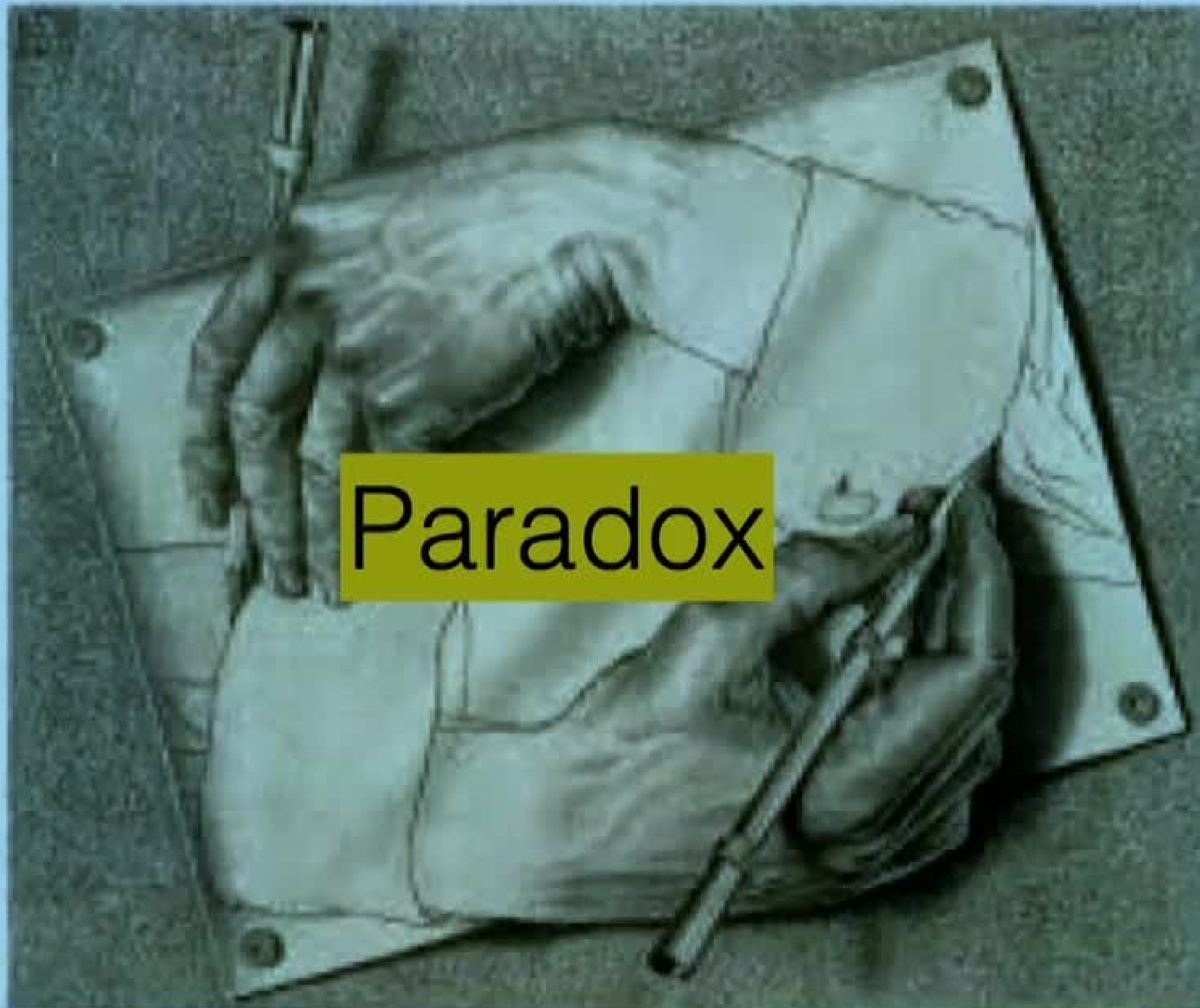
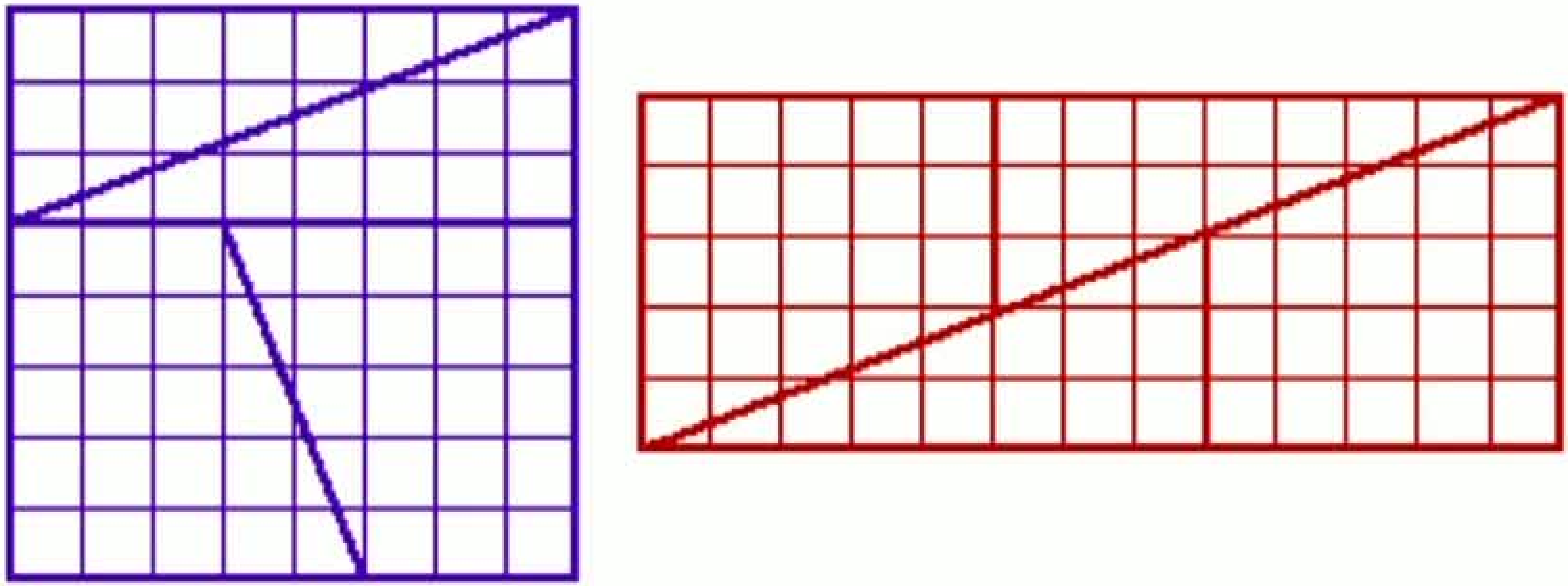

Paradox

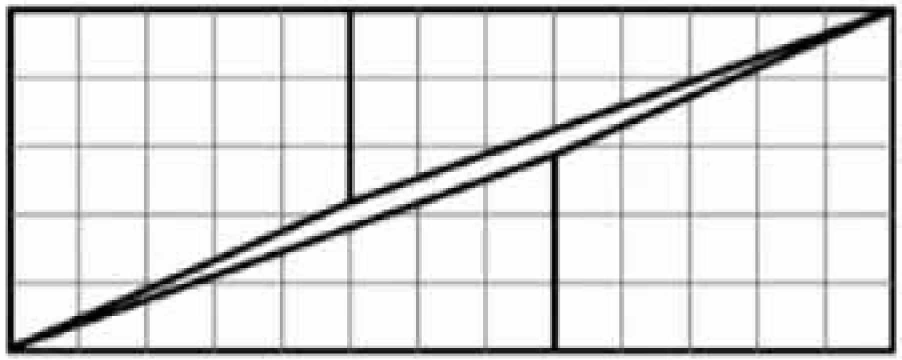
$$64 = 65$$

$$8 \times 8 = 5 \times 13$$



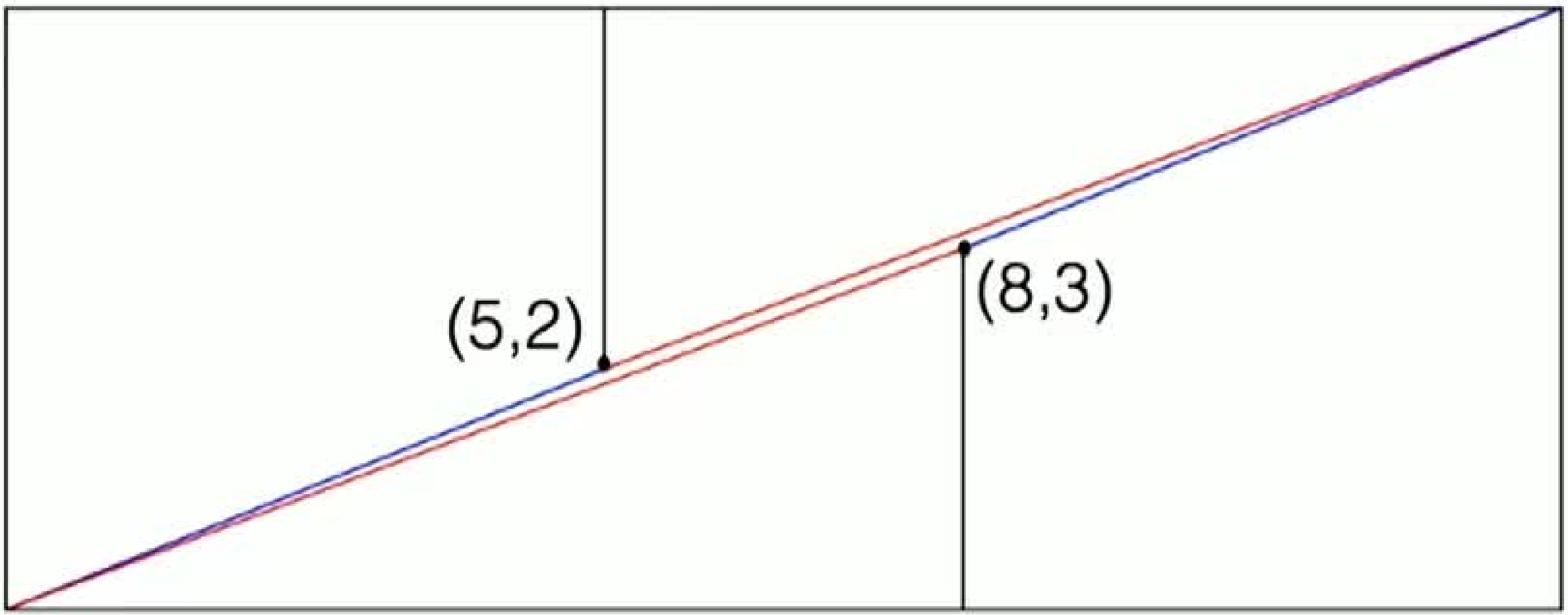
Schlomilch paradox (1868)

