally represented?

Picture of FORM

Real World

Abstract World

Mathematical Reasoning (GORM)

computation

Mathematical Model

logic

New Knowledge

Applications

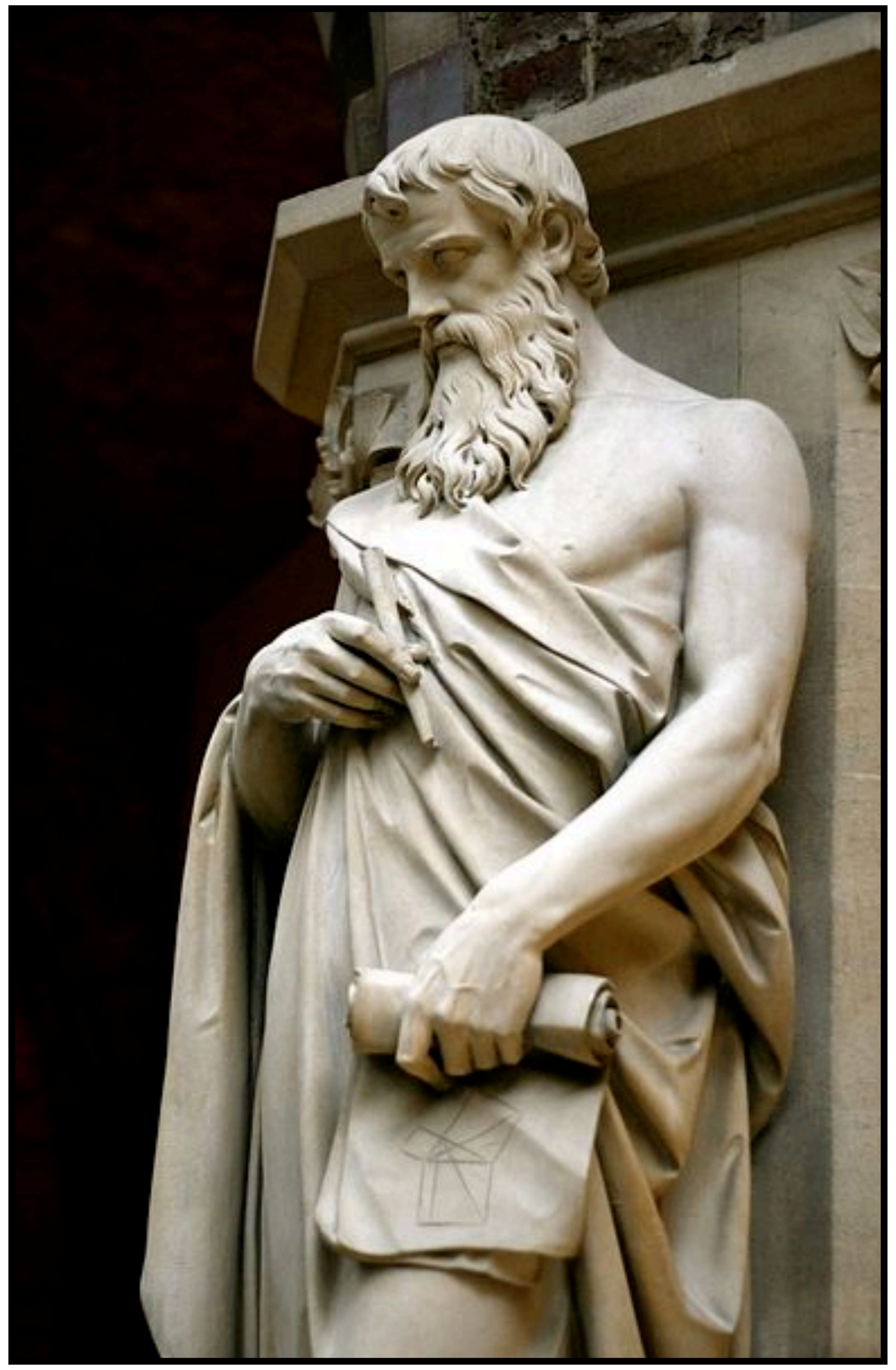
The Quest for FORM

Aristotle ~384 BCE

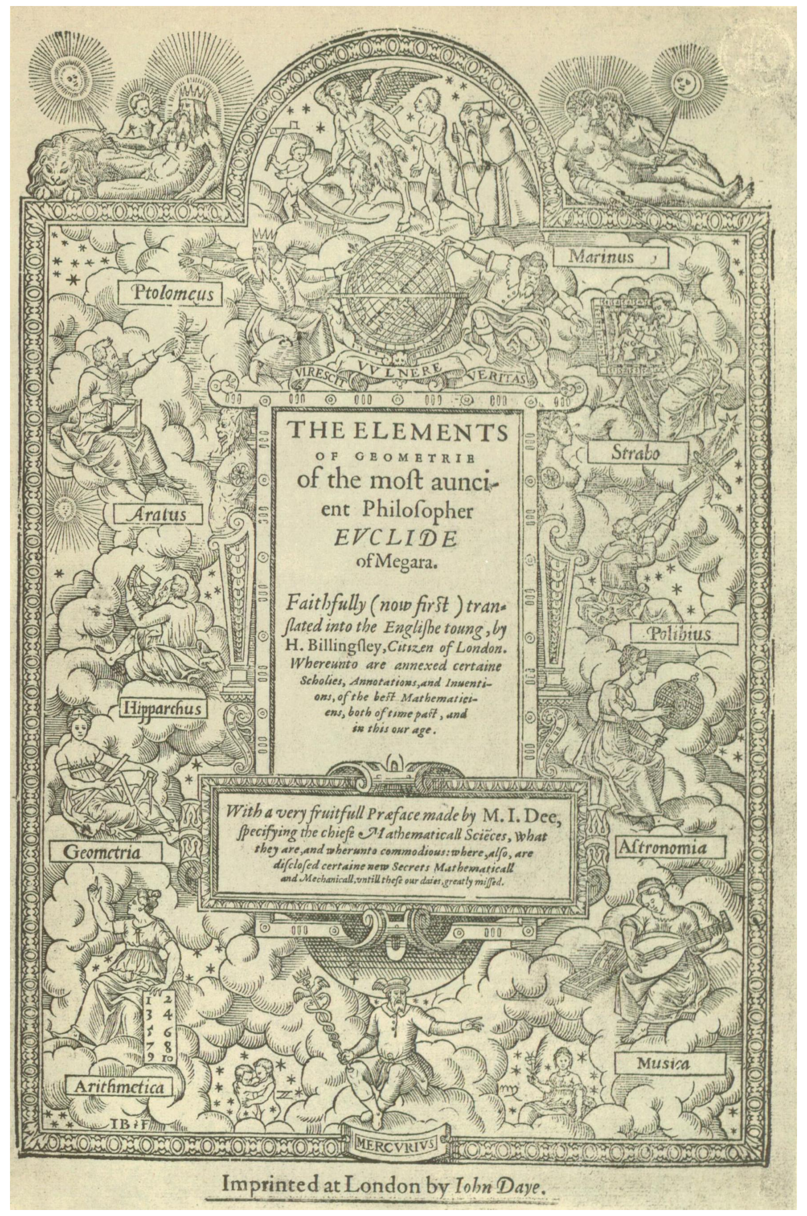
His idea of logic:

