Verifying computational mathematics

Machine Assisted Proofs, IPAM

Assia Mahboubi

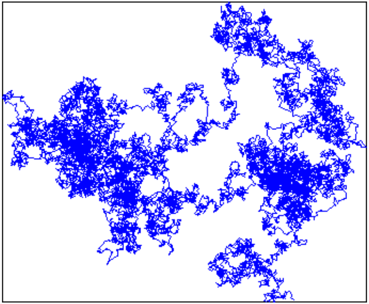
February 15th 2023

Inria, LS2N, Nantes Université, Vrije Universiteit Amsterdam

European Research Council
Established by the European Commission

Computational mathematics

Experimentation



"The notion that these **conjectures** might have been reached by pure thought – with no picture – is simply inconceivable. . . I had my programmer draw a very big sample [Brownian] motion and proceeded to play with it" B. Mandelbrot, 1982[1]

[1] Cited in *Mathematics in the Age of the Turing Machine*, Thomas Hales, ASL Lecture Notes in Logic. 2013.

Birch and Swinnerton-Dyer Conjecture

Mathematicians have always been fascinated by the problem of describing all solutions in whole numbers x,y,z to algebraic equations like

$$x^2 + y^2 = z^2$$

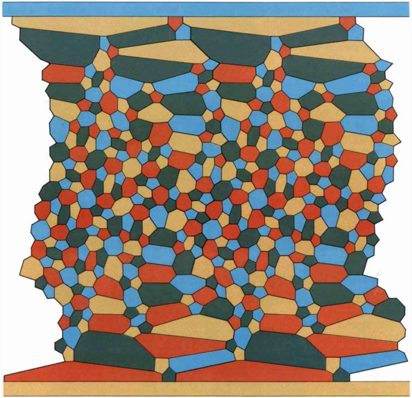
Euclid gave the complete solution for that equation, but for more complicated equations this becomes extremely difficult. Indeed, in 1970 Yu. V. Matiyasevich showed that Hilbert's tenth problem is unsolvable, i.e., there is no general method for determining when such equations have a solution in whole numbers. But in special cases one can hope to say something. When the solutions are the points of an abelian variety, the Birch and Swinnerton-Dyer conjecture asserts that the size of the group of rational points is related to the behavior of an associated zeta function $\zeta(s)$ near the point s=1. In particular this amazing conjecture asserts that if $\zeta(1)$ is equal to 0, then there are an infinite number of rational points (solutions), and conversely, if $\zeta(1)$ is not equal to 0, then there is only a finite number of such points.

This problem is:	Unsolved

Proofs

Four color theorem (K. Appel, W. Haken - 1976)

Every planar map is four colorable.



[A computer-checked proof of the four color theorem, G. Gonthier - 2003]

Proofs

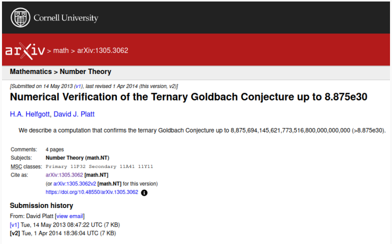
Ternary Goldbach conjecture is true (H. Helfgott - 2013)

Every odd integer greater than 5 is the sum of three primes.

Proofs

Ternary Goldbach conjecture is true (H. Helfgott - 2013)

Every odd integer greater than 5 is the sum of three primes.



Cornell University

arXiv > math > arXiv:1305.3062

Mathematics > Number Theory

[Submitted on 14 May 2013 (v1), last revised 1 Apr 2014 (this version, v2)]

Numerical Verification of the Ternary Goldbach Conjecture up to 8.875e30

H.A. Helfgott, David J. Platt

We describe a computation that confirms the ternary Goldbach Conjecture up to 8,875,694,145,621,773,516,800,000,000,000 (>8.875e30).

Comments:	4 pages
Subjects:	**Number Theory (math.NT)**
MSC classes:	Primary 11P32 Secondary 11A41 11Y11
Cite as:	arXiv:1305.3062 **[math.NT]**
	(or arXiv:1305.3062v2 **[math.NT]** for this version)
	https://doi.org/10.48550/arXiv.1305.3062

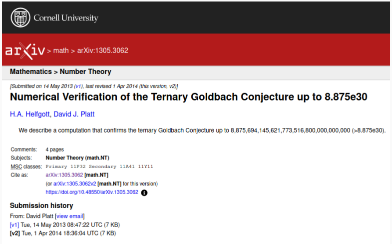
Submission history

From: David Platt [view email]
[v1] Tue, 14 May 2013 08:47:22 UTC (7 KB)
[v2] Tue, 1 Apr 2014 18:36:04 UTC (7 KB)

Proofs

Ternary Goldbach conjecture is true (H. Helfgott - 2013)

Every odd integer greater than 5 is the sum of three primes.



Cornell University

arXiv > math > arXiv:1305.3062

Mathematics > Number Theory

[Submitted on 14 May 2013 (v1), last revised 1 Apr 2014 (this version, v2)]

Numerical Verification of the Ternary Goldbach Conjecture up to 8.875e30

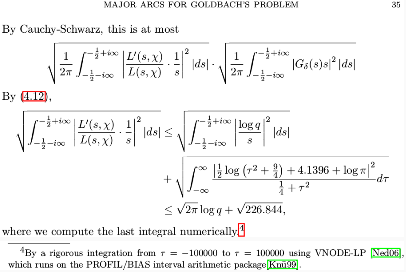
H.A. Helfgott, David J. Platt

We describe a computation that confirms the ternary Goldbach Conjecture up to 8,875,694,145,621,773,516,800,000,000,000 (>8.875e30).

Comments: 4 pages
Subjects: Number Theory (math.NT)
MSC classes: Primary 11P32 Secondary 11A41 11Y11
Cite as: arXiv:1305.3062 [math.NT]
(or arXiv:1305.3062v2 [math.NT] for this version)
https://doi.org/10.48550/arXiv.1305.3062

Submission history

From: David Platt [view email]
[v1] Tue, 14 May 2013 08:47:22 UTC (7 KB)
[v2] Tue, 1 Apr 2014 18:36:04 UTC (7 KB)



MAJOR ARCS FOR GOLDBACH'S PROBLEM 35

By Cauchy-Schwarz, this is at most

$$\sqrt{\frac{1}{2\pi}\int_{-\frac{1}{2}-i\infty}^{-\frac{1}{2}+i\infty}\left|\frac{L'(s,\chi)}{L(s,\chi)}\cdot\frac{1}{s}\right|^2|ds|}\cdot\sqrt{\frac{1}{2\pi}\int_{-\frac{1}{2}-i\infty}^{-\frac{1}{2}+i\infty}|G_\delta(s)s|^2\,|ds|}$$

