Mathématiques assistées par ordinateur

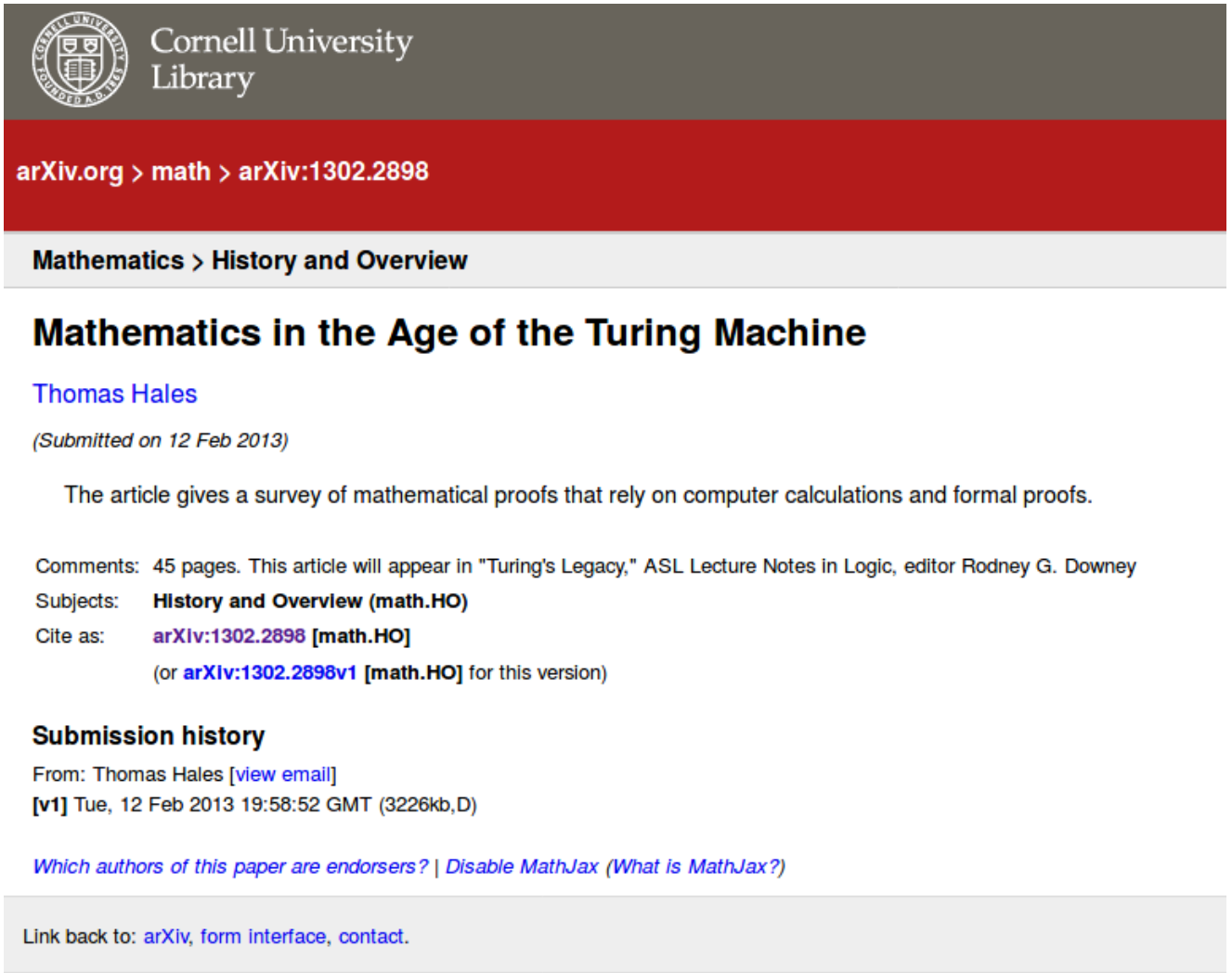
Assia Mahboubi

Mathématique(s)

Ce que se propose pour but essentiel l'axiomatique, c'est précisément ce que le formalisme logique, à lui seul, est incapable de fournir, l'intelligibilité profonde des mathématiques.

Nicolas Bourbaki, L'architecture des mathématiques, 1948

Observation et expérimentation



Cornell University Library

arXiv.org > math > arXiv:1302.2898

Mathematics > History and Overview

Mathematics in the Age of the Turing Machine

Thomas Hales

(Submitted on 12 Feb 2013)

The article gives a survey of mathematical proofs that rely on computer calculations and formal proofs.

Comments: 45 pages. This article will appear in "Turing's Legacy," ASL Lecture Notes in Logic, editor Rodney G. Downey

Subjects: **History and Overview (math.HO)**

Cite as: **arXiv:1302.2898 [math.HO]**

(or **arXiv:1302.2898v1 [math.HO]** for this version)

Submission history

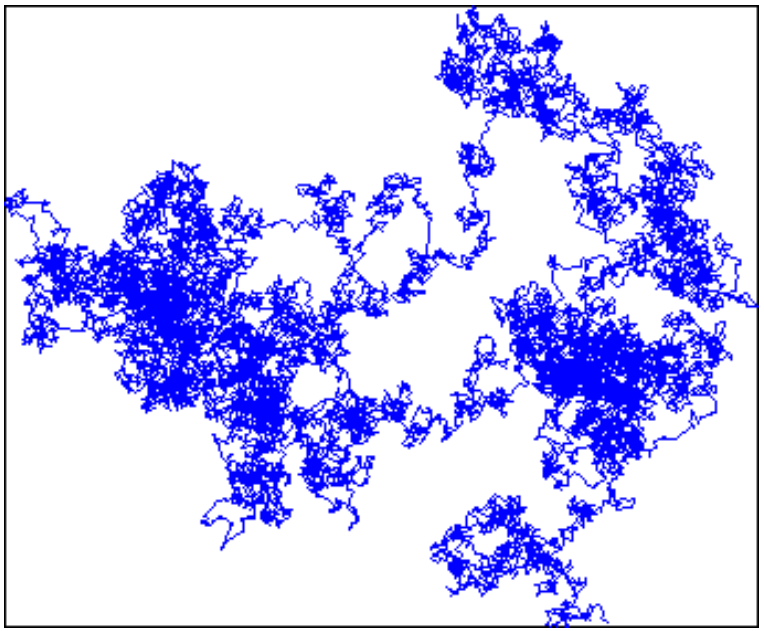
From: Thomas Hales [view email]

