

La démonstration : principes et pratiques.

Catriona Maclean

6 avril 2022

La démonstration en mathématiques

Sociologie et histoire de la démonstration.

Problèmes sociologiques.

Problèmes pédagogiques, retour sur expérience.

Retour sur expérience

Définition

Forme de **raisonnement**

Définition

Forme de **raisonnement**

- ▶ Uniquement **analytique**

Définition

Forme de **raisonnement**

- ▶ Uniquement **analytique**
- ▶ Raisonnement par **analogie** interdit

Définition

Forme de **raisonnement**

- ▶ Uniquement **analytique**
- ▶ Raisonement par **analogie** interdit
- ▶ Raisonement par **observation** également.

Définition

Forme de **raisonnement**

- ▶ Uniquement **analytique**
- ▶ Raisonement par **analogie** interdit
- ▶ Raisonement par **observation** également.

Réputé débiter avec les Eléments d'Euclide vers 300 BCE.

Le raisonnement analytique

”Minecraft” intellectuel

Le raisonnement analytique

"Minecraft" intellectuel

- ▶ un certain nombre de "blocs de base" appelés "axiomes"

Le raisonnement analytique

"Minecraft" intellectuel

- ▶ un certain nombre de "blocs de base" appelés "axiomes"
- ▶ règles de combinaison simples (calcul des prédicats)

Le raisonnement analytique

"Minecraft" intellectuel

- ▶ un certain nombre de "blocs de base" appelés "axiomes"
- ▶ règles de combinaison simples (calcul des prédicats)
- ▶ + des millénaires : résultat très complexe.

En principe...

*54·43. $\vdash \therefore \alpha, \beta \in 1. \supset : \alpha \cap \beta = \Lambda. \equiv . \alpha \cup \beta \in 2$

Dem.

$\vdash . *54·26. \supset \vdash \therefore \alpha = t'x. \beta = t'y. \supset : \alpha \cup \beta \in 2. \equiv . x \neq y.$

[*51·231] $\equiv . t'x \cap t'y = \Lambda.$

[*13·12] $\equiv . \alpha \cap \beta = \Lambda$ (1)

$\vdash . (1). *11·11·35. \supset$

$\vdash \therefore (\exists x, y). \alpha = t'x. \beta = t'y. \supset : \alpha \cup \beta \in 2. \equiv . \alpha \cap \beta = \Lambda$ (2)

$\vdash . (2). *11·54. *52·1. \supset \vdash . \text{Prop}$

From this proposition it will follow, when arithmetical addition has been defined, that $1 + 1 = 2$.

En principe...

*54·43. $\vdash \therefore \alpha, \beta \in 1. \supset : \alpha \cap \beta = \Lambda. \equiv . \alpha \cup \beta \in 2$

Dem.

$\vdash . *54\cdot26. \supset \vdash \therefore \alpha = t'x. \beta = t'y. \supset : \alpha \cup \beta \in 2. \equiv . x \neq y.$

[*51·231] $\equiv . t'x \cap t'y = \Lambda.$

[*13·12] $\equiv . \alpha \cap \beta = \Lambda$ (1)

$\vdash . (1). *11\cdot11\cdot35. \supset$

$\vdash \therefore (\exists x, y). \alpha = t'x. \beta = t'y. \supset : \alpha \cup \beta \in 2. \equiv . \alpha \cap \beta = \Lambda$ (2)

$\vdash . (2). *11\cdot54. *52\cdot1. \supset \vdash . \text{Prop}$

From this proposition it will follow, when arithmetical addition has been defined, that $1 + 1 = 2$.

Démonstration (incomplète) de $1+1=2$

En principe...

*54·43. $\vdash \therefore \alpha, \beta \in 1 . \supset : \alpha \cap \beta = \Lambda . \equiv . \alpha \cup \beta \in 2$

Dem.

$\vdash . *54 \cdot 26 . \supset \vdash \therefore \alpha = t'x . \beta = t'y . \supset : \alpha \cup \beta \in 2 . \equiv . x \neq y .$

[*51·231] $\equiv . t'x \cap t'y = \Lambda .$

[*13·12] $\equiv . \alpha \cap \beta = \Lambda \quad (1)$

$\vdash . (1) . *11 \cdot 11 \cdot 35 . \supset$

$\vdash \therefore (\exists x, y) . \alpha = t'x . \beta = t'y . \supset : \alpha \cup \beta \in 2 . \equiv . \alpha \cap \beta = \Lambda \quad (2)$

$\vdash . (2) . *11 \cdot 54 . *52 \cdot 1 . \supset \vdash . \text{Prop}$

From this proposition it will follow, when arithmetical addition has been defined, that $1 + 1 = 2$.

Démonstration (incomplète) de $1+1=2$ (Principes Mathématiques de Bertrand Russell).

Rôle définissant...

- ▶ Première réaction : qualité définissant communauté

Rôle définissant...

- ▶ Première réaction : qualité définissant communauté
- ▶ Notamment le cas au CNU.

ou pas...

Distinction entre *production* et *procéssus*

ou pas...

Distinction entre *production* et *procédus*

- ▶ la *production* doit être formelle

ou pas...

Distinction entre *production* et *procéssus*

- ▶ la *production* doit être formelle
- ▶ dans le *processus* sur valorisation de la "génie" .

ou pas...

Distinction entre *production* et *procéssus*

- ▶ la *production* doit être formelle
- ▶ dans le *processus* sur valorisation de la "génie" .

Cantor "In re mathematica ars proponendi quaestionem pluris facienda est quam solvendi" .

Hermite sur Poincaré

"Souvent Picard lui a demandé, sur des points d'une grande importance dans ses articles des Comptes Rendus, des éclaircissements et des explications, sans pouvoir jamais rien obtenir qu'une affirmation: "c'est ainsi, c'est comme cela", de sorte qu'il semble comme un voyant auquel apparaissent les vérités dans une vive lumière, mais en grande partie pour lui seulement."

Hardy sur Ramanujan

"For my part, it is difficult to say what I owe to Ramanujan - his originality has been a constant source of suggestion to me ever since I knew him."

Hardy sur Ramanujan

"For my part, it is difficult to say what I owe to Ramanujan - his originality has been a constant source of suggestion to me ever since I knew him."

