L'art de ne pas prouver n'importe quoi

Calculer, démontrer, convaincre

Emmanuel Beffara René Cori

Journée des CII Lycée et Université
Dijon, 18 janvier 2019

1. Introduction
2. Anatomie d'une démonstration
3. Les grands théorèmes
4. Démonstrations formelles
5. Conclusion

Introduction

L'intelligence de la démonstration?

L'algorithme est ce qui reste d'un procédé de calcul quand on n'a plus besoin d'être intelligent pour l'appliquer.

De même, dans le cas des démonstrations:

- il faut être intelligent pour démontrer
  — *l'incomplétude*
- quand on a démontré, plus besoin d'être intelligent pour avoir raison
  — *la démonstration comme programme*

Les étapes de la construction du raisonnement

Calculer	Expérimenter les objets mathématiques.
	Vérifier et infirmer des hypothèses.
Démontrer	Justifier la validité d'une affirmation.
	Établir des faits sans laisser de place au doute.
Convaincre	Expérimenter la démonstration.
	Sentir la validité des arguments.

Qu'est-ce que démontrer?

Démonstration, subst. fém.

A.— Action de montrer.
1. [Pour convaincre]
a) Action de montrer, d'expliquer par des expériences faites sous les yeux de l'assistance la vérité d'une donnée scientifique
. . .
2. [Pour vaincre]
a) Déploiement des forces armées
b) *P. anal.* Manifestation publique.
. . .
B.— Action de démontrer par le raisonnement.
1. Action qui consiste à démontrer quelque chose; raisonnement par lequel on établit la vérité d'une affirmation.
— *LOG.* Raisonnement qui établit la vérité d'une proposition déductivement, c'est-à-dire en la rattachant par un lien nécessaire à d'autres propositions admises comme vraies ou antérieurement démontrées
. . .

Source: TLFi

Anatomie d'une démonstration

Dissection d'une démonstration

On considère l'énoncé suivant:

Théorème

Pour tout entier n, si n est impair alors $n^2 - 1$ est multiple de 8.

Ce théorème est vrai, voyons pourquoi.

Dissection d'une démonstration

On considère l'énoncé suivant:

Théorème

Pour tout entier n, si n est impair alors $n^2 - 1$ est multiple de 8.

Ce théorème est vrai, voyons pourquoi.

On met en scène deux interlocuteurs:

- P veut **p**rouver que c'est vrai,
- O apporte des **o**bjections.

Un exemple pour rien

qui	réplique	but
P	La proposition est vraie.	$\forall n, (\exists \ell, n = 2\ell + 1) \rightarrow (\exists k, n^2 - 1 = 8k)$
O	Non,	$\exists n, (\exists \ell, n = 2\ell + 1) \wedge (\forall k, n^2 - 1 \neq 8k)$
	ça ne marche pas avec 26.	$(\exists \ell, 26 = 2\ell + 1) \wedge (\forall k, 26^2 - 1 \neq 8k)$
P	Si, parce que	$(\forall \ell, 26 \neq 2\ell + 1) \vee (\exists k, 26^2 - 1 = 8k)$
	26 n'est pas impair.	$\forall \ell, 26 \neq 2\ell + 1$
O	Si, il est impair,	$\exists \ell, 26 = 2\ell + 1$
	prends $\ell = 12$.	$26 = 2 \times 12 + 1$
	Ah non, ça ne marche pas.	

Un premier exemple

qui	réplique	but
P	La proposition est vraie.	$\forall n, (\exists \ell, n = 2\ell + 1) \to (\exists k, n^2 - 1 = 8k)$
O	Non,	$\exists n, (\exists \ell, n = 2\ell + 1) \wedge (\forall k, n^2 - 1 \neq 8k)$
	ça ne marche pas avec 7.	$(\exists \ell, 7 = 2\ell + 1) \wedge (\forall k, 7^2 - 1 \neq 8k)$
P	Si, parce que	$(\forall \ell, 7 \neq 2\ell + 1) \vee (\exists k, 7^2 - 1 = 8k)$
	7 n'est pas impair.	$\forall \ell, 7 \neq 2\ell + 1$
O	Si, il est impair	$\exists \ell, 7 = 2\ell + 1$
	prends $\ell = 3$.	$7 = 2 \times 3 + 1$
P	D'accord, mais	$(\forall \ell, 7 \neq 2\ell + 1) \vee (\exists k, 7^2 - 1 = 8k)$
	$7^2 - 1$ est multiple de 8,	$\exists k, 7^2 - 1 = 8k$
	prends $k = 6$.	$7^2 - 1 = 8 \times 6$
O	Je calcule...	$48 = 48$
	D'accord, ça marche avec 7.	