- unambiguous statements
- deductive reasoning
- *first principles* approach

Euclid ~325 BCE



Mathematical incarnation of Aristotelian logic



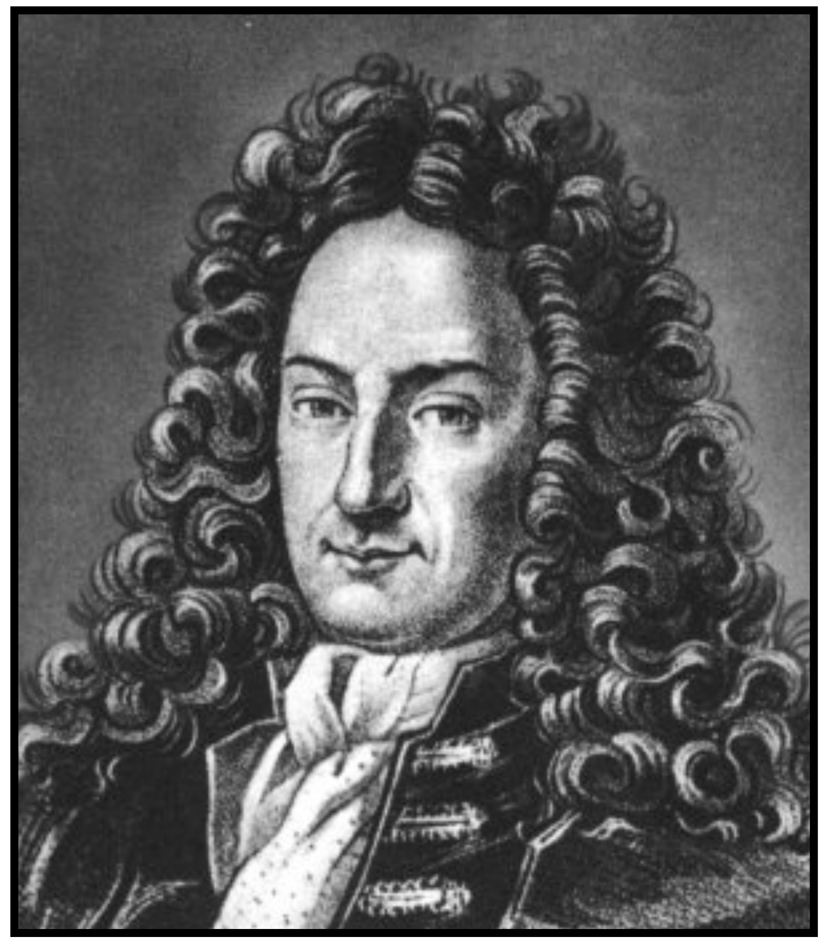
THE ELEMENTS
OF GEOMETRIE
of the moſt aunci-
ent Philoſopher
EVCLIDE
of Megara.

Faithfully (now firſt) tran-
ſlated into the Engliſhe toung, by
H. Billingſley, Citizen of London.
Whereunto are annexed certaine
Scholies, Annotations, and Inventi-
ons, of the beſt Mathematici-
ens, both of time paſt, and
in this our age.

With a very fruitfull Præface made by M. I. Dee,
ſpecifying the chiefe Mathematicall Sciēces, what
they are, and wherunto commodious: where, alſo, are
diſcloſed certaine new Secrets Mathematicall
and Mechanicall, vntill theſe our daies, greatly miſſed.

Imprinted at London by Iohn Daye.

