Exemplifying Contemporary Formal Mathematics

Mathematical proofs as done in the sec. XXI

Summer Workshop in Mathematics

Mauricio Ayala-Rincón UnB

Funded by the Brazilian agencies CNPq, grants Universal 409003/21-2; FAPDF, grant DE 00193-00001175/2021-11 and

FAPEG, grant 202310267000223

February 8 2024

Talk's Plan

1. Formalizing Mathematics
2. Fürstenberg's Topological Proof of the Infinity of Primes

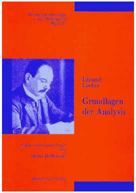
Formalizing Mathematics

Since the early development of computers, implementing mathematical deduction was a very important challenge:

Nicolaas Govert de Bruijn (1918-2012).
Dutch mathematician leader of the
Automath project.

Automath started in 1967:

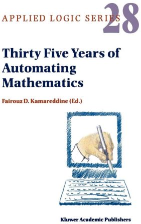
Mechanical verification of the famous
Edmund Landau's (1877-1938) book
Grundlagen der Analysis, Leipzig 1930.



Formalizing Mathematics

https://www.win.tue.nl/automath/

Automath is considered predecessor of modern proof assistants as: Coq, Nurpl, Isabelle, PVS ...



APPLIED LOGIC SERIES 28

Thirty Five Years of Automating Mathematics

Fairouz D. Kamareddine (Ed.)

Kluwer Academic Publishers

STUDIES IN LOGIC
AND
THE FOUNDATIONS OF MATHEMATICS

VOLUME 133

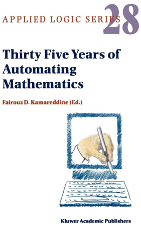
[illegible]
EDITORS

Selected Papers on Automath

Edited by
R.P. NEDERPELT
J.H. GEUVERS
R.C. DE VRIJER

Formalizing Mathematics

In Automath N.G. de Bruijn developed the first formalization of λ-calculus with intuitionistic types and explicit substitutions.



APPLIED LOGIC SERIES 28

Thirty Five Years of Automating Mathematics

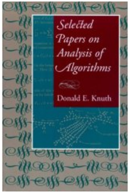
Fairouz D. Kamareddine (Ed.)

Kluwer Academic Publishers

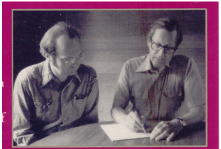
N.G. de Bruijn was a well established mathematician before deciding in 1967 at the age of 49 to work on a new direction related to Automating Mathematics. In the 1960s he became fascinated by the new computer technology and decided to start the new Automath project where he could check, with the help of the computer, the correctness of books of mathematics. Through his work on Automath, de Bruijn started a revolution in using the computer for verification, and since, we have seen more and more proof-checking and theorem-proving systems.

Formalizing Mathematics

N.G. De Bruijn's influence in computing is not restricted to Automath.



Donald Knuth dedicates his book to his mentor, N. G. de Bruijn.



Knuth with his mentor, N. G. de Bruijn, in 1977. Photo courtesy of Jill Knuth

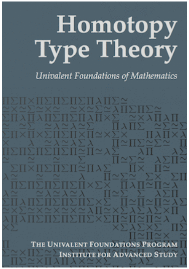
... I'm dedicating this book to N.G. "Dick" de Bruijn because his influence can be felt on every page. Ever since the 1960s he has been my chief mentor, the main person who would answer my questions when I was stuck on a problem that I had not been taught how to solve. I originally wrote Chapter 26 for his $(3 \cdot 4 \cdot 5)$th birthday; now he is 3^4 years young as I gratefully present him with this book.

Donald E. Knuth

Formalizing Mathematics

Vladimir Voevodsky (1966-2017) (2002) popularised the Univalent Foundations that use classical predicate logic as the underlying deductive sytem, categorical approaches, and intuitionistic types, indeed the so called

`https://homotopytypetheory.org`



Homotopy Type Theory

Univalent Foundations of Mathematics

The Univalent Foundations Program
Institute for Advanced Study

Formalizing Mathematics today

Avigad given examples are *"signs that such mechanical tools will allow a fundamental expansion of our capacities for discovering, verifying, and communicating mathematical knowledge."*

Jeremy Avigad **"The Mechanization of Mathematics"**

- Notices of the AMS (2018)

"The history of mathematics is a history of doing whatever it takes to extend our cognitive reach, and designing concepts and methods that augment our capacities to understand. The computer is nothing more than a tool in that respect, but it is one that fundamentally expands the range of structures we can discover and the kinds of truths we can reliably come to know."

