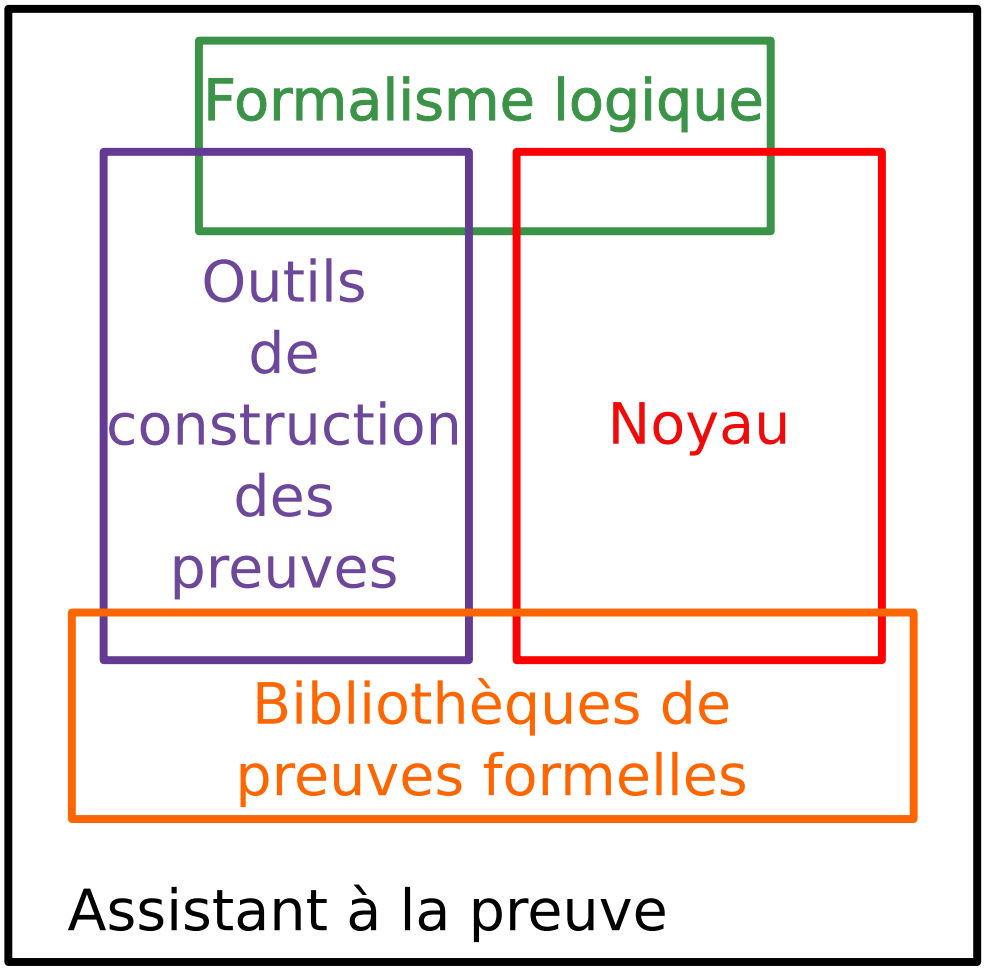
Irrationalité de $\zeta(3)$: du calcul formel aux preuves formelles

F. Chyzak, A. Mahboubi, Th. Sibut-Pinote, E. Tassi

Assistants de preuves



Dans cet exposé on utilise Coq : `http://coq.inria.fr`

Preuves formelles

- Composants critiques :
  - Formalisme logique
  - Implantation du noyau
  - Définitions formelle des objets de travail

Preuves formelles

- Composants critiques :
  - Formalisme logique
  - Implantation du noyau
  - Définitions formelle des objets de travail
- Bénéfices :
  - Sémantique explicite des objets formalisés
  - Correction assurée des preuves vérifiées

Preuves formelles

- Composants critiques :
  - Formalisme logique
  - Implantation du noyau
  - Définitions formelle des objets de travail
- Bénéfices :
  - Sémantique explicite des objets formalisés
  - Correction assurée des preuves vérifiées
- Limitations :
  - Difficulté du développement de bibliothèques formelles
  - Puissance de calcul limitée

Certification des résultats d'un calcul

- Certifier un programme:
  - Implanter l'algorithme dans la logique :

```
f : nat → bool
```

  - Prouver sa correction :

```
Theorem f_correct: ∀ x : nat, f x = true → prime x
```

  - Exemples:

    opérations arithmétiques, normalisations (`ring`, `field`)

[M., Grégoire (2005)]