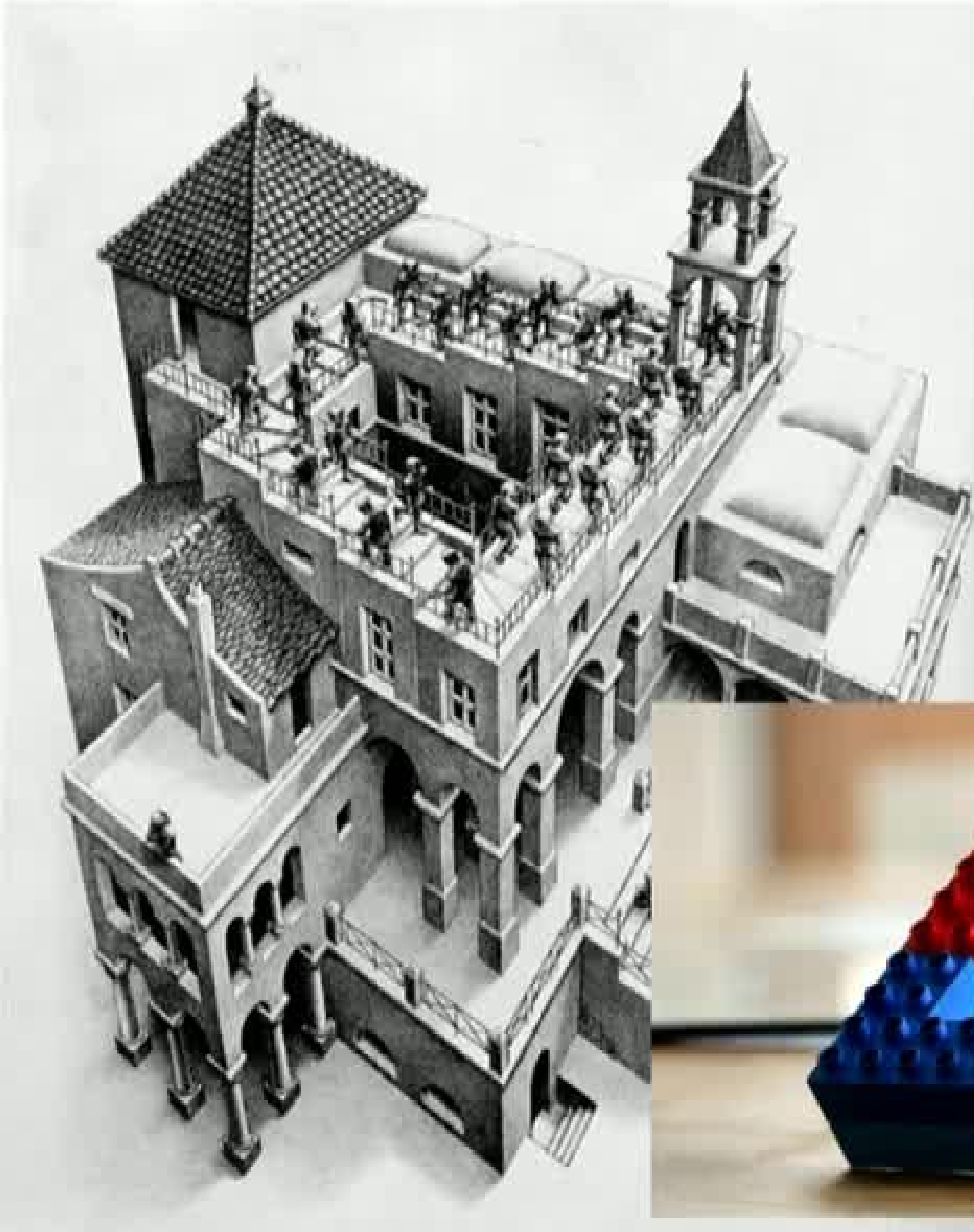
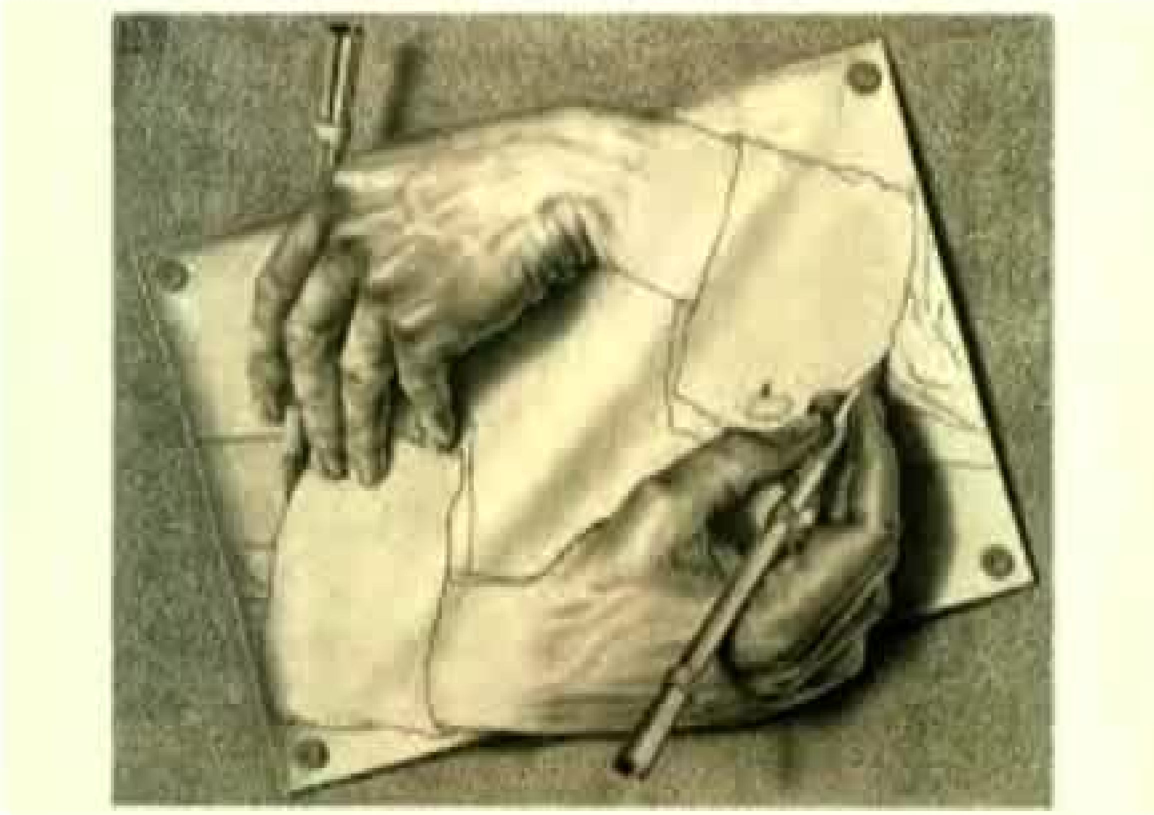
exaggerated

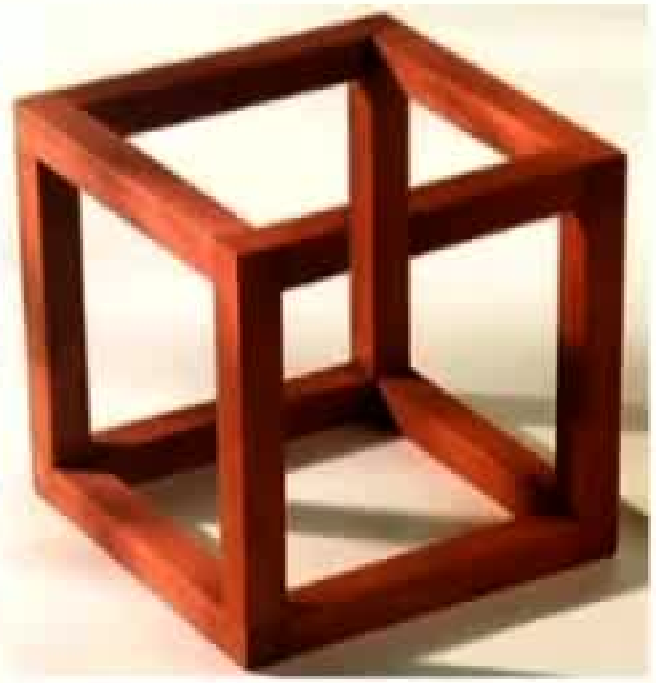


$$\begin{vmatrix} 8 & 5 \\ 3 & 2 \end{vmatrix} = 1.$$

accurate: 64 + 1 = 65

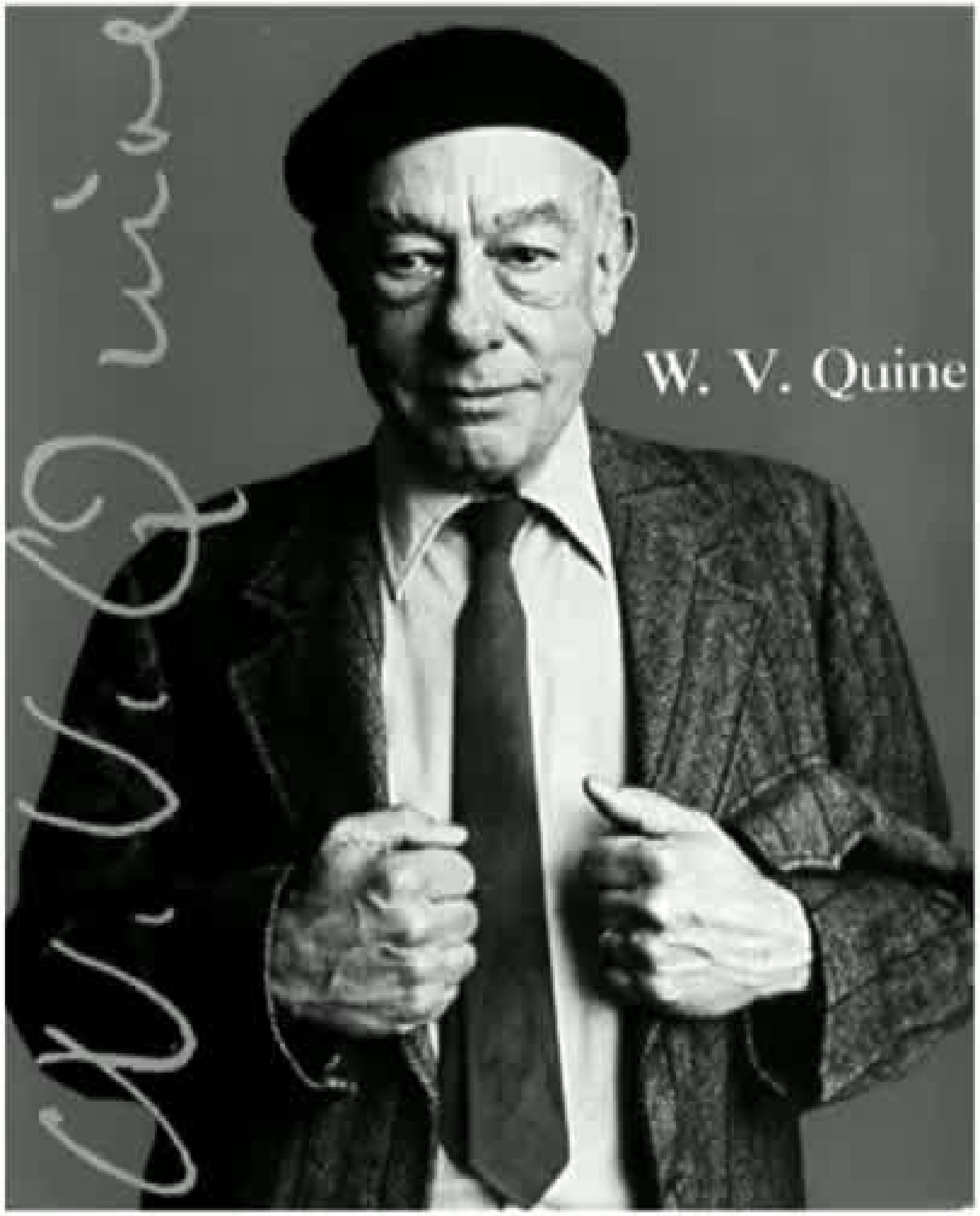




Paradox

- A paradox is a “conclusion that at first sounds absurd but that has an argument to sustain it.” — Quine



PARADOX

Some self-contradictory statements are amusing; others are profoundly puzzling. A few paradoxes have called for major reconstructions of the foundations of logic and mathematics

by W. V. Quine

Frederic, the young protagonist of *The Pirates of Penzance*, has reached the age of 21 after passing only five birthdays. Several circumstances conspire to make this possible. Age is reckoned in elapsed time, whereas a birthday has to match the date of birth; and February 29 comes less frequently than once a year.

Granted that Frederic's situation is possible, wherein is it paradoxical? Merely in its initial air of absurdity. The likelihood that a man will be more than *n* years old on his *n*th birthday is as little as one to 1,460, or slightly better if we

in 1918. In a certain village there is a man, so the paradox runs, who is a barber; this barber shaves all and only those men in the village who do not shave themselves. Query: Does the barber shave himself?

Any man in this village is shaved by the barber if and only if he is not shaved by himself. Therefore in particular the barber shaves himself if and only if he does not. We are in trouble if we say the barber shaves himself and we are in trouble if we say he does

Now compare the two Frederic's situation seemed

quiesce in the sweeping denial just as we acquiesced in the possibility, absurd on first exposure, of Frederic's being so much more than five years old on his fifth birthday.

Both paradoxes are alike, after all, in sustaining prima facie absurdities by conclusive argument. What is strange but true in the one paradox is that one can be 4*n* years old on one's *n*th birthday; what is strange but true in the other paradox is that no village can contain a

Homework: read this!

Grelling’s Paradox

- Autological adjectives are self-descriptive:
  - “short” is short
  - “English” is English
  - “polysyllabic” is polysyllabic
  - “adjectival” is adjectival
- Heterological adjectives are not self-descriptive:
  - “long” is not long
  - “German” is not German
  - “monosyllabic” is not monosyllabic
- Is “heterological” heterological?

Expect to get dizzy

- When you go to a horror film, you expect be frightened.
- When you go on the roller-coaster, you expect to be light-headed.
- When you workout at the gym, you expect physical pain.
- When you go to a talk on paradox, you expect to get dizzy.

