INSTITUT
DE RECHERCHE
EN INFORMATIQUE
FONDAMENTALE

Université Paris Cité

cnrs

Inria

Équipe Preuves Et Programmes

Responsable : Claudia Faggian

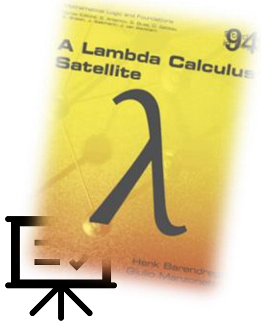
11.5 permanents: 1.5 PR, 1.5 DR, 5.1 MdC, 1.3 CR
0.6 ATER, 0 PostDoc, 10.6 Doc, 1 Émérites
Total : 23.8 membres

Thématiques et enjeux (1/2)

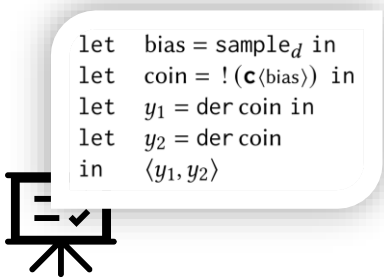
Investigating programming languages and logical formalisms, with operational viewpoint

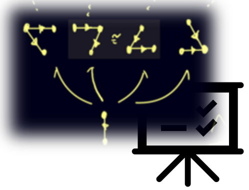
❑ Models of computation, λ-calculi, rewriting

Behr, Bernardi, Ehrhard, Faggian, Férée, Joly, Kesner,
Krivine, Melliès, Padovani, Parigot, Rozière, Saurin



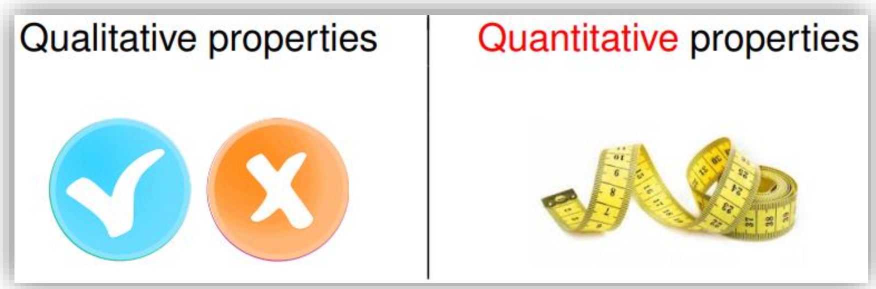
- *Theory of the λ-calculus*
- *Call by-Name / Call by-Value / Call by-Need*
- *Operational theory of probabilistic and effectful computation*
- *Theory of rewriting: terms, graphs, proof-nets*





❑ Type Systems

Amadio, Castagna, Bucciarelli, Ehrhard, Faggian, Guatto, Kesner, Pagani



Thématiques et enjeux (2/2)

❑ Proof theory and computation

Geoffroy, Herbelin

Computing with the axiom of choice?

We know for several decades how to compute with variants of excluded-middle or even the axiom of dependent choice using side effects.

classical reasoning	=	control operators (with some typing)
negative translations	=	continuation-passing-style translations
minimal classical natural deduction	=	typed Parigot's $\lambda\mu$-calculus
classical natural deduction	=	typed $\lambda\mu tp$-calculus
sequent calculus	=	typed $\mu\tilde{\mu}$-calculus (= abstract machine)
Peirce's law	$\simeq$	Scheme's `callcc`
Ex Falso Quodlibet	$\simeq$	Felleisen's $\mathcal{A}bort$ (with some typing)

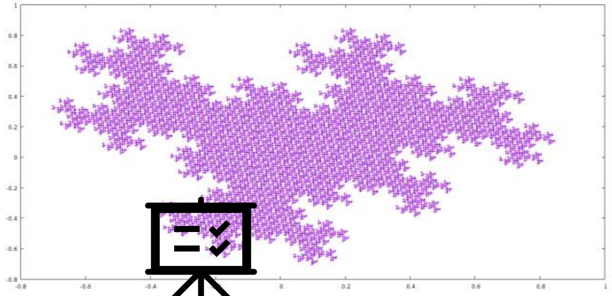
- *Classical realisability*
- *Reverse mathematics of the axiom of choice, Computational contents of separability axioms.*