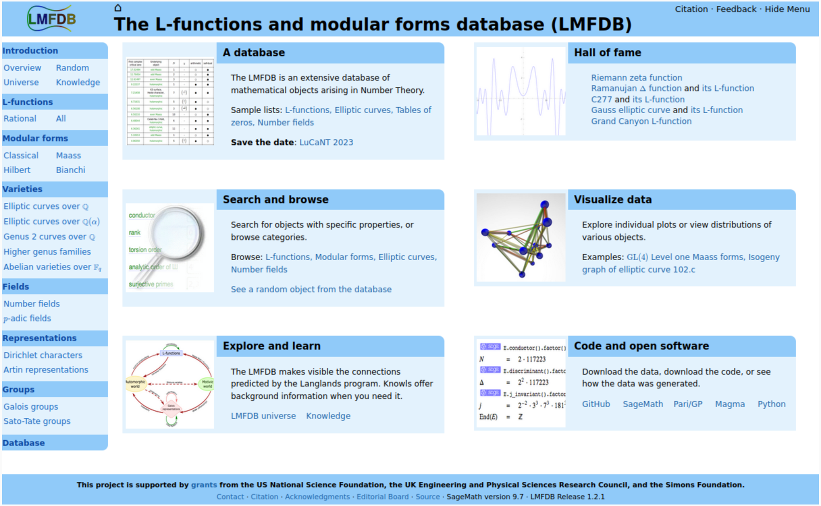
By (4.12),

$$\sqrt{\int_{-\frac{1}{2}-i\infty}^{-\frac{1}{2}+i\infty}\left|\frac{L'(s,\chi)}{L(s,\chi)}\cdot\frac{1}{s}\right|^2|ds|}\leq\sqrt{\int_{-\frac{1}{2}-i\infty}^{-\frac{1}{2}+i\infty}\left|\frac{\log q}{s}\right|^2|ds|}$$
$$+\sqrt{\int_{-\infty}^{\infty}\frac{\left|\frac{1}{2}\log\left(\tau^2+\frac{9}{4}\right)+4.1396+\log\pi\right|^2}{\frac{1}{4}+\tau^2}d\tau}$$
$$\leq\sqrt{2\pi}\log q+\sqrt{226.844},$$

where we compute the last integral numerically.[4]

[4] By a rigorous integration from $\tau=-100000$ to $\tau=100000$ using VNODE-LP [Ned06], which runs on the PROFIL/BIAS interval arithmetic package [Knü99].

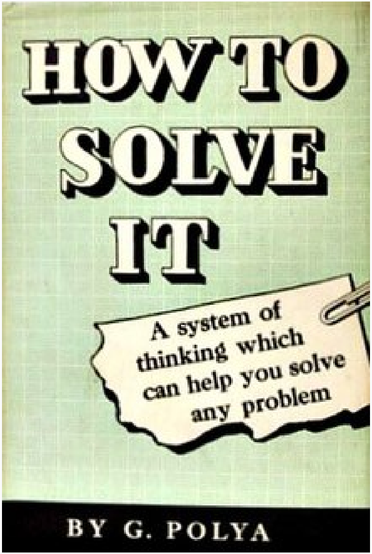
Data


LMFDB
The L-functions and modular forms database (LMFDB)
Citation · Feedback · Hide Menu
Introduction
Overview Random
Universe Knowledge
L-functions
Rational All
Modular forms
Classical Maass
Hilbert Bianchi
Varieties
Elliptic curves over $\mathbb{Q}$
Elliptic curves over $\mathbb{Q}(\alpha)$
Genus 2 curves over $\mathbb{Q}$
Higher genus families
Abelian varieties over $\mathbb{F}_q$
Fields
Number fields
p-adic fields
Representations
Dirichlet characters
Artin representations
Groups
Galois groups
Sato-Tate groups
Database
A database
The LMFDB is an extensive database of mathematical objects arising in Number Theory.
Sample lists: L-functions, Elliptic curves, Tables of zeros, Number fields
Save the date: LuCaNT 2023
Hall of fame
Riemann zeta function
Ramanujan Δ function and its L-function
C277 and its L-function
Gauss elliptic curve and its L-function
Grand Canyon L-function
Search and browse
conductor
rank
torsion order
analytic order of Ш
surjective primes
Search for objects with specific properties, or browse categories.
Browse: L-functions, Modular forms, Elliptic curves, Number fields
See a random object from the database
Visualize data
Explore individual plots or view distributions of various objects.
Examples: GL(4) Level one Maass forms, Isogeny graph of elliptic curve 102.c
Explore and learn
L-functions
Automorphic world
Motivic world
Galois representations
The LMFDB makes visible the connections predicted by the Langlands program. Knowls offer background information when you need it.
LMFDB universe Knowledge
Code and open software
E.conductor().factor()
$N = 2 \cdot 117223$
E.discriminant().factor()
$\Delta = 2^2 \cdot 117223$
E.j_invariant().factor()
End(E) = Z
Download the data, download the code, or see how the data was generated.
GitHub SageMath Pari/GP Magma Python
This project is supported by grants from the US National Science Foundation, the UK Engineering and Physical Sciences Research Council, and the Simons Foundation.
Contact · Citation · Acknowledgments · Editorial Board · Source · SageMath version 9.7 · LMFDB Release 1.2.1

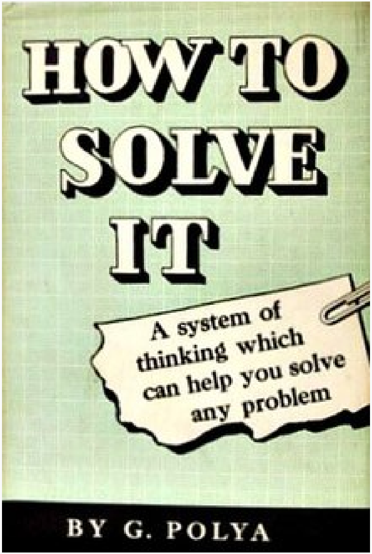
Computer-aided mathematics

- Effective results
- Efficient algorithms
- Smart implementations

Guess and then prove



Guess and then prove



Guessing with Little Data*

Manuel Kauers[a], Christoph Koutschan[b]

[a]Institute for Algebra, Johannes Kepler University, Linz, A4040, Austria, manuel.kauers@jku.at
[b]RICAM, Austrian Academy of Sciences, Linz, A4040, Austria, christoph.koutschan@ricam.oeaw.ac.at

Abstract

Reconstructing a hypothetical recurrence equation from the first terms of an infinite sequence is a classical and well-known technique in experimental mathematics. We propose a variation of this technique which can succeed with fewer input terms.

1 Introduction

A simple but powerful technique which is has become an important tool in experimental mathematics takes as input the first few terms of an infinite sequence and returns as output a plausible hypothesis for a recurrence equation that the sequence may satisfy, or a plausible hypothesis for a differential equation satisfied by its generating function. The principle is known as automated guessing as it somehow makes a guess how the infinite sequence continues beyond the finitely many terms supplied as input. In certain situations where sufficient additional information is available about the sequence at hand, automated guessing can be combined with other techniques from computer algebra that confirm that the guessed equation is correct. One of many successful applications of this paradigm is the proof of the qTSPP conjecture [20].

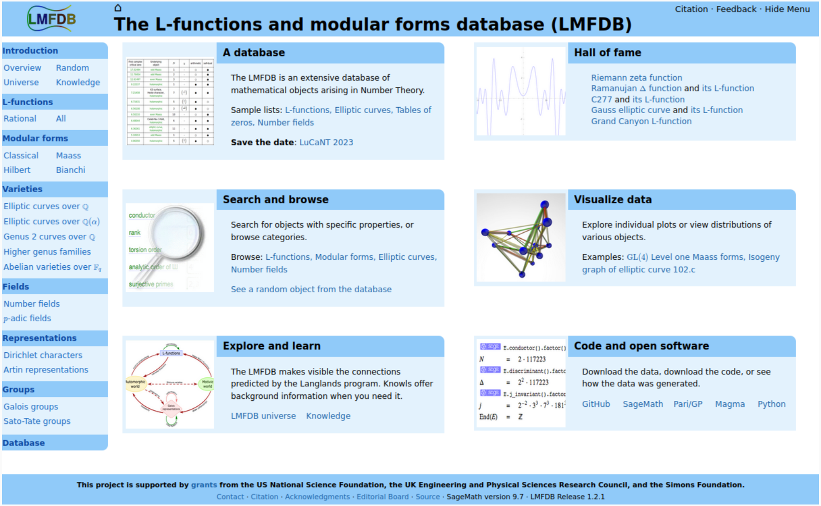
[How to solve it, G. Pólya, Princeton University Press, 1945]
[Guessing with little data, M. Kauers and K. Koutschan, Proceedings of ISSAC 2022]

Trusting computational mathematics ?