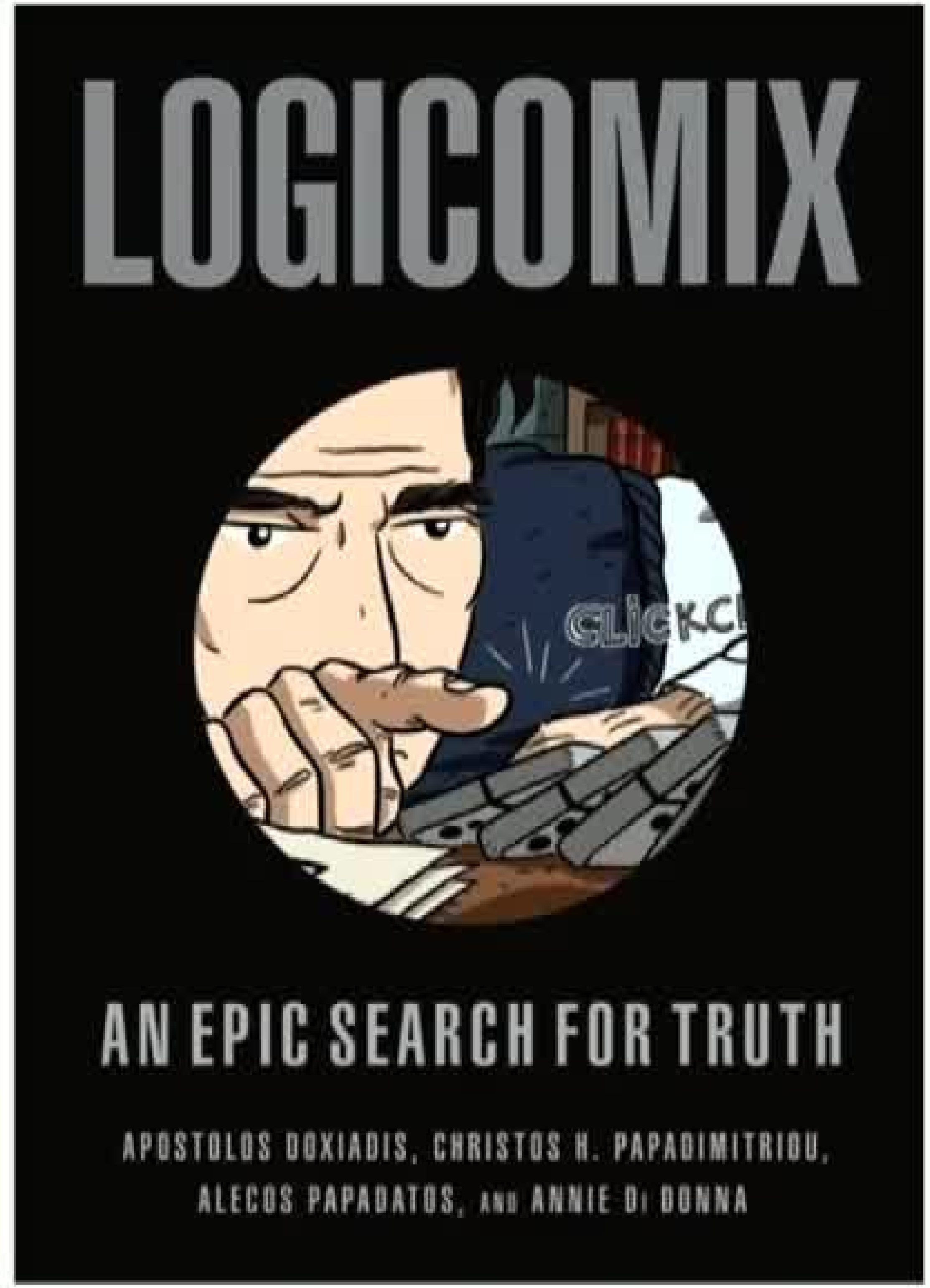
An exam paradox

- An exam has 40 multiple choice questions A,B,C,D.
- “A” is the correct answer on exactly 10 of the first 39 questions.
- Question 40. How many questions on this exam have correct answer “A”?
  - A. At most 10.
  - B. 11 to 20.
  - C. 21 to 30.
  - D. 31 to 40.

The Golden Age of Paradox

1901-1936

Homework: read this!

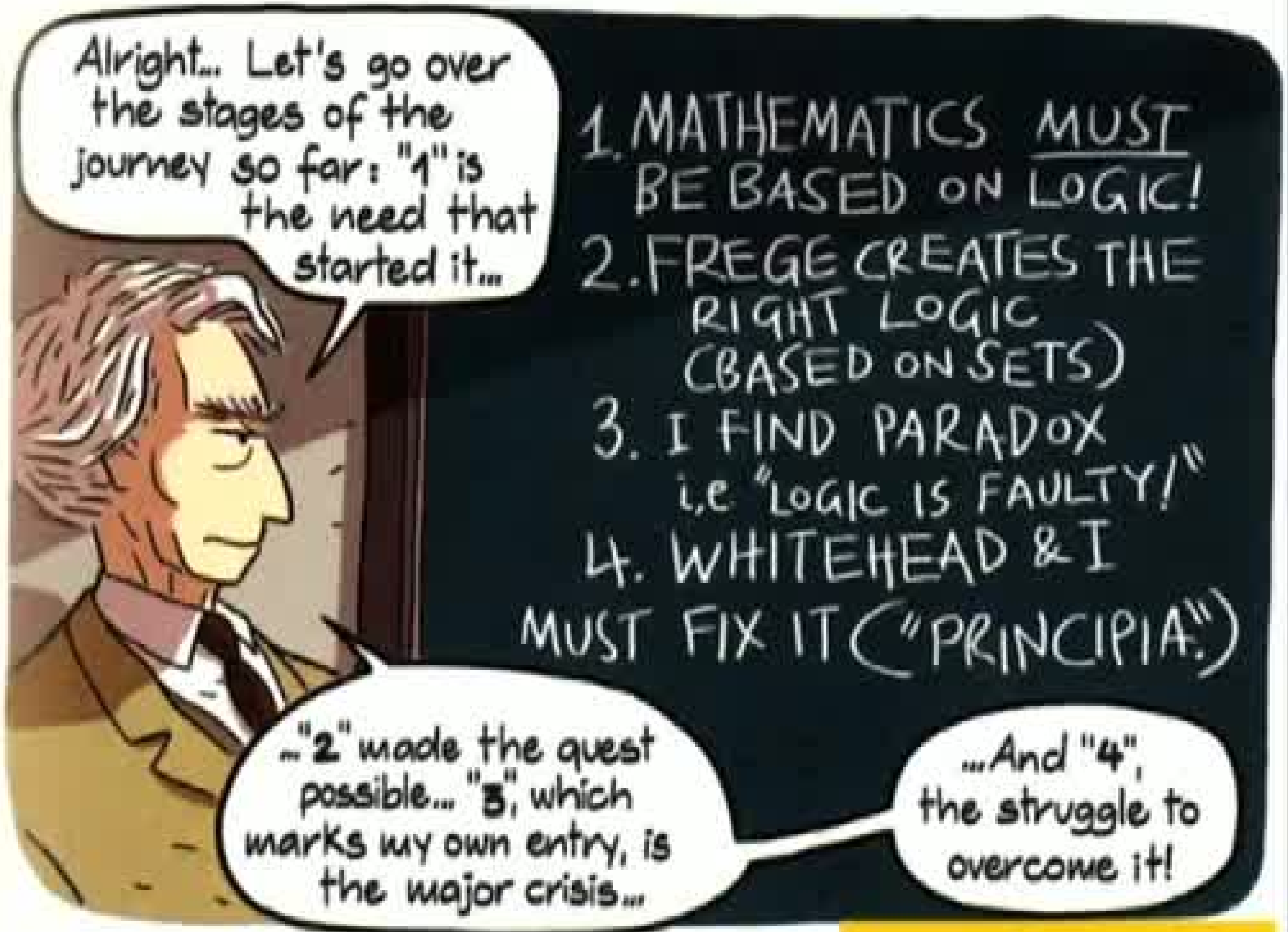


The Barber Paradox

- In a certain village, a male barber shaves exactly those men that do not shave themselves. Does the barber shave himself?

Russell's paradox

- X is the set of all sets that do not have themselves as members. Does X have itself as a member?

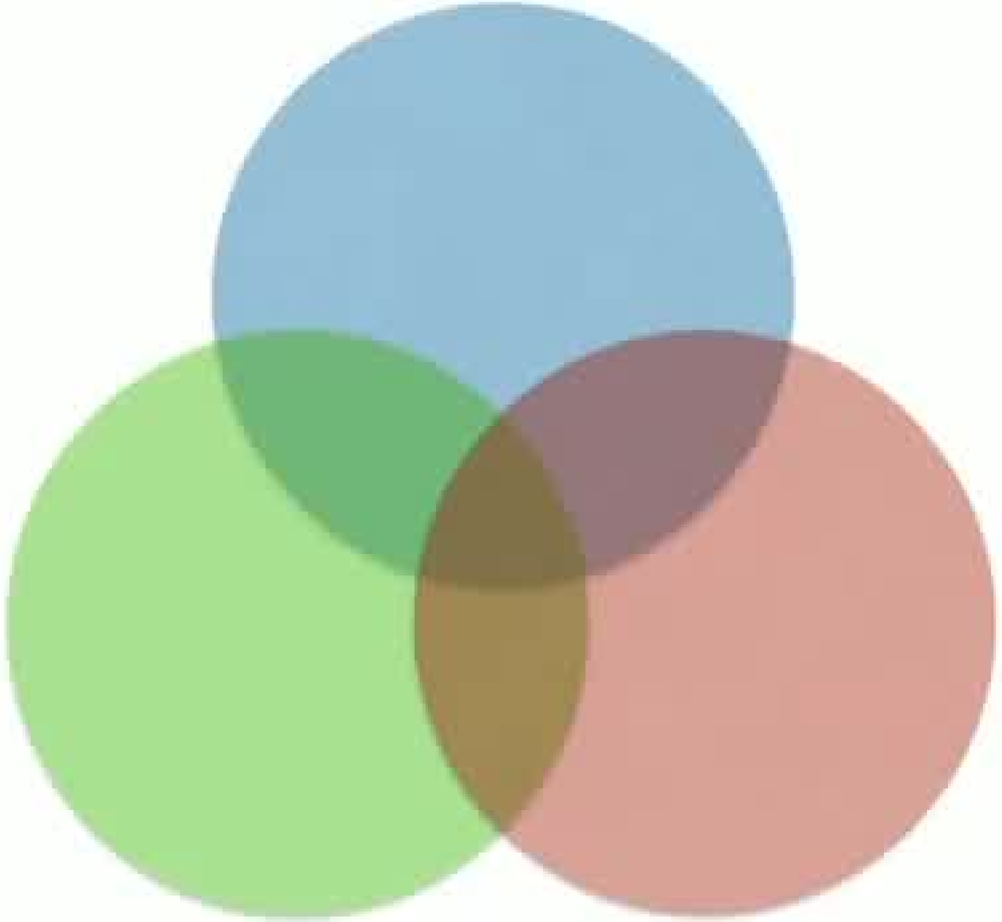


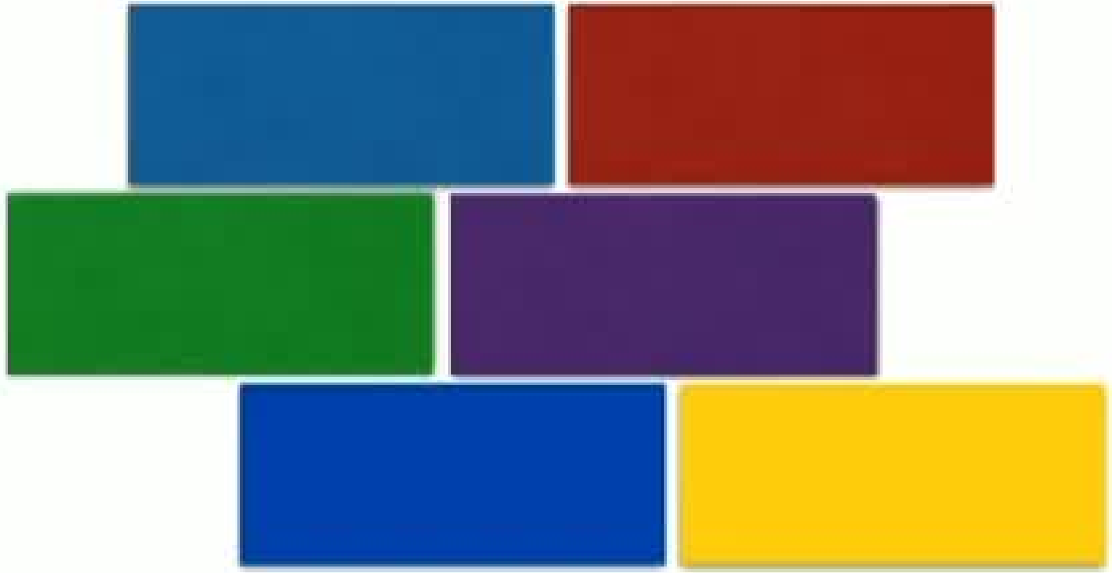
Logicomix

Two responses to Russell's paradox

Set Theory (Zermelo)

Type Theory (Russell)





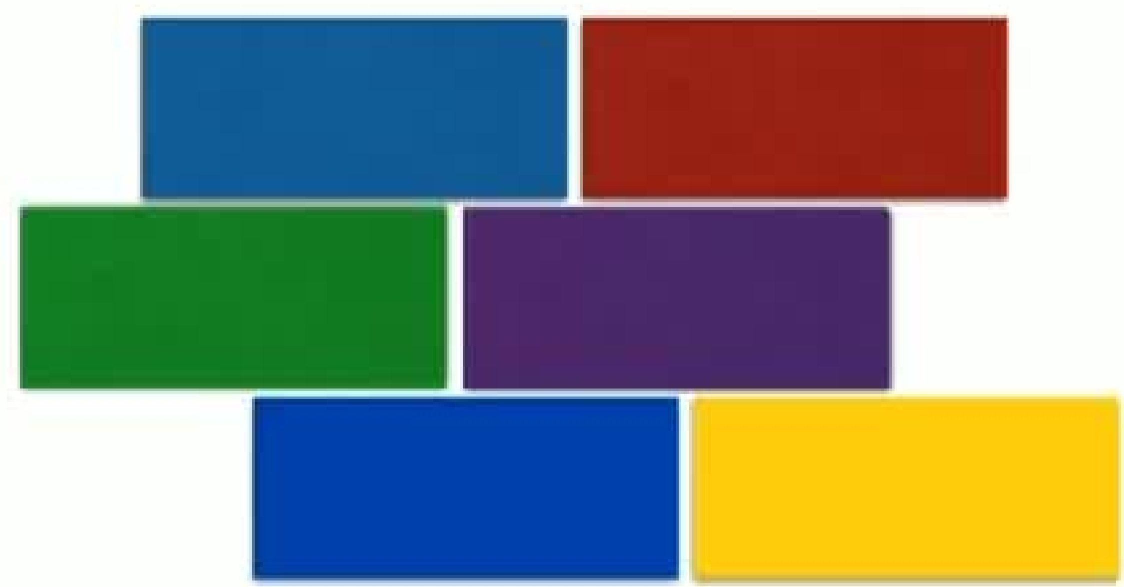
Sets mix.

