Formalización de matemática, una tarea (in)necesaria pero (in)viable

Miguel Pagano

27 de agosto de 2024

FAMAF - Universidad Nacional de Córdoba (Argentina)

¿Qué es una prueba matemática?

¿Qué es una prueba matemática?

¿Qué es formalizar?

Prueba matemática

Definición (Prueba: definición práctica). Una prueba matemática es una secuencia de argumentos que convence a una lectora educada.

(Dierk Schleicher)

Prueba matemática

Definición (Prueba: definición práctica). Una prueba matemática es una secuencia de argumentos que convence a una lectora educada.

(Dierk Schleicher)

En la concepción estándar, sólo son esbozos de alto nivel cuya intención es indicar la existencia de una derivación formal.

(Jeremy Avigad)

¿Debemos formalizar?

La verdad lógica de un enunciado no nos ilumina sobre su sentido.
Quien hace matemáticas busca la iluminación y no la verdad…

(Gian-Carlo Rota, traducción mía)

¿Debemos formalizar?

La verdad lógica de un enunciado no nos ilumina sobre su sentido. Quien hace matemáticas busca la iluminación y no la verdad…

(Gian-Carlo Rota, traducción mía)

Si los enunciados de la matemática **fueran** *formalmente verdaderos pero no iluminadores, la matemática sería un curioso juego jugado por gente extraña.*

¿Debemos formalizar?

La verdad lógica de un enunciado no nos ilumina sobre su sentido. Quien hace matemáticas busca la iluminación y no la verdad…

(Gian-Carlo Rota, traducción mía)

Si los enunciados de la matemática **fueran** *formalmente verdaderos pero no iluminadores, la matemática sería un curioso juego jugado por gente extraña.*

Lo que mantiene a la matemática viva es la iluminación y es esto lo que le da un rango superior entre las disciplinas científicas.

Pero ...

Interludio formal

Una regla lógica dice que ϕ y $\neg\phi$ son inconsistentes:

$$\frac{\phi \qquad \neg\phi}{\bot}\ (\neg\text{E})$$

Interludio formal

Una regla lógica dice que ϕ y $\neg\phi$ son inconsistentes:

$$\frac{\phi \qquad \neg\phi}{\bot}\,(\neg\mathrm{E})$$

Otra regla nos permite concluir cualquier cosa de una inconsistencia:

$$\frac{\bot}{\psi}\,(\bot\mathrm{E})$$

Interludio formal

Una regla lógica dice que ϕ y $\neg\phi$ son inconsistentes:

$$\frac{\phi \qquad \neg\phi}{\bot}\,(\neg\text{E})$$

Otra regla nos permite concluir cualquier cosa de una inconsistencia:

$$\frac{\bot}{\psi}\,(\bot\text{E})$$

Usaremos eso para probar todas las conjeturas del mundo; tomando resultados publicados (ejemplo tomado de Kevin Buzzard).

Quasi-projectivity of moduli spaces of polarized varieties

Annals of Mathematics, **159** (2004), 597–639

Quasi-projectivity of moduli spaces of polarized varieties

By Georg Schumacher and Hajime Tsuji

Dedicated to our wives Rita and Akiko

Abstract

By means of analytic methods the quasi-projectivity of the moduli space of algebraically polarized varieties with a not necessarily reduced complex structure is proven including the case of nonuniruled polarized varieties.

Non-quasi-projective moduli spaces

Annals of Mathematics, **164** (2006), 1077–1096

Non-quasi-projective moduli spaces

By János Kollár

Abstract

We show that every smooth toric variety (and many other algebraic spaces as well) can be realized as a moduli space for smooth, projective, polarized varieties. Some of these are not quasi-projective. This contradicts a recent paper (Quasi-projectivity of moduli spaces of polarized varieties, *Ann. of Math.* **159** (2004) 597–639.).

Teorema (de Riemann)
La parte real de todo cero no trivial de la función ζ de Riemann es $\frac{1}{2}$.

Demostración.
De Kollár obtenemos un espacio de módulos no-cuasi-proyectivo; además ese espacio es cuasi-proyectivo por un resultado de Schumacher y Tsuji.

De la contradicción anterior concluimos el teorema de Riemann. □

¡Es necesario!

Dos medallas Fields sobre su propio trabajo:

1. The groundbreaking 1986 paper “Algebraic Cycles and Higher K-theory” by Spencer Bloch was soon after publication found by Andrej Suslin to contain a mistake in the proof of Lemma 1.1. (Vladimir Voevodsky)
2. En 1999/2000 Voevodsky descubre un error en un lema en un paper de él mismo.

¡Es necesario!