❑ Dependent type theory

Gallego, Letouzey, Herbelin, Melliès, Saurin, Sozeau

Linked to the foundations and development of the Coq proof assistant

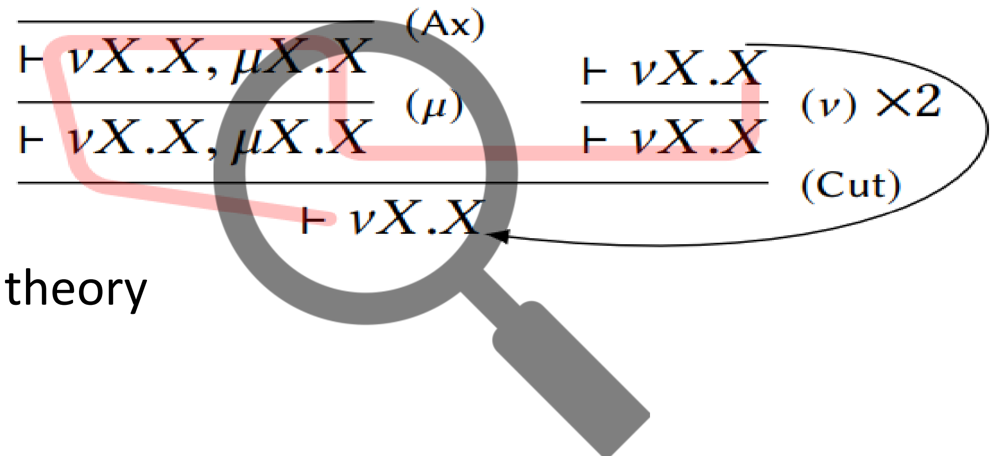
A formalism connecting computer science, logic, geometry and algebra



❑ Structural Proofs for Fixed-point Logics

(co)induction, circular proofs, guarded proofs

Guatto, Saurin



Good foundations for the non well-founded proof theory

Vie et organisation

Scientific life:

- Weekly: PPS seminar
- Journées de Rentrée (Autumn), Journées PPS (Spring)
- Specific working groups:
  Type theory and realisability, Syntax Meets Semantics
- National context:
  - Chocola, GDR Informatique Mathématique (GT Scalp)

Decisions:

- Monthly PPS AG
- Collective coordination among the 4 heads of teams & pole

Faits marquants

- PhD students: currently 20 (most within at least two teams)

  22 PhD Thesis completed in the period

  Prix Gilles Kahn & Ackermann Award 2018 (A. Doumane)

- Scientific production:

Two "Best Student Paper Award" at LICS

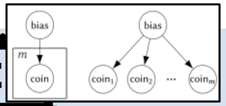
	By affiliation	Pro rata
Int. Conferences	138	80
Int. Journals	88	47

- Structuring projects:
  - **International**: *IRP SINFIN* (CNRS, FR-Argentina), *Crecogi INRIA-JSPS* Associated Team (FR-Japan), EuTypes & *EuroProofNet* (COST actions, EU)
  - **4 ANRs**
  - Inria team **Picube** (πr^2 + formalization of mathematics)

Projection

Team head from 2024: Alexis Saurin

- Models of computation, λ-calculi, rewriting
- Quantitative Type Systems



- Higher-Order Bayesian Networks
- Quantitative effectful programming
- Quantitative CPS translations.
- Coherent differentiation (logical and operational meaning)
- Complexity analysis for higher-order programs
- Solvability in call-by-push-value.
- Tracelet Analysis in the Life Sciences.

$$\sum_{n=0}^{\infty} \frac{1}{n!}\left(\frac{\partial^n P}{\partial x^n}\cdot(\underbrace{Q,\dots,Q}_{\text{n times}})\right)[0/x]$$

- Proof theory and computation
- Dependent type theory

- Understanding the computational contents of choice principles.
- Propositions-as-types-as-categories-as-spaces correspondence.
- Coq-based Rewriting: Towards Executable Applied Category Theory.

- Structural Proofs for Fixed-point Logics

- Finitization problems and denotational semantics of circular proofs.
- Enriching the shape of circular proofs.
- Formalization of the theory of fixed-point logic proof theory.
- Compositionality of circular proofs and circular typing derivation.

Besoins

- Rank A recrutement is essential

$$\frac{rank\ A}{permanents} = \frac{1}{4}$$

▶ a pb common to all PPS:

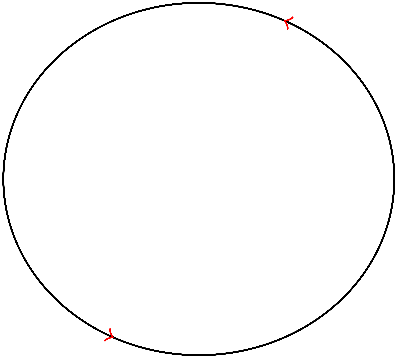
4 PR + 4 DR   within   31 permanents

- Enseignants-chercheurs: time !
    - +72% students in 12 years / same ECs
    - increased administrative responsabilities load
    - décharges well below Référentiel National
      (eg: Master 20h vs 24h-60h, License 20h vs 24h-128h)

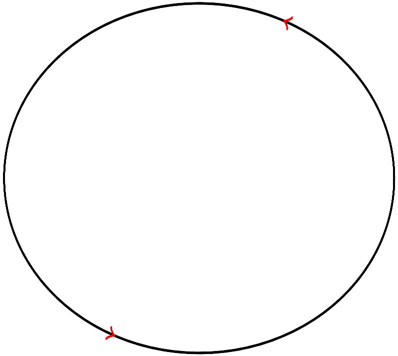
Focus scientifique

(by Alexis Saurin)

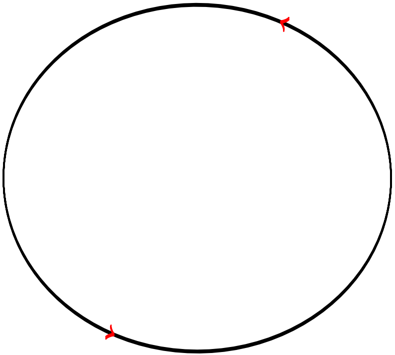
Focus : Rebonds dans les preuves circulaires