(Un certain nombre des "rêves" de Ramanujan était faux

Hardy sur Ramanujan

"For my part, it is difficult to say what I owe to Ramanujan - his originality has been a constant source of suggestion to me ever since I knew him."

(Un certain nombre des "rêves" de Ramanujan était faux cadre de Hardy permet à son talent de s'exprimer)

Réputations des anciens

Mathématiciens célèbres qui ont publié des démonstrations (plus ou moins) fausses

Réputations des anciens

Mathématiciens célèbres qui ont publié des démonstrations (plus ou moins) fausses

- ▶ Euclide (nombreuses assumptions cachées dans les éléments)

Réputations des anciens

Mathématiciens célèbres qui ont publié des démonstrations (plus ou moins) fausses

- ▶ Euclide (nombreuses assumptions cachées dans les éléments)
- ▶ Kepler (arguments loufouques médiévistes)

Réputations des anciens

Mathématiciens célèbres qui ont publié des démonstrations (plus ou moins) fausses

- ▶ Euclide (nombreuses assumptions cachées dans les éléments)
- ▶ Kepler (arguments loufouques médiévistes)
" Pourquoi 6 planètes ? Parce qu'il faut 6 voix pour faire une chorale" .

Réputations des anciens

Mathématiciens célèbres qui ont publié des démonstrations (plus ou moins) fausses

- ▶ Euclide (nombreuses assumptions cachées dans les éléments)
- ▶ Kepler (arguments loufouques médiévistes)
" Pourquoi 6 planètes ? Parce qu'il faut 6 voix pour faire une chorale".
- ▶ Leibniz (utilisation d'infinitesimals)

Reputations des modernes

- ▶ Euler (démonstration fausse du théorème de l'algèbre)

Reputations des modernes

- ▶ Euler (démonstration fausse du théorème de l'algèbre)
- ▶ Lagrange (opposition Fourier, toute fonction développable en série)

Reputations des modernes

- ▶ Euler (démonstration fausse du théorème de l'algèbre)
- ▶ Lagrange (opposition Fourier, toute fonction développable en série)
- ▶ Cauchy (limite de fonctions continues est continue),

Reputations des modernes

- ▶ Euler (démonstration fausse du théorème de l'algèbre)
- ▶ Lagrange (opposition Fourier, toute fonction développable en série)
- ▶ Cauchy (limite de fonctions continues est continue),
- ▶ Poincaré (mémoire pour le prix royal Suède)

Reputations des modernes

- ▶ Euler (démonstration fausse du théorème de l'algèbre)
- ▶ Lagrange (opposition Fourier, toute fonction développable en série)
- ▶ Cauchy (limite de fonctions continues est continue),
- ▶ Poincaré (mémoire pour le prix royal Suède - erreur découverte après impression).

Pourtant nécessaire

Exemple : école italienne de la géométrie algébrique.

Pourtant nécessaire

Exemple : école italienne de la géométrie algébrique.

- ▶ absence de fondations suffisantes

Pourtant nécessaire

Exemple : école italienne de la géométrie algébrique.

- ▶ absence de fondations suffisantes notamment pour les intersections,

Pourtant nécessaire

Exemple : école italienne de la géométrie algébrique.

- ▶ absence de fondations suffisantes notamment pour les intersections,
- ▶ principe " passage à la limite" sans fondation

Pourtant nécessaire

Exemple : école italienne de la géométrie algébrique.

- ▶ absence de fondations suffisantes notamment pour les intersections,
- ▶ principe " passage à la limite" sans fondation
- ▶ Dérive sociologique

Pourtant nécessaire

Exemple : école italienne de la géométrie algébrique.

- ▶ absence de fondations suffisantes notamment pour les intersections,
- ▶ principe " passage à la limite" sans fondation
- ▶ Dérive sociologique "gourou" n'admettant pas la contradiction (Severi)

Pourtant nécessaire

Exemple : école italienne de la géométrie algébrique.

- ▶ absence de fondations suffisantes notamment pour les intersections,
- ▶ principe " passage à la limite" sans fondation
- ▶ Dérive sociologique "gourou" n'admettant pas la contradiction (Severi)
- ▶ effondrement de l'école vers 1950.

Pourtant nécessaire

Exemple : école italienne de la géométrie algébrique.

- ▶ absence de fondations suffisantes notamment pour les intersections,
- ▶ principe " passage à la limite" sans fondation
- ▶ Dérive sociologique "gourou" n'admettant pas la contradiction (Severi)
- ▶ effondrement de l'école vers 1950.

L'importance du groupe social

- ▶ Calcul des prédicats inutilisable en pratique

L'importance du groupe social

- ▶ Calcul des prédicats inutilisable en pratique
- ▶ On approche par le langage naturel

L'importance du groupe social

- ▶ Calcul des prédicats inutilisable en pratique
- ▶ On approche par le langage naturel
- ▶ Quel degré d'approximation autorisée ?

L'importance du groupe social

- ▶ Calcul des prédicats inutilisable en pratique
- ▶ On approche par le langage naturel
- ▶ Quel degré d'approximation autorisée ?
- ▶ Consensus *social*

L'importance du groupe social

- ▶ Calcul des prédicats inutilisable en pratique
- ▶ On approche par le langage naturel
- ▶ Quel degré d'approximation autorisée ?
- ▶ Consensus *social*

Différences nationales en particulier.

Premier écart

La méthode axiomatique est souvent réputée débiter avec les
Eléments d'Euclide...

Premier écart

La méthode axiomatique est souvent réputée débiter avec les
Eléments d'Euclide...
et la première erreur se trouve dans la ligne 4 de la proposition 1.

Avant premier écart

Même la définition d'un point pose problème

Avant premier écart

Même la définition d'un point pose problème
Selon Euclide c'est "ce qui n'a aucune partie"

Sincérité de la littérature

- ▶ Les mathématiciens se trompent...

Sincérité de la littérature

- ▶ Les mathématiciens se trompent...
- ▶ Comment s'assurer de la sincérité de la littérature ?

Sincérité de la littérature

- ▶ Les mathématiciens se trompent...
- ▶ Comment s'assurer de la sincérité de la littérature ?
- ▶ forte inter-dépendance

Sincérité de la littérature

- ▶ Les mathématiciens se trompent...
- ▶ Comment s'assurer de la sincérité de la littérature ?
- ▶ forte inter-dépendance
- ▶ peu de contrôle

Sincérité de la littérature

- ▶ Les mathématiciens se trompent...
- ▶ Comment s'assurer de la sincérité de la littérature ?
- ▶ forte inter-dépendance
- ▶ peu de contrôle

Potentiel d'effondrement.

