ICMS
Formal Abstracts

Thomas Hales

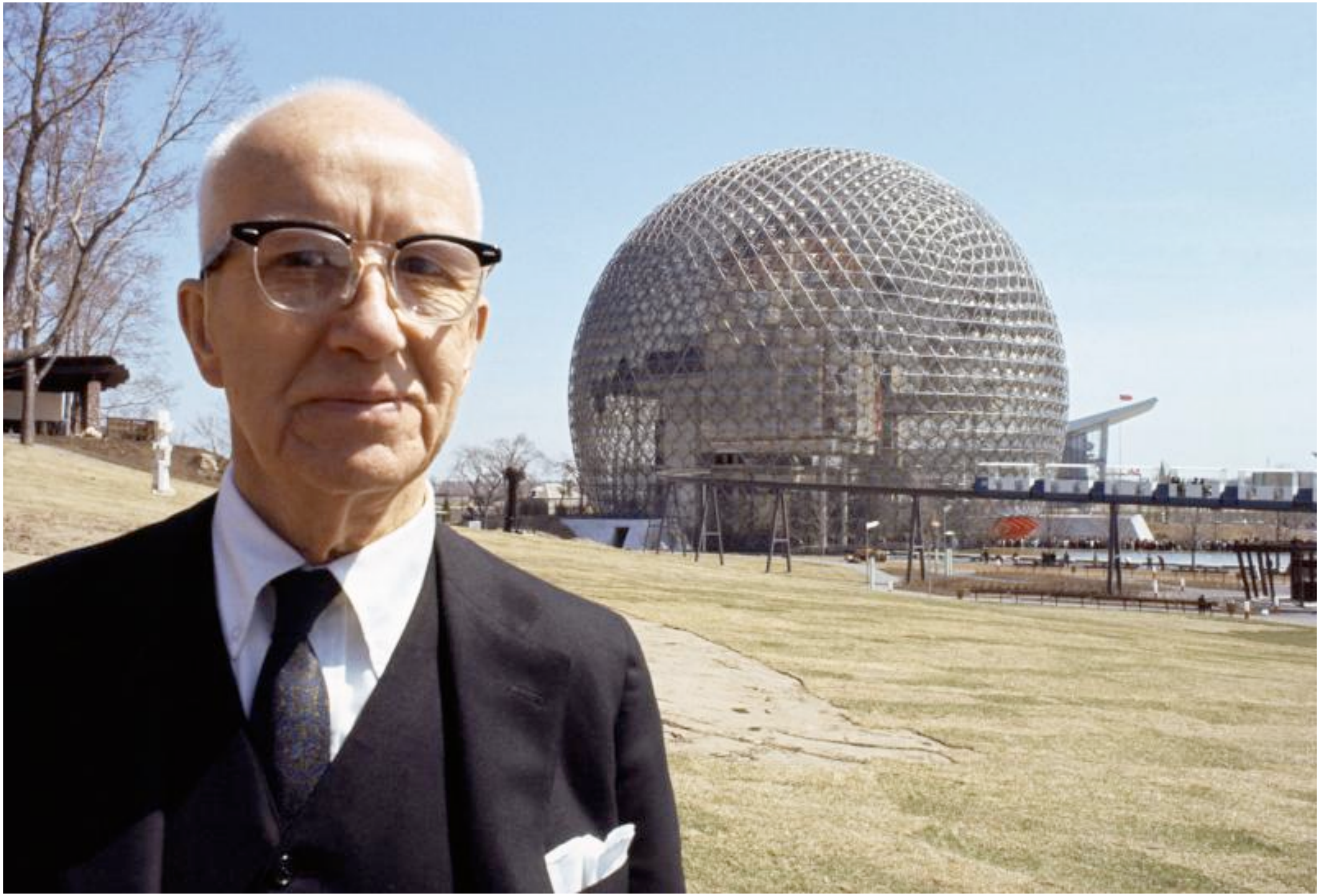
Formal Abstracts in Mathematics

FAB
STRACTS

Alert

But the technology is here now…

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.

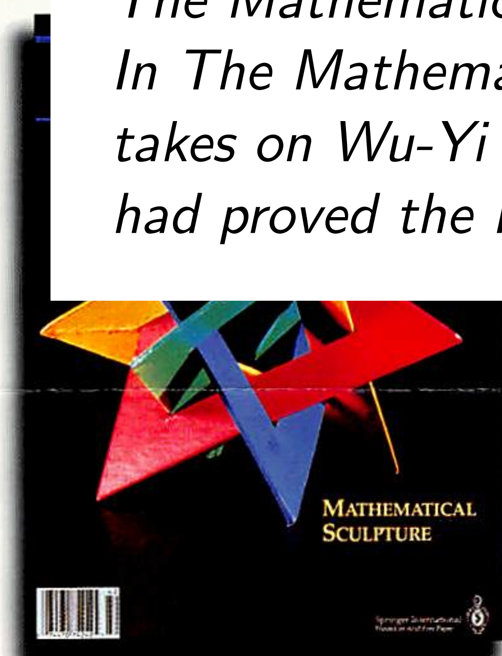
THE KEPLER CONJECTURE CONTROVERSY

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-

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

"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,. . . "

From hales@math.lsa.umich.edu Wed Aug 19 02:43:02 1998
Date: Sun, 9 Aug 1998 09:54:56 -0400 (EDT)
From: Tom Hales <hales@math.lsa.umich.edu>
To:

Subject: Kepler conjecture

Dear colleagues,

I have started to distribute copies of a series of papers giving a solution to the Kepler conjecture, the oldest problem in discrete geometry. These results are still preliminary in the sense that they have not been refereed and have not even been submitted for publication, but the proofs are to the best of my knowledge correct and complete.

Nearly four hundred years ago, Kepler asserted that no packing of congruent spheres can have a density greater than the density of the face-centered cubic packing. This assertion has come to be known as the Kepler conjecture. In 1900, Hilbert included the Kepler conjecture in his famous list of mathematical problems.

In a paper published last year in the journal "Discrete and Computational Geometry," (DCG), I published a detailed plan describing how the Kepler conjecture might be proved. This approach differs significantly from earlier approaches to this

