Formal Abstracts
(SHALLOW-MATH)

Thomas Hales
March 27, 2017
Obergurgl

- I will discuss a vaporware project.
- The intended users for the project are mathematicians, and I am presenting the idea to this group hoping to generate discussion about implementation.
- This is joint nonwork with David Roe.

JOINT MATHEMATICS MEETINGS
AMERICAN MATHEMATICAL SOCIETY
MATHEMATICAL ASSOCIATION OF AMERICA

2016 JOINT MATHEMATICS

Largest Mathematics Meeting in the World

JANUARY 6-9 (WED-SAT), 2016 | WASHINGTON STATE CONVEN

- **Thursday January 7, 2016, 8:00 a.m.-11:50 a.m.**
  AMS Special Session on Mathematical Information in the Digital Age of Science, III
  Room 603, Washington State Convention Center
  Organizers:
  Patrick Ion, University of Michigan, Ann Arbor pion@umich.edu
  Olaf Teschke, zbMATH, Berlin
  Stephen Watt, University of Western Ontario
  - 8:00 a.m.
    Formal Proof.

Proposition 1.3.10 (Poincaré index theorem). *If S is a smooth surface and X is a vector field on S with isolated zeros, the Euler number of S is*

$$\chi(S) = \sum_{z \in \text{zeros}} i(X, z).$$

Consequently, the Euler number of a surface does not depend on the cell division used to compute it—it is a topological invariant.

Proof of 1.3.10. Given a finite cell division of S, start by replacing it with a differentiable triangulation, as discussed just before Proposition 1.3.3. Subdivide and jiggle the triangulation as necessary to make all the zeros lie inside faces, no more than one to a face. Enclose each zero with a polygon contained in a face and transverse to the field, as explained in the paragraph preceding Lemma 1.3.5. Triangulate the annulus formed by taking away the polygon from the face (Exercise 1.3.6). Finally, make the rest of the triangulation transverse, again by using the technique in the proof of Problem 1.3.4.

Each polygon's contribution to the Euler number is the index of the vector field at the corresponding zero. Each triangle's contribution outside the polygons is zero. This proves the formula.

The last sentence of the proposition follows because every closed surface admits a vector field with isolated zeros (Exercise 1.3.8).