Types never mix.

Barber paradox in type theory

- In a certain village, a male barber shaves exactly those men that do not shave themselves. Does the barber shave himself?
- Barbers are one type of person.
- Customers are another type of person.
- Types never mix.
- It is not grammatical to ask if a barber is also a customer.

Type Theory (Russell)

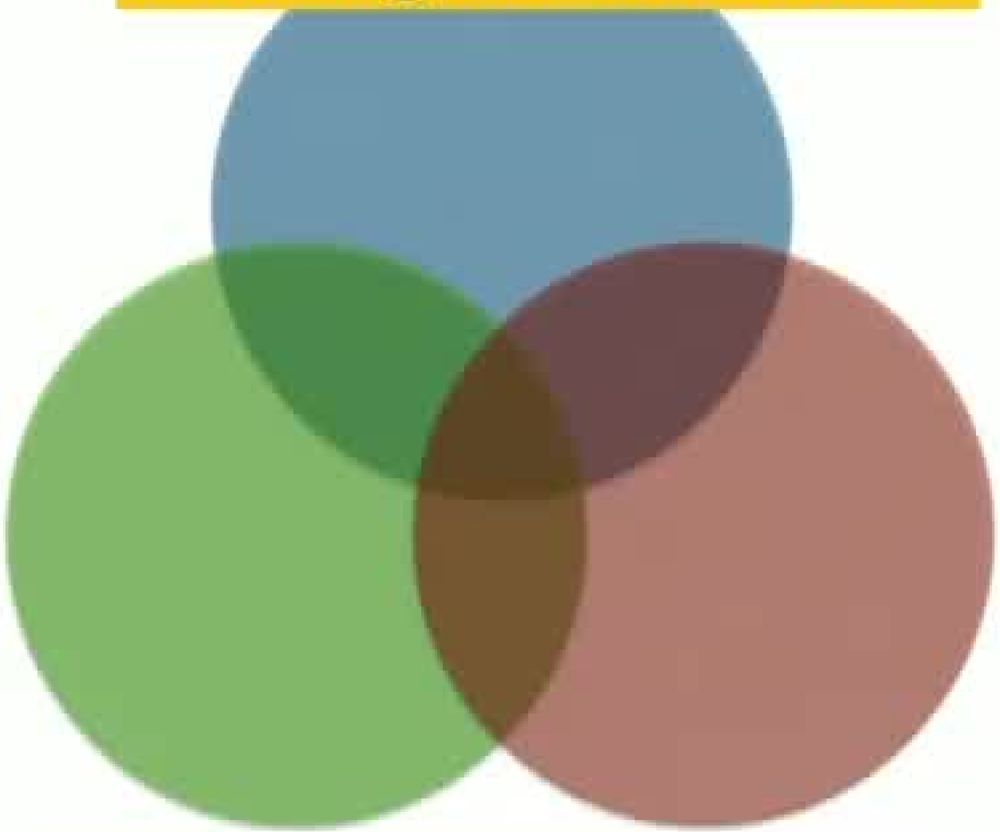


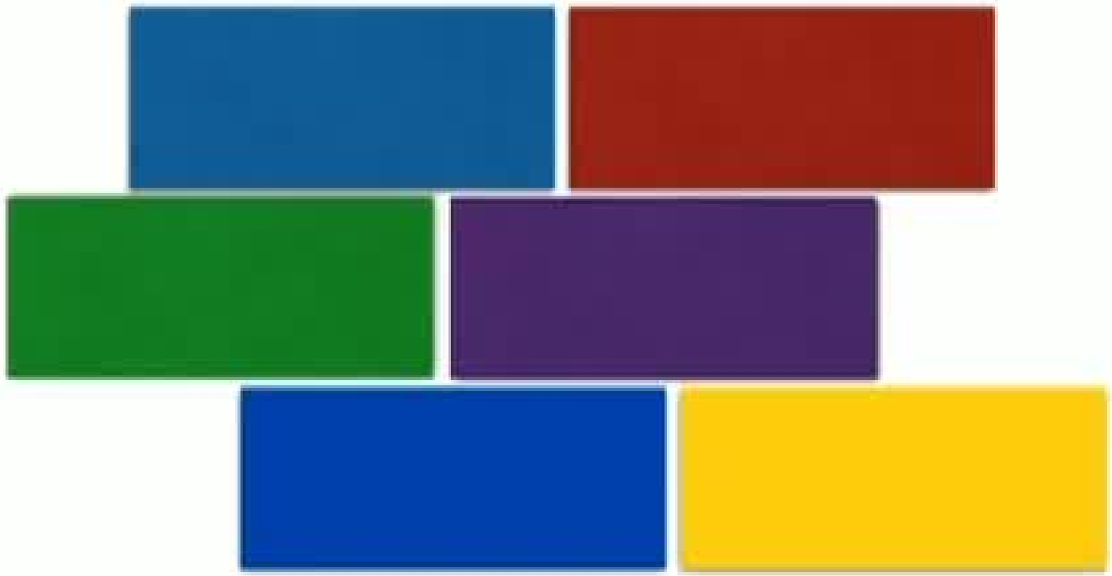
Two responses to Russell's paradox

X is the set of all sets that do not have themselves as members.

Too big for Zermelo!

Doesn't type check!



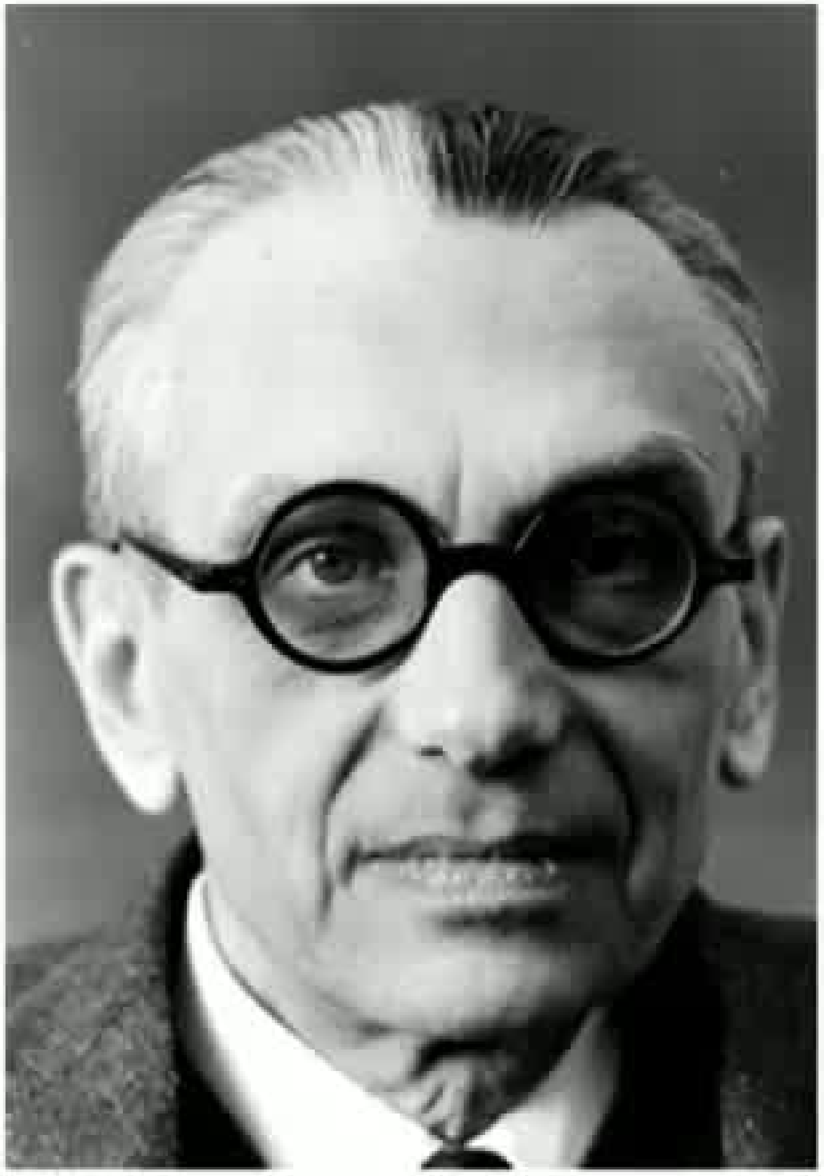


Set Theory (Zermelo)

Type Theory (Russell)

The Golden Age of Paradox
Goedel Incompleteness

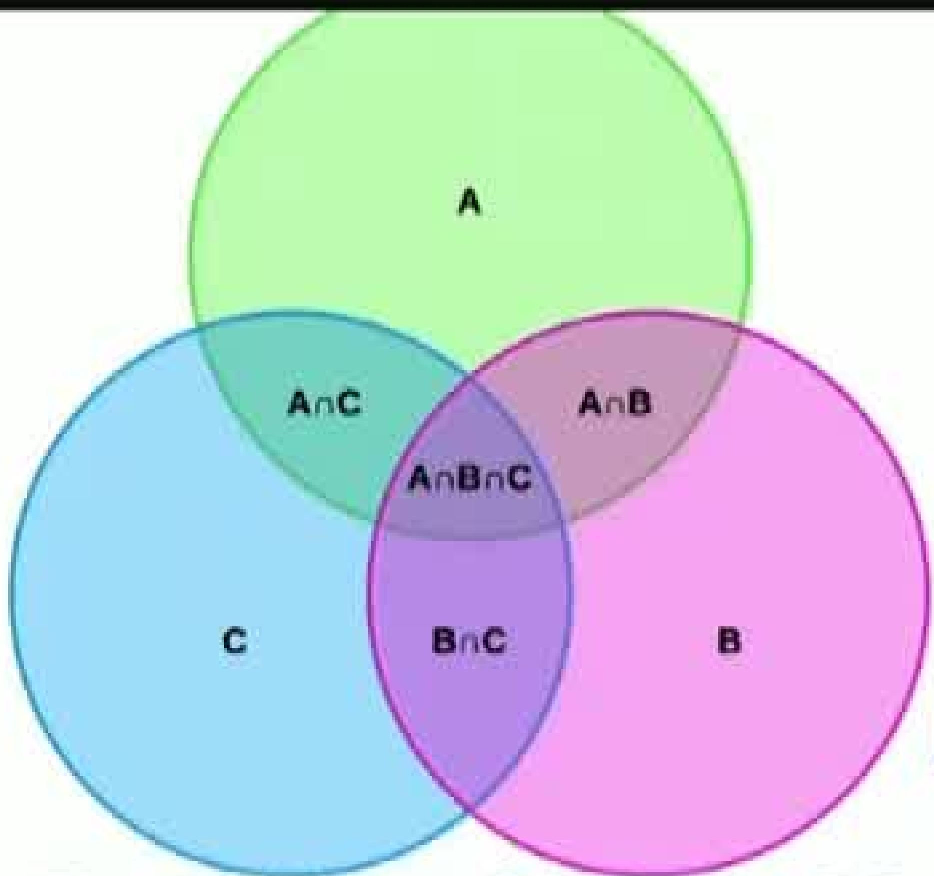
- Every sufficiently powerful deductive system contains a sentence that is true if and only if it is unprovable in that system.
- "On Formally Undecidable Propositions of **Principia Mathematica** and Related Systems I" (1931)