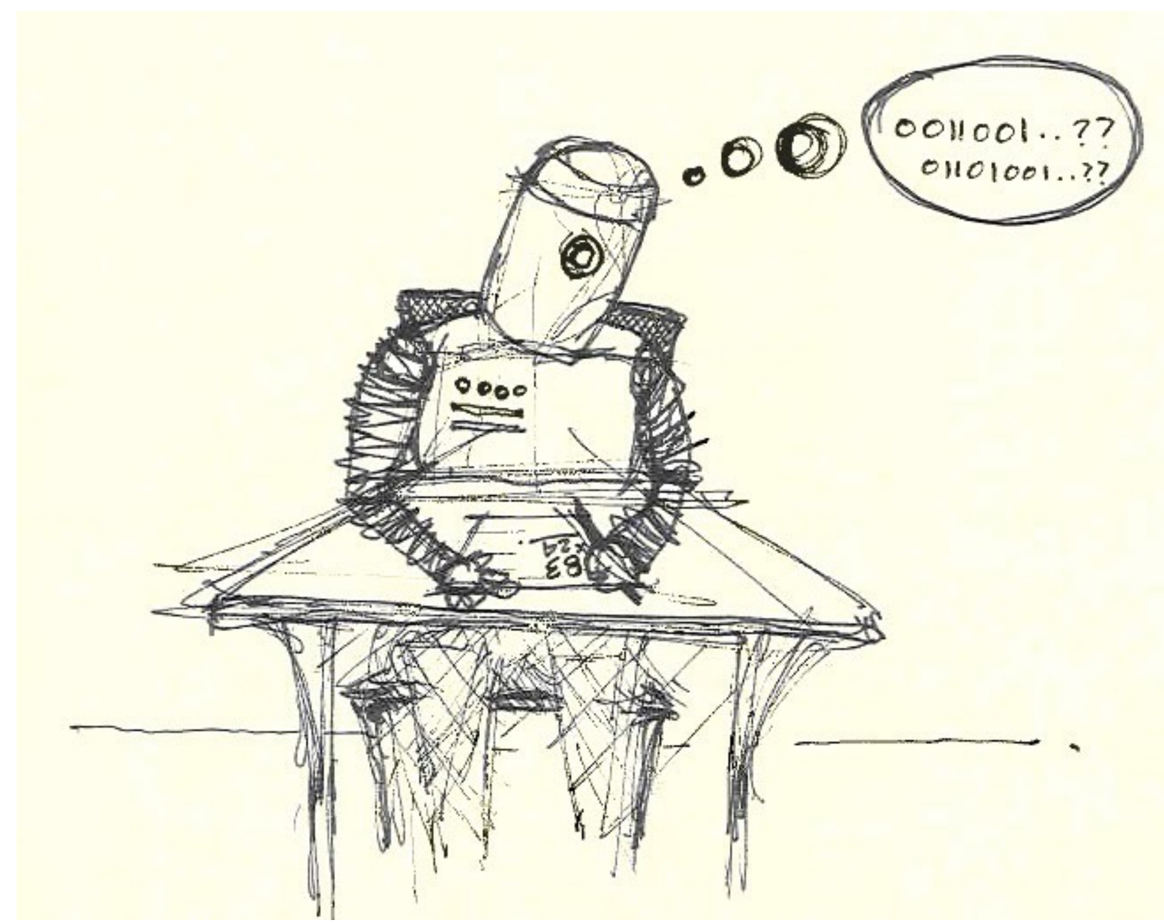
In year 4, the referees of the Kepler conjecture gave up. In the end the computer code was not checked, and the text part of the proof was only spot checked.

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.

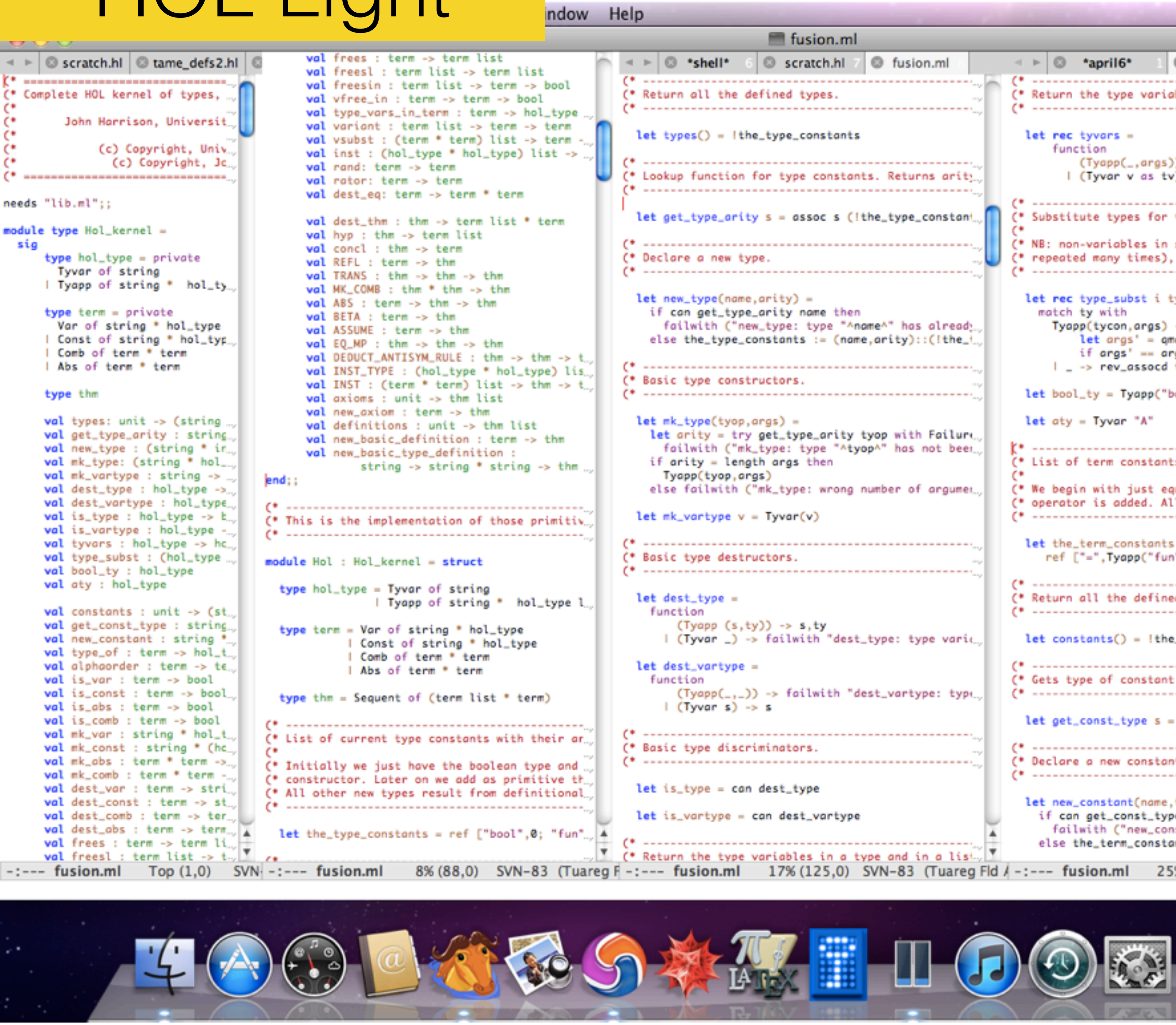
Computers were once human

Referees were once human



A formal proof is a mathematical proof that has been checked by computer. The axioms of mathematics and the fundamental rules of logic are programmed into a computer and every step of the mathematical proof is verified with those axioms and rules. Computer programs – called proof assistants – are used to construct formal proofs. Proof assistants have been under development for decades. There are many of them. Three of the most influential are Mizar, Coq, and HOL (which comes in several dialects).

HOL Light



John Harrison

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]

The formal proof of the Kepler conjecture, which was finally published last year uncovered and corrected hundreds of errors in the proof.

where `the_kepler_conjecture` is defined as the following term

```
`(!V. packing V
        ==> (?c. !r. &1 <= r
                 ==> &(CARD(V INTER ball(vec 0,r))) <=
                     pi * r pow 3 / sqrt(&18) + c * r pow 2))`
```

In standard mathematical language, this states that for every packing V (which is identified with the set of centers of balls of radius 1), there exists a constant c controlling the error term, such that for every radius r that is at least 1, the number of ball centers inside a spherical container of radius r is at most `pi * r^3 / sqrt(18)`, plus an error term of smaller order. As r tends to infinity, this gives the density bound `pi / sqrt(18) = 0.74+`, which is the density of the face-centered-cubic packing.

