Initiation à la Recherche
Crise en mathématique et naissance de l'informatique

Polytech Lille — IS 4
François Boulier

6 septembre 2022

1. Introduction
2. Intermède 1
3. Intermède 2
4. Intermède 3
5. Crise en mathématiques
6. Le deuxième problème de Hilbert
7. L'Entscheidungsproblem
8. Retour sur Kuhn

Les sciences, selon Kuhn

Une discipline scientifique progresse suivant le processus suivant (les trois dernières étapes se répétant indéfiniment) :

1. pré-science,
2. émergence d'un premier paradigme,
3. science normale (avec apparition intermittente d'anomalies),
4. crise,
5. révolution scientifique et changement de paradigme.

Les mathématiques sont-elles une science ? Ont-elles connu des crises ?

Les mathématiques sont-elles une science ?

Kuhn suggère que oui mais ne donne aucun exemple.

Les mathématiques sont-elles une science ?

Kuhn suggère que oui mais ne donne aucun exemple.

Y a-t-il des paradigmes en mathématiques ?

Les mathématiques sont-elles une science ?

Kuhn suggère que oui mais ne donne aucun exemple.

Y a-t-il des paradigmes en mathématiques ?

« Une *définition* du mot « science » a-t-elle une si grande importance ? Une définition peut-elle assurer à quelqu'un qu'il est ou n'est pas un homme de science ? [. . .] On en arrive inévitablement à supposer que l'enjeu du problème est plus fondamental. Sans doute les questions que l'on se pose réellement sont-elles plutôt : pourquoi ma spécialité ne réussit-elle pas à progresser comme la physique, par exemple ? Ce ne sont pas là pourtant des questions auxquelles on puisse répondre en se mettant d'accord sur une définition. »

Ce cours raconte l'histoire d'une crise en mathématiques et l'influence qu'elle a eue sur les débuts de l'informatique.

1 Introduction

2 Intermède 1

3 Intermède 2

4 Intermède 3

5 Crise en mathématiques

6 Le deuxième problème de Hilbert

7 L'Entscheidungsproblem

8 Retour sur Kuhn

Suites ultimement périodiques et algorithme de Floyd

Déf. Une suite (u_n) est **ultimement périodique** si

$$\exists\, i, k \in \mathbb{N}, \quad \forall\, j \geq i\,, \quad u_j = u_{j+k}\,.$$

Prop. Si E est fini et (u_n) est une suite d'éléments de E de la forme $u_{n+1} = f(u_n)$ alors (u_n) est ultimement périodique.

Algo. Si (u_n) est ultimement périodique, l'algorithme de **Floyd** détecte l'entrée dans la période.

$u = a$
$v = f(a)$
while $u \neq v$ do
  $u = f(u)$
  $v = f(f(v))$
od

1 Introduction

2 Intermède 1

3 Intermède 2

4 Intermède 3

5 Crise en mathématiques

6 Le deuxième problème de Hilbert

7 L'Entscheidungsproblem

8 Retour sur Kuhn

L'arrêt des algorithmes est algorithmiquement indécidable

Fixons un langage de programmation.

Toute fonction $P(x \in \mathbb{N})$, peut être codée par un entier p.

On note $\mathbb{E}$ l'ensemble des entiers qui codent des fonctions.

On suppose l'existence d'une fonction A, à deux paramètres $p \in \mathbb{E}$ et $x \in \mathbb{N}$, qui retourne *true* si $P(x)$ s'arrête, *false* sinon.

function $M(q \in \mathbb{E})$
  if $A(q, q) =$ *vrai* then
    while *vrai* do
    od
  fi

On note $\mathbb{H} = \{q \in \mathbb{E} \mid M(q) \text{ s'arrête}\}$. Est-ce que $m \in \mathbb{H}$?

L'arrêt des algorithmes est algorithmiquement indécidable

Fixons un langage de programmation.

Toute fonction $P(x \in \mathbb{N})$, peut être codée par un entier p.

On note $\mathbb{E}$ l'ensemble des entiers qui codent des fonctions.