[v1] Tue, 12 Feb 2013 19:58:52 GMT (3226kb,D)

Which authors of this paper are endorsers? | Disable MathJax (What is MathJax?)

Link back to: arXiv, form interface, contact.

Observation et expérimentation



"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

Observation et expérimentation

CMI

ABOUT PROGRAMS MILLENNIUM PROBLEMS PEOPLE PUBLICATIONS EVEN

Birch and Swinnerton-Dyer Conjecture

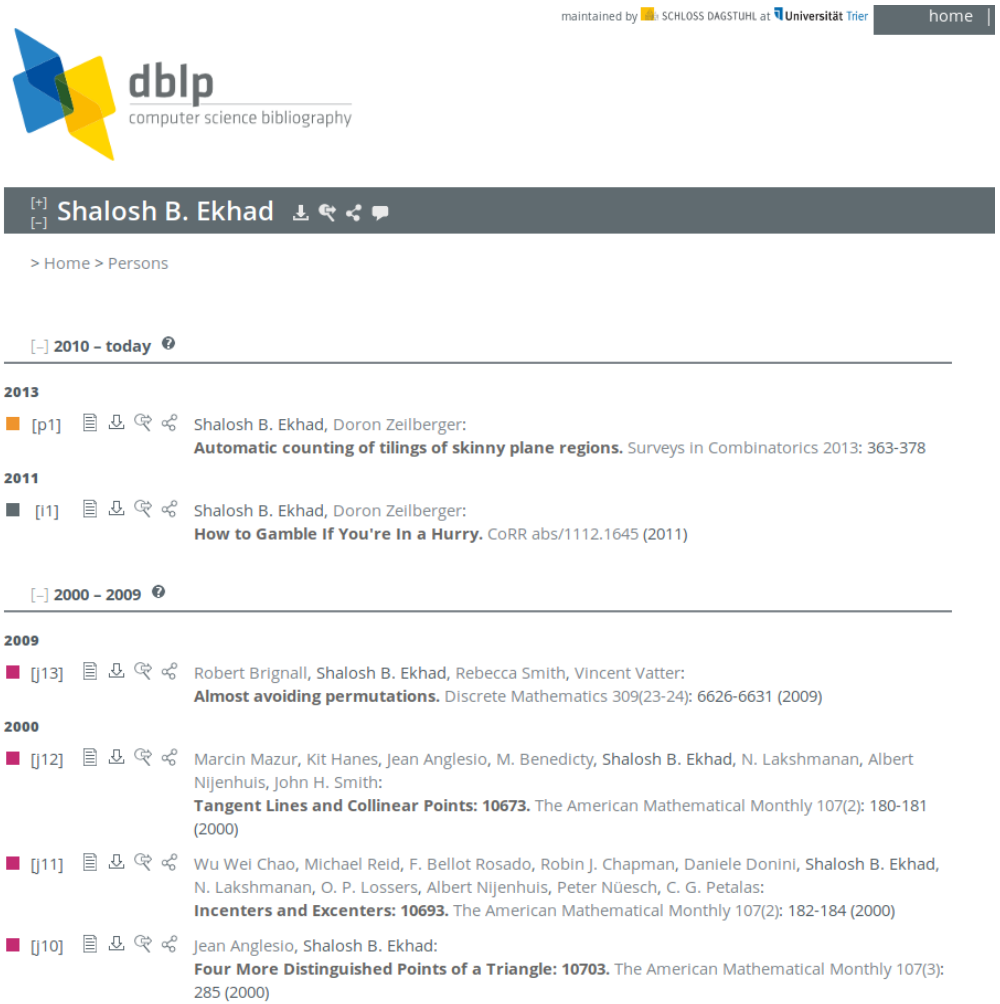
Mathematicians have always been fascinated by the problem of describing all solutions in whole numbers x,y,z to algebraic equations like

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

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

Preuve par calcul



maintained by SCHLOSS DAGSTUHL at Universität Trier home |

dblp
computer science bibliography

[+] [−] Shalosh B. Ekhad

> Home > Persons

[−] 2010 – today

2013

[p1] Shalosh B. Ekhad, Doron Zeilberger:
Automatic counting of tilings of skinny plane regions. Surveys in Combinatorics 2013: 363-378

2011

[I1] Shalosh B. Ekhad, Doron Zeilberger:
How to Gamble If You're In a Hurry. CoRR abs/1112.1645 (2011)

[−] 2000 – 2009

2009

[j13] Robert Brignall, Shalosh B. Ekhad, Rebecca Smith, Vincent Vatter:
Almost avoiding permutations. Discrete Mathematics 309(23-24): 6626-6631 (2009)

2000

[j12] Marcin Mazur, Kit Hanes, Jean Anglesio, M. Benedicty, Shalosh B. Ekhad, N. Lakshmanan, Albert Nijenhuis, John H. Smith:
Tangent Lines and Collinear Points: 10673. The American Mathematical Monthly 107(2): 180-181 (2000)

[j11] Wu Wei Chao, Michael Reid, F. Bellot Rosado, Robin J. Chapman, Daniele Donini, Shalosh B. Ekhad, N. Lakshmanan, O. P. Lossers, Albert Nijenhuis, Peter Nüesch, C. G. Petalas:
Incenters and Excenters: 10693. The American Mathematical Monthly 107(2): 182-184 (2000)

[j10] Jean Anglesio, Shalosh B. Ekhad:
Four More Distinguished Points of a Triangle: 10703. The American Mathematical Monthly 107(3): 285 (2000)

Conjecture faible de Goldbach

Tout nombre impair ≥ 9 est la somme
de trois nombres premiers impairs.