The term `the_nonlinear_inequalities` is defined as a conjunction of several hundred nonlinear inequalities. The domains of these inequalities have been partitioned to create more than 23,000 inequalities. The verification of all nonlinear inequalities in HOL Light on the Microsoft Azure cloud took approximately 5000 processor-hours. Almost all verifications were made in parallel with 32 cores, hence the real time is about 5000 / 32 = 156.25 hours. Nonlinear inequalities were verified with compiled versions of HOL Light and the verification tool developed in Solovyev's 2012 thesis.

To check that no pieces were overlooked in the distribution of inequalities to various cores, the pieces have been reassembled in a specially modified version of HOL Light that allows the import of theorems from other sessions of HOL light. In that version, we obtain a formal proof of the theorem

```
|- the_nonlinear_inequalities
```

Published as a conference paper at ICLR 2017

HOLSTEP: A MACHINE LEARNING DATASET FOR HIGHER-ORDER LOGIC THEOREM PROVING

Cezary Kaliszyk
University of Innsbruck
cezary.kaliszyk@uibk.ac.at

François Chollet, Christian Szegedy
Google Research
{fchollet,szegedy}@google.com

ABSTRACT

Large computer-understandable proofs consist of millions of intermediate logical steps. The vast majority of such steps originate from manually selected and manually guided heuristics applied to intermediate goals. So far, machine learning has generally not been used to filter or generate these steps. In this paper, we introduce a new dataset based on Higher-Order Logic (HOL) proofs, for the purpose of developing new machine learning-based theorem-proving strategies. We make this dataset publicly available under the BSD license. We propose various machine learning tasks that can be performed on this dataset, and discuss their significance for theorem proving. We also benchmark a set of simple baseline machine learning models suited for the tasks (including logistic regression, convolutional neural networks and recurrent neural networks). The results of our baseline models show the promise of applying machine learning to HOL theorem proving.

1.1 Contribution and Overview

First, we develop a dataset for machine learning based on the proof steps used in a large interactive proof section 2. We focus on the HOL Light (Harrison, 2009) ITP, its multivariate analysis library (Harrison, 2013), as well as the formal proof of the Kepler conjecture (Hales et al., 2010). These formalizations constitute a diverse proof dataset containing basic mathematics, analysis, trigonometry, as well as reasoning about data structures such as graphs. Furthermore these formal proof developments have been used as benchmarks for automated reasoning techniques (Kaliszyk & Urban, 2014).

The dataset consists of 2,013,046 training examples and 196,030 testing examples that originate from 11,400 proofs. Precisely half of the examples are statements that were useful in the currently proven conjectures and half are steps that have been derived either manually or as part of the automated proof search but were not necessary in the final proofs. The dataset contains only proofs of non-trivial theorems, that also do not focus on computation but rather on actual theorem proving. For each proof, the conjecture that is being proven as well as its dependencies (axioms) and may be exploited in machine learning tasks. Furthermore, for each statement both its human-readable (pretty-printed) statement and a tokenization designed to make machine learning tasks more manageable are included.

Digital Age of Science

This project is one piece of a major long-term initiative of the International Math Union to digitize mathematical assets.
It is long been the aim of many in the mathematical community to build major digital libraries (1994, QED manifesto). In 2006, the International Mathematical Union (IMU) endorsed a statement envisioning a digital math library and that vision has grown over time. The early focus was on digitization, aggregation, metadata, and access.

The relationship between the computer and mathematics is decisively different from the relationship between the computer and the empirical sciences. The essential difference is that mathematics is capable of exact representation by computer, but the external world only admits approximate representation by computer. This difference has enormous implications for the correct architecture of mathematical databases. A database of formal math abstracts can capture true mathematical content in a way that say a database of chemical compounds never will.

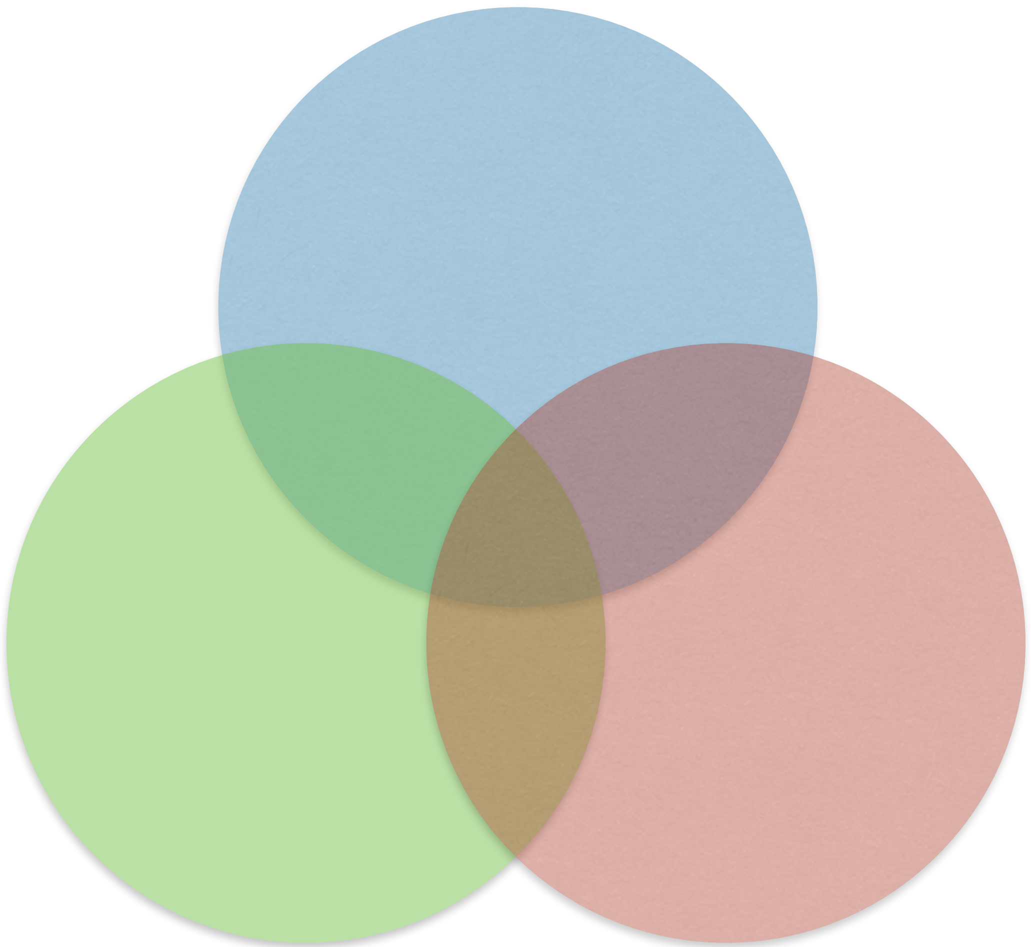
A concrete proposal: mathematical FABSTRACTS (formal abstracts)

Given today's technology, it is not reasonable to ask for all proofs to be formalized. But with today's technology, it seems that it should be possible to create a formal abstract service that