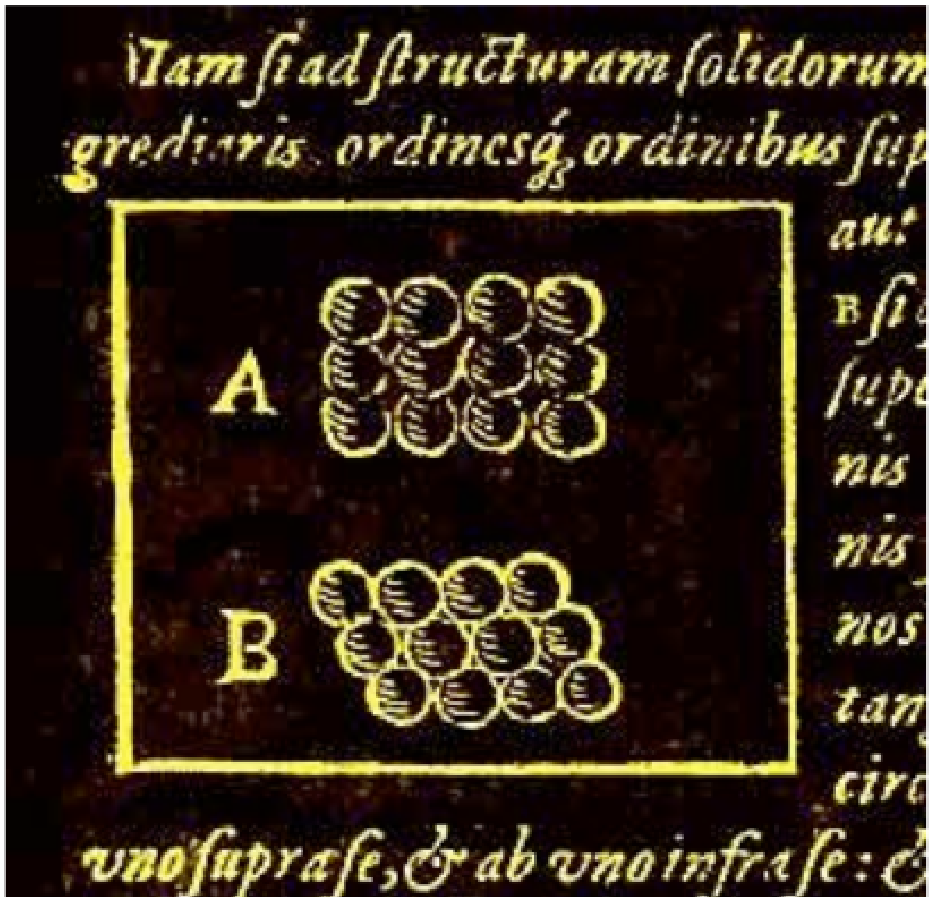
$\boxed{1.3.10}$

but what good is a tinkertoy set if the holes are all filled in with modeling clay?

In the present exposition, many of the "holes" or questions are explicitly labeled as exercises, questions, or problems. *Most of these are not walking-the-dog exercises* where the dog follows behind on a leash until the awaited event. You may or may not be able to answer the questions, even if you completely understand the text. Some of the questions form connections with ideas discussed more fully later on. Other questions have to do with details that otherwise would have been "left as an exercise for the reader." Still others relate the material under discussion to topics which are neither discussed nor assumed in the main text.

It is important to read through and think about the exercises, questions and problems. It should be possible to solve some of the more straightforward questions. But please don't be discouraged if you can't solve all, or even most, of the questions, any more than you are discouraged when you can't immediately answer questions which occur to you spontaneously.

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)



The Kepler conjecture asserts that no packing of congruent balls in $\mathbb{R}^3$ can have density greater than the face-centered cubic packing. The Kepler conjecture is a theorem whose proof relies on many computer calculations [31]. The Kepler conjecture has been formalized [(7)] in a combination of the HOL Light and Isabelle proof assistants [32]. This formalization has been a large collaborative effort.

|– "g ∈ PlaneGraphs" **and** "tame g" **shows** "fgraph g $\in_{\simeq}$ Archive"

$\vdash$ the_nonlinear_inequalities

$\vdash$ import_tame_classification $\wedge$
 the_nonlinear_inequalities $\wedge$
 $\Longrightarrow$ the_kepler_conjecture

$\vdash$ the_kepler_conjecture $\Longleftrightarrow$
 ($\forall$V. packing V
 $\Longrightarrow$ ($\exists$c. $\forall$r. &1 $\leq$ r
 $\Longrightarrow$ &(CARD(V $\cap$ ball(vec 0,r))) $\leq$
 $\pi * r^3$ / sqrt(&18) + c $* r^2$))

A FORMAL PROOF OF THE KEPLER CONJECTURE

THOMAS HALES, MARK ADAMS, GERTRUD BAUER, DANG TAT DAT, JOHN HARRISON, HOANG LE TRUONG, CEZARY KALISZYK, VICTOR MAGRON, SEAN MCLAUGHLIN, NGUYEN TAT THANG, NGUYEN QUANG TRUONG, TOBIAS NIPKOW, STEVEN OBUA, JOSEPH PLESO, JASON RUTE, ALEXEY SOLOVYEV, TA THI HOAI AN, TRAN NAM TRUNG, TRIEU THI DIEP, JOSEF URBAN, VU KHAC KY, ROLAND ZUMKELLER,

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.

We wish to acknowledge the help, support, influence, and various contributions of the following individuals: Nguyen Duc Thinh, Nguyen Duc Tam, Vu Quang Thanh, Vuong Anh Quyen, Catalin Anghel, Jeremy Avigad, Henk Barendregt, Herman Geuvers, Georges Gonthier, Daron Green, Mary Johnston, Christian Marchal, Laurel Martin, Robert Solovay, Erin Susick, Dan Synek, Nicholas Volker, Matthew Wampler-Doty, Benjamin Werner, Freek Wiedijk, Carl Witty, and Wenming Ye.