Certification des résultats d'un calcul

- Certifier un programme:
  - Implanter l'algorithme dans la logique :

    ```
    f : nat → bool
    ```

  - Prouver sa correction :

    ```
    Theorem f_correct: ∀ x : nat, f x = true → prime x
    ```

  - Exemples:

    opérations arithmétiques, normalisations (`ring`, `field`)

    [M., Grégoire (2005)]

- Certifier les résultats d'un programme:
  - Programmer dans un langage de programmation adapté
  - Prouver la correction d'un vérificateur de certificat:

    ```
    Theorem f_check: ∀ (x : nat)(c : cert), f x c = true → prime x
    ```

  - Exemples: primalité, positivité par somme de carrés

    [Grégoire, Théry (2006); Besson (2007); Monniaux, Corbineau (2011)]

Suites ∂-finies

suites P-récursives (ou holonomiques, or ∂-finies)

Une suite $u := (u_n)_{n\in\mathbb{N}} \in \mathbb{C}^{\mathbb{N}}$ est P-récursive si pour tout $n \in \mathbb{N}$

$$p_r(n)u_{n+r} + \cdots + p_0(n)u_n = 0$$

où $p_i \in \mathbb{C}[n]$ sont des coefficients polynomiaux et $p_r \neq 0$.

- Les solutions de tels systèmes sont aussi P-récursives.
- La définition se généralise aux suites de plusieurs index.

[Chyzak, Salvy (1998)].

Clôtures: $+$, $\times$, Σ

Si u et v sont ∂-finies, on peut calculer:

- des récurrences qui caractérisent $(u + v)$;
- des récurrences qui caractérisent $(u \times v)$;
- des récurrences qui caractérisent $U_n := \sum_{k=0}^{n} u_{n,k}$.

Par exemple, on peut ainsi calculer un système caractérisant:

$$c_{n,k} := \binom{n}{k}^2 \binom{n+k}{k}^2 \left(\sum_{i=1}^{n} \frac{1}{i^3} + \sum_{m=1}^{k} \frac{(-1)^{m+1}}{2m^3 \binom{n}{m} \binom{n+m}{m}} \right)$$

[Zeilberger (1990); Wilf, Zeilberger (1992); Stanley (1997); Wegshaider (1997); Chyzak, Salvy (1998); Schneider (2008);...]

La constante d'Apéry

Le nombre réel $\zeta(3)$ est défini comme $\sum_{k=1}^{+\infty} \frac{1}{k^3}$.

Theorem (Apéry, 1978)

La constante $\zeta(3)$ est irrationnelle.

[van der Poorten (1979), Apéry (1979)]

Esquisse de la preuve

Apéry exhibe deux suites $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}} \in \mathbb{Q}^{\mathbb{N}}$ telles que :

- $a_n\zeta(3) - b_n \to 0$;
- $a_n\zeta(3) - b_n > 0$ pour n assez grand.

Esquisse de la preuve

Apéry exhibe deux suites $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}} \in \mathbb{Q}^{\mathbb{N}}$ telles que :

- $a_n\zeta(3) - b_n \to 0$;
- $a_n\zeta(3) - b_n > 0$ pour n assez grand.

De plus:

- $l_n = ppcm(1 \ldots n)$ croît très vite (comme e^n);
- $a_n\zeta(3) - b_n \to 0$ plus vite encore;
- de sorte que $2l_n^3(a_n\zeta(3) - b_n) \to 0$.

Esquisse de la preuve

En résumé:

- $2I_n^3(a_n\zeta(3) - b_n) \to 0$;
- $2I_n^3(a_n\zeta(3) - b_n) > 0$ pour n assez grand.

Mais si $\zeta(3) \in \mathbb{Q}$:

- $2I_n^3(a_n\zeta(3) - b_n) \in \mathbb{Z}$ pour n assez grand.

Ainsi $\zeta(3) \notin \mathbb{Q}$.

Esquisse de la preuve

En résumé:

- $2I_n^3(a_n\zeta(3) - b_n) \to 0$;
- $2I_n^3(a_n\zeta(3) - b_n) > 0$ pour n assez grand.

Mais si $\zeta(3) \in \mathbb{Q}$:

- $2I_n^3(a_n\zeta(3) - b_n) \in \mathbb{Z}$ pour n assez grand.

Ainsi $\zeta(3) \notin \mathbb{Q}$.