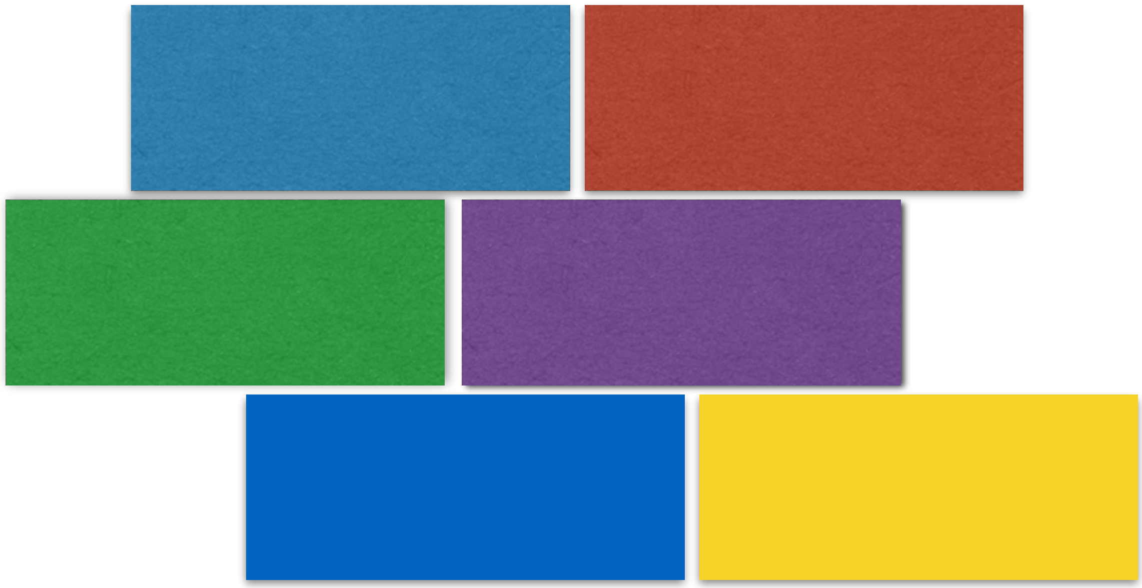
- Gives a statement of the main theorem(s) of each published mathematical paper in a language that is both human and machine readable,
- Links each term in theorem statements to a precise definition of that term (again in human/machine readable form), and
- Grounds every statement and definition is the system in some foundational system for doing mathematics.

Two responses to Russell's paradox

Set Theory (Zermelo)



Type Theory (Russell)



Sets mix.

Types never mix.

A Primer on Type Theory

$\mathbb{N}$ $\mathbb{R}$

3 3

$\mathbb{R}^3$

dependent types

$1 + 1 = 2$

p

Curry-Howard

HOL Light

HOL Light has an exquisite minimal design. It has the smallest kernel of any system. John Harrison is the sole

Mizar

Once the clear front-runner, it now shows signs of age. Do not expect
to understand the inner workings of this system unless you have been

Coq

Coq is built of modular components on a foundation of dependent type theory. This system has grown one PhD thesis at a time.

Isabelle

Designed for use with multiple foundational architectures, Isabelle's early
development featured classical constructions in set theory. However,

Metamath

Does this really work? Defying expectations, Metamath seems to function
shockingly well for those who are happy to live without plumbing.

Lean

Lean is ambitious, and it will be massive. Do not be fooled by the name.
"*Construction area keep out*" signs are prominently posted on the perimeter fencing.

Every foundational system needs to deal with subsets.

Most type systems in use for mathematics do not have an intrinsic notion of subtype.

Gonthier makes great efforts to accommodate subgroups in Coq (centralizers, normalizers, Sylow-subgroups, etc.). He rebrands *group theory* as *subgroup theory.* He considers the groups in a given context as all subgroups of a large *universal group.* This eliminates the difficulty of treating the carrier of each subgroup as a separate type. In some way it is a throwback to Weil's obsolete *Foundations of Algebraic Geometry*, which takes the fields in a given context of a given characteristic as all subfields of a large algebraically closed *universal domain*.

Even proof assistants based on set theory need to make decisions about subsets. In ZFC, we do not naturally have

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

The Mizar proof assistant achieves these inclusions by an act of butchery. The image of $\mathbb{N}$ in $\mathbb{Z}$ is excised from $\mathbb{Z}$ and replaced by $\mathbb{N}$, and so forth. But these decisions are quite arbitrary. Why not $\mathbb{Q} \subset \mathbb{Q}_p$?

The HOL Light proof assistant maintains the explicit embeddings:

$$\mathbb{N} \to \mathbb{Z}, \quad \mathbb{Z} \to \mathbb{R}, \quad \text{etc.},$$

(but $\mathbb{Q} \subset \mathbb{R}$).

Proof assistants also need to deal with identifications.

(Univalence offers a general solution to this issue, but is univalence inevitable? See Chris Kapulkin's talk today at 16:20.)

For example, we identify $\mathbb{Q}_p$ (the completion of the field $\mathbb{Q}$ with respect to the p-adic norm) with the field of fractions of $\mathbb{Z}_p$ (defined as an inverse limit of $\mathbb{Z}/p^n\mathbb{Z}$).

We identify

$$GL(2, \mathbb{A}) \quad \text{and} \quad \Pi'_v GL(2, \mathbb{Q}_v),$$

where $\mathbb{A} = \Pi'_v \mathbb{Q}_v$. However, the elements of one are matrices with coefficients in a restricted product of fields, but the right hand side is are restricted product of groups.

We identify $X \times (X \times X)$ with $(X \times X) \times X$, except when we don't.

This example illustrates how Lean is both a programming language and a theorem prover, allowing formal mathematics and its metadata to be combined seamlessly into a single document. We stress that the mathematics is machine readable by a computer proof assistant. We display the formal abstract in its raw (computer) form, but we anticipate that viewing tools will convert this raw format into English text, Mathematica notebook data, user friendly web browser display, MathSciNet data, and so forth:

```
-- the statement of Fermat's Last Theorem
axiom fermats_last_theorem :
∀ (x y z n : ℕ), x > 0 → y > 0 → n > 2 → x ^ n + y ^ n ≠ z ^ n

def paper : document := {
authors := [ {name := "Andrew Wiles"} ],
title := "Modular elliptic curves and Fermat's last theorem",
doi := "10.2307/2118559"
}

definition fabstract : fabstract := {
description := "This theorem bearing Fermat's name
was stated without proof by Pierre de Fermat in 1637
in the margins of his copy of Diophantus' Arithmetica.
Andrew Wiles announced a proof in 1994,
and his corrected proof was published in 1995."
sources := [cite.Document paper],
results := [result.Proof fermats_last_theorem]
}
```

Here is a fragment of the formal abstract for the statement of the Riemann hypothesis. The full formal abstract will include links to each of the definitions (such as the specification of the field of complex numbers):

```
def holomorphic_on (domain : set ℂ) (f : subtype domain → ℂ) :=
(∀ z : subtype domain, ∃ f'z,
has_complex_derivative_at (extend_by_zero domain f) f'z z)

class holomorphic_function :=
(domain : set ℂ)
(f : subtype domain → ℂ)
(open_domain : is_open domain)
(has_derivative : holomorphic_on domain f)

-- notation f(z), for holomorphic functions
instance : has_coe_to_fun holomorphic_function :=
{ F := λ h, subtype h.domain → ℂ, coe := λ h, h.f }

-- converges for Re(s) > 1
def riemann_zeta_sum (s : ℂ) : ℂ :=
Σ  (λ n,  complex.pow n  (-s) )

-- trivial zeros at -2, -4, -6,...
def riemann_zeta_trivial_zero (s : ℂ) : Prop :=
(∃ n : ℕ, n > 0 ∧ s = (-2)*n)

-- analytic continuation of Riemann zeta function.
axiom riemann_zeta_exists :
(∃! ζ : holomorphic_function, ζ.domain = (set.univ \ {1}) ∧
∀ s : subtype ζ.domain, re(s) > 1 → ζ(s) = riemann_zeta_sum s)

def ζ := classical.some riemann_zeta_exists

--  (s ≠ 1) implicit in the domain constraints:
def riemann_hypothesis :=
(∀ s, ζ(s) = 0 ∧ ¬(riemann_zeta_trivial_zero s) →
re (s) = 1/2)
```

Aise Johan de Jong

The Stacks Project

About

The Stacks project started in 2005. The initial idea was for it to be a collaborative web-based project with the aim of writing an introductory text about algebraic stacks. Temporarily there was a mailing list and some discussion as to how to proceed. For example, there are issues with referencing such a document, how to distribute credit, who does what, and many more. Although we have definite ideas about most of these points we would like to take a more positive approach. Namely, to simply create something and solve problems and answer questions as they come up.