Gottfried Leibniz 1646

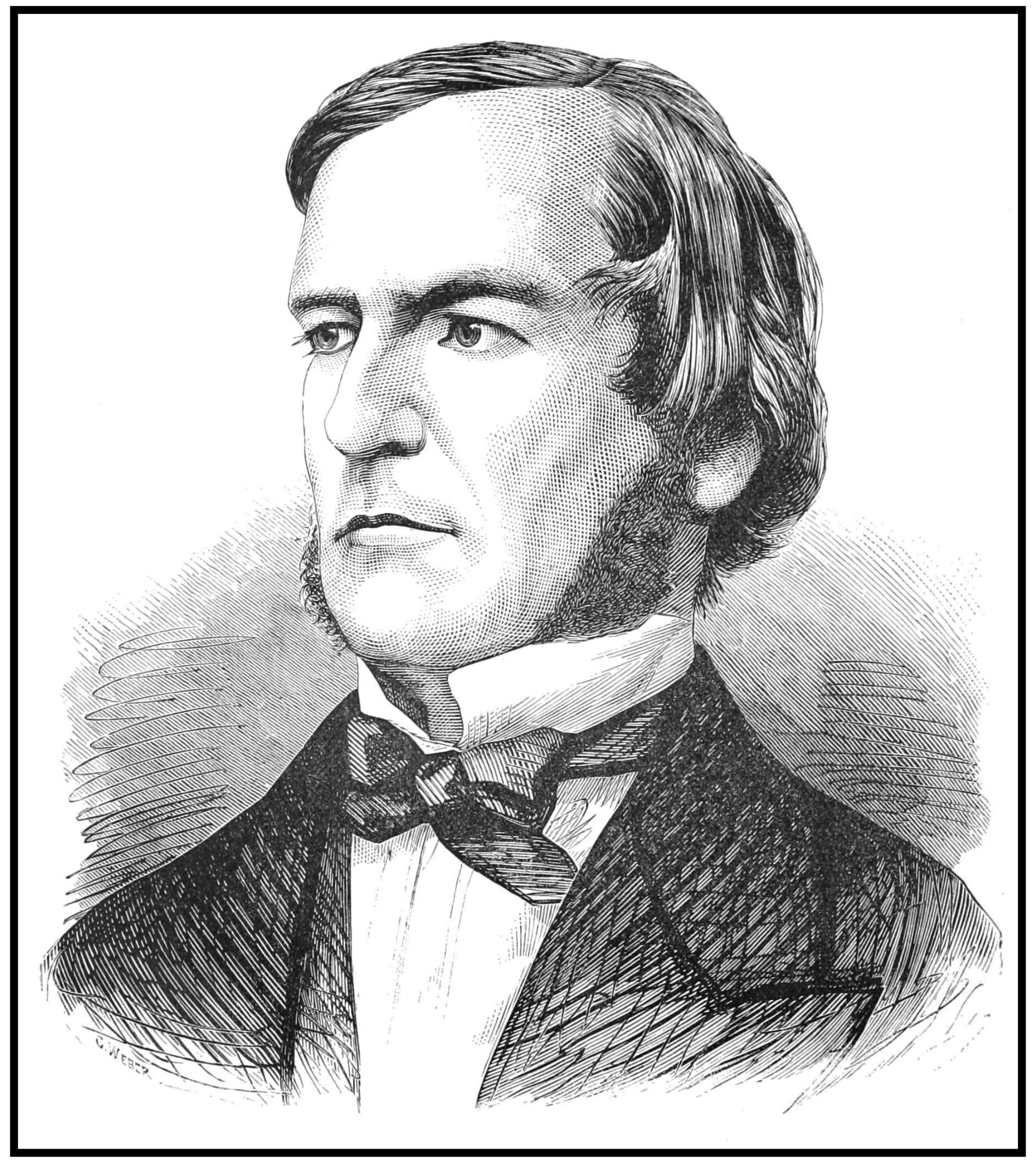


Envisioned an algebra/calculus for logic

(computational propositional logic)

"Let us calculate, without further ado, to see who is right."

George Boole 1815



Inventor of Propositional Calculus

Variables have value True/False (or 0/1).

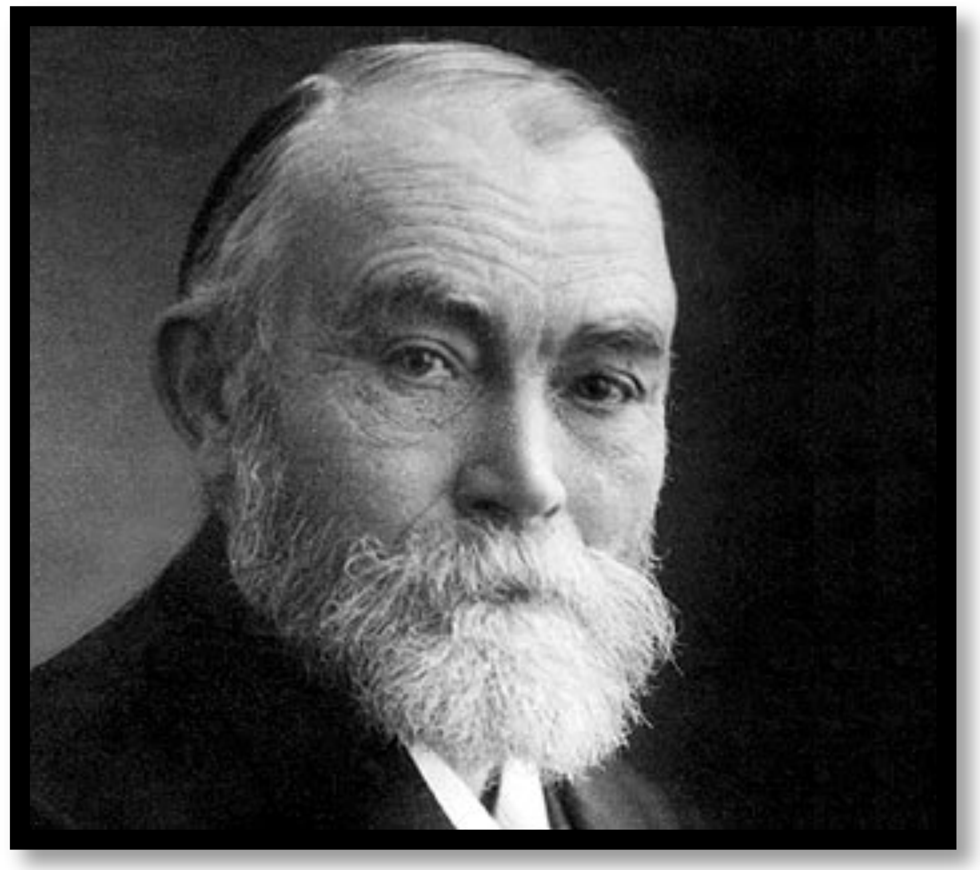
$$\neg(x \wedge y) = \neg x \vee \neg y$$

Georg Cantor 1845

Father of Set Theory

The person who dared to tackle infinity head-on.

