Topos Institute Colloquium 6/10/2022

THE NEW ERA OF FORMALISED MATHEMATICS AND THE ALEXANDRIA PROJECT

UNIVERSITY OF CAMBRIDGE

Angeliki Koutsoukou-Argyraki

Department of Computer Science and Technology
(Computer Laboratory)
University of Cambridge, UK

European Research Council

Established by the European Commission

Supported by the ERC Advanced Grant ALEXANDRIA 742178

Plan

* A discussion on the philosophy and motivation behind the use of proof assistants to formalise mathematics.

* A discussion on the current state of the art and potential of the area: recently the area has seen a big boost, with fast-expanding, flourishing communities attracting computer scientists and mathematicians.

(Other past related talks on this topic at the Topos Institute Colloquium: by Kevin Buzzard, Jeremy Avigad, Lawrence C. Paulson, Johan Commelin)

* An overview of the contributions and achievements so far by my colleagues and me within the ALEXANDRIA Project at Cambridge (led by Professor Lawrence C. Paulson).

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?)

Today

Modern proof assistants (interactive theorem provers)

Software tools for formal verification/ the development of formal proofs by user-computer interaction. A human user writes the proof in a formal language via an interactive interface to be checked by a computer. Intermediate proof steps are often given by automation.

A variety of proof assistants available, based on different logical formalisms:
Based on: set theory (e.g. Mizar, Metamath); simple type theory (e.g. HOL4, HOL Light, Isabelle); dependent type theory (e.g. Coq, Agda,Lean, PVS).
Extensive libraries of formalised mathematics available.

For a direct comparison with examples, see, e.g. the webpage maintained by Wiedijk, “Formalising 100 theorems”.

“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)).

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.

* Deeper understanding, new insights: even familiar material can be seen in 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.

* A way of keeping track of all the details of a complicated proof (see Commelin's talk)

* Educational tools.

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

Why formalise mathematics?

...and a comment on an additional personal motivation

Work in applied proof theory- proof mining: pen-and-paper extraction of constructive/quantitative information from proofs in the form of computable bounds (requiring a logical analysis of a proof and rewriting it to make the logical form of all the statements involved explicit via revealing the hidden quantifiers).

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?
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.

Why formalise mathematics?
A vision for the future of research mathematics:

Timothy Gowers (Fields Medal 1998) describes how a ”dialogue” between a user and a computer would ideally look like in the future to interactively assist the human mathematician to arrive at (new) conclusions. The computer would have access to an extensive database of mathematical material.

W.T. Gowers (2010). Rough Structure and Classification. In: Alon, N., Bourgain, J., Connes, A., Gromov, M., Milman, V. (eds) Visions in Mathematics. Modern Birkhäuser Classics. Birkhäuser Basel. https://doi.org/10.1007/978-3-0346-0422-2_4

More suggested reading

The QED Manifesto*

May 15, 1994

The development of mathematics toward greater precision has led, as is well known, to the formalization of large tracts of it, so that one can prove any theorem using nothing but a few mechanical rules.

– K. Gödel

If civilization continues to advance, in the next two thousand years the overwhelming novelty in human thought will be the dominance of mathematical understanding.

– A. N. Whitehead

1 What Is the QED Project and Why Is It Important?

QED is the very tentative title of a project to build a computer system that effectively represents all of mathematical knowledge for relevant results and, using tools of the QED system, build upon such results with reliability and confidence but without the need for minute comprehension of the details or even the ultimate foundations of the parts of the system upon which they build. Note that the approach will almost surely be

J. Fixed Point Theory Appl. 11 (2012) 43–63
DOI 10.1007/s11784-012-0071-6
Published online March 6, 2012

Journal of Fixed Point Theory and Applications

How to write a 21st century proof

Leslie Lamport

To D. Palais

Abstract. A method of writing proofs is described that makes it harder to prove things that are not true. The method, based on hierarchical structuring, is simple and practical. The author's twenty years of experience writing such proofs is discussed.

Mathematics Subject Classification (2010). 03B35, 03F07.

Keywords. Structured proofs, teaching proofs.

In addition to developing the students' intuition about the beautiful concepts of analysis, it is surely equally important to persuade them that precision and rigor are neither deterrents to intuition, nor ends in themselves, but the natural medium in which to formulate and think about mathematical questions.

Michael Spivak, *Calculus* [7]

More suggested reading

OPINION

The Mechanization of Mathematics

Jeremy Avigad

Communicated by Daniel Velleman

Note: The opinions expressed here are not necessarily those of Notices.

ABSTRACT. In computer science, *formal methods* are used to specify, develop, and verify hardware and software systems. Such methods hold great promise for mathematical discovery and verification of mathematics as well.

searched for a word containing the initial letters of the words "formal," "proof," and "Kepler," and settled on "Flyspeck," which means "to scrutinize, or examine carefully." The project was completed in August of 2014.[1]

In May of 2016, three computer scientists, Marijn Heule, Oliver Kullmann, and Victor Marek, announced a solution to an open problem posed by Ronald Graham. Graham had

FEATURES

Computers and Mathematics

KEVIN BUZZARD

Mathematicians currently use computers to do tedious calculations which would be unfeasible to do by hand. In the future, could they be helping us to prove theorems, or to teach students how to write proofs?

