Controlled/Certifiable Natural Mathematics (CNM)

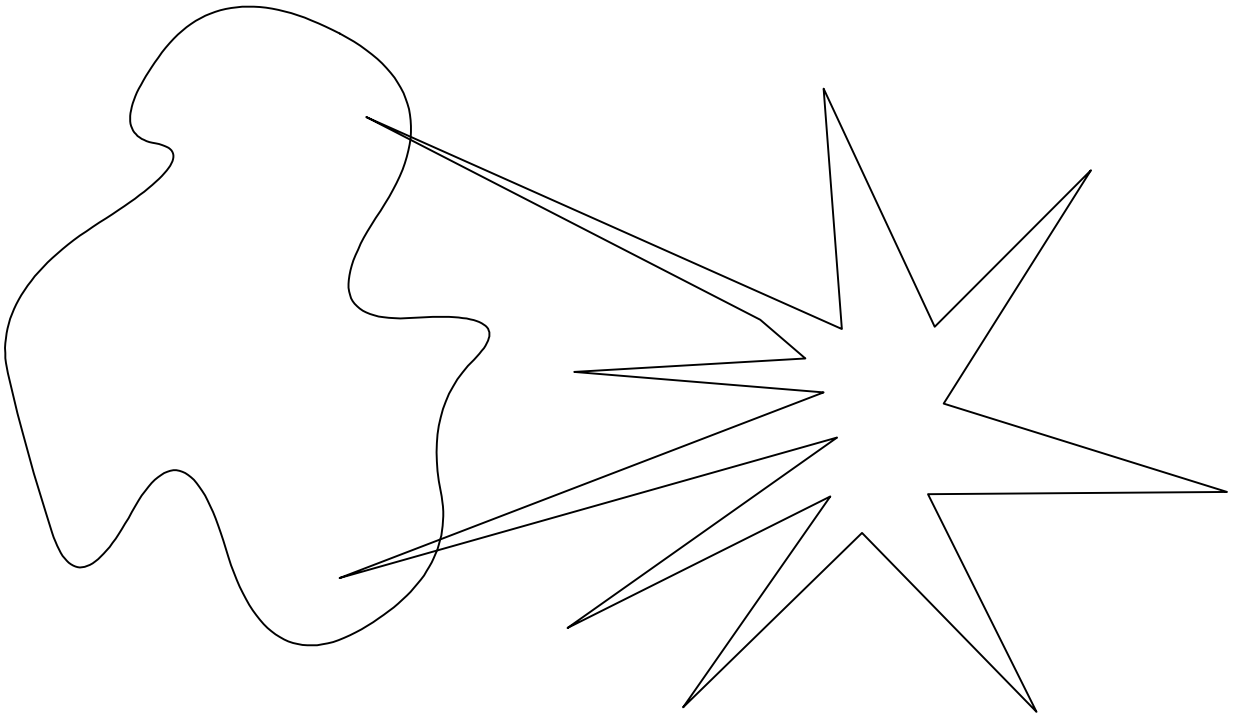
by Peter Koepke

University of Bonn, Germany, https://www.math.uni-bonn.de/ag/logik/

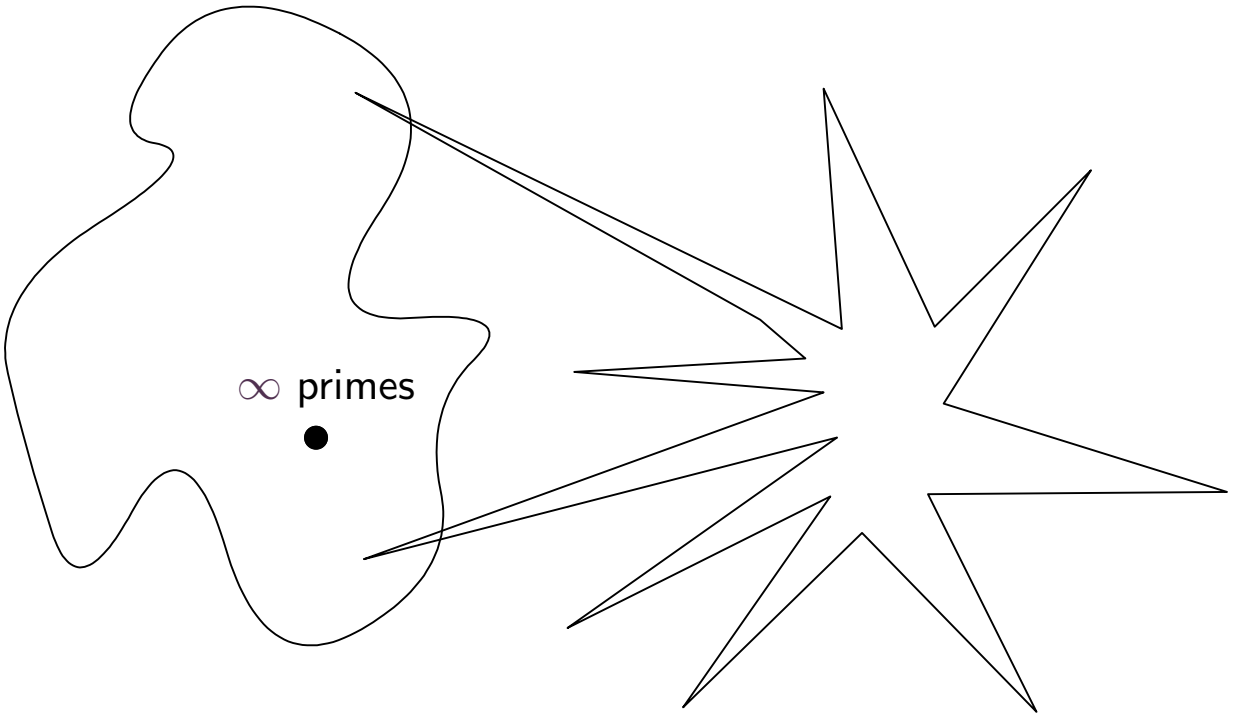
Text-Driven Approaches to the Philosophy of Mathematics (TDPhiMa 2)
Online, 1–3 September 2021