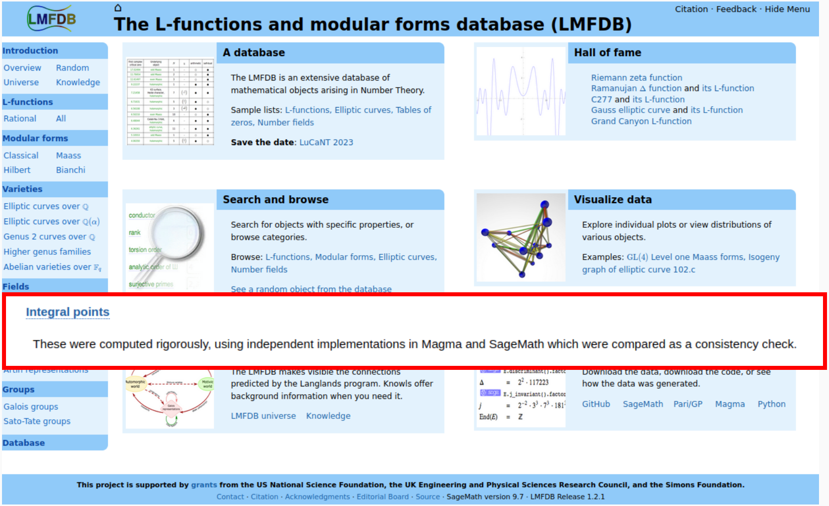
Reproducibility

- Commercial software
- Closed code
- Single implementations

Reproducibility



Reproducibility



Integral points

These were computed rigorously, using independent implementations in Magma and SageMath which were compared as a consistency check.

Cross-verification is not enough

In SymPy 1.7.1 [2], compare

```
>>> simplify(hyper([n],[m],x).subs({m:-1, n:-1, x:1}))
                                                        2
```

with

```
>>> simplify(hyper([n],[m],x).subs(m, n)).subs({n:-1, x:1})
                                                       E
```

[2]Example suggested by F. Johansson.

Cross-verification is not enough

In SymPy 1.7.1 [2], compare

```
>>> simplify(hyper([n],[m],x).subs({m:-1, n:-1, x:1}))
                                                        2
```

with

```
>>> simplify(hyper([n],[m],x).subs(m, n)).subs({n:-1, x:1})
                                                       E
```

$\Rightarrow$ A posteriori verification techniques cannot apply.

[2] Example suggested by F. Johansson.

Cross-verification is not enough

In SymPy 1.7.1 [2], compare

```
>>> simplify(hyper([n],[m],x).subs({m:-1, n:-1, x:1}))
                                                         2
```

with

```
>>> simplify(hyper([n],[m],x).subs(m, n)).subs({n:-1, x:1})
                                                        E
```

$\Rightarrow$ A posteriori verification techniques cannot apply.

Wolfram Language (Mathematica) exhibit the exact same phenomenon.

$\Rightarrow$ Cross-verification is not enough.

[2] Example suggested by F. Johansson.

Proofs can go wrong

Proofs can go wrong

MAJOR ARCS FOR GOLDBACH'S PROBLEM 35

By Cauchy-Schwarz, this is at most

$$\sqrt{\frac{1}{2\pi}\int_{-\frac{1}{2}-i\infty}^{-\frac{1}{2}+i\infty}\left|\frac{L'(s,\chi)}{L(s,\chi)}\cdot\frac{1}{s}\right|^2|ds|}\cdot\sqrt{\frac{1}{2\pi}\int_{-\frac{1}{2}-i\infty}^{-\frac{1}{2}+i\infty}|G_\delta(s)s|^2\,|ds|}$$

By (4.12),

$$\begin{aligned}\sqrt{\int_{-\frac{1}{2}-i\infty}^{-\frac{1}{2}+i\infty}\left|\frac{L'(s,\chi)}{L(s,\chi)}\cdot\frac{1}{s}\right|^2|ds|} &\leq \sqrt{\int_{-\frac{1}{2}-i\infty}^{-\frac{1}{2}+i\infty}\left|\frac{\log q}{s}\right|^2|ds|}\\ &\quad+\sqrt{\int_{-\infty}^{\infty}\frac{\left|\frac{1}{2}\log\left(\tau^2+\frac{9}{4}\right)+4.1396+\log\pi\right|^2}{\frac{1}{4}+\tau^2}d\tau}\\ &\leq \sqrt{2\pi}\log q+\sqrt{226.844},\end{aligned}$$

where we compute the last integral numerically.[4]

[4] By a rigorous integration from $\tau = -100000$ to $\tau = 100000$ using VNODE-LP [Ned06], which runs on the PROFIL/BIAS interval arithmetic package [Knü99].

Proofs can go wrong

By Cauchy-Schwarz, this is at most

$$\sqrt{\frac{1}{2\pi}\int_{-\frac{1}{2}-i\infty}^{-\frac{1}{2}+i\infty}\left|\frac{L'(s,\chi)}{L(s,\chi)}\cdot\frac{1}{s}\right|^2|ds|}\cdot\sqrt{\frac{1}{2\pi}\int_{-\frac{1}{2}-i\infty}^{-\frac{1}{2}+i\infty}|G_\delta(s)s|^2\,|ds|}$$

By (4.12),

$$\begin{aligned}\sqrt{\int_{-\frac{1}{2}-i\infty}^{-\frac{1}{2}+i\infty}\left|\frac{L'(s,\chi)}{L(s,\chi)}\cdot\frac{1}{s}\right|^2|ds|} &\leq \sqrt{\int_{-\frac{1}{2}-i\infty}^{-\frac{1}{2}+i\infty}\left|\frac{\log q}{s}\right|^2|ds|}\\ &\quad+\sqrt{\int_{-\infty}^{\infty}\frac{\left|\frac{1}{2}\log\left(\tau^2+\frac{9}{4}\right)+4.1396+\log\pi\right|^2}{\frac{1}{4}+\tau^2}d\tau}\\ &\leq\sqrt{2\pi}\log q+\sqrt{226.844},\end{aligned}$$

where we compute the last integral numerically.[4]

[4] By a rigorous integration from $\tau = -100000$ to $\tau = 100000$ using VNODE-LP [Ned06], which runs on the PROFIL/BIAS interval arithmetic package [Knü99].

- This estimation is wrong (although the proof can be repaired).

[Formally Verified Approximations of Definite Integrals - A. Mahboubi, G. Melquiond, Th. Sibut-Pinote, JAR 2018]

Proofs can go wrong

Testing reference implementations of rigorous quadratures on:

$$\int_0^1 |(x^4 + 10x^3 + 19x^2 - 6x - 6)e^x| dx \simeq 11.14731055005714$$

Proofs can go wrong

Testing reference implementations of rigorous quadratures on:

$$\int_0^1 |(x^4 + 10x^3 + 19x^2 - 6x - 6)e^x| dx \simeq 11.14731055005714$$

- Octave's `quad`/`quadgk`: only 10/9 correct digits;
- INTLAB verifyquad: false answer without warning;
- VNODE-LP: cannot be used because of the absolute value.

Proofs can go wrong

Testing reference implementations of rigorous quadratures on:

$$\int_0^1 |(x^4 + 10x^3 + 19x^2 - 6x - 6)e^x| dx \simeq 11.14731055005714$$

- Octave's `quad`/`quadgk`: only 10/9 correct digits;
- INTLAB verifyquad: false answer without warning;
- VNODE-LP: cannot be used because of the absolute value.