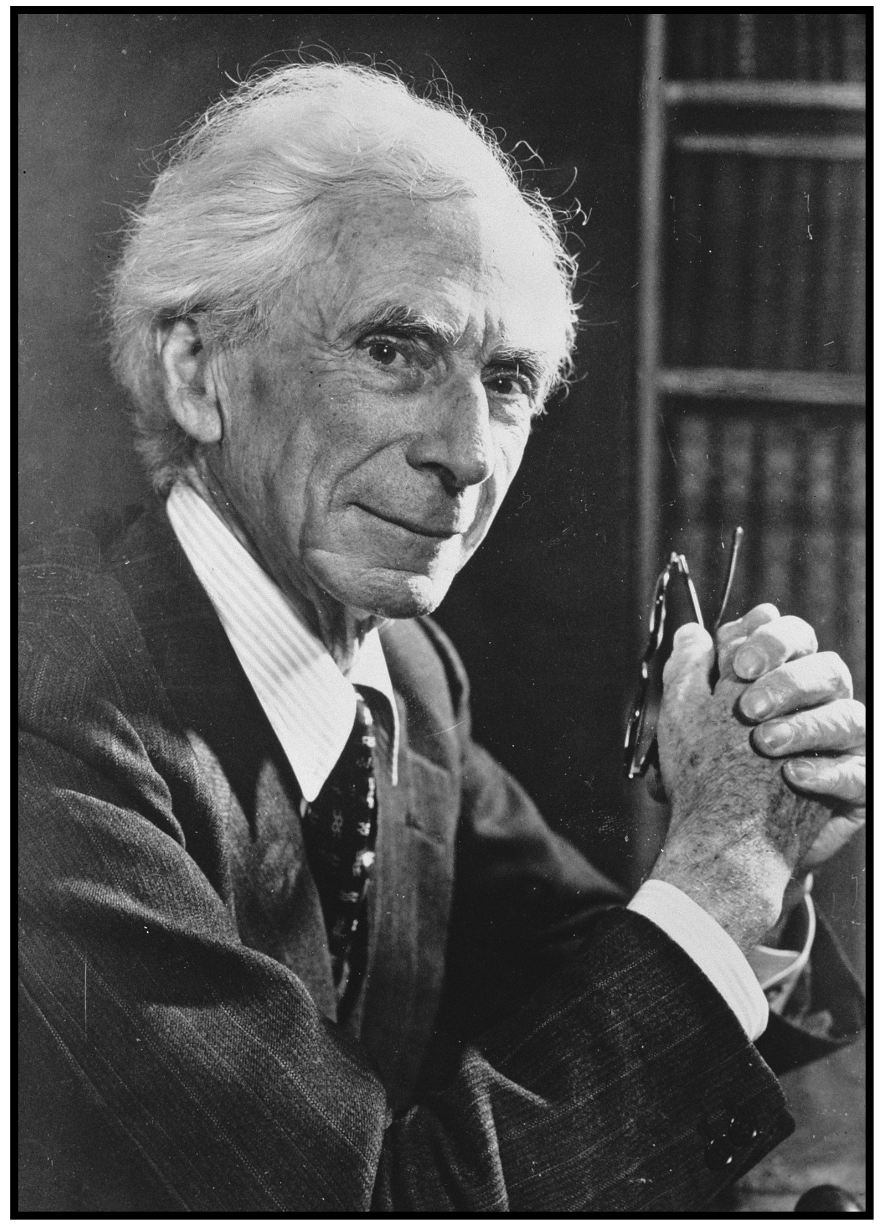
Gottlob Frege 1848



Lays the foundation for **First Order Logic** (predicate calculus).

Proposes axioms for set theory.

Spends 10 years writing two thick books about the system.



"Consider the set of all sets that do not contain themselves.

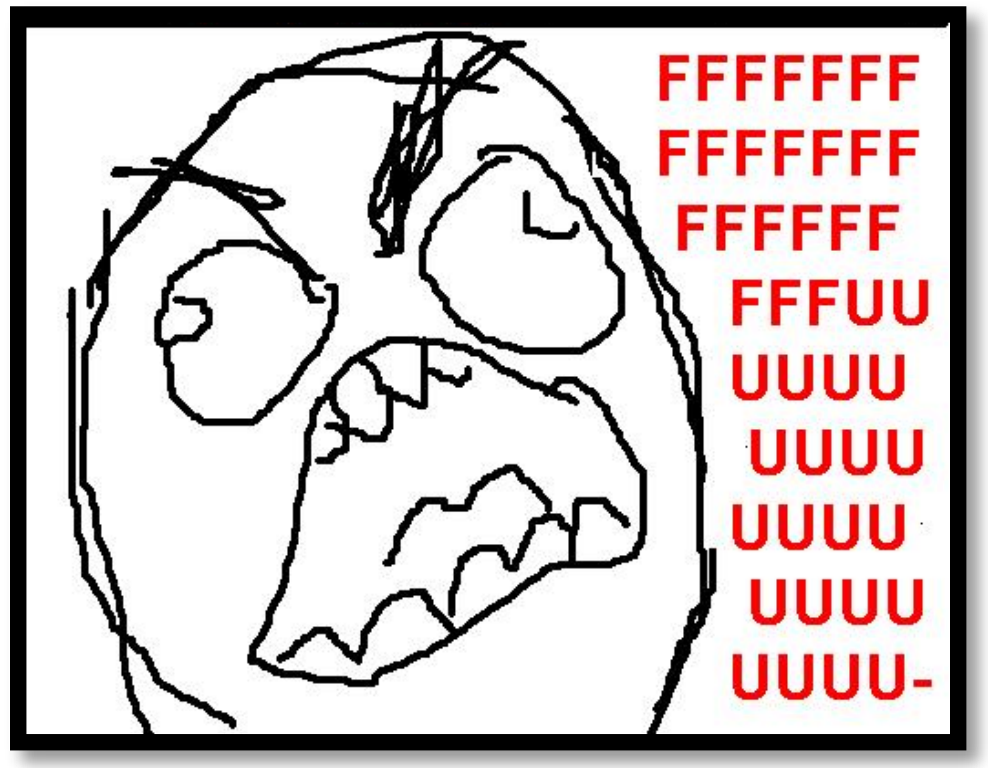
$D = \{\text{set } X : X \notin X\}$.

So for any set Y: $Y \in D$ **iff** $Y \notin Y$.

Setting $Y = D$: $D \in D$ **iff** $D \notin D$.

Inconsistency. **Boom!**"