Can one restrict/regulate/control natural mathematics to a fully formal subset which still covers wide parts of pure mathematics?

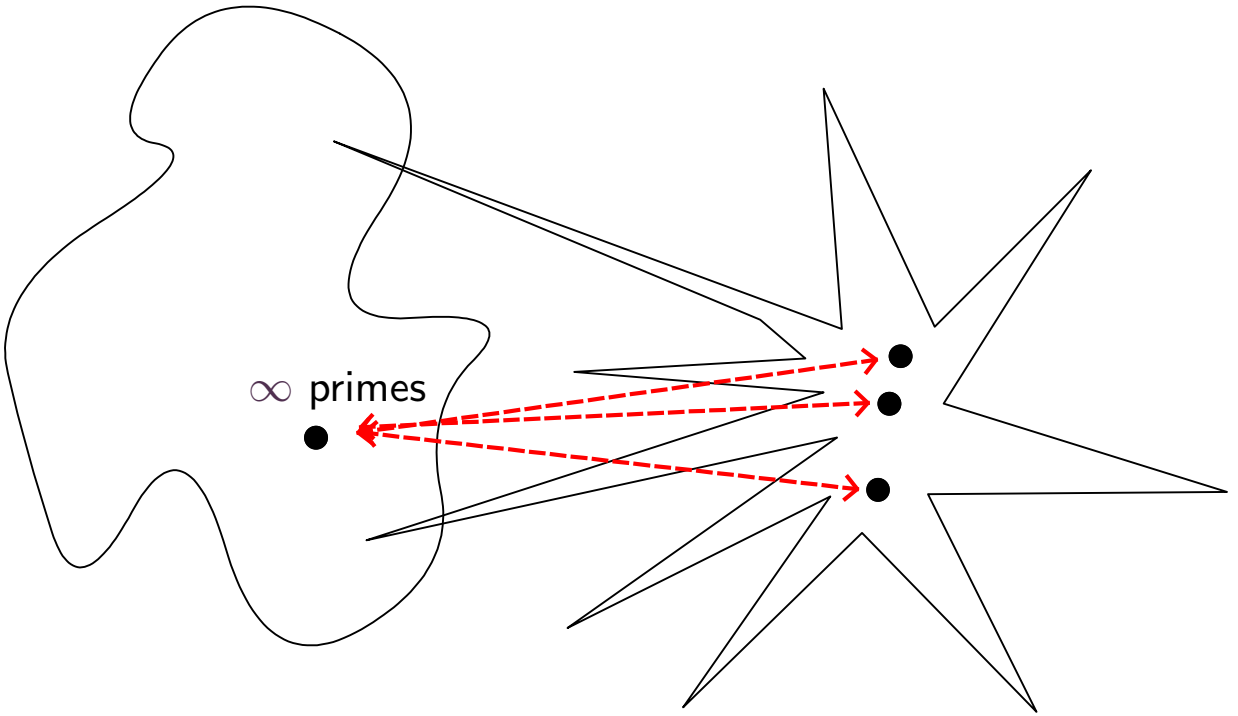
Natural mathematics and formal mathematics