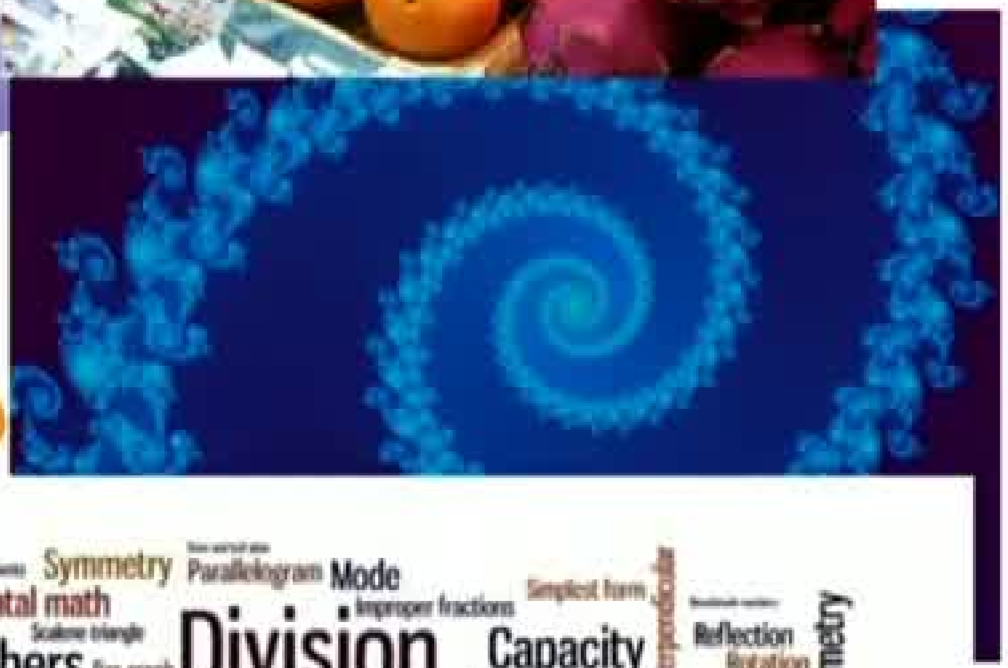


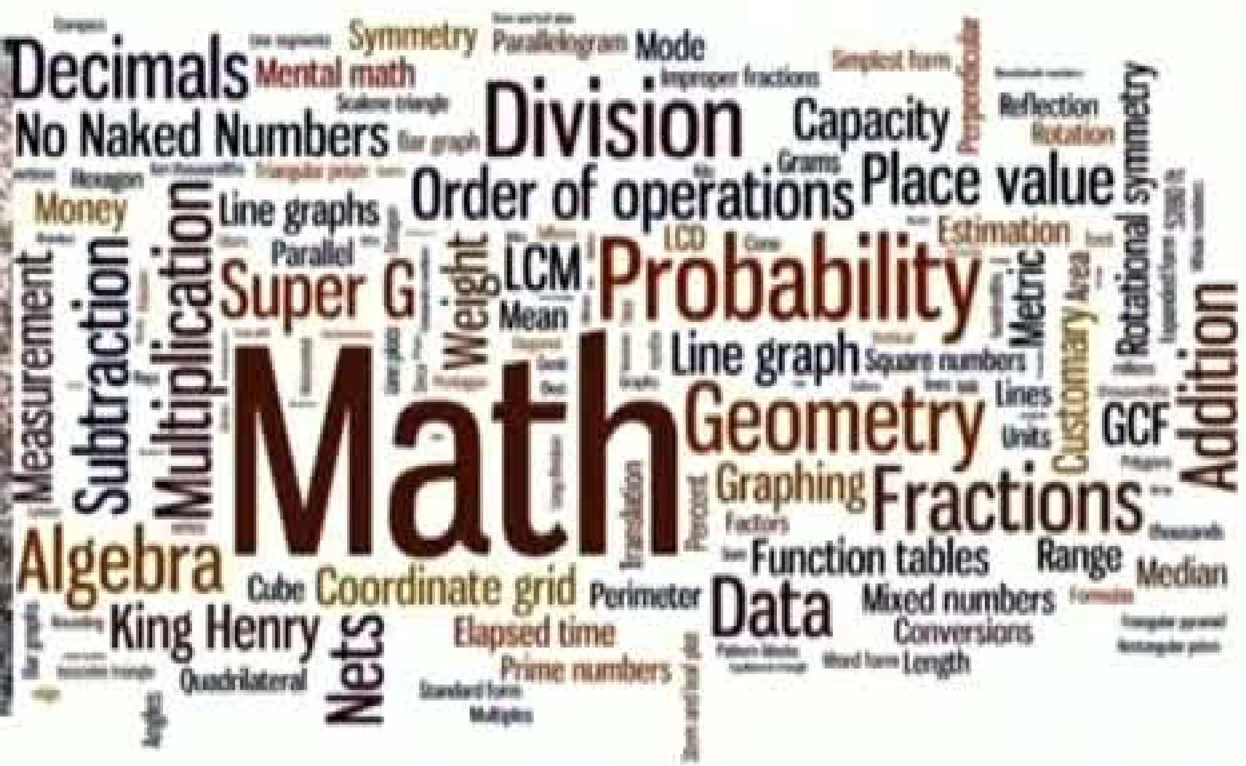
The Golden Age of Paradox

- Church and Turing (1936) gave a negative answer to Hilbert's Entscheidungsproblem (decision problem).
- Turing reduced Hilbert's problem to the halting problem.
- The halting problem can be solved by a paradoxical construction: an algorithm that takes input a data-encoding of itself.

Grothendieck Universes


A
A∩C
A∩B
A∩B∩C
C
B∩C
B



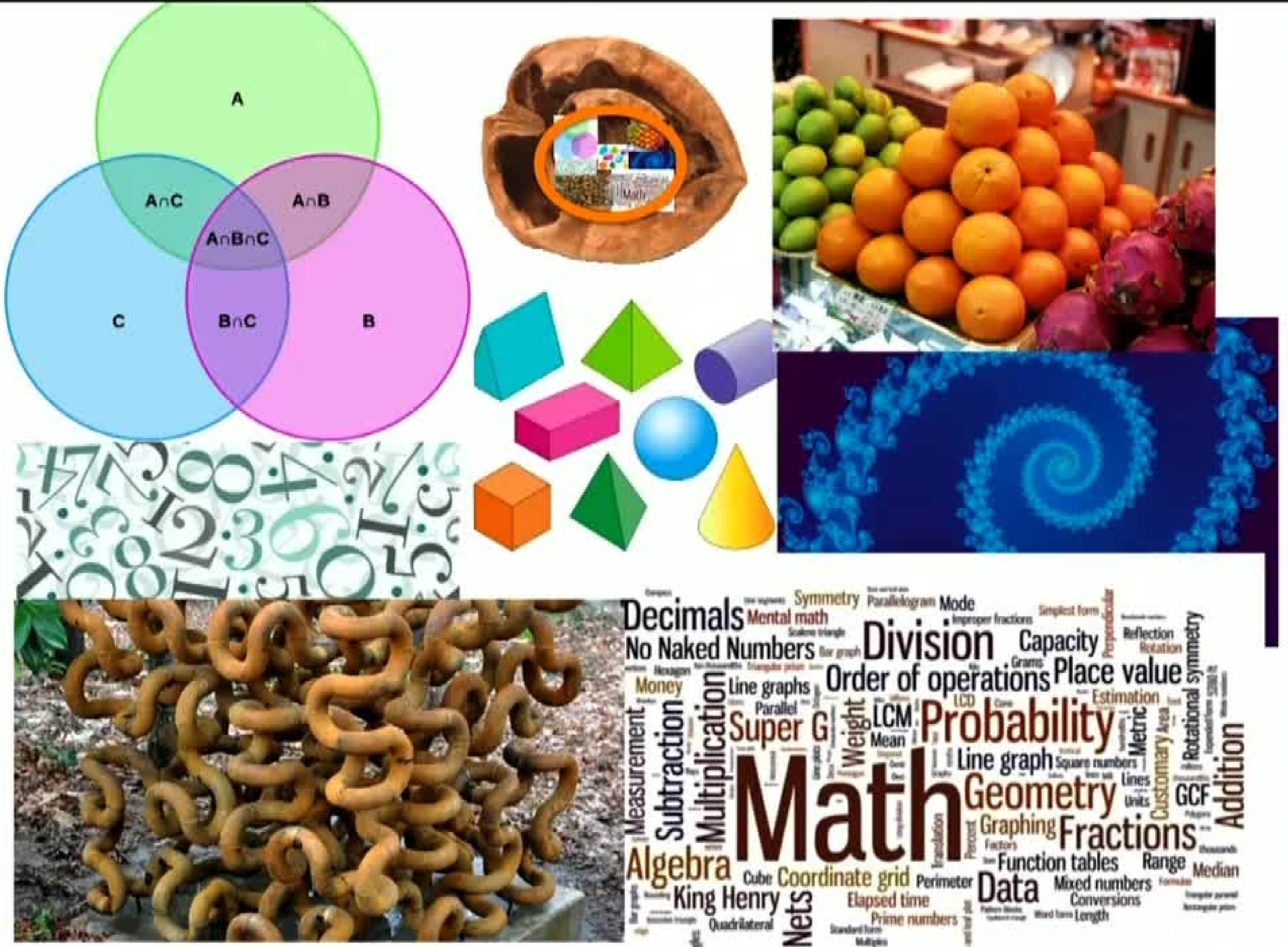

Symmetry
Parallelogram
Mode
Decimals
Mental math
Improper fractions
Simplest form
Division
Capacity
Reflection
Rotation
No Naked Numbers
Perpendicular
Place value
Order of operations
Rotational symmetry
Money
Line graphs
Estimation
Parallel
LCD
Super G
LCM
Probability
Weight
Mean
Measurement
Subtraction
Multiplication
Line graph
Square numbers
Metric
Math
Geometry
Lines
Customary
GCF
Addition
Units
Graphing
Fractions
Factors
Function tables
Range
Algebra
Cube
Coordinate grid
Perimeter
Data
Mixed numbers
Median
King Henry
Elapsed time
Conversions
Nets
Prime numbers
Length
Quadrilateral

A Cartoon of Universes

Mathematical Universe

Universe in a Nutshell

I could be bounded in a nutshell, and count myself a king of infinite space - Hamlet

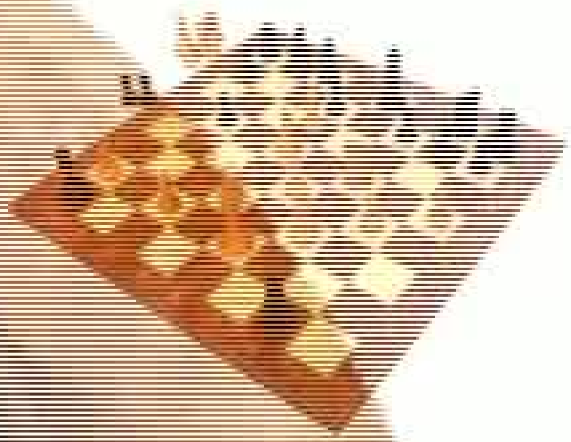

A
A∩C
A∩B
A∩B∩C
C
B∩C
B
Decimals
Mental math
Symmetry
Parallelogram
Mode
Improper fractions
Simplest form
Perpendicular
Division
No Naked Numbers
Capacity
Reflection
Rotation
Order of operations
Place value
Rotational symmetry
Money
Line graphs
Estimation
Parallel
LCD
Measurement
Subtraction
Multiplication
Super G
Weight
LCM
Probability
Mean
Metric
Area
Addition
Line graph
Square numbers
Math
Geometry
Lines
GCF
Customary
Units
Graphing
Fractions
Factors
Algebra
Function tables
Range
Cube
Coordinate grid
Perimeter
Data
Mixed numbers
Median
King Henry
Elapsed time
Conversions
Length
Nets
Prime numbers
Quadrilateral

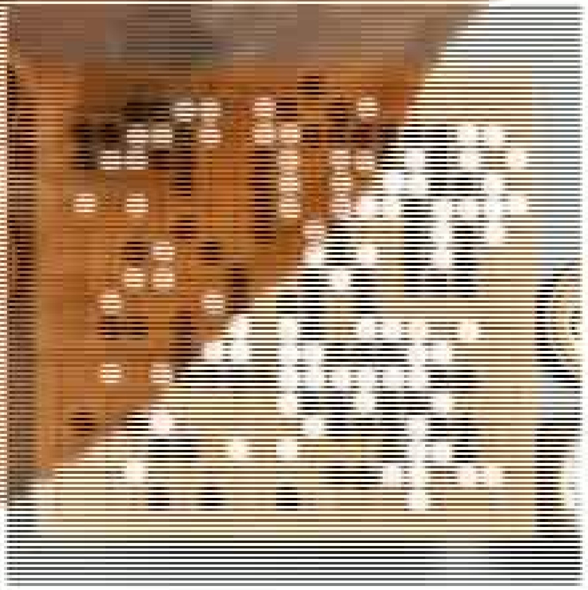
There is a smallest universe, but no largest universe

Hypergame Paradox

(Zwicker 1987)

- Some games necessarily end after a finite number of moves: (chess, tic-tac-toe, go).
- Other games might continue forever (rock-paper-scissors played until somebody is up by five).
- **Hypergame**:
  - first move: pick any game that necessarily ends after finitely many moves.
  - remaining moves: play the game that was picked.
- Hypergame necessarily ends after finitely many moves.





Hypergame Paradox

(Zwicker 1987)

- Some games necessarily end after a finite number of moves: (chess, tic-tac-toe, go).
- Other games might continue forever (rock-paper-scissors played until somebody is up by five).
- **Hypergame**:
  - first move: pick any game that necessarily ends after finitely many moves
  - remaining moves: play the game that was picked.
- Hypergame necessarily ends after finitely many moves.

Hypergame Paradox

(Zwicker 1987)

- **Hypergame**:
  - first move: pick any game that necessarily ends after finitely many moves
  - remaining moves: play the game that was picked.
- Hypergame necessarily ends after finitely many moves.
- But hypergame does not necessarily end after finitely many moves. What if the first move picks hypergame, and the second, etc.?

THEOREM PROVER

Microsoft Research

- Lean is a programming language.
- Lean is proof assistant - it checks the correctness of mathematical proofs.
- Lean can be used to specify and verify computer software.
- Lean contains powerful mathematical foundations, including Grothendieck universes.