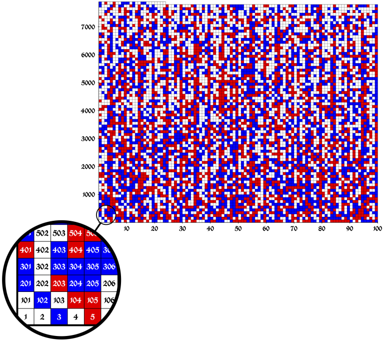
Formalizing Mathematics today

Jonas Bayer, Christoph Benzmüller, Kevin Buzzard, Marco David, Leslie Lamport, Yuri Matiyasevich, Lawrence Paulson, Dierk Schleicher, Benedikt Stock, and Efim Zelmanov **“Mathematical Proof Between Generations”**

- Notices of the AMS (2024)

“... Now may be the time to reconcile theory and practice, i.e., precision and intuition, through the advent of computer proof assistants. This used to be a topic for experts in specialized communities. However, mathematical proofs have become increasingly sophisticated, stretching the boundaries of what is humanly comprehensible, so that leading mathematicians have asked for formal verification of their proofs. At the same time, major theorems in mathematics have recently been computer-verified by people from outside of these communities, even by beginning students.”

Formalizing Mathematics today

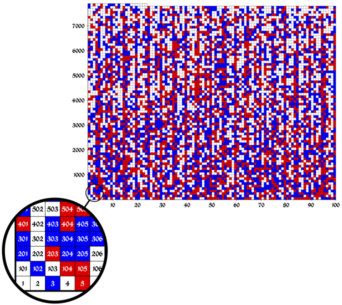


Can all positive naturals be colored red and blue, so that all *Pythagorean Triples* use different colors?

A Pythagorean triple (i, j, k) satisfies $i^2 + j^2 = k^2$, as $(3, 4, 5)$, and $(6, 8, 10)$.

Marijn Heule, Oliver Kullmann and Victor W. Marek (SAT 2016) solved the so called **Boolean Pythagorean triples problem** proving that such a coloring is only possible up to the number 7824.

Formalizing Mathematics today



Essentially, they proved mechanically that $\Phi(n)$ holds for $n \leq 7824$, but not for $\Phi(7825)$, where:

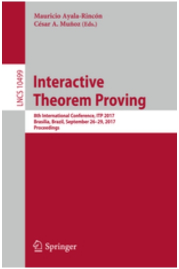
$$\Phi(n) := \bigwedge_{\substack{1 \leq i < j < k \leq n \\ i^2 + j^2 = k^2}} (x_i \vee x_j \vee x_k) \wedge (\bar{x_i} \vee \bar{x_j} \vee \bar{x_k})$$

Boolean solvers may be applied to prove satisfiability of $\Phi(n)$ for $n \leq 7824$, but proving that unsatisfiability of $\Phi(7825)$ required too much effort[†]: checking that all of the 2^{7825} possible bi-partitions of the set $\{1, \ldots, 7825\}$ includes a Pythagorean triple in one of the two sets.

[†] Creating the proof took about 4 CPU years on a cluster with 800 cores in about 2 days. It is the largest proof ever: almost 200 terabytes in size, from which it was extracted a compressed certificate of 68 gigabytes.

Formalizing Mathematics

Some related conferences/journals:



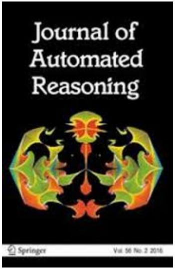
Mauricio Ayala-Rincón
César A. Muñoz (Eds.)

LNCS 10499

Interactive Theorem Proving

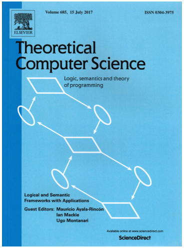
8th International Conference, ITP 2017
Brasília, Brazil, September 26–29, 2017
Proceedings

Springer



Journal of Automated Reasoning

Springer Vol. 56 No. 2 2016



Volume 685, 15 July 2017 ISSN 0304-3975

ELSEVIER

Theoretical Computer Science

Logic, semantics and theory of programming

Logical and Semantic Frameworks with Applications

Guest Editors: Mauricio Ayala-Rincón
Ian Mackie
Ugo Montanari

Available online at www.sciencedirect.com

ScienceDirect

MSCS

Mathematical Structures in Computer Science

A journal in the applications of categorical, algebraic and geometric methods in Computer Science