Un deuxième exemple

qui	réplique	but
P	La proposition est vraie.	$\forall n, (\exists \ell, n = 2\ell + 1) \to (\exists k, n^2 - 1 = 8k)$
O	Non,	$\exists n, (\exists \ell, n = 2\ell + 1) \wedge (\forall k, n^2 - 1 \neq 8k)$
	ça ne marche pas avec 19.	$(\exists \ell, 19 = 2\ell + 1) \wedge (\forall k, 19^2 - 1 \neq 8k)$
P	Si, parce que	$(\forall \ell, 19 \neq 2\ell + 1) \vee (\exists k, 19^2 - 1 = 8k)$
	19 n'est pas impair.	$\forall \ell, 19 \neq 2\ell + 1$
O	Si, il est impair,	$\exists \ell, 19 = 2\ell + 1$
	prends $\ell = 9$.	$19 = 2 \times 9 + 1$
P	D'accord, mais	$(\forall \ell, 19 \neq 2\ell + 1) \vee (\exists k, 19^2 - 1 = 8k)$
	$19^2 - 1$ est multiple de 8,	$\exists k, 19^2 - 1 = 8k$
	prends $k = 45$.	$19^2 - 1 = 8 \times 45$
O	Je calcule...	$360 = 360$
	D'accord, ça marche aussi.	

Généralisation des exemples

qui	réplique	but
P	La proposition est vraie.	$\forall n, (\exists \ell, n = 2\ell + 1) \to (\exists k, n^2 - 1 = 8k)$
O	Non,	$\exists n, (\exists \ell, n = 2\ell + 1) \wedge (\forall k, n^2 - 1 \neq 8k)$
	ça ne marche pas avec N.	$(\exists \ell, N = 2\ell + 1) \wedge (\forall k, N^2 - 1 \neq 8k)$
P	Si, parce que	$(\forall \ell, N \neq 2\ell + 1) \vee (\exists k, N^2 - 1 = 8k)$
	N n'est pas impair.	$\forall \ell, N \neq 2\ell + 1$
O	Suppose qu'il est impair,	$\exists \ell, N = 2\ell + 1$
	prends $\ell = L$.	$N = 2 \times L + 1$
P	Admettons, mais	$(\forall \ell, N \neq 2\ell + 1) \vee (\exists k, N^2 - 1 = 8k)$
	$N^2 - 1$ est multiple de 8,	$\exists k, N^2 - 1 = 8k$
	prends $k = L(L + 1)/2$	$N^2 - 1 = 8 \times L(L + 1)/2$
	et développe N.	$(2L + 1)^2 - 1 = 8 \times L(L + 1)/2$
O	Je calcule...	$4L^2 + 4L = 4L^2 + 4L$
	D'accord, ça marche.	

Démonstration rédigée

P écrit:

Soit $n \in \mathbb{N}$.
Soit $\ell \in \mathbb{N}$
tel que $n = 2\ell + 1$.
On a $n^2 - 1 = (2\ell + 1)^2 - 1 = 4\ell^2 + 4\ell = 8 \times \ell(\ell + 1)/2$.
Donc $n^2 - 1$ *est multiple de 8.*
Donc si $n = 2\ell + 1$ *alors* $n^2 - 1$ *est multiple de 8.*
Donc si n est impair alors $n^2 - 1$ *est multiple de 8.*
Donc pour tout n, si n est impair alors $n^2 - 1$ *est multiple de 8.*

O est d'accord (s'il est d'accord avec le fait que $\ell(\ell + 1)/2$ est un entier).