On suppose l'existence d'une fonction A, à deux paramètres $p \in \mathbb{E}$ et $x \in \mathbb{N}$, qui retourne *true* si $P(x)$ s'arrête, *false* sinon.

function $M(q \in \mathbb{E})$
  if $A(q, q) =$ *vrai* then
    while *vrai* do
    od
  fi

On note $\mathbb{H} = \{q \in \mathbb{E} \mid M(q) \text{ s'arrête}\}$. Est-ce que $m \in \mathbb{H}$?

L'algorithme A ne peut pas exister puisque l'hypothèse de son existence conduit à un paradoxe.

L'arrêt des programmes est algorithmiquement décidable

L'ensemble S des états possibles d'un ordinateur est fini

$$|S| \simeq 2^{\text{le nombre de bits de la mémoire}}$$

Un ordinateur qui exécute un programme énumère les termes d'une suite (u_n) à valeurs dans S, de la forme :

$$u_{n+1} = f(u_n)\,.$$

Si un programme ne s'arrête pas, la suite (u_n) est ultimement périodique.

L'arrêt des programmes est algorithmiquement décidable

L'ensemble S des états possibles d'un ordinateur est fini

$$|S| \simeq 2^{\text{le nombre de bits de la mémoire}}$$

Un ordinateur qui exécute un programme énumère les termes d'une suite (u_n) à valeurs dans S, de la forme :

$$u_{n+1} = f(u_n)\,.$$

Si un programme ne s'arrête pas, la suite (u_n) est ultimement périodique.

Grâce à l'algorithme de Floyd, le problème de l'arrêt des programmes est algorithmiquement décidable.

Un algorithme n'est pas un programme

Un algorithme n'est pas limité en mémoire (le pivot de Gauss s'applique à des matrices de dimension abitrairement grande).

On n'a pas besoin d'une définition de la notion d'algorithme pour se convaincre qu'un procédé particulier est bien un algorithme.

En 1935, dans le cadre d'une crise en mathématiques, Turing cherche à démontrer l'inexistence d'un algorithme.

Il tente une définition :
les machines de Turing

1 Introduction

2 Intermède 1

3 Intermède 2

4 Intermède 3

5 Crise en mathématiques

6 Le deuxième problème de Hilbert

7 L'Entscheidungsproblem

8 Retour sur Kuhn

Les machines de Turing

- Ce sont des tentatives de définition précise de la notion d'algorithme.
- Ce ne sont pas des modèles abstraits d'ordinateurs (la mémoire infinie change tout).
- Leur description ressemble à celle d'une machine physique.

Exemples de machines de Turing

Symbole de fin de ruban $*$, vide Λ.
État initial q_1. États finaux q_2 (vrai) et q_3 (faux).
Déplacements L (left), R (right) et S (sur place).
La configuration initiale du ruban est la donnée de la machine.

if 1 then *true* else *false*

$q_1 * \to * S\ q_3$, $q_1\, 0 \to 0\, S\ q_3$, $q_1\, 1 \to 1\, S\ q_2$, $q_1\, \Lambda \to \Lambda\, S\ q_3$.

while *true* do done

$q_1 * \to * S\ q_1$, $q_1\, 0 \to 0\, S\ q_1$, $q_1\, 1 \to 1\, S\ q_1$, $q_1\, \Lambda \to \Lambda\, S\ q_1$.

if 1 then *true* else while *true* do done

$q_1 * \to * S\ q_4$, $q_1\, 0 \to 0\, S\ q_4$, $q_1\, 1 \to 1\, S\ q_2$, $q_1\, \Lambda \to \Lambda\, S\ q_4$,
$q_4 * \to * S\ q_4$, $q_4\, 0 \to 0\, S\ q_4$, $q_4\, 1 \to 1\, S\ q_4$, $q_4\, \Lambda \to \Lambda\, S\ q_4$.

L'arrêt des machines de Turing est indécidable par machine de Turing

- On peut numéroter les machines de Turing
- On peut même définir des machines de Turing universelles, qui prennent en entrée un couple (i, x) d'entiers et qui appliquent la machine de Turing numéro i à l'entrée x

Théorème (Turing, 1936). Il n'existe pas de machine de Turing A, qui prenne en entrée un couple (i, x) d'entiers, qui retourne *vrai* si la machine de Turing numéro i s'arrête lorsqu'on l'applique à x et *faux* sinon.