INTLAB bug report (2016) $\Rightarrow$ Removed support for the absolute value

Mathematical functions on paper

$$\sqrt{x}$$

Mathematical functions for the computer

```c
arb_sqrt(arb_t z, const arb_t x, slong prec)
{
    mag_t rx, zr;
    int inexact;

    if (mag_is_zero(arb_radref(x)))
    {
        arb_sqrt_arf(z, arb_midref(x), prec);
    }
    else if (arf_is_special(arb_midref(x)) ||
                arf_sgn(arb_midref(x)) < 0 || mag_is_inf(arb_radref(x)))
    {
        if (arf_is_pos_inf(arb_midref(x)) && mag_is_finite(arb_radref(x)))
            arb_sqrt_arf(z, arb_midref(x), prec);
        else
            arb_indeterminate(z);
    }
    else  /* now both mid and rad are non-special values, mid > 0 */
    {
        slong acc;

        acc = _fmpz_sub_small(ARF_EXPREF(arb_midref(x)), MAG_EXPREF(arb_radref(x)));
        acc = FLINT_MIN(acc, prec);
        prec = FLINT_MIN(prec, acc + MAG_BITS);
        prec = FLINT_MAX(prec, 2);

        if (acc < 0)
        {
            arb_indeterminate(z);
        }
        else if (acc <= 20)
        {
            mag_t t, u;

            mag_init(t);
            mag_init(u);

            arb_get_mag_lower(t, x);

            if (mag_is_zero(t) && arb_contains_negative(x))
            {
```

[Arb: efficient arbitrary-precision midpoint-radius interval arithmetic, Johansson, IEEE Trans. on Computers 2017]

Trusting computational mathematics

Program verification

Recipe:

- State expected properties on input
- State desired theorem on outcome
- Inspect of the code to prove implication

Ingredients:

- Appropriate specification language, expressive enough
- (Human insight)
- Automated proofs

Example: in-place inversion of a permutation

- From a permutation array and a few extra slots:

2	4	5	1	3			

- Compute the array of the inverse permutation:

4	1	5	2	3			

Rules of the game:

- Overwritten data is lost.
- The number of extra slot does not depend on the permutation.

Program verification

Recipe:

- State expected properties on input
- State desired theorem on outcome
- Inspect of the code to prove implication

Ingredients:

- Appropriate specification language, expressive enough
- Automated proofs
- (Human insight)

Program verification for mathematics

Recipe:

- State expected properties on input
- State desired theorem on outcome
- Inspect of the code to prove implication
- Interpret symbolic data

Ingredients:

- Appropriate specification language, expressive enough
- Automated proofs
- (Human insight)
- Libraries of verified theorems

Example: computing rigorous quadratures

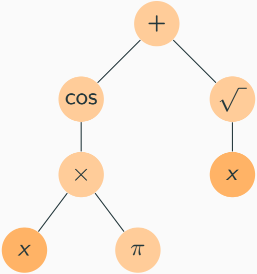
$$\int_0^1 |(x^4 + 10x^3 + 19x^2 - 6x - 6)e^x| dx \simeq 11.14731055005714$$

Example: computing rigorous quadratures

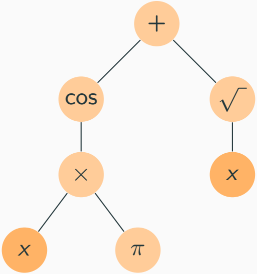
$$\int_0^1 |(x^4 + 10x^3 + 19x^2 - 6x - 6)e^x| dx \simeq 11.14731055005714$$

- Trade floating point numbers for intervals.
- Implement interval extensions for mathematical functions.

Abstract syntax trees for univariate expressions

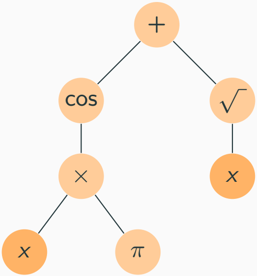


Abstract syntax trees for univariate expressions



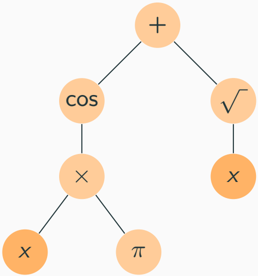
$$[e]_{\mathbb{R}} \quad : \; \mathbb{R} \quad \to \mathbb{R}$$

Abstract syntax trees for univariate expressions



$$[e]_{\mathbb{R}} \quad : \quad \mathbb{R} \quad \to \mathbb{R} \qquad\qquad x \mapsto \cos\left(x \times \pi\right) + \sqrt{x}$$

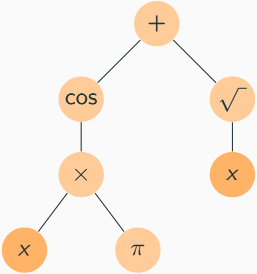
Abstract syntax trees for univariate expressions



$[e]_{\mathbb{R}_\perp} \;:\; \mathbb{R}_\perp \to \mathbb{R}_\perp$

$x \mapsto \cos(x \times \pi) + \sqrt{x}$

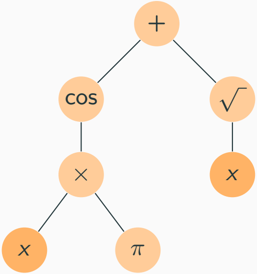
Abstract syntax trees for univariate expressions



$$[e]_{\mathbb{R}_\perp} : \mathbb{R}_\perp \to \mathbb{R}_\perp \qquad x \mapsto \cos(x \times \pi) + \sqrt{x}$$

$$[e]_{\mathbb{I}} : \mathbb{I} \to \mathbb{I}$$

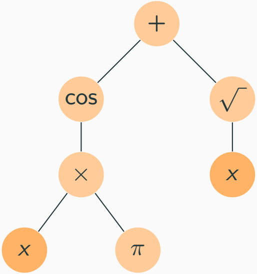
Abstract syntax trees for univariate expressions



$$[e]_{\mathbb{R}_\perp} \ : \ \mathbb{R}_\perp \to \mathbb{R}_\perp \qquad x \mapsto \cos(x \times \pi) + \sqrt{x}$$

$$[e]_{\mathbb{I}} \ : \ \mathbb{I} \to \mathbb{I} \qquad \boldsymbol{x \mapsto \cos(x \times \pi) + \sqrt{x}}$$

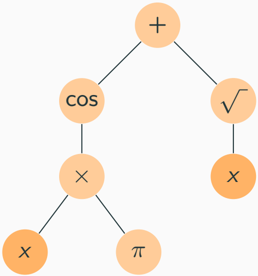
Abstract syntax trees for univariate expressions



$[e]_{\mathbb{R}_\perp} \; : \; \mathbb{R}_\perp \to \mathbb{R}_\perp \qquad x \mapsto \cos(x \times \pi) + \sqrt{x}$

$[e]_{\mathbb{I}_\perp} \; : \; \mathbb{I}_\perp \to \mathbb{I}_\perp \qquad \boldsymbol{x \mapsto \cos(x \times \pi) + \sqrt{x}}$

Abstract syntax trees for univariate expressions



$$[e]_{\mathbb{R}_\perp} \; : \; \mathbb{R}_\perp \to \mathbb{R}_\perp \qquad x \mapsto \cos(x \times \pi) + \sqrt{x}$$

$$[e]_{\mathbb{I}_\perp} \; : \; \mathbb{I}_\perp \to \mathbb{I}_\perp \qquad \boldsymbol{x} \mapsto \mathbf{cos}\,(\boldsymbol{x} \times \boldsymbol{\pi}) + \sqrt{\boldsymbol{x}}$$

Correctness theorem of interval extensions:

$$\forall e \in \mathcal{E}, \quad \forall \boldsymbol{i} \in \mathbb{I}_\perp, \quad \forall x \in \boldsymbol{i}, \quad [e]_{\mathbb{R}_\perp}(x) \in [e]_{\mathbb{I}_\perp}(\boldsymbol{i})$$