- ▶ Ecole de géométrie algébrique italienne,

Potentiel d'effondrement.

- ▶ Ecole de géométrie algébrique italienne,
- ▶ Bourbaki et le calcul intégral/différentiel,

Potentiel d'effondrement.

- ▶ Ecole de géométrie algébrique italienne,
- ▶ Bourbaki et le calcul intégral/différentiel,
- ▶ Théorie des catégories fin 20ième/début 21ième siècle

Etude de cas : théorie des catégories/groupoïdes/homotopie

- ▶ 1984 : circulation d'un texte "Esquisse d'un programme" de Groethendieck

Etude de cas : théorie des catégories/groupoïdes/homotopie

- ▶ 1984 : circulation d'un texte "Esquisse d'un programme" de Groethendieck
- ▶ 1986 : publication de Algebraic Cycles and Higher K-theory de Spencer Bloch.

Etude de cas : théorie des catégories/groupoïdes/homotopie

- ▶ 1984 : circulation d'un texte "Esquisse d'un programme" de Groethendieck
- ▶ 1986 : publication de Algebraic Cycles and Higher K-theory de Spencer Bloch. Censé établir les fondations de la cohomologie des motifs.

Etude de cas : théorie des catégories/groupoïdes/homotopie

- ▶ 1984 : circulation d'un texte "Esquisse d'un programme" de Groethendieck
- ▶ 1986 : publication de Algebraic Cycles and Higher K-theory de Spencer Bloch. Censé établir les fondations de la cohomologie des motifs.
- ▶ 1989 : publication de "∞-Groupoids as a Model for a Homotopy Category" de Voevodsky et Kapranov,

Etude de cas : théorie des catégories/groupoïdes/homotopie

- ▶ 1984 : circulation d'un texte "Esquisse d'un programme" de Groethendieck
- ▶ 1986 : publication de Algebraic Cycles and Higher K-theory de Spencer Bloch. Censé établir les fondations de la cohomologie des motifs.
- ▶ 1989 : publication de "∞-Groupoids as a Model for a Homotopy Category" de Voevodsky et Kapranov, censé établir les fondations des groupoïdes sur la base du programme de Groethendieck.

Le diable commence à s'en mêler

- ▶ Peu de temps après publication : erreur dans "Algebraic Cycles and Higher K-theory."

Le diable commence à s'en mêler

- ▶ Peu de temps après publication : erreur dans "Algebraic Cycles and Higher K-theory."
- ▶ Rien du papier ne survit.

Le diable commence à s'en mêler

- ▶ Peu de temps après publication : erreur dans "Algebraic Cycles and Higher K-theory."
- ▶ Rien du papier ne survit.
- ▶ Voevodsky : construction alternative en 1993,

Le diable commence à s'en mêler

- ▶ Peu de temps après publication : erreur dans "Algebraic Cycles and Higher K-theory."
- ▶ Rien du papier ne survit.
- ▶ Voevodsky : construction alternative en 1993, "Cohomological Theory of Presheaves with Transfers".

Le diable commence à s'en mêler

- ▶ Peu de temps après publication : erreur dans "Algebraic Cycles and Higher K-theory."
- ▶ Rien du papier ne survit.
- ▶ Voevodsky : construction alternative en 1993, "Cohomological Theory of Presheaves with Transfers".
- ▶ 1989-1999 nombreux groupes de mathématiciens travaillent sur la base des deux papiers de Voevodsky et Kapranov.

Le diable commence à s'en mêler

- ▶ Peu de temps après publication : erreur dans "Algebraic Cycles and Higher K-theory."
- ▶ Rien du papier ne survit.
- ▶ Voevodsky : construction alternative en 1993, "Cohomological Theory of Presheaves with Transfers".
- ▶ 1989-1999 nombreux groupes de mathématiciens travaillent sur la base des deux papiers de Voevodsky et Kapranov.
- ▶ 2002 Médaille Fields de Voevodsky.

On frle l'effondrement

- ▶ 1998 Preprint arxiv de Simpson, proposant un contre exemple au papier de 1989.

On frle l'effondrement

- ▶ 1998 Preprint arxiv de Simpson, proposant un contre exemple au papier de 1989. Débat dans la communauté.

On frle l'effondrement

- ▶ 1998 Preprint arxiv de Simpson, proposant un contre exemple au papier de 1989. Débat dans la communauté.
- ▶ 1999-2000 Voevodsky découvre une erreur dans "Cohomological Theory of Presheaves with Transfers".

On frle l'effondrement

- ▶ 1998 Preprint arxiv de Simpson, proposant un contre exemple au papier de 1989. Débat dans la communauté.
- ▶ 1999-2000 Voevodsky découvre une erreur dans "Cohomological Theory of Presheaves with Transfers".
- ▶ Dix ans de travail communautaire mis en danger.

On frle l'effondrement

- ▶ 1998 Preprint arxiv de Simpson, proposant un contre exemple au papier de 1989. Débat dans la communauté.
- ▶ 1999-2000 Voevodsky découvre une erreur dans "Cohomological Theory of Presheaves with Transfers".
- ▶ Dix ans de travail communautaire mis en danger.
- ▶ Aucun des groupes n'a vu le problème.

On recule de l'abys

- ▶ 2006 publication d'un lemme correctif de "Cohomological Theory"

On recule de l'abys

- ▶ 2006 publication d'un lemme correctif de "Cohomological Theory"
- ▶ 2013 Débat sur preprint tranché en faveur de Simpson

On recule de l'abys

- ▶ 2006 publication d'un lemme correctif de "Cohomological Theory"
- ▶ 2013 Débat sur preprint tranché en faveur de Simpson
- ▶ Voevodsky abandonne son travail sur les motifs en faveur des *fondements univalents*.

Fondements univalents

Voevodsky s'est convaincu de la nécessité de **démonstrations vérifiables** par ordinateur.

Fondements univalents

Voevodsky s'est convaincu de la nécessité de **démonstrations vérifiables** par ordinateur.

- ▶ Problème : l'ordinateur lit la logique formel.

Fondements univalents

Voevodsky s'est convaincu de la nécessité de **démonstrations vérifiables** par ordinateur.

