

Mechanizing Mathematics

Mathematical Deduction

Universidad Nacional de Colombia - Sede Manizales
Facultad de Ciencias Exactas y Naturales

Thaynara Arielly de Lima (IME)  **UFG**

Mauricio Ayala-Rincón (CIC-MAT)  **UnB**

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

FAPEG, grant 202310267000223.

May 29 - June 02 , 2023

Talk's Plan

- 1 Formalizing Mathematics
- 2 Gentzen's Calculus

Formalizing Mathematics

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

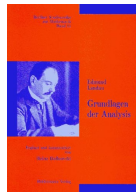
Nicolaas Govert de Bruijn (1918-2012).
Dutch mathematician leader of the
[Automath](#) project.



[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, Nuprl, Isabelle, PVS ...

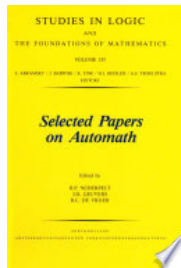
APPLIED LOGIC SERIES **28**

Thirty Five Years of Automating Mathematics

Fairouz D. Kamareddine (Ed.)



Kluwer Academic Publishers



Formalizing Mathematics

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



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.

APPLIED LOGIC SERIES **28**

**Thirty Five Years of
Automating
Mathematics**

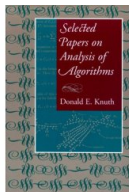
Faiyaz D. Kamareddine (Ed.)



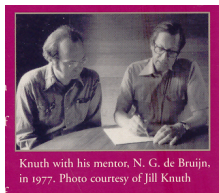
Kluwer Academic Publishers

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.




... 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.

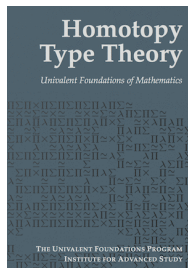
Donald E. Knuth

Formalizing Mathematics



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

<https://homotopytypetheory.org>



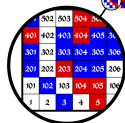
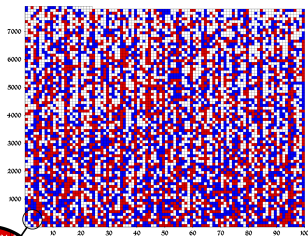
Formalizing Mathematics today

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 ACM 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



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.

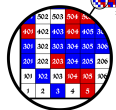
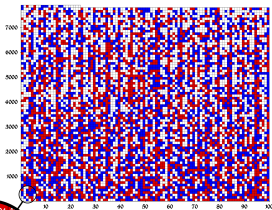
Formalizing Mathematics today

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

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

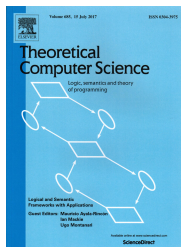
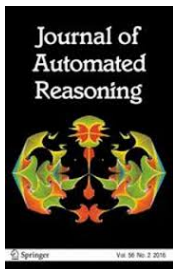
Boolean solvers may be applied to prove satisfiability of $\Phi(n)$ for $n \leq 7824$, but proving that unsatisfiability of $\Phi(7825)$ required too much effort[†]: checking that all of the 2^{7825} possible bi-partitions of the set $\{1, \dots, 7825\}$ includes a Pythagorean triple in one of the two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



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 Ramos (PhD Informatics Student), Ariane Alves Almeida ([PhD Informatics 2021](#)), Andréia Borges Avelar ([PhD Math 2014](#)) Mariano Moscato & César Muñoz, Aaron Dutle, Anthony Narkawicz (NIA / 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"



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

Presented in  ITP (2021) .

Formalized Mathematics by GTC members:

Nominal Equational Reasoning

nominal.cic.unb.br

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 student).



(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"*

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"*

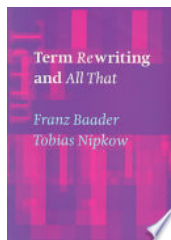
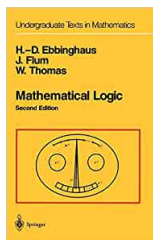
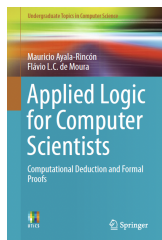


(2021) *"Formalization of Ring Theory in PVS - Isomorphism Theorems, Principal, Prime and Maximal Ideals, Chinese Remainder Theorem"*

(Submitted 2023) *"Formalizing Factorization on Euclidean Domains and Abstract Euclidean Algorithms"*

Formalizing Mathematics at GTC (PPGs in Mathematics & Informatics — UnB)

You are welcome!



