Interactions of Proof Assistants and Mathematics,

International Summer School, Regensburg

PART 1: FORMALISING MATHEMATICS IN ISABELLE/HOL

22/9/2023

Angeliki Koutsoukou-Argyraki

Royal Holloway, University of London, UK
and
University of Cambridge, UK

UNIVERSITY OF CAMBRIDGE

European Research Council
Established by the European Commission

Plan

PART 1:

* A brief discussion on the philosophy and motivation behind the use of proof assistants to formalise mathematics. A brief discussion on the state of the art and potential of the area.

* Basic information on Isabelle/HOL and available tools

(* Brief pointers to selected aspects of my work within ALEXANDRIA)

PART 2:

* Formalisation of Additive Combinatorics in Isabelle/HOL

Why formalise mathematics?

...a comment on my original personal motivation: insights into the nature of proofs

Work in applied proof theory/proof mining: pen-and-paper extraction of constructive/quantitative information from proofs in the form of computable bounds...

...Provokes the question:

What is it that makes a “good” proof?

* a shorter proof;

* a more “elegant” proof;

* a simpler proof (consider Hilbert’s 24th problem (1900)): “find criteria for simplicity of proofs, or, to show that certain proofs are simpler than any others.”;

* in terms of Reverse Mathematics – a proof in a weaker subsystem of Second Order Arithmetic;

* an interdisciplinary proof (e.g. a geometric proof for an algebraic problem or vice-versa would be considered to give a deeper mathematical insight);

* a proof that is easier to reuse i.e. if it provides some algorithm or technique or intermediate result that can be useful in different contexts too;

* a proof giving “better” computational content.

What do we mean by “better” computational content?

* a bound of lower complexity?

* a bound that is more precise numerically?

* a bound that is more “elegant”?

Why formalise mathematics?

* Verification: Mathematicians can be fallible. (Example: the Fields medalist Vladimir Voevodsky started working in formalisation after discovering errors in his own work).

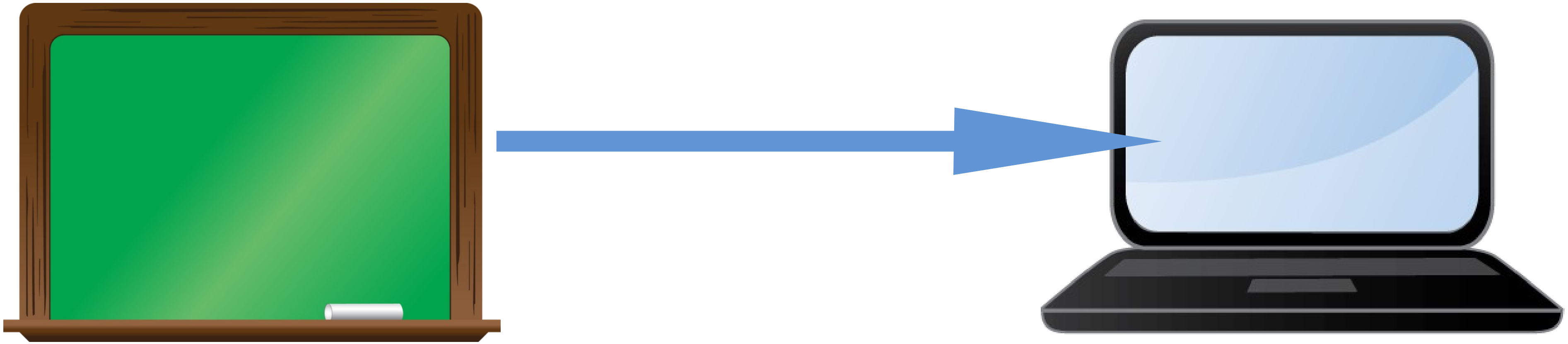
* (Future of?) Reviewing.

* Preserving mathematical knowledge in big libraries of formalised mathematics: databases with an enormous potential for the creation of future AI tools to assist mathematicians in the discovery(/invention) of new results.

Why formalise mathematics?

* Deeper understanding, new insights: even familiar material can be seen in a new light when using new tools. High level of detail in which a formalised proof must be written forces to think and rethink proofs and definitions.

The computer as a "magic mirror"



Why formalise mathematics?

* A way of keeping track of all the details of a complicated proof.

> the other way around! The Lean Proof Assistant was really that: An assistant in navigating through the thick jungle that this proof is. Really, one key problem I had when I was trying to find this proof was that I was essentially unable to keep all the objects in my "RAM", and I think the same problem occurs when trying to read the proof. Lean always gives you a clear formulation of the current goal, and Johan confirmed to me that when he formalized the proof of Theorem 9.4, he could — with the help of Lean — really only see one or two steps ahead, formalize those, and then proceed to the next step. So I think here we have witnessed an experiment where the proof assistant has actually assisted in understanding the proof.

(Peter Scholze, June 2021, Xena Project Blog)

* Educational tools.

* Last but not least: it is fulfilling and fun!

“We believe that when later generations look back at the development of mathematics one will recognise four important steps:

(1) the Egyptian-Babylonian-Chinese phase, in which correct computations were made, without proofs;

(2) the ancient Greeks with the development of “proof”;

(3) the end of the nineteenth century when mathematics became “rigorous”;

(4) the present, when mathematics (supported by computer) finally becomes fully precise and fully transparent.”

Barendregt, H. and Wiedijk, F. (The challenge of computer mathematics, Philos. Trans. - Royal Soc., Math. Phys. Eng. Sci. 36(1835):2351-2375 (2005)).

A vision for the future of research mathematics:

To create an interactive assistant that would help research mathematicians in their creative work by

* providing “brainstorming”/ hints:
proof recommendations, counterexamples, proofs of auxiliary lemmas/intermediate steps;
* suggesting conjectures;
* providing information on relevant literature results;
* helping with bookkeeping on the proof structure/proof goals and details;
* formally verifying the new results.

The goal is to assist mathematicians, not to replace them.

A bit of history

Leibniz (1666)

“Dissertatio de arte combinatoria”: proposes the development of a symbolic language that could express any rational thought (characteristica universalis) and a mechanical method to determine its truth (calculus ratiocinator). To resolve any dispute: “Let us calculate!”/ “Calculemus!”

Boole (1847)

“The mathematical analysis of logic”: propositional logic.

Frege (1879)

“Begriffsschrift”: an expressive formal language equipped with logical axioms and rules of inference.

A bit of history

Whitehead and Russell (1910-1913)

“Principia Mathematica”: (logicism) goal to express all mathematical propositions in symbolic logic & solve paradoxes of set theory. Developed type theory.

Hilbert (1920)

Formalism and Hilbert’s program: All mathematical statements should be written in a precise formal language, follow from a provably consistent finite system of axioms, according to well-defined rules. Completeness, Consistency, Conservation, Decidability.