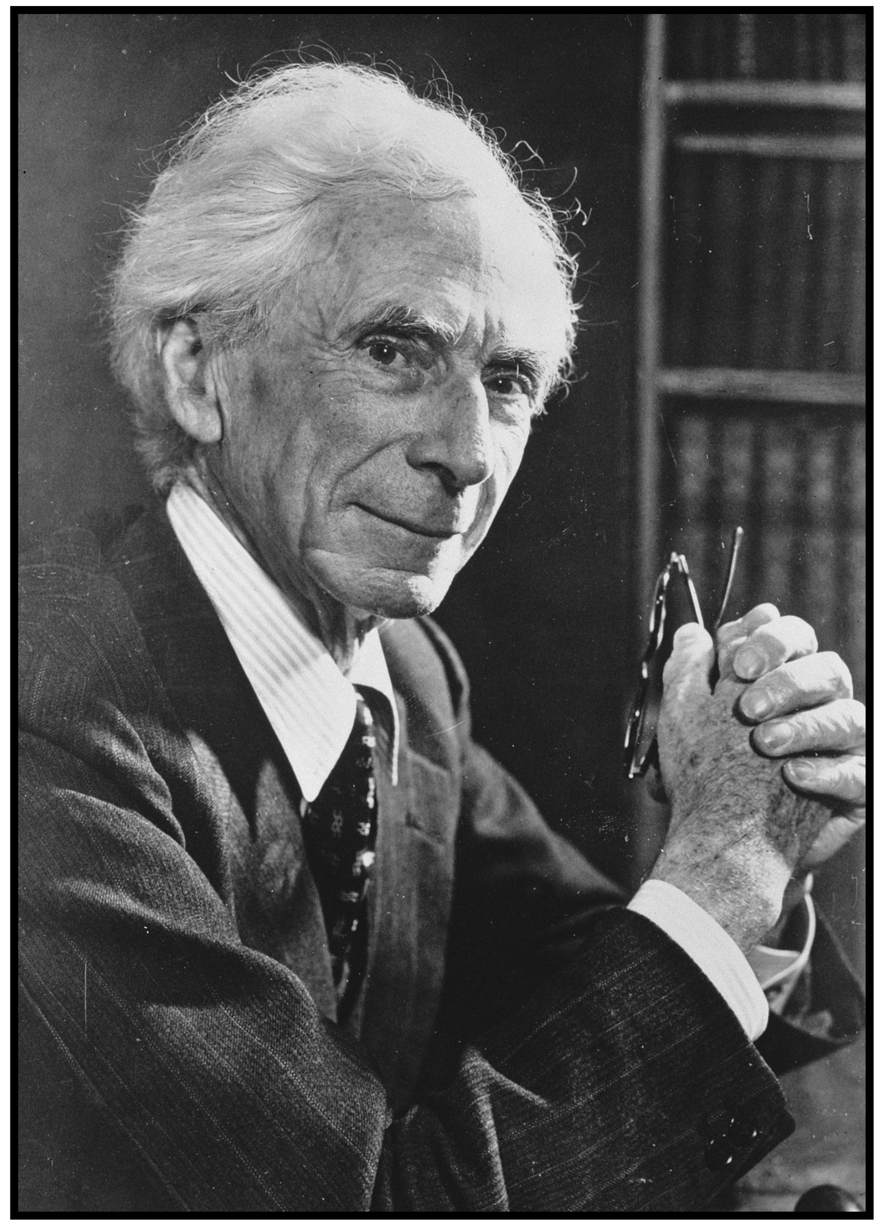
Gottlob Frege 1848



Lays the foundation for **First Order Logic** (predicate calculus).

Proposes axioms for set theory.

Spends 10 years writing two thick books about the system.



"Consider the set of all sets that do not contain themselves.

$D = \{\text{set } X : X \notin X\}$.

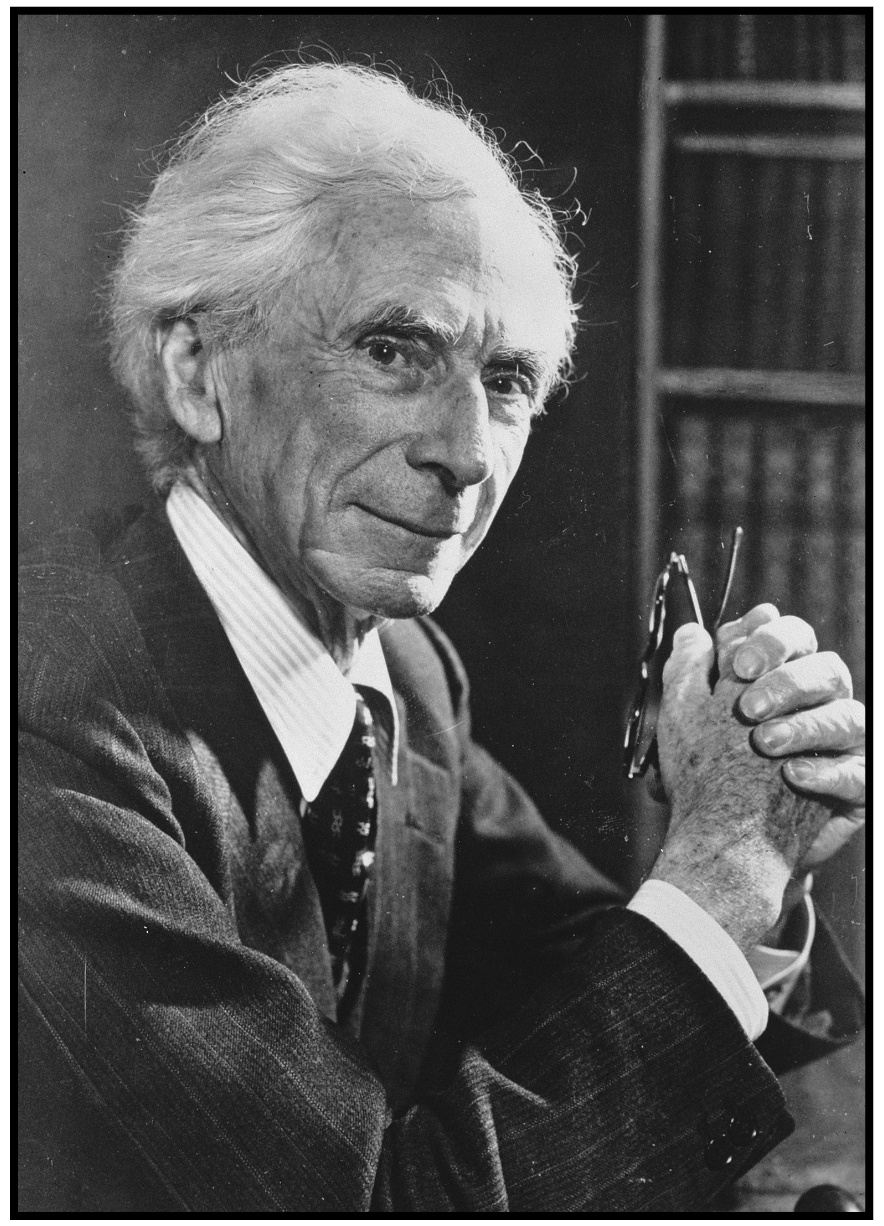
So for any set Y: $Y \in D$ **iff** $Y \notin Y$.

Setting $Y = D$: $D \in D$ **iff** $D \notin D$.