Conjecture faible de Goldbach

Minor arcs for Goldbach's problem

H. A. Helfgott

(Submitted on 23 May 2012 (v1), last revised 30 Dec 2013 (this version, v4))

The ternary Goldbach conjecture states that every odd number n>=7 is the sum of three primes. The estimation of sums of the form \sum_{p\leq x} e(\alpha p), \alpha = a/q + O(1/q^2), has been a central part of the main approach to the conjecture since (Vinogradov, 1937). Previous work required q or x to be too large to make a proof of the conjecture for all n feasible.
The present paper gives new bounds on minor arcs and the tails of major arcs. This is part of the author's proof of the ternary Goldbach conjecture.
The new bounds are due to several qualitative improvements. In particular, this paper presents a general method for reducing the cost of Vaughan's identity, as well as a way to exploit the tails of minor arcs in the context of the large sieve.

Comments: 79 pages; third version. (A couple of explanatory paragraphs have been added.)

Major arcs for Goldbach's problem

H. A. Helfgott

(Submitted on 13 May 2013 (v1), last revised 14 Apr 2014 (this version, v4))

The ternary Goldbach conjecture states that every odd number $n \geq 7$ is the sum of three primes. The estimation of the Fourier series $\sum_{p \leq x} e(\alpha p)$ and related sums has been central to the study of the problem since Hardy and Littlewood (1923). Here we show how to estimate such Fourier series for α in the so-called major arcs, i.e., for α close to a rational of small denominator. This is part of the author's proof of the ternary Goldbach conjecture. In contrast to most previous work on the subject, we will rely on a finite verification of the Generalized Riemann Hypothesis up to a bounded conductor and bounded height, rather than on zero-free regions. We apply a rigorous verification due to D. Platt; the results we obtain are both rigorous and unconditional. The main point of the paper will be the development of estimates on parabolic cylinder functions that make it possible to use smoothing functions based on the Gaussian. The generality of our explicit formulas will allow us to work with a wide variety of such functions.

Numerical Verification of the Ternary Goldbach Conjecture up to 8.875e30

H.A. Helfgott, David J. Platt

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

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

Calculs d'intégrales

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),

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

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].

Calculs d'intégrales

Rigorous numerical integration

9

2

I need to evaluate some (one-variable) integrals that neither SAGE nor Mathematica can do symbolically. As far as I can tell, I have two options:

(a) Use GSL (via SAGE), Maxima or Mathematica to do numerical integration. This is really a non-option, since, if I understand correctly, the "error bound" they give is not really a guarantee.

(b) Cobble together my own programs using the trapezoidal rule, Simpson's rule, etc., and get rigorous error bounds using bounds I have for the second (or fourth, or what have you) derivative of the function I am integrating. This is what I have been doing.

Is there a third option? Is there standard software that does (b) for me?

na.numerical-analysis

share cite improve this question

asked Mar 5 '13 at 23:03

H A Helfgott

3,620 ● 21 ● 69

Calculs d'intégrales

$$\int_{\pi}^{+\infty} \frac{1 + \left(\frac{0.5 \cdot \ln(1+2.25/\tau^2)+4.1396+\ln \pi}{\ln \tau}\right)^2}{1 + 0.25/\tau^2} \cdot \frac{\ln^2 \tau}{\tau^2}\, d\tau$$

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

Calculs d'intégrales

$$m \leq \int_{\pi}^{+\infty} \frac{1 + \left(\frac{0.5 \cdot \ln(1+2.25/\tau^2)+4.1396+\ln \pi}{\ln \tau}\right)^2}{1 + 0.25/\tau^2} \cdot \frac{\ln^2 \tau}{\tau^2} \, d\tau \leq M$$

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

$\mathbb{R}, \mathbb{F}, \mathbb{I}$

- $\mathbb{R}$: corps des nombres réels;

$\mathbb{R}, \mathbb{F}, \mathbb{I}$

- $\mathbb{R}$: corps des nombres réels;
- $\mathbb{F}$: arithmétique flottante, support du calcul en machine;

$\mathbb{R}, \mathbb{F}, \mathbb{I}$

- $\mathbb{R}$: corps des nombres réels;
- $\mathbb{F}$: arithmétique flottante, support du calcul en machine;
- $\mathbb{I}$: arithmétique d'intervalle, support du calcul rigoureux.