Note: Gödel’s Incompleteness Theorems (1931)

A bit of history

de Bruijn (late 1960s)

AUTOMATH: a predecessor of modern proof assistants based on type theory. Used Curry–Howard correspondence. Late 1970's: van Benthem Jutting translated Landau's "Foundations of Analysis" into AUTOMATH.

The QED Manifesto (1994)

A proposal for a central computer-based library of all known mathematics fully formalised and formally verified (automatically checked by computers).

The project was soon abandoned.

(Or was it?)

Towards a new era in Mathematics?

A big shift: Formalisation was until recently an area of computer science. Now it is quickly attracting the interest of working mathematicians and mathematics students too. Enthusiastic online communities and tools e.g. Zulip enable massive collaborative projects. Libraries of formal proofs are expanding at an increasingly high pace, day-by-day. Student-run projects are emerging too. Everyone welcome to join.

* The 2020 Mathematics Subject Classification includes for the first time subject classes on the formalisation of mathematics using proof assistants (68VXX).

* Kevin Buzzard and Georges Gonthier invited at the 2022 International Congress of Mathematicians to talk about the formalisation of mathematics.

Main Obstacles

* Better automation is needed to provide proofs for intermediate proof steps (proofs are analysed in an extremely high level of detail).

* Efficient search features.

* Efficient organisation and management of libraries.

* Readability of formal proofs by humans.

* Interoperability of proof systems, translation of proofs between proof assistants needed (Goals of the Dedukti System/ EuroProofNet COST Action).

AI/ machine learning and the future of research mathematics

New advances in artificial intelligence and machine learning can promise novel developments in mathematical practice through their applications to automated theorem proving and proof assistants. E.g.: pattern recognition tools from machine learning can find applications in searching the libraries of formal proofs and in recognising proof patterns and providing proof recommendation methods thus enhancing automation.

The communities of machine learning and formal verification have been growing increasingly close during the past few years:

Successful conference series e.g. AITP, CICM, MATH-AI.

Isabelle – A Quick Introduction

Developed by Lawrence C. Paulson (since late 1980's),
Tobias Nipkow, Makarius Wenzel.

Interactive development of verifiable proofs

(Integrates automated reasoning tools in an interactive setting:

Proof scripts in Isabelle are interactive sessions between user and theorem prover)

- Isabelle/HOL: Higher Order Logic (HOL) (Includes AC; Proofs in classical logic). Simple types.
- Emphasis on producing structured, easy-to-read proofs:

  ISAR (Intelligible Semi-Automated Reasoning) proof language.
  Internal languages: ML and Scala.
- Features efficient automation (Sledgehammer and counterexample-finding tools like nitpick and Quickcheck).

cl.cam.ac.uk/research/hvg/Isabelle/index.html

Isabelle

UNIVERSITY C
CAMBRIDG
Computer Laborato

- Home
- Overview
- Installation
- Documentation

Site Mirrors:
Cambridge (.uk)
Munich (.de)
Sydney (.au)
Potsdam, NY (.us)

What is Isabelle?

Isabelle is a generic proof assistant. It allows mathematical formulas to be expressed in a formal language and provides tools for proving those fo logical calculus. Isabelle was originally developed at the University of Cambridge and Technische Universität München, but now includes numerous c from institutions and individuals worldwide. See the Isabelle overview for a brief introduction.

Now available: Isabelle2023 (September 2023)

Download for macOS

Download for Linux (Intel) - Download for Linux (ARM) - Download for Windows - Download for macOS

Hardware requirements:

- *Small experiments:* 4 GB memory, 2 CPU cores
- *Medium applications:* 8 GB memory, 4 CPU cores
- *Large projects:* 16 GB memory, 8 CPU cores
- *Extra-large projects:* 64 GB memory, 16 CPU cores

Some notable changes:

- Documents: interactive document preparation via Isabelle/jEdit panel.
- Documents: demos for well-known LaTeX classes.
- Documents: more formal LaTeX citations.
- HOL: various improvements of theory libraries, notably in HOL-Analysis.
- HOL: updates and improvements of Sledgehammer.
- ML: more robust support for ARM64 platform (native Apple Silicon).

Isabelle – A Quick Introduction

https://www.cl.cam.ac.uk/research/hvg/Isabelle/dist/library/HOL/index.html

Isabelle/HOL sessions

HOL

Classical Higher-order Logic.

HOL-Algebra

Author: Clemens Ballarin, started 24 September 1999, and many others

The Isabelle Algebraic Library.

HOL-Analysis
HOL-Analysis-ex
HOL-Auth

A new approach to verifying authentication protocols.

HOL-Bali
HOL-Cardinals

Ordinals and Cardinals, Full Theories.

HOL-Codegenerator_Test
HOL-Combinatorics
HOL-Complex_Analysis
HOL-Computational_Algebra
HOL-Corec_Examples

Corecursion Examples.

HOL-Data_Structures
HOL-Datatype_Benchmark

Big (co)datatypes.

HOL-Datatype_Examples

(Co)datatype Examples.

HOL-Decision_Procs

Various decision procedures, typically involving reflection.

Isabelle – A Quick Introduction

https://www.cl.cam.ac.uk/research/hvg/Isabelle/dist/library/HOL/HOL-Analysis/index.html

