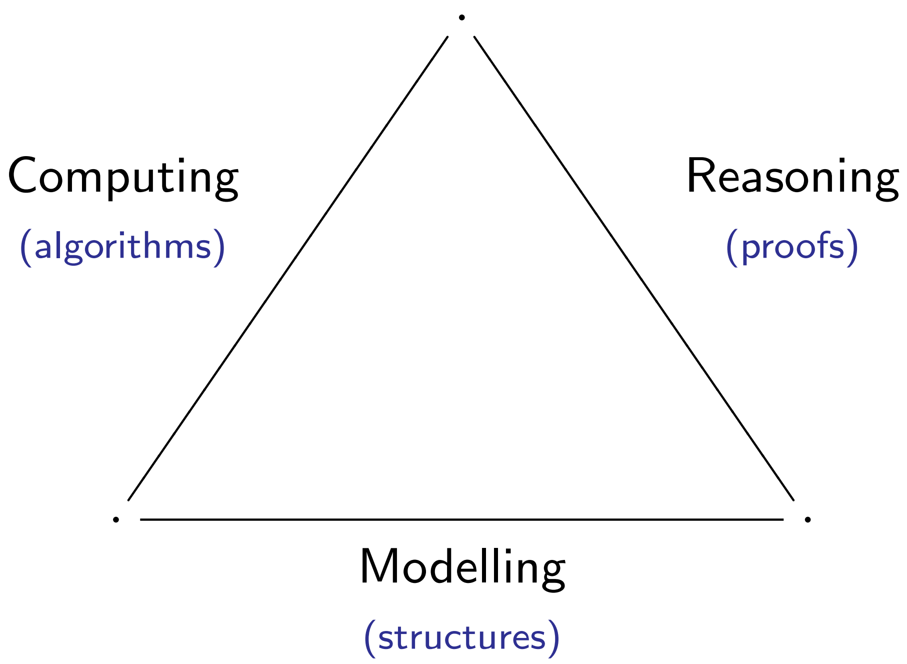
# Main Issues in Computer Mathematics

Henk Barendregt

Brouwer Institute
Radboud University
Nijmegen, The Netherlands

# Overview

Mathematical activity (stylised): modelling, computing, reasoning




Mathematics is usually done with *informal* rigour

refereeing playing an important role

The Babylonians set a standard for computing

The Greek set a standard of proving and the axiomatic method

Archimede, al-Khôwarizmî, Newton partially combined the two

Euler, based on Leibniz's version of analysis, made many computational contributions

Augustin-Louis Cauchy (1789-1857)
increased the rigour of proofs for dealing with arbitrarily small quantities
providing an interface between computing and proving

Then mathematics bloomed as never before, leading to applications like
Maxwell's equations, Relativity and Quantum Physics

The Babylonean and Greek traditions diverged in the 20-th century:
Computer Algebra systems versus Proof Checking systems

Mathematical Assistants, yielding Computer Mathematics, will unify the two

Robert Musil (The man without qualities):
*The precision, force and certainty of this thinking,*
*unequaled in life, almost filled him with melancholy*

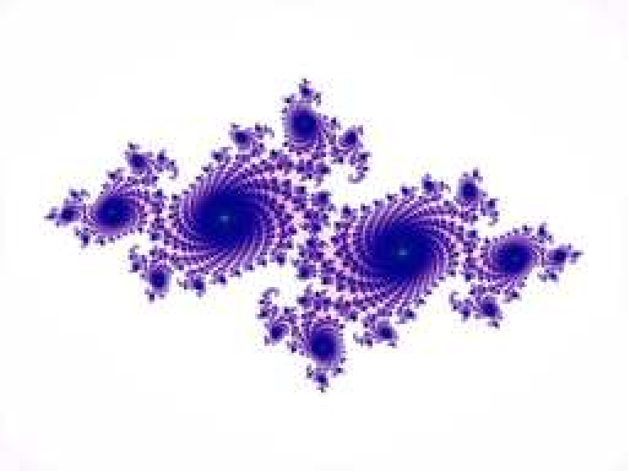
- Numerical computing
- Symbolic computing
- Text editing (latex)
- Visualization
- Developing mathematics: Computer Mathematics

- $\int_0^\pi \frac{1}{\sqrt{1-\frac{1}{4}\sin^2\varphi}} d\varphi \quad \longmapsto \quad 3.371500710$