1 Introduction

2 Intermède 1

3 Intermède 2

4 Intermède 3

5 Crise en mathématiques

6 Le deuxième problème de Hilbert

7 L'Entscheidungsproblem

8 Retour sur Kuhn

La notion de vérité en mathématiques

- Jusqu'au XVIIIème siècle, les objets dont traitent les mathématiciens sont très proches de ceux dont traitent les sciences de la nature. Ils sont connaissables à la fois par l'intuition et par le raisonnement.
- Les axiomes de la géométrie euclidienne sont « vrais ».

Les axiomes de la géométrie euclidienne

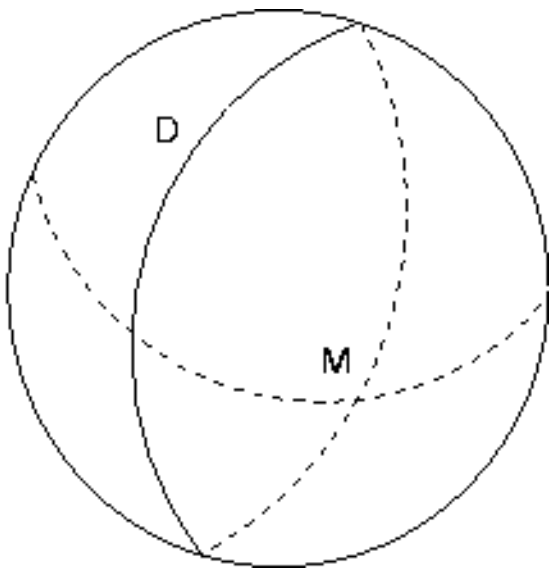
Version simplifiée :

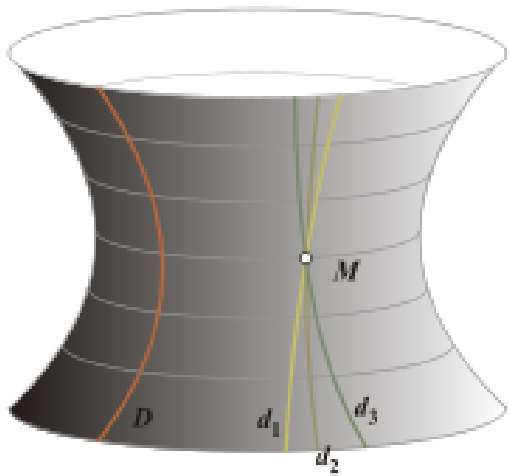
1. étant donnés deux points A et B, il existe une droite passant par A et B ;
2. tout segment $[AB]$ est prolongeable en une droite passant par A et B ;
3. pour tout point A et tout point B distinct de A, on peut décrire un cercle de centre A passant par B ;
4. tous les angles droits sont égaux entre eux ;
5. par un point extérieur à une droite, on peut mener une parallèle et une seule à cette droite.

Géométries non euclidiennes

Au XIXème siècle, on s'aperçoit qu'on peut nier le cinquième postulat et construire des géométries cohérentes.

L'opinion courante que les axiomes de la géométrie (ou de n'importe quelle discipline) peuvent être établis en raison de leur évidence, s'effondre.





Les définitions informelles peuvent poser problème

L'ensemble de tous les ensembles

Les définitions informelles peuvent poser problème

L'ensemble de tous les ensembles

Si on autorise des ensembles qui se contiennent eux-mêmes, que penser de l'ensemble E de tous les ensembles qui ne se contiennent pas eux-mêmes ?

Les définitions informelles peuvent poser problème

L'ensemble de tous les ensembles

Si on autorise des ensembles qui se contiennent eux-mêmes, que penser de l'ensemble E de tous les ensembles qui ne se contiennent pas eux-mêmes ?

Les définitions en Français

Soit F l'ensemble de tous les entiers qui peuvent se définir par moins de seize mots en Français.