Session HOL-Analysis

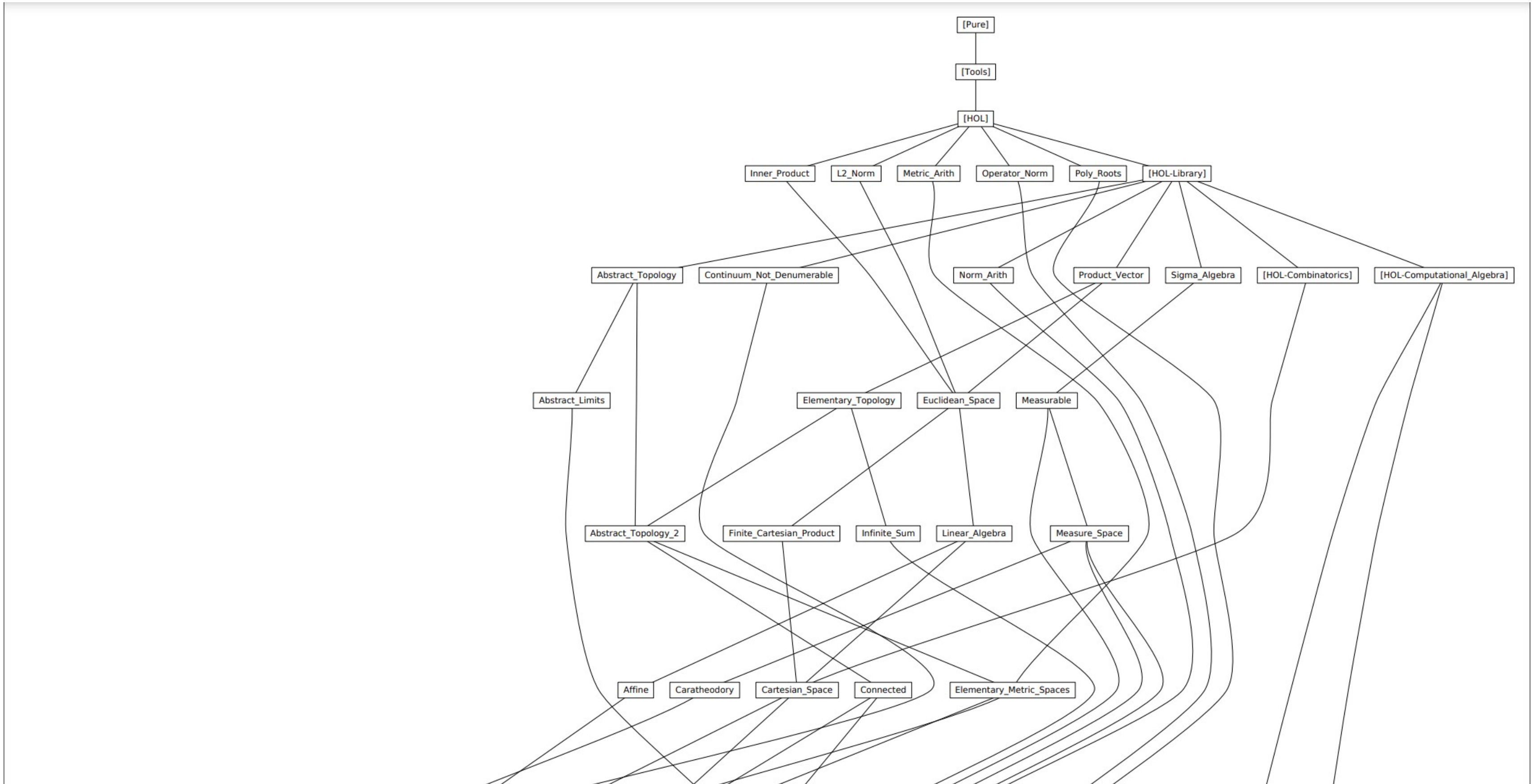
View theory dependencies
View document
View manual

Theories

- L2_Norm
- Inner_Product
- Product_Vector
- Euclidean_Space
- Linear_Algebra
- Affine
- Convex
- Finite_Cartesian_Product
- Cartesian_Space
- Determinants
- Elementary_Topology
- Abstract_Topology
- Abstract_Topology_2
- Connected
- Abstract_Limits
- Metric_Arith
    - File ‹metric_arith.ML›
- Elementary_Metric_Spaces

Isabelle – A Quick Introduction

Theory dependencies in the Analysis library
https://www.cl.cam.ac.uk/research/hvg/Isabelle/dist/library/HOL/HOL-Analysis/session_graph.pdf



Example of a structured proof in Isabelle/HOL

(from Theory Weierstrass_Theorems in the Isabelle Analysis Library)

```
lemma has_vector_derivative_polynomial_function:
  fixes p :: "real ⇒ 'a::euclidean_space"
  assumes "polynomial_function p"
  obtains p' where "polynomial_function p'" "⋀x. (p has_vector_derivative (p' x)) (at x)"
proof -
  { fix b :: 'a
    assume "b ∈ Basis"
    then
    obtain p' where p': "real_polynomial_function p'" and pd: "⋀x. ((λx. p x ∙ b) has_real_derivative p' x) (at x)"
      using assms [unfolded polynomial_function_iff_Basis_inner] has_real_derivative_polynomial_function
      by blast
    have "polynomial_function (λx. p' x *R b)"
      using ‹b ∈ Basis› p' const [where 'a=real and c=0]
      by (simp add: polynomial_function_iff_Basis_inner inner_Basis)
    then have "∃q. polynomial_function q ∧ (∀x. ((λu. (p u ∙ b) *R b) has_vector_derivative q x) (at x))"
      by (fastforce intro: derivative_eq_intros pd)
  }
  then obtain qf where qf:
      "⋀b. b ∈ Basis ⟹ polynomial_function (qf b)"
      "⋀b x. b ∈ Basis ⟹ ((λu. (p u ∙ b) *R b) has_vector_derivative qf b x) (at x)"
    by metis
  show ?thesis
  proof
    show "⋀x. (p has_vector_derivative (∑b∈Basis. qf b x)) (at x)"
      apply (subst euclidean_representation_sum_fun [of p, symmetric])
      by (auto intro: has_vector_derivative_sum qf)
  qed (force intro: qf)
qed
```

Isabelle – A Quick Introduction

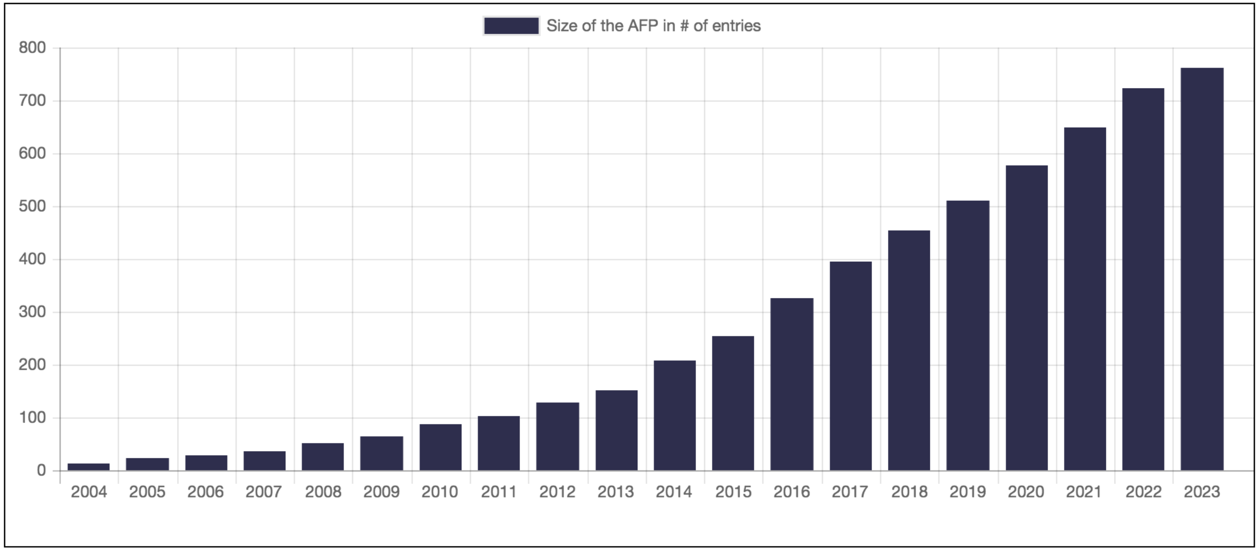
The Archive of Formal Proofs

A vast collection of formalised material in Mathematics, Computer Science and Logic.