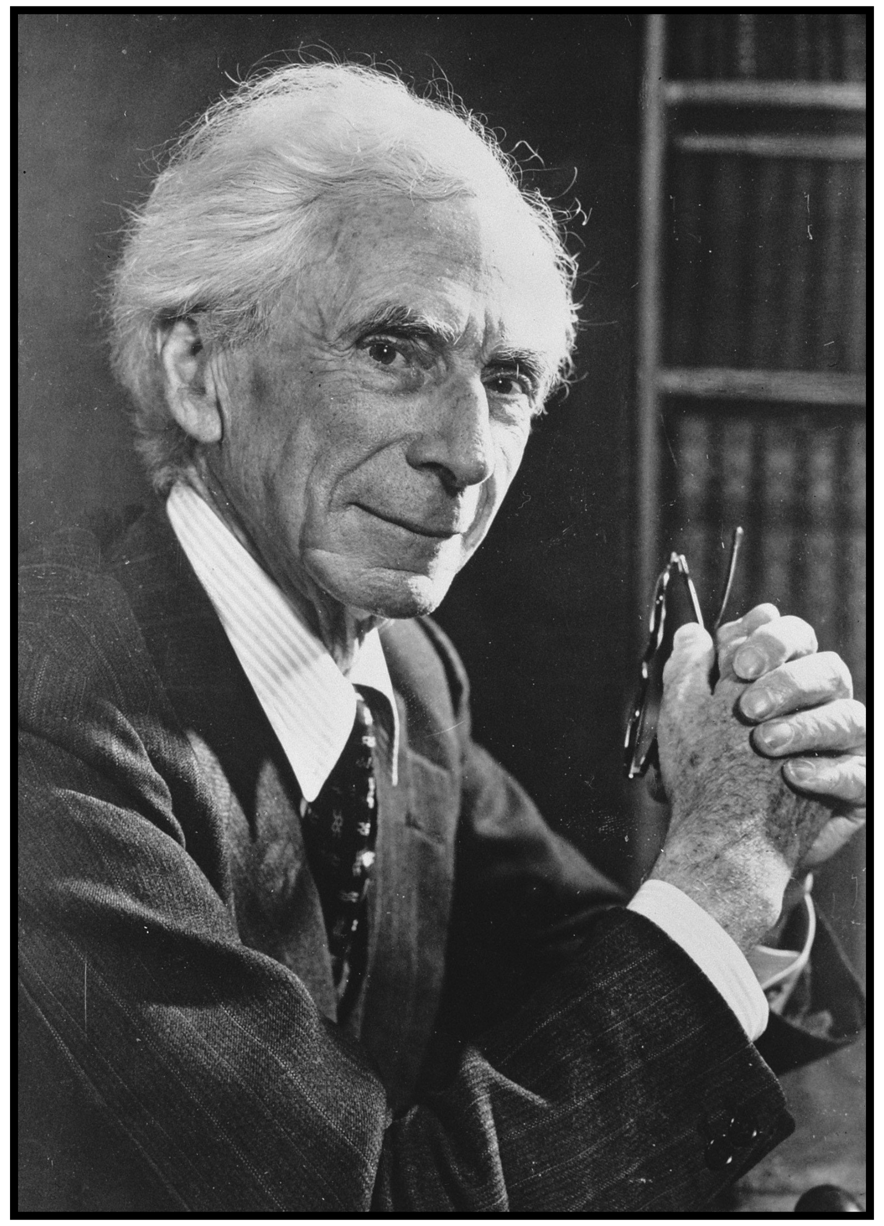
Inconsistency. **Boom!**"

Russell: "As I think about acts of integrity and grace, I realise that there is nothing in my knowledge to compare to Frege's dedication to truth. His entire life's work was on the verge of completion, much of his work had been ignored to the benefit of men infinitely less capable, his second volume was about to be published, and upon finding that his fundamental assumption was in error, he responded with intellectual pleasure, clearly submerging any feelings of disappointment. It was almost superhuman, and a telling indication of that of which men are capable if their dedication is to creative work and knowledge instead of cruder efforts to dominate and be known."

Bertrand Russell 1872



Alfred North Whitehead 1861



Principia Mathematica, Volume 2

86 CARDINAL ARITHMETIC [PART III

*110·632. $\vdash : \mu \in \mathrm{NC} \,.\supset.\, \mu +_c 1 = \hat{\xi}\{(\exists y) \,.\, y \in \xi \,.\, \xi - \iota' y \in \mathrm{sm}``\mu\}$

Dem.

$\vdash .$ *110·631 . *51·211·22 . $\supset$

$\vdash : \mathrm{Hp} \,.\supset.\, \mu +_c 1 = \hat{\xi}\{(\exists \gamma, y) \,.\, \gamma \in \mathrm{sm}``\mu \,.\, y \in \xi \,.\, \gamma = \xi - \iota' y\}$

[*13·195] $= \hat{\xi}\{(\exists y) \,.\, y \in \xi \,.\, \xi - \iota' y \in \mathrm{sm}``\mu\} : \supset \vdash .$ Prop

*110·64. $\vdash . 0 +_c 0 = 0$ [*110·62]

*110·641. $\vdash . 1 +_c 0 = 0 +_c 1 = 1$ [*110·51·61 . *101·2]

*110·642. $\vdash . 2 +_c 0 = 0 +_c 2 = 2$ [*110·51·61 . *101·31]

*110·643. $\vdash . 1 +_c 1 = 2$

Dem.

$\vdash .$ *110·632 . *101·21·28 . $\supset$

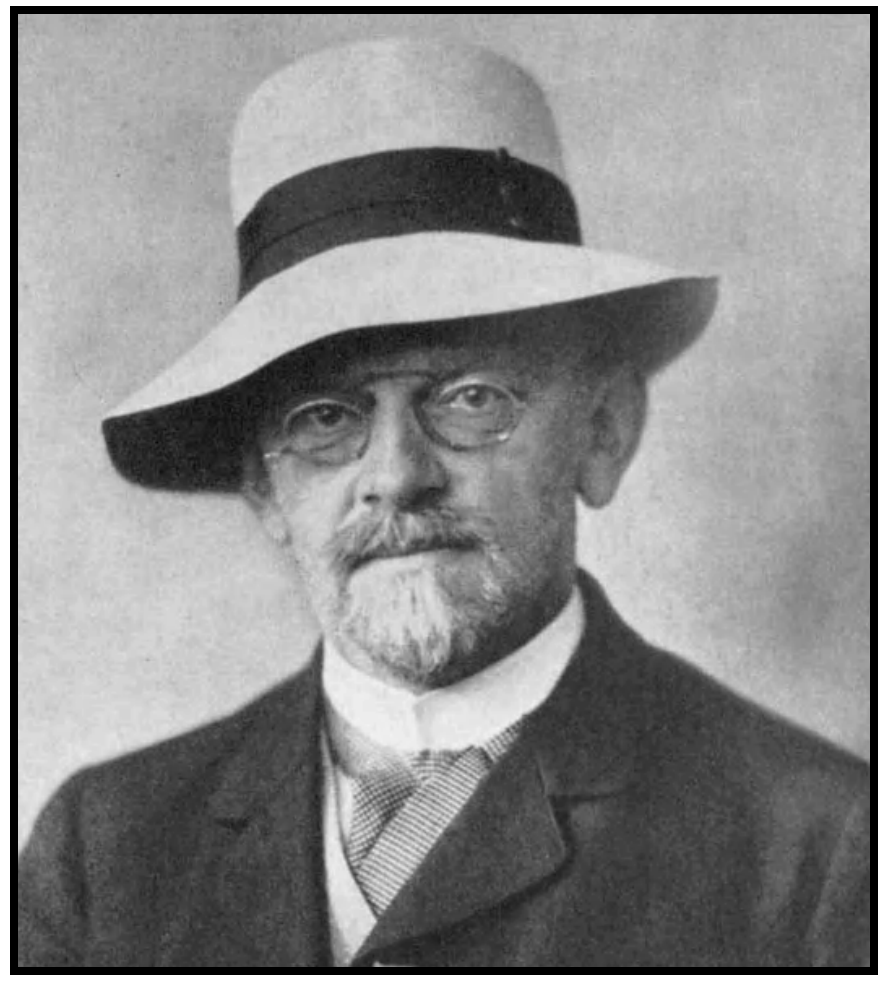
$\vdash . 1 +_c 1 = \hat{\xi}\{(\exists y) \,.\, y \in \xi \,.\, \xi - \iota' y \in 1\}$

[*54·3] $= 2 \,.\supset \vdash .$ Prop

The above proposition is occasionally useful. It is used at least three times, in *113·66 and *120·123·472.