- ▶ Problème : l'ordinateur lit la logique formel.
- ▶ ce qui ne fait personne.

Fondements univalents

Voevodsky s'est convaincu de la nécessité de **démonstrations vérifiables** par ordinateur.

- ▶ Problème : l'ordinateur lit la logique formel.
- ▶ ce qui ne fait personne.
- ▶ Impraticable avec le calcul des prédicats.

Fondements univalents

Voevodsky s'est convaincu de la nécessité de **démonstrations vérifiables** par ordinateur.

- ▶ Problème : l'ordinateur lit la logique formel.
- ▶ ce qui ne fait personne.
- ▶ Impraticable avec le calcul des prédicats.
- ▶ Fondements univalents : langage de logique formel alternatif

Fondements univalents

Voevodsky s'est convaincu de la nécessité de **démonstrations vérifiables** par ordinateur.

- ▶ Problème : l'ordinateur lit la logique formel.
- ▶ ce qui ne fait personne.
- ▶ Impraticable avec le calcul des prédicats.
- ▶ Fondements univalents : langage de logique formel alternatif
- ▶ But : rendre faisable l'écriture formelle.

Avoir la foi

- ▶ Plus possible de maitriser tout ce qui sous tend un article.

Avoir la foi

- ▶ Plus possible de maîtriser tout ce qui sous tend un article.
- ▶ Taux de publication d'arxiv : 16,000 par mois.

Avoir la foi

- ▶ Plus possible de maîtriser tout ce qui sous tend un article.
- ▶ Taux de publication d'arxiv : 16,000 par mois.
- ▶ 12 articles dans mon domaine hier (géométrie algébrique)

Avoir la foi

- ▶ Plus possible de maîtriser tout ce qui sous tend un article.
- ▶ Taux de publication d'arxiv : 16,000 par mois.
- ▶ 12 articles dans mon domaine hier (géométrie algébrique)
- ▶ dont 5 potentiellement pertinent à moi

Un exemple

Citation d'un de mes articles

Un exemple

Citation d'un de mes articles

"After blowing up, we obtain a birational morphism $\pi^{\text{sm}} : X^{\text{sm}} \rightarrow X$ from a smooth variety, X^{sm} , to X . "

Un exemple

Citation d'un de mes articles

"After blowing up, we obtain a birational morphism $\pi^{\text{sm}} : X^{\text{sm}} \rightarrow X$ from a smooth variety, X^{sm} , to X ."

Résultat de Hironaka, années 60, 100 pages.

Un exemple

Citation d'un de mes articles

"After blowing up, we obtain a birational morphism $\pi^{\text{sm}} : X^{\text{sm}} \rightarrow X$ from a smooth variety, X^{sm} , to X . "

Résultat de Hironaka, années 60, 100 pages.

Potentiel de propagation des erreurs.

Un exemple

Citation d'un de mes articles

"After blowing up, we obtain a birational morphism
 $\pi^{\text{sm}} : X^{\text{sm}} \rightarrow X$ from a smooth variety, X^{sm} , to X ."

Résultat de Hironaka, années 60, 100 pages.

Potential de propagation des erreurs.

Système de rapportage insuffisant.

Robustesse procédure

Les procédures de vérification peu robustes.

Robustesse procédure

Les procédures de vérification peu robustes.

- ▶ souvent un seul vérificateur

Robustesse procédure

Les procédures de vérification peu robustes.

- ▶ souvent un seul vérificateur
- ▶ pas de vérification "n+1"

Robustesse procédure

Les procédures de vérification peu robustes.

- ▶ souvent un seul vérificateur
- ▶ pas de vérification "n+1"
- ▶ pression à bâcler la vérification

Robustesse procédure

Les procédures de vérification peu robustes.

- ▶ souvent un seul vérificateur
- ▶ pas de vérification "n+1"
- ▶ pression à bâcler la vérification
- ▶ aucune pression à bien faire.

Robustesse procédure

Les procédures de vérification peu robustes.

- ▶ souvent un seul vérificateur
- ▶ pas de vérification "n+1"
- ▶ pression à bâcler la vérification
- ▶ aucune pression à bien faire.

Erreurs trouvées au moment de l'utilisation.

Incitations institutionnelle

Le travail de rapporteur est

- ▶ très chronophage si bien fait

Incitations institutionnelle

Le travail de rapporteur est

- ▶ très chronophage si bien fait
- ▶ pas reconnu.

Problème du crédit

- ▶ Le système fonctionne sur le crédit des rapporteurs

Problème du crédit

- ▶ Le système fonctionne sur le crédit des rapporteurs et des auteurs

Problème du crédit

- ▶ Le système fonctionne sur le crédit des rapporteurs et des auteurs
- ▶ Comme cette crédibilité est elle construite ?

Problème du crédit

- ▶ Le système fonctionne sur le crédit des rapporteurs et des auteurs
- ▶ Comme cette crédibilité est elle construite ?
- ▶ Est ce qu'elle est justifiée ?

Problème du crédit

- ▶ Le système fonctionne sur le crédit des rapporteurs et des auteurs
- ▶ Comme cette crédibilité est elle construite ?
- ▶ Est ce qu'elle est justifiée ?

Contribution à la situation de Voevodsky.

L'avis de l'intéressé

Voevodsky sur les problèmes de ses papiers :

L'avis de l'intéressé

Voevodsky sur les problèmes de ses papiers :

"A technical argument by a trusted author, which is hard to check and looks similar to arguments known to be correct, is hardly ever checked in detail."

L'avis de l'intéressé

Voevodsky sur les problèmes de ses papiers :

"A technical argument by a trusted author, which is hard to check and looks similar to arguments known to be correct, is hardly ever checked in detail."

Voevodsky sur le fait qu'il a fallu 14 ans pour que la communauté accepte le contre exemple de Carlos Simpson

L'avis de l'intéressé

Voevodsky sur les problèmes de ses papiers :

"A technical argument by a trusted author, which is hard to check and looks similar to arguments known to be correct, is hardly ever checked in detail."

Voevodsky sur le fait qu'il a fallu 14 ans pour que la communauté accepte le contre exemple de Carlos Simpson

"Mathematical research currently relies on a complex system of mutual trust based on reputations. By the time Simpson's paper appeared, both Kapranov and I had strong reputations. Simpson's paper created doubts in our result, which led to it being unused by other researchers, but no one came forward and challenged us on it."