[Coquelicot: a user-friendly library of real analysis for Coq - S. Boldo and C. Lelay, G. Melquiond; MSCS, vol 9.1 2015]
[Flocq: A Unified Library for Proving Floating-Point Algorithms in Coq - S. Boldo, G. Melquiond, Proc. of ARITH'11]

[Proving bounds on real-valued functions with computations - G. Melquiond, Proc. of IJCAR 2008]

Catalogue de fonctions univariées

Décrit par des arbres de syntaxe abstraite:

$$
\begin{array}{rcl}
\mathcal{E} & := & x \mid \mathbb{F} \mid \pi \mid \\
& & \mathcal{E} + \mathcal{E} \mid \mathcal{E} - \mathcal{E} \mid \mathcal{E} \times \mathcal{E} \mid \mathcal{E} \div \mathcal{E} \mid -\mathcal{E} \mid \|\mathcal{E}\| \mid \\
& & \sqrt{\mathcal{E}} \mid \mathcal{E}^k \mid \\
& & \cos(\mathcal{E}) \mid \sin(\mathcal{E}) \mid \tan(\mathcal{E}) \mid \operatorname{atan}(\mathcal{E}) \mid \\
& & \exp(\mathcal{E}) \mid \ln(\mathcal{E})
\end{array}
$$

Interprétation des expressions

Comme fonctions d'une variable réelle:

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

Interprétation des expressions

Comme fonctions d'une variable réelle:

- $[e]_{\mathbb{R}} : \mathbb{R} \to \mathbb{R}$
  $[x]_{\mathbb{R}} \simeq x \mapsto x$

Interprétation des expressions

Comme fonctions d'une variable réelle:

- $$\begin{array}{lcl} [e]_{\mathbb{R}} & : & \mathbb{R} \to \mathbb{R} \\ [x]_{\mathbb{R}} & \simeq & x \mapsto x \\ [\pi + cos(x)]_{\mathbb{R}} & \simeq & x \mapsto \pi + cos(x) \end{array}$$

Interprétation des expressions

Comme fonctions d'une variable intervalle:

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

Interprétation des expressions

Comme fonctions d'une variable intervalle:

- $[e]_{\mathbb{I}} : \mathbb{I} \to \mathbb{I}$
  $[x]_{\mathbb{I}} \simeq \mathbf{x} \mapsto \mathbf{x}$

Interprétation des expressions

Comme fonctions d'une variable intervalle:

- $$\begin{array}{lcl} [e]_{\mathbb{I}} & : & \mathbb{I} \to \mathbb{I} \\ [x]_{\mathbb{I}} & \simeq & \mathbf{x} \mapsto \mathbf{x} \\ [\pi + cos(x)]_{\mathbb{I}} & \simeq & \mathbf{x} \mapsto \boldsymbol{\pi} + \mathbf{cos}(\mathbf{x}) \end{array}$$

Spécification

En fait, on a besoin d'une valeur exceptionnelle $\perp$:

- $[e]_{\mathbb{R}_\perp} \quad : \quad \mathbb{R}_\perp \to \mathbb{R}_\perp$
- $[e]_{\mathbb{I}_\perp} \quad : \quad \mathbb{I}_\perp \to \mathbb{I}_\perp$

Spécification

En fait, on a besoin d'une valeur exceptionnelle $\perp$:

- $[e]_{\mathbb{R}_\perp} \quad : \quad \mathbb{R}_\perp \to \mathbb{R}_\perp$
- $[e]_{\mathbb{I}_\perp} \quad : \quad \mathbb{I}_\perp \to \mathbb{I}_\perp$

Théorème de correction des extensions par intervalles:

Spécification

En fait, on a besoin d'une valeur exceptionnelle $\perp$:

- $[e]_{\mathbb{R}_\perp} \quad : \quad \mathbb{R}_\perp \to \mathbb{R}_\perp$
- $[e]_{\mathbb{I}_\perp} \quad : \quad \mathbb{I}_\perp \to \mathbb{I}_\perp$

Théorème de correction des extensions par intervalles:

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

Approximation formellement vérifiée

Problème initial:

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

Approximation formellement vérifiée

Entrée dans le catalogue:

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

Approximation formellement vérifiée

Calcul vérifié:

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

Approximation formellement vérifiée

Calcul vérifié:

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

Approximation formellement vérifiée

Calcul vérifié:

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

Exemple

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

Exemple

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

Mai 2016:

- Octave: `quad`/`quadgk`: seulement 10/9 chiffres corrects;

Exemple

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

Mai 2016:

- Octave: `quad`/`quadgk`: seulement 10/9 chiffres corrects;
- INTLAB `verifyquad`: réponse fausse, sans avertissement;

Exemple

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

Mai 2016:

- Octave: `quad`/`quadgk`: seulement 10/9 chiffres corrects;
- INTLAB `verifyquad`: réponse fausse, sans avertissement;
- VNODE-LP: inutilisable (cf. valeur absolue).

Exemple

$$\int_{100000}^{+\infty} \frac{1+\left(\frac{0.5\cdot\ln(1+2.25/\tau^2)+4.1396+\ln\pi}{\ln\tau}\right)^2}{1+0.25/\tau^2}\cdot\frac{\ln^2\tau}{\tau^2}\,d\tau \simeq -3.2555895745\cdot 10^{-6}$$

Error	Time	Accuracy	Degree	Depth	Precision
10^{-3}	0.6	2	3	0	30
10^{-4}	0.8	5	5	2	30
10^{-5}	1.5	8	7	6	30
10^{-6}	3.1	11	9	11	30
10^{-7}	5.6	15	12	12	30
10^{-8}	11.2	18	15	15	30

Ainsi:

$$\int_{-\infty}^{+\infty} \frac{1+\left(\frac{0.5\cdot\ln(1+2.25/\tau^2)+4.1396+\ln\pi}{\ln\tau}\right)^2}{1+0.25/\tau^2}\cdot\frac{\ln^2\tau}{\tau^2}\,d\tau \in [226.849; 226.850]$$

Exemple

$$\int_{100000}^{+\infty} \frac{1+\left(\frac{0.5\cdot\ln(1+2.25/\tau^2)+4.1396+\ln\pi}{\ln\tau}\right)^2}{1+0.25/\tau^2}\cdot\frac{\ln^2\tau}{\tau^2}\,d\tau \simeq -3.2555895745\cdot 10^{-6}$$

Error	Time	Accuracy	Degree	Depth	Precision
10^{-3}	0.6	2	3	0	30
10^{-4}	0.8	5	5	2	30
10^{-5}	1.5	8	7	6	30
10^{-6}	3.1	11	9	11	30
10^{-7}	5.6	15	12	12	30
10^{-8}	11.2	18	15	15	30

Ainsi:

$$\int_{-\infty}^{+\infty} \frac{1+\left(\frac{0.5\cdot\ln(1+2.25/\tau^2)+4.1396+\ln\pi}{\ln\tau}\right)^2}{1+0.25/\tau^2}\cdot\frac{\ln^2\tau}{\tau^2}\,d\tau \in [226.849; 226.850]$$

La borne 226.844 donnée dans le preprint est incorrecte.