- $\int \sqrt{x+x^2}dx \quad \longmapsto \sqrt{1+x}(\frac{\sqrt{x}}{4}+\frac{x^{\frac{3}{2}}}{2}) - \frac{\mathtt{ArcSinh}(\sqrt{\mathtt{x}})}{4}$

- `$\sum^\infty_{i=0}\frac{x^i}{i!}$` $\longmapsto \quad \sum_{i=0}^\infty \frac{x^i}{i!}$

- Julia set $J_z$ [1918] with
  $f_c(z) = z^2 + c$, where $z, c \in \mathbb{C}$
  $J_c = \{z \in \mathbb{C} \mid \lim_{n\to\infty} f_c^n(z) \neq \infty\}$
  $c = -0.7268953477091140714 39 +$
  $0.1888871290438459547 92 * i$

  $\longmapsto$ 

Mathematical assistant (Computer Mathematics System) helps human user:

Representing arbitrary mathematical structures (modelling)

Manipulating these (computing)

Stating and proving results about them (reasoning)

*in an impeccable way*

Not just symmetric group $S_{50}$ also $S_n$ for a variable $n \in \mathbb{N}$

An infinite dimensional Hilbert-space $\mathcal{H}$

beyond Computer Algebra

- Representing “computable” objects

  $\sqrt{2}$ becomes a symbol $\alpha$

  $\alpha^2 - 2$ becomes $0$ $\alpha + 1$ cannot be simplified

- Representing “non-computable” objects

  Hilbert space $H$, again just a symbol

  $P(H) :=$ “$H$ *is locally compact*” is not decidable

But $\vdash p :^1 P(H)$ is decidable

Hence we need formalized proofs

---

[1] $p$ is a proof of $P(H)$

The foundations of reasoning, modelling and computing all fit onto one page

$\Rightarrow$ A proof-checking program can be written that can be checked by a human

| Introduction Rules | Elimination Rules |
|---|---|
| $\dfrac{\Gamma, x\ A \vdash M : B}{\Gamma \vdash (\lambda x\ A.M) : (A \to B)}$ | $\dfrac{\Gamma \vdash F : (A \to B) \quad \Gamma \vdash p : A}{\Gamma \vdash (F p) : B}$ |
| $\dfrac{\Gamma \vdash p : A \quad \Gamma \vdash q : B}{\Gamma \vdash \langle p, q \rangle : (A \mathbin{\&} B)}$ | $\dfrac{\Gamma \vdash z : (A \mathbin{\&} B)}{\Gamma \vdash z.1 : A} \quad \dfrac{\Gamma \vdash z : (A \mathbin{\&} B)}{\Gamma \vdash z.2 : B}$ |
| $\dfrac{\Gamma \vdash p : A}{\Gamma \vdash (\mathrm{in}_1\ p) : (A \vee B)} \quad \dfrac{\Gamma \vdash p : B}{\Gamma \vdash (\mathrm{in}_2\ p) : (A \vee B)}$ | $\dfrac{\Gamma \vdash p : (A \vee B) \quad \Gamma, x\ A \vdash q : C \quad \Gamma, y\ B \vdash r : C}{\Gamma \vdash ([\lambda x\ A.q, \lambda y\ B.r]p) : C}$ |
| **Absurdum Rule** | **Classical Negation** |
| $\dfrac{\Gamma \vdash p : \bot}{\Gamma \vdash (\mathrm{abs}_A\ p) : A}$ | $\dfrac{\Gamma, \neg A \vdash \bot}{\Gamma \vdash A} \quad \neg A {:=} (A \to \bot)$ |

Classical/Intuitionistic Propositional Logic Natural Deduction Style (Gentzen)

Blue proofs as $\lambda$-terms

| | | |
|---|---|---|
| Hilbert | [1926] | Primitive Computable Functions<br>via primitive recursive schemes |
| Herbrand-Gödel | [1931] | Total Computable Functions<br>via some kind of Term Rewrite Systems |
| Church-Turing | [1936] | Partial Computable Functions<br>via $\lambda$-calculus and Turing Machines |