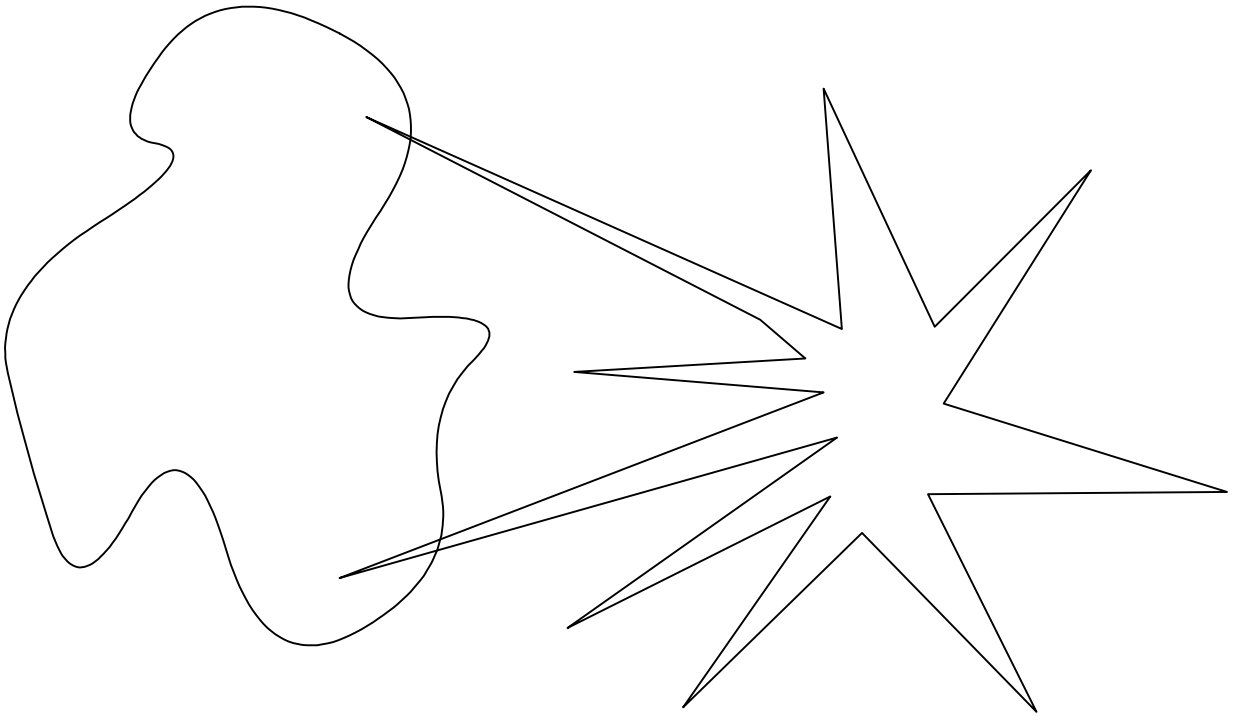
Natural mathematics and formal mathematics



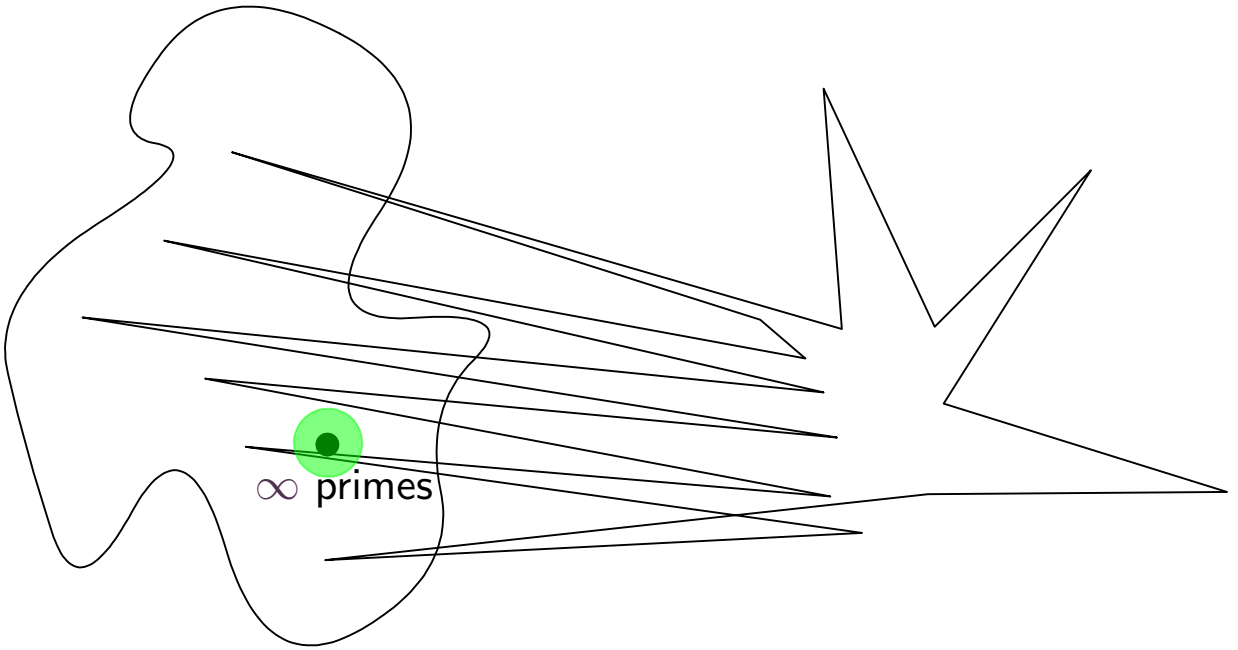
Natural mathematics and formal mathematics



Natural mathematics and formal mathematics



Natural mathematics and formal mathematics



Overview

- Formalizing intuitive mathematical statements

Overview

- Formalizing intuitive mathematical statements
- Controlled natural languages for mathematics

Overview

- Formalizing intuitive mathematical statements
- Controlled natural languages for mathematics
- $\mathbb{N}$aproche and the language ForTheL

Overview

- Formalizing intuitive mathematical statements
- Controlled natural languages for mathematics
- $\mathbb{N}$aproche and the language ForTheL
- Controlled/certifiable natural mathematics (CNM)

Overview

- Formalizing intuitive mathematical statements
- Controlled natural languages for mathematics
- $\mathbb{N}$aproche and the language ForTheL
- Controlled/certifiable natural mathematics (CNM)
- $\mathbb{N}$aproche and CNM

Overview

- Formalizing intuitive mathematical statements
- Controlled natural languages for mathematics
- $\mathbb{N}$aproche and the language ForTheL
- Controlled/certifiable natural mathematics (CNM)
- $\mathbb{N}$aproche and CNM
- Towards current mathematical research