Preuves longues

Certains résultats majeurs ont des démonstrations trop longues pour une vérification "à la main" fiable

Preuves longues

Certains résultats majeurs ont des démonstrations trop longues pour une vérification "à la main" fiable

- ▶ problème de Kepler (250 pages, plusieurs Gigabytes de code)

Preuves longues

Certains résultats majeurs ont des démonstrations trop longues pour une vérification "à la main" fiable

- ▶ problème de Kepler (250 pages, plusieurs Gigabytes de code)
- ▶ classification des groupes finis simples (10,000 pages au total)

Preuves longues

Certains résultats majeurs ont des démonstrations trop longues pour une vérification "à la main" fiable

- ▶ problème de Kepler (250 pages, plusieurs Gigabytes de code)
- ▶ classification des groupes finis simples (10,000 pages au total)
- ▶ Éléments de géométrie algébrique. (non publié en format article)

Preuves longues

Certains résultats majeurs ont des démonstrations trop longues pour une vérification "à la main" fiable

- ▶ problème de Kepler (250 pages, plusieurs Gigabytes de code)
- ▶ classification des groupes finis simples (10,000 pages au total)
- ▶ Eléments de géométrie algébrique. (non publié en format article)

Que faire ?

Un cas de figure : la démonstration de la conjecture de Kepler

- ▶ Conjecture de Kepler (1611) - densité optimale des oranges.

Un cas de figure : la démonstration de la conjecture de Kepler

- ▶ Conjecture de Kepler (1611) - densité optimale des oranges.
- ▶ 1998 Hales a annoncé une démonstration.

Un cas de figure : la démonstration de la conjecture de Kepler

- ▶ Conjecture de Kepler (1611) - densité optimale des oranges.
- ▶ 1998 Hales a annoncé une démonstration.
- ▶ Basée sur la résolution de 100,000 problèmes d'optimisation.

Kepler Hales bis

- ▶ La démonstration de Hales contenait 250 pages de maths

Kepler Hales bis

- ▶ La démonstration de Hales contenait 250 pages de maths
- ▶ et 3 Gbtes de programmes, code et données.

Kepler Hales bis

- ▶ La démonstration de Hales contenait 250 pages de maths
- ▶ et 3 Gbtes de programmes, code et données.
- ▶ Comment vérifier une chose pareille ?

Publication

- ▶ Annals of Mathematics a nominé un panel de 12 rapporteurs

Publication

- ▶ Annals of Mathematics a nommé un panel de 12 rapporteurs
- ▶ qui n'ont pas suffi.

Publication

- ▶ Annals of Mathematics a nommé un panel de 12 rapporteurs
- ▶ qui n'ont pas suffit.
- ▶ Ils ont rapporté qu'ils étaient convaincus à 99%, mais n'avaient pas pu certifier tout le code.

Publication

- ▶ Annals of Mathematics a nommé un panel de 12 rapporteurs
- ▶ qui n'ont pas suffi.
- ▶ Ils ont rapporté qu'ils étaient convaincus à 99%, mais n'avaient pas pu certifier tout le code.

Que faire dans ce genre de situation ?

Quelques pistes.

- ▶ Vérification communautaire ?

Quelques pistes.

- ▶ Vérification communautaire ?
- ▶ Vérification par équipe ?

Quelques pistes.

- ▶ Vérification communautaire ?
- ▶ Vérification par équipe ?
- ▶ Vérification par ordinateur ?

Quelques pistes.

- ▶ Vérification communautaire ?
- ▶ Vérification par équipe ?
- ▶ Vérification par ordinateur ?

Quid de l'ordinateur ?

Quelle place dans les mathématiques pour les démonstrations appuyées sur du code ?

Quid de l'ordinateur ?

Quelle place dans les mathématiques pour les démonstrations appuyées sur du code ?

Quid si le code est trop long pour être vérifiable ?

Quid de l'ordinateur ?

Quelle place dans les mathématiques pour les démonstrations appuyées sur du code ?

Quid si le code est trop long pour être vérifiable ?

Quelle place pour la vérification automatique des preuves ?

Démonstration vérifiée par ordinateur

- ▶ Principe : vérification automatique de démonstrations

Démonstration vérifiée par ordinateur

- ▶ Principe : vérification automatique de démonstrations
- ▶ suggestions de étapes

Démonstration vérifiée par ordinateur

- ▶ Principe : vérification automatique de démonstrations
- ▶ suggestions de étapes
- ▶ (base de données d'objets et résultats)

Démonstration vérifiée par ordinateur

- ▶ Principe : vérification automatique de démonstrations
- ▶ suggestions de étapes
- ▶ (base de données d'objets et résultats)
- ▶ écrites dans langage lisible par machine

Démonstration vérifiée par ordinateur

- ▶ Principe : vérification automatique de démonstrations
- ▶ suggestions de étapes
- ▶ (base de données d'objets et résultats)
- ▶ écrites dans langage lisible par machine

Projet Flyspeck

- ▶ But : produire une démonstration formelle de Kepler

Projet Flyspeck

- ▶ But : produire une démonstration formelle de Kepler
- ▶ Dbut : 1998

Projet Flyspeck

- ▶ But : produire une démonstration formelle de Kepler
- ▶ Dbut : 1998
- ▶ Démonstration finie : 2014

Projet Flyspeck

- ▶ But : produire une démonstration formelle de Kepler
- ▶ Dbut : 1998
- ▶ Démonstration finie : 2014
- ▶ Basée sur “Isabelle” et “Hol” .

” Folklore”

Pratique communautaire ou des résultats sont admis comme ” bien connus”

”Folklore”

Pratique communautaire ou des résultats sont admis comme ”bien connus” sans qu’une démo ait été donnée.

”Folklore”

Pratique communautaire ou des résultats sont admis comme ”bien connus” sans qu’une démo ait été donnée.

folklore, [] is a technical term for a method of publication in category theory. It means that someone sketched it on the back of an envelope, mimeographed it (whatever that means) and showed it to three people in a seminar in Chicago in 1973, except that the only evidence that we have of these events is a comment that was overheard in another seminar at Columbia in 1976. Nevertheless, if some younger person is so presumptuous as to write out a proper proof and attempt to publish it, they will get shot down in flames.