La mystérieuse récurrence d'Apéry

Point crucial de la preuve : $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ sont solutions de

$$(n+2)^3 y_{n+2} - (17n^2 + 51n + 39)(2n+3) y_{n+1} + (n+1)^3 y_n = 0$$

La mystérieuse récurrence d'Apéry

Point crucial de la preuve : $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ sont solutions de

$$(n+2)^3 y_{n+2} - (17n^2+51n+39)(2n+3)y_{n+1} + (n+1)^3 y_n = 0$$

avec:

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

Preuves alternatives

- Preuves papier :
  Beukers (1979, 1987), Nesterenko (1996), Rajkumar (2012), ...
- Preuves algorithmiques :
  Zeilberger (1993), Zudilin (2002, 2009), Salvy (2003), Schneider (2007), ...

Calculer la récurrence d'Apéry

$$a_n = \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2, \quad b_n = \sum_{k=1}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2 \left(\sum_{m=1}^{n} \frac{1}{m^3} + \sum_{m=1}^{k} \frac{(-1)^{m+1}}{2m^3 \binom{n}{m} \binom{n+m}{m}} \right).$$

étape	forme explicite	système	opération	entrée(s)
1	$c_{n,k} = \binom{n}{k}^2 \binom{n+k}{k}^2$	C	direct	
2	$a_n = \sum_{k=1}^{n} c_{n,k}$	A	Σ	C
3	$d_{n,m} = \frac{(-1)^{m+1}}{2m^3 \binom{n}{m} \binom{n+m}{m}}$	D	direct	
4	$s_{n,k} = \sum_{m=1}^{k} d_{n,m}$	S	Σ	D
5	$z_n = \sum_{m=1}^{n} \frac{1}{m^3}$	Z	direct	
6	$u_{n,k} = z_n + s_{n,k}$	U	$+$	Z et S
7	$v_{n,k} = c_{n,k} u_{n,k}$	V	$\times$	C et U
8	$b_n = \sum_{k=1}^{n} v_{n,k}$	B	Σ	V

Calculer la récurrence d'Apéry

$$a_n = \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2, \quad b_n = \sum_{k=1}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2 \left(\sum_{m=1}^{n} \frac{1}{m^3} + \sum_{m=1}^{k} \frac{(-1)^{m+1}}{2m^3 \binom{n}{m} \binom{n+m}{m}} \right).$$

étape	forme explicite	système	opération	entrée(s)
1	$c_{n,k} = \binom{n}{k}^2 \binom{n+k}{k}^2$	C	direct	
2	$a_n = \sum_{k=1}^{n} c_{n,k}$	A	Σ	C
3	$d_{n,m} = \frac{(-1)^{m+1}}{2m^3 \binom{n}{m} \binom{n+m}{m}}$	D	direct	
4	$s_{n,k} = \sum_{m=1}^{k} d_{n,m}$	S	Σ	D
5	$z_n = \sum_{m=1}^{n} \frac{1}{m^3}$	Z	direct	
6	$u_{n,k} = z_n + s_{n,k}$	U	$+$	Z et S
7	$v_{n,k} = c_{n,k} u_{n,k}$	V	$\times$	C et U
8	$b_n = \sum_{k=1}^{n} v_{n,k}$	B	Σ	V

Calculer la récurrence d'Apéry

$$a_n = \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2, \quad b_n = \sum_{k=1}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2 \left(\sum_{m=1}^{n} \frac{1}{m^3} + \sum_{m=1}^{k} \frac{(-1)^{m+1}}{2m^3 \binom{n}{m} \binom{n+m}{m}} \right).$$

étape	forme explicite	système	opération	entrée(s)
1	$c_{n,k} = \binom{n}{k}^2 \binom{n+k}{k}^2$	C	direct	
2	$a_n = \sum_{k=1}^{n} c_{n,k}$	A	Σ	C
3	$d_{n,m} = \frac{(-1)^{m+1}}{2m^3 \binom{n}{m} \binom{n+m}{m}}$	D	direct	
4	$s_{n,k} = \sum_{m=1}^{k} d_{n,m}$	S	Σ	D
5	$z_n = \sum_{m=1}^{n} \frac{1}{m^3}$	Z	direct	
6	$u_{n,k} = z_n + s_{n,k}$	U	$+$	Z et S
7	$v_{n,k} = c_{n,k} u_{n,k}$	V	$\times$	C et U
8	$b_n = \sum_{k=1}^{n} v_{n,k}$	B	Σ	V

Calculer la récurrence d'Apéry

$$a_n = \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2, \quad b_n = \sum_{k=1}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2 \left(\sum_{m=1}^{n} \frac{1}{m^3} + \sum_{m=1}^{k} \frac{(-1)^{m+1}}{2m^3 \binom{n}{m} \binom{n+m}{m}} \right).$$