Polysémie: cosinus

$$\sum_{n=0}^{+\infty} (-1)^n \frac{x^{2n}}{(2n)!}$$

Polysémie: cosinus

```
#include "acb.h"

void
acb_sin_cos(acb_t s, acb_t c,
       const acb_t z, slong
      prec)
{
#define a acb_realref(z)
#define b acb_imagref(z)
    if (arb_is_zero(b))
    {
        arb_sin_cos(
              acb_realref(s),
              acb_realref(c),
              a, prec);
        arb_zero(acb_imagref(s
              ));
        arb_zero(acb_imagref(c
              ));
    }
    else if (arb_is_zero(a))
    {
      arb_sinh_cosh(
            acb_imagref(s),
            acb_realref(c),
            b, prec);
      arb_zero(acb_realref(s
            ));
      arb_zero(acb_imagref(c
            ));
    }
  else
    {
      arb_t sa, ca, sb, cb;

      arb_init(sa);
      arb_init(ca);
      arb_init(sb);
      arb_init(cb);
      arb_sin_cos(sa, ca, a,
            prec);
      arb_sinh_cosh(sb, cb, b,
            prec);

      arb_mul(acb_realref(s), sa
            , cb, prec);
      arb_mul(acb_imagref(s), sb
            , ca, prec);


      arb_mul(acb_realref(c), ca
            , cb, prec);
      arb_mul(acb_imagref(c), sa
            , sb, prec);
      arb_neg(acb_imagref(c),
            acb_imagref(c));

      arb_clear(sa);
      arb_clear(ca);
      arb_clear(sb);
      arb_clear(cb);
      }
#undef a
#undef b
```

[Arb - a C library for arbitrary-precision ball arithmetic, v2.15, Fredrik Johansson]

Polysémie: cosinus

$$\begin{cases} f'' + f = 0 \\ f(0) = 1 \end{cases}$$

Linear Differential Equations as a Data-Structure, B. Salvy, 2018, arXiv:1811.08616

Structure de groupe (fini)

Un groupe (fini) est:

- Un ensemble (fini) : G;
- Une loi binaire: $g * h$;
- Un élément neutre: 1;

tel que:

- La loi de groupe est associative:
- Tout élément $g \in G$ a un inverse g^{-1}.

Rubik

Structure

```
Record mixin_of (T : Type) : Type := BaseMixin {
  mul : T -> T -> T;
  one : T;
  inv : T -> T;
  _ : associative mul;
  _ : left_id one mul;
  _ : involutive inv;
  _ : {morph inv : x y / mul x y >-> mul y x}
}.
```

Structure

```
Record mixin_of (T : Type) : Type := BaseMixin {
  mul : T -> T -> T;
  one : T;
  inv : T -> T;
  _ : associative mul;
  _ : left_id one mul;
  _ : involutive inv;
  _ : {morph inv : x y / mul x y >-> mul y x}
}.

Structure base_type : Type := PackBase {
  sort : Type;
   _ : mixin_of sort;
   _ : Finite.class_of sort
}.
```

Figure de style

Un groupe (fini) est:

- Un ensemble (fini) : G;
- Une loi binaire: $g * h$;
- Un élément neutre: 1;

tel que:

- La loi de groupe est associative:
- Tout élément $g \in G$ a un inverse g^{-1}.

Par abus de notation,

Figure de style

Un groupe (fini) est:

- Un ensemble (fini) : G;
- Une loi binaire: $g * h$;
- Un élément neutre: 1;

tel que:

- La loi de groupe est associative:
- Tout élément $g \in G$ a un inverse g^{-1}.

Par abus de notation, on pourra écrire:
"soit G un groupe tel que pour tout $g \in G, g * g = 1$".

Synecdoque, ou coercion

```
Fact cardG_gt0 gT (G : {group gT}) : 0 < #| G|.
```

Synecdoque, ou coercion

```
Fact cardG_gt0 gT (G : {group gT}) : 0 < #| G|.
```

avec:

```
#| _ | : {finset gT} -> nat
```

Synecdoque, ou coercion

```
Fact cardG_gt0 gT (G : {group gT}) : 0 < #| gset G|.
```

avec:

```
#| _ | : {finset gT} -> nat
```

Synecdoque, ou coercion

```
Fact cardG_gt0 gT (G : {group gT}) : 0 < #| gset G|.
```

avec:

```
#| _ | : {finset gT} -> nat
```

et

```
gset : {group gT} -> {finset gT}
```

Synecdoque, ou coercion

```
Fact cardG_gt0 gT (G : {group gT}) : 0 < #| G|.
```

Sous-groupes

Soit $\mathbf{H}, \mathbf{K}$ sont des sous-groupes d'un groupe $\mathcal{G}$:

$$\mathbf{H} \cap \mathbf{K} \quad \mathbf{N}(\mathbf{H}) \quad \mathbf{Z}(\mathbf{H}) \quad \ldots \text{ sont des groupes.}$$

Sous-groupes

Soit $\mathbf{H}, \mathbf{K}$ sont des sous-groupes d'un groupe $\mathcal{G}$:

$$\mathbf{H} \cap \mathbf{K} \quad \mathbf{N}(\mathbf{H}) \quad \mathbf{Z}(\mathbf{H}) \quad \ldots \text{ sont des groupes.}$$

En particulier:
$\mathbf{H} \cap \mathbf{K}$ est un groupe d'ensemble sous-jacent $H \cap K$;

Sous-groupes

Soit $\mathbf{H}, \mathbf{K}$ sont des sous-groupes d'un groupe $\mathcal{G}$:

$$\mathbf{H} \cap \mathbf{K} \quad \mathbf{N}(\mathbf{H}) \quad \mathbf{Z}(\mathbf{H}) \quad \ldots \text{ sont des groupes.}$$

En particulier:
$\mathbf{H} \cap \mathbf{K}$ est un groupe d'ensemble sous-jacent $H \cap K$;
$\mathbf{N(G)}$ est un groupe d'ensemble sous-jacent $N(G)$;
...