We do want to answer a few basic questions that the casual visitor may have about this project:

1. The Stacks project is no longer an introductory text, but aims to build up
geometry as foundations for algebraic stacks. This implies a good deal o
algebra, schemes, varieties, algebraic spaces, has to be developed en ro
2. The Stacks project has a maintainer (currently Aise Johan de Jong) who a
proposed by contributors. Although everyone is encouraged to participa
3. The Stacks project is meant to be read online, and therefore we do not w
chapters, etc. Moreover, with hyperlinks it is possible to quickly browse
find the lemmas, theorems, etc. that a given result depends on.

Statistics

The Stacks project now consists of

- 600496 lines of code
- 18083 tags (58 inactive tags)
- 2918 sections
- 109 chapters
- 6214 pages
- 186 slogans

Lemma 6.30.4. *Let X be a topological space. Let $\mathcal{B}$ be a basis for the topology on X. Assume that for every pair $U, U' \in \mathcal{B}$ we have $U \cap U' \in \mathcal{B}$. For each $U \in \mathcal{B}$, let $C(U) \subset \text{Cov}_{\mathcal{B}}(U)$ be a cofinal system. Let $\mathcal{F}$ be a presheaf of sets on $\mathcal{B}$. The following are equivalent*

(1) *The presheaf $\mathcal{F}$ is a sheaf on $\mathcal{B}$.*

(2) *For every $U \in \mathcal{B}$ and every covering $\mathcal{U} : U = \bigcup U_i$ in $C(U)$ and for every family of sections $s_i \in \mathcal{F}(U_i)$ such that $s_i|_{U_i \cap U_j} = s_j|_{U_i \cap U_j}$ there exists a unique section $s \in \mathcal{F}(U)$ which restricts to s_i on U_i.*

Proof. This is a reformulation of Lemma 6.30.3 above in the special case where the coverings $\mathcal{U}_{ij}$ each consist of a single element. But also this case is much easier and is an easy exercise to do directly. □

« previous lemma next lemma »

numbers

View Lemma 6.30.4 as pdf

history

statistics

Comments (0)

There are also:

- 6 comment(s) on Section 6.30: Bases and sheaves

Post a comment

Stacks project in Lean

```
structure scheme :=
(α : Type u)
(T : topological_space α)
(O_X : presheaf_of_rings α)
(O_X_sheaf : is_sheaf_of_rings O_X)
(locally_affine : ∃ β : Type v, ∃ cov : β → {U : set α // T.is_open U},
  set.Union (λ b, (cov b).val) = set.univ ∧
  ∀ b : β, ∃ R : Type*, ∃ RR : comm_ring R, ∃ fR : (X R) → α,
    fR '' set.univ = (cov b).val ∧ -- thanks Johan Commelin!!
    open_immersion fR ∧ Π H : open_immersion fR,
    are_isomorphic_presheaves_of_rings
      (presheaf_of_rings_pullback_under_open_immersion O_X fR H)
      (structure_presheaf_of_rings_on_affine_scheme R)
)
```

Kevin Buzzard

```
definition scheme_of_affine_scheme (R : Type u) [comm_ring R] : scheme :=
{ α := X R,
  T := by apply_instance,
  O_X := zariski.structure_presheaf_of_rings R,
  O_X_sheaf := zariski.structure_presheaf_is_sheaf_of_rings R,
  locally_affine := begin
    existsi (punit : Type u),
    existsi (λ _, set.univ),
    existsi (λ _, is_open_univ),
    split,
    { intro x,
      existsi punit.star,
      trivial },
    intro _,
    existsi R,
    existsi _,tactic.swap,apply_instance,
    existsi id,
    split,
    { apply set.eq_univ_of_forall,
      intro x, existsi x, refl },
    existsi topological_space.open_immersion_id _,
    -- are_isomorphic_presheaves_of_rings
    -- (presheaf_of_rings_pullback_under_open_immersion (zariski.structure_presheaf_of_rings R) id H)
    -- (zariski.structure_presheaf_of_rings R)

    -- WAIT A MINUTE ISN'T THIS OBVIOUS
```

Kevin Buzzard

GitHub, Inc. (US) https://github.com/kbuzzard/lean-stacks-p

Tree: 6617de7dd5 lean-stacks-project / src / tag009L.lean

kbuzzard moving compactness of basis elts to 04PM

1 contributor

179 lines (172 sloc) 6.48 KB

```
/- The lemma in this tag says that if we have a top space
and a basis with the property that the intersection of two
basis elements is in the basis, then to give a sheaf on B
is to give a "sheaf on a cofinal system of covers of B".
In the application to schemes, this means a presheaf with
the property that it satisfies the sheaf axiom for
finite covers of basic opens by basic opens, noting that
the intersection of two basis opens is a basic open.
-/

import tag009J

universe u
-- A "standard" basis -- I just mean intersection of two basic opens is basic open.
-- Makes the sheaf axiom easier, and is satisfied in the case of Spec of a ring.
-- Below is the statement of the sheaf axiom for a given open cover in this case.
definition sheaf_property_for_standard_basis
  {X : Type u} [T : topological_space X]
  {B : set (set X)}
  (HB : topological_space.is_topological_basis B)
  (FPTB : presheaf_of_types_on_basis HB)
  (Hstandard : ∀ {U V : set X}, B U → B V → B (U ∩ V))
  (U : set X)
  (BU : B U)
```

Kenny Lau

Imperial College London

Local Langlands Correspondence in the Abelian Case

Kenny Lau

Torus

In Algebraic Geometry, a torus is an affine algebraic group T over a field F such that there is a finite Galois extension K of F with the property that $T \times_F \mathrm{Spec}(K)$ is isomorphic to $\mathrm{Spec}(K[\mathbb{Z}^n])$ for some n as affine algebraic groups. In that case, we call T an F-torus that splits over K. If $K = F$, we call it a split torus.

Here are some objects associated to T:

1. $X^*(T) := \mathrm{Hom}_{K\text{-}\mathbf{GS}}(T_K, GL_1)$, its **character group**;
2. $X_*(T) := \mathrm{Hom}_{K\text{-}\mathbf{GS}}(GL_1, T_K)$, its **cocharacter group**;
3. $\widehat{T} := \mathrm{Hom}_{\mathbf{Ab}}(X_*(T), \mathbb{C}^\times)$;
4. ${}^L T := \widehat{T} \rtimes \mathrm{Gal}(K/F)$, its **Langlands dual**

where:

- $GL_1 := \mathrm{Spec}(K[\mathbb{Z}])$;
- K-**GS** is the category of group schemes over K

Note that the Langlands dual is a topological group, since $\widehat{T}$ is a finite product of copies of $\mathbb{C}^\times$, and so ${}^L T$ is a finite union of copies of $\widehat{T}$.