Les définitions informelles peuvent poser problème

L'ensemble de tous les ensembles

Si on autorise des ensembles qui se contiennent eux-mêmes, que penser de l'ensemble E de tous les ensembles qui ne se contiennent pas eux-mêmes ?

Les définitions en Français

Soit F l'ensemble de tous les entiers qui peuvent se définir par moins de seize mots en Français.

Que penser de n : « le plus petit entier qui n'est pas définissable par moins de seize mots Français ».

Les définitions informelles peuvent poser problème

L'ensemble de tous les ensembles

Si on autorise des ensembles qui se contiennent eux-mêmes, que penser de l'ensemble E de tous les ensembles qui ne se contiennent pas eux-mêmes ?

Les définitions en Français

Soit F l'ensemble de tous les entiers qui peuvent se définir par moins de seize mots en Français.

Que penser de n : « le plus petit entier qui n'est pas définissable par moins de seize mots Français ».

Supposons que n n'existe pas. Cela signifie-t-il que *tout* entier est définissable par moins de seize mots en Français ?

Le point de vue formaliste

« Comment l'intuition peut-elle nous tromper à ce point ? » (Henri Poincaré, 1905)

Fin XIXème, un groupe dominant de mathématiciens adopte un point de vue beaucoup plus formel et abstrait.

Les mathématiques sont vues comme l'art de déduire des théorèmes à partir d'axiomes par des raisonnements de pure logique, mais où la question de la véracité des axiomes n'a plus de sens.

David Hilbert

Exemple de théorie axiomatique : l'arithmétique de Peano

Sept axiomes « arithmétiques ». Un schéma d'axiome pour le raisonnement par récurrence. Cinq schémas d'axiomes logiques. Deux règles d'inférence.

1. $\forall x\ \neg(sx = 0)$
2. $\forall x\ \exists y\ (\neg x = 0 \to sy = x)$
3. $\forall x\ \forall y\ (sx = sy \to x = y)$
4. $\forall x\ (x + 0 = x)$
5. $\forall x\ \forall y\ (x + sy = s(x + y))$
6. $\forall x\ (x \cdot 0 = 0)$
7. $\forall x\ \forall y\ (x \cdot sy = (x \cdot y) + x)$
   - $[P(0) \wedge (\forall x\ P(x) \to P(sx))] \to \forall x\ P(x)$

1. $A \to (B \to A)$
2. $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$
3. $(\neg A \to \neg B) \to (B \to A)$
4. $\forall x\ A(x) \to A(t)$
5. $(A \to B) \to (A \to \forall x\ B)$

modus ponens. Des formules $A \to B$ et A on peut déduire B ;

généralisation. De la formule A, on peut déduire $\forall x\ A(x)$.

Démonstration dans le cadre d'une théorie axiomatique

On montre qu'on peut déduire $\forall\ z\ p(z,z)$ à partir de l'hypothèse $\forall x\ \forall y\ p(x,y)$.

f_1	$\forall x\ \forall y\ p(x,y)$	(hypothèse)
f_2	$\forall x\ \forall y\ p(x,y) \to \forall y\ p(z,y)$	(schéma d'axiome logique 4)
f_3	$\forall y\ p(z,y)$	(modus ponens avec f_1 et f_2)
f_4	$\forall y\ p(z,y) \to p(z,z)$	(schéma d'axiome logique 4)
f_5	$p(z,z)$	(modus ponens avec f_3 et f_4)
f_6	$\forall z\ p(z,z)$	(généralisation)

La vérification d'une démonstration ne demande aucune intelligence.

Questions qu'on peut se poser sur une théorie axiomatique

- est-elle consistante ? Est-on sûr qu'il est impossible de démontrer une chose (un théorème) et son contraire (la négation de ce théorème) ?
- est-elle complète ? Étant donné une formule, est-on sûr qu'il existe soit une démonstration de la formule, soit une démonstration de la négation de la formule ?
- est-elle algorithmiquement décidable ? Existe-t-il un algorithme, qui prenne en entrée une formule quelconque, et qui détermine si la formule admet une démonstration dans le cadre de cette théorie ?

Ces questions « ont été posées » par Hilbert entre 1900 et 1930.

Clarifier les sens qu'on peut donner aux différents mots a fait partie du travail des mathématiciens. Attention à l'histoire des sciences !