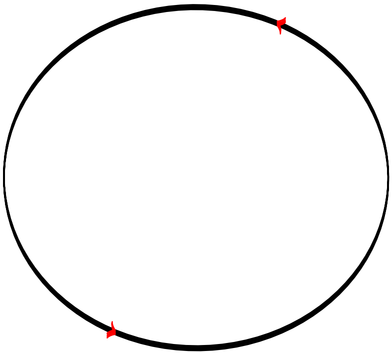
Focus : Rebonds dans les preuves circulaires



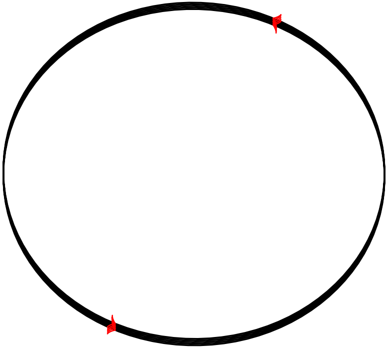
Focus : Rebonds dans les preuves circulaires



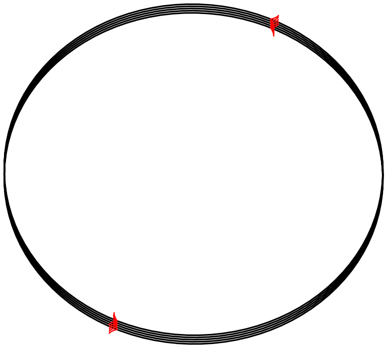
Focus : Rebonds dans les preuves circulaires



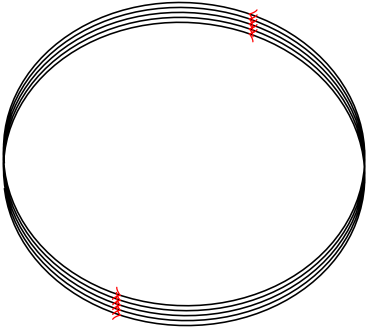
Focus : Rebonds dans les preuves circulaires



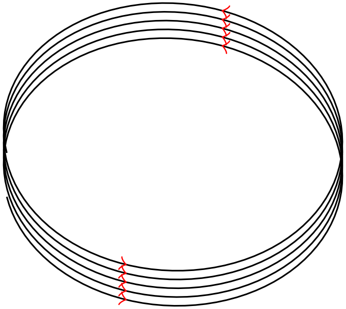
Focus : Rebonds dans les preuves circulaires



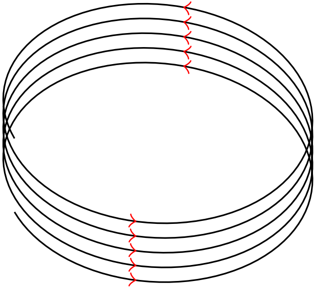
Focus : Rebonds dans les preuves circulaires



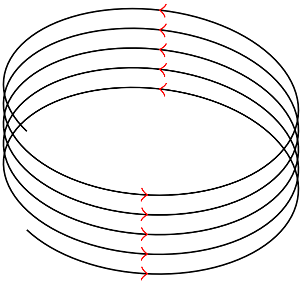
Focus : Rebonds dans les preuves circulaires



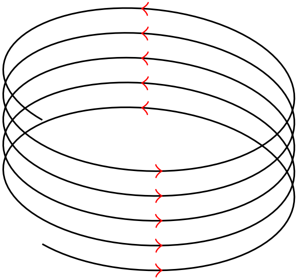
Focus : Rebonds dans les preuves circulaires



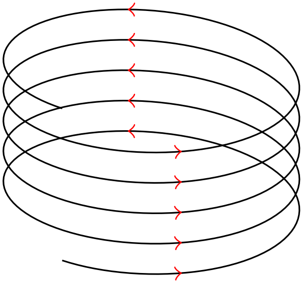
Focus : Rebonds dans les preuves circulaires



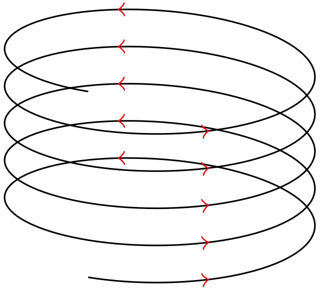
Focus : Rebonds dans les preuves circulaires



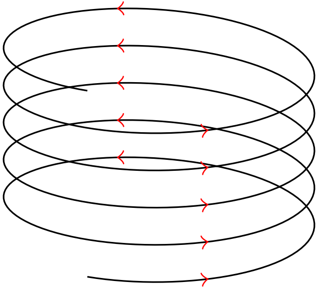
Focus : Rebonds dans les preuves circulaires



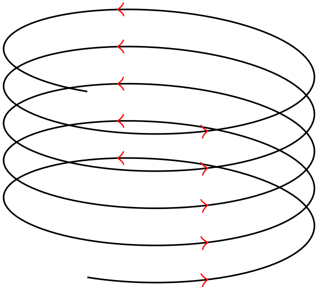
Focus : Rebonds dans les preuves circulaires



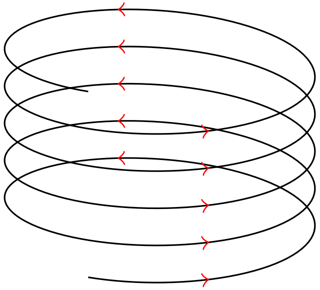
Focus : Rebonds dans les preuves circulaires



Focus : Rebonds dans les preuves circulaires



Focus : Rebonds dans les preuves circulaires



De la descente infinie aux preuves circulaires

Une vieille histoire mathématique, déjà dans les *Éléments* d'Euclide (Livre VII)

PROPOSITION 31

Any composite number is measured by some prime number.