The infinitude of primes

- Euclid IX, 20: “Prime numbers are more than any assigned multitude of prime numbers” (4.430 Google hits)

The infinitude of primes

- Euclid IX, 20: “Prime numbers are more than any assigned multitude of prime numbers” (4.430 Google hits)
- ”There are infinitely many prime numbers” (31.800)

The infinitude of primes

- Euclid IX, 20: “Prime numbers are more than any assigned multitude of prime numbers” (4.430 Google hits)
- ”There are infinitely many prime numbers” (31.800)
- ”There are infinitely many primes” (65.300)

The infinitude of primes

- Euclid IX, 20: “Prime numbers are more than any assigned multitude of prime numbers” (4.430 Google hits)
- ”There are infinitely many prime numbers” (31.800)
- ”There are infinitely many primes” (65.300)
- ”The number of primes is infinite” (34.100)

The infinitude of primes

- Euclid IX, 20: “Prime numbers are more than any assigned multitude of prime numbers” (4.430 Google hits)
- ”There are infinitely many prime numbers” (31.800)
- ”There are infinitely many primes” (65.300)
- ”The number of primes is infinite” (34.100)
- ”The set of primes is infinite” (48.300)

The infinitude of primes

- Euclid IX, 20: “Prime numbers are more than any assigned multitude of prime numbers” (4.430 Google hits)
- ”There are infinitely many prime numbers” (31.800)
- ”There are infinitely many primes” (65.300)
- ”The number of primes is infinite” (34.100)
- ”The set of primes is infinite” (48.300)
- ”The set of prime numbers is infinite” (69.000)

Theoretical aspects

- finite/infinite sets

Theoretical aspects

- finite/infinite sets
- cardinality (“number”)

Theoretical aspects

- finite/infinite sets
- cardinality (“number”)
- unboundedness in $\mathbb{N}$

Theoretical aspects

- finite/infinite sets
- cardinality ("number")
- unboundedness in $\mathbb{N}$
- generalized quantifier $\exists^{\infty}$, there exist infinitely many

Theoretical aspects

- finite/infinite sets
- cardinality (“number”)
- unboundedness in $\mathbb{N}$
- generalized quantifier $\exists^{\infty}$, there exist infinitely many
- ...

Formalizations

F. Wiedijk, `https://www.cs.ru.nl/~freek/100/`: Formalizing 100 Theorems, The Infinitude of Primes

- HOL Light: `|- INFINITE {p | prime p}`

Formalizations

F. Wiedijk, `https://www.cs.ru.nl/~freek/100/`: Formalizing 100 Theorems, The Infinitude of Primes

- HOL Light: `|- INFINITE {p | prime p}`
- Isabelle/HOL: `lemma primes_infinite: "¬finite {p::nat. prime p}"`

Formalizations

F. Wiedijk, `https://www.cs.ru.nl/~freek/100/`: Formalizing 100 Theorems, The Infinitude of Primes

- HOL Light: `|- INFINITE {p | prime p}`
- Isabelle/HOL: `lemma primes_infinite: "¬finite {p::nat. prime p}"`
- Metamath: $\vdash S \approx \mathbb{N}$

Formalizations

F. Wiedijk, `https://www.cs.ru.nl/~freek/100/`: Formalizing 100 Theorems, The Infinitude of Primes

- HOL Light: `|- INFINITE {p | prime p}`
- Isabelle/HOL: `lemma primes_infinite: "¬finite {p::nat. prime p}"`
- Metamath: $\vdash S \approx \mathbb{N}$
- Coq: `Theorem ManyPrimes : ~(EX l:(list Prime) | (p:Prime)(In p l)).`

Formalizations

F. Wiedijk, `https://www.cs.ru.nl/~freek/100/`: Formalizing 100 Theorems, The Infinitude of Primes

- HOL Light: `|- INFINITE {p | prime p}`
- Isabelle/HOL: `lemma primes_infinite: "¬finite {p::nat. prime p}"`
- Metamath: $\vdash S \approx \mathbb{N}$
- Coq: `Theorem ManyPrimes : ~(EX l:(list Prime) | (p:Prime)(In p l)).`
- Mizar: `theorem :: NEWTON:79  SetPrimes is infinite;`

Formalizations

F. Wiedijk, `https://www.cs.ru.nl/~freek/100/`: Formalizing 100 Theorems, The Infinitude of Primes

- HOL Light: `|- INFINITE {p | prime p}`
- Isabelle/HOL: `lemma primes_infinite: "¬finite {p::nat. prime p}"`
- Metamath: $\vdash S \approx \mathbb{N}$
- Coq: `Theorem ManyPrimes : ~(EX l:(list Prime) | (p:Prime)(In p l)).`
- Mizar: `theorem :: NEWTON:79  SetPrimes is infinite;`
- Lean: theorem nat.exists_infinite_primes (n : $\mathbb{N}$) :