Dos medallas Fields sobre su propio trabajo:

1. The groundbreaking 1986 paper “Algebraic Cycles and Higher K-theory” by Spencer Bloch was soon after publication found by Andrej Suslin to contain a mistake in the proof of Lemma 1.1. (Vladimir Voevodsky)
2. En 1999/2000 Voevodsky descubre un error en un lema en un paper de él mismo.
3. “I once had a full proof of the weight-monodromy conjecture that passed the judgment of some top mathematicians, but then it turned out to contain a fatal mistake.” (Peter Scholze)

¡Es necesario! (2)

Otros dos ejemplos:

1. Baker proved in 1970 that a transcendental entire function cannot have two disjoint completely invariant domains.

¡Es necesario! (2)

Otros dos ejemplos:

1. Baker proved in 1970 that a transcendental entire function cannot have two disjoint completely invariant domains. In 2016 Julien Duval observed that there is a flaw in Baker's proof.

(Rempe-Gillen y Sixsmith)

¡Es necesario! (2)

Otros dos ejemplos:

1. Baker proved in 1970 that a transcendental entire function cannot have two disjoint completely invariant domains. In 2016 Julien Duval observed that there is a flaw in Baker's proof.

   (Rempe-Gillen y Sixsmith)

2. Patriksson (2004) analyzes the sensitivity of solutions of traffic equilibrium problems. One of his central results deals with directional differentiability in the elastic-demand case. Unfortunately, his proof contains crucial errors.

   (Stephen Robinson)

¿Qué es una prueba matemática?

¿Qué criterios tenemos para saber si una secuencia de argumentos es válida?

¿Qué es una prueba matemática?

¿Qué criterios tenemos para saber si una secuencia de argumentos es válida?

> *Definición (Prueba: definición formal). Una prueba matemática es una secuencia de argumentos que deduce formalmente consecuencias a partir de un conjunto de axiomas siguiendo reglas formales de deducción.*
>
> *(D. Schleicher)*

¿Qué es(era) formalizar matemática? (2)

Quien quiera satisfacerse con la corrección perfecta de una prueba dificilmente recurra a alguno de las formalizaciones completas disponibles al día de hoy (ni siquiera a las formalizaciones parciales e incompletas provistas por los cálculos algebraicos u otros cálculos).

¿Qué es(era) formalizar matemática? (2)

Quien quiera satisfacerse con la corrección perfecta de una prueba dificilmente recurra a alguno de las formalizaciones completas disponibles al día de hoy (ni siquiera a las formalizaciones parciales e incompletas provistas por los cálculos algebraicos u otros cálculos).

En general se contenta con llevar la exposición al punto donde su experiencia y conocimiento matemático le digan que la traducción a un ***lenguaje formal*** no será más que un ejercicio de paciencia, ***sin duda, un ejercicio muy tedioso***.

¿Qué es(era) formalizar matemática? (2)

Quien quiera satisfacerse con la corrección perfecta de una prueba dificilmente recurra a alguno de las formalizaciones completas disponibles al día de hoy (ni siquiera a las formalizaciones parciales e incompletas provistas por los cálculos algebraicos u otros cálculos).

En general se contenta con llevar la exposición al punto donde su experiencia y conocimiento matemático le digan que la traducción a un ***lenguaje formal*** no será más que un ejercicio de paciencia, ***sin duda, un ejercicio muy tedioso***.

La corrección de un texto matemático se verifica comparándolo, más o menos explícitamente, con las reglas de un lenguaje formal.

(Bourbaki)

¿Es posible formalizar?

No se necesita mucha experiencia para darse cuenta que tal proyecto es absolutamente irrealizable: la más pequeña prueba de los inicios de la teoría de conjuntos requeriría cientos de símbolos para su completa formalización.

¿Es posible formalizar?

> *No se necesita mucha experiencia para darse cuenta que tal proyecto es absolutamente irrealizable: la más pequeña prueba de los inicios de la teoría de conjuntos requeriría cientos de símbolos para su completa formalización.*

Lo que no dice Bourbaki es que ***verificar*** una prueba absolutamente formal es tedioso y propenso a errores… justamente porque es algo **mayormente *mecánico***.

¿Es posible formalizar?

> *No se necesita mucha experiencia para darse cuenta que tal proyecto es absolutamente irrealizable: la más pequeña prueba de los inicios de la teoría de conjuntos requeriría cientos de símbolos para su completa formalización.*

Lo que no dice Bourbaki es que ***verificar*** una prueba absolutamente formal es tedioso y propenso a errores… justamente porque es algo **mayormente *mecánico***.

La idea de verificar mecánicamente la corrección de argumentos fue sugerida inicialmente por Leibniz en el siglo XVII.

¿Es posible formalizar?