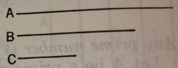
Let A be a composite number;

I say that A is measured by some prime number.

For, since A is composite,

some number will measure it.

Let a number measure it, and let it be B.



Now, if B is prime, what was enjoined will have been done.

But if it is composite, some number will measure it.

Let a number measure it, and let it be C.

Then, since C measures B,

and B measures A,

therefore C also measures A.

And, if C is prime, what was enjoined will have been done.

But if it is composite, some number will measure it.

Thus, if the investigation be continued in this way, some prime number will be found which will measure the number before it, which will also measure A.

For, if it is not found, an infinite series of numbers will measure the number A, each of which is less than the other:

which is impossible in numbers.

Therefore some prime number will be found which will measure the one before it, which will also measure A.

Therefore any composite number is measured by some prime number.

Q. E. D.

De la descente infinie aux preuves circulaires

Une vieille histoire mathématique, déjà dans les *Éléments* d'Euclide (Livre VII)

PROPOSITION 31

Any composite number is measured by some prime number.

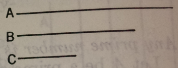
Let A be a composite number;

I say that A is measured by some prime number.

For, since A is composite,

some number will measure it.

Let a number measure it, and let it be B.



Now, if B is prime, what was enjoined will have been done.

But if it is composite, some number will measure it.

Let a number measure it, and let it be C.

Then, since C measures B,

and B measures A,

therefore C also measures A.

And, if C is prime, what was enjoined will have been done.

But if it is composite, some number will measure it.

Thus, if the investigation be continued in this way, some prime number will be found which will measure the number before it, which will also measure A.

For, if it is not found, an infinite series of numbers will measure the number A, each of which is less than the other:

which is impossible in numbers.

Therefore some prime number will be found which will measure the one before it, which will also measure A.

Therefore any composite number is measured by some prime number.

Q. E. D.

Origine de la méthode de **descente infinie** de Fermat.

De la descente infinie aux preuves circulaires

Une vieille histoire mathématique : Fermat identifie une puissante heuristique

Pierre de Fermat a étudié en profondeur la descente infinie et l'utilisant largement. Voir la lettre d'août 1659 à Carcavaci où Fermat dresse une liste de 10 théorèmes qu'il a démontrés avec la descente infinie :

1. *Aucun nombre de la forme, moindre de l'unité qu'un multiple de 3, ne peut être composé d'un carré et du triple d'un autre carré.*
2. *Aucun triangle rectangle en nombres n'a une aire carrée.*
3. *Tout nombre premier qui surpasse de l'unité un multiple de 4 est somme de deux carrés.*

(...)

9. *Toutes les puissances carrées de 2, augmentées de 1, sont des nombres premiers.*
10. *Il n'y a que 1 et 7 qui sont moindres de 1 qu'un double carré et aient un carré de même nature.*

De la descente infinie aux preuves circulaires

Une vieille histoire mathématique : Fermat identifie une puissante heuristique

Pierre de Fermat a étudié en profondeur la descente infinie et l'utilisant largement. Voir la lettre d'août 1659 à Carcavaci où Fermat dresse une liste de 10 théorèmes qu'il a démontrés avec la descente infinie :

1. *Aucun nombre de la forme, moindre de l'unité qu'un multiple de 3, ne peut être composé d'un carré et du triple d'un autre carré.*
2. *Aucun triangle rectangle en nombres n'a une aire carrée.*
3. *Tout nombre premier qui surpasse de l'unité un multiple de 4 est somme de deux carrés.*

(...)

9. *Toutes les puissances carrées de 2, augmentées de 1, sont des nombres premiers.*
10. *Il n'y a que 1 et 7 qui sont moindres de 1 qu'un double carré et aient un carré de même nature.*

... **et qui contient même des énoncés faux !**

(La propriété 9 affirme que tout nombre de Fermat est premier, ce qui sera plus tard réfuté par Euler qui factorisera – à la main ! – $F_5 = 2^{2^5} + 1$ *comme le produit* $641 \times 6,700,417$*.)*

1. Supposons $\sqrt{2}$ rationnel : il existe alors $x_0 > x_1 \in \mathbb{N}^\star$ tels que $x_0^2 = 2x_1^2$;
2. x_0^2 et x_0, sont pairs : il existe x_2 tel que $x_0 = 2x_2$, d'où $x_1^2 = 2x_2^2$ et $x_1 > x_2$;
3. d'où l'existence d'une suite strictement décroissante dans $\mathbb{N}^\star$, ce qui n'est pas ;
4. on en déduit que $\sqrt{2}$ n'est pas rationnel.