CAMBRIDGE

Formalized Mathematics by GTC members

- Term Rewriting Theory: TRS NASA PVS Library
- Program Termination: PVS0 and CCG NASA PVS Library
- Nominal Equational Reasoning: Nominal PVS theory
- Group and Ring's Theories: Algebra NASA PVS Library

Formalized Mathematics by GTC members:

Term Rewriting theory - TRS trs.cic.unb.br

- Termination — Ariane Alves Almeida (PhD Informatics 2021)

  (2020) *"Formalizing the Dependency Pair Criterion for Innermost Termination"*

- Confluence — André Luiz Galdino (PhD Mathematics 2008), Ana Cristina Oliveira (PhD Informatics 2016)

  JFR (2008) *"A Formalization of Newman's and Yokouchi's Lemmas in a Higher-Order Language"*

  (2017) *"Confluence of Orthogonal Term Rewriting Systems in the Prototype Verification System"*

- Knuth-Bendix Critical Pairs — André Luiz Galdino (PhD Mathematics 2008)

  (2010) *"A Formalization of the Knuth-Bendix(-Huet) Critical Pair Theorem"*

- Existence of First-order Unification — Andréia Borges Avelar (PhD Math 2014)

  (2014) *"First-order unification in the PVS proof assistant"*

Formalized Mathematics by GTC members: Program Termination Analysis - PVS0 and CCG

- Formalization of the Computational Theory of a functional language - Thiago M. F. Ramos (PhD Informatics 2023), Ariane Alves Almeida (PhD Informatics 2021), Andréia Borges Avelar (PhD Math 2014) Mariano Moscato & César Muñoz, Aaron Dutle, Anthony Narkawicz (NIA / AMA / NASA LaRC FM)

  (2018) *"Formalization of the Undecidability of the Halting Problem for a Functional Language"*

  (2020) *"Formalizing the Dependency Pair Criterion for Innermost Termination"*

  (2022) *"Formalization of the Computational Theory of a Turing Complete Functional Language Model"*

  (2023) *"Formal Verification of Termination Criteria for First-Order Recursive Functions"*.

  Presented in ITP (2021).

Formalized Mathematics by GTC members:

Nominal Equational Reasoning nominal

equality check: $s = t?$ matching: $\exists \sigma : s\sigma = t?$ unification: $\exists \sigma : s\sigma = t\sigma?$

- Formalization of Functional Nominal Equality Check, matching, and Unification modulo C, A, and AC —

  Ana Cristina Oliveira (PhD Informatics 2016), Washington de Carvalho Segundo (PhD Informatics 2019), Gabriel Silva (PhD Informatics 26th January 2024).

(2015) *"Completeness in PVS of a Nominal Unification Algorithm"*

(2017) *"Nominal C-Unification"*

(2019) *"A formalisation of nominal α-equivalence with A, C, and AC function symbols"*

(2019) *"A Certified Functional Nominal C-Unification Algorithm"*

(2021) *"Formalising nominal C-unification generalised with protected variables"*

(2023) *"Nominal AC-matching"* **Best Paper Award** - 16th Int. Conf. on Intelligent Computer Mathematics (CICM), Cambridge, September 5–8, 2023.

Formalized Mathematics by GTC members:

Groups and Rings algebra

- Thaynara A. de Lima (UFG), André Galdino (UFCat), Andréia Avelar (UnB), Mauricio Ayala-Rincón (UnB)

  (2018) *"Formalizing Ring Theory in PVS "*

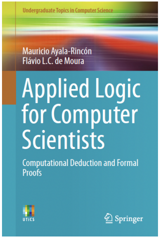
  (2021) *"Formalization of Ring Theory in PVS - Isomorphism Theorems, Principal, Prime and Maximal Ideals,Chinese Remainder Theorem"*

  (LPAR 2023) *"Formalization of Algebraic Theorems in PVS (Invited Talk)"*

  (In progress) *"Formalizing Factorization on Euclidean Domains and Abstract Euclidean Algorithms"*

Formalizing Mathematics at GTC

You are welcome!



