Automated & Certified Proofs of Summation Formulae

Assia Mahboubi (j.w.w. F. Chyzak and T. Sibut-Pinote)

Computer calculations and mathematical proofs

Using computer calculations is the only way we know to prove:

- The Four Color Theorem (Appel-Haken, 1976)
- The Kepler conjecture (Hales, 1998)
- ...
- The ternary Goldbach conjecture (Helfgott, 2013)
- ...

Summation/Integral identities

$$\sum_{k\in\mathbb{Z}} \frac{(3k)!}{k!(k+1)!(k+2)!27^k} = \frac{(81n^2+261n+200)(3n+2)!}{40(n+2)!(n+1)!n!27^n} - \frac{9}{2}$$

$$\sum_{k\in\mathbb{Z}} (-1)^k \binom{a+b}{a+k}\binom{a+c}{c+k}\binom{b+c}{b+k} = \frac{(a+b+c)!}{a!b!c!}$$

$$\int_0^{+\infty} \frac{e^{-px}T_n(x)}{\sqrt{1-x^2}}dx = (-1)^n \pi I_n(p)$$

Mathematical riddles

Some simple ones:

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n \qquad \sum_{k=0}^{n} \binom{n}{k} (-1)^k = 0$$

Mathematical riddles

Some simple ones:

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n \qquad \sum_{k=0}^{n} \binom{n}{k} (-1)^k = 0$$

that can be obtained easily by specialization of the binomial formula:

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

considering $(1+1)^n = 2^n$ and $((-1)+1)^n = 0$ respectively.

Answers as closed forms

By similar tricks:

$$\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n} \qquad \sum_{k=0}^{n} \binom{n}{k}^2 (-1)^k = 0$$

Answers as closed forms

By similar tricks:

$$\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n} \qquad \sum_{k=0}^{n} \binom{n}{k}^2 (-1)^k = 0$$

but there is no hope to obtain any such *closed* form for higher powers of the binomial coefficients like $\sum_{k=0}^{n} \binom{n}{k}^3$, ...

Properties of sequences like $u_n := \sum_{k=0}^{n} \binom{n}{k}^3$ should be deduced from other informations than a closed form.

Answers as recurrences

A very informative data is a recurrence relation canceling the sequence:

- Optimized evaluation of the terms
- Asymptotic
- ...

Answers as recurrences: examples

- Our previous $u_n := \sum_{k=0}^{n} \binom{n}{k}^3$ is solution of:

$$(n+1)^2 a_{n+1} - (7n^2+7n+2)a_n - 8n^2 a_{n-1} = 0 \quad \text{(Franel, 1894)}$$

Answers as recurrences: examples

- Our previous $u_n := \sum_{k=0}^{n} \binom{n}{k}^3$ is solution of:

  $(n+1)^2 a_{n+1} - (7n^2+7n+2)a_n - 8n^2 a_{n-1} = 0$ (Franel, 1894)

- The sequence $u_n := \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2$ is solution of:

  $n^3 a_n - (34n^3 - 51n^2 + 27n - 5)a_{n-1} + (n-1)^3 a_{n-2} = 0$ (Apéry, 1978)

  which is a crucial point in its proof that $\zeta(3) := \sum_{k>0} \frac{1}{k^3}$ is irrational.

Checking a conjecture: easy cases

In these problems, checking a conjecture can be much easier than finding it. Example:

Let us prove the Cassini (1680) identity:

$$\forall n \in \mathbb{N}, F_{n+2}F_n - F_{n+1}^2 = (-1)^n$$

where F_n is the n-th Fibonacci number:

$$\forall n \in \mathbb{N}, F_{n+2} = F_{n+1} + F_n, \quad F(0) = 1, \quad F(1) = 1$$

Checking a conjecture: less easy cases

But checking a conjecture can also be extremely difficult:

Checking Apéry's claim that $u_n := \sum_k \binom{n}{k}^2 \binom{n+k}{k}^2$ verifies

$$n^3 u_n - (34n^3 - 51n^2 + 27n - 5)u_{n-1} + (n-1)^3 u_{n-2} = 0$$

took several months of effort to experts in number theory before being proved correct by Cohen and Zagier (1979).