Formally verified approximations

$$\int_0^1 |(x^4 + 10x^3 + 19x^2 - 6x - 6)e^x|dx \simeq 11.14731055005714$$

$$\int_a^b f(x)dx \in [m, M] \quad ?$$

Formally verified approximations

$$\int_0^1 |(x^4 + 10x^3 + 19x^2 - 6x - 6)e^x| dx \simeq 11.14731055005714$$

$$\int_{[e_a]_{\mathbb{R}}}^{[e_b]_{\mathbb{R}}} [e_f]_{\mathbb{R}} dx \in [m, M] \quad ?$$

Formally verified approximations

$$\int_0^1 |(x^4 + 10x^3 + 19x^2 - 6x - 6)e^x| dx \simeq 11.14731055005714$$

$$\int_{[e_a]_{\mathbb{R}}}^{[e_b]_{\mathbb{R}}} [e_f]_{\mathbb{R}} \, dx$$

Formally verified approximations

$$\int_0^1 |(x^4 + 10x^3 + 19x^2 - 6x - 6)e^x| dx \simeq 11.14731055005714$$

$$\int_{[e_a]_{\mathbb{R}}}^{[e_b]_{\mathbb{R}}} [e_f]_{\mathbb{R}} dx \in \int_{[e_a]_{\mathbb{I}}}^{[e_b]_{\mathbb{I}}} [e_f]_{\mathbb{I}} dx$$

Formally verified approximations

$$\int_0^1 |(x^4 + 10x^3 + 19x^2 - 6x - 6)e^x| dx \simeq 11.14731055005714$$

$$\int_{[e_a]_{\mathbb{R}}}^{[e_b]_{\mathbb{R}}} [e_f]_{\mathbb{R}} dx \in \int_{[e_a]_{\mathbb{I}}}^{[e_b]_{\mathbb{I}}} [e_f]_{\mathbb{I}} dx \subseteq [m, M]$$

[Formally Verified Approximations of Definite Integrals, A. Mahboubi, G. Melquiond, Th. Sibut-Pinote, JAR 2018]

Formally verified approximations

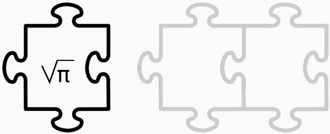
Verified computation, using rigorous polynomial approximations:

$$\int_{[e_a]_{\mathbb{R}}}^{[e_b]_{\mathbb{R}}} [e_f]_{\mathbb{R}}\, dx \in \int_{[e_a]_{\mathbb{TM}}}^{[e_b]_{\mathbb{TM}}} [e_f]_{\mathbb{TM}}\, dx \subseteq [m, M]$$

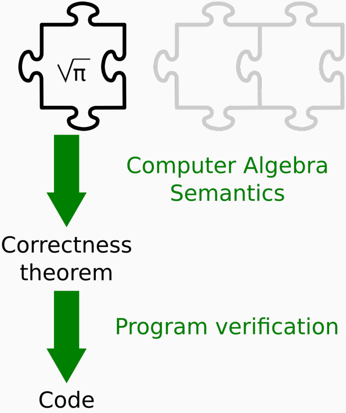
[Formally Verified Approximations of Definite Integrals, A. Mahboubi, G. Melquiond, Th. Sibut-Pinote, JAR 2018]

Benefits

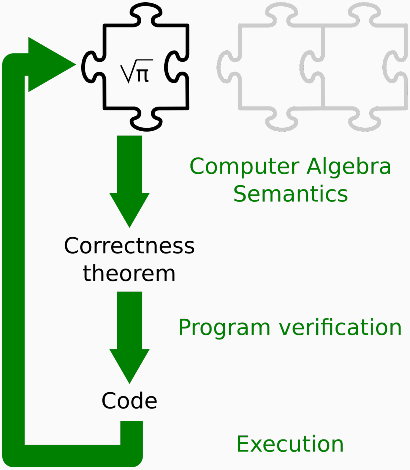
Formally verified computational mathematics



Formally verified computational mathematics



Formally verified computational mathematics



Homological algebra

FIGURE 2. The zero-th page of the tropical spectral sequence ${}_p\mathsf{C}_0^{\bullet,\bullet}$ over $\mathbf{F}^p$.

$$\begin{tikzcd}
\bigoplus\limits_{|\delta|=0} \bigwedge^0 \mathrm{T}^\star\delta \otimes \mathbf{F}^p(\underline{0}^\delta) \arrow[r, dashed, "\pi^* + \mathrm{d}^{\mathrm{i}}"] \arrow[d, "\mathrm{i}^*_{/\!/} \otimes \mathrm{i}^*_{\perp}"] & \bigoplus\limits_{|\delta|=1} \bigwedge^0 \mathrm{T}^\star\delta \otimes \mathbf{F}^p(\underline{0}^\delta) \arrow[d] & \cdots & \bigoplus\limits_{|\delta|=d-p} \bigwedge^0 \mathrm{T}^\star\delta \otimes \mathbf{F}^p(\underline{0}^\delta) \arrow[d] \\
\bigoplus\limits_{|\delta|=1} \bigwedge^1 \mathrm{T}^\star\delta \otimes \mathbf{F}^{p-1}(\underline{0}^\delta) \arrow[r, dashed] \arrow[d] & \bigoplus\limits_{|\delta|=2} \bigwedge^1 \mathrm{T}^\star\delta \otimes \mathbf{F}^{p-1}(\underline{0}^\delta) \arrow[d] & \cdots & \bigoplus\limits_{|\delta|=d-p+1} \bigwedge^1 \mathrm{T}^\star\delta \otimes \mathbf{F}^{p-1}(\underline{0}^\delta) \arrow[d] \\
\vdots \arrow[d] & \vdots \arrow[d] & \cdots & \vdots \arrow[d] \\
\bigoplus\limits_{|\delta|=p} \bigwedge^p \mathrm{T}^\star\delta \otimes \mathbf{F}^0(\underline{0}^\delta) \arrow[r, dashed] & \bigoplus\limits_{|\delta|=p+1} \bigwedge^p \mathrm{T}^\star\delta \otimes \mathbf{F}^0(\underline{0}^\delta) & \cdots & \bigoplus\limits_{|\delta|=d} \bigwedge^p \mathrm{T}^\star\delta \otimes \mathbf{F}^0(\underline{0}^\delta)
\end{tikzcd}$$

where

$${}_p\mathsf{C}_0^{a,b} = \mathrm{gr}^a_W C^{a+b}(X, \mathbf{F}^p) = \bigoplus_{\substack{\delta \in X \\ |\delta| = a+b}} \bigwedge^b \mathrm{T}^\star\delta \otimes \mathbf{F}^{p-b}(\underline{0}^\delta)$$

and the differentials in page zero, which are of bidegree $(0, 1)$, are given by Proposition 5.15. We call this the *tropical spectral sequence*. The zero-th page of this spectral sequence is given in Figure 2. The dashed arrows correspond to the maps of the first page. The explicit form of all these maps appear later in this section.