> *No se necesita mucha experiencia para darse cuenta que tal proyecto es absolutamente irrealizable: la más pequeña prueba de los inicios de la teoría de conjuntos requeriría cientos de símbolos para su completa formalización.*

Lo que no dice Bourbaki es que ***verificar*** una prueba absolutamente formal es tedioso y propenso a errores… justamente porque es algo **mayormente *mecánico***.

La idea de verificar mecánicamente la corrección de argumentos fue sugerida inicialmente por Leibniz en el siglo XVII.

Ahora tenemos programas que verifican la corrección y también programas que ***asisten*** en la construcción de pruebas matemáticas.

Computación mainstream

1. CompCert: compilador de C

Computación mainstream

1. CompCert: compilador de C
2. CakeML: a certified implementation of ML

Computación mainstream

1. CompCert: compilador de C
2. CakeML: a certified implementation of ML
3. seL4: Microkernel verificado en Isabelle/HOL

Computación mainstream

1. CompCert: compilador de C
2. CakeML: a certified implementation of ML
3. seL4: Microkernel verificado en Isabelle/HOL
4. Jasmin: Criptografía segura

Matemática mainstream

1. Liquid Tensor Experiment

Matemática mainstream

1. Liquid Tensor Experiment
2. On a Density Conjecture about Unit Fractions

Matemática mainstream

1. Liquid Tensor Experiment
2. On a Density Conjecture about Unit Fractions
3. Gardam's disproof of Kaplansky's Unit Conjecture

Matemática mainstream

1. Liquid Tensor Experiment
2. On a Density Conjecture about Unit Fractions
3. Gardam's disproof of Kaplansky's Unit Conjecture
4. The Balog–Szemerédi–Gowers Theorem

Matemática mainstream

1. Liquid Tensor Experiment
2. On a Density Conjecture about Unit Fractions
3. Gardam's disproof of Kaplansky's Unit Conjecture
4. The Balog–Szemerédi–Gowers Theorem
5. Perfectoid Spaces

¿Por qué formalizar?

- Obtener certeza sobre la validez de una prueba matemática.

¿Por qué formalizar?

- Obtener certeza sobre la validez de una prueba matemática.
- Comprender los detalles de una prueba.

¿Por qué formalizar?

- Obtener certeza sobre la validez de una prueba matemática.
- Comprender los detalles de una prueba.
- Comprender el enunciado de un teorema y las definiciones de las estructuras involucradas.

¿Por qué formalizar?

- Obtener certeza sobre la validez de una prueba matemática.
- Comprender los detalles de una prueba.
- Comprender el enunciado de un teorema y las definiciones de las estructuras involucradas.
- Aprender una teoría.

¿Por qué formalizar?

- Obtener certeza sobre la validez de una prueba matemática.
- Comprender los detalles de una prueba.
- Comprender el enunciado de un teorema y las definiciones de las estructuras involucradas.
- Aprender una teoría.

Advertencia: ¡puede ser adictivo!

Otros ejemplos

- Conjetura de Kepler: Thomas Hales lo necesitaba porque si bien se publicó no hubo una determinación absoluta sobre la corrección de la prueba.

Otros ejemplos

- Conjetura de Kepler: Thomas Hales lo necesitaba porque si bien se publicó no hubo una determinación absoluta sobre la corrección de la prueba.
- Teorema de los cuatro colores: la prueba de Appel y Haken usaba programas; la prueba de Gonthier y su equipo en Coq incluye la corrección de esos programas.

Otros ejemplos

- Conjetura de Kepler: Thomas Hales lo necesitaba porque si bien se publicó no hubo una determinación absoluta sobre la corrección de la prueba.
- Teorema de los cuatro colores: la prueba de Appel y Haken usaba programas; la prueba de Gonthier y su equipo en Coq incluye la corrección de esos programas.
- Feit-Thompson: prueba descomunalmente larga.

Otros ejemplos

- Conjetura de Kepler: Thomas Hales lo necesitaba porque si bien se publicó no hubo una determinación absoluta sobre la corrección de la prueba.
- Teorema de los cuatro colores: la prueba de Appel y Haken usaba programas; la prueba de Gonthier y su equipo en Coq incluye la corrección de esos programas.
- Feit-Thompson: prueba descomunalmente larga.
- Lean: toda la currícula matemática de una carrera de grado.

¿Qué tanto tiempo lleva aprender?

En un curso de cuatro meses se puede aprender lo suficiente para:

- Teorema de Kőnig para grafos bipartitos (Mateo Carranza Vélez, Lean).

¿Qué tanto tiempo lleva aprender?

En un curso de cuatro meses se puede aprender lo suficiente para:

- Teorema de Kőnig para grafos bipartitos (Mateo Carranza Vélez, Lean).
- Coloreo de grafos cíclicos y grafos camino (Iván Renison, Lean).

¿Qué tanto tiempo lleva aprender?