Application: the von Neumann computer

Simple computational model (Schönfinkel)

$$\begin{aligned} \mathsf{I}\, x &= x \\ \mathsf{K}\, x\, y &= x \\ \mathsf{S}\, x\, y\, z &= (x\, z)\, (y\, z) \end{aligned}$$

Ontology: set theory, type theory

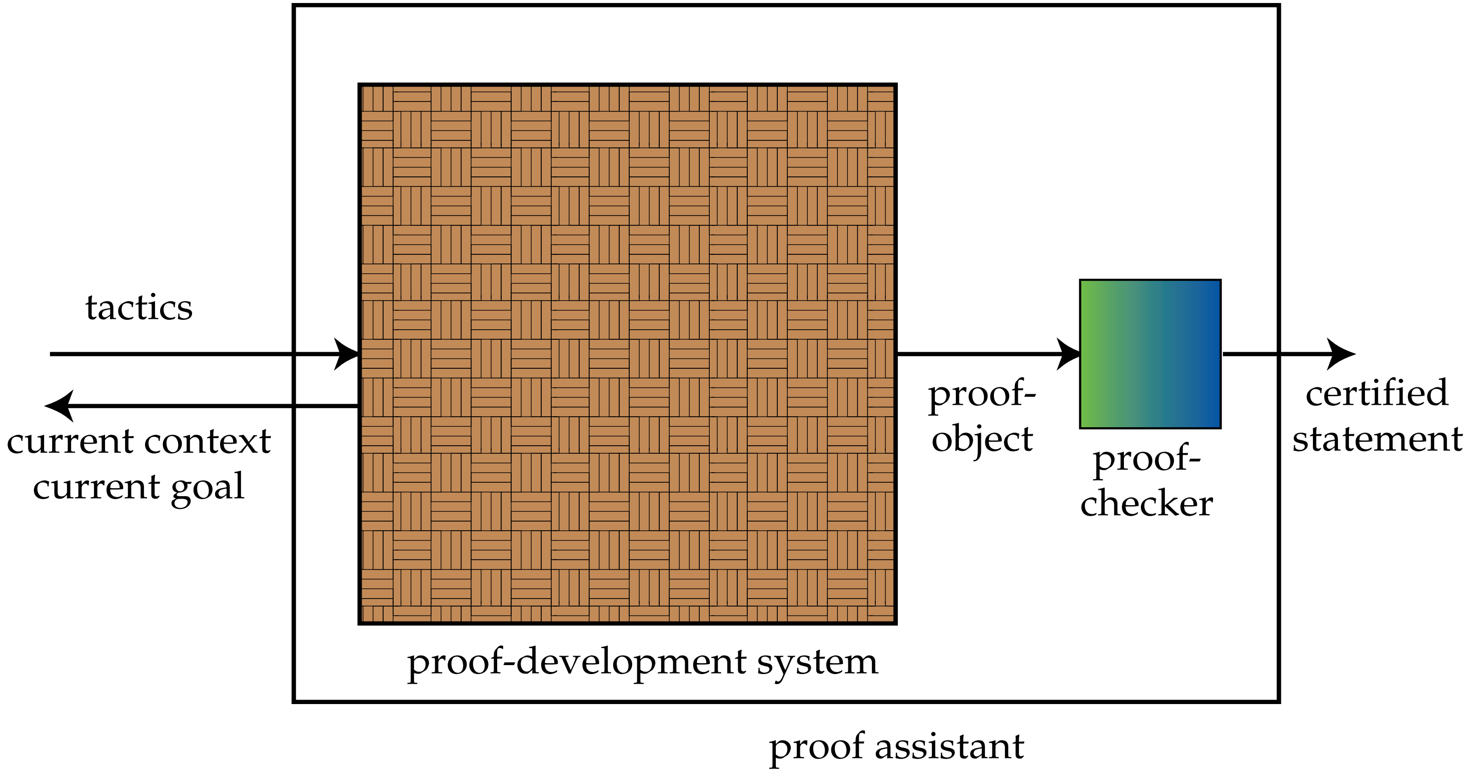
| | | |
|---|---|---|
| set theory | $\mathbb{N}$ | Infinity |
| | $\{A, B\}$ | Pair |
| | $\{a{\in}A \mid P(a)\}$ | Subset Selection |
| | $\{X \mid X \subseteq A\} = \mathcal{P}(A)$ | Power Set |
| | $\{F(a) \mid a{\in}A\} = F``A$ | Replacement |

type theory: inductively defined data types with their recursively defined functions and closed under function spaces $A{\to}B$ and dependent products $\Pi x\, A.B_x$ developed by Russell, de Bruijn (for Automath), extended by Scott, Martin-Löf, Girard, Huet and Coquand