étape	forme explicite	système	opération	entrée(s)
1	$c_{n,k} = \binom{n}{k}^2 \binom{n+k}{k}^2$	C	direct	
2	$a_n = \sum_{k=1}^{n} c_{n,k}$	A	Σ	C
3	$d_{n,m} = \frac{(-1)^{m+1}}{2m^3 \binom{n}{m} \binom{n+m}{m}}$	D	direct	
4	$s_{n,k} = \sum_{m=1}^{k} d_{n,m}$	S	Σ	D
5	$z_n = \sum_{m=1}^{n} \frac{1}{m^3}$	Z	direct	
6	$u_{n,k} = z_n + s_{n,k}$	U	$+$	Z et S
7	$v_{n,k} = c_{n,k} u_{n,k}$	V	$\times$	C et U
8	$b_n = \sum_{k=1}^{n} v_{n,k}$	B	Σ	V

Calculer la récurrence d'Apéry

$$a_n = \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2, \quad b_n = \sum_{k=1}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2 \times \left(\sum_{m=1}^{n} \frac{1}{m^3} + \sum_{m=1}^{k} \frac{(-1)^{m+1}}{2m^3 \binom{n}{m} \binom{n+m}{m}} \right).$$

étape	forme explicite	système	opération	entrée(s)
1	$c_{n,k} = \binom{n}{k}^2 \binom{n+k}{k}^2$	C	direct	
2	$a_n = \sum_{k=1}^{n} c_{n,k}$	A	Σ	C
3	$d_{n,m} = \frac{(-1)^{m+1}}{2m^3 \binom{n}{m} \binom{n+m}{m}}$	D	direct	
4	$s_{n,k} = \sum_{m=1}^{k} d_{n,m}$	S	Σ	D
5	$z_n = \sum_{m=1}^{n} \frac{1}{m^3}$	Z	direct	
6	$u_{n,k} = z_n + s_{n,k}$	U	$+$	Z et S
7	$v_{n,k} = c_{n,k} u_{n,k}$	V	$\times$	C et U
8	$b_n = \sum_{k=1}^{n} v_{n,k}$	B	Σ	V

Calculer la récurrence d'Apéry

$$a_n = \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2, \quad b_n = \sum_{k=1}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2 \left(\sum_{m=1}^{n} \frac{1}{m^3} + \sum_{m=1}^{k} \frac{(-1)^{m+1}}{2m^3 \binom{n}{m} \binom{n+m}{m}} \right).$$

étape	forme explicite	système	opération	entrée(s)
1	$c_{n,k} = \binom{n}{k}^2 \binom{n+k}{k}^2$	C	direct	
2	$a_n = \sum_{k=1}^{n} c_{n,k}$	A	Σ	C
3	$d_{n,m} = \frac{(-1)^{m+1}}{2m^3 \binom{n}{m} \binom{n+m}{m}}$	D	direct	
4	$s_{n,k} = \sum_{m=1}^{k} d_{n,m}$	S	Σ	D
5	$z_n = \sum_{m=1}^{n} \frac{1}{m^3}$	Z	direct	
6	$u_{n,k} = z_n + s_{n,k}$	U	$+$	Z et S
7	$v_{n,k} = c_{n,k}\, u_{n,k}$	V	$\times$	C et U
8	$b_n = \sum_{k=1}^{n} v_{n,k}$	B	Σ	V

Vérification de récurrences

Utilisons:

$$\binom{n+1}{k} = \frac{n+1}{n+1-k}\binom{n}{k}, \quad \binom{n}{k+1} = \frac{n-k}{k+1}\binom{n}{k}$$

Vérification de récurrences

Utilisons:

$$\binom{n+1}{k} = \frac{n+1}{n+1-k}\binom{n}{k}, \quad \binom{n}{k+1} = \frac{n-k}{k+1}\binom{n}{k}$$

pour montrer la récurrence du triangle de Pascal:

$$\begin{aligned}
\binom{n+1}{k+1} - \binom{n}{k+1} - \binom{n}{k} &= \\
\left(\frac{n+1}{n-k}\frac{n-k}{k+1} - \frac{n-k}{k+1} - 1\right)\binom{n}{k} &= \\
0 \times \binom{n}{k} &= \\
0.
\end{aligned}$$