We wish to thank the following sources of institutional support: NSF grant 0503447 on the "Formal Foundations of Discrete Geometry" and NSF grant 0804189 on the "Formal Proof of the Kepler Conjecture," Microsoft Azure Research, William Benter Foundation, University of Pittsburgh, Radboud Research Facilities, Institute of Math (VAST), and VIASM.

WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikimedia Shop

Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools

Print/export

Create account Log in

Article Talk Read Edit View history Search

List of long proofs

From Wikipedia, the free encyclopedia

This is a list of unusually long mathematical proofs.

As of 2011, the longest mathematical proof, measured by number of published journal pages, is the classification of finite simple groups with well over 10000 pages. There are several proofs that would be far longer than this if the details of the computer calculations they depend on were published in full.

Contents [hide]

Long proofs [edit]

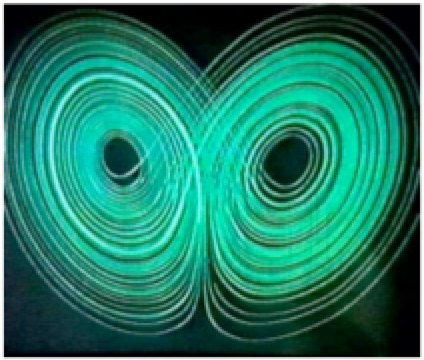
The length of unusually long proofs has increased with time. As a rough rule of thumb, 100 pages in 1900, or 200 pages in 1950, or 500 pages in 2000 is unusually long for a proof.

- 1799 The Abel–Ruffini theorem was nearly proved by Paolo Ruffini, but his proof, spanning 500 pages, was mostly ignored and later, in 1824, Niels Henrik Abel published a proof that required just six pages
- 1890 Killing's classification of simple complex Lie algebras, including his discovery of the exceptional Lie algebras, took 180 pages in 4 papers.
- 1894 The ruler-and-compass construction of a polygon of 65537 sides by Johann Gustav Hermes took over 200 pages.
- 1905 Lasker–Noether theorem Emanuel Lasker's original proof took 98 pages, but has since been simplified: modern proofs are less than a page long.
- 1963 Odd order theorem This was 255 pages long, which at the time was over 10 times as long as what had previously been considered a long paper in group theory.
- 1964 Resolution of singularities Hironaka's original proof was 216 pages long; it has since been simplified considerably down to about 10 or 20 pages.

+ Four-color theorem, Grothendieck, Weil conjectures, Harish-Chandra, Lafforgue, Langlands, Arthur, Almgren, Kepler conjecture, geometrization theorem, etc.

Mathematics is making the transition to computer based systems.

Birch-Swinnerton Dyer conjecture, Sato-Tate Conjecture, Lyons-Sims group of order $2^8 3^7 5^6 7^1 11^1 31^1 37^1 67^1$, original proof of the Calalan conjecture $x^m - x^n = 1$, $\mathtt{qWZ}$ proof of the Rogers-Ramunujan identities, conjectural optimal packings of tetrahedra (Chen-Engel-Glotzer), 4-color theorem, finite projective plane of order 10, Smale's 14th problem on strange attractors in the Lorenz oscillator, Mandelbrot's conjectures in fractal geometry, visualization of sphere eversions and Costa surface embeddings, the double bubble conjecture, construction of counterexamples to the Kelvin conjecture, calculation of kissing numbers (Sloane-Odlyzko), the character table for E^8 (Atlas project), Cohn-Kumar proof of the packing optimality of the Leech and E^8 packings among lattices, classification of fake projective planes, weak Goldbach, twin prime problem (2013).



On Digital Math Libraries

We should not compromise rigorous mathematical standards as we move from paper to computer. In fact, this is an opportunity to drastically improve standards. Many computer bugs are simply slips in logical and mathematical reasoning made by programmers and software designers.

- Mathematics influences the standards of scientific discourse, in the statistical sciences, in computer science, and throughout the sciences. If we promote sloppy platforms, the entire world will be worse off.
- Bugs in computer systems can lead to disaster: Intel Pentium FDIV bug, Ariane V explosion, . . .
- Bugs and design weaknesses in cryptographic software can be exploited by adversaries: Heartbleed, Logjam, Freak bug, . . .