Checking a conjecture: telescopes

In order to prove that $u_n := \sum_k v_{n,k}$ with $v_{n,k} := \binom{n}{k}^2 \binom{n+k}{k}^2$ verifies

$$n^3 u_n - (34n^3 - 51n^2 + 27n - 5)u_{n-1} + (n-1)^3 u_{n-2} = 0$$

Checking a conjecture: telescopes

In order to prove that $u_n := \sum_k v_{n,k}$ with $v_{n,k} := \binom{n}{k}^2 \binom{n+k}{k}^2$ verifies

$$n^3 u_n - (34n^3 - 51n^2 + 27n - 5)u_{n-1} + (n-1)^3 u_{n-2} = 0$$

Cohen and Zagier construct $w_{n,k}$ such that:

$$n^3 v_{n,k} - (34n^3 - 51n^2 + 27n - 5)v_{n-1,k} + (n-1)^3 v_{n-2,k} = w_{n,k+1} - w_{n,k}$$

Checking a conjecture: telescopes

In order to prove that $u_n := \sum_k v_{n,k}$ with $v_{n,k} := \binom{n}{k}^2 \binom{n+k}{k}^2$ verifies

$$n^3 u_n - (34n^3 - 51n^2 + 27n - 5)u_{n-1} + (n-1)^3 u_{n-2} = 0$$

Cohen and Zagier construct $w_{n,k}$ such that:

$$n^3 v_{n,k} - (34n^3 - 51n^2 + 27n - 5)v_{n-1,k} + (n-1)^3 v_{n-2,k} = w_{n,k+1} - w_{n,k}$$

Then they sum over k both hand sides:

Checking a conjecture: telescopes

In order to prove that $u_n := \sum_k v_{n,k}$ with $v_{n,k} := \binom{n}{k}^2 \binom{n+k}{k}^2$ verifies

$$n^3 u_n - (34n^3 - 51n^2 + 27n - 5)u_{n-1} + (n-1)^3 u_{n-2} = 0$$

Cohen and Zagier construct $w_{n,k}$ such that:

$$n^3 v_{n,k} - (34n^3 - 51n^2 + 27n - 5)v_{n-1,k} + (n-1)^3 v_{n-2,k} = w_{n,k+1} - w_{n,k}$$

Then they sum over k both hand sides:

$$\sum_k (n^3 v_{n,k} - (34n^3 - 51n^2 + 27n - 5)v_{n-1,k} + (n-1)^3 v_{n-2,k}) = \sum_k (w_{n,k+1} - w_{n,k})$$

Checking a conjecture: telescopes

In order to prove that $u_n := \sum_k v_{n,k}$ with $v_{n,k} := \binom{n}{k}^2 \binom{n+k}{k}^2$ verifies

$$n^3 u_n - (34n^3 - 51n^2 + 27n - 5)u_{n-1} + (n-1)^3 u_{n-2} = 0$$

Cohen and Zagier construct $w_{n,k}$ such that:

$$n^3 v_{n,k} - (34n^3 - 51n^2 + 27n - 5)v_{n-1,k} + (n-1)^3 v_{n-2,k} = w_{n,k+1} - w_{n,k}$$

Then they sum over k both hand sides:

$$\sum_k (n^3 v_{n,k} - (34n^3 - 51n^2 + 27n - 5)v_{n-1,k} + (n-1)^3 v_{n-2,k}) = \sum_k (w_{n,k+1} - w_{n,k})$$

$$= 0$$

Checking a conjecture: telescopes

In order to prove that $u_n := \sum_k v_{n,k}$ with $v_{n,k} := \binom{n}{k}^2 \binom{n+k}{k}^2$ verifies

$$n^3 u_n - (34n^3 - 51n^2 + 27n - 5)u_{n-1} + (n-1)^3 u_{n-2} = 0$$

Cohen and Zagier construct $w_{n,k}$ such that:

$$n^3 v_{n,k} - (34n^3 - 51n^2 + 27n - 5)v_{n-1,k} + (n-1)^3 v_{n-2,k} = w_{n,k+1} - w_{n,k}$$