Mathematics from the future

Take a look at the following piece of computer code.

```
lemma continuous_iff_is_closed
 {f : α → β} :
 continuous f ↔ (∀s, is_closed s →
    is_closed (f ⁻¹' s)) :=
⟨assume hf s hs, hf (-s) hs,
 assume hf s, by rw [←is_closed_compl_iff,
    ←is_closed_compl_iff]; exact hf _⟩
```

analysis, topology and so on. Were software like this to be adopted by a broader class of mathematicians we might see a future where these systems start to become useful for a broader class of researchers too.

In this article we will see an overview of why these systems exist and what they are currently capable of. They are getting better, faster, and smarter every year, and I believe that it is only a matter of time until mathematicans will be forced to sit up and take notice. Note however that computers will not be prov

A. Koutsoukou-Argyraki, What can formal systems do for mathematics? A discussion through the lens of proof assistants: some recent advances, Q&A with Jeremy Avigad, Jasmin Blanchette, Frédéric Blanqui, Kevin Buzzard, Johan Commelin, Manuel Eberl, Timothy Gowers, Peter Koepke, Assia Mahboubi, Ursula Martin, Lawrence C. Paulson. Invited contribution. To appear in: Benedikt Löwe and Deniz Sarikaya (eds), *60 Jahre DVMLG* (special issue for the 60 years of the DVMLG), Series: "Tributes", vol. 48 of Tributes, College Publications, London, 2022

More suggested reading

The Origins and Motivations of Univalent Foundations

Professor Voevodsky's Personal Mission to Develop Computer Proof Verification to Avoid Mathematical Mistakes

BY VLADIMIR VOEVODSKY

In January 1984, Alexander Grothendieck submitted to the French National Centre for Scientific Research his proposal "Esquisse d'un Programme." Soon copies of this text started circulating among mathematicians. A few months later, as a first-year undergraduate at Moscow University, I was given a copy of it by George Shabat,

is hardly ever checked in detail.

But this is not the only problem that allows mistakes in mathematical texts to persist. In October 1998, Carlos Simpson submitted to the arXiv preprint server a paper called "Homotopy Types of Strict 3-groupoids." It claimed to provide an argument that implied that the main result of the "∞-groupoids" paper, which Kapranov and I had published in 1989, cannot be true. However, Kapranov and I had consid-

MATHEMATICAL PROOF BETWEEN GENERATIONS

JONAS BAYER [a], CHRISTOPH BENZMÜLLER [b,a], KEVIN BUZZARD [c], MARCO DAVID [d], LESLIE LAMPORT [e], YURI MATIYASEVICH [f], LAWRENCE PAULSON [g], DIERK SCHLEICHER [h], BENEDIKT STOCK [i], AND EFIM ZELMANOV [j]

AFFILIATIONS.
[a] Freie Universität Berlin
[b] Otto-Friedrich-Universität Bamberg
[c] Imperial College London
[d] École Normale Supérieure de Paris
[e] Microsoft Research
[f] Steklov Institute of Mathematics at St. Petersburg
[g] University of Cambridge
[h] Aix-Marseille Université
[i] University of Oxford
[j] University of California, San Diego

ABSTRACT. A *proof* is one of the most important concepts of mathematics. However, there is a striking difference between how a proof is defined in theory and how it is used in practice. This puts the unique status of mathematics as exact science into peril. Now may be the time to reconcile theory and practice, i.e. precision and intuition, through the advent of *computer proof assistants*. For the most time this has been a topic for experts in specialized communities. However, mathematical proofs have become increasingly sophisticated, stretching the boundaries of what is humanly comprehensible,

Some milestones & recent advances

* Formalisation of the proof of the four-colour theorem in Coq by Gonthier (2008).

* Gonthier has also formalised the Feit–Thompson proof of the odd-order theorem in Coq (2012).

* Formalisation of the proof (1998 publ. 2005) by Hales of the Kepler conjecture (sphere packing problem) in HOL Light and Isabelle/HOL by Hales et al. (Flyspeck project, 2003-compl. 2014).

* Formalisation of Gödel's Incompleteness theorems in Isabelle/HOL by Paulson (2013).

Some milestones & recent advances

* Formalisation of an irrationality proof of ζ(3) by Apéry (evaluation of the Riemann zeta function) in Coq by Chyzak, Mahboubi, Sibut-Pinote & Tassi (2014).

* Verification of an algorithm with Isabelle/HOL to verify Tucker's proof that the Lorenz attractor is chaotic in a rigorous mathematical sense by Immler (2015).

* Formalisation of Scholze's perfectoid spaces in Lean by Buzzard, Commelin and Massot (2019).

* Grothendieck's schemes in Lean by Buzzard, Hughes, Lau, Livingston, Fernández Mir, R., Morrison, S. (2020). Independently in Isabelle/HOL by Bordg, Li and Paulson (2021).

Some milestones & recent advances

* Formalisation of a substantial amount of material in analytic number theory in Isabelle/HOL by Manuel Eberl (2019).

* The independence of the Continuum Hypothesis by Han & van Doorn in Lean (2021). Independently in Isabelle/ZF by Gunther, Pagano, Sánchez Terraf & Steinberg (2022).

* Formalisation of the solution to the cap set problem (Ellenberg & Gijswijt, 2017) by Dahmen, Hölzl and Lewis in Lean (2019).

* Szemerédi's Regularity Lemma and Roth's Theorem on Arithmetic Progressions in Isabelle/HOL by Edmonds, Koutsoukou-Argyraki and Paulson. Independently in Lean by Dillies and Mehta (2021).