  $\exists$ (p : $\mathbb{N}$), n $\leq$ p $\wedge$ nat.prime p

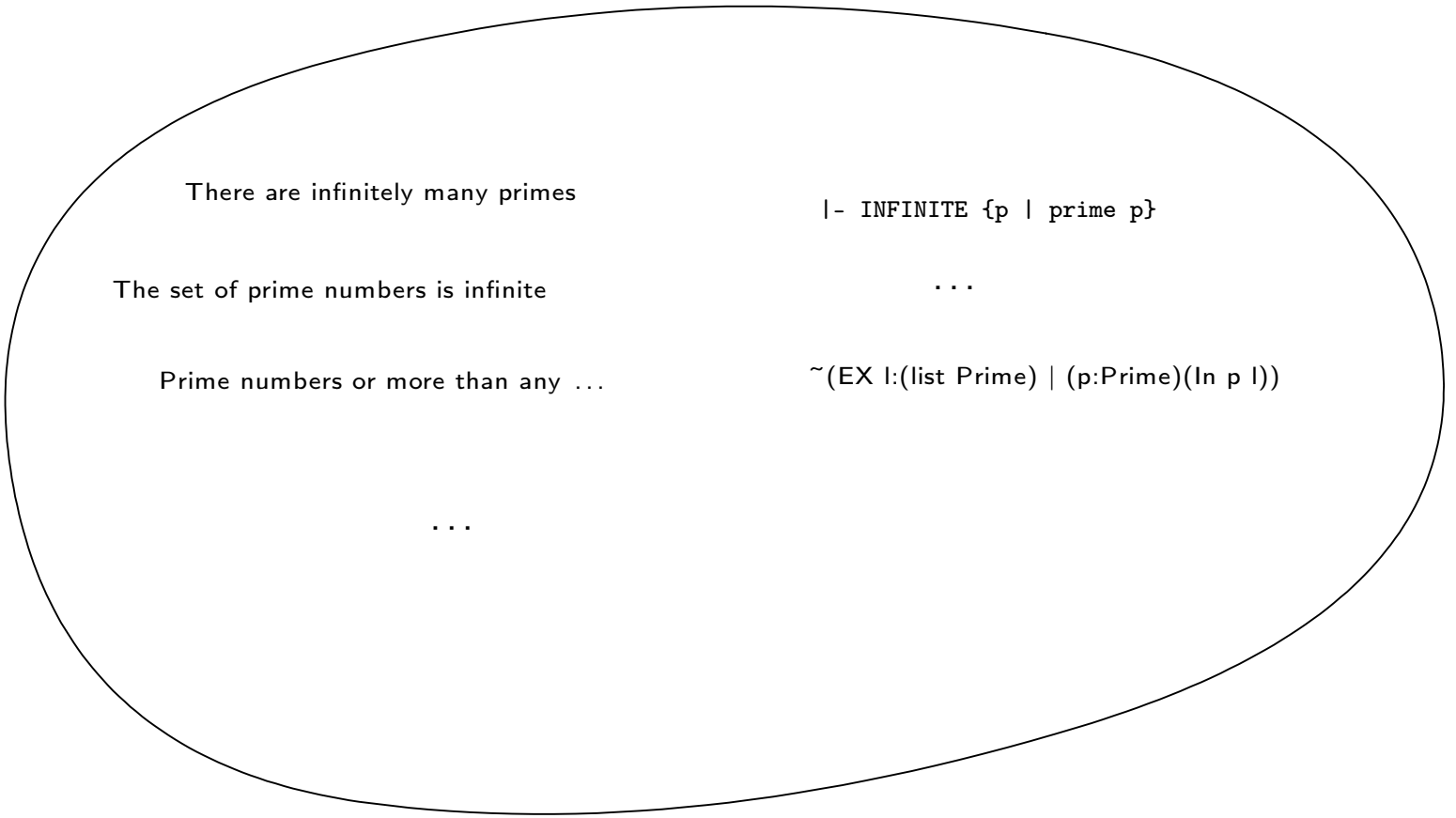
Formalizations

F. Wiedijk, `https://www.cs.ru.nl/~freek/100/`: Formalizing 100 Theorems, The Infinitude of Primes

- HOL Light: `|- INFINITE {p | prime p}`
- Isabelle/HOL: `lemma primes_infinite: "¬finite {p::nat. prime p}"`
- Metamath: $\vdash S \approx \mathbb{N}$
- Coq: `Theorem ManyPrimes : ~(EX l:(list Prime) | (p:Prime)(In p l)).`
- Mizar: `theorem :: NEWTON:79  SetPrimes is infinite;`
- Lean: theorem nat.exists_infinite_primes (n : $\mathbb{N}$) :

  $\exists$ (p : $\mathbb{N}$), n $\leq$ p $\wedge$ nat.prime p
- ...

The infinitude of the infinitudes of primes



What *is* the infinitude of primes?

- the collection of all those (equivalent?) statements?

What *is* the infinitude of primes?

- the collection of all those (equivalent?) statements?
- one particular representative?

What *is* the infinitude of primes?

- the collection of all those (equivalent?) statements?
- one particular representative?
- in some formal language?

What *is* the infinitude of primes?

- the collection of all those (equivalent?) statements?
- one particular representative?
- in some formal language?
- in natural language?

The (natural) language of mathematics

- Let $f\colon \mathbb{C} \to \mathbb{C}$ be holomophic, and let $\gamma\colon [a,b] \to \mathbb{C}$ be a smooth closed curve. Then:

$$\int_\gamma f(z)\,dz = 0.$$

The (natural) language of mathematics

- Let $f\colon \mathbb{C} \to \mathbb{C}$ be holomophic, and let $\gamma\colon [a, b] \to \mathbb{C}$ be a smooth closed curve. Then:

$$\int_\gamma f(z)\, dz = 0.$$

- A. Ranta. *Type theory and the informal language of mathematics.* 1994.