Then they sum over k both hand sides:

$$\sum_k (n^3 v_{n,k} - (34n^3 - 51n^2 + 27n - 5)v_{n-1,k} + (n-1)^3 v_{n-2,k}) = \sum_k (w_{n,k+1} - w_{n,k})$$

$$n^3 u_n - (34n^3 - 51n^2 + 27n - 5)u_{n-1} + (n-1)^3 u_{n-2} =$$

Checking a conjecture: telescopes

In order to prove that $u_n := \sum_k v_{n,k}$ with $v_{n,k} := \binom{n}{k}^2 \binom{n+k}{k}^2$ verifies

$$n^3 u_n - (34n^3 - 51n^2 + 27n - 5)u_{n-1} + (n-1)^3 u_{n-2} = 0$$

Cohen and Zagier construct $w_{n,k}$ such that:

$$n^3 v_{n,k} - (34n^3 - 51n^2 + 27n - 5)v_{n-1,k} + (n-1)^3 v_{n-2,k} = w_{n,k+1} - w_{n,k}$$

Then they sum over k both hand sides:

$$\sum_k (n^3 v_{n,k} - (34n^3 - 51n^2 + 27n - 5)v_{n-1,k} + (n-1)^3 v_{n-2,k}) = \sum_k (w_{n,k+1} - w_{n,k})$$

$$n^3 u_n - (34n^3 - 51n^2 + 27n - 5)u_{n-1} + (n-1)^3 u_{n-2} = w_{n,\infty} - w_{n,0} = 0$$

More than recipes

The collection of proofs we have seen so far is not a bag of tricks. There is:

- An algebraic framework and effective results
- Advances in algorithmics
- Efficient implementations in computer algebra systems

that systematize these lines of reasoning.

They provide automated ways of guessing and checking these identities/recurrences and their differential analogues.

Linear recurrences with polynomial coefficients

A sequence $u := (u_n)_{n\in\mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$ is holonomic (or P-recursive) if it is a solution of a linear recurrence with coefficients in $\mathbb{K}[n]$.

- $F_{n+2} = F_{n+1} + F_n$
- $nu_{n+2} - (n^2 + 100)u_{n+1} - u_n = 0$

In the special case when the recurrence is of order 1 (and $u_0 \neq 0$) the sequence u is said to be hypergeometric.

- $(n+1)u_{n+1} = nu_n$

The definition extends obviously to sequences with several indexes and multivariate polynomial coefficients.

Linear recurrences with polynomial coefficients

- Elementary remark: Linear recurrences impose a structure of vector space to their set of solution.
- Hence in order to prove the equality of two holonomic sequences it is sufficient to:
  - Find a common linear recurrence relation
  - Check that the two sequences coincide on sufficiently many initial conditions.

Remember the Cassini identity $F_{n+2}F_n - F_{n+1}^2 = (-1)^n$.

Linear recurrences with polynomial coefficients

- Less obvious remark: The set of holonomic sequences on a field $\mathbb{K}$ is a $\mathbb{K}$-algebra.
- Hence if u and v are holonomic it is possible to:
  - Find a recurrence canceling $(u + v)$
  - Find a recurrence canceling $(u * v)$