Le deuxième problème de Hilbert (1900)

- dans une théorie axiomatique, si on peut démontrer une formule et sa négation, alors *toute* formule est démontrable ;
- des définitions axiomatiques très naturelles des théories peuvent conduire à des phénomèmes contre-intuitifs et même, à des paradoxes.

Le deuxième problème

Démontrer la consistance de l'arithmétique de Peano.

Hilbert cherche une démonstration qui n'emploie que des « procédés finis », pour éviter de démontrer une théorie dont on doute avec une autre théorie, plus compliquée, et donc encore plus douteuse.

Réponse négative au deuxième problème

En 1931, Kurt Gödel montra que le deuxième problème n'a pas de solution, sous la forme recherchée par Hilbert (n'utilisant que des « procédés finis »).

L'idée de Kurt Gödel

- On peut coder une formule de l'arithmétique de Peano par un entier.
- On peut même coder une « démonstration dans l'arithmétique de Peano » par un entier.
- Des énoncés comme « x est un nombre pair » sont tout aussi arithmétiques que « x est une démonstration dans l'arithmétique de Peano »
- Gödel construisit une formule G signifiant « la formule G n'est pas démontrable dans l'arithmétique de Peano ».

L'arithmétique de Peano est, soit incomplète, soit inconsistante.

La construction de Gödel est « générique ».

Remarques

- La consistance de l'arithmétique de Peano a été démontrée par Gentzen en 1936 mais en utilisant une théorie plus puissante que l'arithmétique de Peano (pas uniquement des « procédés finis »).
- L'arithmétique de Peano est donc incomplète.
- Exemple (Pour La Science, Jean-Paul Delahaye, Sept. 2021)

$$M(x) \quad = \quad \text{si } x < 0 \text{ alors } -x \text{ sinon } M(x - M(x-1))/2$$

L'énoncé « $M(x)$ s'arrête pour tout entier x » peut être codé dans l'arithmétique de Peano mais, dans le cadre de cette arithmétique, il n'a aucune démonstration. Pourtant il est vrai : il a été démontré en utilisant une théorie plus puissante.

1 Introduction

2 Intermède 1

3 Intermède 2

4 Intermède 3

5 Crise en mathématiques

6 Le deuxième problème de Hilbert

7 L'Entscheidungsproblem

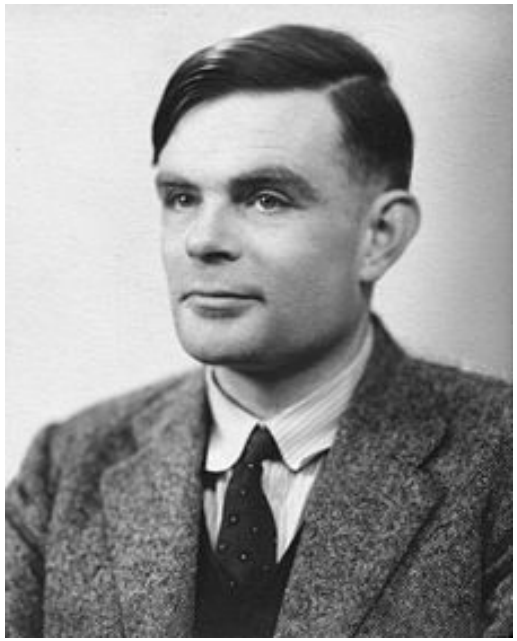
8 Retour sur Kuhn

Le problème de la décidabilité algorithmique de l'arithmétique de Peano

En 1935, Turing suit un cours de logique qui se conclut par la preuve du théorème de Gödel.

Il décide de s'attaquer au problème de la décidabilité algorithmique de l'arithmétique de Peano (Entscheidungsproblem).

Si l'arithmétique de Peano avait été complète, elle aurait été algorithmiquement décidable. Parce qu'elle ne l'est pas (si on la suppose consistante), l'Entscheidungsproblem se pose.