Gentzen Calculus

Sequents:

$$\begin{array}{ccc} \Gamma & \Rightarrow & \Delta \\ \uparrow & & \uparrow \\ \text{antecedent} & & \text{succedent} \end{array}$$

Gentzen Calculus

Table: RULES OF DEDUCTION *à la* GENTZEN FOR PREDICATE LOGIC

Left rules	Right rules
Axioms:	
$\Gamma, \varphi \Rightarrow \varphi, \Delta$ (<i>Ax</i>)	$\perp, \Gamma \Rightarrow \Delta$ (L_{\perp})
Structural rules:	
$\frac{\Gamma \Rightarrow \Delta}{\varphi, \Gamma \Rightarrow \Delta}$ (<i>LW</i> eakening)	$\frac{\Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, \varphi}$ (<i>RW</i> eakening)
$\frac{\varphi, \varphi, \Gamma \Rightarrow \Delta}{\varphi, \Gamma \Rightarrow \Delta}$ (<i>LC</i> ontraction)	$\frac{\Gamma \Rightarrow \Delta, \varphi, \varphi}{\Gamma \Rightarrow \Delta, \varphi}$ (<i>RC</i> ontraction)

Gentzen Calculus

Table: RULES OF DEDUCTION *à la* GENTZEN FOR PREDICATE LOGIC

Left rules	Right rules
Logical rules:	
$\frac{\varphi_{i \in \{1,2\}}, \Gamma \Rightarrow \Delta}{\varphi_1 \wedge \varphi_2, \Gamma \Rightarrow \Delta} \quad (L_{\wedge})$	$\frac{\Gamma \Rightarrow \Delta, \varphi \quad \Gamma \Rightarrow \Delta, \psi}{\Gamma \Rightarrow \Delta, \varphi \wedge \psi} \quad (R_{\wedge})$
$\frac{\varphi, \Gamma \Rightarrow \Delta \quad \psi, \Gamma \Rightarrow \Delta}{\varphi \vee \psi, \Gamma \Rightarrow \Delta} \quad (L_{\vee})$	$\frac{\Gamma \Rightarrow \Delta, \varphi_{i \in \{1,2\}}}{\Gamma \Rightarrow \Delta, \varphi_1 \vee \varphi_2} \quad (R_{\vee})$
$\frac{\Gamma \Rightarrow \Delta, \varphi \quad \psi, \Gamma \Rightarrow \Delta}{\varphi \rightarrow \psi, \Gamma \Rightarrow \Delta} \quad (L_{\rightarrow})$	$\frac{\varphi, \Gamma \Rightarrow \Delta, \psi}{\Gamma \Rightarrow \Delta, \varphi \rightarrow \psi} \quad (R_{\rightarrow})$
$\frac{\varphi[x/t], \Gamma \Rightarrow \Delta}{\forall x \varphi, \Gamma \Rightarrow \Delta} \quad (L_{\forall})$	$\frac{\Gamma \Rightarrow \Delta, \varphi[x/y]}{\Gamma \Rightarrow \Delta, \forall x \varphi} \quad (R_{\forall}), \quad y \notin \text{fv}(\Gamma, \Delta)$
$\frac{\varphi[x/y], \Gamma \Rightarrow \Delta}{\exists x \varphi, \Gamma \Rightarrow \Delta} \quad (L_{\exists}), \quad y \notin \text{fv}(\Gamma, \Delta)$	$\frac{\Gamma \Rightarrow \Delta, \varphi[x/t]}{\Gamma \Rightarrow \Delta, \exists x \varphi} \quad (R_{\exists})$

Gentzen Calculus

Derivation of the Peirce's law: $\vdash ((\varphi \rightarrow \psi) \rightarrow \varphi) \rightarrow \varphi$

$$\varphi \Rightarrow \varphi \quad (Ax)$$

Gentzen Calculus

Derivation of the Peirce's law: $\vdash ((\varphi \rightarrow \psi) \rightarrow \varphi) \rightarrow \varphi$

$$(RW) \frac{\varphi \Rightarrow \varphi \quad (Ax)}{\varphi \Rightarrow \varphi, \psi}$$