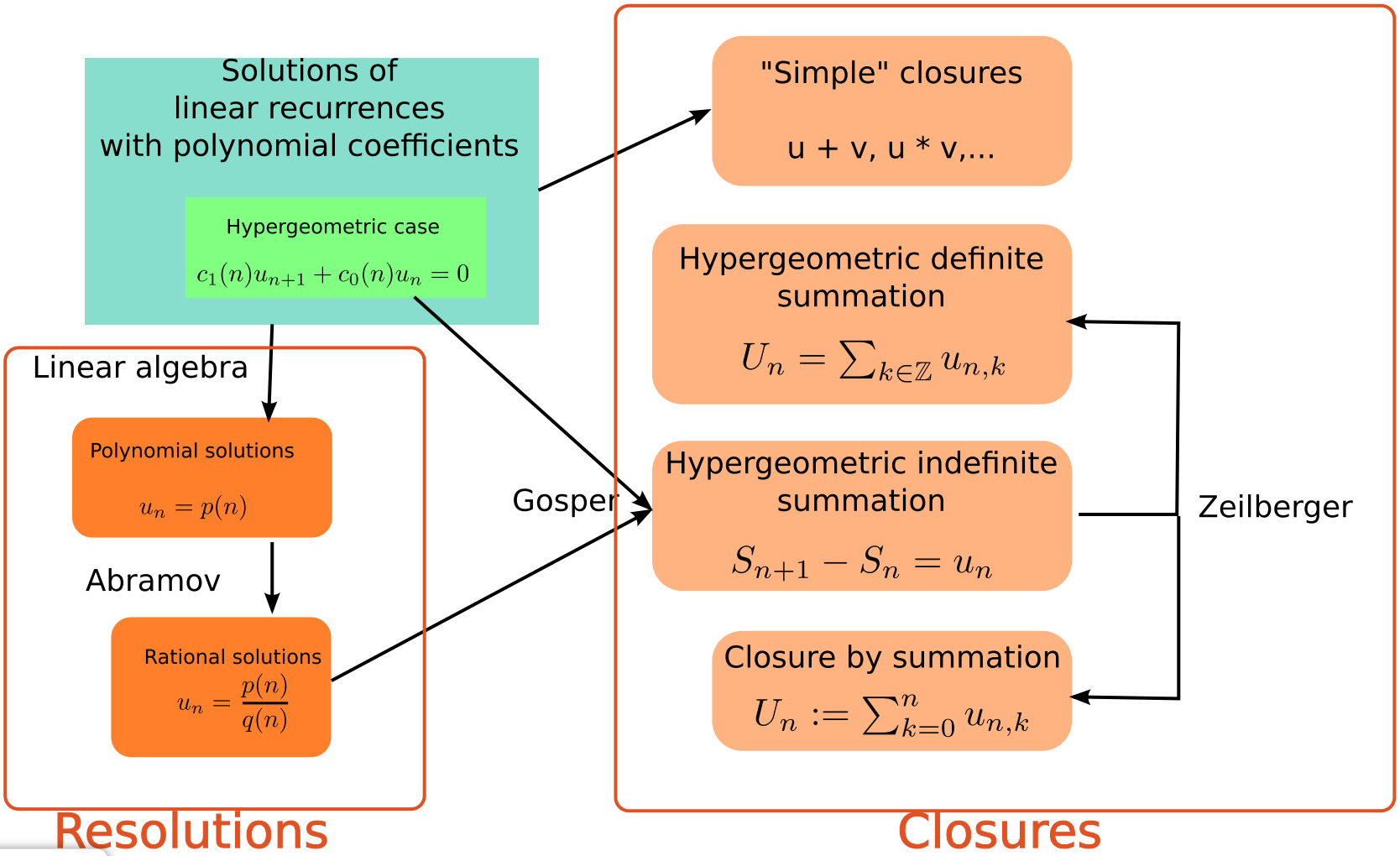
Find a recurrence canceling $\binom{n}{k} + k!F_n$.