Version 1

```lean
universe u

structure game : Type u :=
(states : Type u)
(legal : states → states → Prop)
(terminal : states → Prop)
(terminal_stable : ∀ x y, terminal x → legal x y → terminal y)

#check game
```

PROBLEMS 2 OUTPUT DEBUG CONSOLE TERMINAL

hypergame.lean src 2

[Lean] universe level of type_of(arg #1) of 'game.mk' is too big for the corresponding inductive datatype (7, 1)

Version 2

```lean
universe u

structure game : Type (u+1) :=
(states : Type u)
(legal : states → states → Prop)
(terminal : states → Prop)
(terminal_stable : ∀ x y, terminal x → legal x y → terminal y)

#check game
```

PROBLEMS 1 OUTPUT DEBUG CONSOLE TERMINAL

hypergame.lean src 1

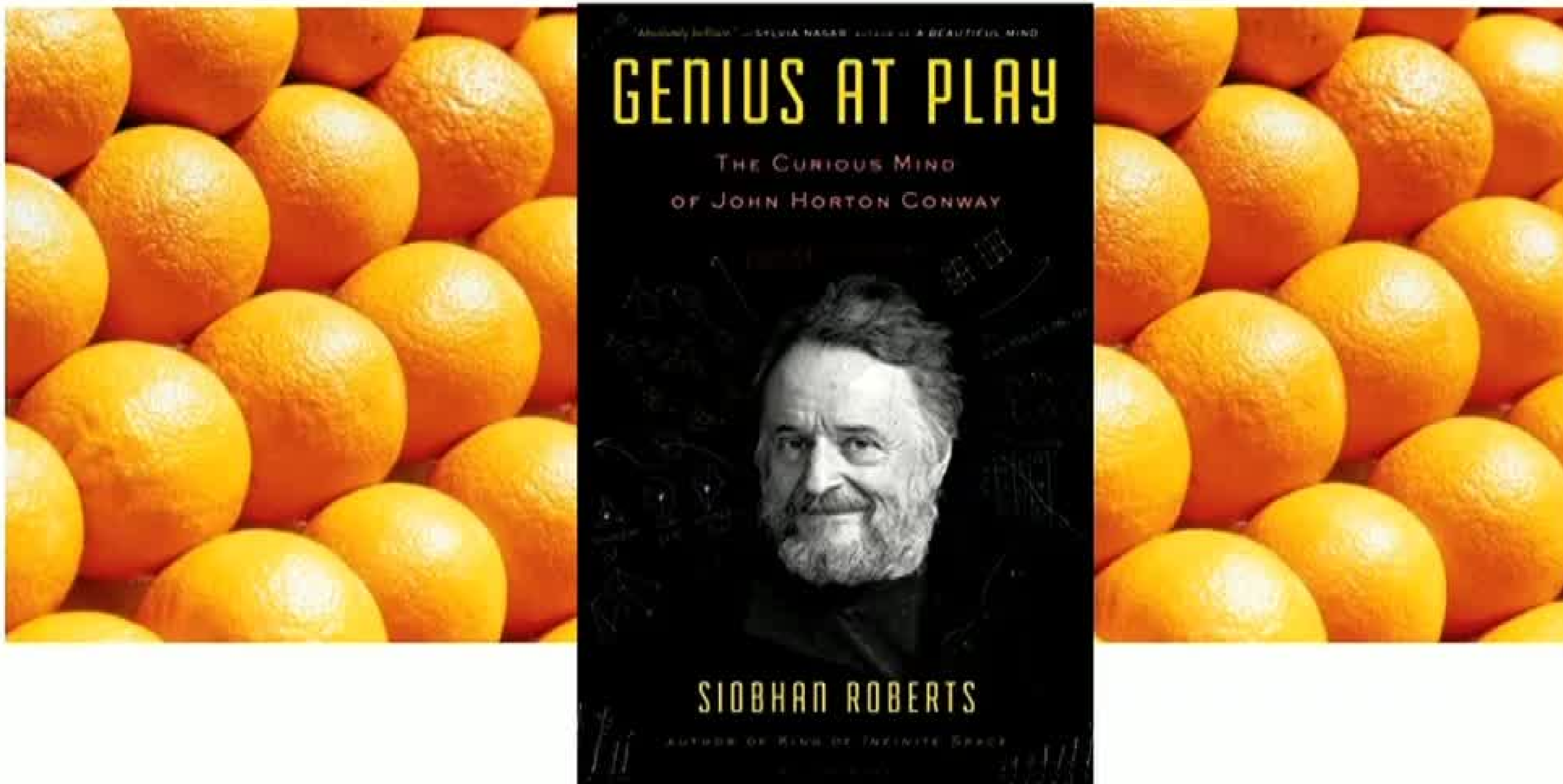
Credit: Earlier formal analysis of hypergame was made by Krebbers.

```
universe u

class finite_game : Type (u+1) :=
(states : Type u)
(legal : states → states → Prop)
(terminal : states → Prop)
(terminal_absorbent : ∀ x y, terminal x → legal x y → terminal y)
(finite: ∀ (f : ℕ → states), (∀ n, legal (f n) (f (n+1)) → ∃ m, terminal (f m)))

instance hypergame : finite_game :=
{
    states :=  option (Σ (G : finite_game), G.states),
    legal := sorry,
    terminal := sorry,
    terminal_absorbent := sorry,
    finite := sorry
}
```

Hypergame in Lean

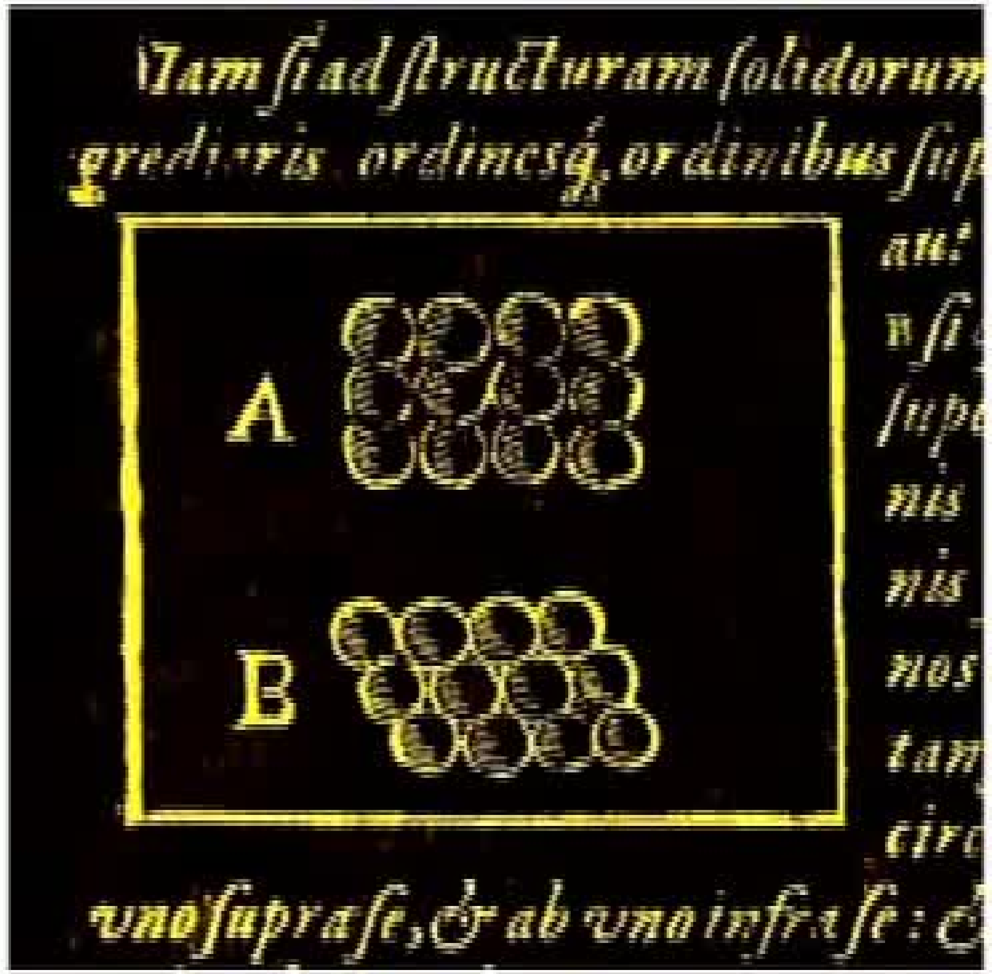
- The hypergame has universe level one greater than the games it plays from.
- Each choice of hypergame as the first move of hypergame drops the universe level by one.
- At the lowest universe level, only ordinary games are available, and the hypergame necessarily ends after finitely many moves.

Interlude
Sphere Packings

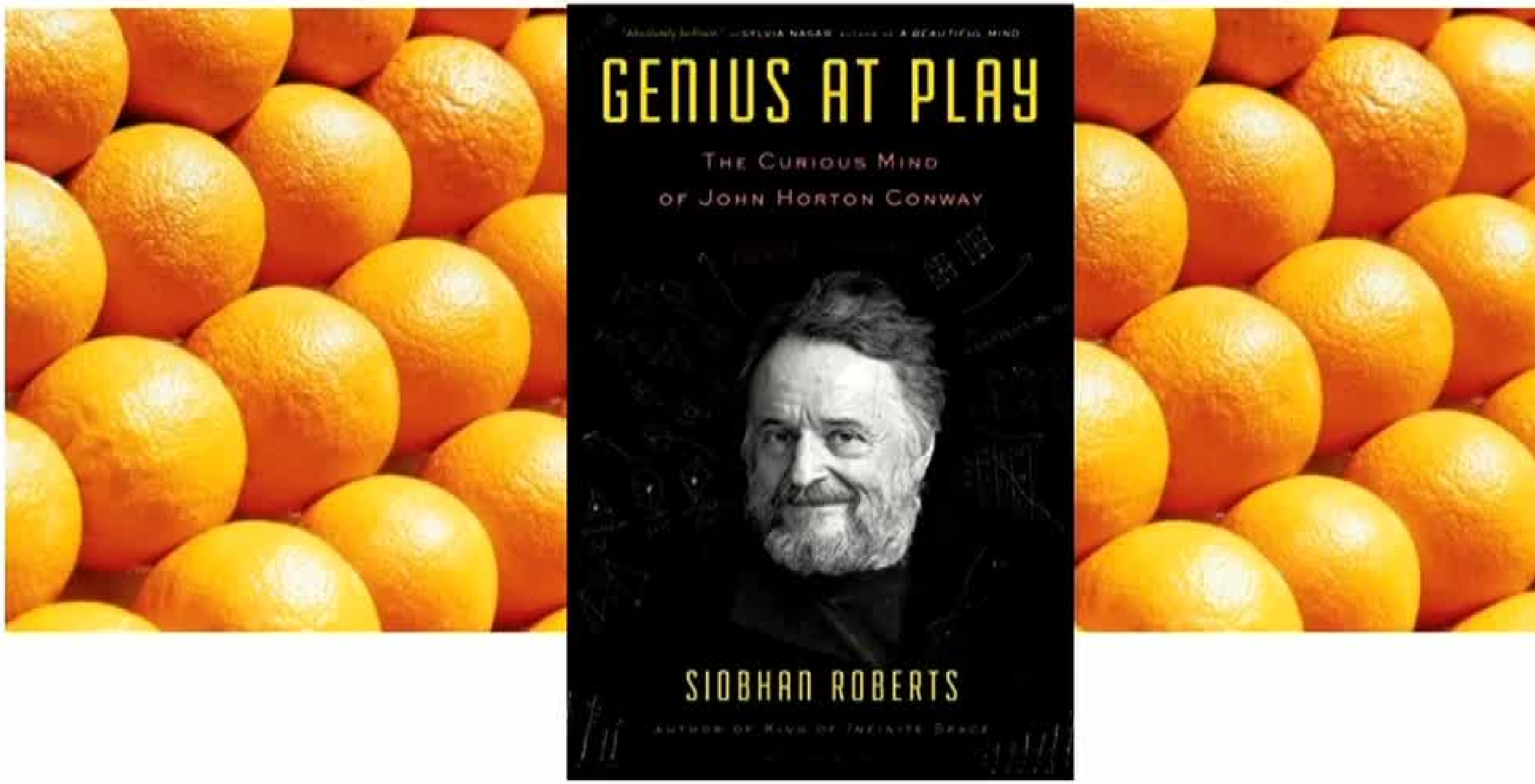


Interlude Sphere Packings

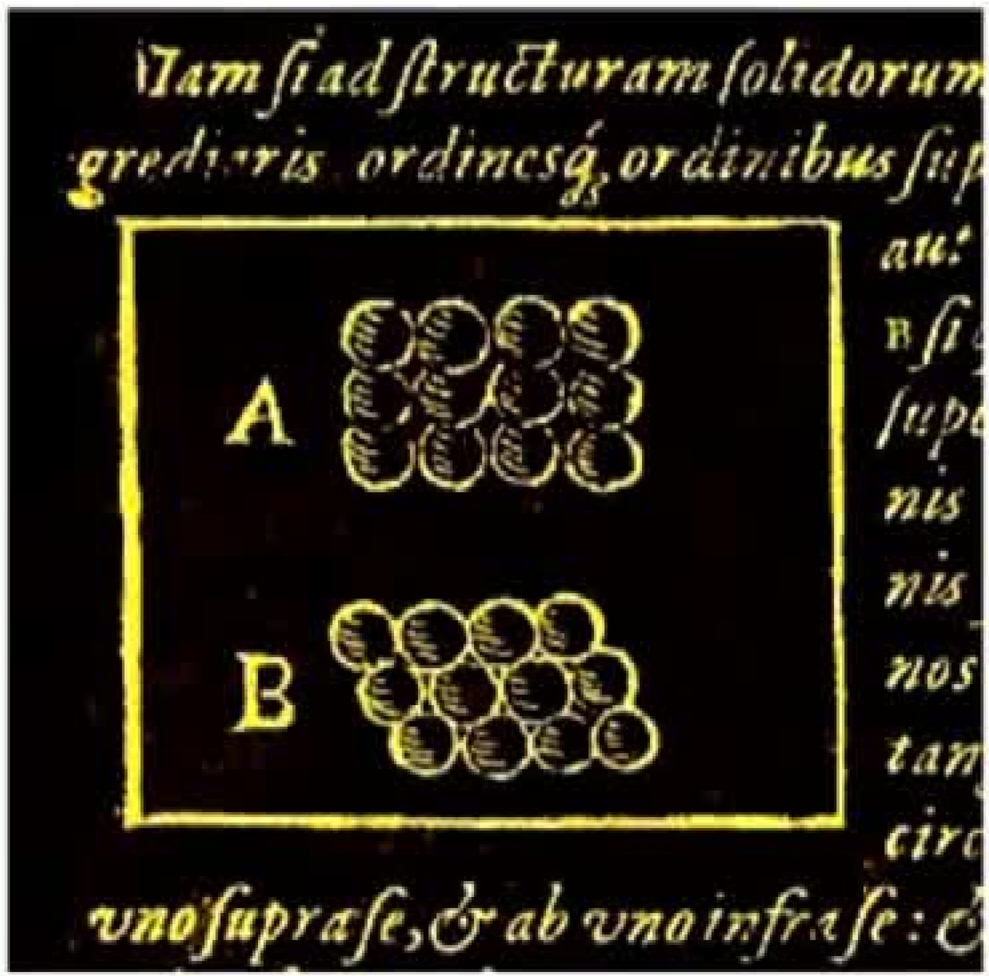
The face-centered cubic packing is "the tightest possible, so that in no other arrangement could more pellets be stuffed into the same container." (Kepler, 1611)



Interlude
Sphere Packings



The face-centered cubic packing is "the tightest possible, so that in no other arrangement could more pellets be stuffed into the same container." (Kepler, 1611)



Interlude Sphere Packings

"Many mathematicians believe and all physicists know" [that the pyramid arrangement is best]. (Rogers, 1958)

The "problem in 3-dimensions remains unsolved. This is a scandalous situation since the (presumably) correct answer has been known since the time of Gauss . . . All this is missing is a proof." (Milnor, 1976)

Interlude Sphere Packings


The Mathematical
Intelligencer
We're Not Afraid
Of
Controversy...
We Welcome It!
The Mathematical Intelligencer has long been the main forum for debate between some of the world's most renowned and respected mathematicians. The Mathematical Intelligencer has always provided a place for the debate of all mathematical issues. Inside you'll find just a few of the most notable controversies that The Mathematical Intelligencer has proudly published in the past, and some of the controversies you can look forward to in the future.