"Folklore" d'aujourd'hui

Pressions à publier + taille critique communautaire

"Folklore" d'aujourd'hui

Pressions à publier + taille critique communautaire
moindre importance du folklore

"Folklore" d'aujourd'hui

Pressions à publier + taille critique communautaire
moins importance du folklore
remplacé par "preprint de référence".

"Folklore" d'aujourd'hui

Pressions à publier + taille critique communautaire
moindre importance du folklore
remplacé par "preprint de référence".

Exemples :

- ▶ un papier fondationnel sur arxiv pendant plus que 10 ans - sans publication.

"Folklore" d'aujourd'hui

Pressions à publier + taille critique communautaire
moindre importance du folklore
remplacé par "preprint de référence".

Exemples :

- ▶ un papier fondationnel sur arxiv pendant plus que 10 ans - sans publication.
- ▶ un refus de projet basé sur un preprint arxiv.

"Folklore" d'aujourd'hui

Pressions à publier + taille critique communautaire
moindre importance du folklore
remplacé par "preprint de référence".

Exemples :

- ▶ un papier fondationnel sur arxiv pendant plus que 10 ans - sans publication.
- ▶ un refus de projet basé sur un preprint arxiv.
- ▶ un refus d'article basé sur un preprint non publié.

Publicabilité réduite

Règles communautaires stricte sur la publicabilité :

Publicabilité réduite

Règles communautaires stricte sur la publicabilité :

- ▶ pas de redémonstration

Publicabilité réduite

Règles communautaires stricte sur la publicabilité :

- ▶ pas de redémonstration
- ▶ pas de discussion de méthode

Publicabilité réduite

Règles communautaires stricte sur la publicabilité :

- ▶ pas de redémonstration
- ▶ pas de discussion de méthode

Limitent les possibilités de "contrôle de qualité".

Refus de l'erreur

- ▶ Communauté se définissant par la certitude

Refus de l'erreur

- ▶ Communauté se définissant par la certitude
- ▶ peu de tolérance de l'erreur

Refus de l'erreur

- ▶ Communauté se définissant par la certitude
- ▶ peu de tolérance de l'erreur
- ▶ problématique pour le contrôle qualité

Refus de l'erreur

- ▶ Communauté se définissant par la certitude
- ▶ peu de tolérance de l'erreur
- ▶ problématique pour le contrôle qualité
- ▶ problématique pour le développement du sujet

Tabou de la correction

- ▶ La littérature mathématique se caractérise par un taux bas de corrections

Tabou de la correction

- ▶ La littérature mathématique se caractérise par un taux bas de corrections
- ▶ 0,6% de la littérature mathématiques (contre un peu plus que 1% en gnral)

Tabou de la correction

- ▶ La littérature mathématique se caractérise par un taux bas de corrections
- ▶ 0,6% de la littérature mathématiques (contre un peu plus que 1% en gnral)
- ▶ Quel part d'auto-censure ?

Tabou de la correction

- ▶ La littérature mathématique se caractérise par un taux bas de corrections
- ▶ 0,6% de la littérature mathématiques (contre un peu plus que 1% en gnral)
- ▶ Quel part d'auto-censure ?
- ▶ Survol des erreurs du 19ième siècle : rarement soulev par les auteurs

Tabou de la correction

- ▶ La littérature mathématique se caractérise par un taux bas de corrections
- ▶ 0,6% de la littérature mathématiques (contre un peu plus que 1% en gnral)
- ▶ Quel part d'auto-censure ?
- ▶ Survol des erreurs du 19^{ième} siècle : rarement soulev par les auteurs
- ▶ Grand nombre d'erreurs publiées “discrètement” .

Vérification communautaire

- ▶ Résultats centraux - émergence vérification communautaire.

Vérification communautaire

- ▶ Résultats centraux - émergence vérification communautaire.
- ▶ Exemples : BCHM, Perelmann.

Vérification communautaire

- ▶ Résultats centraux - émergence vérification communautaire.
- ▶ Exemples : BCHM, Perelmann.
- ▶ Cf Voevodsky - Deligne

Vérification communautaire

- ▶ Résultats centraux - émergence vérification communautaire.
- ▶ Exemples : BCHM, Perelmann.
- ▶ Cf Voevodsky - Deligne
- ▶ Peu formalisé.

Vérification communautaire

- ▶ Résultats centraux - émergence vérification communautaire.
- ▶ Exemples : BCHM, Perelmann.
- ▶ Cf Voevodsky - Deligne
- ▶ Peu formalisé.
- ▶ Limites : non applicable à la masse des articles

Vérification communautaire

- ▶ Résultats centraux - émergence vérification communautaire.
- ▶ Exemples : BCHM, Perelmann.
- ▶ Cf Voevodsky - Deligne
- ▶ Peu formalisé.
- ▶ Limites : non applicable à la masse des articles
- ▶ Reconnaissance travail ?

A quoi sert un journal ?

Le rôle des journaux est peu clair

A quoi sert un journal ?

Le rôle des journaux est peu clair

- ▶ plus de rôle de distribution

A quoi sert un journal ?

Le rôle des journaux est peu clair

- ▶ plus de rôle de distribution
- ▶ reste vérification/évaluation

A quoi sert un journal ?

Le rôle des journaux est peu clair

- ▶ plus de rôle de distribution
- ▶ reste vérification/évaluation
- ▶ calqué sur modèle de distribution

A quoi sert un journal ?

Le rôle des journaux est peu clair

- ▶ plus de rôle de distribution
- ▶ reste vérification/évaluation
- ▶ calqué sur modèle de distribution

Quasi-totalité des articles de recherche publié en amont sur arxiv.

Quasi-totalité des articles de recherche publié en amont sur arxiv.
Avantages :

Quasi-totalité des articles de recherche publié en amont sur arxiv.

Avantages :

- ▶ Distribution rapide des connaissances

Quasi-totalité des articles de recherche publié en amont sur arxiv.

Avantages :

- ▶ Distribution rapide des connaissances
- ▶ Moindre nécessité d'être dans un groupe puissant

Quasi-totalité des articles de recherche publié en amont sur arxiv.

Avantages :

- ▶ Distribution rapide des connaissances
- ▶ Moindre nécessité d'être dans un groupe puissant
- ▶ Vérification communautaire.

Désavantages

- ▶ "Preprint de référence"

Désavantages

- ▶ " Preprint de référence"
- ▶ Difficulté à maintenir la sincérité de la littérature

Désavantages

- ▶ " Preprint de référence"
- ▶ Difficulté à maintenir la sincérité de la littérature
- ▶ Absence de confidentialité (rapports/erreurs).