Undergraduate Topics in Computer Science

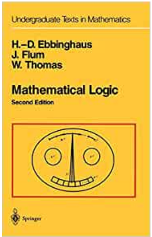
Mauricio Ayala-Rincón
Flávio L.C. de Moura

Applied Logic for Computer Scientists

Computational Deduction and Formal Proofs

UTiCS

Springer



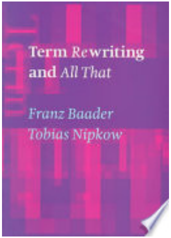
Undergraduate Texts in Mathematics

H.-D. Ebbinghaus
J. Flum
W. Thomas

Mathematical Logic

Second Edition

Springer



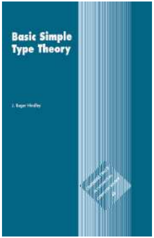
Term Rewriting and *All That*

Franz Baader
Tobias Nipkow

Basic Proof Theory

Second Edition

A. S. Troelstra and
H. Schwichtenberg



Basic Simple Type Theory

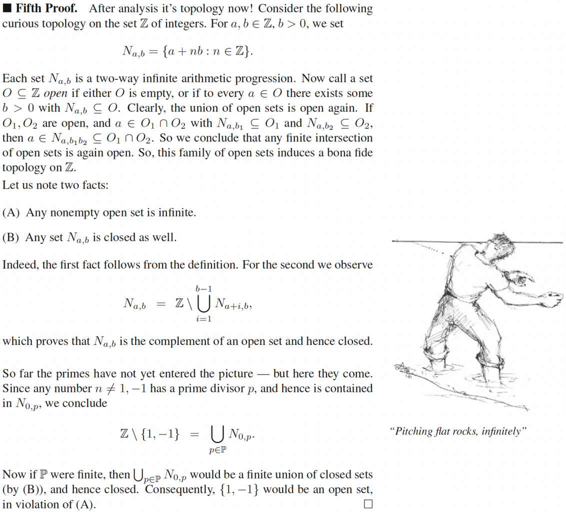
J. Roger Hindley

⇑

Second edition, in progress, will include *“and mathematicians”*

Fürstenberg's Topological Proof of the Infinity of Primes

Hillel Fürstenberg's Topological Proof of the Infinity of Primes [3], [2]



■ **Fifth Proof.** After analysis it's topology now! Consider the following curious topology on the set $\mathbb{Z}$ of integers. For $a, b \in \mathbb{Z}$, $b > 0$, we set

$$N_{a,b} = \{a + nb : n \in \mathbb{Z}\}.$$

Each set $N_{a,b}$ is a two-way infinite arithmetic progression. Now call a set $O \subseteq \mathbb{Z}$ *open* if either O is empty, or if to every $a \in O$ there exists some $b > 0$ with $N_{a,b} \subseteq O$. Clearly, the union of open sets is open again. If O_1, O_2 are open, and $a \in O_1 \cap O_2$ with $N_{a,b_1} \subseteq O_1$ and $N_{a,b_2} \subseteq O_2$, then $a \in N_{a,b_1 b_2} \subseteq O_1 \cap O_2$. So we conclude that any finite intersection of open sets is again open. So, this family of open sets induces a bona fide topology on $\mathbb{Z}$.

Let us note two facts:

(A) Any nonempty open set is infinite.

(B) Any set $N_{a,b}$ is closed as well.

Indeed, the first fact follows from the definition. For the second we observe

$$N_{a,b} \;=\; \mathbb{Z} \setminus \bigcup_{i=1}^{b-1} N_{a+i,b},$$

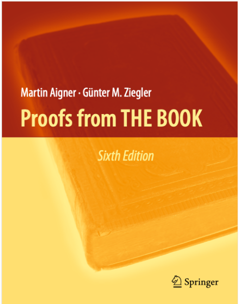
which proves that $N_{a,b}$ is the complement of an open set and hence closed.

So far the primes have not yet entered the picture — but here they come. Since any number $n \neq 1, -1$ has a prime divisor p, and hence is contained in $N_{0,p}$, we conclude

$$\mathbb{Z} \setminus \{1, -1\} \;=\; \bigcup_{p \in \mathbb{P}} N_{0,p}.$$

Now if $\mathbb{P}$ were finite, then $\bigcup_{p \in \mathbb{P}} N_{0,p}$ would be a finite union of closed sets (by (B)), and hence closed. Consequently, $\{1, -1\}$ would be an open set, in violation of (A). □

"Pitching flat rocks, infinitely"



Fürstenberg's topological approach

Topology

A topology over a set X is a collection τ of subsets of X satisfying the following properties:

i) $\emptyset$ and X belong to τ;

ii) The union of **any** sub-collection of τ belongs to τ;

iii) The intersection of a **finite** sub-collection of τ belongs to τ.

- A set X equipped with a topology τ is called a **topological space**.
- A subset of τ, a topological space over X, is called an **open set**.