Some milestones & recent advances

A group of undergraduate students formalised in Isabelle/HOL Matiyasevich's proof of the DPRM theorem (1970):
every recursively enumerable set of natural numbers is Diophantine. This gives a negative solution to Hilbert's 10th problem over the integers.

AFP entry:
-Diophantine Equations and the DPRM Theorem
(Jonas Bayer, Marco David, Benedikt Stock, Abhik Pal, Yuri Matiyasevich and Dierk Schleicher, 2022)

Hilbert Meets Isabelle*

Formalisation of the DPRM Theorem in Isabelle/HOL

Deepak Aryal[1], Jonas Bayer[1], Bogdan Ciurezu[1], Marco David[1], Yiping Deng[1], Prabhat Devkota[1], Simon Dubischar[2], Malte Sophian Hassler[1], Yufei Liu[1], Maria Antonia Oprea[1], Abhik Pal[1], and Benedikt Stock[1]

[1] Jacobs University Bremen gGmbH. Campus Ring 1, 28759 Bremen, Germany.
[2] Kippenberg-Gymnasium. Schwachhauser Heerstraße 62-64, 28209 Bremen, Germany.
[3] St. Petersburg Department of Steklov Mathematical Institute of Russian Academy of Sciences. 27 Fontanka, St. Petersburg, Russia.

Abstract. Hilbert's tenth problem, posed in 1900 by David Hilbert, asks for a general algorithm to determine the solvability of any given Diophantine equation. In 1970, Yuri Matiyasevich proved the DPRM theorem which implies such an algorithm cannot exist. This paper will outline our attempt to formally state the DPRM theorem and verify Matiyasevich's proof using the proof assistant Isabelle/HOL.

Keywords: Hilbert's tenth problem · DPRM Theorem · Isabelle · Diophantine equations · recursively enumerable

1 Background

In October 2017, Yuri Matiyasevich visited Jacobs University in Bremen, Germany. During his short stay, he gave a few talks on Hilbert's tenth problem and his negative proof of the problem. He was interested in a formal verification of the proof. And as a result of his visit, we as a small group of undergraduate students developed into the Hilbert–10 research group at Jacobs University Bremen under the supervision of Yuri Matiyasevich and Prof. Dierk Schleicher.

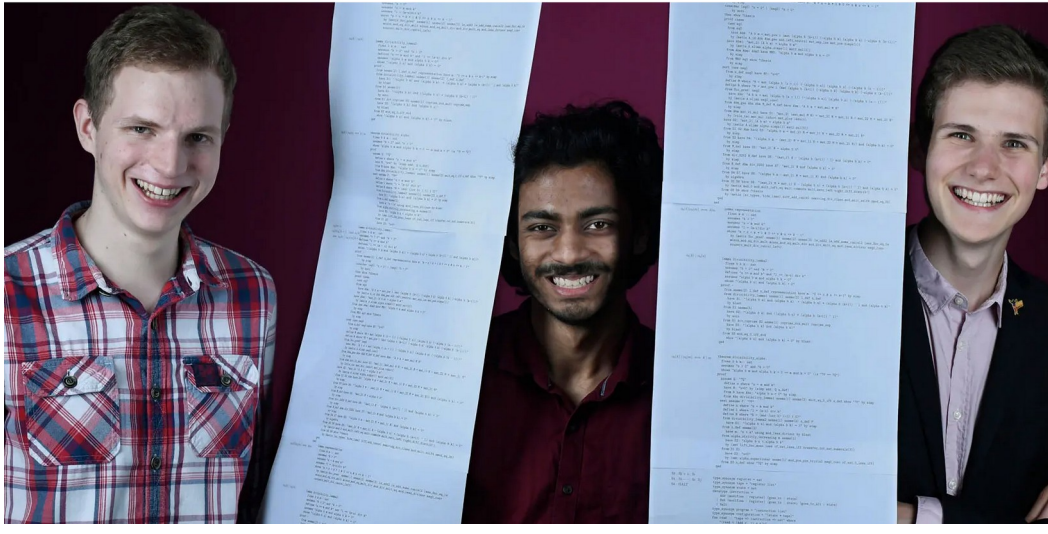
Magazin
20.02.2019
Lesedauer ca. 1 Minute
Drucken
Teilen

MATHEMATISCHE UNTERHALTUNGEN

Hilbert und Isabelle

Eine Gruppe von Jungforschern hat die Lösung für eines der Jahrhundertprobleme des berühmten David Hilbert bestätigt, mit einem Mittel, von dem Hilbert damals nur träumen konnte: einer Software namens Isabelle. Weiteren drei Nachwuchswissenschaftlern gelang es, die für dieses Ergebnis zentralen diophantischen Gleichungen zu optimieren.

von Christoph Pöppe



Some milestones & recent advances

The Liquid Tensor Experiment (see Commelin's talk)

Condensed Mathematics is a theory by Clausen and Scholze (Fields Medal 2018) introducing condensed sets (an alternative notion to topological spaces).

In Dec. 2020, Scholze posed a challenge to the Xena Project Blog: to formalise the proof of a result of his he had doubts about.

The Lean Prover Community took up the challenge: a huge collaborative effort led by Commelin succeeded to complete the proof in the summer of 2022.

Scholze had been reporting on the progress in subsequent Xena blogposts.