Démonstration rédigée avec des formules

P écrit:

Soit $n \in \mathbb{N}$.
Soit $\ell \in \mathbb{N}$
tel que $n = 2\ell + 1$.
On a $n^2 - 1 = (2\ell + 1)^2 - 1 = 4\ell^2 + 4\ell = 8 \times \ell(\ell + 1)/2$.
Donc $\exists k \in \mathbb{N}, n^2 - 1 = 8k$, *en posant* $k = \ell(\ell + 1)/2$.
Donc si $n = 2\ell + 1$ *alors* $\exists k \in \mathbb{N}, n^2 - 1 = 8k$.
Donc si $\exists \ell \in \mathbb{N}, n = 2\ell + 1$ *alors* $\exists k \in \mathbb{N}, n^2 - 1 = 8k$.
Donc $(\exists \ell \in \mathbb{N}, n = 2\ell + 1) \rightarrow (\exists k \in \mathbb{N}, n^2 - 1 = 8k)$.
Donc $\forall n \in \mathbb{N}, (\exists \ell \in \mathbb{N}, n = 2\ell + 1) \rightarrow (\exists k \in \mathbb{N}, n^2 - 1 = 8k)$.

O est toujours d'accord.

Démonstration à la Gentzen

P écrit:

- $n = 2\ell + 1 \vdash n = 2\ell + 1$ (axiome)
- $n = 2\ell + 1 \vdash n^2 - 1 = (2\ell + 1)^2 - 1$ (substitution)
- $n = 2\ell + 1 \vdash n^2 - 1 = 8 \times \ell(\ell + 1)/2$ (calcul)
- $n = 2\ell + 1 \vdash \exists k \in \mathbb{N}, n^2 - 1 = 8k$ (introduction $\exists$ avec $k = \ell(\ell + 1)/2$)
- $\exists \ell \in \mathbb{N}, n = 2\ell + 1 \vdash \exists k \in \mathbb{N}, n^2 - 1 = 8k$ (introduction de $\exists$ en hypothèse)
- $\vdash (\exists \ell \in \mathbb{N}, n = 2\ell + 1) \to (\exists k \in \mathbb{N}, n^2 - 1 = 8k)$ (introduction de l'implication)
- $\vdash \forall n \in \mathbb{N}, (\exists \ell \in \mathbb{N}, n = 2\ell + 1) \to (\exists k \in \mathbb{N}, n^2 - 1 = 8k)$ (introduction de $\forall$)

O ne sait plus trop quoi penser...

Faisons le point

On est passé par plusieurs étapes:

- Tester la propriété sur différentes valeurs.
- Trouver des arguments pour se convaincre que P saurait avoir raison contre chaque tentative de contre-exemple de O.
- Poser cette *stratégie* sous forme d'un raisonnement argumenté.

La démonstration finale comporte deux aspects:

- la structure argumentative, guidée par la forme de l'énoncé à démontrer,
- le contenu constructif, qui donne le témoin d'existence dans chaque cas (le choix de $k = \ell(\ell + 1)/2$).

Une fois que la démonstration est posée par P, il n'y a plus de place pour la discussion. La seule chose que O peut faire, c'est de vérifier que la démonstration est bien construite.

Pour aller plus loin

J'ai passé des choses sous silence:

- Justifier que $\ell(\ell+1)/2$ est un entier, raisonnement par cas sur la parité.
- Comment utiliser des résultats connus
  Exemple: tout entier est pair ou impair.

Pour aller plus loin

J'ai passé des choses sous silence:

- Justifier que $\ell(\ell+1)/2$ est un entier, raisonnement par cas sur la parité.
- Comment utiliser des résultats connus
  Exemple: tout entier est pair ou impair.

L'arithmétique se prête bien à la démonstration, comment passer à des objets plus complexes?

- Nombres réels
- Objets géométriques
- Fonctions
- Structures plus abstraites. . .

Les grands théorèmes

Les enjeux

Lors de la *crise des fondements* à la fin du XIXème sciècle, on cherche à fonder les mathématiques sur des bases formelles solides, pour résoudre les paradoxes et garantir l'absence de contradictions.

Il apparaît nécessaire de formaliser le langage mathématique.

Une formalisation sera acceptable si elle est

- **cohérente**: on ne peut pas y démontrer une chose et son contraire,
- **correcte**: les énoncés qu'on y démontre formellement sont vrais,
- **complète**: tout ce qui est vrai peut y être démontré,
- **décidable**: on peut déterminer si un énoncé donné est vrai ou faux,
- **expressive**: toutes les notions mathématiques peuvent y être représentées.

Les enjeux

Lors de la *crise des fondements* à la fin du XIXème sciècle, on cherche à fonder les mathématiques sur des bases formelles solides, pour résoudre les paradoxes et garantir l'absence de contradictions.