Linear recurrences with polynomial coefficients

- Non obvious at all: If $(u_{n,k})$ is holonomic, it is possible to:
  - Find a recurrence canceling $U_n := \sum_{k=0}^{+\infty} u_{n,k}$
  - Find a recurrence canceling $U_n := \sum_{k=0}^{n} u_{n,k}$

Remember Apéry's sequence $u_n := \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2$

From existence theorems to efficient algorithms



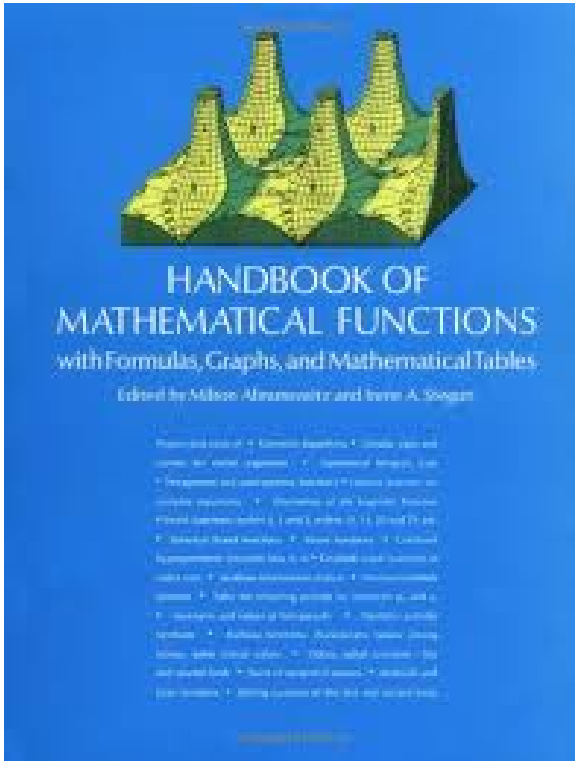
Linear differential operators with polynomial coefficients

The underlying theory (of D-modules and Ore/Weyl algebra) applies just as well to functions of a continuous variable:

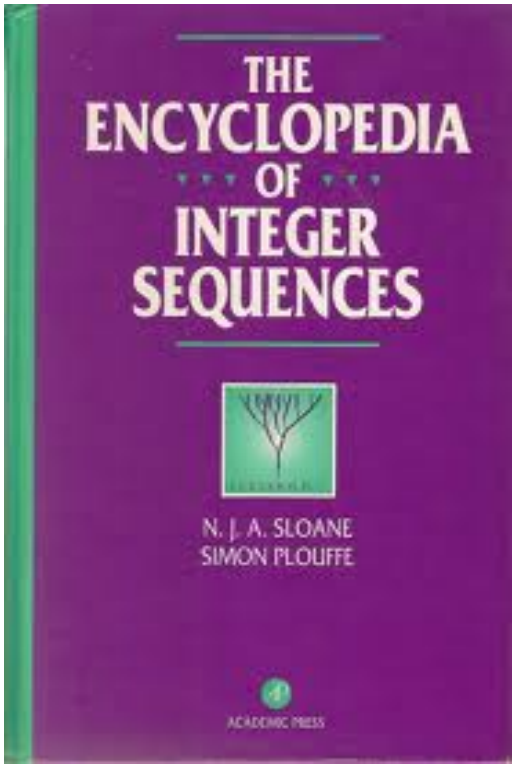
- A formal series $\sum_{n\geq 0} a_n X^n$ is holonomic (or D-finite) if it is solution of a differential equation with polynomial coefficients.
- Remark: A formal series is holonomic $\sum_{n\geq 0} a_n X^n$ if and only if the sequence (a_n) of its coefficients is holonomic.

And algorithms also transpose.

A large class of objects



Abramowitz and Stegun
$\sim 60\%$ of the entries are holonomic



Plouffe and Sloane
$\sim 25\%$ of the entries are holonomic

Implementations and their applications

- Several packages are available in mainstream computer algebra systems (Maple, Mathematica).
- Computer-algebra aided proofs of several theorems (irrationality of $\zeta(3)$, q-TSPP conjecture,...)
- A Dynamic Dictionary of Mathematical Functions

  `http://ddmf.msr-inria.inria.fr/1.9.1/ddmf`

Confidence

- Static large tables of formulae are quite error-prone.
- Data-bases generated by generic computer-algebra algorithms are much more reliable.
- Generating these data-bases benchmarks the computer-algebra libraries and increase the confidence in computer algebra aided proofs.