Currently:

Number of Entries: 762
Number of Authors: 466
Number of Lemmas: ~244,000
Lines of Code: ~3,957,800

Growth in number of entries:



isa-afp.org

- Home
- Topics
- Download
- Help
- Submission
- Statistics
- About

Archive of Formal Proofs

The Archive of Formal Proofs is a collection of proof libraries, examples, and larger scientific developments, mechanically checked in the theorem prover **Isabelle**. It is organized in the way of a scientific journal, is indexed by **dblp** and has an ISSN: 2150-914x. Submissions are refereed and we encourage companion AFP submissions to conference and journal publications. To cite an entry, please use the **preferred citation style**.

A **development version** of the archive is available as well.

Search

2023

Ceva's Theorem
by **Mathias Schack Rabing** — Aug 16

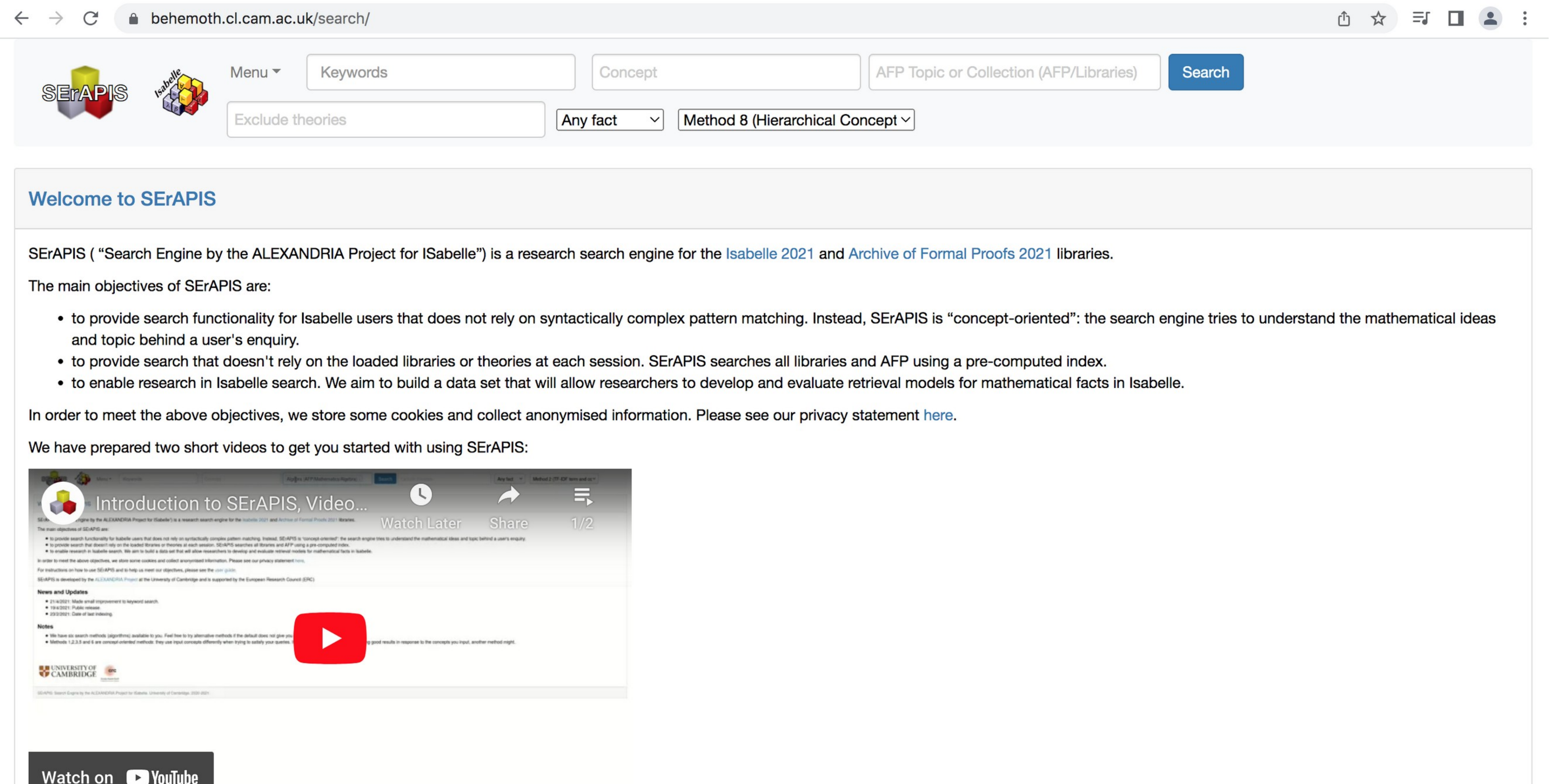
Fixed-length vectors
by **Lars Hupel** — Aug 14

