



**UNE HISTOIRE DE  
LA LOGIQUE AU **XXE** SIÈCLE:  
DE LA PHILOSOPHIE À L'INFORMATIQUE**

**Christian Retoré**

**Professeur, Université de Montpellier & LIRMM-CNRS**

# LA LOGIQUE EST ELLE SULFUREUSE?

- **"Forse tu non pensavi ch'io loico fossi. [Lucifero]"** Dante Alighieri (1265-1321)  
Comedia, Inferno XXVII  
Une traduction pourrait être: "*sans doute ne savais tu pas que j'étais aussi bon logicien*".
- *En tout cas, en France la logique est peu enseignée:*
  - *Philosophie?*
  - *Mathématiques?*
  - *Informatique?*
  - *Linguistique (sémantique et philosophie du langage)?*



# AVANT LA LOGIQUE MODERNE

3  
Aristote  
Antiquité  
Scolastique

# LA LOGIQUE

- Art de raisonner correctement
- Avec la rigueur des raisonnements mathématiques
- Dériver correctement des énoncés  
...mais à partir de quels axiomes?
- Etude de la vérité dans une situation particulière, mais cela est plus récent.

# AUPARAVANT: ARISTOTE (III AV JC) L'ANTIQUITÉ & LA SCOLASTIQUE (MOYEN ÂGE)

- Certains types d'énoncés:
  - A Tout A est B
  - E Certains A sont B
  - I Aucun A est B
  - O Tous les A ne sont pas B.  
(ou Certains A ne sont pas B, mais le thème est différent)
- Les fameux syllogismes (règles de déduction)
  - Barbara : *tout M est P, or tout S est M, donc tout S est P;*
  - Baroco : *tout P est M, or quelque S n'est pas M, donc quelque S n'est pas P*

# PRINCIPES ARISTOTE & LES STOÏQUES

## ○ Aristotele

- Identité: Tout A est A
- Non contradiction NON (A et NON A)
- *"Tout personne niant le principe de non contradiction devrait être battue et brûlée jusqu'à ce qu'elle admette qu'être battu n'est pas la même chose que ne pas être battu, et qu'être brûlé n'est pas la même chose que ne pas être brûlé"* Avicenne (980-1037)
- Tiers exclus: A ou NON A (**tertium non datur**)

## ○ Stoïciens (calcul propositionnel)

- Modus ponens Si A alors B Or A donc B.
- Modus tollens Si A alors B. Or NON B. Donc A.
- **Ex falso quodlibet sequitur**

# PLACE DE LA LOGIQUE EN PHILOSOPHIE

- A étudier en premier pour raisonner correctement (Organon Catégories,..)
- « *Celui qui souhaite atteindre la perfection humaine doit d'abord étudier la logique, puis les diverses branches des mathématiques dans l'ordre qui convient, puis la physique et enfin la métaphysique.* » (Maimonides, XIIe)

# XIXE: LOGIQUE ALGÈBRIQUE ANGLAISE

## BOOLE, DE MORGAN, PIERCE

- Lois et calculs
- Calcul propositionnel: tables de vérités
  - $X \rightarrow \text{VRAI}: \text{VRAI}$
  - $\text{FAUX} \rightarrow X: \text{VRAI}$
  - $\text{VRAI} \rightarrow \text{FAUX}: \text{FAUX}$   
(si Paris est en France alors Rome est en Chine)
- Pour les prédicats des règles parfois fausses  
 $\forall x [I(x) \rightarrow (F(x) \vee M(x))]$   
 $\Leftrightarrow$   
 $\forall x (I(x) \rightarrow F(x)) \text{ ou } \forall x (I(x) \rightarrow M(x))$   
pensez à  $F = \text{femme}$   $M = \text{homme}$  ...