Limits of computer algebra aided proofs

Beyond the possible but rather rare bugs that can affect these programs:

- Computer algebra systems manipulate symbolic expressions, not functions

$$\frac{0}{0} = \text{Error}, \qquad \frac{x-y}{x-y} = 1$$

- Equality almost everywhere is equality.
- Experts know the dark corners of the algorithms they design, but not necessarily the user.

Non-expert users can go wrong very quickly.

Limits of computer algebra aided proofs

Examples of dark corners:

- Singularities: $(n-4)u_{n+1} - (n-4)u_n = 0 \quad u_5 = ?$

  $\Rightarrow$ germs of sequences, not sequences.

Limits of computer algebra aided proofs

Examples of dark corners:

- Singularities: $(n-4)u_{n+1} - (n-4)u_n = 0 \quad u_5 = ?$
  $\Rightarrow$ germs of sequences, not sequences.
- Rational fractions: $u_{n+1} - \frac{1}{n-4}u_n = 0 \quad u_5 = ?$

Limits of computer algebra aided proofs

Examples of dark corners:

- Singularities: $(n-4)u_{n+1} - (n-4)u_n = 0 \quad u_5 = ?$
  $\Rightarrow$ germs of sequences, not sequences.
- Rational fractions: $u_{n+1} - \frac{1}{n-4}u_n = 0 \quad u_5 = ?$
  $\Rightarrow$ germs of sequences, not sequences.

Limits of computer algebra aided proofs

Examples of dark corners:

- Singularities: $(n-4)u_{n+1} - (n-4)u_n = 0 \quad u_5 = ?$
  $\Rightarrow$ germs of sequences, not sequences.
- Rational fractions: $u_{n+1} - \frac{1}{n-4}u_n = 0 \quad u_5 = ?$
  $\Rightarrow$ germs of sequences, not sequences.
- Rational fractions: $u_{n+1} - \frac{n-4}{n-4}u_n = 0 \quad u_5 = ?$

Limits of computer algebra aided proofs

Examples of dark corners:

- Singularities: $(n-4)u_{n+1} - (n-4)u_n = 0 \quad u_5 = ?$
  $\Rightarrow$ germs of sequences, not sequences.
- Rational fractions: $u_{n+1} - \frac{1}{n-4}u_n = 0 \quad u_5 = ?$
  $\Rightarrow$ germs of sequences, not sequences.
- Rational fractions: $u_{n+1} - \frac{n-4}{n-4}u_n = 0 \quad u_5 = ?$
  $\Rightarrow$ Are we sure it never happens?

Limits of computer algebra aided proofs

Examples of dark corners:

- Singularities: $(n-4)u_{n+1} - (n-4)u_n = 0 \quad u_5 = ?$
  $\Rightarrow$ germs of sequences, not sequences.
- Rational fractions: $u_{n+1} - \frac{1}{n-4}u_n = 0 \quad u_5 = ?$
  $\Rightarrow$ germs of sequences, not sequences.
- Rational fractions: $u_{n+1} - \frac{n-4}{n-4}u_n = 0 \quad u_5 = ?$
  $\Rightarrow$ Are we sure it never happens? No.

Limits of computer algebra aided proofs

Examples of dark corners:

- Singularities: $(n-4)u_{n+1} - (n-4)u_n = 0 \quad u_5 = ?$
  $\Rightarrow$ germs of sequences, not sequences.
- Rational fractions: $u_{n+1} - \frac{1}{n-4}u_n = 0 \quad u_5 = ?$
  $\Rightarrow$ germs of sequences, not sequences.
- Rational fractions: $u_{n+1} - \frac{n-4}{n-4}u_n = 0 \quad u_5 = ?$
  $\Rightarrow$ Are we sure it never happens? No.
- Summation of rational fractions: $\sum_k (u_{n,k+1} - \frac{1}{k-4}u_{n,k})$
  $\Rightarrow$ Are we sure it never happens?