Il apparaît nécessaire de formaliser le langage mathématique.

Une formalisation sera acceptable si elle est

- **cohérente**: on ne peut pas y démontrer une chose et son contraire,
- **correcte**: les énoncés qu'on y démontre formellement sont vrais,
- **complète**: tout ce qui est vrai peut y être démontré,
- **décidable**: on peut déterminer si un énoncé donné est vrai ou faux,
- **expressive**: toutes les notions mathématiques peuvent y être représentées.

Spoiler: c'est impossible.

Formaliser les démonstrations

La première question est la **cohérence**: on ne doit pas pouver démontrer une chose et son contraire.

Pour établir qu'une chose n'est **pas** démontrable,
il faut montrer qu'il n'en existe pas de démonstration,
donc il faut définir l'ensemble des démonstrations,
donc définir mathématiquement ce qu'est une démonstration.

Il y a différentes façons de le faire, on y reviendra plus loin.

La complétude

théorie = ensemble d'axiomes (énoncés clos)
modèle = structure qui valide les axiomes

Théorème de complétude

Si un énoncé A est satisfait dans tout modèle d'une théorie $\mathcal{T}$, alors A est démontrable dans $\mathcal{T}$.

Des façons adéquates de reformuler ce théorème:

- Si un énoncé est toujours vrai, alors on peut le démontrer.
- Si on peut démontrer un énoncé au moyen d'une démonstration usuelle, alors on peut le faire par une démonstration formelle.
- La notion formelle capture correctement la notion de notion intuitive de démonstration.

On établit généralement le théorème en montrant que toute théorie non contradictoire admet un modèle.

L'incomplétude

Premier théorème d'incomplétude

Toute théorie permettant d'exprimer l'arithmétique élémentaire contient des énoncés indécidables.

Précisons les mots:

- L'**arithmétique élémentaire** est le vocabulaire de l'arithmétique (addition, multiplication) et les règles de calcul de base qui s'y rapportent. Même pas besoin de parler du principe de récurrence.
- Un énoncé est **indécidable** s'il ne peut être ni démontré ni réfuté dans la théorie considérée.

Indécidabilité?

Exemples classiques d'énoncés indécidables:

- Le postulat des parallèles dans la géométrie d'Euclide.
- L'hypothèse du continu, dans la théorie des ensembles.

La méthode de Gödel pour montrer l'incomplétude en général:

- Poser un *codage* des énoncés et des démonstrations dans les entiers.
- Utiliser ce codage pour écrire le paradoxe du menteur:
  « Cette phrase n'est pas démontrable ».
- Conclure que si l'arithmétique est cohérente, alors cet énoncé n'est ni démontrable ni réfutable.

Cela nécessite un dialogue subtil entre les démonstrations intuitives, les démonstrations formelles et leur représentation dans le système étudié.

Remarque: la phrase « Cette phrase n'est pas démontrable » est donc à la fois **vraie** et **non démontrable**.

L'incomplétude

Second théorème d'incomplétude

Si $\mathcal{T}$ est une théorie non-contradictoire qui peut exprimer l'arithmétique, alors la cohérence de $\mathcal{T}$ n'est pas démontrable dans $\mathcal{T}$.

Reformulations:

- Une théorie ne peut pas démontrer sa propre cohérence.
- Si une théorie démontre sa propre cohérence, alors elle est incohérente!
- Il ne peut pas y avoir de justification interne de la cohérence des mathématiques.

Où va-t-on à partir de là?

Démonstrations formelles

Pourquoi formaliser?

Si l'incomplétude interdit de justifier la cohérence des mathématiques de façon interne, quel est l'intérêt de formaliser les démonstrations?

- Cela permet d'établir les grands théorèmes
- Cela d'interdit pas de justifier la cohérence d'un système à partir d'un système plus puissant.
- Cela permet de comprendre la structure des démonstrations et de calculer avec.

Les questionnements qui en découlent:

- Que signifie une démonstration?
- Pourquoi les règles logiques sont-elles ce qu'elles sont?

Démonstrations à la Hilbert

Définition

Une démonstration est une suite finie d'énoncés telle que chacun est soit un axiome soit l'application d'une règle logique valide à des énoncés précédents.