Weil group

If F is a non-archimedean local field, fix an algebraic closure $\overline{F}$ of F. The **Weil group** $W_{\overline{F}/F}$ is defined to be:

$$\{\sigma \in \mathrm{Gal}(\overline{F}/F) \ : \ \sigma|_{F^{ur}} = \mathrm{Frob}^k \ \text{ for some } k \in \mathbb{Z}\}$$

where F^{ur} is the maximal unramified extension of F and Frob is Frobenius map. Local class field theory says that $W^{ab}_{\overline{F}/F} \cong F^\times$ canonically. If K is a finite Galois extension of F, then $W_{\overline{F}/K}$ is a normal subgroup of $W_{\overline{F}/F}$, since they fit in this short exact sequence:

$$1 \longrightarrow W_{\overline{F}/K} \longrightarrow W_{\overline{F}/F} \longrightarrow \mathrm{Gal}(K/F) \longrightarrow 1$$

Then, we define the **relative Weil group** $W_{K/F} := W_{\overline{F}/F}/W^c_{\overline{F}/K}$, where $W^c_{\overline{F}/K}$ denotes the closure of the commutator of $W_{\overline{F}/K}$. We have this short exact sequence:

$$1 \longrightarrow K^\times \longrightarrow W_{K/F} \longrightarrow \mathrm{Gal}(K/F) \longrightarrow 1$$

Similar groups can be constructed for the two archimedean local fields based on the last short exact sequence.

Example: The Trivial Case

Let us consider the simplest case, i.e. the case where the torus is just GL_1, i.e. $\mathrm{Spec}(F[\mathbb{Z}])$. This torus is split, and $W_{F/F} = F^\times$ acts on $\widehat{T} = \mathbb{C}^\times$ trivially, and $T(F)$ is just $F^\times$. Since the action is trivial, cohomological classes are just group homomorphisms, so the theorem is verified since both sides are the same. The actual content in this case is actually the fact that $W_{F/F} = F^\times$, which is the main theorem of local class field theory. Therefore, local Langlands Correspondence for GL_1 is just local class field theory.

Statement and Motivation of Theorem

The theorem states that for any local field F, finite galois extension K, T an F-torus that splits over K, there is a canonical bijection:

$$H^1_c(W_{K/F}, \widehat{T}) \to \mathrm{Hom}_{\mathbf{TopGrp}}(T(F), \mathbb{C}^\times)$$

where:

- **TopGrp** is the category of topological groups;
- $T(F)$ is the F-points of the torus T

Langlands is interested in representations of affine algebraic groups in general, GL_n in particular, not just for tori. However, since a torus is isomorphic to $(GL_1)^n$ after a base change, it becomes a slight generalization of local class field theory (see above), a stepping stone for the greater Langlands correspondence. Langlands wants to parametrize the representations (i.e. the right hand side of the bijection) by representations of the Weil group onto the Langlands dual. Note that we are only interested in one-dimensional representations since all irreducible representations of $T(F)$ is one-dimensional.

Example: The Actual Torus

The torus everyone is familiar with is $(S^1)^2$ where $S^1 \subseteq \mathbb{R}^2$ is the unit circle. We shall build the correspondent torus in the algebraic geometry land.

Classically, $S^1 = \{(x,y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$, so we can build an affine $\mathbb{R}$-scheme whose $\mathbb{R}$-points is S^1, namely $\mathrm{Spec}(\mathbb{R}[X,Y]/(X^2+Y^2-1))$, which we call S^1 from now on. $\mathbb{R}$-product of affine schemes correspond to $\mathbb{R}$-tensor product of the coordinate rings, so we get $(S^1)^2 = \mathrm{Spec}(\mathbb{R}[X,Y,Z,W]/(X^2+Y^2-1, W^2+Z^2-1))$.

To see that it is actually an torus, note that the scheme after base change to $\mathbb{C}$ is just $\mathrm{Spec}(\mathbb{C}[\mathbb{Z}^2])$, identifying $X+iY$ with $(1,0)$, $X-iY$ with $(-1,0)$, $Z+iW$ with $(0,1)$, and $Z-iW$ with $(0,-1)$.

Representation of Weil group

We consider continuous group homomorphisms φ making the diagram commute:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & W_{\overline{F}/K} & \longrightarrow & W_{\overline{F}/F} & \longrightarrow & \mathrm{Gal}(K/F) & \longrightarrow & 1 \\
 & & & & \downarrow \varphi & & \downarrow \mathrm{id} & & \\
1 & \longrightarrow & \widehat{T} & \longrightarrow & {}^L T & \longrightarrow & \mathrm{Gal}(K/F) & \longrightarrow & 1
\end{array}$$

We obtain a homomorphism $\varphi' : W_{\overline{F}/K} \to \widehat{T}$ in the second column. The codomain is abelian, so $\ker \varphi' \subseteq W^c_{\overline{F}/K}$. This gives a homomorphism $\varphi^* : W_{K/F} \to {}^L T$. Viewing the underlying set of ${}^L T$ as a cartesian product, the second coordinate of $\varphi^*(\sigma)$ is determined by σ, so we can focus on the first coordinate, i.e. $\pi_1 \circ \varphi^* : W_{K/F} \to \widehat{T}$. This is not a group homomorphism, but a crossed homomorphism, i.e. a 1-cocycle. The isomorphism classes of such φ correspond to continuous cohomology classes of degree 1, denoted $H^1_c(W_{K/F}, \widehat{T})$.

Implementation in Lean

I formalized the important parts and the fundamental parts of the statement of this theorem in Lean, a proof assistant. My Github repo is located at: `https://github.com/kckennylau/local-langlands-abelian`.

Here is a list of the files in my repo as of June 18: `Weil_group.lean`, `abelianization.lean`, `algebra.lean`, `algebra_tensor.lean`, `field_extensions.lean`, `group_cohomology.lean`, `monoid_ring.lean`, `polynomial.lean`, `quotient_group.lean`, `statement.lean`, `tensor_product.lean`, `topological_group.lean`, `torus.lean`.

There is currently 3102 lines in the repo.

The statement of the theorem becomes:

```
H1c (relative_Weil_group F AC W ht.split)
(torus.hat F AC T ht) ≃ topological_group_hom
(torus.rat_pt F AC T ht) (units ℂ)
```

References

[1] K. Buzzard. Trivial Remarks About Tori. accessed June 8 2018 http://wwwf.imperial.ac.uk/~buzzard/maths/research/notes/trivial_remarks_about_tori.pdf

[2] J.S. Milne. Basic Theory of Affine Group Schemes. 2012

[3] J. Tate. Number Theoretic Background. 1979

Representation of Weil group

We consider continuous group homomorphisms φ making the diagram commute:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & W_{\overline{F}/K} & \longrightarrow & W_{\overline{F}/F} & \longrightarrow & \mathrm{Gal}(K/F) & \longrightarrow & 1 \\ & & & & \big\downarrow{\scriptstyle \varphi} & & \big\downarrow{\scriptstyle \mathrm{id}} & & \\ 1 & \longrightarrow & \widehat{T} & \longrightarrow & {}^L T & \longrightarrow & \mathrm{Gal}(K/F) & \longrightarrow & 1 \end{array}$$

We obtain a homomorphism $\varphi' : W_{\overline{F}/K} \to \widehat{T}$ in the second column. The codomain is abelian, so $\ker \varphi' \subseteq W_{\overline{F}/K}^c$. This gives a homomorphism $\varphi^* : W_{K/F} \to {}^L T$. Viewing the underlying set of ${}^L T$ as a cartesian product, the second coordinate of $\varphi^*(\sigma)$ is determined by σ, so we can focus on the first coordinate, i.e. $\pi_1 \circ \varphi^* : W_{K/F} \to \widehat{T}$. This is not a group homomorphism, but a crossed homomorphism, i.e. a 1-cocycle. The isomorphism classes of such φ correspond to continuous cohomology classes of degree 1, denoted $H_c^1(W_{K/F}, \widehat{T})$.