Exemple

L'énoncé précédent:

```
Fact cardG_gt0 gT (G : {group gT}) : 0 < #| G|.
```

Exemple

L'énoncé précédent:

```
Fact cardG_gt0 gT (G : {group gT}) : 0 < #| G|.
```

doit pouvoir servir à montrer que:

```
  gT : finGroupType
   K : {group gT}
   H : {group gT}
  ==================
   0 < #|H ∩ N(K)|
```

Unification

```
  a : nat
  b : nat
  H : forall x y : nat, impair (2 * x + y * 2)
============================================
    impair (2 * (17 + a * b) + 6 * 2)
```

Unification

```
  a : nat
  b : nat
  H : forall x y : nat, impair (2 * x + y * 2)
 ============================================
    impair (2 * (17 + a * b) + 6 * 2)
```

```
apply H.
```

Unification

```
  a : nat
  b : nat
  H : forall x y : nat, impair (2 * x + y * 2)
 ============================================
    impair (2 * (17 + a * b) + 6 * 2)
```

```
apply H.
```

```
     impair 2 * ?x + ?y * 2    ≡    impair (2 * (17 + a * b)+ 6 * 2)
```

Unification

```
  a : nat
  b : nat
  H : forall x y : nat, impair (2 * x + y * 2)
 ============================================
    impair (2 * (17 + a * b) + 6 * 2)
```

```
apply H.
```

```
     impair 2 * ?x + ?y * 2    ≡    impair (2 * (17 + a * b)+ 6 * 2)
```

Solution:

```
?x    ≡    17 + a * b
?y    ≡    6
```

Ce procédé ne s'occupe bien sûr du sens, ni du nom du prédicat `impair`.

Unification?

L'énoncé précédent:

```
Fact cardG_gt0 gT (G : {group gT}) : 0 < #| G|.
```

doit pouvoir servir à montrer que:

```
  gT : finGroupType
   K : {group gT}
   H : {group gT}
  ==================
   0 < #|H ∩ N(K)|
```

Unification?

L'énoncé précédent:

```
Fact cardG_gt0 gT (G : {group gT}) : 0 < #|gset G|.
```

doit pouvoir servir à montrer que:

```
  gT : finGroupType
   K : {group gT}
   H : {group gT}
  ================
   0 < #|gset H ∩ N(gset K)|
```

Unification?

L'énoncé précédent:

```
Fact cardG_gt0 gT (G : {group gT}) : 0 < #|gset G|.
```

doit pouvoir servir à montrer que:

```
  gT : finGroupType
   K : {group gT}
   H : {group gT}
  ================
   0 < #|gset H ∩ N(gset K)|
```

On doit résoudre:

```
gset ?G ≡ (gset H) ∩ N(gset K)
```

Inférence

- On doit résoudre:

  `gset ?G` $\equiv$ `(gset H)` $\cap$ `N(gset K)`

Inférence

- On doit résoudre:

  `gset ?G` $\equiv$ `(gset H)` $\cap$ `N(gset K)`

- Mais il n'y a en général pas de solution pour:

  `gset ?X` $\equiv$ `A1` $\cap$ `A2`

Inférence

- On doit résoudre:

  `gset ?G` $\equiv$ `(gset H)` $\cap$ `N(gset K)`

- Mais il n'y a en général pas de solution pour:

  `gset ?X` $\equiv$ `A1` $\cap$ `A2`

- Sauf si A_1 et A_2 sont munis d'une structure de groupe: c'est la construction précédemment notée $\mathbf{A_1} \cap \mathbf{A_2}$.

Inférence

- On doit résoudre:

  `gset ?G ≡ (gset H) ∩ N(gset K)`

- Mais il n'y a en général pas de solution pour:

  `gset ?X ≡ A1 ∩ A2`

- Sauf si A_1 et A_2 sont munis d'une structure de groupe: c'est la construction précédemment notée $\mathbf{A_1} \cap \mathbf{A_2}$.

  ```
  gset ?X ≡ (gset A1) ∩ (gset A2)
  ?X ≡ A1 ∩ A2
  ```

Inférence

- On doit résoudre:

```
gset ?G ≡ (gset H) ∩ N(gset K)
```

- Mais il n'y a en général pas de solution pour:

```
gset ?X ≡ A1 ∩ A2
```

- Sauf si A_1 et A_2 sont munis d'une structure de groupe: c'est la construction précédemment notée $\mathbf{A_1} \cap \mathbf{A_2}$.

```
gset ?X ≡ (gset A1) ∩ (gset A2)
?X ≡ A1 ∩ A2
```

- On doit donc résoudre:

```
gset ?G ≡ (gset H) ∩ N(gset K)
gset (H ∩ ?G2) ≡ (gset H) ∩ N(gset K)
gset ?G2 ≡ N(gset K)
```

Inférence

- On doit résoudre:

  `gset ?G2` $\equiv$ `N(gset K)`

Inférence

- On doit résoudre:

  `gset ?G2` $\equiv$ `N(gset K)`

- Mais il n'y a pas a priori de solution pour:

  `gset ?X` $\equiv$ `N(A)`

Inférence

- On doit résoudre:

  `gset ?G2` $\equiv$ `N(gset K)`

- Mais il n'y a pas a priori de solution pour:

  `gset ?X` $\equiv$ `N(A)`

- En fait, $N(A)$ est toujours muni d'une structure de groupe: c'est la construction $\mathbf{N}(\mathbf{A})$.