Writing a proof like this is like writing a computer program in machine language.

David Hilbert 1862



Hilbert's Program

- A precise formal language manipulated according to well-defined rules.
- Completeness & Consistency:
  A proof that for all statements S, exactly one of S or $\neg S$ is provable.
- Entscheidungsproblem:
  An algorithm for determining the truth of any statement.

Hilbert System

FOL deductive calculus (FOL + deduction rules)

For us there is no ignorabimus, and in my opinion none whatever in natural science. In opposition to the foolish ignorabimus our slogan shall be "We must know - we will know."

Kurt Gödel 1906

Completeness Theorem

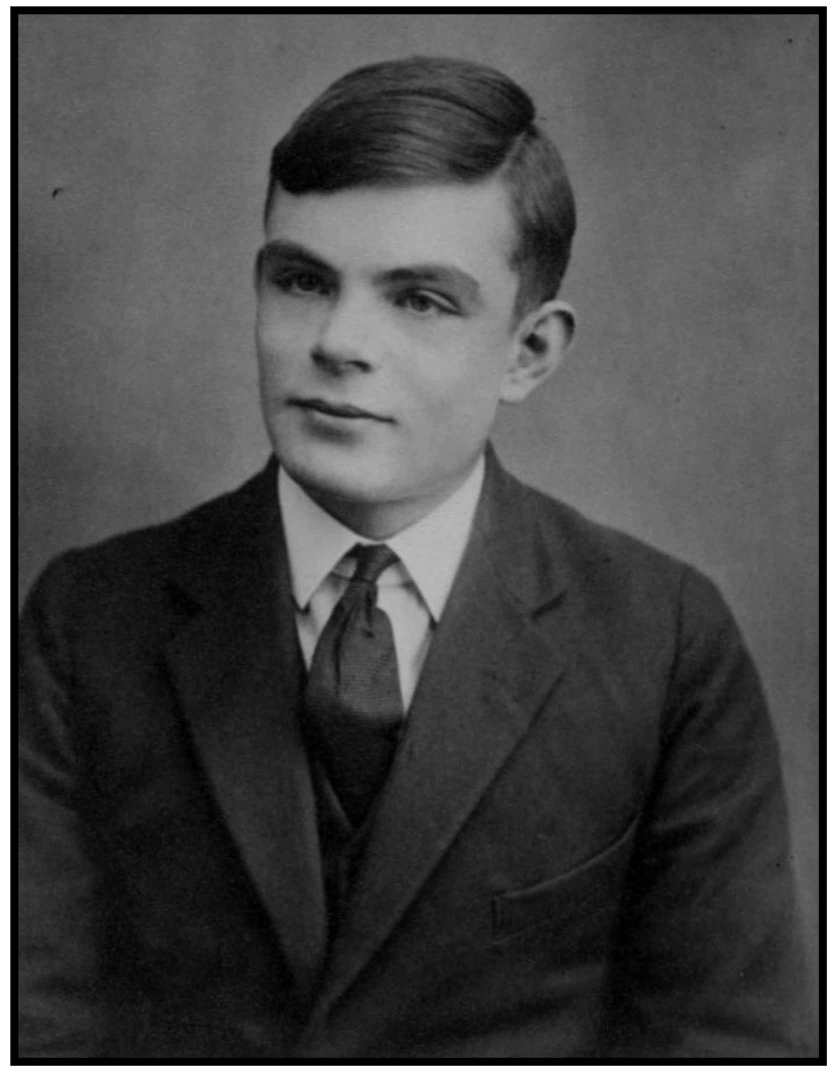
Any statement that is a logical consequence of the axioms can in fact be deduced/proved in the Hilbert system.

Incompleteness Theorem

There will always be some true statement that you cannot prove.

(The axioms will never be good enough.)

Alan Turing 1912



Father of Computer Science

Finds a satisfactory definition for "algorithm".

Shows there is no algorithm for Entscheidungsproblem.

LOGICOMIX

AN EPIC SEARCH FOR TRUTH

APOSTOLOS DOXIADIS AND CHRISTOS H. PAPADIMITRIOU
ART BY ALECOS PAPADATOS AND ANNIE Di DONNA

The Upshot:

You ***can*** rigorously formalize mathematical proofs.

There are limits to what can be proved.

Computer science is born. Computing revolution begins.

Computers elevate the significance of formal proofs.

One last story…

Lord Wacker von Wackenfels

(1550 - 1619)