De la descente infinie aux preuves circulaires

Vers le calcul des séquents : irrationalité de $\sqrt{2}$

1. Supposons $\sqrt{2}$ rationnel : il existe alors $x_0 > x_1 \in \mathbb{N}^\star$ tels que $x_0^2 = 2x_1^2$;
2. x_0^2 et x_0, sont pairs : il existe x_2 tel que $x_0 = 2x_2$, d'où $x_1^2 = 2x_2^2$ et $x_1 > x_2$;
3. d'où l'existence d'une suite strictement décroissante dans $\mathbb{N}^\star$, ce qui n'est pas ;
4. on en déduit que $\sqrt{2}$ n'est pas rationnel.

$$
\dfrac{
\dfrac{
\dfrac{}{\begin{array}{c}0 < x_0, x_0^2 = 2x_1^2 \vdash \\ 0 < x_1 < x_0 \wedge \\ \exists x_2 . x_0 = 2x_2\end{array}}
\qquad
\dfrac{
\dfrac{
\dfrac{
\dfrac{}{\begin{array}{c}0 < x_1, x_1^2 = 2x_2^2 \vdash \\ 0 < x_2 < x_1 \wedge \\ \exists x_3 . x_1 = 2x_3\end{array}}
\qquad
\dfrac{
\dfrac{
\dfrac{}{\begin{array}{c}0 < x_2, x_2^2 = 2x_3^2 \vdash \\ 0 < x_3 < x_2 \wedge \\ \exists x_4 . x_2 = 2x_4\end{array}}
\qquad
\dfrac{
\dfrac{\vdots}{0 < x_3, x_4^2 = 2x_4^2 \vdash \bot}\,(\text{Cut})
}{\underline{x_3 < x_2}, 0 < x_3, 4x_4^2 = 2x_3^2 \vdash \bot}
}{0 < x_2, x_2^2 = 2x_3^2 \vdash \bot}\,(\text{Cut})
}{\underline{x_2 < x_1}, 0 < x_2, 4x_3^2 = 2x_2^2 \vdash \bot}
}{0 < x_1, x_1^2 = 2x_2^2 \vdash \bot}\,(\text{Cut})
}{\underline{x_1 < x_0}, 0 < x_1, 4x_2^2 = 2x_1^2 \vdash \bot}
}{0 < x_0, x_0^2 = 2x_1^2, 0 < x_1 < x_0 \wedge \exists x_2 . x_0 = 2x_2 \vdash \bot}
}{0 < x_0, x_0^2 = 2x_1^2 \vdash \bot}\,(\text{Cut})
}{\vdash \neg(\exists x_0, x_1 . 0 < x_0 \wedge x_0^2 = 2x_1^2)}
$$

De la descente infinie aux preuves circulaires

Vers le calcul des séquents : irrationalité de $\sqrt{2}$

1. Supposons $\sqrt{2}$ rationnel : il existe alors $x_0 > x_1 \in \mathbb{N}^\star$ tels que $x_0^2 = 2x_1^2$;
2. x_0^2 et x_0, sont pairs : il existe x_2 tel que $x_0 = 2x_2$, d'où $x_1^2 = 2x_2^2$ et $x_1 > x_2$;
3. d'où l'existence d'une suite strictement décroissante dans $\mathbb{N}^\star$, ce qui n'est pas ;
4. on en déduit que $\sqrt{2}$ n'est pas rationnel.

$$\dfrac{\dfrac{\dfrac{}{\begin{array}{c}0<x_0,x_0^2=2x_1^2\vdash\\ 0<x_1<x_0\wedge\\ \exists x_2.x_0=2x_2\end{array}} \quad \dfrac{\dfrac{\dfrac{\dfrac{}{\begin{array}{c}0<x_1,x_1^2=2x_2^2\vdash\\ 0<x_2<x_1\wedge\\ \exists x_3.x_1=2x_3\end{array}} \quad \dfrac{\dfrac{\dfrac{}{\begin{array}{c}0<x_2,x_2^2=2x_3^2\vdash\\ 0<x_3<x_2\wedge\\ \exists x_4.x_2=2x_4\end{array}} \quad \dfrac{\dfrac{\vdots}{0<x_3,x_4^2=2x_4^2\vdash\bot}\,(\text{Cut})}{\underline{x_3<x_2},0<x_3,4x_4^2=2x_3^2\vdash\bot}}{0<x_2,x_2^2=2x_3^2\vdash\bot}\,(\text{Cut})}{\underline{x_2<x_1},0<x_2,4x_3^2=2x_2^2\vdash\bot}}{0<x_1,x_1^2=2x_2^2\vdash\bot}\,(\text{Cut})}{\underline{x_1<x_0},0<x_1,4x_2^2=2x_1^2\vdash\bot}}{0<x_0,x_0^2=2x_1^2,0<x_1<x_0\wedge\exists x_2.x_0=2x_2\vdash\bot}}{0<x_0,x_0^2=2x_1^2\vdash\bot}\,(\text{Cut})}{\vdash\neg(\exists x_0,x_1.0<x_0\wedge x_0^2=2x_1^2)}$$

De la coupure vient le calcul... et les difficultés !