Zermelo set theory as Pure Type System (Miquel)

| | |
|---|---|
| Axioms | $* : \square_1 : \square_2 : \square_3$ |
| Rules | $(*, *, *), (\square_k, *, *), (\square_i, \square_j, \square_{\max\{i,j\}})$ |
| | $k{\in}\{1, 2, 3\}, i, j{\in}\{1, 2\}$ |

Proof development system




assisting humans to learn, teach, referee, develop and apply mathematics

Some mathematical results have long and/or complex proofs

Reliability? The de Bruijn criterion: have a small checker.

Brouwer: Aristotelian logic is unreliable

It may promise existence without being able to give a witness

$$\vdash \exists n{\in}\mathbb{N}.P(n), \text{ but } \not\vdash P(0), \not\vdash P(1), \ldots$$

Example of such a $P$

$$P(n) \iff (n = 0 \ \& \ \mathsf{P} = \mathsf{NP}) \vee (n = 1 \ \& \ \mathsf{P} \neq \mathsf{NP})$$

Cause: the law of exluded middle.

Intuitionistic logic does not have this defect

Heyting: charted Brouwer's logic

Gentzen: gave it a nice form

"Intuitionism has become technology" (Constable)

FACTS.

1. $\vdash_{\mathbf{HA}} \forall x \exists y\, A(x,y) \quad \Rightarrow \quad \vdash_{\mathbf{HA}} \forall x\, A(x, f(x))$ with $f$ computable
2. $\vdash_{\mathbf{PA}} A \quad \Rightarrow \quad \vdash_{\mathbf{HA}} A$ if $A$ is $\Pi^2_0$, i.e. $\forall \vec{x} \exists \vec{y}\, B(\vec{x}, \vec{y})$ with $B$ having only bounded quantifiers $\forall z \leq n$, $\exists z \leq n$

Claim: competing way to obtain correct and efficient programs.

PROPOSITION. [Smullyan] *Given a non-empty set $C$ and a property $S$ on $C$. Then there is an element $c$ in $C$ such that*

$$S(c) \Rightarrow \forall x{\in}C.S(x) \qquad (*)$$

PROOF. Case 1. There is an $x{\in}C$ such that $\neg S(x)$. Take $c = x$.
Then implication $(*)$ holds vacuously (False $\Rightarrow$ anything).

Case 2. There is no $x{\in}C$ such that $\neg S(x)$. Then

$$\forall x{\in}C.S(x).$$

Then take any $c{\in}C$, which exists as $C$ is non-empty.
Now implication $(*)$ holds trivially (anything $\Rightarrow$ True). QED

Classical logic makes this 'unnatural' statement provable.

Classical mathematics is infested with such unreliable proofs.

Intuitionistic logic does not have these unsatisfactory effects.