Vérification de récurrences

Utilisons:

$$\binom{n+1}{k} = \frac{n+1}{n+1-k}\binom{n}{k}, \quad \binom{n}{k+1} = \frac{n-k}{k+1}\binom{n}{k}$$

pour montrer la récurrence du triangle de Pascal:

$$\begin{aligned}
\binom{n+1}{k+1} - \binom{n}{k+1} - \binom{n}{k} &= \\
\left(\frac{n+1}{n-k}\frac{n-k}{k+1} - \frac{n-k}{k+1} - 1\right)\binom{n}{k} &= \\
0 \times \binom{n}{k} &= \\
0.
\end{aligned}$$

pour $n \neq k, k+1 \neq 0$

Vérification de récurrences

On veut vérifier $(P.U)_n = 0$:

- avec $U_n = \sum_{k=0}^{n} u_{n,k}$;
- avec $(P.x)_n = p_r(n)x_{n+r} + \ldots p_0(n)x_n$;
- en connaissant un système caractérisant u.

Cas favorable: $(P.u_{\_,k})_n = w_{k+1} - w_k$

Vérification de récurrences

On veut vérifier $(P.U)_n = 0$:

- avec $U_n = \sum_{k=0}^{n} u_{n,k}$;
- avec $(P.x)_n = p_r(n)x_{n+r} + \ldots p_0(n)x_n$;
- en connaissant un système caractérisant u.

Cas favorable: $(P.u_{\_,k})_n = w_{k+1} - w_k$

- $\sum_{k=0}^{n}(P.u_{\_,k})_n = P(\sum_{k=0}^{n} u_{n,k}) + P_{border}.(u_{\_,k})_n$

Vérification de récurrences

On veut vérifier $(P.U)_n = 0$:

- avec $U_n = \sum_{k=0}^{n} u_{n,k}$;
- avec $(P.x)_n = p_r(n)x_{n+r} + \ldots p_0(n)x_n$;
- en connaissant un système caractérisant u.

Cas favorable: $(P.u_{\_,k})_n = w_{k+1} - w_k$

- $\sum_{k=0}^{n}(P.u_{\_,k})_n = P(\sum_{k=0}^{n} u_{n,k}) + P_{border}.(u_{\_,k})_n$
- $= (P.U)_n + (P_{border}.u_{\_,k})_n$

Vérification de récurrences

On veut vérifier $(P.U)_n = 0$:

- avec $U_n = \sum_{k=0}^{n} u_{n,k}$;
- avec $(P.x)_n = p_r(n)x_{n+r} + \ldots p_0(n)x_n$;
- en connaissant un système caractérisant u.

Cas favorable: $(P.u_{\_,k})_n = w_{k+1} - w_k$

- $\sum_{k=0}^{n}(P.u_{\_,k})_n = P(\sum_{k=0}^{n} u_{n,k}) + P_{border}.(u_{\_,k})_n$
- $= (P.U)_n + (P_{border}.u_{\_,k})_n$
- $= w_{n+1} - w_0$ (par télescopage)

Vérification de récurrences

On veut vérifier $(P.U)_n = 0$:

- avec $U_n = \sum_{k=0}^{n} u_{n,k}$;
- avec $(P.x)_n = p_r(n)x_{n+r} + \ldots p_0(n)x_n$;
- en connaissant un système caractérisant u.

Cas favorable: $(P.u_{\_,k})_n = w_{k+1} - w_k$

- $\sum_{k=0}^{n}(P.u_{\_,k})_n = P(\sum_{k=0}^{n} u_{n,k}) + P_{border}.(u_{\_,k})_n$
- $= (P.U)_n + (P_{border}.u_{\_,k})_n$
- $= w_{n+1} - w_0$ (par télescopage)

Si de plus $w_{n+1} - w_0 - (P_{border}.u_{\_,k})_n = 0$, alors $(P.U)_n = 0$.

Vérification de récurrences

Les algorithmes de création télescopique établissent $(P.U)_n = 0$ en produisant un certificat Q:

$$(i) \quad (P.u\_,_k)_n = (Q.u)_{n,k+1} - (Q.u)_{n,k}$$

Ils promettent de plus que:

$$(ii) \quad (Q.u)_{n+1} - (Q.u)_n - (P_{rem}.u\_,_k) = 0$$

Vérification de récurrences

Les algorithmes de création télescopique établissent $(P.U)_n = 0$ en produisant un certificat Q:

$$(i) \quad (P.u\_,_k)_n = (Q.u)_{n,k+1} - (Q.u)_{n,k}$$

Ils promettent de plus que:

$$(ii) \quad (Q.u)_{n+1} - (Q.u)_n - (P_{rem}.u\_,_k) = 0$$

Ainsi

- Vérifier (i) et (ii) prouve $(P.U)_n = 0$;
- Ces vérifications sont faisables en connaissant les récurrences caractérisant u.