Catoids, Categories, Groupoids
by **Georg Struth** — Aug 14

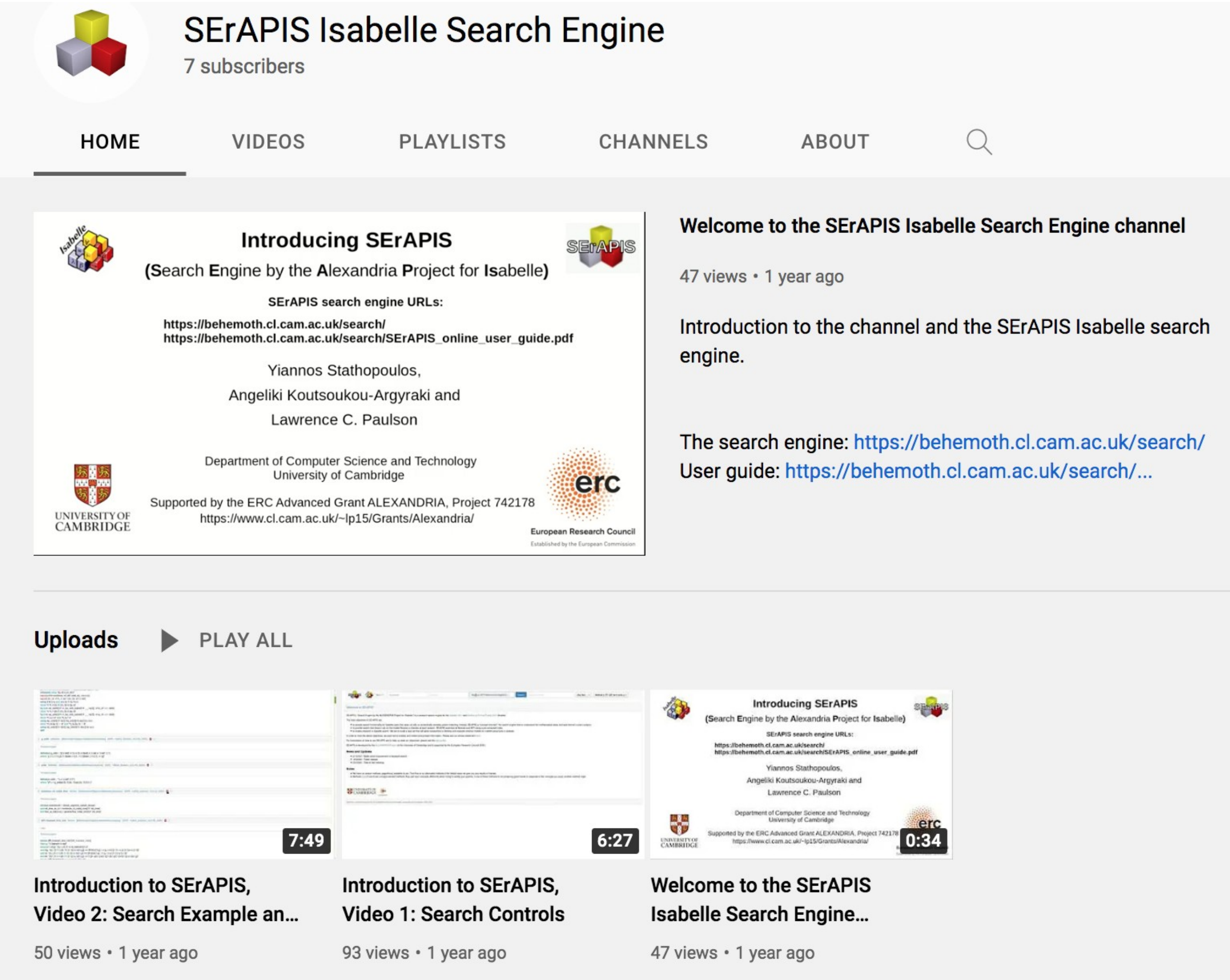
Polygonal Number Theorem
by **Kevin Lee**, **Zhengkun Ye** and **Angeliki Koutsoukou-Argyraki** — Aug 10

SErAPIS: A new, concept-oriented search engine for the Isabelle libraries and AFP

By Yiannos Stathopoulos and A. K.-A.



Please visit our YouTube channel for short demo videos, also see our user manual.



isabelle.systems

Isabelle Quick Access Links

Quick link: isabelle.systems/<code>, e.g. isabelle.systems/doc

- home: The official website and download page.

Communication

- dev-email: The Isabelle development e-mail list.
- dev: Isabelle development hub hosting the repository, ongoing tasks, build status information, etc.
- email: The Isabelle users e-mail list.
- zulip: Real-time discussion platform to exchange ideas, ask questions, and collaborate on Isabelle projects.

Infrastructure

- build: Build status information including performance statistics and graphs.
- ci: Isabelle/Jenkins continuous integration service.
- repo: The development repository.

Lawrence Paulson’s Blog:

lawrencecpaulson.github.io

Machine Logic

At the junction of computation, logic and mathematics

The formal verification of computer systems has become practical. It has an essential role in tech firms such as Amazon, AMD, Intel, Microsoft and Nvidia. In recent years, researchers have started asking whether verification technology could also benefit research mathematicians. Here, we explore every aspect of doing logic on the computer: its foundations, its applications and the issues involved with formalising mathematics.

Archive

`general` `examples` `Isabelle` `logic` `Isar` `Kurt_Gödel` `set_theory` `David_Hilbert`
`Archive_of_Formal_Proofs` `philosophy` `newbies` `NG_de_Bruijn` `Martin-Löf_type_theory` `verification`

A friendly online community of Isabelle users (from early beginners to experts) open to everyone:

plenty of direct help available! :-)

See stackoverflow

Also...

The Isabelle Zulip chat

isabelle.zulipchat.com/accounts/login/

ZULIP

Log in Sign up

Log in to Zulip

Isabelle

https://isabelle.zulipchat.com

A cool place for beginners and experts alike playing with mathematics and algorithms in the Isabelle theorem prover!

View without an account

OR

Email

Password

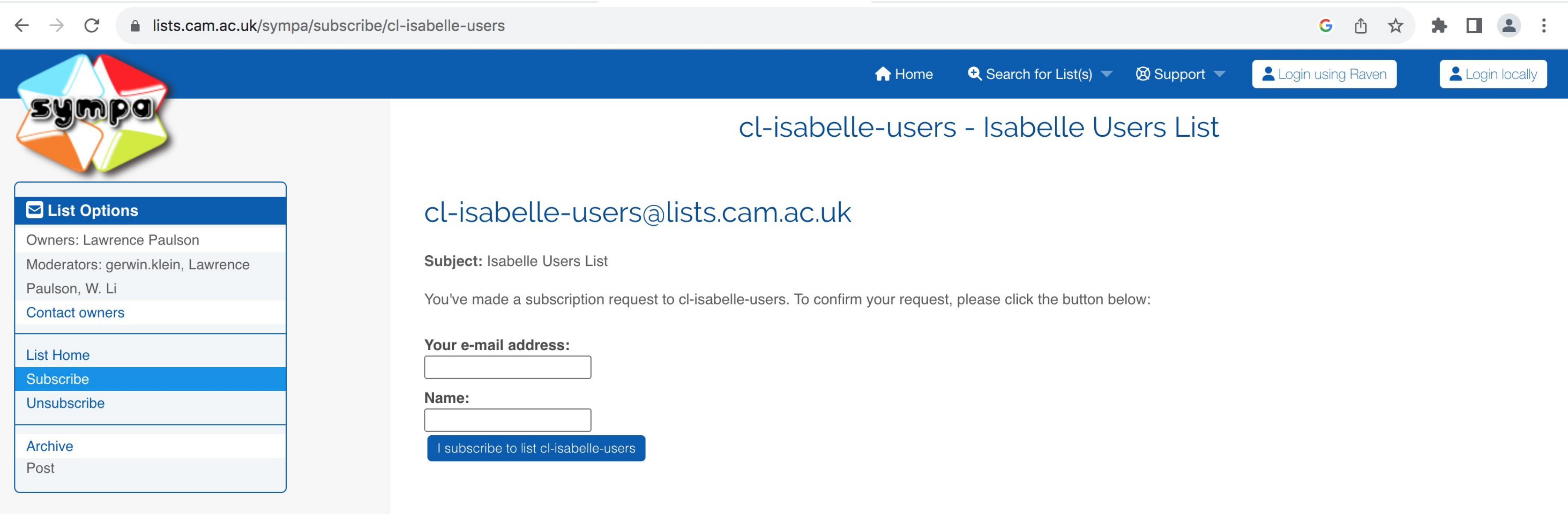
Log in

OR

Log in with Google

Log in with GitHub

The Isabelle mailing list



The ALEXANDRIA Project at Cambridge

Large Scale Formal Proof for the Working Mathematician
led by Professor Lawrence C. Paulson FRS (2017-2023)