Sleeper's principle := `(exists x:C,sleeps x -> forall y:C, sleeps y).`

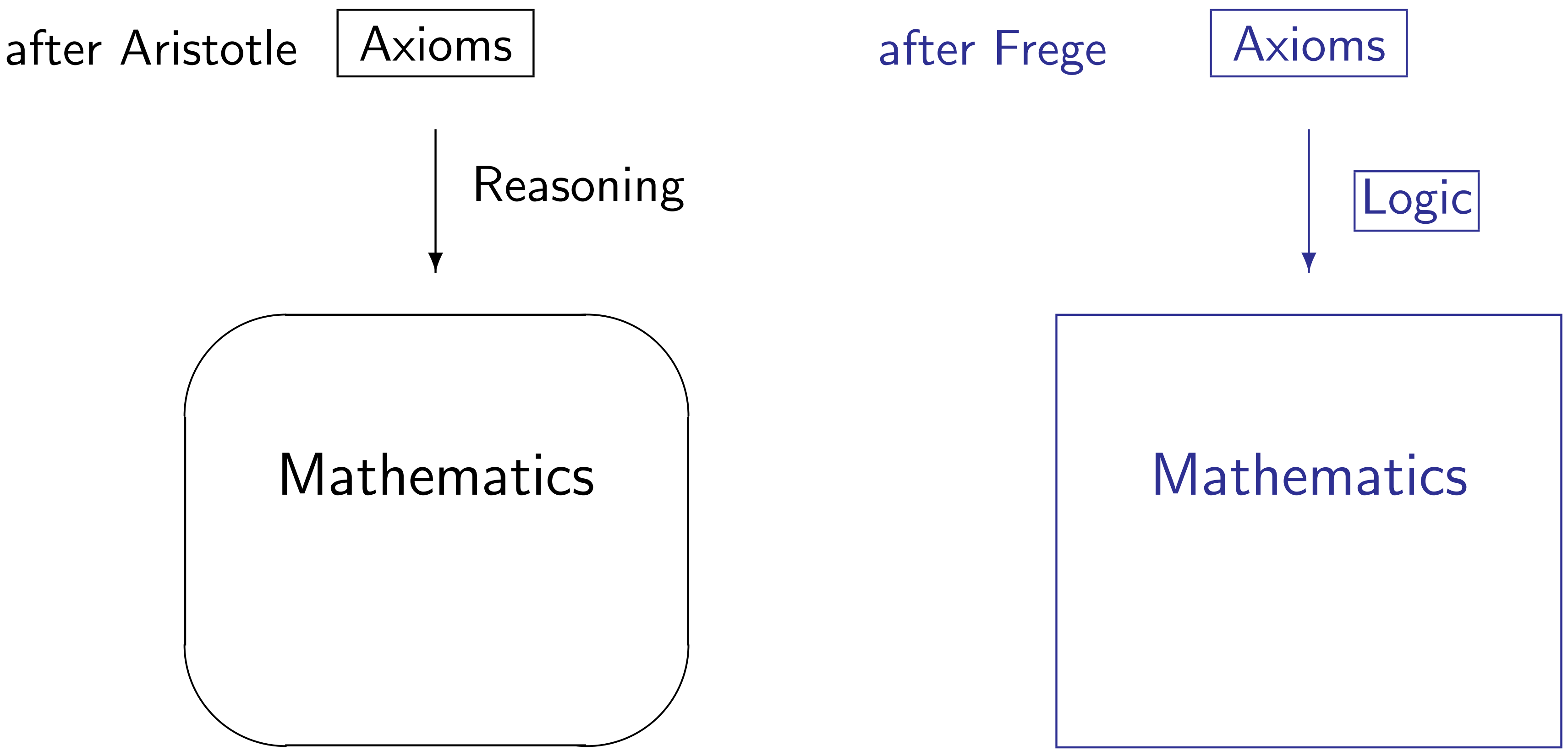
There is someone in this class,
such that if (s)he falls asleep during my lecture,
then everyone in this class falls asleep during my lecture.

```
Proof.
Or_ind
  (fun H : exists x:C, ~ sleeps x =>
   ex_ind
     (fun (x:C) (H0 : ~ sleeps x) =>
      ex_intro (fun x0:C => sleeps x0 -> forall y:C, sleeps y) x
        (fun S : sleeps x => False_ind (forall y:C, sleeps y) (H0 S))) H)
  (fun H : ~ (exists x:C, ~ sleeps x) =>
   ex_intro (fun x:C => sleeps x -> forall y:C, sleeps y) i
     (fun (_ : sleeps i) (y:C) =>
      or_ind (fun H0 : sleeps y => H0)
        (fun H0 : ~ sleeps y =>
         False_ind (sleeps y) (H (ex_intro (fun x:C => ~ sleeps x) y H0)))
        (classic (sleeps y)))) (classic (exists x:C, ~ sleeps x)). Qed
```

⟼ "Sleeper's principle" is proved, from assumptions
`C:Set, i:C, sleeps:C->Prop, classic:(forall p:Prop,p\/~p).`

Views on Mathematics

"$\vdash A$" stands for "$A$ is provable"




| | | | |
|---|---|---|---|
| Gödel | (1931) | Mathematics is incomplete | $\nvdash G$ and $\nvdash \neg G$ for some $G$ |
| | | | '$p$ is a proof of $A$' is decidable |
| Turing | (1936) | Mathematics is undecidable | $\{A \mid \vdash A\}$ non-computable |