The (natural) language of mathematics

- Let $f\colon \mathbb{C} \to \mathbb{C}$ be holomophic, and let $\gamma\colon [a,b] \to \mathbb{C}$ be a smooth closed curve. Then:

$$\int_\gamma f(z)\,dz = 0.$$

- A. Ranta. *Type theory and the informal language of mathematics.* 1994.
- M. Ganesalingam. *The Language of Mathematics.* 2013.

The (natural) language of mathematics

- Let $f\colon \mathbb{C} \to \mathbb{C}$ be holomophic, and let $\gamma\colon [a,b] \to \mathbb{C}$ be a smooth closed curve. Then:

$$\int_\gamma f(z)\,dz = 0.$$

- A. Ranta. *Type theory and the informal language of mathematics.* 1994.
- M. Ganesalingam. *The Language of Mathematics.* 2013.
- Ganesalingam: *. . . long-term project to construct a computer language for expressing pure mathematics in a way that was as close as possible to real mathematics. . . .*
  . . . half of sentences drawn from textbooks can be expressed without any changes.

Controlled natural languages (CNL)

- Subsets of natural languages that are obtained by restricting the grammar and vocabulary in order to reduce or eliminate ambiguity and complexity.

Controlled natural languages (CNL)

- Subsets of natural languages that are obtained by restricting the grammar and vocabulary in order to reduce or eliminate ambiguity and complexity.
- We consider CNLs with a formal syntax and semantics that can be mapped to an existing formal language.

Controlled natural languages (CNL)

- Subsets of natural languages that are obtained by restricting the grammar and vocabulary in order to reduce or eliminate ambiguity and complexity.
- We consider CNLs with a formal syntax and semantics that can be mapped to an existing formal language.
- N. Fuchs. *Attempto Controlled English*.

Controlled natural languages (CNL)

- Subsets of natural languages that are obtained by restricting the grammar and vocabulary in order to reduce or eliminate ambiguity and complexity.
- We consider CNLs with a formal syntax and semantics that can be mapped to an existing formal language.
- N. Fuchs. *Attempto Controlled English*.
- `A customer enters a card X and a code Y.`
  `If the code Y is valid then the ATM accepts the card X.`

Controlled natural languages for mathematics

- Evidence Algorithm (Victor Glushkov, $\sim$ 1970), ForTheL Input Language (Formula Theory Language, Konstantin Vershinin $\sim$ 1975)

Controlled natural languages for mathematics

- Evidence Algorithm (Victor Glushkov, $\sim$ 1970), ForTheL Input Language (Formula Theory Language, Konstantin Vershinin $\sim$ 1975)
- System for Automated Deduction (Andrei Paskevich, $\sim$ 2007)

Controlled natural languages for mathematics

- Evidence Algorithm (Victor Glushkov, $\sim$ 1970), ForTheL Input Language (Formula Theory Language, Konstantin Vershinin $\sim$ 1975)
- System for Automated Deduction (Andrei Paskevich, $\sim$ 2007)
- "ForTheL ... is a formal language of mathematical texts, which imitates the natural (English) language of mathematical publications issued by human beings. ...
...The ForTheL language can be seen as a kind of controlled English."

Controlled natural languages for mathematics

- Evidence Algorithm (Victor Glushkov, $\sim$ 1970), ForTheL Input Language (Formula Theory Language, Konstantin Vershinin $\sim$ 1975)
- System for Automated Deduction (Andrei Paskevich, $\sim$ 2007)
- "ForTheL ... is a formal language of mathematical texts, which imitates the natural (English) language of mathematical publications issued by human beings. ...
  ... The ForTheL language can be seen as a kind of controlled English."
- Naproche Project, 1st Phase (Bernhard Schröder, PK, $\sim$ 2002), Naproche System (Marcos Cramer, 2013)

Naproche (Natural (Language) Proof Checking)

- Naproche-SAD (Steffen Frerix, PK, 2018)

ℕaproche (Natural (Language) Proof Checking)

- Naproche-SAD (Steffen Frerix, PK, 2018)
- Isabelle/Naproche (Steffen Frerix, Makarius Wenzel, PK, 2019)

ℕaproche (Natural (Language) Proof Checking)

- Naproche-SAD (Steffen Frerix, PK, 2018)
- Isabelle/Naproche (Steffen Frerix, Makarius Wenzel, PK, 2019)
- Integration of ℕaproche in Isabelle 2021

ℕaproche (Natural (Language) Proof Checking)

- Naproche-SAD (Steffen Frerix, PK, 2018)
- Isabelle/Naproche (Steffen Frerix, Makarius Wenzel, PK, 2019)
- Integration of ℕaproche in Isabelle 2021
- LaTeX dialect of ForTheL for mathematical typesetting

ℕaproche (Natural (Language) Proof Checking)

- Naproche-SAD (Steffen Frerix, PK, 2018)
- Isabelle/Naproche (Steffen Frerix, Makarius Wenzel, PK, 2019)
- Integration of ℕaproche in Isabelle 2021
- LaTeX dialect of ForTheL for mathematical typesetting
- ℕaproche as a proof language for Isabelle/HOL

The infinitude of primes in Euclid and ℕaproche

M. Aigner, G. Ziegler, *Proofs from the Book*:

For any finite set $\{p_1, \ldots, p_r\}$ of primes,

consider the number $n = p_1\, p_2 \cdots p_r + 1$.
This n has a prime divisor p.
But p is not one of the p_i:

otherwise

p would be a divisor of n and of the product $p_1\, p_2 \cdots p_r$ and thus also the the difference
$n - p_1\, p_2 \cdots p_r = 1$,
which is impossible.
So a finite set $\{p_1, \ldots, p_r\}$ cannot be the collection of *all* prime numbers. □

ℕaproche formalization:

Signature. $\mathbb{P}$ is the class of prime natural numbers.