https://www.cl.cam.ac.uk/~lp15/Grants/Alexandria/

UNIVERSITY OF CAMBRIDGE

- Expanding the body of formalised material on the Archive of Formal Proofs and the Isabelle Libraries.
- Case studies to explore the limits of formalisation.
- Tools for managing large bodies of formal mathematical knowledge (intelligent search/ computer-aided knowledge discovery).
- Automated and semi-automated environments and tools to aid *working mathematicians.*

erc
European Research Council
Established by the European Commission

Isabelle

SPRINGER LINK

Find a journal   Publish with us   Search

International Conference on Intelligent Computer Mathematics

↳ CICM 2023: **Intelligent Computer Mathematics** pp 3–15 | Cite as

Home > Intelligent Computer Mathematics > Conference paper

Large-Scale Formal Proof for the Working Mathematician—Lessons Learnt from the ALEXANDRIA Project

Lawrence C. Paulson

Conference paper | First Online: 28 August 2023

79 Accesses

Part of the Lecture Notes in Computer Science book series (LNAI,volume 14101)

UNIVERSITY OF CAMBRIDGE

European Research Council
Established by the European Commission

Selected contributions of mine within ALEXANDRIA

* Irrationality and Transcendence Criteria for Infinite Series in Isabelle/HOL (A.K.-A., Wenda Li & Lawrence C. Paulson, Experimental Mathematics, Special Issue on Interactive Theorem Proving in Mathematics Research, Vol. 31 , 2022- issue 2, pp. 401-412, online 21/10/2021).

AFP entries:
-Irrationality criteria for series by Erdős & Straus (A. K.-A. & Wenda Li, 2020). Original paper from 1974.
-The transcendence of certain infinite series (A. K.- A. & Wenda Li, 2019). Original paper by Hančl & Rucki (2005).
-Irrational rapidly convergent series (A. K.-A. & Wenda Li, 2018). Original paper by Hančl (2002).

Background material on infinite products (Paulson). Calculations with real asymptotics/limits. Reasoning with prime numbers.
Roth’s theorem on rational approximations assumed as a given.

Selected contributions of mine within ALEXANDRIA

Erdős & Straus (1974)

Let $\{b_n\}_{n=1}^{\infty}$ be a sequence of integers and $\{\alpha_n\}_{n=1}^{\infty}$ a sequence of positive integers with $\alpha_n > 1$ for all large n and

$$\lim_{n=1, n\to\infty} \frac{|b_n|}{\alpha_{n-1}\alpha_n} = 0.$$

Then the sum

$$\sum_{n=1}^{\infty} \frac{b_n}{\prod_{i=1}^{n} \alpha_i}$$

is rational if and only if there exists a positive integer B and a sequence of integers $\{c_n\}_{n=1}^{\infty}$ so that for all large n,

$$Bb_n = c_n\alpha_n - c_{n+1}, \ |c_{n+1}| < \alpha_n/2.$$

```
theorem theorem_2_1_Erdos_Straus :
  "(∑n. (b n / (∏i ≤ n. a i))) ∈ ℚ ⟷ (∃ (B::int)>0. ∃ c::nat⇒ int.
              (∀F n in sequentially. B*b n = c n * a n - c(n+1) ∧ ¦c(n+1)¦<a n/2))"
  using ab_rationality_imp imp_ab_rational by auto
```

Selected contributions of mine within ALEXANDRIA

Erdős & Straus (1974)

Let $\{\alpha_n\}_{n=1}^{\infty}$ and $\{b_n\}_{n=1}^{\infty}$ satisfy the hypotheses of the theorem above and in addition that for all large n we have $b_n > 0$, $\alpha_{n+1} \geq \alpha_n$, $\lim_{n\to\infty}(b_{n+1} - b_n)/\alpha_n \leq 0$ and $\liminf_{n\to\infty} \alpha_n/b_n = 0$. Then the sum

$$\sum_{n=1}^{\infty} \frac{b_n}{\prod_{i=1}^{n} \alpha_i}$$

is irrational.

```
corollary corollary_2_10_Erdos_Straus:
  assumes ab_event:"∀F n in sequentially. b n > 0 ∧ a (n+1) ≥ a n"
    and ba_lim_leq:"lim (λn. (b(n+1) - b n )/a n) ≤ 0"
    and ba_lim_exist:"convergent (λn. (b(n+1) - b n )/a n)"
    and "liminf (λn. a n / b n) = 0 "
  shows "(∑n. (b n / (∏i ≤ n. a i))) ∉ ℚ"
```

Selected contributions of mine within ALEXANDRIA

Erdős & Straus (1974)

Let p_n be the nth prime number and let $\{\alpha_n\}_{n=1}^{\infty}$ be a monotonic sequence of positive integers satisfying $\lim_{n\to\infty} p_n/\alpha_n^2 = 0$ and $\liminf_{n\to\infty} \alpha_n/p_n = 0$. Then the sum

$$\sum_{n=1}^{\infty} \frac{p_n}{\prod_{i=1}^{n} \alpha_i}$$

is irrational.

```
theorem theorem_3_10_Erdos_Straus:
  fixes a::"nat ⇒ int"
  assumes a_pos:"∀ n. a n >0" and "mono a"
    and nth_1:"(λn. nth_prime n / (a n)^2) ⟶ 0"
    and nth_2:"liminf (λn. a n / nth_prime n) = 0"
  shows "(∑n. (nth_prime n / (∏i ≤ n. a i))) ∉ ℚ"
```

Selected contributions of mine within ALEXANDRIA

Hančl (2002) Let $A > 1$ be a real number. Let $\{d_n\}_{n=1}^{\infty}$ be a sequence of real numbers greater than one. Let $\{\alpha_n\}_{n=1}^{\infty}$ and $\{b_n\}_{n=1}^{\infty}$ be sequences of positive integers such that $\lim_{n\to\infty} \alpha_n^{\frac{1}{2^n}} = A$ and for all sufficiently large n

$$\frac{A}{\alpha_n^{\frac{1}{2^n}}} > \prod_{j=n}^{\infty} d_j \quad \text{and} \quad \lim_{n\to\infty} \frac{d_n^{2^n}}{b_n} = \infty.$$