Vérification de la récurrence d'Apéry

étape	forme explicite	GB	opération	vérifiée avec
8	$b_n = \sum_{k=1}^{n} v_{n,k}$	B	télescopage créatif	V
7	$v_{n,k} = c_{n,k}\, u_{n,k}$	V	produit	C et U
6	$u_{n,k} = z_n + s_{n,k}$	U	addition	Z et S
5	$z_n = \sum_{m=1}^{n} \frac{1}{m^3}$	Z	direct	
4	$s_{n,k} = \sum_{m=1}^{k} d_{n,m}$	S	télescopage créatif	D
3	$d_{n,m} = \frac{(-1)^{m+1}}{2m^3 \binom{n}{m} \binom{n+m}{m}}$	D	direct	
2	$a_n = \sum_{k=1}^{n} c_{n,k}$	A	télescopage créatif	C
1	$c_{n,k} = \binom{n}{k}^2 \binom{n+k}{k}^2$	C	direct	

Opérateurs de récurrences formels

On note $\mathcal{A} = \mathbb{Q}(n,k)\langle S_n, S_k\rangle$ l'anneau des polynômes:

- en les indéterminées S_n et S_k (qui commutent)
- à coefficients dans $\mathbb{Q}(n,k)$
- avec la règle de commutation:

$$S_n^i S_k^j c(n,k) = c(n+i,k+j) S_n^i S_k^j.$$

Les éléments de $\mathcal{A}$ peuvent être vus comme les représentations algébriques des récurrences linéaires à coefficients dans les fractions rationnelles.

Opérateurs de récurrences formels

Considérons

- $P = \sum_{(i,j)\in I} p_{i,j}(n,k) S_n^i S_k^j \in \mathcal{A}$,
- f une suite (ou plutôt un germe de suite).

- L'opérateur P agit sur f :

$$(P \cdot f)_{n,k} = \sum_{(i,j)\in I} p_{i,j}(n,k) f_{n+i,k+j}$$

- On sait calculer une base de Gröbner pour l'idéal:

$$\mathcal{I}_f := \{P \mid P \cdot f = 0\}$$

Un détail?

Utilisons:

$$\binom{n+1}{k} = \frac{n+1}{n+1-k}\binom{n}{k}, \quad \binom{n}{k+1} = \frac{n-k}{k+1}\binom{n}{k}$$

pour montrer la récurrence du triangle de Pascal:

$$\begin{aligned}
\binom{n+1}{k+1} - \binom{n}{k+1} - \binom{n}{k} &= \\
\left(\frac{n+1}{n-k}\frac{n-k}{k+1} - \frac{n-k}{k+1} - 1\right)\binom{n}{k} &= \\
0 \times \binom{n}{k} &= \\
0.
\end{aligned}$$

pour $n \neq k, k+1 \neq 0$

Certificats de création télescopique

$$(n,k) \in \Delta \Rightarrow (P \cdot u_{\_,k})_n = (Q \cdot u)_{n,k+1} - (Q \cdot u)_{n,k}$$

Certificats de création télescopique

$$(n,k) \in \Delta \Rightarrow (P \cdot u_{\_,k})_n = (Q \cdot u)_{n,k+1} - (Q \cdot u)_{n,k}$$

On peut prouver pour $U_n = \sum_{k=\alpha}^{n+\beta} u_{n,k}$ que:

Certificats de création télescopique

$$(n,k) \in \Delta \Rightarrow (P \cdot u_{\_,k})_n = (Q \cdot u)_{n,k+1} - (Q \cdot u)_{n,k}$$

On peut prouver pour $U_n = \sum_{k=\alpha}^{n+\beta} u_{n,k}$ que:

$$(P \cdot U)_n = \Big((Q \cdot u)_{n,n+\beta+1} - (Q \cdot u)_{n,\alpha} \Big) \qquad \text{(télescope)}$$