Theorem (Euclid). $\mathbb{P}$ is infinite.

Proof.

Assume that r is a natural number and p is a sequence of length r and $\{p_1, \ldots, p_r\}$ is a subclass of $\mathbb{P}$.
(1) p_i is a nonzero natural number for every i such that $1 \leqslant i \leqslant r$.
Consider $n = p_1 \cdots p_r + 1$.
Take a prime divisor q of n.
Let us show that $q \neq p_i$ for all i such that $1 \leqslant i \leqslant r$.
Proof by contradiction. Assume that $q = p_i$ for some natural number i such that $1 \leqslant i \leqslant r$.
q is a divisor of n and q is a divisor of $p_1 \cdots p_r$ (by factor property, 1).
Thus q divides 1.
Contradiction. qed.
Hence $\{p_1, \ldots, p_r\}$ is not the class of prime natural numbers. □

Controlled/Certifiable Natural Mathematics (CNM)

- Recall: *CNL: Subsets of natural languages that are obtained by restricting the grammar and vocabulary in order to reduce or eliminate ambiguity and complexity.*

Controlled/Certifiable Natural Mathematics (CNM)

- **CNM: Comprehensive subset of natural mathematical language and of mathematical texts that is obtained by restricting the grammar in order to eliminate ambiguity and by reducing proof gaps to the capabilities of current automated theorem proving (ATP).**

Controlled/Certifiable Natural Mathematics (CNM)

- **CNM: Comprehensive subset of natural mathematical language and of mathematical texts that is obtained by restricting the grammar in order to eliminate ambiguity and by reducing proof gaps to the capabilities of current automated theorem proving (ATP).**
- A formal syntax and semantics that can be mapped to existing formal languages and axiomatic systems.

Controlled/Certifiable Natural Mathematics (CNM)

- **CNM: Comprehensive subset of natural mathematical language and of mathematical texts that is obtained by restricting the grammar in order to eliminate ambiguity and by reducing proof gaps to the capabilities of current automated theorem proving (ATP).**
- A formal syntax and semantics that can be mapped to existing formal languages and axiomatic systems.
- Identify natural mathematical texts that can be transformed into each other by truth-preserving linguistic equivalences, e.g., "infinite" $\leftrightarrow$ "not finite", or "A and B." $\leftrightarrow$ "A. B."

Formal Abstracts

- T. Hales, The Formal Abstracts project, `https://formalabstracts.github.io/`

Formal Abstracts

- T. Hales, The Formal Abstracts project, `https://formalabstracts.github.io/`
- give a statement of the main theorem of each published mathematical paper in a language that is both human and machine readable

Formal Abstracts

- T. Hales, The Formal Abstracts project, `https://formalabstracts.github.io/`
- give a statement of the main theorem of each published mathematical paper in a language that is both human and machine readable
- link each term in theorem statements to a precise definition of that term (again in human/machine readable form)

Formal Abstracts

- T. Hales, The Formal Abstracts project, `https://formalabstracts.github.io/`
- give a statement of the main theorem of each published mathematical paper in a language that is both human and machine readable
- link each term in theorem statements to a precise definition of that term (again in human/machine readable form)
- ground every statement and definition in the system in some foundational system for doing mathematics

$\mathbb{N}$aproche $\rightsquigarrow$ CNM

- $\mathbb{N}$aproche as proof of concept for CNM?

$\mathbb{N}$aproche $\rightsquigarrow$ CNM

- $\mathbb{N}$aproche as proof of concept for CNM?
- extending ForTheL for wider coverage; richer text structurings; richer statement grammar; semantically enriched standard vocabulary of words and symbols

$\mathbb{N}$aproche $\rightsquigarrow$ CNM

- $\mathbb{N}$aproche as proof of concept for CNM?
- extending ForTheL for wider coverage; richer text structurings; richer statement grammar; semantically enriched standard vocabulary of words and symbols
- type derivation and elaboration (like Mizar, Lean)

$\mathbb{N}$aproche $\rightsquigarrow$ CNM

- $\mathbb{N}$aproche as proof of concept for CNM?
- extending ForTheL for wider coverage; richer text structurings; richer statement grammar; semantically enriched standard vocabulary of words and symbols
- type derivation and elaboration (like Mizar, Lean)
- Sledgehammer-like methods for using external provers (ATPs)

$\mathbb{N}$aproche $\rightsquigarrow$ CNM

- $\mathbb{N}$aproche as proof of concept for CNM?
- extending ForTheL for wider coverage; richer text structurings; richer statement grammar; semantically enriched standard vocabulary of words and symbols
- type derivation and elaboration (like Mizar, Lean)
- Sledgehammer-like methods for using external provers (ATPs)
- libraries of ForTheL documents with natural import and export mechanisms