Then the sum

$$\sum_{n=1}^{\infty} \frac{b_n}{\alpha_n}$$

is irrational.

```
theorem Hancl3:
  fixes d ::"nat⇒real" and  a b :: "nat⇒int"
  assumes "A > 1" and d: "∀n. d n > 1" and a: "∀n. a n>0" and b: "∀n. b n > 0" and "s>0"
    and assu1: "(λn. (a n) powr(1 / of_int(2^n))) ⟶ A"
    and assu2: "∀n ≥ s. A / (a n) powr (1 / of_int(2^n)) > (∏j. d (n+j))"
    and assu3: "LIM n sequentially. d n ^ 2 ^ n / b n :> at_top"
    and "convergent_prod d"
  shows "(∑n. b n / a n) ∉ ℚ"
```

Selected contributions of mine within ALEXANDRIA

Hančl (2002) Let $A > 1$ and let $\{\alpha_n\}_{n=1}^{\infty}$ and $\{b_n\}_{n=1}^{\infty}$ be sequences of positive integers such that $\lim_{n\to\infty} \alpha_n^{\frac{1}{2^n}} = A$. Then, assuming that for every sufficiently large positive integer n, $\alpha_n^{\frac{1}{2^n}}(1+4(2/3)^n) \le A$ and $b_n \le 2^{(4/3)^{n-1}}$, the sum $\sum_{n=1}^{\infty} b_n/\alpha_n$ is irrational.

```
corollary Hancl3corollary:
  fixes A::real and  a b :: "nat⇒int"
  assumes "A > 1" and a: "∀n. a n>0" and b: "∀n. b n>0"
    and assu1: "(λn. (a n) powr(1 / of_int(2^n))) ⟶ A"
    and asscor2: "∀n ≥ 6. a n powr(1 / of_int (2^n)) * (1 + 4*(2/3)^n) ≤ A
                            ∧ b n ≤ 2 powr (4/3)^(n-1)"
  shows "(∑n. b n / a n) ∉ ℚ"
```

Selected contributions of mine within ALEXANDRIA

Hančl & Rucki (2005)

Let δ be a positive real number. Let $\{\alpha_n\}_{n=1}^\infty$ and $\{b_n\}_{n=1}^\infty$ be sequences of positive integers such that

$$\limsup_{n\to\infty} \frac{\alpha_{n+1}}{(\prod_{i=1}^n \alpha_i)^{2+\delta}} \cdot \frac{1}{b_{n+1}} = \infty$$

and

$$\liminf_{n\to\infty} \frac{\alpha_{n+1}}{\alpha_n} \cdot \frac{b_n}{b_{n+1}} > 1.$$

Then the sum

$$\sum_{n=1}^\infty \frac{b_n}{\alpha_n}$$

is transcendental.

Let δ and ϵ be positive real numbers. Let $\{\alpha_n\}_{n=1}^\infty$ and $\{b_n\}_{n=1}^\infty$ be sequences of positive integers such that

$$\limsup_{n\to\infty} \frac{\alpha_{n+1}}{(\prod_{i=1}^n \alpha_i)^{2+2/\epsilon+\delta}} \cdot \frac{1}{b_{n+1}} = \infty$$

and for every sufficiently large n

$$\sqrt[1+\epsilon]{\frac{\alpha_{n+1}}{b_{n+1}}} \geq \sqrt[1+\epsilon]{\frac{\alpha_n}{b_n}} + 1.$$

Then the sum

$$\sum_{n=1}^\infty \frac{b_n}{\alpha_n}$$

is transcendental.

Selected contributions of mine within ALEXANDRIA

```
theorem (in RothsTheorem) HanclRucki1:
  fixes a b ::"nat⇒int" and δ ::real
  defines "aa≡(λn. real_of_int (a n))" and "bb≡(λn. real_of_int (b n))"
  assumes a_pos:"∀ k. a k >0" and b_pos:"∀ k. b k >0" and "δ >0"
      and limsup_infy:"limsup (λ k. aa (k+1)/(∏i = 0..k. aa i)powr(2+δ)*(1/bb (k+1))) = ∞"
      and liminf_1:"liminf (λk. aa (k+1) / aa k * bb k / bb (k+1)) > 1"
  shows "¬ algebraic(suminf  (λ k. bb k / aa k))"
```

```
theorem (in RothsTheorem) HanclRucki2:
  fixes a b ::"nat⇒int" and δ ε ::real
  defines "aa≡(λn. real_of_int (a n))" and "bb≡(λn. real_of_int (b n))"
  assumes a_pos:"∀ k. a k >0" and b_pos:"∀ k. b k >0" and "δ >0"
    and "ε >0"
    and limsup_infi:"limsup (λ k.(aa (k+1)/(∏i = 0..k. aa i)powr(2+(2/ε) + δ))
            * (1/(bb (k+1)))) = ∞"
    and ratio_large:"∀ k. ( k ≥ t ⟶  (( aa(k+1)/bb( k+1)) ) powr(1/(1+ε))
                ≥  (( aa k/bb k) powr(1/(1+ε)))+1)"
  shows "¬ algebraic(suminf (λ k. bb k /aa k))  "
```

Selected contributions of mine within ALEXANDRIA

Roth (1955)

Let a be any algebraic number, not rational. If the inequality

$$|a - \frac{p}{q}| < \frac{1}{q^\kappa}$$

has infinitely many solutions in coprime integers p and q where $q > 0$, then $\kappa \leq 2$.

```
text ‹Since the proof of Roth's theorem has not been formalized yet, we formalize the statement in a locale
      and use it as an assumption.›
locale RothsTheorem =
  assumes RothsTheorem:"∀ξ κ. algebraic ξ ∧ ξ ∉ ℚ ∧ infinite {(p,q). q>0 ∧
            coprime p q ∧ ¦ξ - of_int p / of_int q¦ < 1 / q powr κ} ⟶ κ ≤ 2"
```

Selected contributions of mine within ALEXANDRIA

* Formalising Ordinal Partition Relations Using Isabelle/HOL (Mirna Džamonja, A. K.-A. & Lawrence C. Paulson, Experimental Mathematics, Special Issue on Interactive Theorem Proving in Mathematics Research, Vol. 31 , 2022-issue 2, pp. 383-400, online 11/10/2021)

Results in infinitary combinatorics and set theory by Erdős–Milner, Specker, Larson and Nash-Williams, leading to Larson's proof of an unpublished result by E.C. Milner.

AFP entries:

-Ordinal Partitions (Paulson, 2020).
-The Nash-Williams Partition Theorem (Paulson, 2020).
-Zermelo-Fraenkel Set Theory in Higher-Order Logic (Paulson, 2019).

Selected contributions of mine within ALEXANDRIA

* Formalising Szemerédi's Regularity Lemma and Roth's Theorem on Arithmetic Progressions in Isabelle/HOL (Chelsea Edmonds, A. K.-A. & Lawrence C. Paulson, Journal of Automated Reasoning, vol. 67, Article number: 2 (2023), online 19/12/2022.)