THE KEPLER CONJECTURE CONTROVERSY

Perhaps the most controversial topic to be covered in **The Mathematical Intelligencer** is the Kepler Conjecture. In **The Mathematical Intelligencer** (16:3), Thomas C. Hales takes on Wu-Yi Hsiang's 1990 announcement that he had proved the Kepler Conjecture, the conjecture that no arrangement of spheres of equal radius in 3-space has density greater than that of the face-centered cubic packing.

Following are excerpts from the article *"The Status of the Kepler Conje*

Hsiang was honored for his work in January meetings of the AMS-MAA, by being inv plenary address entitled "The proof of Kepler's conjecture on the sphere-packing problem."

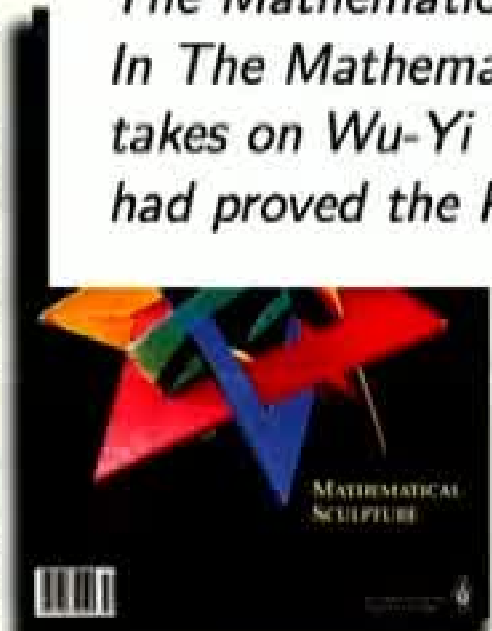
As a result of such announcements, many are prone to accept Hsiang's solution to the sphere-packing problem. Even if Hsiang withdraws his claims, some might continue to believe, for years to come, that the problem has been successfully solved. It has become necessary, therefore, to write this article on the status of the Kepler conjecture, to correct the public record.

What is the significance of this negative result? Hsiang's early preprint omitted the argument for seven-faced polyhedra; it merely remarked that "it is easy to see that no vertices...have more than six forks." (The number of forks is the number of edges or faces surrounding the vertex.) The fact that this much analysis was required to study a single arrangement shows that those who challenged his "easy to see" claim had more than ample justification for doing so. He claims to use deformation arguments, and deformation arguments (properly developed), even if linearized, require the solution to large systems of equations.

His packing bounds are dependent on this result. In later arguments he uses case-by-case arguments that list all relevant polyhedra with only four, five, or six faces around a given edge. Hence, we must put all his later conclusions on indefinite hold. One is left to conclude that his hasty reduction has no real substance to it and that his critical case remains an isolated test case.

In the end, I feel that Hsiang has missed the point of the subject of sphere packings. Many packing problems have geo-

"Perhaps the most controversial topic to be covered in The Mathematical Intelligencer is the Kepler Conjecture. In The Mathematical Intelligencer, Thomas C. Hales takes on Wu-Yi Hsiang's 1990 announcement that he had proved the Kepler Conjecture,..."



implausible configurations could be dismissed without proof. But rigor requires that proofs be given.

One of the most unsettling aspects of his article is his deliberate and persistent use of methods that are known to be defective. The errors in his hole-fitting principle and his size-decreasing deformation were pointed out to him some time ago. His claims over the last 3 years that the next revision will answer all objections have grown tiresome.

In conclusion, I offer a suggestion. First, Hsiang should withdraw his claim to have resolved the Kepler conjecture. Mathematicians can easily spot the difference between handwaving and proof. Then, Hsiang should isolate the statements in his article that he was unable to prove rigorously. He should show carefully how the Kepler conjecture would follow from these statements. In this way, his work would make an important contribution to the field. It would provide a concrete program that could eventually lead to a solution to the problem. Instead, by presenting experimental hypothesis as fact, he destroys the credibility of his own work.

HSIANG RESPONDS

Wu-Yi Hsiang has agreed to publish his rejoinder to Thomas Hales, and the

Interlude Sphere Packings

Section A.2.7†. If the circumradius of a quasi-regular tetrahedron is ≥ 1.41, then by [1.9.17], $\tau > 1.8\,pt$, and many of the inequalities hold.

In Sections A.2.7 and A.2.8, let $S_1, \ldots, S_5$ be 5 simplices arranged around a common edge $(0, v)$, with $|v| \in [2, 2.51]$. Let $y_i(S_j)$ be the edges, with $y_1(S_j) = |v|$ for all j, $y_3(S_j) = y_2(S_{j+1})$, and $y_5(S_j) = y_6(S_{j+1})$. where the subscripts j are extended modulo 5. In Sections A.2.7 and A.2.8, $\sum \mathrm{dih}(S_j) \leq 2\pi$. Set $\pi_0 = 2\xi_V + \xi_\Gamma$ if $\sigma = \mathrm{vor}_0$ in the cases ($y_4 \geq 2.6, y_1 \geq 2.2$) and ($y_1 \geq 2.7$). Set $\pi_0 = 0$, otherwise.

$\tau(S_1) + \tau(S_2) + \tau(S_4) > 1.4\,pt$, if $y_4(S_3), y_4(S_5) \geq 2\sqrt{2}$. (551665569)

$\tau(S_1) + \tau(S_2) + \tau(S_3) > 1.4\,pt$, if $y_4(S_4), y_4(S_5) \geq 2\sqrt{2}$. (824762926)

$\tau(S_1) + \tau(S_2) + (\hat\tau(S_3) - \pi_0) + \tau(S_4) > 1.4\,pt + D(3,1)$, if $y_4(S_3) \in [2.51, 2\sqrt{2}]$, $y_4(S_5) \geq 2.51$, $\mathrm{dih}(S_5) > 1.32$. (675785884)

$\tau(S_1) + \tau(S_2) + \tau(S_3) + (\hat\tau(S_4) - \pi_0) > 1.4\,pt + D(3,1)$, if $y_4(S_4) \in [2.51, 2\sqrt{2}]$, $y_4(S_5) \geq 2.51$, $\mathrm{dih}(S_5) > 1.32$. (193592217)

Section A.2.8†. As in A.2.7, the quasi-regular tetrahedra are generally compression scored. Define π_0 as in Section A.2.7. The constraint $\sum_{(5)} \mathrm{dih}(S_j) = 2\pi$ is assumed.

$\tau(S_1) + \tau(S_2) + \tau(S_3) + \tau(S_4) > 1.5\,pt$, if $y_4(S_5) \geq 2\sqrt{2}$. (325738864)

$\tau(S_1) + \tau(S_2) + \tau(S_3) + \tau(S_4) + (\hat\tau(S_5) - \pi_0) > 1.5\,pt + D(3,1)$, if $y_4(S_5) \in [2.51, 2\sqrt{2}]$. (314974315)

Section A.3.1.

$\tau - 0.2529\,\mathrm{dih} > -0.3442$, if $y_1 \in [2.3, 2.51]$, and $\mathrm{dih} \geq 1.51$. (572068135)

$\pi_0 - 0.2529\,\mathrm{dih} > -0.1787$, if $y_1 \in [2.3, 2.51]$, $y_6 \in [2\sqrt{2}, 3.02]$, $1.26 \leq \mathrm{dih} \leq 1.63$. (723700608)

$\hat\tau - 0.2529\,\mathrm{dih}_2 > -0.2137$, if $y_2 \in [2.3, 2.51]$, $y_4 \in [2.51, 2\sqrt{2}]$. (560470084)

$\pi_0 - 0.2529\,\mathrm{dih} > -0.1371$, if $y_1 \in [2.3, 2.51]$, $y_5, y_6 \in [2.51, 3.02]$, $1.14 \leq \mathrm{dih} \leq 1.51$. (535502975)

Section A.3.8.

A. $\mathrm{dih} < 1.63$, if $y_6 \geq 2.51$, $y_2, y_3 \in [2, 2.168]$. (821707685)

B. $\mathrm{dih} < 1.51$, if $y_5 = 2.51$, $y_6 \geq 2.51$, $y_2, y_3 \in [2, 2.168]$. (115383627)

C. $\mathrm{dih} < 1.93$, if $y_6 \geq 2.51$, $y_4 = 2\sqrt{2}$, $y_2, y_3 \in [2, 2.168]$. (576221766)

D. $\mathrm{dih} < 1.77$, if $y_5 = 2.51$, $y_6 \geq 2.51$, $y_4 = 2\sqrt{2}$, $y_2, y_3 \in [2, 2.168]$. (122081309)

$\pi_0 - 0.2529\,\mathrm{dih} > -0.2301$, if $y_6 \geq 2.51$, $\mathrm{dih} \geq 1.2$, $y_2, y_3 \in [2, 2.168]$. (644534985)

$\pi_0 - 0.2529\,\mathrm{dih} > -0.1376$, if $y_5 = 2.51$, $y_6 \geq 2.51$, $\mathrm{dih} \geq 1.2$, and $y_2, y_3 \in [2, 2.168]$. (467530297)

$\pi_0 - 0.2529\,\mathrm{dih} > -0.266$, if $y_6 \geq 2.51$, $y_4 \in [2.51, 2\sqrt{2}]$, $\mathrm{dih} \geq 1.2$, $y_2, y_3 \in [2, 2.168]$. (603910880)

$\pi_0 - 0.2529\,\mathrm{dih} > -0.12$, if $y_5 = 2.51$, $y_6 \geq 2.51$, $y_4 \in [2.51, 2\sqrt{2}]$, $\mathrm{dih} \geq 1.2$, $y_2, y_3 \in [2, 2.168]$. (135427691)

$\mathrm{dih} < 1.16$, if $y_5 = 2.51$, $y_6 \geq 2.51$, $y_4 = 2$, $y_2, y_3 \in [2, 2.168]$. (60314528)

$\pi_0 - 0.2529\,\mathrm{dih} > -0.1453$, if $y_2, y_3 \in [2, 2.168]$, $y_5 \in [2.51, 3.488]$, $y_6 = 2.51$. (312132053)

June 2002 referee report (4 years in)

iii. Checking (and re-running) the program, which is working in Phase 3, might detect a "case" in which the mentioned function is negative. Then the theory would collapse (in its present form), and would require amendment, since the suggested decomposition of the space would not have the claimed property.

With all this in mind one would prefer to have Phase 2 and Phase 3 checked *prior to start working on Phase* 1 (and minimize the chance that the essential work of careful reading of the manuscript might prove useless). Since I am not planning to read any part of Phase 2 and/or 3, — and some other referees might share my views — I would like to ask you to inform me whether the Editorial Board has organized any separate proceedings regarding the checking of Phase 2 and 3 or no support of this kind can be expected.