Scholze (June 2021,
Xena Project Blog):

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.

NEWS | 18 June 2021

Mathematicians welcome computer-assisted proof in 'grand unification' theory

Proof-assistant software handles an abstract concept at the cutting edge of research, revealing a bigger role for software in mathematics.

Davide Castelvecchi

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. 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).

* Hoskinson Center for Formal Mathematics at Carnegie Mellon University led by Jeremy Avigad inaugurated in 2021.

* Kevin Buzzard and Georges Gonthier were both invited speakers 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.

* 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

Proof assistants and foundations are only one side of the story. Progress seems to require the combination of alternative approaches. An interesting analogy due to Georg Gottlob:

``rule knowledge and logical reasoning VS machine learning e.g. neural networks'' as

``left part of the brain VS right part of the brain''.

Different but complementary functions:
inducing rationality VS inducing imagination and creativity.

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.

NewScientist

AI translates maths problems into code to make them easier to solve

An artificial intelligence that can turn mathematical concepts written in English into a formal proving language for computers could make problems easier for other AIs to solve

MATHEMATICS 6 June 2022

By Alex Wilkins

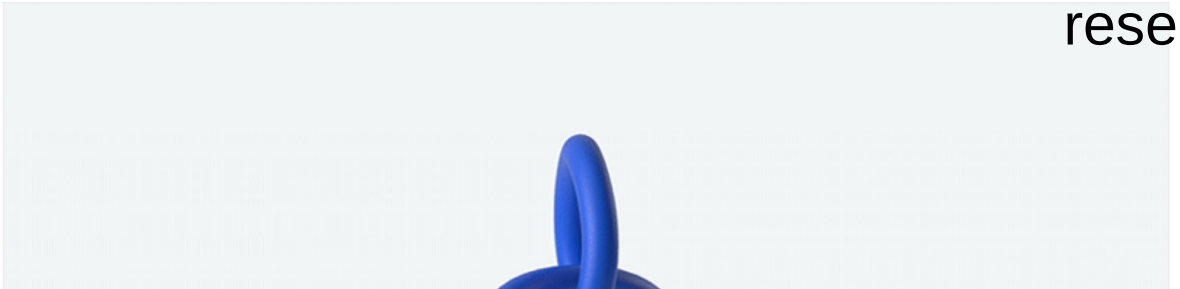
Autoformalization with Large Language Models
Wu, Y., Jiang, A. Q., Li, W., Rabe, M. N., Staats, C., Jamnik, M., Szegedy, C. arXiv:2205.12615v1 To appear in NeurIPS 2022.

NEWS | 01 December 2021

DeepMind's AI helps untangle the mathematics of knots

The machine-learning techniques could benefit other areas of maths that involve large data sets.

Davide Castelvecchi



Davies, A., Juhász, A., Lackenby, M., Tomasev, N., The signature and cusp geometry of hyperbolic knots, arXiv:2111.15323v1

(Not related to proof assistants but demonstrates the pattern-matching efficiency of AI to assist research mathematics.)

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:

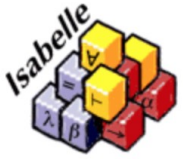
Proof scripts in Isabelle are interactive sessions between user and theorem prover)

- 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).

Isabelle – A Quick Introduction

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



Isabelle

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

TECHNISCHE UNIVERSITÄT MÜNCHEN

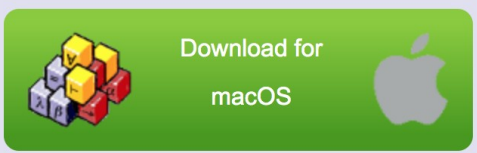
- Home
- Overview
- Installation
- Documentation

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 formulas in a logical calculus. Isabelle was originally developed at the University of Cambridge and Technische Universität München, but now includes numerous contributions from institutions and individuals worldwide. See the Isabelle overview for a brief introduction.

Now available: Isabelle2021-1 (December 2021)



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:

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

Corecursion Examples.

HOL-Computational_Algebra
HOL-Corec_Examples
HOL-Data_Structures

Big (co)datatypes.

HOL-Datatype_Benchmark
HOL-Datatype_Examples

(Co)datatype Examples.