Fundamental results in extremal graph theory and combinatorics/number theory. (simultaneously and independently formalised in Lean by Mehta and Dillies)

AFP entries:

-Roth's Theorem on Arithmetic Progressions (Edmonds, A. K.-A. & Paulson, 2021).
-Szemerédi's Regularity Lemma (Edmonds, A. K.-A. & Paulson, 2021).

Main sources: book by Y. Zhao, notes from course by W. T. Gowers.

Selected contributions of mine within ALEXANDRIA

The *upper asymptotic density* of a set $A \subseteq \mathbb{Z}$ is defined as

$$\limsup_{N \to \infty} \frac{|A \cap [1, N]|}{N}.$$

Szemerédi (1975)

Every set of integers A with positive upper asymptotic density contains a k-term arithmetic progression for every $k \in \mathbb{N}$.

Roth (1953)

Every subset of the integers with positive upper asymptotic density contains a 3-term arithmetic progression.

```
theorem RothArithmeticProgressions:
  assumes "upper_asymptotic_density A > 0"
  shows "∃k d. d>0 ∧ progression3 k d ⊆ A"
```

For sets of vertices X, $Y \subseteq V(G)$, let $e(X,Y)$ be the number of edges between X and Y. That is,

$$e(X,Y) = |\{(x,y) \in X \times Y : xy \in E(G)\}|.$$

Given a graph G, for sets of vertices $X, Y \subseteq V(G)$, we define the edge density between X and Y to be

$$d(X,Y) = \frac{e(X,Y)}{|X||Y|}.$$

Given a graph G and $\epsilon > 0$, for sets of vertices X, $Y \subseteq V(G)$, we call (X,Y) an ϵ-regular pair (in G) if for all $A \subseteq X$, $B \subseteq Y$ with $|A| \geq \epsilon|X|$, $|B| \geq \epsilon|Y|$, one has

$$|d(A,B) - d(X,Y)| \leq \epsilon.$$

Given a graph G and $\epsilon > 0$, a partition $P = \{V_1, \dots, V_k\}$ of $V(G)$ is an ϵ-regular partition if

$$\sum_{\substack{(i,j)\in[k]^2 \\ (V_i, V_j) \text{ not } \epsilon\text{-regular}}} |V_i||V_j| \leq \epsilon|V(G)|^2.$$

Selected contributions of mine within ALEXANDRIA

Szemerédi (1975) Regularity Lemma

For every $\epsilon > 0$, there exists a constant M such that every graph has an ϵ-regular partition of its vertex set into at most M parts.

```
theorem Szemeredi_Regularity_Lemma:
  assumes "ε > 0"
  obtains M where "⋀G. card (uverts G) > 0 ⟹ ∃P. regular_partition ε G P ∧ card P ≤ M"
```

Selected contributions of mine within ALEXANDRIA

Triangle Counting Lemma

Given a graph G, let $X, Y, Z \subseteq V(G)$ so that $(X, Y), (Y, Z), (Z, X)$ are all ϵ-regular pairs for some $\epsilon > 0$. Assuming that $d(X, Y), d(X, Z), d(Z, Y) \geq 2\epsilon$, the number of triples $(x, y, z) \in X \times Y \times Z$ such that x, y, z form a triangle in G is at least

$$(1 - 2\epsilon)(d(X, Y) - \epsilon)(d(X, Z) - \epsilon)(d(Y, Z) - \epsilon)|X||Y||Z|.$$

```
theorem triangle_counting_lemma:
  fixes ε::real
  assumes xss: "X ⊆ uverts G" and yss: "Y ⊆ uverts G" and zss: "Z ⊆ uverts G" and en0: "ε > 0"
    and finG: "finite (uverts G)" and wf: "uwellformed G"
    and rp1: "regular_pair X Y G ε" and rp2: "regular_pair Y Z G ε" and rp3: "regular_pair X Z G ε"
    and ed1: "edge_density X Y G ≥ 2*ε" and ed2: "edge_density X Z G ≥ 2*ε" and ed3: "edge_density Y Z G ≥ 2*ε
  shows "card (triangle_triples X Y Z G)
        ≥ (1-2*ε) * (edge_density X Y G - ε) * (edge_density X Z G - ε) * (edge_density Y Z G - ε)*
           card X * card Y * card Z"
```

Selected contributions of mine within ALEXANDRIA

Triangle Removal Lemma

For all $\epsilon > 0$, there exists $\delta > 0$ such that any graph on N vertices with less than or equal to δN^3 triangles can be made triangle-free by removing at most ϵN^2 edges.

```
theorem triangle_removal_lemma:
  fixes ε :: real
  assumes egt: "ε > 0"
  shows "∃δ::real > 0. ∀G. card(uverts G) > 0 ⟶ uwellformed G ⟶
          card (triangle_set G) ≤ δ * card(uverts G) ^ 3 ⟶
          (∃G'. triangle_free_graph G' ∧ uverts G' = uverts G ∧ uedges G' ⊆ uedges G ∧
          card (uedges G - uedges G') ≤ ε * (card (uverts G)) ²)"
    (is "∃δ::real > 0. ∀G. _ ⟶ _ ⟶ _ ⟶ (∃Gnew. ?Φ G Gnew)")
```

Some other smaller formalisations of mine on the Archive of Formal Proofs

* A. K.-A., Amicable Numbers (2020):

Involves various relevant definitions, results and examples, as well as various rules for the generation of amicable pairs such as Thābit ibn Qurra's Rule, Euler's Rule, te Riele's Rule and Borho's Rule with breeders.

* A. K.-A., Aristotle’s Assertoric Syllogistic (2019):

Deductions shown very easily thanks to Isabelle’s automation.
Aristotle’s Metatheorem on reducing certain deductions to others becomes obvious from the formal proofs.
Isabelle’s counterexample automation tools detect need for assumptions.

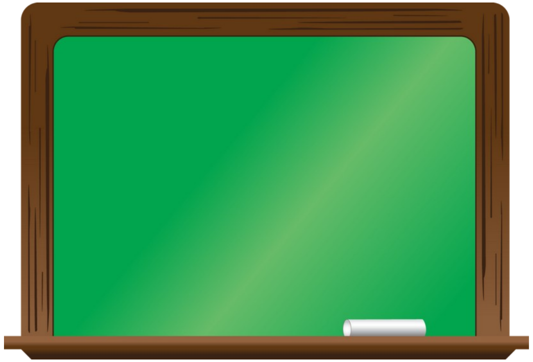
Some other smaller formalisations of mine on the Archive of Formal Proofs

* A. K.-A., Octonions (2018):

Basic theory of Octonions (normed division algebra over the real numbers) incl. various identities and properties of the octonions and of the octonionic product, a description of 7D isometries and representations of orthogonal transformations.
Developed theory of the vector cross product in 7D.
Inspired by the theory of Quaternions by Paulson (2018).

Thank you

(Stay tuned for PART 2 which will cover our series of recent formalisations in combinatorics...)



+

=