Une question de correction… logique

Ne pas prouver tout et son contraire

$$\dfrac{\dfrac{\dfrac{\vdots}{\vdash \mu X.X}\,(\mu)}{\vdash \mu X.X}\,(\mu) \qquad \dfrac{\dfrac{\vdots}{\vdash \nu X.X, F}\,(\nu)}{\vdash \nu X.X, F}\,(\nu)}{\vdash F}\,(\mathrm{Cut}) \qquad \dfrac{\dfrac{\dfrac{\vdots}{\vdash \mu X.X}\,(\mu)}{\vdash \mu X.X}\,(\mu) \qquad \dfrac{\dfrac{\vdots}{\vdash \nu X.X, \neg F}\,(\nu)}{\vdash \nu X.X, \neg F}\,(\nu)}{\vdash \neg F}\,(\mathrm{Cut})$$

Une question de correction... logique

Ne pas prouver tout et son contraire

$$\dfrac{\dfrac{\dfrac{\vdots}{\vdash \mu X.X}\,(\mu)}{\vdash \mu X.X}\,(\mu) \qquad \dfrac{\dfrac{\vdots}{\vdash \nu X.X, F}\,(\nu)}{\vdash \nu X.X, F}\,(\nu)}{\vdash F}\,(\mathrm{Cut}) \qquad \dfrac{\dfrac{\dfrac{\vdots}{\vdash \mu X.X}\,(\mu)}{\vdash \mu X.X}\,(\mu) \qquad \dfrac{\dfrac{\vdots}{\vdash \nu X.X, \neg F}\,(\nu)}{\vdash \nu X.X, \neg F}\,(\nu)}{\vdash \neg F}\,(\mathrm{Cut})$$

Les dérivations infinies circulaires ne sont pas toutes correctes...

Besoin d'un critère de correction !

Une question de correction... logique

Ne pas prouver tout et son contraire

$$\dfrac{\dfrac{\dfrac{\vdots}{\vdash \mu X.X}\,(\mu)}{\vdash \mu X.X}\,(\mu) \qquad \dfrac{\dfrac{\vdots}{\vdash \nu X.X, F}\,(\nu)}{\vdash \nu X.X, F}\,(\nu)}{\vdash F}\,(\mathrm{Cut}) \qquad \dfrac{\dfrac{\dfrac{\vdots}{\vdash \mu X.X}\,(\mu)}{\vdash \mu X.X}\,(\mu) \qquad \dfrac{\dfrac{\vdots}{\vdash \nu X.X, \neg F}\,(\nu)}{\vdash \nu X.X, \neg F}\,(\nu)}{\vdash \neg F}\,(\mathrm{Cut})$$

Les dérivations infinies circulaires ne sont pas toutes correctes...

Besoin d'un critère de correction !

Condition de parité – chaque branche infinie doit contenir une trace validante :

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash a, a^{\perp}}\,(\mathrm{Ax})}{\vdash a \parr a^{\perp}}\,(\parr) \qquad \dfrac{\dfrac{\vdash F}{\vdash !F}\,(!\mathrm{p}) \qquad \dfrac{\vdash F}{\vdash G}\,(\mu)}{\vdash !F \otimes G}\,(\otimes)}{\vdash (a \parr a^{\perp}) \otimes (!F \otimes G)}\,(\otimes)}{\vdash F}\,(\nu)$$

$$F = \nu X.((a \parr a^{\perp}) \otimes (!X \otimes \mu Y.X)).$$
$$G = \mu Y.F$$

Une question de correction... logique

Ne pas prouver tout et son contraire

$$\dfrac{\dfrac{\dfrac{\vdots}{\vdash \mu X.X}\,(\mu)}{\vdash \mu X.X}\,(\mu) \qquad \dfrac{\dfrac{\vdots}{\vdash \nu X.X, F}\,(\nu)}{\vdash \nu X.X, F}\,(\nu)}{\vdash F}\,(\mathrm{Cut}) \qquad \dfrac{\dfrac{\dfrac{\vdots}{\vdash \mu X.X}\,(\mu)}{\vdash \mu X.X}\,(\mu) \qquad \dfrac{\dfrac{\vdots}{\vdash \nu X.X, \neg F}\,(\nu)}{\vdash \nu X.X, \neg F}\,(\nu)}{\vdash \neg F}\,(\mathrm{Cut})$$

Les dérivations infinies circulaires ne sont pas toutes correctes...

Besoin d'un critère de correction !

Condition de parité – chaque branche infinie doit contenir une trace validante :

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash a, a^{\perp}}\,(\mathrm{Ax})}{\vdash a \parr a^{\perp}}\,(\parr) \qquad \dfrac{\dfrac{\vdash F}{\vdash !F}\,(!\mathrm{p}) \qquad \dfrac{\vdash F}{\vdash G}\,(\mu)}{\vdash !F \otimes G}\,(\otimes)}{\vdash (a \parr a^{\perp}) \otimes (!F \otimes G)}\,(\otimes)}{\vdash F}\,(\nu)$$

$$F = \nu X.((a \parr a^{\perp}) \otimes (!X \otimes \mu Y.X)).$$
$$G = \mu Y.F$$

$\Longrightarrow$ ***La correction garantit qu'on peut éliminer les coupures.***

[Baelde, Doumane & S. 16]

Assure que la logique est correcte et qu'on peut l'utiliser pour calculer.