En un curso de cuatro meses se puede aprender lo suficiente para:

- Teorema de Kőnig para grafos bipartitos (Mateo Carranza Vélez, Lean).
- Coloreo de grafos cíclicos y grafos camino (Iván Renison, Lean).
- Open-mapping theorem (Álfredo Álzaga, Isabelle/HOL).

¿Qué tanto tiempo lleva aprender?

En un curso de cuatro meses se puede aprender lo suficiente para:

- Teorema de Kőnig para grafos bipartitos (Mateo Carranza Vélez, Lean).
- Coloreo de grafos cíclicos y grafos camino (Iván Renison, Lean).
- Open-mapping theorem (Álfredo Álzaga, Isabelle/HOL).
- Descomposicíon de BL-cadenas (Sebastián Buss, Isabelle/HOL).

¿Qué tanto tiempo lleva aprender?

En un curso de cuatro meses se puede aprender lo suficiente para:

- Teorema de Kőnig para grafos bipartitos (Mateo Carranza Vélez, Lean).
- Coloreo de grafos cíclicos y grafos camino (Iván Renison, Lean).
- Open-mapping theorem (Álfredo Álzaga, Isabelle/HOL).
- Descomposicíon de BL-cadenas (Sebastián Buss, Isabelle/HOL).
- Algoritmos para punto flotante (Christian Moreno, Agda).

¿Qué tanto tiempo lleva aprender?

En un curso de cuatro meses se puede aprender lo suficiente para:

- Teorema de Kőnig para grafos bipartitos (Mateo Carranza Vélez, Lean).
- Coloreo de grafos cíclicos y grafos camino (Iván Renison, Lean).
- Open-mapping theorem (Álfredo Álzaga, Isabelle/HOL).
- Descomposicíon de BL-cadenas (Sebastián Buss, Isabelle/HOL).
- Algoritmos para punto flotante (Christian Moreno, Agda).
- Morfismos de algebras implicativas (Mati Steinberg, Coq)

¡Muchas gracias!

Bibliografía

1. Vladimir Voevodsky. ***Univalent Foundations***. Presentación en el Institute of Advanced Studies. 2014. online
2. Jeremy Avigad. ***Reliability of mathematical inference***. Synthese. 2019.
3. Dierk Schleicher. ***What is a mathematical proof?*** en ***Mathematical Proofs between Generations***. 2022. arxiv
4. Peter Scholze. ***Liquid tensor experiment***. 2020. online
5. Kevin Buzzard. ***The future of mathematics?*** 2020. slides
6. Gian-Carlo Rota. ***Indiscrete Thoughts***. 2008
7. Nicolas Bourbaki. ***Elements of Mathematics, Theory of Sets***. 2004.

Bibliografía

1. D. S. Lasse Rempe-Gillen. ***On connected preimages of simply-connected domains under entire functions***. 2018. arxiv
2. Stephen M. Robinson. ***Strong Regularity and the Sensitivity Analysis of Traffic Equilibria: A Comment***. Transportation Science. 2006.

¿Cómo luce?

Ejemplos locales (computación):

1. Corrección de compiladores para distintos lenguajes pequeños (en Coq y Agda).
   Trabajo conjunto con mucha gente (Leo Rodríguez, Daniel Fridlender, Alberto Pardo, Marco Viera).

¿Cómo luce?

Ejemplos locales (computación):

1. Corrección de compiladores para distintos lenguajes pequeños (en Coq y Agda).
   Trabajo conjunto con mucha gente (Leo Rodríguez, Daniel Fridlender, Alberto Pardo, Marco Viera).
2. Coherencia de semántica intrínseca (en Coq).
   Trabajo conjunto con Ale Gadea.

¿Cómo luce?

Ejemplos locales (computación):

1. Corrección de compiladores para distintos lenguajes pequeños (en Coq y Agda).
   Trabajo conjunto con mucha gente (Leo Rodríguez, Daniel Fridlender, Alberto Pardo, Marco Viera).
2. Coherencia de semántica intrínseca (en Coq).
   Trabajo conjunto con Ale Gadea.
3. Arquitectura LEGv8 (en Agda).
   Trabajo conjunto con Santi Arranz Olmos, Mati Steinberg, Ale Gadea, Manu Gunther, Martín Fernández.

¿Cómo luce?

Ejemplos locales (matemática):

1. Álgebra universal heterogénea (en Agda).
   Trabajo conjunto con Manu Gunther (y Ale Gadea).

¿Cómo luce?

Ejemplos locales (matemática):

1. Álgebra universal heterogénea (en Agda).
   Trabajo conjunto con Manu Gunther (y Ale Gadea).
2. Independencia de CH respecto de axiomas de ZF (en Isabelle/ZF).
   Trabajo conjunto con Manu Gunther, Mati Steinberg y Pedro Sánchez Terraf.