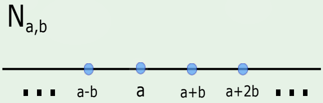
Fürstenberg's topological approach

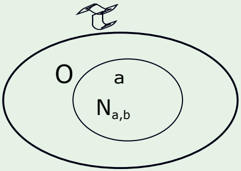
Fürstenberg's topological space

Consider the sets of integers:

$$N_{a,b} = \{a + nb \mid n \in \mathbb{Z}\}, a, b \in \mathbb{Z}, b > 0$$

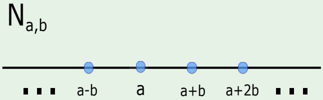
A subset $O \subseteq \mathbb{Z}$ is called **open** if and only if $O = \emptyset$ or for every $a \in O$, there is an integer $b > 0$ such that $N_{a,b} \subseteq O$.

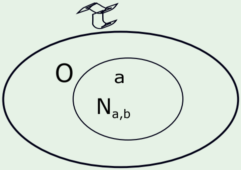




Fürstenberg's topological approach

Fürstenberg's topological space





The collection τ, induced by such open sets is a topology over $\mathbb{Z}$:

i) $\emptyset \in \tau$, and $\mathbb{Z} \in \tau$;

ii) arbitrary unions of subsets of τ belong to τ;

iii) finite intersections of subsets of τ belong to τ.
Proof: if $O_1, O_2 \in \tau$ then $O_1 \cap O_2 \in \tau$:

- In fact, consider $a \in O_1 \cap O_2$ implies there are b_1 and b_2 such that $N_{a,b_1} \subseteq O_1$ and $N_{a,b_2} \subseteq O_2$. Therefore, $N_{a,b_1 \cdot b_2} \subseteq O_1 \cap O_2$.

Fürstenberg's topological approach

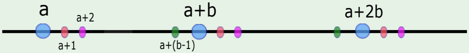
- **Statement 1:** Any nonempty open set is infinite.
    - Proof: if $O \neq \emptyset$ then $N_{a,b} \subset O$, for some $a \in O$ and $b > 0$.
- **Statement 2:** For any $a \in \mathbb{Z}$ and $b > 0$, $N_{a,b}$ is an open set.

Closed sets

In a topological space X **closed** sets are defined as the complement of open sets.

- **Statement 3:** For any $a \in \mathbb{Z}$ and $b > 0$, $N_{a,b}$ is closed.

$$N_{a,b} = \mathbb{Z} \setminus \bigcup_{i=1}^{b-1} N_{a+i,b}$$



and $\bigcup_{i=1}^{b-1} N_{a+i,b}$ is an open set.

Fürstenberg's topological approach

Some properties of closed sets

If X is a topological space then:

P1. $\emptyset$ and X are closed sets;

P2. The finite union of closed sets is a closed set;

- Consider A_i, $1 \leq i \leq n$ closed sets. Thus,

$$X \setminus \bigcup_{i=1}^{n} A_i = \bigcap_{i=1}^{n} (X \setminus A_i) \text{ is an open set}$$

P3. The arbitrary intersection of closed sets is a closed set.

- Consider A_α, a family of closed sets. Thus,

$$X \setminus \bigcap A_\alpha = \bigcup (X \setminus A_\alpha) \text{ is an open set}$$

Fürstenberg's topological approach

- **Statement 4:** Consider k an integer number such that $k \neq 1$ and $k \neq -1$. Therefore, k has a prime divisor p and, consequently, $k \in N_{0,p}$.
  Also,
  $$\mathbb{Z} \setminus \{-1, 1\} = \bigcup_{p \in \mathbb{P}} N_{0,p}, \text{ where } \mathbb{P} \text{ denotes the set of prime numbers.}$$

If $\mathbb{P}$ is finite then:

- $\bigcup_{p \in \mathbb{P}} N_{0,p}$ is a closed set (**Statement 3 + P2**);
- Thus, $\{-1, 1\}$ is an open set (**By the definition of a closed set)**.
- Consequently $\{-1, 1\}$ is an infinite set. (**Statement 1**)

Therefore, the set $\mathbb{P}$ of the prime numbers is infinite.

Referências I

- T.A. de Lima and M. Ayala-Rincón. "Mechanizing Mathematics", Short course at Universidad Nacional de Colombia - Manizalez (2023)
- Aigner, Martin and Ziegler, Günter M. Proofs from THE BOOK. 6th.Springer (2018)
- Hillel Fürstenberg. On the Infinitude of Primes. Amer. Math, Monthly. **62**(5) (1955)