Ecart production-processus

- ▶ Présentation uniquement de produit final

Ecart production-processus

- ▶ Présentation uniquement de produit final
- ▶ : processus disparue

Ecart production-processus

- ▶ Présentation uniquement de produit final
- ▶ : processus disparue
- ▶ difficultés à investir la production

Ecart production-processus

- ▶ Présentation uniquement de produit final
- ▶ : processus disparue
- ▶ difficultés à investir la production

Commentaire récurrent : "je suis quand vous faites, mais je ne sais pas commencer moi même"

Lien à la "peur" de l'erreur

Un constant : difficulté à accepter de tatonner

Lien à la "peur" de l'erreur

Un constant : difficulté à accepter de tatonner
Blocage à l'idée d'écrire quelque chose d'erronée.

Difficultés de formalisation

- ▶ l'étudiant "sent" l'idée

Difficultés de formalisation

- ▶ l'étudiant "sent" l'idée
- ▶ mais n'arrive pas à le formaliser

Difficultés de formalisation

- ▶ l'étudiant "sent" l'idée
- ▶ mais n'arrive pas à le formaliser

Commentaire récurrent : "je vois que c'est vrai, mais je ne sais pas le démontrer"

Lien au temps

- ▶ défaut de traduction

Lien au temps

- ▶ défaut de traduction
- ▶ compétence peu travaillée

Lien au temps

- ▶ défaut de traduction
- ▶ compétence peu travaillée
- ▶ pourtant, nécessite du temps.

Lien au temps

- ▶ défaut de traduction
- ▶ compétence peu travaillée
- ▶ pourtant, nécessite du temps.

Fuite en arrière

- ▶ Remonter jusqu'à ou dans la chaîne ?

Fuite en arrière

- ▶ Remonter jusqu'à ou dans la chaîne ?
- ▶ pas jusqu'à Peano chaque fois ?

Fuite en arrière

- ▶ Remonter jusqu'à ou dans la chaîne ?
- ▶ pas jusqu'à Peano chaque fois ?
- ▶ Conventions "cachées" sur les axiomes

Fuite en arrière

- ▶ Remonter jusqu'à ou dans la chaîne ?
- ▶ pas jusqu'à Peano chaque fois ?
- ▶ Conventions "cachées" sur les axiomes
- ▶ variable selon les niveaux/communautés.

Fuite en arrière

- ▶ Remonter jusqu'à ou dans la chaîne ?
- ▶ pas jusqu'à Peano chaque fois ?
- ▶ Conventions "cachées" sur les axiomes
- ▶ variable selon les niveaux/communautés.

Commentaire récurrent : "Est ce que j'ai le droit d'écrire **** ?"

Problème de temps

- ▶ La démonstration est présentée dès la L1

Problème de temps

- ▶ La démonstration est présentée dès la L1
- ▶ mais devient nécessaire qu'en L3

Problème de temps

- ▶ La démonstration est présentée dès la L1
- ▶ mais devient nécessaire qu'en L3
- ▶ Entrée en L3 : gros écarts

Problème de temps

- ▶ La démonstration est présentée dès la L1
- ▶ mais devient nécessaire qu'en L3
- ▶ Entrée en L3 : gros écarts

Nécessité du temps

- ▶ La démonstration = langage à assimiler

Nécessité du temps

- ▶ La démonstration = langage à assimiler
- ▶ grand temps incompressible d'apprentissage

Nécessité du temps

- ▶ La démonstration = langage à assimiler
- ▶ grand temps incompressible d'apprentissage
- ▶ (Enfant bilingue : estimations vers 30% du temps d'immersion pour un bilinguisme parfait)

Nécessité du temps

- ▶ La démonstration = langage à assimiler
- ▶ grand temps incompressible d'apprentissage
- ▶ (Enfant bilingue : estimations vers 30% du temps d'immersion pour un bilinguisme parfait)

Pressions sur le part des démonstrations

- ▶ Mutualisations nombreuses

Pressions sur le part des démonstrations

- ▶ Mutualisations nombreuses
- ▶ Compensations

Pressions sur le part des démonstrations

- ▶ Mutualisations nombreuses
- ▶ Compensations
- ▶ UEs non disciplinaires

Pressions sur le part des démonstrations

- ▶ Mutualisations nombreuses
- ▶ Compensations
- ▶ UEs non disciplinaires

Raisonnements par imitation/analogie

- ▶ Production naturelle des étudiants.

Raisonnements par imitation/analogie

- ▶ Production naturelle des étudiants.
- ▶ Difficultés à s'auto-corriger.

Raisonnements par imitation/analogie

- ▶ Production naturelle des étudiants.
- ▶ Difficultés à s'auto-corriger.
- ▶ Nécessaire dans la processus.

Langage naturel

- ▶ On approche la précision mathématique par le langage naturel.

Langage naturel

- ▶ On approche la précision mathématique par le langage naturel.
- ▶ Jugement : jusqu'à ou doit on aller ?

Langage naturel

- ▶ On approche la précision mathématique par le langage naturel.
- ▶ Jugement : jusqu'à ou doit on aller ?
- ▶ Variable selon les coutumes, pays, disciplines.

Langage naturel

- ▶ On approche la précision mathématique par le langage naturel.
- ▶ Jugement : jusqu'à ou doit on aller ?
- ▶ Variable selon les coutumes, pays, disciplines.
- ▶ Pas évident même pour nous !

Langage bas niveau vs langage haut niveau

- ▶ Quelle est la taille de blocs admissibles ?

Langage bas niveau vs langage haut niveau

- ▶ Quelle est la taille de blocs admissibles ?
- ▶ Très variable selon le niveau

Langage bas niveau vs langage haut niveau

- ▶ Quelle est la taille de blocs admissibles ?
- ▶ Très variable selon le niveau et selon le sujet...

Langage bas niveau vs langage haut niveau

- ▶ Quelle est la taille de blocs admissibles ?
- ▶ Très variable selon le niveau et selon le sujet...
- ▶ Non homogène entre enseignants.

Pédagogie inversée

Depuis 2016 : basculement des TDs en mode inversée.

- ▶ en TD : travail en groupe sous ma direction

Pédagogie inversée

Depuis 2016 : basculement des TDs en mode inversée.