Limits of computer algebra aided proofs

Examples of dark corners:

- Singularities: $(n-4)u_{n+1} - (n-4)u_n = 0 \quad u_5 = ?$
  $\Rightarrow$ germs of sequences, not sequences.
- Rational fractions: $u_{n+1} - \frac{1}{n-4}u_n = 0 \quad u_5 = ?$
  $\Rightarrow$ germs of sequences, not sequences.
- Rational fractions: $u_{n+1} - \frac{n-4}{n-4}u_n = 0 \quad u_5 = ?$
  $\Rightarrow$ Are we sure it never happens? No.
- Summation of rational fractions: $\sum_k (u_{n,k+1} - \frac{1}{k-4}u_{n,k})$
  $\Rightarrow$ Are we sure it never happens? No.

Proof assistants

In a proof assistant, like the Coq system, the situation is much different:

- The user defines the mathematical objects inside the logic.
- The user specifies the mathematical objects inside the logic.
- For instance, the comparison relation between objects or the behavior of partial operations are made precise.
- A machine-checked, axiom-free proof is very much trustable.

Proof assistants

In a proof assistant, like the Coq system, the situation is much different:

- The user defines the mathematical objects inside the logic.
- The user specifies the mathematical objects inside the logic.
- For instance, the comparison relation between objects or the behavior of partial operations are made precise.
- A machine-checked, axiom-free proof is very much trustable.

But the efficiency of computations is poorer and certification is not an easy task.

Computer algebra aided formal proofs

We can benefit from both ways of doing mathematics with a computer:

- We guess recurrence operators using a computer algebra system (here Maple).
- We check formally their validity inside the proof assistant (here Coq).

We just pretty-print the output of a Maple session is some files, later included in the files describing the formal proof.

Formally proving Maple's recurrences

- We prove new recurrences from known ones.
- We normalize the conjectured recurrence using the known relations.
- The recurrence is reduced on independent shifts of the known sequences (Grobner basis).
- We normalize their (rational fraction) coefficients: they should be zero.

Formally proving Maple's recurrences

- We prove new recurrences from known ones.
- We normalize the conjectured recurrence using the known relations.
- The recurrence is reduced on independent shifts of the known sequences (Grobner basis).
- We normalize their (rational fraction) coefficients: they should be zero.

But we should handle denominators with care, which makes the normalization less systematic.

Example: Apéry's proof that $\zeta(3) \notin \mathbb{Q}$

The crux of the proof is to verify that the two sequences:

- $a_n := \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2$
- $b_n := a_n \sum_{k=1}^{n} \frac{1}{k^3} + \sum_{k=1}^{n} \sum_{m=1}^{k} \frac{(-1)^{m+1}}{2m^3 \binom{n}{m} \binom{n+m}{m}} c_{n,k}$

satisfy the same linear recurrence of order two.

Example: Apéry's proof that $\zeta(3) \notin \mathbb{Q}$

For this we follow the syntactic tree of the expressions defining a_n and b_n:

- We (easily) know the recurrences canceling the leaves of the expressions of a_n and b_n: $\binom{n}{m}$, $\binom{n+m}{m}$, $\sum_{k=1}^{n} \frac{1}{k^3}$.

Example: Apéry's proof that $\zeta(3) \notin \mathbb{Q}$

For this we follow the syntactic tree of the expressions defining a_n and b_n:

- We (easily) know the recurrences canceling the leaves of the expressions of a_n and b_n: $\binom{n}{m}$, $\binom{n+m}{m}$, $\sum_{k=1}^{n} \frac{1}{k^3}$.
- At each node of the tree we use Maple to guess new recurrences for the auxiliary sequence, using the ones previously computed.