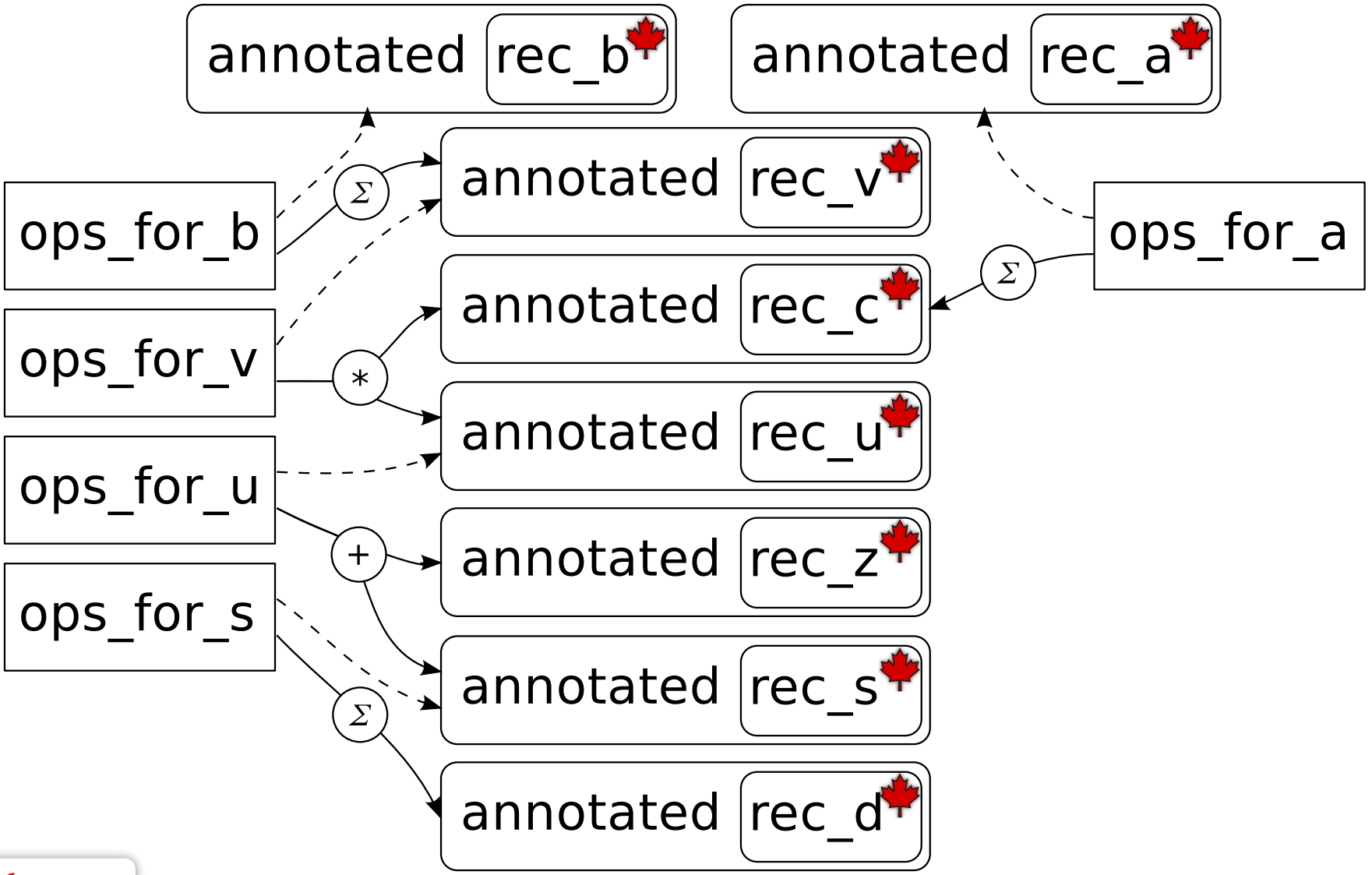
$$+ \sum_{i=1}^{r} \sum_{j=1}^{i} p_i(n)\, u_{n+i,n+\beta+j} \qquad \text{(bord)}$$

$$+ \sum_{\substack{\alpha \le k \le n+\beta \\ (n,k) \notin \Delta}} (P \cdot u_{\_,k})_n - (Q \cdot u)_{n,k+1} + (Q \cdot u)_{n,k} \qquad \text{(hors } \Delta\text{)}$$