- ▶ en TD : travail en groupe sous ma direction
- ▶ chaque groupe avance à son rythme

Pédagogie inversée

Depuis 2016 : basculement des TDs en mode inversée.

- ▶ en TD : travail en groupe sous ma direction
- ▶ chaque groupe avance à son rythme
- ▶ postage vidéo correction après le cours

Pédagogie inversée

Depuis 2016 : basculement des TDs en mode inversée.

- ▶ en TD : travail en groupe sous ma direction
- ▶ chaque groupe avance à son rythme
- ▶ postage vidéo correction après le cours
- ▶ quand tous les groupes ont travaillé

Pédagogie inversée

Depuis 2016 : basculement des TDs en mode inversée.

- ▶ en TD : travail en groupe sous ma direction
- ▶ chaque groupe avance à son rythme
- ▶ postage vidéo correction après le cours
- ▶ quand tous les groupes ont travaillé

Temps de TD essentiellement concentré sur le processus.

Pour la production.

- ▶ vidéos : correction complète

Pour la production.

- ▶ vidéos : correction complète
- ▶ DMs hebdomadaires

Pour la production.

- ▶ vidéos : correction complète
- ▶ DMs hebdomadaires
- ▶ "exercice d'écriture"

Pour la production.

- ▶ vidéos : correction complète
- ▶ DMs hebdomadaires
- ▶ "exercice d'écriture"
- ▶ exercices simples, rédaction précise attendue.

Différentiation

- ▶ Cours de L2 : expérimentation de différentiation

Différentiation

- ▶ Cours de L2 : expérimentation de différentiation
- ▶ Cours en présentiel “de base”

Différentiation

- ▶ Cours de L2 : expérimentation de différenciation
- ▶ Cours en présentiel “de base”
- ▶ Cours écrit “supplémentaire”

Différentiation

- ▶ Cours de L2 : expérimentation de différenciation
- ▶ Cours en présentiel “de base”
- ▶ Cours écrit “supplémentaire”

Pendant le cours

- ▶ passage de groupe en groupe

Pendant le cours

- ▶ passage de groupe en groupe
- ▶ recadre

Pendant le cours

- ▶ passage de groupe en groupe
- ▶ recadre rebondit

Pendant le cours

- ▶ passage de groupe en groupe
- ▶ recadre rebondit indique des pistes

Pendant le cours

- ▶ passage de groupe en groupe
- ▶ recadre rebondit indique des pistes indique des développements.

Pendant le cours

- ▶ passage de groupe en groupe
- ▶ recadre rebondit indique des pistes indique des développements.
- ▶ Adaption via indices au niveau des groupes

Pendant le cours

- ▶ passage de groupe en groupe
- ▶ recadre rebondit indique des pistes indique des développements.
- ▶ Adaption via indices au niveau des groupes
- ▶ Blocage généralisé : bascule en vertical.

Interaction en groupe

- ▶ Partir de la production de l'étudiant

Interaction en groupe

- ▶ Partir de la production de l'étudiant
- ▶ Quelles sont les bonnes idées ?

Interaction en groupe

- ▶ Partir de la production de l'étudiant
- ▶ Quelles sont les bonnes idées ?
- ▶ Que manque-t-il ?

Interaction en groupe

- ▶ Partir de la production de l'étudiant
- ▶ Quelles sont les bonnes idées ?
- ▶ Que manque-t-il ?
- ▶ Que ne fonctionne pas ?

Interaction en groupe

- ▶ Partir de la production de l'étudiant
- ▶ Quelles sont les bonnes idées ?
- ▶ Que manque-t-il ?
- ▶ Que ne fonctionne pas ?

Avantages généraux

- ▶ Travail principal sur le processus

Avantages généraux

- ▶ Travail principal sur le processus
- ▶ Etudiants actifs

Avantages généraux

- ▶ Travail principal sur le processus
- ▶ Etudiants actifs
- ▶ donc engagés.

Avantages généraux

- ▶ Travail principal sur le processus
- ▶ Etudiants actifs
- ▶ donc engagés.
- ▶ Suivi proche de la compréhension

Avantages généraux

- ▶ Travail principal sur le processus
- ▶ Etudiants actifs
- ▶ donc engagés.
- ▶ Suivi proche de la compréhension
- ▶ Travail par niveau possible

Avantages généraux

- ▶ Travail principal sur le processus
- ▶ Etudiants actifs
- ▶ donc engagés.
- ▶ Suivi proche de la compréhension
- ▶ Travail par niveau possible
- ▶ Choix des vidéos à regarder.

Points de vigilance

- ▶ Plus de temps par exercice

Points de vigilance

- ▶ Plus de temps par exercice
- ▶ Dépendance à l'autonomie

Points de vigilance

- ▶ Plus de temps par exercice
- ▶ Dépendance à l'autonomie
- ▶ Vigilance à tourner assez vite

Points de vigilance

- ▶ Plus de temps par exercice
- ▶ Dépendance à l'autonomie
- ▶ Vigilance à tourner assez vite
- ▶ Passer rapidement aux groupes susceptibles de bloquer

Points de vigilance

- ▶ Plus de temps par exercice
- ▶ Dépendance à l'autonomie
- ▶ Vigilance à tourner assez vite
- ▶ Passer rapidement aux groupes susceptibles de bloquer
- ▶ Groupes trop hétérogènes

Points de vigilance

- ▶ Plus de temps par exercice
- ▶ Dépendance à l'autonomie
- ▶ Vigilance à tourner assez vite
- ▶ Passer rapidement aux groupes susceptibles de bloquer
- ▶ Groupes trop hétérogènes
- ▶ Reflexe de demander de l'aide

Points de vigilance

- ▶ Plus de temps par exercice
- ▶ Dépendance à l'autonomie
- ▶ Vigilance à tourner assez vite
- ▶ Passer rapidement aux groupes susceptibles de bloquer
- ▶ Groupes trop hétérogènes
- ▶ Reflexe de demander de l'aide

Avantages spécifiques à la démonstration

- ▶ Erreurs debusquées

Avantages spécifiques à la démonstration

- ▶ Erreurs debusquées
- ▶ Rebondir : démonstration partielles valorisées

Avantages spécifiques à la démonstration

- ▶ Erreurs debusquées
- ▶ Rebondir : démonstration partielles valorisées