Before introducing the second spectral sequence, let us consider the $2p$-th row $\mathsf{ST}_1^{\bullet,2p}$ of the Steenbrink spectral sequence. This row can be decomposed into a double complex as follows. We define the double complex ${}_p\mathsf{St}^{\bullet,\bullet}$ by

$${}_p\mathsf{St}^{a,b} := \begin{cases} \bigoplus\limits_{\substack{\delta \in X_\mathfrak{f} \\ |\delta| = p+a-b}} H^{2b}(\delta) & \text{if } a \geqslant 0 \text{ and } b \leqslant p, \\ 0 & \text{otherwise,} \end{cases}$$

[Tropical Hodge theory and applications, Matthieu Piquerez' PhD - 2021]

Diagram chasing as invisible mathematics

for any $k \geqslant 1$. By HL, we also know that we have an isomorphism

$$0 \to H^{-1}(C^\bullet) \to H^1(D^\bullet) \to 0.$$

Gluing all these short exact sequences, we almost get the long exact sequences of the theorem. In fact, we directly get the long exact sequence in which all the degrees are odd integers, i.e., with k in the statement of the theorem is even. To see this, note that for a positive even integer k, we have

$$\cdots \to \underbrace{H^{-k-1}(K^\bullet)}_{0} \to H^{-k-1}(C^\bullet) \xrightarrow{L} H^{-k+1}(D^\bullet) \to H^{-k+1}(R^\bullet) \to \underbrace{H^{-k+1}(K^\bullet)}_{0} \to \cdots$$

$$\cdots \to \underbrace{H^{-1}(K^\bullet)}_{0} \to H^{-1}(C^\bullet) \xrightarrow{L} H^{1}(D^\bullet) \to \underbrace{H^{1}(R^\bullet)}_{0} \to \cdots$$

$$\cdots \to \underbrace{H^{k-1}(R^\bullet)}_{0} \to H^{k-1}(K^\bullet) \to H^{k-1}(C^\bullet) \xrightarrow{L} H^{k+1}(D^\bullet) \to \underbrace{H^{k+1}(R^\bullet)}_{0} \to H^{k-1}(K^\bullet) \to \cdots$$

which is exactly the above exact sequences, combined together.

For the other exact sequence in the theorem, i.e., when all the degrees are even, we can apply a similar argument as above to treats all the other cases and reduce to proving the exactness of the following six-term sequence

$$0 \to H^{-2}(C^\bullet) \to H^0(D^\bullet) \xrightarrow{\mathrm{d}^{-1}} H^0(R^\bullet) \xrightarrow{\mathrm{d}^0} H^0(K^\bullet) \xrightarrow{\mathrm{d}^1} H^0(C^\bullet) \to H^2(D^\bullet) \to 0. \quad (7.2)$$

The exactness of the beginning of this sequence is a consequence of (7.1) and the injectivity of $L\colon H^{-2}(C^\bullet) \to H^0(D^\bullet)$. By a symmetric argument, we infer the exactness of the end of the sequence. It thus remains to describe the central map d^0, and to prove the exactness of the sequence at other places, i.e., to show that $\mathrm{Im}(\mathrm{d}^{-1}) = \ker(\mathrm{d}^0)$ and $\mathrm{Im}(\mathrm{d}^0) = \ker(\mathrm{d}^1)$.

The end of the proof is essentially a diagram chasing. The definition of d^0 is given by the diagram depicted in Figure 6.

[Tropical Hodge theory and applications, Matthieu Piquerez' PhD - 2021]

Diagram chasing as invisible mathematics

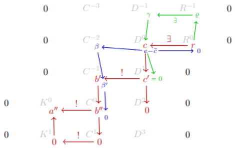


Figure 6. Definition of d^0 in the six-term exact sequence (7.2).

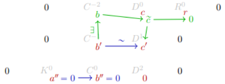


Figure 7. Proof of the inclusion $\ker(\mathrm{d}^0) \subseteq \mathrm{Im}(\mathrm{d}^{-1})$.

cocycle $\widetilde{b'} \in C^{-1}$ such that $L\mathrm{cl}(\widetilde{b'}) = \mathrm{cl}(c')$. In particular, there exists a coboundary $\widetilde{c'} \in D^1$ such that $L\widetilde{b'} = c' - \widetilde{c'}$. For the green part, we consider the element $b' - \widetilde{b'}$, and every green arrow is clear. Finally, we construct a cocycle r in R^0 such that $\mathrm{d}^0\mathrm{cl}(r) = \mathrm{cl}(a'')$.

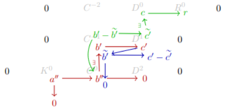
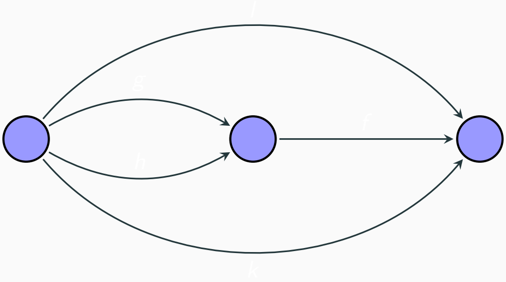


Figure 8. Proof of the inclusion $\ker(\mathrm{d}^1) \subseteq \mathrm{Im}(\mathrm{d}^0)$.

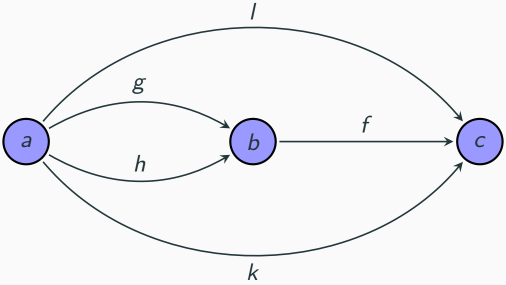
[Tropical Hodge theory and applications, Matthieu Piquerez' PhD - 2021]

Diagram chasing as invisible mathematics



f is a mono:

$$\forall g, \forall h, \quad g \circ f = h \circ f \Rightarrow g = h$$



f is a mono:

$$\forall g, \forall h, \quad g \circ f = h \circ f \Rightarrow g = h$$

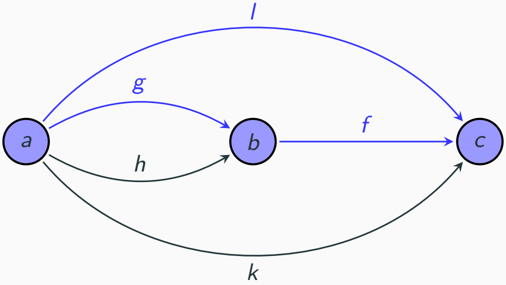


Diagram chasing as invisible mathematics

f is a mono:

$$\forall g, \forall h, \quad g \circ f = h \circ f \Rightarrow g = h$$

$$\begin{tikzcd}
a \arrow[r, bend left, "g"] \arrow[r, bend right, "h"'] \arrow[rr, bend left=50, "g \circ f"] \arrow[rr, bend right=50, "k"'] & b \arrow[r, "f"] & c
\end{tikzcd}$$

Diagram chasing as invisible mathematics

f is a mono:

$$\forall g, \forall h, \quad g \circ f = h \circ f \Rightarrow g = h$$

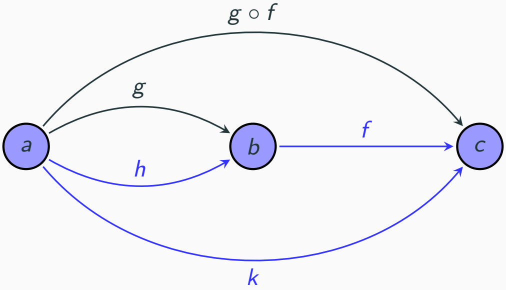


Diagram chasing as invisible mathematics

f is a mono:

$$\forall g, \forall h, \quad g \circ f = h \circ f \Rightarrow g = h$$

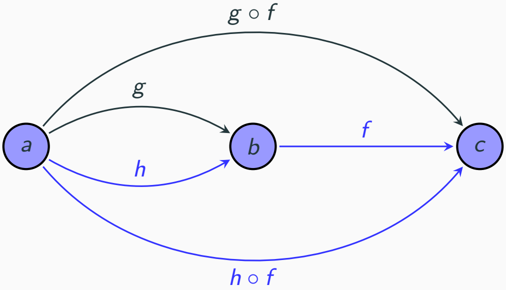


Diagram chasing as invisible mathematics

f is a mono:

$$\forall g, \forall h, \quad g \circ f = h \circ f \Rightarrow g = h$$

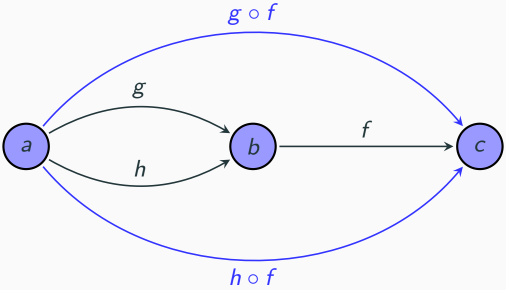


Diagram chasing as invisible mathematics

f is a mono:

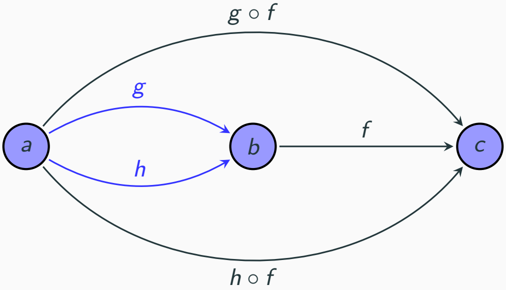
$$\forall g, \forall h, \quad g \circ f = h \circ f \Rightarrow g = h$$

$$\begin{tikzcd}
a \arrow[r, bend left, "g"] \arrow[r, bend right, "h"'] \arrow[rr, bend left=60, "g \circ f"] \arrow[rr, bend right=60, "h \circ f"'] & b \arrow[r, "f"] & c
\end{tikzcd}$$

Diagram chasing as invisible mathematics

f is a mono:

$$\forall g, \forall h, \quad g \circ f = h \circ f \Rightarrow g = h$$

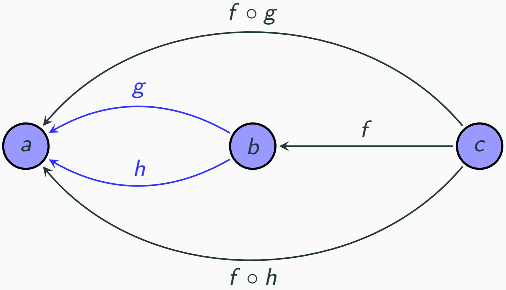


[Recently, Master theses of Markus Himmel (2020), Yannis Monbru (2022)]

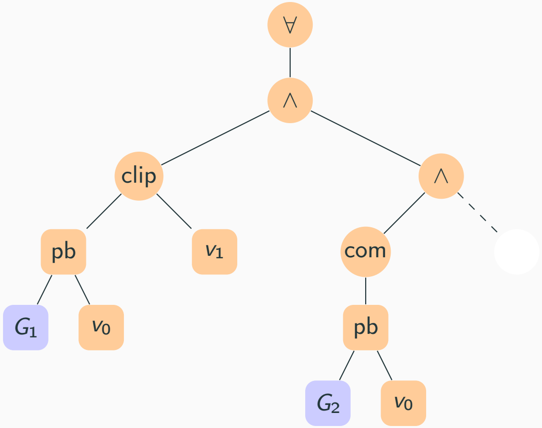
Diagram chasing as invisible mathematics

f is an epi:

$$\forall g, \forall h, \quad f \circ g = f \circ h \Rightarrow g = h$$

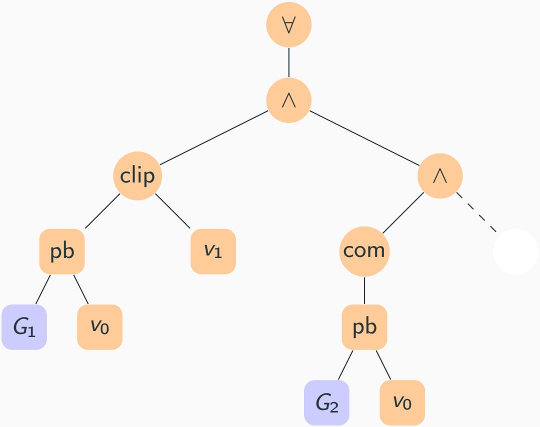


Formal(ized) abstract nonsense



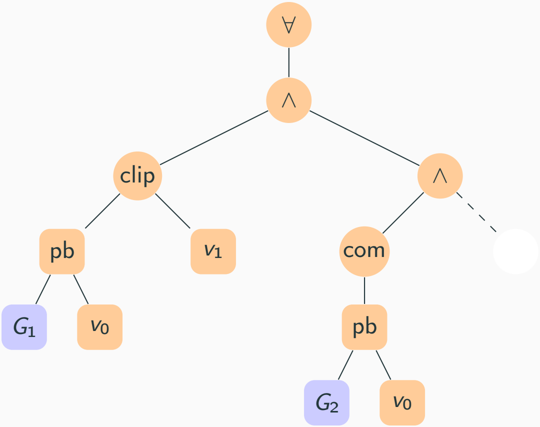
[Joint work in progress with Matthieu Piquerey]

Formal(ized) abstract nonsense



$[e]_{\mathcal{A}}$ is a predicate on diagrams.

Formal(ized) abstract nonsense



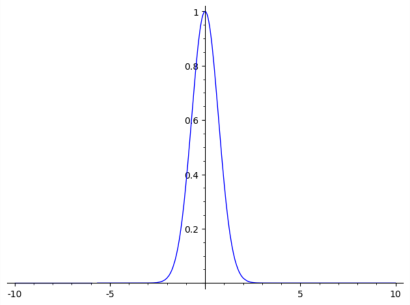
$[e]_{\mathcal{A}}$ is a predicate on diagrams.

Duality theorem:

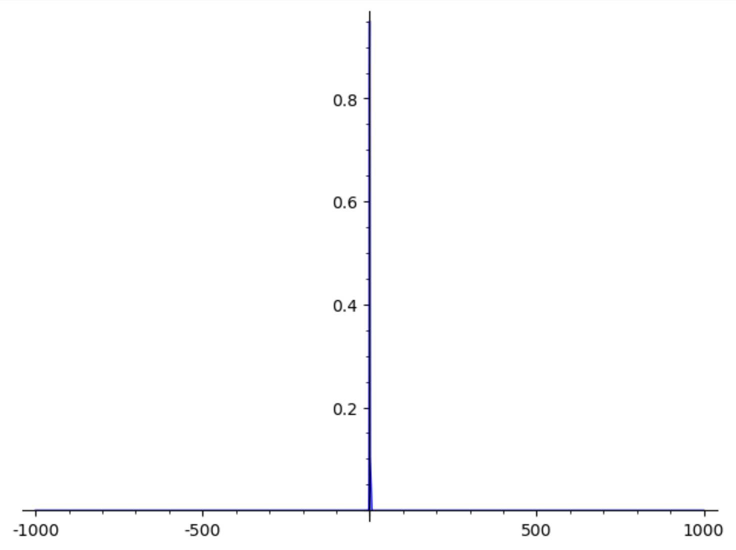
$$\forall e, \forall I, \quad [e]_{\mathcal{A},I} \Rightarrow [\text{dual } e]_{\mathcal{A},I}$$

[Joint work in progress with Matthieu Piquerey]