HOL-Decision_Procs

Isabelle – A Quick Introduction

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

Session HOL-Analysis

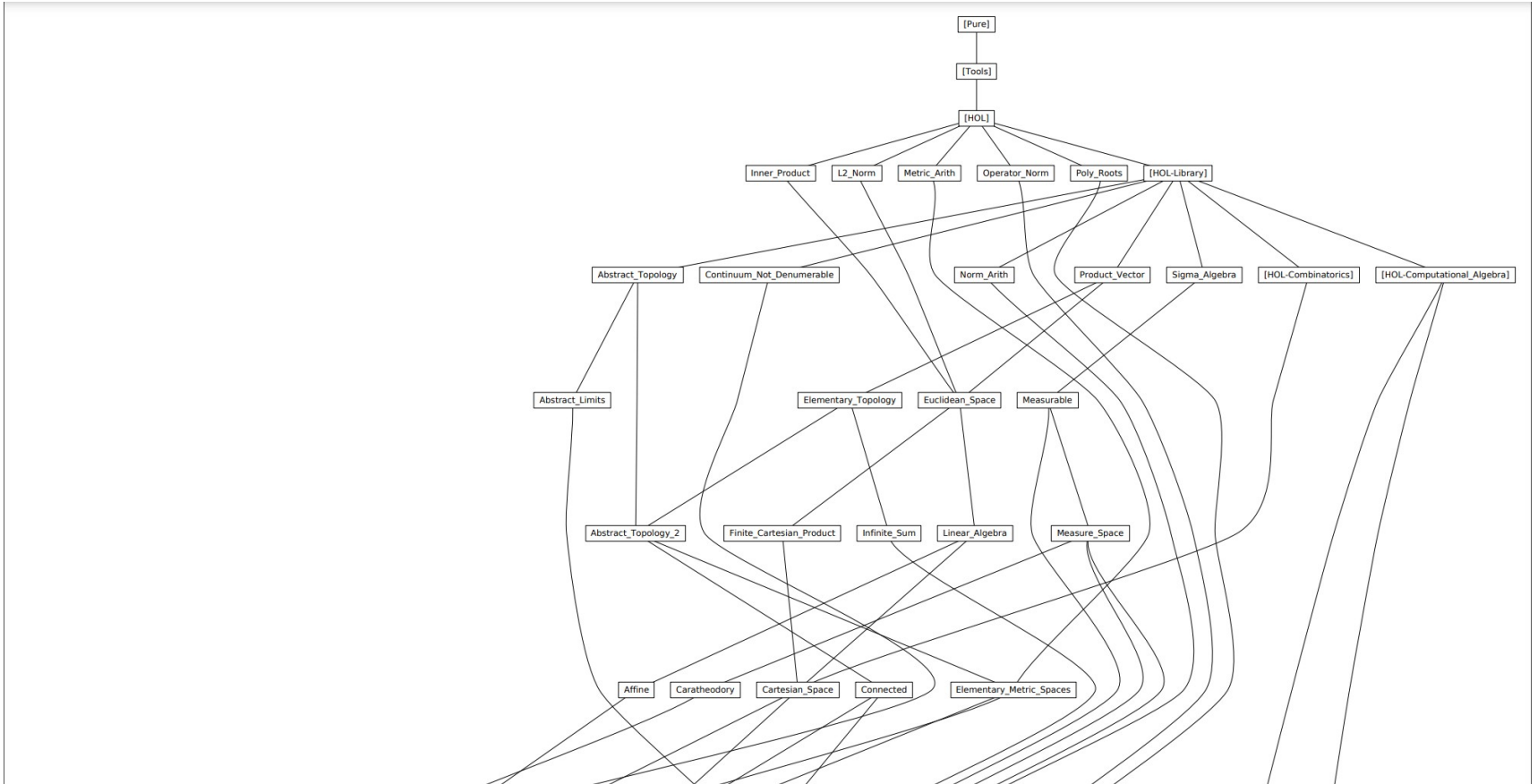
View theory dependencies
View document
View manual

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

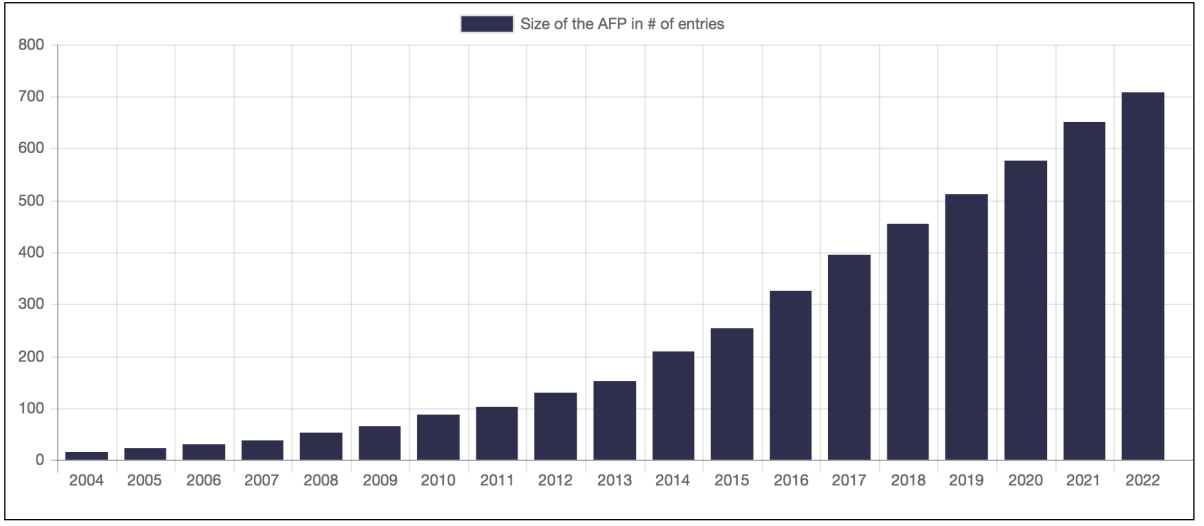
https://www.isa-afp.org/index.html

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

Currently:

Number of Entries: 709
Number of Authors: 428
Number of Lemmas: ~220,100
Lines of Code: ~3,594,500

Growth in number of entries:



The ALEXANDRIA Project at Cambridge

Large Scale Formal Proof for the Working Mathematician

https://www.cl.cam.ac.uk/~lp15/Grants/Alexandria/
(since Autumn 2017)

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.*

European Research Council
Established by the European Commission

Directly funded: PI: Lawrence C. Paulson FRS
Postdocs: Wenda Li, Anthony Bordg, Yiannos Stathopoulos, Angeliki Koutsoukou-Argyraki. Many external collaborators and interns.