Corollary. There are relatively short statements with very long proofs

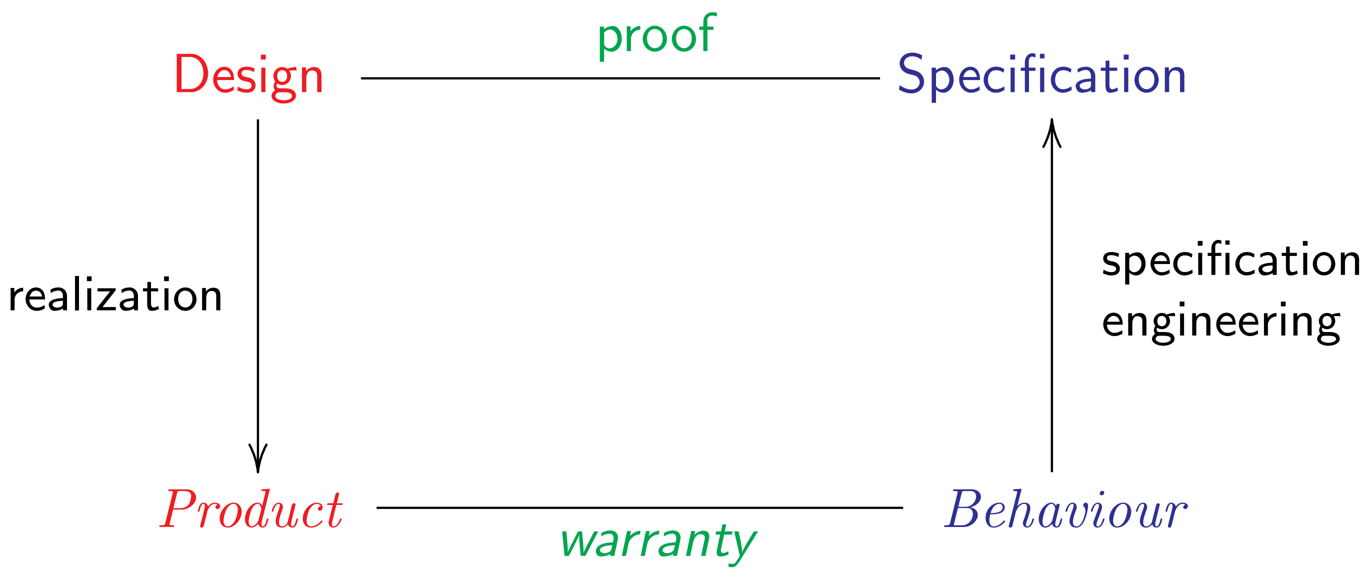
| System | Foundations | Proofs |
|---|---|---|
| Mizar | ZFC in First-Order Logic | petrified proofs, no Poincaré Pr. |
| HOL&Isabelle | Higher-Order Logic | ephemeral proofs, no Poincaré Pr. |
| Coq, NuPRL | Intuitionistic Type Theory | petrified proofs, Poincaré Pr. |
| PVS | Higher-Order Classical Logic | not de Bruijn, Poncaré Pr. |

| | Company | PI |
|---|---|---|
| Hol-light | intel | John Harrison |
| Coq | Microsoft<br>under BSD, not GPL | Georges Gonthier |