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 idea of FORMAL-ABSTRACTS will be to start with tens of thousands of formal definitions to support all major areas of mathematics, and then to add formals statements of new theorems as they are published. We do not aim to do any formal proofs. We plan to use classical logic.

If we do not do proofs, there are various issues that come up.

- ▶ It is well-known in the formalization community that it is extremely difficult to get definitions correct until theorems are proved about the definitions.
- ▶ Mathematicians are notorious bad at giving the complete context needed for definitions.
- ▶ Example: one definition in the formal proof of the Kepler conjecture took nearly 40 revisions to get right.
- ▶ Various definitions are specifications that take a theorem asserting the existence of something, and that thing that exists is given a name. Definition building cannot take place without theorem proving.
- ▶ Building definitions requires non-obvious identifications: Qp is the completion of Q with respect to the nonarchimedean metric, and it is the tensor product of Q and Zp = the profinite limit of Z/p^nZ.
- ▶ Example: TFAE. Define X to be any of the equivalent Properties.

Solution: Do FORMAL-ABSTRACTS anyway.

Simple notions in math can have many views. For example the circle is both a group and a metric space.

A circle is a group, a metric space, a topological space, a homotopoy type, an Eilenberg Mac Lane space, a compact Lie group, a locally compact topological group, the Pontryagin dual of the integers, a compact torus, a Cartan subgroup of SU(2), a sphere, a parallelizable manifold, a real projective space, a unitary group, the suspension of two points, an ellipse of eccentricity 0, set of norm one elements of the field of complex numbers, the real points of a smooth projective curve of genus 0, the boundary of the Poincaré ball model of hyperbolic geometry.

Most of my experience is with HOL-Light. My test of the foundational power of a proof assistant is whether all the appropriate abelian categories (say of sheaves) have enough injectives. It is not clear that abelian categories in HOL-Light would have enough injectives.

```
(:A) <_c (:univ A) ∧
((:B) <_c (:univ A) ∧
 (:C) <_c (:univ A) ==>
 (:B → C) <_c (:univ A))
```

Other reasons I might move away from HOL-Light

- ▶ It is expensive to create new types.
- ▶ It has large libraries for real and complex analysis (which were indispensible for the formal proof of the Kepler conjecture),
but it is not clear that it will deal with more abstract parts of mathematics equally well.

I have been doing experiments in Lean with classical logic, which has various good features.

- It has a large presence in Pittsburgh.
- It seems to have learned from Gonthier's formal proof of Feit-Thompson.
- It has powerful type elaborations that does things like coercions, type classes (canonical classes), unification hints, implicit arguments,. . .

However, it is still very experimental and changes with annoying frequency.

Short term goals for FORMAL-ABSTRACTS

- ▶ Move beyond the subject areas of math that are traditionally covered by formalization projects.
- ▶ Clay Problem statements
- ▶ Automorphic Representation theory

The Clay Problems (million-dollar problems)

- ▶ Birch-Swinnerton-Dyer: elliptic curves and L-functions
- ▶ Poincaré conjecture: 3-sphere, manifold, homotopy
- ▶ Hodge conjecture: deRham cohomology (differential forms), complex varieties
- ▶ Navier Stokes equations: easy statement PDE in 3-dimension.
- ▶ P versus NP: easy statement (Turing machine)
- ▶ Riemann hypothesis: Riemann zeta function is in HOL-Light. Analytic continuation?
- ▶ Yang-Mills and mass gap: it probably cannot be stated formally. The problem requires the winner to build a theory.

Formalizing statements in Automorphic Representation Theory (a branch of number theory).

This will require a great deal of work just to state the theorems that are proved: algebraic geometry (schemes, motives, stacks, moduli spaces, and sheaves), measure theory and functional analysis, algebra (rings, modules, Galois theory, homological algebra, derived categories), category theory, complex analysis (L-functions and modular forms), class field theory (local and global), Lie theory and linear algebraic groups (Cartan classification and structure theory), representation theory (infinite dimensional, spectral theory), Shimura varieties, locally symmetric spaces, Hecke operators, cohomology (singular, deRham, intersection homology, l-adic), rigid geometry, perfectoid spaces,. . .