Calculer/Programmer avec des preuves

$$\mathsf{N} = \mu X.1 \oplus X$$

$$\begin{array}{lcl} double & : & N \to N \\ double(0) & = & 0 \\ double(succ(m)) & = & succ(succ(double(m))) \end{array}$$

$$\pi_0 = \cfrac{\cfrac{\cfrac{}{\vdash 1}\ (1)}{\vdash 1 \oplus N}\ (\oplus_1)}{\vdash N}\ (\mu) \qquad \pi_{k+1} = \cfrac{\cfrac{\pi_k}{\vdash 1 \oplus N}\ (\oplus_2)}{\vdash N}\ (\mu)$$

$$\pi_{succ} = \cfrac{\cfrac{\cfrac{}{N \vdash N}\ (Ax)}{N \vdash 1 \oplus N}\ (\oplus_2)}{N \vdash N}\ (\mu)$$

$$\cfrac{\pi_k \qquad \pi_{succ}}{\vdash N}\ (Cut) \longrightarrow^{\star} \pi_{k+1}$$

Calculer/Programmer avec des preuves circulaires

$$\mathsf{N} = \mu X.1 \oplus X$$

$$\begin{array}{lcl} double & : & N \to N \\ double(0) & = & 0 \\ double(succ(m)) & = & succ(succ(double(m))) \end{array}$$

$$\pi_0 = \dfrac{\dfrac{\dfrac{}{\vdash 1}\,(1)}{\vdash 1 \oplus N}\,(\oplus_1)}{\vdash N}\,(\mu) \qquad \pi_{\mathrm{k}+1} = \dfrac{\dfrac{\pi_k}{\vdash 1 \oplus N}\,(\oplus_2)}{\vdash N}\,(\mu)$$

$$\pi_{\mathrm{succ}} = \dfrac{\dfrac{\dfrac{}{N \vdash N}\,(\mathrm{Ax})}{N \vdash 1 \oplus N}\,(\oplus_2)}{N \vdash N}\,(\mu)$$

$$\dfrac{\pi_{\mathrm{k}} \qquad \pi_{\mathrm{succ}}}{\vdash N}\,(\mathrm{Cut}) \longrightarrow^{\star} \pi_{\mathrm{k}+1}$$

$$\pi_{double} = \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash 1}\,(1)}{\vdash 1 \oplus N}\,(\oplus_1)}{\vdash N}\,(\mu)}{1 \vdash N}\,(\bot) \qquad \dfrac{\dfrac{\dfrac{\dfrac{N \vdash N}{N \vdash 1 \oplus N}\,(\oplus_2)}{N \vdash N}\,(\mu)}{N \vdash 1 \oplus N}\,(\oplus_2)}{N \vdash N}\,(\mu)}{1 \oplus N \vdash N}\,(\&)}{N \vdash N}\,(\nu)$$

$$\dfrac{\pi_k \qquad \pi_{double}}{\vdash N}\,(\mathrm{Cut}) \longrightarrow^{\star} \pi_{2k}$$

Calculer/Programmer avec des preuves circulaires

$$\mathsf{N} = \mu X.1 \oplus X$$

$$\begin{array}{lcl} double & : & N \to N \\ double(0) & = & 0 \\ double(succ(m)) & = & succ(succ(double(m))) \end{array}$$

$$\pi_0 = \dfrac{\dfrac{\dfrac{}{\vdash 1}\,(1)}{\vdash 1 \oplus N}\,(\oplus_1)}{\vdash N}\,(\mu) \qquad \pi_{\mathrm{k+1}} = \dfrac{\dfrac{\pi_k}{\vdash 1 \oplus N}\,(\oplus_2)}{\vdash N}\,(\mu)$$

$$\pi_{\mathrm{succ}} = \dfrac{\dfrac{\dfrac{}{N \vdash N}\,(\mathrm{Ax})}{N \vdash 1 \oplus N}\,(\oplus_2)}{N \vdash N}\,(\mu)$$

$$\dfrac{\pi_{\mathrm{k}} \qquad \pi_{\mathrm{succ}}}{\vdash N}\,(\mathrm{Cut}) \longrightarrow^{\star} \pi_{\mathrm{k+1}}$$

$$\pi_{double} = \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash 1}\,(1)}{\vdash 1 \oplus N}\,(\oplus_1)}{\vdash N}\,(\mu)}{1 \vdash N}\,(\bot) \qquad \dfrac{\dfrac{\dfrac{\dfrac{N \vdash N}{N \vdash 1 \oplus N}\,(\oplus_2)}{N \vdash N}\,(\mu)}{N \vdash 1 \oplus N}\,(\oplus_2)}{N \vdash N}\,(\mu)}{1 \oplus N \vdash N}\,(\&)}{N \vdash N}\,(\nu)$$

$$\dfrac{\pi_k \qquad \pi_{double}}{\vdash N}\,(\mathrm{Cut}) \longrightarrow^{\star} \pi_{2k}$$

Condition de validité trop restrictive pour écrire des programmes aisément : comment l'étendre ?