- Reprend formellement l'idée d'une suite d'assertion qui découlent des axiomes par nécessité.
- Peu de règles de déduction:
  - *modus ponens*
  - principe de généralisation
- Différents schémas d'axiomes logiques
  - $\alpha \to (\beta \to \alpha)$
  - $(\alpha \to (\beta \to \gamma)) \to ((\alpha \to \beta) \to (\alpha \to \gamma))$
  - $(\neg\alpha \to \neg\beta) \to (\beta \to \alpha)$
  - etc.

Des objets formellement assez simples, mais leur construction et leur étude n'est pas facile.

Démonstrations à la Gentzen

Définition

Une démonstration est un arbre formé de règles de déduction comme

$$\frac{A \quad A \to B}{B} \qquad \frac{A \quad B}{A \wedge B} \qquad \frac{A \wedge B}{A} \qquad \ldots$$

dont les feuilles sont des axiomes.

- On démontre des *séquents*: des assertions de la forme $A_1, A_2, \ldots, A_n \vdash B$ (sous les hypothèses $A_1, A_2, \ldots, A_n$, la conclusion B est valide).
- Pour chaque connecteur logique, des règle d'introduction et d'élimination.

On y gagne la possibilité de démontrer la cohérence du système logique sans avoir recours à la notion de modèle:

- Toute démonstration peut être mise sous une forme canonique par un procédé *calculatoire*,
- les formes canoniques ne peuvent pas démontrer l'absurde.

L'interprétation fonctionnelle

Le sens d'une démonstration est un procédé pour calculer une "preuve" de l'énoncé démontré:

- une preuve de $P \wedge Q$ est la donnée d'une preuve de P et d'une preuve de Q
- une preuve de $P \vee Q$ est le choix de P ou de Q et une preuve associée
- une preuve de $P \to Q$ est une procédé qui calcule une preuve de Q si on lui donne une preuve de P
- une preuve de $\exists x \in E, P(x)$ est la donnée d'une valeur $a \in E$ et d'une preuve de $P(a)$
- une preuve de $\forall x \in E, P(x)$ est un procédé qui calcule une preuve de $P(a)$ si on lui donne une valeur a
- etc.

Cela formalise l'interprétation d'une démonstration comme programme pour calculer un témoin de la validité du théorème.

Démonstrations comme stratégies

En poussant plus loin l'interprétation, on peut mettre en évidence le côté *interactif* de la démonstration.

Une démonstration est un procédé pour réfuter toute contradiction:

- pour prouver P, réfuter $\neg P$

La façon de réfuter un énoncé dépend de sa forme:

- pour réfuter $P \wedge Q$, choisir P ou Q et le réfuter
- pour réfuter $P \vee Q$, réfuter P et réfuter Q
- pour réfuter $P \rightarrow Q$, affirmer P et réfuter Q
- pour réfuter $\forall x \in E, P(x)$, fournir un $a \in E$ et réfuter $P(a)$
- pour réfuter $\exists x \in E, P(x)$, donner un procédé pour réfuter tout $P(x)$
- etc.

La démonstration permet de *calculer* quel coup jouer dans un tel jeu d'argumentation.

Conclusion

Stratégies de calcul et de démonstration

L'algorithme est une stratégie de calcul,
la démonstration est une stratégie d'argumentation.

- énoncé = type d'information = règle du jeu
- démonstration = programme = stratégie
- exemple = exécution = partie

Une démonstration peut être vue comme un algorithme pour gagner dans une argumentation visant à justifier une assertion.

Cette analogie prend une forme très précise sous le nom de *correspondance de Curry-Howard*, élément central en théorie de la démonstration et des langages de programmation.

Où est le calcul dans la démonstration?

Calculer Un démonstration *formelle* est un programme de calcul qui permet de produire de façon systématique des justifications pour une affirmation donnée.

Avec une démonstration complète, plus besoin de créativité pour avoir raison.

Démontrer L'incomplétude montre qu'on ne peut pas calculer automatiquement si un énoncé est démontrable ou pas (et donc calculer une démonstration).

La créativité reste nécessaire pour trouver des démonstrations (à moins de se limiter à des cadres moins expressifs).

Convaincre En quelque sorte, une démonstration en langue naturelle explique à l'interlocuteur comment reconstruire la démonstration formelle.

D'où l'importance de l'expérimentation dans le développement du raisonnement mathématique...