Inférence

- On doit résoudre:

```
gset ?G2 ≡ N(gset K)
```

- Mais il n'y a pas a priori de solution pour:

```
gset ?X ≡ N(A)
```

- En fait, $N(A)$ est toujours muni d'une structure de groupe: c'est la construction $\mathbf{N}(\mathbf{A})$.

```
gset ?X ≡ N(gset A)
?X ≡ N(A)
```

Inférence

- On doit résoudre:

```
gset ?G2 ≡ N(gset K)
```

- Mais il n'y a pas a priori de solution pour:

```
gset ?X ≡ N(A)
```

- En fait, $N(A)$ est toujours muni d'une structure de groupe: c'est la construction **N**(**A**).

```
gset ?X ≡ N(gset A)
?X ≡ N(A)
```

- On a donc résolu:

```
gset ?G2 ≡ N(gset K)
G2 = N(K)
```

Inférence par classes de types

```
Fact cardG_gt0 gT (G : {group gT}) : 0 < #|gset G|.
```

```
  gT : finGroupType
   K : {group gT}
   H : {group gT}
  ================
   0 < #|gset H ∩ N(gset K)|
```

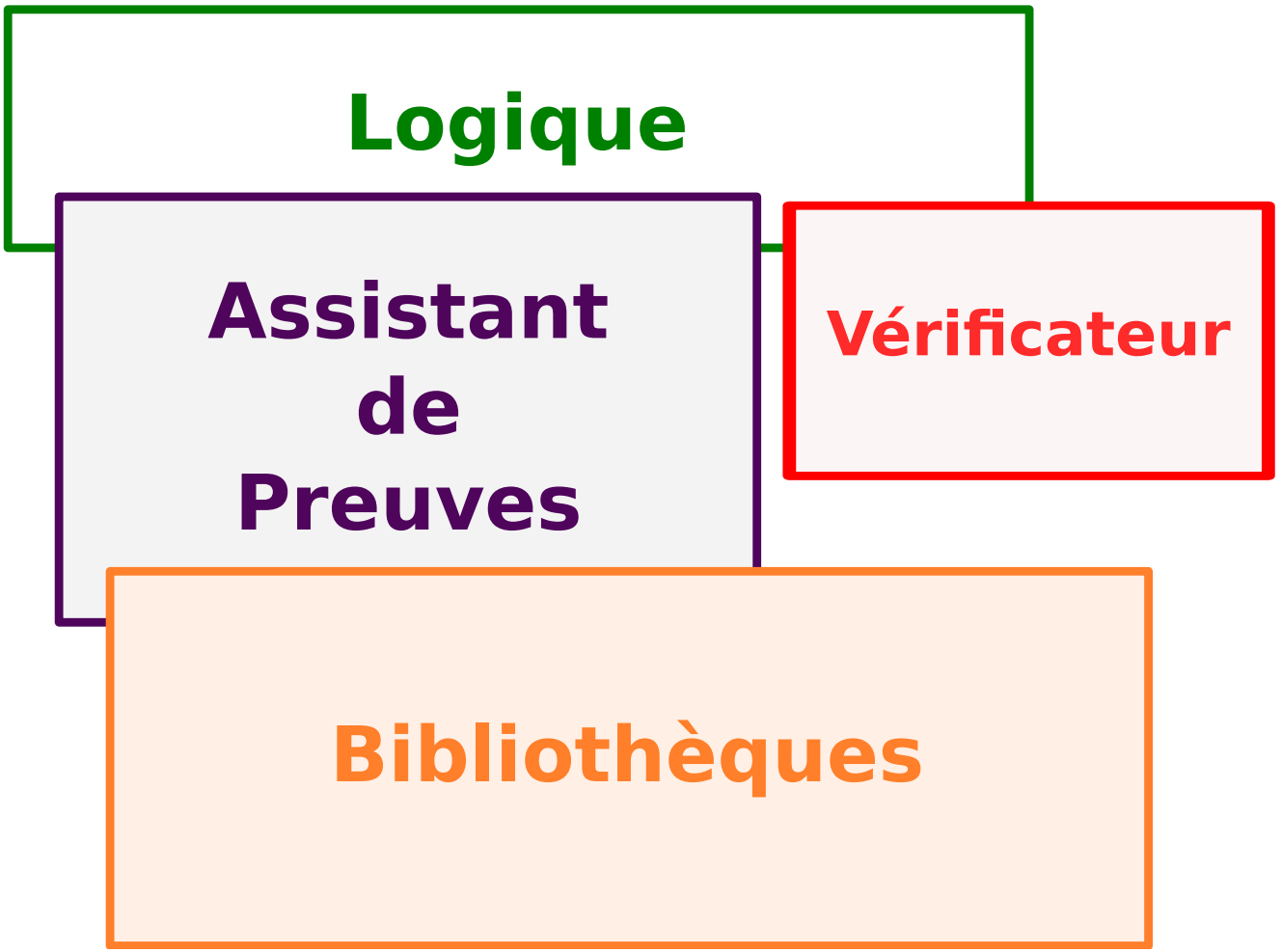
Inférence par classes de types

```
Fact cardG_gt0 gT (G : {group gT}) : 0 < #|gset G|.
```

```
  gT : finGroupType
   K : {group gT}
   H : {group gT}
  ==================
   0 < #|gset H ∩ N(gset K)|
```

```
apply: cardG_gt0.
```