Contributions by members of the ALEXANDRIA Project
(I) New formalised material

* 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 (2021).

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

Developed background material on infinite products (Paulson). Roth's theorem on rational approximations assumed as a given.

Contributions by members of the ALEXANDRIA Project
(I) New formalised material

* 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 (2021)). See Paulson's talk at the Topos Institute.

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.

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

Contributions by members of the ALEXANDRIA Project
(I) New formalised material

* Formalising Szemerédi's Regularity Lemma and Roth's Theorem on Arithmetic Progressions in Isabelle/HOL (Chelsea Edmonds, A. K.-A. & Lawrence C. Paulson, arXiv:2207.07499v2, 2022)

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

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

Contributions by members of the ALEXANDRIA Project
(I) New formalised material

* Simple Type Theory is not too Simple: Grothendieck's schemes without dependent types (Anthony Bordg, Lawrence C. Paulson & Wenda Li, Experimental Mathematics, 2021).

Schemes independently formalised in Lean by Buzzard et al. A case study to respond to a “challenge” related to the expressiveness of simple type theory.

See AFP entry:
-Grothendieck's Schemes in Algebraic Geometry (Bordg, Paulson & Li, 2021).

Contributions by members of the ALEXANDRIA Project
(I) New formalised material

* Encoding Dependently-Typed Constructions into Simple Type Theory (Anthony Bordg & Adrián Doña Mateo, 2022, submitted preprint).

In the same spirit of demonstrating the expressiveness of simple type theory, this time the case study involved the formalisation of higher category theory.

Upcoming AFP entry.

Contributions by members of the ALEXANDRIA Project
(I) New formalised material

* Material in additive combinatorics, on the structure of sumsets of finite subsets of abelian groups.
Source: Introduction to Additive Combinatorics, Course notes for Part III of Cambridge Mathematics Tripos by W.T. Gowers (2022).

In particular,

See AFP entries:

- The Plünnecke-Ruzsa Inequality (A. K.-A. & Lawrence C. Paulson, 2022).
- Khovanskii's Theorem (A. K.-A. & Lawrence C. Paulson, 2022).

Contributions by members of the ALEXANDRIA Project
(I) New formalised material

Upcoming AFP entry:

- Kneser’s Theorem and the Cauchy-Davenport Theorem (Mantas Bakšys & A. K.-A.)

Source:
DeVos, M. (2014). A Short Proof of Kneser’s Addition Theorem for Abelian Groups. In: Nathanson, M. (eds) Combinatorial and Additive Number Theory. Springer Proceedings in Mathematics & Statistics, vol 101. Springer, New York, NY. https://doi.org/10.1007/978-1-4939-1601-6_3

Contributions by members of the ALEXANDRIA Project
(I) New formalised material

* A formalisation of the Balog-Szemerédi-Gowers Theorem in Isabelle/HOL (A. K.-A., Mantas Bakšys & Chelsea Edmonds, 2022, submitted preprint).

A profound result in additive combinatorics (2001) which played a central role in Gowers's proof deriving the first effective bounds for Szemerédi's Theorem. Interplay between graph theory, probability theory, additive combinatorics involving algebraic objects, expressed via an implementation of locales, Isabelle's module system.

Made use of a new, general undirected graph theory library by Edmonds.

Source: Introduction to Additive Combinatorics, Course notes for Part III of Cambridge Mathematics Tripos by W.T. Gowers (2022).
Upcoming AFP entries.

Contributions by members of the ALEXANDRIA Project
(I) New formalised material

* Elements of Differential Geometry in Lean (Anthony Bordg & Nicolo Cavalleri, proceedings of FMM 2021, the Fifth Workshop on Formal Mathematics for Mathematicians-part of CICM 2021).

* Certified Quantum Computation in Isabelle/HOL (Anthony Bordg, Hanna Lachnitt & Yijun He, Journal of Automated Reasoning, 65(5), 691-709, 2020).

AFP entry:
-Isabelle Marries Dirac: A Library for Quantum Computation and Quantum Information (Bordg, Lachnitt & He, 2020)

Contributions by members of the ALEXANDRIA Project
(I) New formalised material

* Wetzel: Formalisation of an Undecidable Problem Linked to the Continuum Hypothesis (Lawrence C. Paulson, CICM 2022)

Material combining complex analysis and set theory. A proof by Erdős showing that if the CH fails, every family of analytic functions satisfying the Wetzel property had to be countable; but if the CH holds, there exists (by a transfinite construction) an uncountable family satisfying the Wetzel property.

AFP entry:
-Wetzel's Problem and the Continuum Hypothesis (Paulson, 2022).

Contributions by members of the ALEXANDRIA Project

(I) New formalised material

* Turán's graph theorem formalised by my MPhil student Nils Lauermann (co-supervised with Paulson), 2022.

Contributions by members of the ALEXANDRIA Project
(I) New formalised material

* Even more AFP entries by ALEXANDRIA members:

- Fisher's Inequality: Linear Algebraic Proof Techniques for Combinatorics (Edmonds & Paulson, 2022).

- Constructing the Reals as Dedekind Cuts of Rationals (Fleuriot & Paulson, 2022).

- Ackermann's Function Is Not Primitive Recursive (Paulson, 2022).