Gentzen Calculus

Derivation of the Peirce's law: $\vdash ((\varphi \rightarrow \psi) \rightarrow \varphi) \rightarrow \varphi$

$$\begin{array}{c}
 (RW) \frac{\varphi \Rightarrow \varphi \quad (Ax)}{\varphi \Rightarrow \varphi, \psi} \\
 (R_{\rightarrow}) \frac{\varphi \Rightarrow \varphi, \psi}{\Rightarrow \varphi, \varphi \rightarrow \psi}
 \end{array}$$

Gentzen Calculus

Derivation of the Peirce's law: $\vdash ((\varphi \rightarrow \psi) \rightarrow \varphi) \rightarrow \varphi$

$$\begin{array}{c}
 (RW) \frac{\varphi \Rightarrow \varphi (Ax)}{\varphi \Rightarrow \varphi, \psi} \\
 (R_{\rightarrow}) \frac{\varphi \Rightarrow \varphi, \psi}{\Rightarrow \varphi, \varphi \rightarrow \psi} \quad \varphi \Rightarrow \varphi (Ax)
 \end{array}$$

Gentzen Calculus

Derivation of the Peirce's law: $\vdash ((\varphi \rightarrow \psi) \rightarrow \varphi) \rightarrow \varphi$

$$\begin{array}{c}
 (RW) \frac{\varphi \Rightarrow \varphi \quad (Ax)}{\varphi \Rightarrow \varphi, \psi} \\
 (R_{\rightarrow}) \frac{\varphi \Rightarrow \varphi, \psi}{\Rightarrow \varphi, \varphi \rightarrow \psi} \qquad \varphi \Rightarrow \varphi \quad (Ax) \\
 \hline
 (\varphi \rightarrow \psi) \rightarrow \varphi \Rightarrow \varphi \quad (L_{\rightarrow})
 \end{array}$$

Gentzen Calculus

Derivation of the Peirce's law: $\vdash ((\varphi \rightarrow \psi) \rightarrow \varphi) \rightarrow \varphi$

$$\begin{array}{c}
 (RW) \frac{\varphi \Rightarrow \varphi (Ax)}{\varphi \Rightarrow \varphi, \psi} \\
 (R_{\rightarrow}) \frac{\varphi \Rightarrow \varphi, \psi}{\Rightarrow \varphi, \varphi \rightarrow \psi} \quad \varphi \Rightarrow \varphi (Ax) \\
 \hline
 (\varphi \rightarrow \psi) \rightarrow \varphi \Rightarrow \varphi \quad (L_{\rightarrow}) \\
 \hline
 \Rightarrow ((\varphi \rightarrow \psi) \rightarrow \varphi) \rightarrow \varphi \quad (R_{\rightarrow})
 \end{array}$$

Gentzen Calculus

Derivation of: $\vdash \exists x \neg \varphi \Rightarrow \neg \forall x \varphi$

$$\begin{array}{c}
 (L_{\forall}) \frac{\varphi[x/t] \Rightarrow \varphi[x/t]}{\forall x \varphi \Rightarrow \varphi[x/t]} \\
 \frac{\forall x \varphi \Rightarrow \varphi[x/t]}{\neg \varphi[x/t], \forall x \varphi \Rightarrow} \text{ (C-EQUIV)} \\
 \frac{\neg \varphi[x/t], \forall x \varphi \Rightarrow}{\neg \varphi[x/t] \Rightarrow \neg \forall x \varphi} \text{ (C-EQUIV)} \\
 \frac{\neg \varphi[x/t] \Rightarrow \neg \forall x \varphi}{\exists x \neg \varphi \Rightarrow \neg \forall x \varphi} \text{ (L}_{\exists}\text{)}
 \end{array}$$

Gentzen Calculus

Cut rule:

$$\frac{\Gamma \Rightarrow \Delta, \varphi \quad \varphi, \Gamma' \Rightarrow \Delta'}{\Gamma \Gamma' \Rightarrow \Delta \Delta'} \text{ (Cut)}$$

Gentzen Calculus - dealing with negation: c -equivalence

$$\varphi, \Gamma \Rightarrow \Delta \text{ one-step } c\text{-equivalent } \Gamma \Rightarrow \Delta, \neg\varphi$$

$$\Gamma \Rightarrow \Delta, \varphi \text{ one-step } c\text{-equivalent } \neg\varphi, \Gamma \Rightarrow \Delta$$

The c -equivalence is the equivalence closure of this relation.