Assistants de preuve



Assistants de preuve: logique

- E. Zermelo: Untersuchungen über die Grundlagen der Mengenlehre, Math. Annalen 65 (1908), no.2: 261–281

- B. Russell: Mathematical Logic as Based on the Theory of Types, Amer. J. Math. 30 (1908), no. 3, 222–262

Assistants de preuve: logique

- Théorie des ensembles
- Théorie des types

Assistants de preuve: logique

- Théorie des ensembles

  Mizar (A. Trybulec, $\sim$ 1973)

- Théorie des types

Assistants de preuve: logique

- Théorie des ensembles

  Mizar (A. Trybulec, $\sim$ 1973)

- Théorie des types

  AUTOMATH (N. G. de Bruijn, $\sim$ 1967)

Assistants de preuve: logique

- Théorie des ensembles

  Mizar (A. Trybulec, $\sim$ 1973)

- Théorie des types

  AUTOMATH (N. G. de Bruijn, $\sim$ 1967)

  HOL, HOL-Light, Isabelle/HOL, Coq, Agda, Lean, etc.

Assistants de preuve: automatisation

- Synthèse d'énoncés;
- Preuve automatique, à petite et grande échelle.

Assistants de preuve: automatisation

Asymptotique automatique:

$$F(n+2) = F(n+1) + F(n), \quad F(1) = 1 \quad F(0) = 1$$

$$F(n) = \mathcal{O}(1,619^n)$$

[Verified Solving and Asymptotics of Linear Recurrences, M. Eberl Proc. of CPP'2019, to appear]

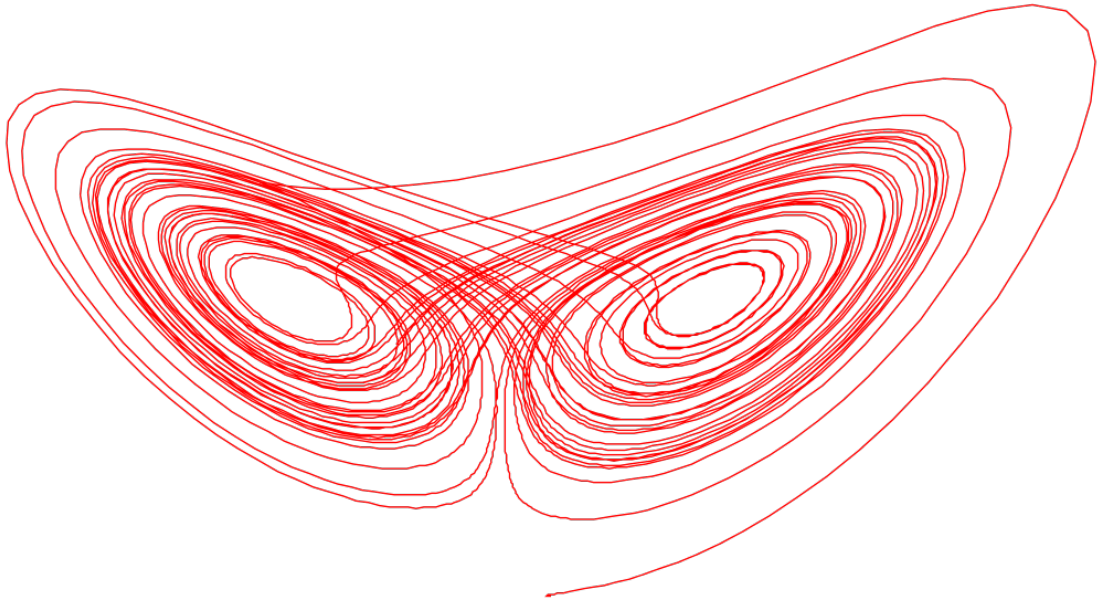
Assistants de preuve: bibliothèques

[A formal proof of the Odd Order theorem, Gonthier et al. ITP 2013]

Assistants de preuves: perspectives

- Preuve de programme, pour les mathématiques

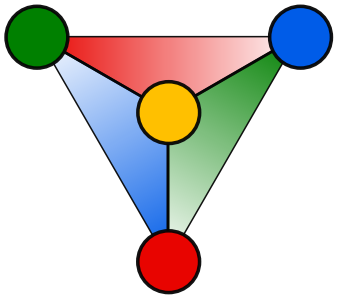
Solveur d'EDO vérifié



- Initié par E. Lorentz (1963);
- 14th problème de S. Smale (1998);
- Résolu par W. Tucker (1999);
- Calculs vérifiés par F. Immler (2018).

[A Verified ODE Solver and Smale's 14th Problem, F. Immler, PhD, 2018]

Théorème des quatre couleurs



- Conjecture: F. Guthrie (1852)
- Preuve: K. Appel - W. Haken (1976)
- Preuve formelle: G. Gonthier - B. Werner (2004)

Flyspeck

- Conjecture: J. Kepler (1611)
- Stratégie, usage de l'ordinateur: L. F. Tóth (1953)
- Preuve: Th. C. Hales, S. Ferguson (1998/2006)
- Preuve formelle: Th. C. Hales et al. (2015)

Assistants de preuves: perspectives

- Preuve de programme, pour les mathématiques;

Assistants de preuves: perspectives

- Preuve de programme, pour les mathématiques;
- Formalisation de mathématiques contemporaines;

Assistants de preuves: perspectives

- Preuve de programme, pour les mathématiques;
- Formalisation de mathématiques contemporaines;
- Découverte de nouvelles mathématiques?

[A Generalized Blakers-Massey Theorem, M. Anel, G. Biedermann, E. Finster, A. Joyal, 2017, arXiv:1703.09050]