- Young's Inequality for Increasing Functions (Paulson, 2022).

- Irrational numbers from THE BOOK (Paulson, 2022).

Contributions by members of the ALEXANDRIA Project
(I) New formalised material

* Even more AFP entries by ALEXANDRIA members (continued:)

- The Theorem of Three Circles (Thomson & Li, 2021).

- Combinatorial Design Theory (Edmonds & Paulson, 2021).

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

- Fourier Series (Paulson, 2019).

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

Contributions by members of the ALEXANDRIA Project
(I) New formalised material

* Even more AFP entries by ALEXANDRIA members (continued:)

- The Prime Number Theorem (Eberl & Paulson, 2018).

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

- Quaternions (Paulson, 2018).

- An Isabelle/HOL formalisation of Green's Theorem (Abdulaziz & Paulson, 2018).

- The Localization of a Commutative Ring (Bordg, 2018).

Contributions by members of the ALEXANDRIA Project
(I) New formalised material

* Even more AFP entries by ALEXANDRIA members (continued:)

- Projective Geometry (Bordg, 2018).

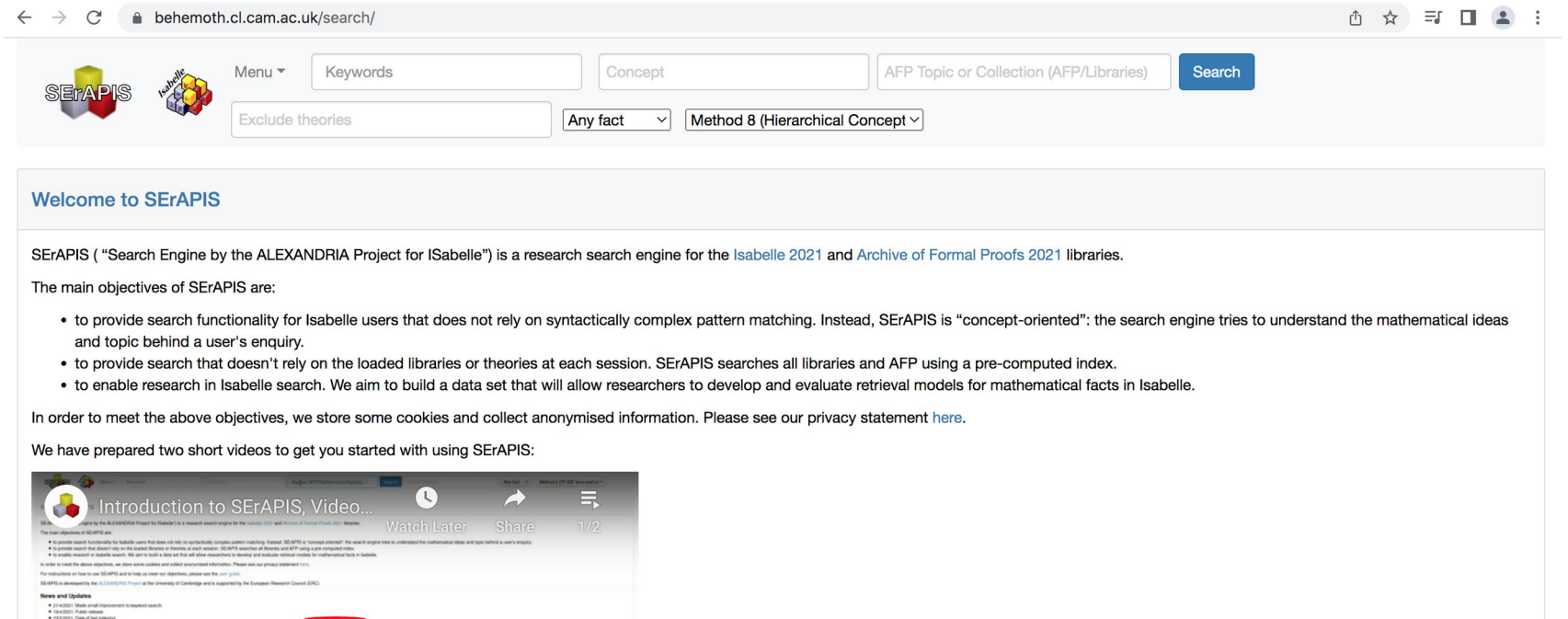
- The Budan-Fourier Theorem and Counting Real Roots with Multiplicity (Li, 2018).

- Evaluate Winding Numbers through Cauchy Indices (Li, 2017).