Kepler Conjecture

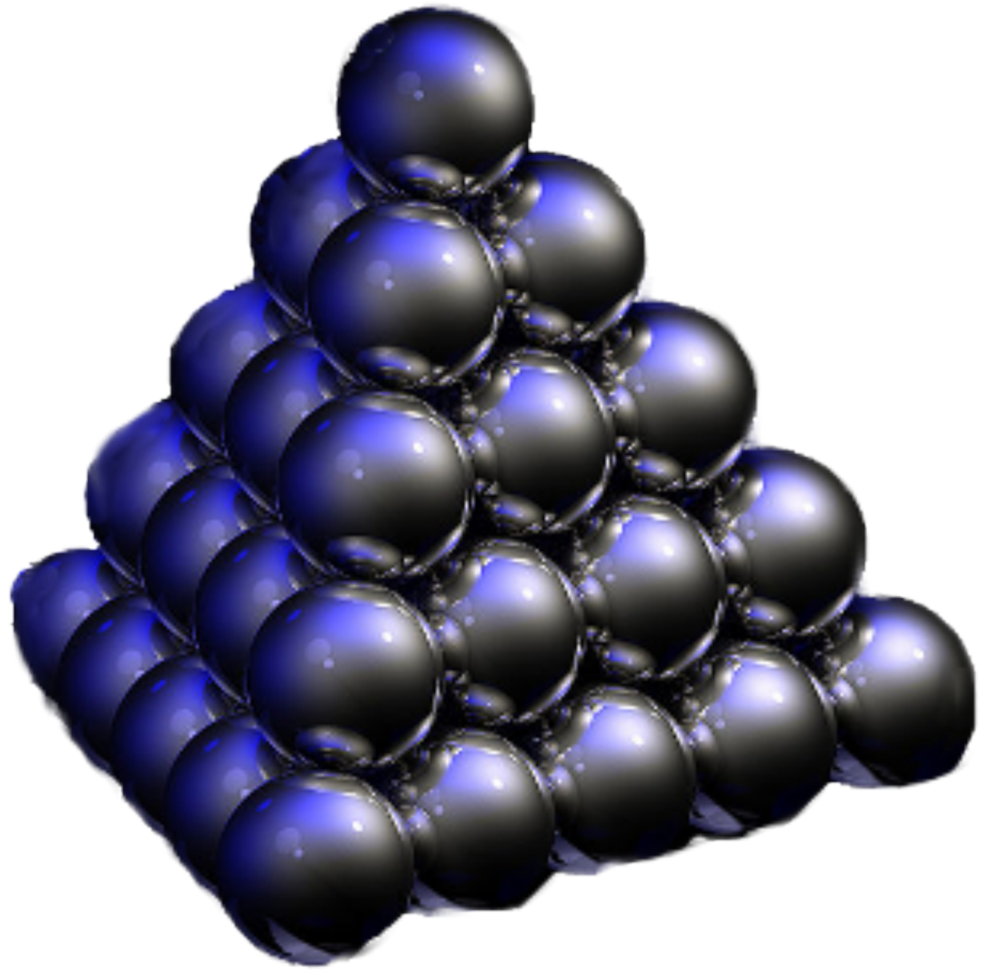
1611: Kepler as a New Year's present (!) for his patron, Lord Wacker von Wackenfels, wrote a paper with the following conjecture.

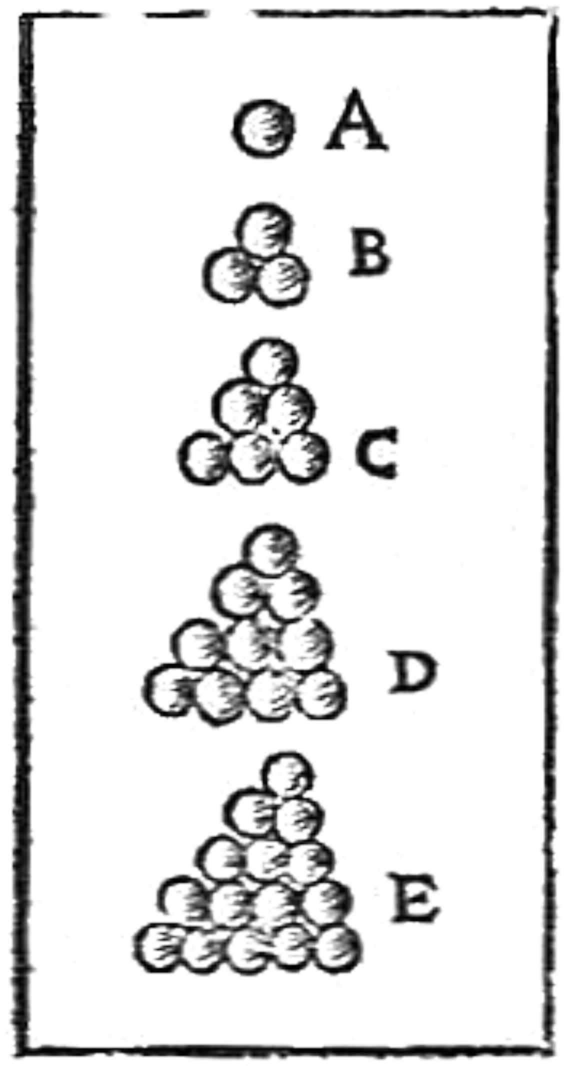
The densest way to pack oranges is like this:

Kepler Conjecture

1611: Kepler as a New Year's present (!) for his patron, Lord Wacker von Wackenfels, wrote a paper with the following conjecture.

The densest way to pack spheres is like this:





Kepler Conjecture

2005: Pittsburgher Tom Hales submits 120 page proof in *Annals of Math*.

Plus code to solve 100,000 optimization problems (~2000 hrs compute time).

Annals recruited a team of 20 refs.

They worked for 4 years.

Some quit. Some retired. One died.

In the end, they gave up.

They said they were “99% sure” it was a proof.

Kepler Conjecture

Hales: *"I will code up a completely formal axiomatic deductive proof, checkable by a computer."*

2004 - 2014: Open source "Project Flyspeck"

2015: Hales and 21 collaborators publish "A formal proof of the Kepler conjecture".

Computer-assisted proofs

Proof assistant softwares (e.g. HOL Light, Mizar, Coq, Isabelle, Agda) do 2 things:

1. Check that a formal axiomatic deductive proof is valid.
2. Help users code up such proofs.

Robbins Conjecture: (open for 63 years)
All Robbins algebras are Boolean algebras.

Proof by automated theorem prover EQP.

Formally proved theorems

Fundamental Theorem of Calculus *(Harrison)*

Fundamental Theorem of Algebra *(Milewski)*

Prime Number Theorem *(Avigad @ CMU, et al.)*

Gödel's Incompleteness Theorem *(Shankar)*

Jordan Curve Theorem *(Hales)*

Brouwer Fixed Point Theorem *(Harrison)*

Four Color Theorem *(Gonthier)*

Feit-Thompson Theorem *(Gonthier)*

Kepler Conjecture *(Hales++)*

…

What does this all mean for CS251?

What is a proof in CS251?

GORM territory

FORM

informal reasoning with real objects

start reasoning with mathematical objects

"formal" definitions, and deductions

more absolute formalism

What is a proof in CS251?

GORM territory

FORM

informal reasoning with real objects

start reasoning with mathematical objects

"formal" definitions, and deductions

more absolute formalism

Proof (CS251):

An argument, using precise definitions and logical reasoning, that convinces the reader that the assumptions lead to the desired conclusion.

What is a proof in CS251?

GORM territory

FORM

informal reasoning with real objects

start reasoning with mathematical objects

"formal" definitions, and deductions

more absolute formalism

Proof (CS251):

An argument, using precise definitions and logical reasoning, that **convinces the reader** that the assumptions lead to the desired conclusion.

What is a proof in CS251?

A proof is an argument that can withstand all criticisms from a highly caffeinated adversary (your TA).

FORM and Computation

Picture of FORM

Real World

Mathematical Reasoning (GORM)

computation

Applications

Abstract World

Mathematical Model

Explore Consequences

More on this later...