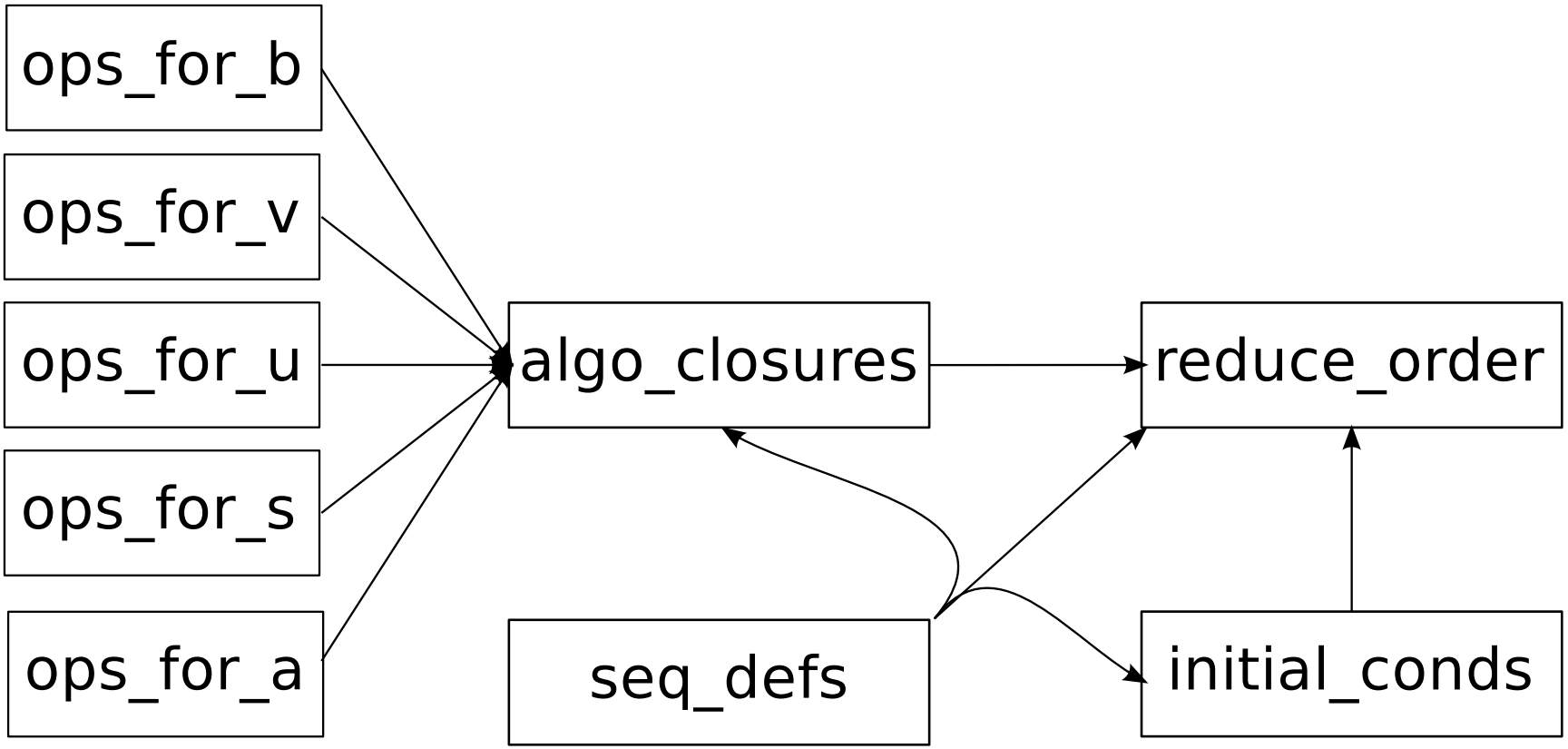
Récurrences gardées

- Les opérateurs de récurrences sont annotés par des conditions de validités.
- Ces conditions dépendent (a priori) du chemin de preuve.
- Elle ne se lisent pas (seulement) sur énoncé de la récurrence à prouver.
- On perd les bonnes propriétés de normalisation.
- On perd l'automatisation de la vérification.

Schéma général du développement



Preuve complète de la récurrence



Bilan

- Traduction automatisée d'une session Maple en conjectures pour Coq;
- Procédure systématique d'annotation par des gardes;
- Normalisation manuelle;
- Automatisation des preuves formelles de conditions et des normalisations de fractions rationnelles.

Conclusion

Preuves de récurrences:

- Une méthode systématique mais pas automatique;
- Un prototype utilisable pour d'autres récurrences;
- Pas d'automatisation sans une meilleur compréhension des algorithmes;

[Kauers (2011), Harrison (2014), Lairez (2014),...?]

- Cadre différentiel?

Conclusion

Preuves de récurrences:

- Une méthode systématique mais pas automatique;
- Un prototype utilisable pour d'autres récurrences;
- Pas d'automatisation sans une meilleur compréhension des algorithmes;

[Kauers (2011), Harrison (2014), Lairez (2014),...?]

- Cadre différentiel?

Preuve de l'irrationalité de $\zeta(3)$:

- Bibliothèques de théorie des nombres élémentaire;
- Raisonnements sur les propriétés asymptotiques;
- Estimation de l'asymptotique de $ppcm(1 \ldots n)$ en cours de formalisation.