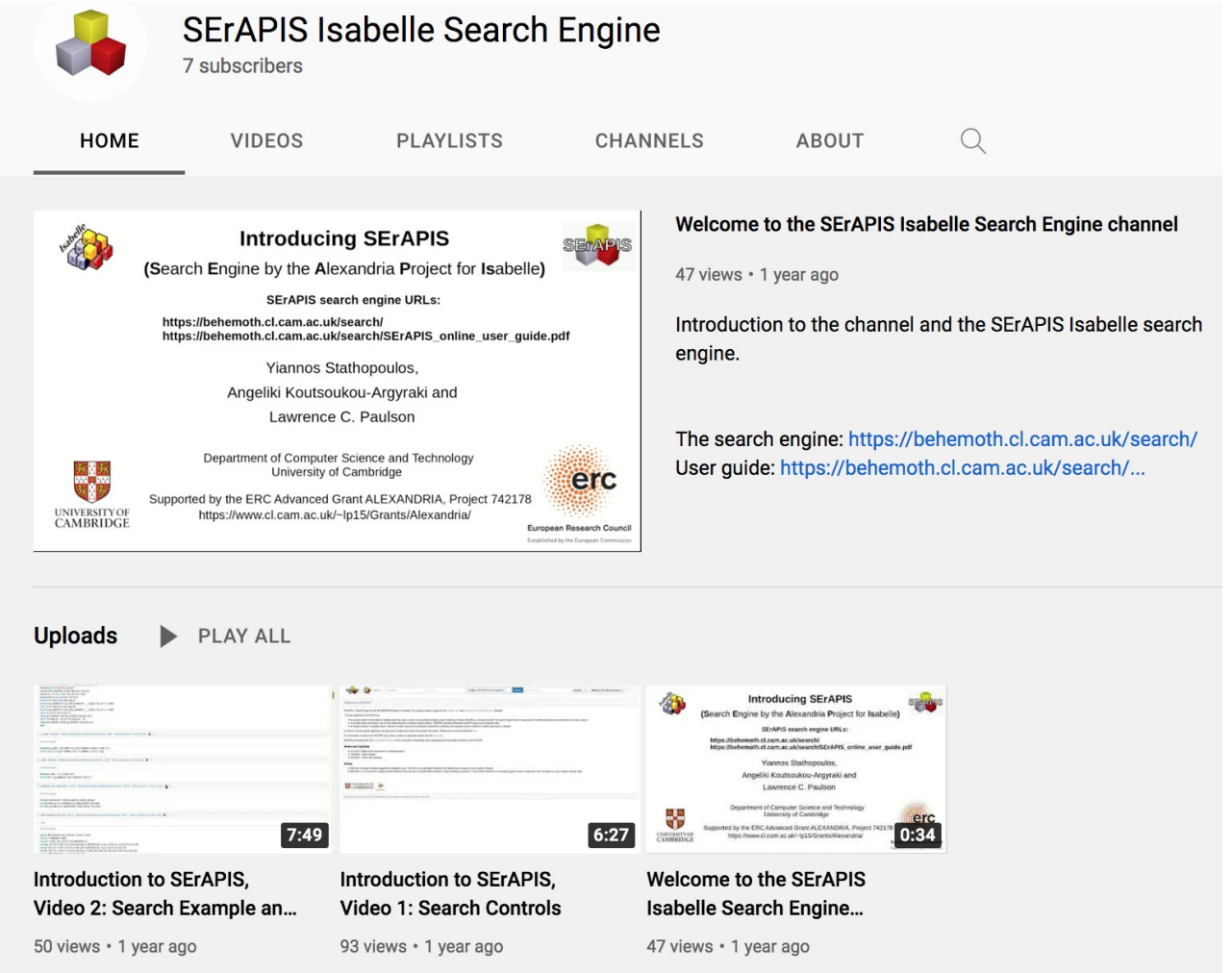
- Count the Number of Complex Roots (Li, 2017).

Contributions by members of the ALEXANDRIA Project
(II) Search: SErAPIS (Search Engine by the Alexandria Project for ISabelle)
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.



Contributions my members of the ALEXANDRIA Project (III) AI/ machine learning tools

* Wenda Li, Lei Yu, Yuhuai Wu & Lawrence C. Paulson: IsarStep: a Benchmark for High-level Mathematical Reasoning, 9th International Conference on Learning Representations (ICLR 2021).

* Yuhuai Wu, Markus Rabe, Wenda Li, Jimmy Ba, Roger Grosse & Christian Szegedy: LIME: Learning Inductive Bias for Primitives of Mathematical Reasoning, Proceedings of the 38th International Conference on Machine Learning (ICML 2021).

* Albert Qiaochu Jiang, Wenda Li, Jesse Michael Han & Yuhuai Wu: LISA: Language models of ISAbelle proofs, 6th Conference on Artificial Intelligence and Theorem Proving (AITP 2021).

Contributions by members of the ALEXANDRIA Project (III) AI/ machine learning tools

* Albert Q. Jiang, Wenda Li, Szymon Tworkowski, Konrad Czechowski, Tomasz Odrzygóźdź, Piotr Miłoś, Yuhuai Wu & Mateja Jamnik: Thor: Wielding Hammers to Integrate Language Models and Automated Theorem Provers.To appear in NeurIPS 2022.

* Yuhuai Wu, Albert Q. Jiang, Wenda Li, Markus N. Rabe, Charles Staats, Mateja Jamnik & Christian Szegedy: Autoformalization with Large Language Models. To appear in NeurIPS 2022.

* Yiannos Stathopoulos, Anthony Bordg & Lawrence Paulson, A Parallel Corpus of Natural Language and Isabelle Artefacts, AITP 2022.

Contributions by members of the ALEXANDRIA Project

(III) AI/ machine learning tools

A research suggestion to use machine learning to extract computational content of formal proofs, based on extensive formal libraries of simple proofs formalised with their computational content made explicit.

* A.K. -A., On preserving the computational content of mathematical proofs: toy examples for a formalising strategy. (Invited contribution). In: De Mol L., Weiermann A., Manea F., Fernández-Duque D. (eds) Connecting with Computability. CiE 2021. Lecture Notes in Computer Science, vol 12813. Springer, Cham (2021).

Thank you