Réponse négative au problème de la décidabilité algorithmique de l'arithmétique de Peano

- On a vu que le problème de l'arrêt des machines de Turing est algorithmiquement indécidable : il n'existe pas de machine de Turing, qui prenne en entrée un couple quelconque (i, x) d'entiers, qui retourne *vrai* si la machine de Turing numéro i s'arrête lorsqu'on l'applique à x et *faux* sinon (théorème de Turing, 1936).
- Or l'énoncé « la machine de Turing numéro i ne s'arrête pas lorsqu'on l'applique à l'entrée x » peut être codé par une formule de l'arithmétique de Peano.
- Donc l'arithmétique de Peano n'est pas « décidable par machine de Turing » (sinon, le problème de l'arrêt serait algorithmiquement décidable).

Et en quoi ça nous concerne ?

En quoi ça prouve qu'il n'existe pas d' algorithme au sens intuitif, qui décide si une formule de l'arithmétique de Peano est démontrable ou pas ?

Et en quoi ça nous concerne ?

En quoi ça prouve qu'il n'existe pas d' algorithme au sens intuitif, qui décide si une formule de l'arithmétique de Peano est démontrable ou pas ?

Tout procédé réalisable par machine de Turing est un algorithme au sens intuitif. Mais est-ce que la réciproque est vraie ? La définition des machines de Turing est surchargée de détails.

Et en quoi ça nous concerne ?

En quoi ça prouve qu'il n'existe pas d' algorithme au sens intuitif, qui décide si une formule de l'arithmétique de Peano est démontrable ou pas ?

Tout procédé réalisable par machine de Turing est un algorithme au sens intuitif. Mais est-ce que la réciproque est vraie ? La définition des machines de Turing est surchargée de détails.

Des études ont montré que les « objets » calculés par les machines de Turing sont insensibles aux variations de détails.

Et en quoi ça nous concerne ?

En quoi ça prouve qu'il n'existe pas d' algorithme au sens intuitif, qui décide si une formule de l'arithmétique de Peano est démontrable ou pas ?

Tout procédé réalisable par machine de Turing est un algorithme au sens intuitif. Mais est-ce que la réciproque est vraie ? La définition des machines de Turing est surchargée de détails.

Des études ont montré que les « objets » calculés par les machines de Turing sont insensibles aux variations de détails.

Thèse de Church. Les deux notions (algorithmes au sens intuitif et algorithmes réalisables par machines de Turing) coïncident.

La thèse de Church (si on l'admet) et le thm de Turing montrent que l'Entscheidungsproblem n'a pas de solution.

1 Introduction

2 Intermède 1

3 Intermède 2

4 Intermède 3

5 Crise en mathématiques

6 Le deuxième problème de Hilbert

7 L'Entscheidungsproblem

8 Retour sur Kuhn

Les mathématiques sont-elles une science ?

L'idée que les axiomes de la géométrie euclidienne sont vrais a pu faire partie d'un paradigme. Et l'idée que toutes les théories mathématiques devraient être axiomatisées a pu faire partie du paradigme qui lui aurait succédé.

Les mathématiques sont-elles une science ?

L'idée que les axiomes de la géométrie euclidienne sont vrais a pu faire partie d'un paradigme. Et l'idée que toutes les théories mathématiques devraient être axiomatisées a pu faire partie du paradigme qui lui aurait succédé.

Lors des changements de paradigmes, il arrive fréquemment que des problèmes considérés comme scientifiques deviennent vides de sens.

Bourbaki écrit :

« Gauss et Lobatchevsky croient que le débat entre les différentes géométries peut être tranché par l'expérience [...] mais c'est là un problème qui n'a plus rien à voir avec la mathématique. »

Réflexions

- Pensée dominante : toutes les branches des mathématiques devraient être complètement axiomatisées.
- Les énoncés « à la Gödel » sont des anomalies.
- Beaucoup de mathématiciens pensent que les énoncés « à la Gödel » sont des énoncés qui ne concernent pas les vraies mathématiques. Mais ces énoncés « se rapprochent ». Articles de Jean-Paul Delahaye dans *Pour la Science* (novembre 1999, mai 2007 et septembre 2021).

La pensée dominante est peut-être un élément d'un paradigme. Et les théorèmes de Gödel marquent peut-être le début d'une crise.