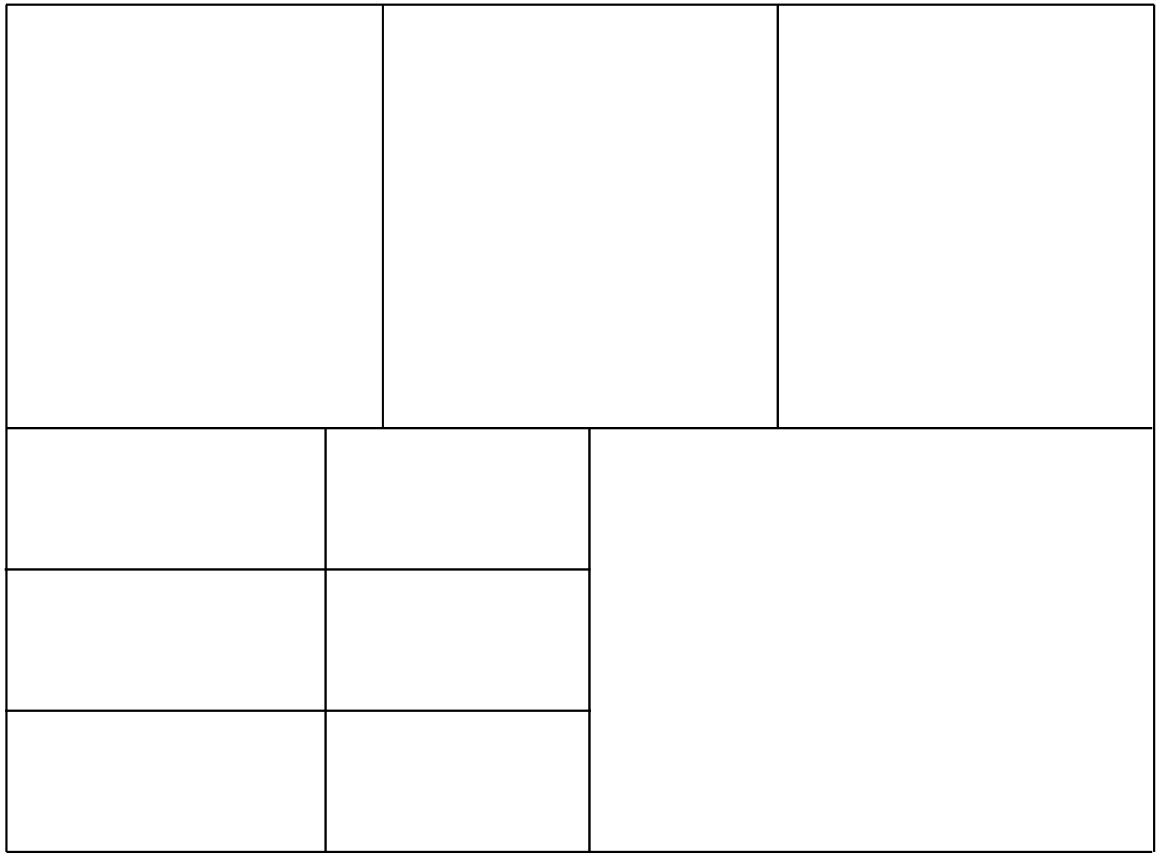
Applications

Verification of microcode floating-point arithmetic of Intel Itanium chip

Protocol verification for embedded software (both via proofs, not tests)




Rationality square (H. Wupper)



Chinese box: $P = f(p_1, \ldots, p_n)$

$$S_1(p_1) \;\&\; \ldots \;\&\; S_n(p_n) \;\Rightarrow\; S(P)$$

Mathematical developments

| | | |
|---|---|---|
| Fundamental Theorem of Algebra | Geuvers, Wiedijk, Zwanenburg, Pollack and Niqui | Coq |
| Fundamental Theorem of Calculus | Cruz-Filipe | Coq |
| Correctness Buchberger's algorithm | Person, Théry | Coq |
| Primality of $90262580833849968604493660721423078019 63$ | Oostdijk, Caprotti | Coq |
| Correctness of Fast Fourier Transform | Capretta | Coq |
| Book "Continuous lattices" (in part) | Bancerek et al. | Mizar |
| Impossibility of trisecting angles | Harrison | Hol-light |
| $\sum_{k=1}^{\infty} \frac{1}{k^2} = \frac{\pi^2}{6}$ | Harrison | Hol-light |
| Prime Number Theorem | Avigad | Isabelle-Hol |
| Four Colour Theorem | Gonthier | Coq |
| Jordan Curve Theorem | Hales | Hol |
| Primality of $>100$ digit numbers | Grégoire, Théry, Werner | Coq |
| $\lambda\beta\eta$SP conservative over $\lambda\beta\eta$ | Stoevring | Twelve |

Full integration of

modelling—computing—proving

checked by computer

- via a small program
- cool but also romantic
- absolute unambiguity
- correctness

Challenge

Developing libraries and tools (140 manyear for undergraduate mathematics)
Making formalizing as easy as writing LaTeX (or more easy!)

Present de Bruijn factor: 4 (space) 10 (time)
formalization of 1 page mathematics occupies 4 pages and takes a week

Tools should not be patented (stifling innovation), but risk to be!