Lemma 1 (One-step c -equivalence)

- ❶ $\vdash_G \varphi, \Gamma \Rightarrow \Delta$, iff $\vdash_G \Gamma \Rightarrow \Delta, \neg\varphi$;
- ❷ $\vdash_G \neg\varphi, \Gamma \Rightarrow \Delta$, iff $\vdash_G \Gamma \Rightarrow \Delta, \varphi$.

Gentzen Calculus - dealing with negation

Proof.

Ⓜ **Necessity:**

$$\frac{\varphi, \Gamma \Rightarrow \Delta}{\varphi, \Gamma \Rightarrow \Delta, \perp} \text{ (RW)}$$

$$\frac{\varphi, \Gamma \Rightarrow \Delta, \perp}{\Gamma \Rightarrow \Delta, \neg\varphi} \text{ (R}_{\rightarrow}\text{)}$$

Sufficiency:

$$\text{(LW)} \frac{\Gamma \Rightarrow \Delta, \neg\varphi}{\varphi, \Gamma \Rightarrow \Delta, \neg\varphi}$$

$$\frac{(Ax) \varphi, \Gamma \Rightarrow \Delta, \varphi \quad \perp, \varphi, \Gamma \Rightarrow \Delta \text{ (L}_{\perp}\text{)}}{\neg\varphi, \varphi, \Gamma \Rightarrow \Delta} \text{ (L}_{\rightarrow}\text{)}$$

$$\frac{\varphi, \Gamma \Rightarrow \Delta, \neg\varphi \quad \neg\varphi, \varphi, \Gamma \Rightarrow \Delta}{\varphi, \Gamma \Rightarrow \Delta} \text{ (CUT)}$$

Gentzen Calculus - dealing with negation

ⓘ Necessity:

$$\begin{array}{c}
 \text{(R}_{\rightarrow}\text{)} \frac{(Ax) \varphi, \Gamma \Rightarrow \Delta, \varphi, \varphi, \perp}{\Gamma \Rightarrow \Delta, \varphi, \varphi, \neg\varphi} \quad \perp, \Gamma \Rightarrow \Delta, \varphi, \varphi \text{ (L}_{\perp}\text{)} \\
 \text{(L}_{\rightarrow}\text{)} \frac{\Gamma \Rightarrow \Delta, \varphi, \varphi, \neg\varphi}{\neg\neg\varphi, \Gamma \Rightarrow \Delta, \varphi, \varphi} \\
 \text{(R}_{\rightarrow}\text{)} \frac{\neg\neg\varphi, \Gamma \Rightarrow \Delta, \varphi, \varphi}{\Gamma \Rightarrow \Delta, \varphi, \neg\neg\varphi \rightarrow \varphi} \\
 \hline
 \Gamma \Rightarrow \Delta, \varphi
 \end{array}
 \qquad
 \begin{array}{c}
 \frac{\neg\varphi, \Gamma \Rightarrow \Delta}{\neg\varphi, \Gamma \Rightarrow \Delta, \varphi, \perp} \text{ (RW)} \\
 \frac{\neg\varphi, \Gamma \Rightarrow \Delta, \varphi, \perp}{\Gamma \Rightarrow \Delta, \varphi, \neg\neg\varphi} \text{ (R}_{\rightarrow}\text{)} \\
 \frac{\Gamma \Rightarrow \Delta, \varphi, \neg\neg\varphi}{\neg\neg\varphi \rightarrow \varphi, \Gamma \Rightarrow \Delta, \varphi} \text{ (L}_{\rightarrow}\text{)} \\
 \hline
 \neg\neg\varphi \rightarrow \varphi, \Gamma \Rightarrow \Delta, \varphi \text{ (Cut)}
 \end{array}$$

Sufficiency:

$$\frac{\Gamma \Rightarrow \Delta, \varphi \quad \perp, \Gamma \Rightarrow \Delta}{\neg\varphi, \Gamma \Rightarrow \Delta} \text{ (L}_{\rightarrow}\text{)}$$

□