Implementation in Lean

I formalized the important parts and the fundamental parts of the statement of this theorem in Lean, a proof assistant. My Github repo is located at: `https://github.com/kckennylau/local-langlands-abelian`.

Other Lean Sessions ICMS

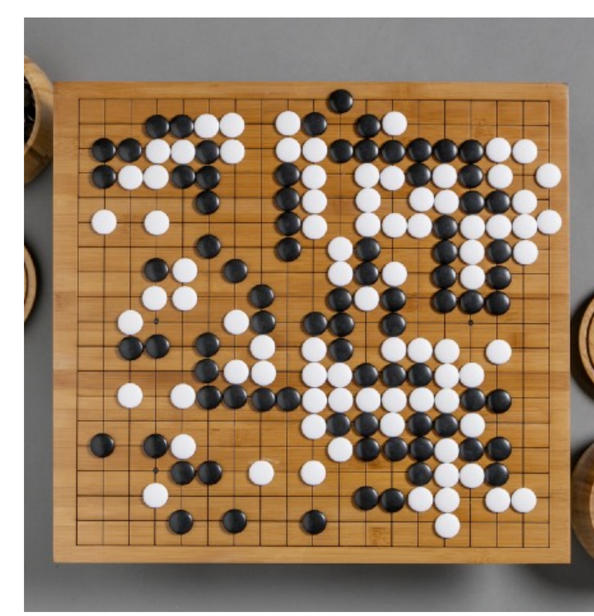
Wed 15:30 Mario Carneiro: Lean 3 Mathematical Library

Wed 15:55 Rob Lewis: Interface between Lean and Mathematica

Hypergame Paradox

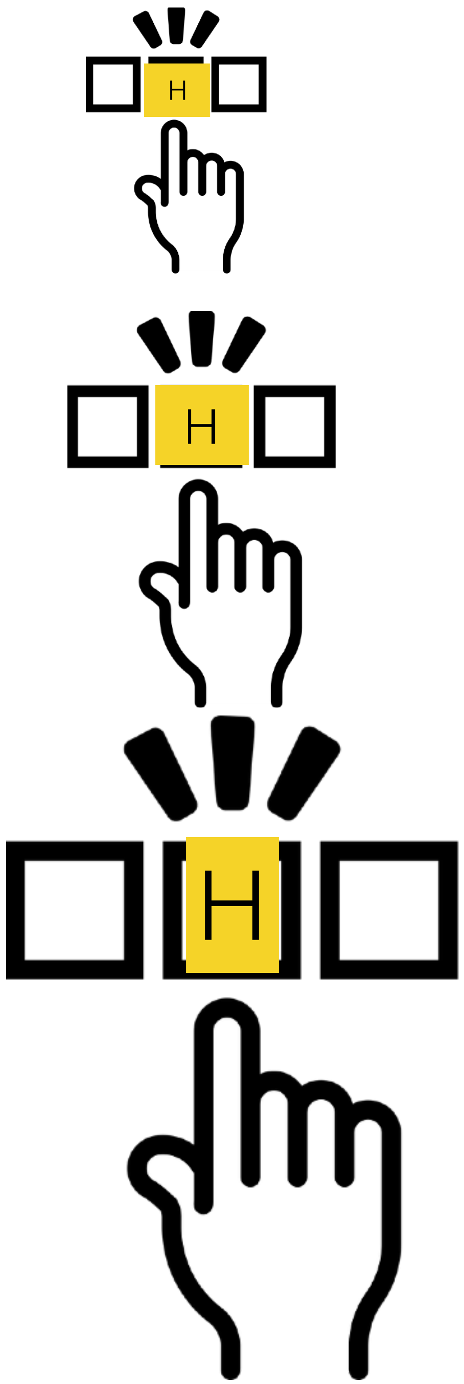
(Zwicker 1987)

- 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.?

Version 1

```
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

```
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.