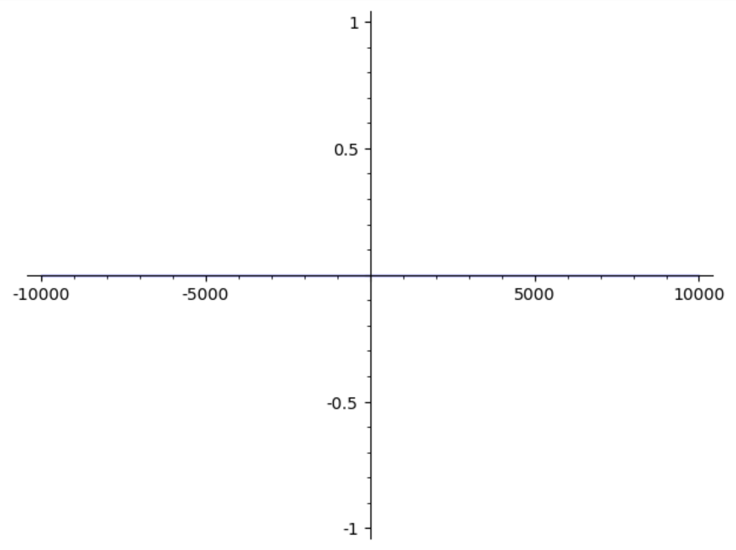
Plotting $exp(-x^2)$ with sagemath



Plotting $exp(-x^2)$ with sagemath

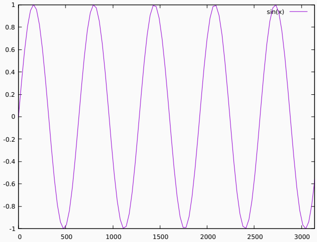


Plotting $exp(-x^2)$ with sagemath



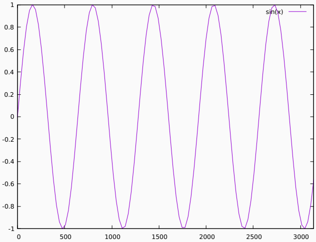
Plotting $sin(x)$ for $x \in [0, 3141]$

Plotting $sin(x)$ for $x \in [0, 3141]$

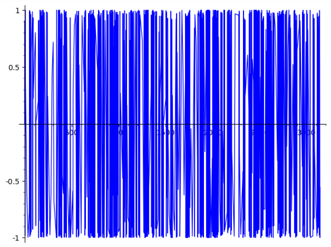


Gnuplot

Plotting $sin(x)$ for $x \in [0, 3141]$



Gnuplot



Sagemath

Faithful plotting is hard

Issues:

- Sampling
- Accuracy
- Bugs

Faithful plotting is hard

Issues:

- Sampling
- Accuracy
- Bugs

Desired properties:

- Correctness: blank pixels are not traversed by the function graph
- Completeness: filled pixels are traversed by the function graph

Faithful plotting is hard

Issues:

- Sampling
- Accuracy
- Bugs

Desired properties:

- Correctness: blank pixels are not traversed by the function graph
- Completeness: filled pixels are traversed by the function graph

$\Rightarrow$ Formally verified plots: guarantee correctness and strive for completeness

Generating formally verified plots

To obtain a verified plot for $f(x)$ for $x \in X$:

- Partition X in $(X_i)_{i=1\ldots n}$
- Produce a list $(\ell_i)_{i=1\ldots n}$ of intervals
- Ensure (with a formal proof) that for every $i = 1 \ldots n$:

$$\forall x \in X_i, f(x) \in \ell_i$$

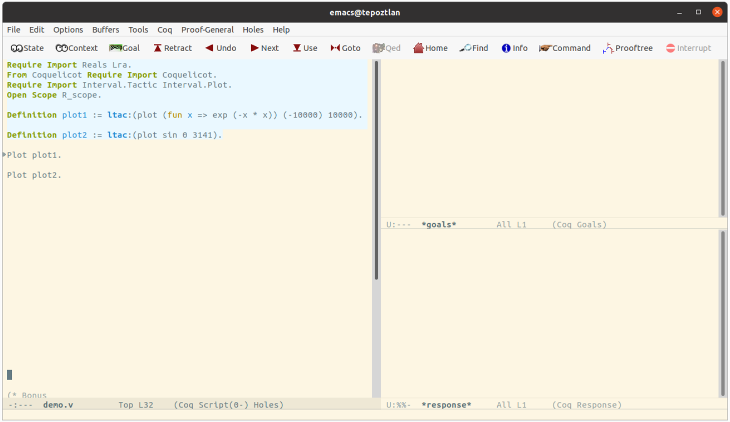
- Fill the corresponding pixels.

Rigorous polynomial approximation make computations efficient enough.

[Plotting in a formally verified way, G. Melquiond, F-IDE 2021]

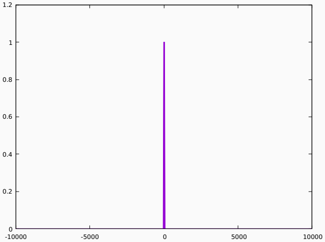
.

Demo



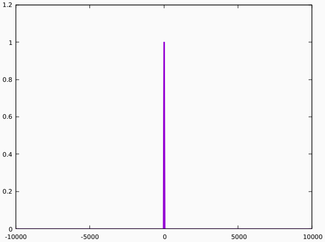
emacs@tepoztlan
File Edit Options Buffers Tools Coq Proof-General Holes Help
State Context Goal Retract Undo Next Use Goto Qed Home Find Info Command Prooftree Interrupt
Require Import Reals Lra.
From Coquelicot Require Import Coquelicot.
Require Import Interval.Tactic Interval.Plot.
Open Scope R_scope.
Definition plot1 := ltac:(plot (fun x => exp (-x * x)) (-10000) 10000).
Definition plot2 := ltac:(plot sin 0 3141).
Plot plot1.
Plot plot2.
(* Bonus
-:--- demo.v Top L32 (Coq Script(0-) Holes)
U:--- *goals* All L1 (Coq Goals)
U:%%- *response* All L1 (Coq Response)

Demo

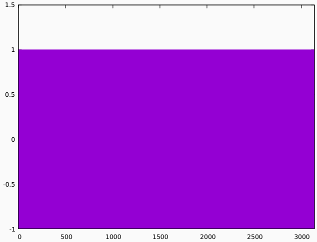


Verified plot of $exp(-x^2)$ for $x \in [-10000, 10000]$

Demo



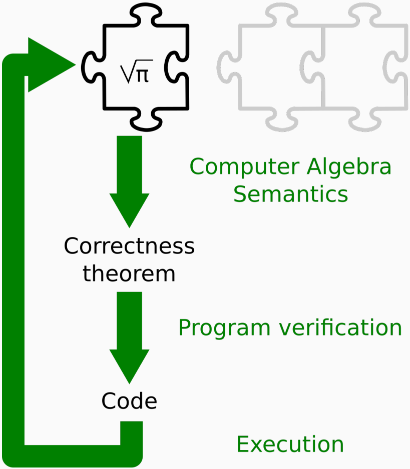
Verified plot of $exp(-x^2)$ for $x \in [-10000, 10000]$



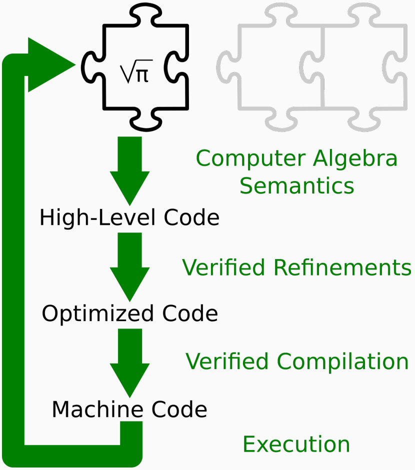
Verified plot of $sin(x)$ for $x \in [0, 3141]$

Conclusions

Doing mathematics by computer



Doing mathematics by computer



Agenda

- Blur the fronteer between environments for experimenting and for proving
- Expand the computational skills of proof assistants