Computers were once human

Referees were once human

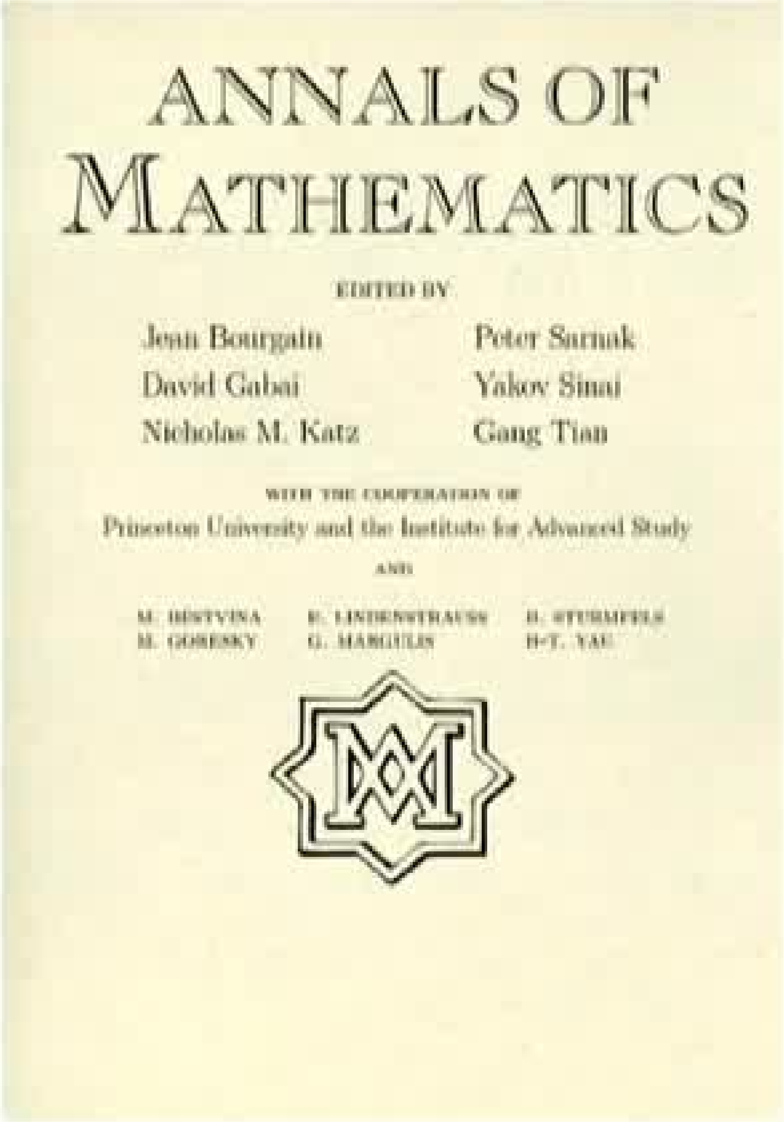
Interlude Sphere Packings

"It is very unusual to have such a large set of reviewers. The main portion of the reviewing took place in a seminar at Eötvos University, Budapest, over a three year period. Some reviewers made computer experiments, in a detailed check of specific parts of the proof.. . . In this process detailed checking of many specific assertions found them to be essentially correct in every case. This result of the reviewing process produced in these reviewers a strong degree of conviction of the essential correctness of this proof approach,. . . " (J. Lagarias, editor)

Robert MacPherson, editor of the Annals, wrote a report that states

"The news from the referees is bad, from my perspective. They have not been able to certify the correctness of the proof, and will not be able to certify it in the future, because they have run out of energy to devote to the problem. This is not what I had hoped for."

"Fejes Toth thinks that this situation will occur more and more often in mathematics. He says it is similar to the situation in experimental science - other scientists acting as referees can't certify the correctness of an experiment, they can only subject the paper to consistency checks. He thinks that the mathematical community will have to get used to this state of affairs."



Forum of Mathematics, Pi

Search F

Article Metrics

Volume 5 2017 , e2

A FORMAL PROOF OF THE KEPLER CONJECTURE

THOMAS HALES [a1], MARK ADAMS [a2] [a3], GERTRUD BAUER [a4], TAT DAT DANG [a5] ...

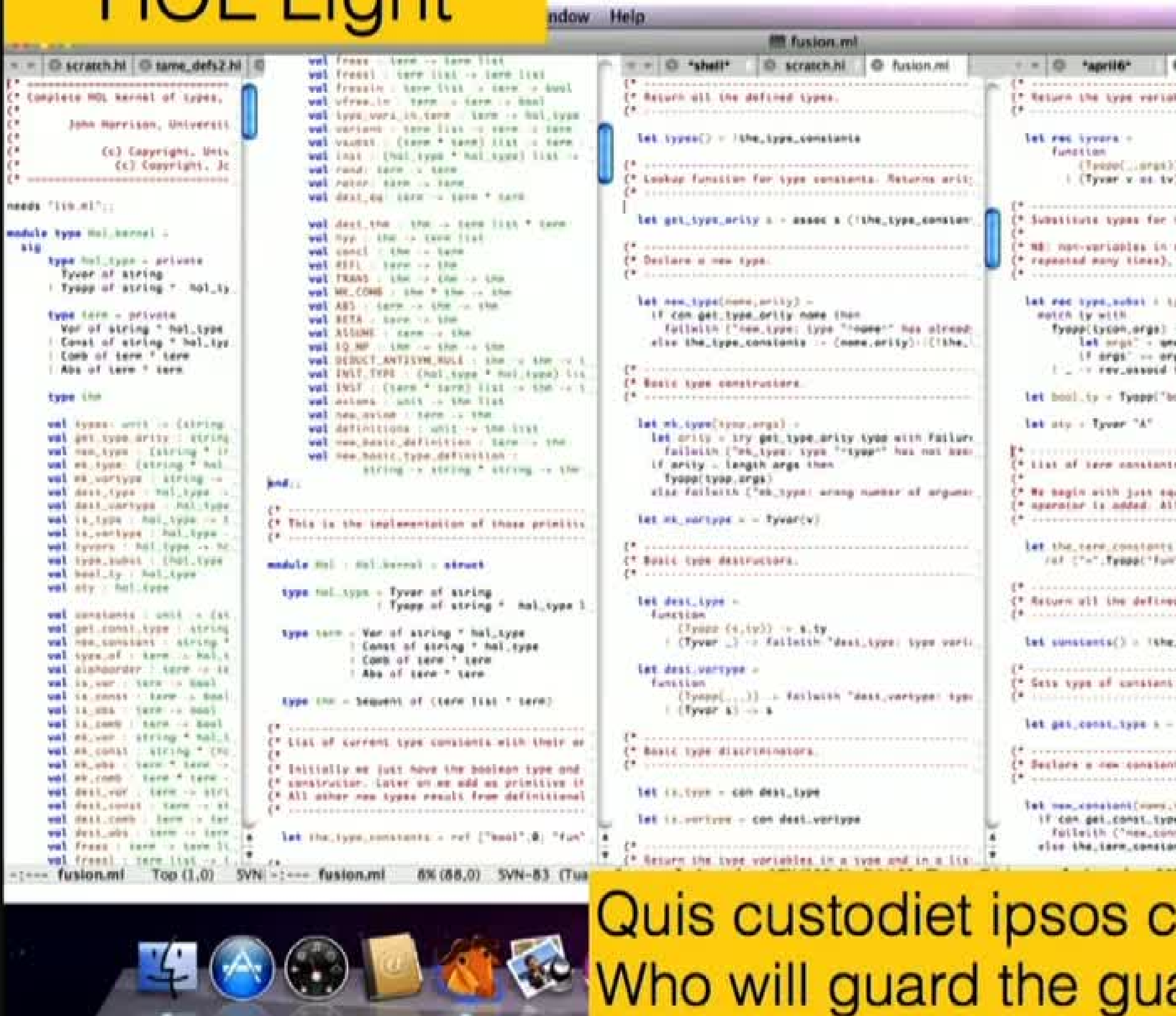
https://doi.org/10.1017/fmp.2017.1 Published online: 29 May 2017

Abstract

This article describes a formal proof of the Kepler conjecture on dense sphere packings in a combination of the HOL Light and Isabelle proof assistants. This paper constitutes the official published account of the now completed Flyspeck project.

THOMAS HALES [a1], MARK ADAMS [a2] [a3], GERTRUD BAUER [a4], TAT DAT DANG [a5], JOHN HARRISON [a6], LE TRUONG HOANG [a7], CEZARY KALISZYK [a8], VICTOR MAGRON [a9], SEAN MCLAUGHLIN [a10], TAT THANG NGUYEN [a7], QUANG TRUONG NGUYEN [a1], TOBIAS NIPKOW [a11], STEVEN OBUA [a12], JOSEPH PLESO [a13], JASON RUTE [a14], ALEXEY SOLOVYEV [a15], THI HOAI AN TA [a7], NAM TRUNG TRAN [a7], THI DIEP TRIEU [a16], JOSEF URBAN [a17], KY VU [a18] and ROLAND ZUMKELLER [a19]

HOL Light



John Harrison

Quis custodiet ipsos custodes?
Who will guard the guards themselves?

Towards self-verification of HOL Light

John Harrison.

Proceedings of IJCAR 2006, the third International Joint Conference on Automated Reasoning. Springer LNCS 4130, pp. 177-191.

Abstract:

The HOL Light prover is based on a logical kernel consisting of about 400 lines of mostly functional OCaml, whose complete formal verification seems to be quite feasible. We would like to formally verify (i) that the abstract HOL logic is indeed correct, and (ii) that the OCaml code does correctly implement this logic. We have performed a full verification of an imperfect but quite detailed model of the basic HOL Light core, without definitional mechanisms, and this verification is entirely conducted with respect to a set-theoretic semantics within HOL Light itself. We will duly explain why the obvious logical and pragmatic difficulties do not vitiate this approach, even though it looks impossible or useless at first sight. Extension to include definitional mechanisms seems straightforward enough, and the results so far allay most of our practical worries.

Steps Towards Verified Implementations of HOL Light

Magnus O. Myreen[1], Scott Owens[2], and Ramana Kumar[1]

[1] Computer Laboratory, University of Cambridge, UK
[2] School of Computing, University of Kent, UK

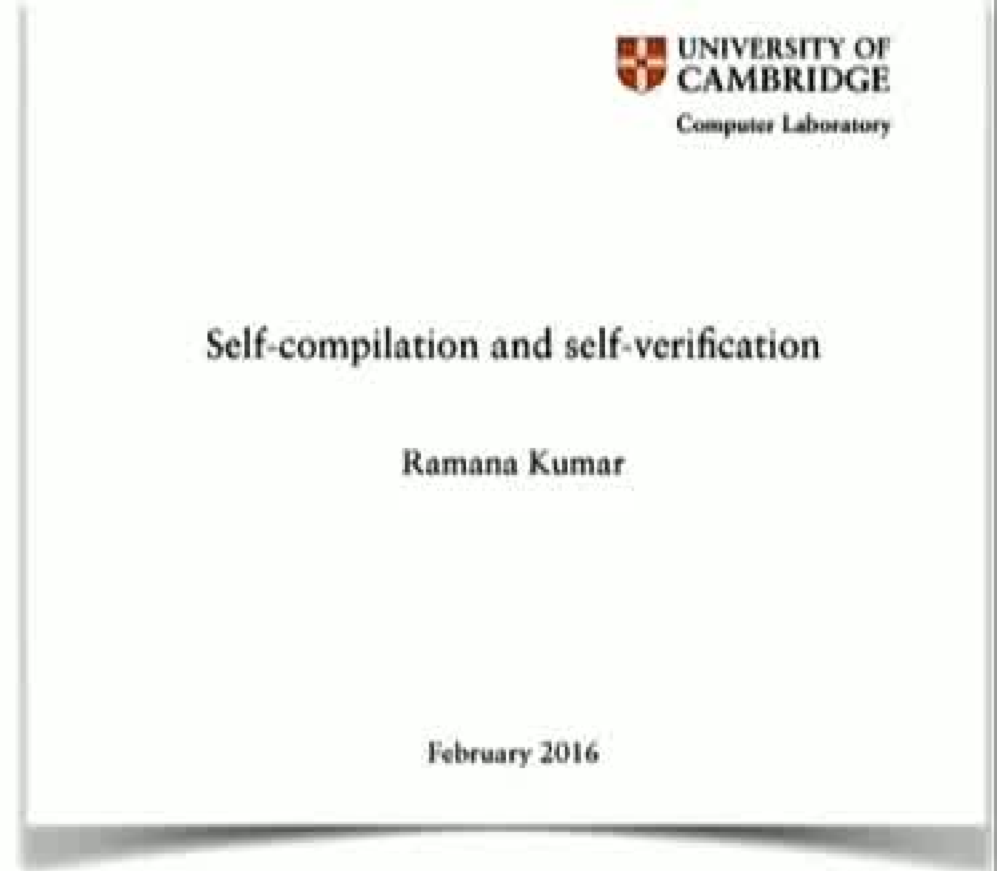
Abstract. This short paper describes our plans and progress towards construction of verified ML implementations of HOL Light: the first formally proved soundness result for an LCF-style prover. Building on Harrison's formalisation of the HOL Light logic and our previous work on proof-producing synthesis of ML, we have produced verified implementations of each of HOL Light's kernel functions. What remains is extending Harrison's soundness proof and proving that ML's module system provides the required abstraction for soundness of the kernel to relate to the entire theorem prover. The proofs described in this paper involve the HOL Light and HOL4 theorem provers and the OpenTheory toolchain.

1 Introduction

We are developing a new verification friendly dialect of ML, called CakeML. This ML dialect is approximately a subset of Standard ML carefully carved out to be convenient to program in and to reason about formally. We plan to build verified implementations of CakeML (a compiler, an implementation of a read-eval-print loop and possibly custom hardware) and also produce tools for generating and

CAKEML

A Verified Implementation of ML


UNIVERSITY OF CAMBRIDGE
Computer Laboratory

Self-compilation and self-verification

Ramana Kumar

February 2016

About

CakeML is a functional programming language and an ecosystem of proofs and tools built around the language. The ecosystem includes a proven-correct compiler that can bootstrap itself.

The CakeML project consists of the following components, all of which are free software.

Language definition. The CakeML language is based on a substantial subset of Standard ML. Its formal semantics is specified in higher-order logic (HOL) in a functional big-step style. The core of the language (its syntax and semantics) is quite stable, but the standard basis library is still undergoing development. Contributions are welcome!

Compiler bootstrapping. The CakeML compiler has been bootstrapped inside HOL. By bootstrapped we mean that the compiler has compiled itself. This was achieved by noticing that frontend 2 combined with the backend is a HOL function which we can feed into the tool-chain consisting of frontend 1 and the backend. The result is a verified binary that provably implements the compiler itself (with frontend 2). The latest bootstrapped binary is on our downloads page. The bootstrapping is described here.