Example: Apéry's proof that $\zeta(3) \notin \mathbb{Q}$

For this we follow the syntactic tree of the expressions defining a_n and b_n:

- We (easily) know the recurrences canceling the leaves of the expressions of a_n and b_n: $\binom{n}{m}$, $\binom{n+m}{m}$, $\sum_{k=1}^{n} \frac{1}{k^3}$.
- At each node of the tree we use Maple to guess new recurrences for the auxiliary sequence, using the ones previously computed.
- We prove formally and independently Maple's conjectures using the recurrences previously formally established.

Example: Apéry's proof that $\zeta(3) \notin \mathbb{Q}$

For this we follow the syntactic tree of the expressions defining a_n and b_n:

- We (easily) know the recurrences canceling the leaves of the expressions of a_n and b_n: $\binom{n}{m}$, $\binom{n+m}{m}$, $\sum_{k=1}^{n} \frac{1}{k^3}$.
- At each node of the tree we use Maple to guess new recurrences for the auxiliary sequence, using the ones previously computed.
- We prove formally and independently Maple's conjectures using the recurrences previously formally established.
- When proving a conjecture produced by Maple, we decorate it with the necessary side conditions.

Sketch of the proof

In order to prove that $\zeta(3) \notin \mathbb{Q}$ we show that otherwise we could exhibit a sequence S_n such that:

- $\forall n, \quad S_n$ is an integer
- $\forall n, \quad S_n > 0$
- $\lim_{n \to \infty} S_n = 0$

Sketch of the proof

In fact prove that:

$$a_n\zeta(3) - b_n \to 0 \quad \text{and} \quad \forall n, a_n \in \mathbb{Z}^* \quad b_n \in \mathbb{Q}^*$$

Now in fact if we pose $d_n := lcm(1, \ldots, n)$ we even have:

$$2d_n^3(a_n\zeta(3) - b_n) \to 0$$

Sketch of the proof

In fact prove that:

$$a_n\zeta(3) - b_n \to 0 \quad \text{and} \quad \forall n, a_n \in \mathbb{Z}^* \quad b_n \in \mathbb{Q}^*$$

Now in fact if we pose $d_n := lcm(1, \ldots, n)$ we even have:

$$2d_n^3(a_n\zeta(3) - b_n) \to 0$$

In fact:

$S_n := 2d_n^3(a_n\zeta(3) - b_n)$ is the desired absurd sequence.

Steps in the proof

- $a_n\zeta(3) - b_n \to 0$

  considered elementary.
- $2d_n^3 b_n \in \mathbb{Z}$:

  considered as elementary arithmetic.
- $d_n \sim e^n$:

  considered as standard.
- $a_n\zeta(3) - b_n > 0$:

  asymptotic of a remainder since $a_n\zeta(3) - b_n \to 0$
- $2d_n^3(a_n\zeta(3) - b_n) \to 0$:

  asymptotic of the sequence $a_n\zeta(3) - b_n$

Current state of the formalization

Today we have checked in Coq that: $d_n = O(3^n) \Rightarrow \zeta(3) \notin \mathbb{Q}$.

- Proof of the common recurrence using a Maple session;
- Some elementary number theory (p-valuation, discrete log, binomials);
- A formal study of creative telescoping filling holes in the computer algebra literature;
- Improved formal proof-producing normalization procedures for ring/field expressions;
- Asymptotic reasoning using Cauchy reals and tactics for the bureaucracy of $\epsilon\delta$ reasoning.

Conclusion

- We now dispose of a systematic protocol to validate with a formal proof the recurrences for holonomic sequences guessed by th Algolib Maple library.
- We have used this protocol to formalize a large part of Apéry's proof that $\zeta(3) \in \mathbb{Q}$.
- Libraries from the Feit-Thompson proof have been instrumental in many places.
- But good data structures are still to be found (for proofs and for computations).
- Obtaining formal proofs in the differential case will be the next challenge, but a lot more formalized material is needed.