Modularité des preuves infinies

$$\dfrac{\dfrac{\dfrac{}{\vdash \nu X.X, \mu X.X}\,(\mathsf{Ax})}{\vdash \nu X.X, \mu X.X}\,(\mu) \qquad \dfrac{\dfrac{\vdash \nu X.X}{\vdash \nu X.X}\,(\nu)}{\vdash \nu X.X}\,(\nu)}{\vdash \nu X.X}\,(\mathsf{Cut})$$

Modularité des preuves infinies

$$\dfrac{\dfrac{\dfrac{}{\vdash \nu X.X, \mu X.X}\,(\mathrm{Ax})}{\vdash \nu X.X, \mu X.X}\,(\mu) \qquad \dfrac{\dfrac{\vdash \nu X.X}{\vdash \nu X.X}\,(\nu)}{\vdash \nu X.X}\,(\nu)}{\vdash \nu X.X}\,(\mathrm{Cut})$$

Cut-elimination

$$\dfrac{\vdash \nu X.X}{\vdash \nu X.X}\,(\nu)$$

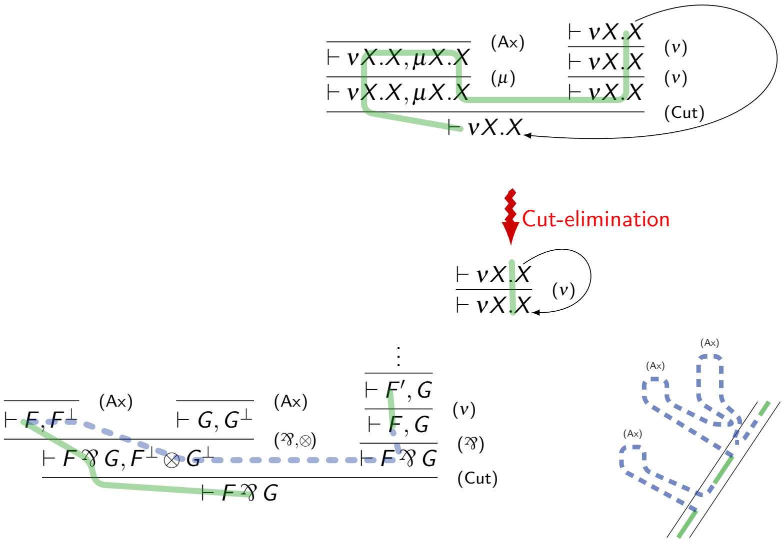
Modularité des preuves infinies

$$\dfrac{\dfrac{\dfrac{}{\vdash \nu X.X, \mu X.X}\,(\mathrm{Ax})}{\vdash \nu X.X, \mu X.X}\,(\mu) \qquad \dfrac{\dfrac{\vdash \nu X.X}{\vdash \nu X.X}\,(\nu)}{\vdash \nu X.X}\,(\nu)}{\vdash \nu X.X}\,(\mathrm{Cut})$$

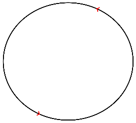
Cut-elimination

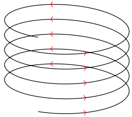
$$\dfrac{\vdash \nu X.X}{\vdash \nu X.X}\,(\nu)$$

Modularité des preuves infinies



[Baelde, Doumane, Kuperberg & S. 22], extension en cours avec Bauer.





Perspectives futures

Au sein des équipes thématiques de PPS :

Comprendre les invariants sémantiques des preuves circulaires ;
(en cours avec Ehrhard et Jafarrahmani)

Types (co)inductifs en programmation fonctionnelle et dans les assistants de preuves (traitement des coinductifs en Coq) (Dagand, Guatto, Letouzey, Herbelin).

Connexion avec d'autres approches coalgébriques et infinitaires dans le pôle (Bernardi, Melliès, Petrisan, van Gool...)

Plus largement dans l'IRIF :

Liens forts avec automates de parité (déjà exploré par Melliès) ;

Techniques de vérification logicielle récemment relues comme de la recherche de preuves circulaires [Tsukada & Unno 22].

Équipe Preuves Et Programmes

- 23.8 membres (11.5 permanent, of which 3 RP/DR)
- Axes:
  - Models of computation, λ-calculi, rewriting
  - Quantitative Type Systems
  - Proof theory and computation
  - Dependent type theory
  - Structural Proofs for Fixed-point Logics

	By affiliation	Pro rata
Int. Conferences	138	80
Int. Journals	88	47
PhD Thesis	22	12

Projection

Team head from 2024: Alexis Saurin

- Models of computation, λ-calculi, rewriting
- Quantitative Type Systems

• Higher-Order Bayesian Networks
• Quantitative effectful programming
• Quantitative CPS translations.
• Coherent differentiation (logical and operational meaning)
• Complexity analysis for higher-order programs
• Solvability in call-by-push-value.
• Tracelet Analysis in the Life Sciences.

- Proof theory and computation
- Dependent type theory

• Understanding the computational contents of choice principles.
• Propositions-as-types-as-categories-as-spaces correspondence.
• Coq-based Rewriting: Towards Executable Applied Category Theory.

- Structural Proofs for Fixed-point Logics

• Finitization problems and denotational semantics of circular proofs.
• Enriching the shape of circular proofs.
• Formalization of the theory of fixed-point logic proof theory.
• Compositionality of circular proofs and circular typing derivation.