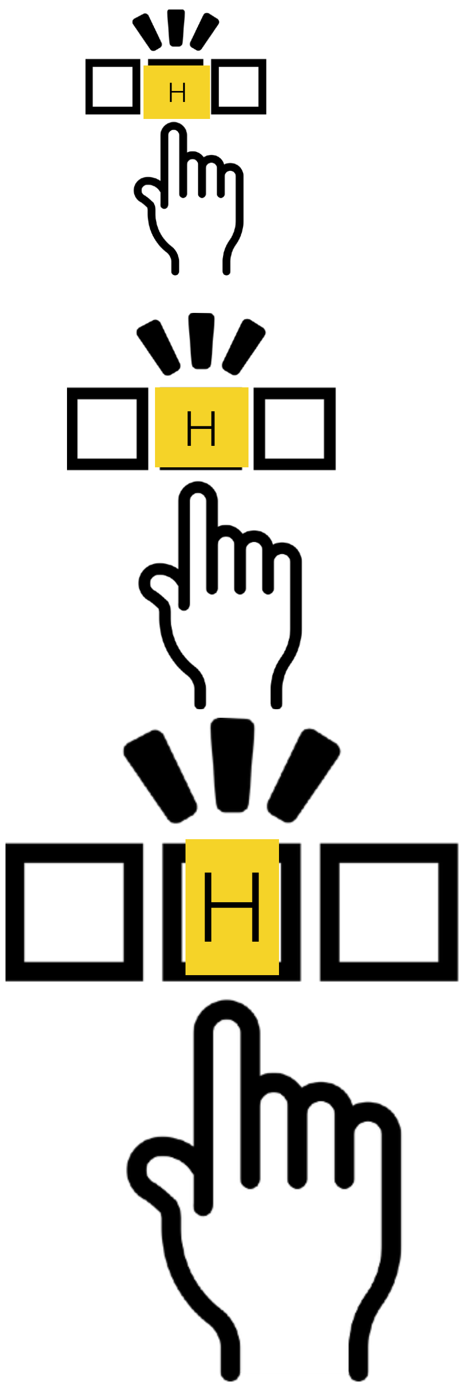
```
universe u

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.



The technology has reached maturity. Major projects involving hundreds of thousands of lines of computer code have been completed. Here are the *big four* :

- SeL4: the formal verification of the microkernel of an operating system;
- CompCert: the formal verification of a C compiler;
- Feit-Thompson Odd Order Theorem: the formal verification of a major result in finite group theory;
- the formal verification of the proof of the sphere packing problem (the Kepler conjecture) in three dimensional Euclidean space.

Formal Abstracts in Mathematics

FAB
STRACTS

A concrete proposal: mathematical FABSTRACTS (formal abstracts)

Given today's technology, it is not reasonable to ask for all proofs to be formalized. But with today's technology, it seems that it should be possible to create a formal abstract service that

- Gives a statement of the main theorem(s) of each published mathematical paper in a language that is both human and machine readable,
- Links each term in theorem statements to a precise definition of that term (again in human/machine readable form), and
- Grounds every statement and definition is the system in some foundational system for doing mathematics.

The definitions of mathematics

The Oxford English dictionary (2nd edition) has 273,000 headwords and over 600,000 word forms. (The longest entry is for the word set, which continues for 25 pages).

Medicine has a specialized terminology of approximately 250,000 items [Kucharz].

The Math Subject Classification (MSC) lists over 6000 subfields of mathematics.

https://en.wikipedia.org/wiki/Normal

Search

What is normal in math?

There are many unrelated notions of "normality" in mathematics.

Algebra and number theory [edit source]

- Normal basis (of a Galois extension), used heavily in cryptography
- Normal degree, a rational curve on a surface that meets certain conditions
- Normal domain (integrally closed domain), a ring integrally closed in its fraction field
  - Normal ring, a reduced ring whose localizations at prime ideals are integrally closed domains
  - Normal scheme, an algebraic variety or scheme that meets certain conditions
- Normal extensions (or quasi-Galois) field extensions, splitting fields for a set of polynomials over the base field
- Normal variety, a projective variety embedded by a complete linear system, as in a rational normal scroll (unrelated to the concept of normal scheme above)
- Normal order of an arithmetic function, a type of asymptotic behavior useful in number theory
- Normal subgroup, a subgroup invariant under conjugation

Analysis [edit source]

- Normal family, a pre-compact family of continuous functions
- Normal number, a real number with a "uniform" distribution of digits
- Normal number (computing), a floating-point number within the balanced range supported by a given format (unrelated to the previous notion)
- Normal operator, an operator that commutes with its Hermitian adjoint
  - Normal matrix, a complex square matrix that meets certain conditions
- Normal modes of vibration in an oscillating system

Geometry [edit source]

- Normal (geometry), a vector perpendicular to a surface (normal vector)
- Normal bundle, a term related to the preceding concept
- Normal cone, of a subscheme in algebraic geometry
- Normal coordinates, in differential geometry, local coordinates obtained from the exponential map (Riemannian geometry)
- Normal invariants, in geometric topology
- Normal polytopes, in polyhedral geometry and computational commutative algebra
- Normal space (or T_4) spaces, topological spaces characterized by separation of closed sets

Logic and foundations [edit source]

- Normal function, in set theory
- Normal measure, in set theory

Mathematical physics [edit source]

- Normal order or Wick order in Quantum Field Theory

Probability and statistics [edit source]

- Normal, the middle 95% of a bell curve (see 1.96)
- Normal distribution, the Gaussian continuous probability distribution

Other mathematics [edit source]

- Normal form (disambiguation)
- Normalization (disambiguation)

What is a group?

Definitions of group (algebra)

- A group is a set with a binary operation, identity element, and inverse operation, satisfying axioms of associativity, inverse, and identity.
- A group object in a category. A group in the first sense is a group object in the category of sets. A Lie group is a group object in the category of smooth manifolds. A topological group is a group object in the category of topological spaces. An affine group scheme is a group object in the category of affine schemes. (Caution: the Zariski product topology is not the product topology.)
- A Poisson-Lie group a group object in the category of Poisson manifolds, except that the inverse operation is not required to be a morphism of Poisson manifolds. (In

What is a group?

general, the inverse is an anti-Poisson morphism.)

- A quantum group is an object in the opposite category to the category of Hopf algebras.
- A compact matrix quantum group is a C^*-algebra with additional structure (Woronowicz).
- A strict 2-group is a group object in the category of categories (or a category object in the category of groups).
- A 2-group ...
- An n-group ...

Project: give formal abstracts for next week's Fields medals.

Popular candidates for next week's Fields medal, according to `https://poll.pollcode.com/44839318_result?v`

- Peter Scholze 1246 votes
- Fernando Coda Marques 946 votes
- Alesso Figalli 592 votes
- Geordie Williamson 422 votes
- Ciprian Manolescu 441 votes
- Simon Brendle 372 votes
- Maryna Viazovska 326 votes

How difficult are formal abstracts of their main theorems?

Scholze

Scholze - perfectoid spaces. There has been a discussion led by Kevin Buzzard about putting this work into the Lean theorem prover.

Michael Harris, “the concept of a perfectoid space is one of the most difficult notions ever introduced in arithmetic geometry, which has a long tradition of difficult notions.”

Fix a prime number p. A perfectoid field K is a complete non-archimedean field with residue characteristic p such that the value group of K^* in $\mathbb{R}_{>0}$ is not discrete, and such that the Frobenius (p-power) map

$$K^\circ/p \to K^\circ/p$$

is surjective, where $K^\circ = \{x \in K \mid |x| \leq 1\}$ is the *ring of integers* of K.

Marques

Marques: The Willmore energy of a torus immersed in $\mathbb{R}^3$ is at least $2\pi^2$.

(wiki) Let $v : M \to \mathbb{R}^3$ be a smooth immersion of a compact orientable surface, and give M a Riemannian metric from this immersion. Let $H : M \to \mathbb{R}$ be the mean curvature (the arithmetic mean of the principal curvatures κ_1 and κ_2 at each point). The Willmore energy is given by

$$W(M) = \int_M H^2 \, dA.$$

Figalli

Figalli - ?? - Improved versions of this and that in optimal transport.

Williamson

Williamson - algebraic proof of the Kazhdan-Lusztig conjectures.

Previous topic

Strong and weak tableaux

Next topic

Knutson-Tao Puzzles

This Page

Show Source

Quick search

Go

Enter search terms or a module, class or function name.

Kazhdan-Lusztig Polynomials

AUTHORS:

- Daniel Bump (2008): initial version
- Alan J.X. Guo (2014-03-18): `R_tilde()` method.

class `sage.combinat.kazhdan_lusztig.`**`KazhdanLusztigPolynomial`**(*W*, *q*, *trace=False*)

Bases: **`sage.structure.unique_representation.UniqueRepresentation`**, **`sage.structure.sage_object.SageObject`**

A Kazhdan-Lusztig polynomial.

INPUT:

- `W` – a Weyl Group
- `q` – an indeterminate

Manolescu

Manolescu - non-triangulable manifolds exist in any dimension greater than four.

A triangulation is a homeomorphism with the geometric realization of a simplicial complex.

Brendle

Brendle - sphere theorem strengthened to differentiable sphere theorem: If M is a complete, simply-connected, n-dimensional Riemannian manifold with sectional curvature taking values in the interval $(1, 4]$ then M is homeomorphic (and in fact, *diffeomorphic*) to the n-sphere.

Viazovska

Viazovska - No packing of congruent balls in eight-dimensional Euclidean space has density greater than the E_8 packing.

Why?

- bring the benefits of proof assistants to the general mathematical community;
- set standards for the sciences;
- set the stage for applications to ML in mathematical proofs;
- move math closer to the computer.

Partners: CMU, Pitt, Hanoi

Thang Long University, Hanoi, Vietnam

Mathematics Genealogy Project

Hoang Xuan Sinh

Ph.D. Université Paris Diderot - Paris 7 1975

Dissertation: *Gr-catégories*

Mathematics Subject Classification: 14—Algebraic geometry

Advisor: Alexander Grothendieck

Formal Abstracts mini-course,
Thang Long University,
Dec 29, 2017

Thank you!