Formal mathematics and current mathematical research

- Lean: formalization of P. Scholze's *perfectoid spaces*

Formal mathematics and current mathematical research

- Lean: formalization of P. Scholze's *perfectoid spaces*
- P. Scholze: *Liquid Tensor Experiment*; to formalize parts of "condensed mathematics"

Formal mathematics and current mathematical research

- Lean: formalization of P. Scholze's *perfectoid spaces*
- P. Scholze: *Liquid Tensor Experiment*; to formalize parts of "condensed mathematics"
- June 2021: crucial Lemma of Liquid Tensor Experiment formalized in Lean

CNM and current research

From P. Scholze, *Étale cohomology of diamonds*:

Definition. *A Tate ring R is perfectoid if R is complete, uniform, i.e. $R^o \subset R$ is bounded, and there exists a pseudo-uniformizer $\bar{\omega} \in R$ such that $\bar{\omega}^p | \, p$ in R^o and the Frobenius map*

$$\Phi \colon R^o / \bar{\omega} \to R^o / \bar{\omega}^p \colon x \mapsto x^p$$

is an isomorphism.

CNM and current research

From P. Scholze, *Étale cohomology of diamonds*:

Definition. *A Tate ring R is perfectoid if R is complete, uniform, i.e. $R^o \subset R$ is bounded, and there exists a pseudo-uniformizer $\bar{\omega} \in R$ such that $\bar{\omega}^p | p$ in R^o and the Frobenius map*

$$\Phi \colon R^o / \bar{\omega} \to R^o / \bar{\omega}^p \colon x \mapsto x^p$$

is an isomorphism.

From the Lean formalization of perfectoid spaces:

```
structure perfectoid_ring (R : Type) [Huber_ring R] extends Tate_ring R :
(complete  : is_complete_hausdorff R)
(uniform   : is_uniform R)
(ramified : ∃ω : pseudo-uniformizer R, ω^p | p in R°)
(Frobenius : surjective (Frob R°/p))
```

CNM and current research

From P. Scholze, *Étale cohomology of diamonds*:

Definition. *A Tate ring R is perfectoid if R is complete, uniform, i.e. $R^o \subset R$ is bounded, and there exists a pseudo-uniformizer $\bar{\omega} \in R$ such that $\bar{\omega}^p | \, p$ in R^o and the Frobenius map*

$$\Phi \colon R^o / \bar{\omega} \to R^o / \bar{\omega}^p \colon x \mapsto x^p$$

is an isomorphism.

From a $\mathbb{N}$aproche formalization of perfectoid rings:

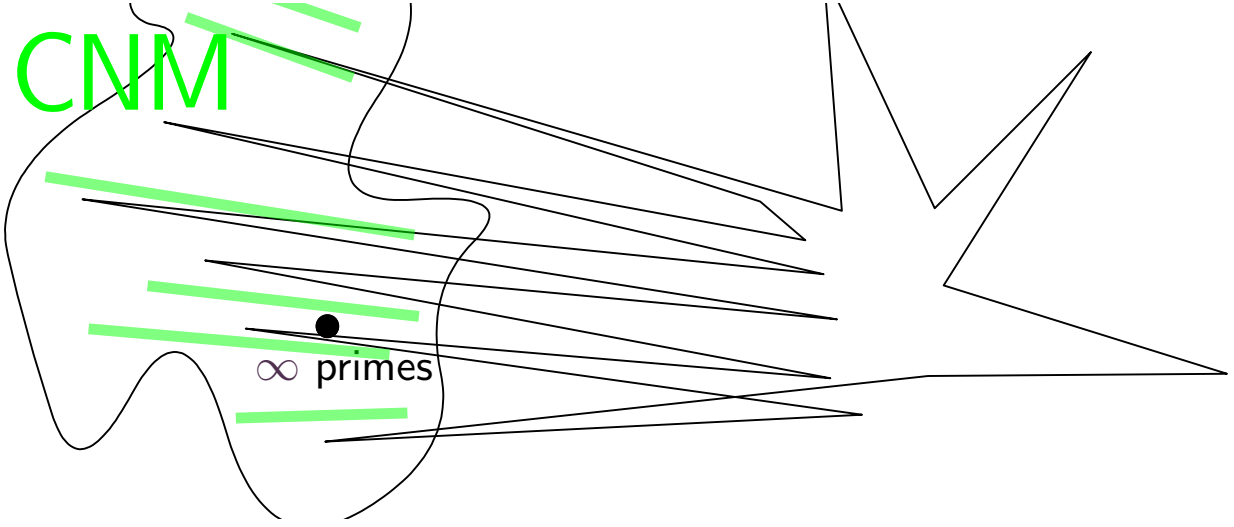
Definition. *R is perfectoid iff R is complete and uniform and there exists a pseudouniformizer ω in R such that $\omega^{p,R} | p$ in R^o within R and*

$$\Phi^R \colon R^o / \omega \cong R^o / \omega^{p,R}.$$

Controlled/Certifiable Natural Mathematics

Formal mathematics should be "dense" in natural mathematics,

i.e., formal mathematics should intersect every equivalence class of natural statements and proofs modulo truth-preserving natural language modifications and reformulations.



Thank you