## XXE SIÈCLE

La crise des fondements des mathématiques

La logique du premier ordre

9

## GOTTLOB FREGE (1878-1925)

- Calcul des prédicats (formules quantifiées)
  - Tout  $x$  est  $P$ :  $(x) P(x)$  ou  $\forall x P(x)$
  - Certains  $x$  sont  $P$ :  $Ex P(x)$  ou  $\exists x P(x)$
- Tout  $A$  est  $B$ :  
 Pour tout  $X$ , SI  $X$  est  $A$  ALORS  $X$  est  $B$   
 $\forall X (A(X) \rightarrow B(X))$
- Certains  $A$  sont  $B$ :  
 Il existe  $X$ , tel  $X$  est  $A$  ET  $X$  est  $B$ .  
 $\exists X (A(X) \text{ ET } B(X))$
- Système déductif avec des règles comme:
  - SI on a établi  $P(x)$  ou  $x$  est une variable dont on ne suppose aucune propriété ALORS on a  $\forall x P(x)$

# FONDEMENTS DES MATHÉMATIQUES

## GEORG CANTOR (1845-1918)

- Infinis, plusieurs sortes de nombres:
  - Ordinaux
  - Cardinaux
- Il ya plusieurs sortes d'infinis
- Il y a plus de nombres réels que d'entiers: Si nous avons une liste des nombres réels entre 0 et 1 (développements décimaux infinis, sans 999999...)
  1. 0,5786086346780965431346789098764666...
  2. 0,8861453781936528901766189918714428...
  3. 0,8623503894729474548494646849947452...
  4. 0,5618903412252820282534176444510186...
- On fabrique un nombre qui est différent du premier sur la première décimale, du second sur la deuxième, du troisième sur la troisième:
  - 0,6939....
- 1. Il n'est pas dans la liste!!!

# GIUSEPPE PEANO (1858-1932)

## AXIOMATISATION DE L'ARITHMÉTIQUE

- Esperanto mathématique ...
- Symboles: 0 (zéro) +, x ...  
fonction S: successeur (l'entier suivant)
- $\forall n \quad S(0) \neq n$
- $\forall n \quad$  si  $n \neq 0$  alors il existe p tel que  $S(p) = n$
- $\forall n p \quad$  si  $S(n) = S(p)$  alors  $n = p$
- $\forall n \quad n + 0 = n$
- $\forall n p \quad n + S(p) = S(n + p)$
- $\forall n \quad n \times 0 = 0$
- $\forall n p \quad n \times S(p) = (n \times p) + n$
- Récurrence: pour établir qu'une propriété P(...) est vraie de tout entier il suffit de:
  1. Monter qu'elle est vraie de 0
  2. Montrer qu'elle passe au successeur:  
si P(n) alors P(S(n))

# DAVID HILBERT (1862-1943)

## ET LE PROGRAMME ÉPONYME

- En 1900 à Paris 23 problèmes majeurs
- Programme de fondements des mathématiques
- Méthode axiomatique
- Montrer en raisonnant sur les preuves (de manière finitaire) que les axiomes ne conduisent jamais à une proposition fausse (par ex.  $0=1$ ) par les règles de déduction formelle

# BERTRAND RUSSELL (1872-1970)

- Paradoxe de Russell:
  - $U = \{X / X \notin X\}$
  - $U \in U ?$
  - $U \notin U ?$
  - Schéma de compréhension restreint.
- Principia mathematica (1910-1913)  
formalisation/ axiomatisation purement logique  
des mathématiques

# THÉORIE AXIOMATIQUE DES ENSEMBLES

## ZERMELO (1871-1953) PUIS FRAENKEL (1891-1965)

- 1 seul symbole:  $X \in Y$  ( $X$  appartient à  $Y$ ) (et  $=$ )
- Deux ensembles sont égaux s'ils ont les mêmes éléments
- Il existe un ensemble sans élément (le vide)  
Formellement:  $\exists y \forall x x \notin y$
- Paire, union, ensemble des parties
- Schéma de compréhension restreint:
  - $\{X \in Y \mid P(X)\}$  est un ensemble (exit le paradoxe de Russell)
- Axiome de l'infini: il existe  $N$  qui contient  $\emptyset$  et  
si  $x \in N$  alors  $(x \cup \{x\}) \in N$

au minimum  $N$  contient:

$\emptyset$ ,	$\{\emptyset\}$ ,	$\{\emptyset, \{\emptyset\}\}$	$\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}$ ,
0,	1,	2,	3

- On peut faire TOUTES les mathématiques dans ZF

# MODÈLE, VÉRITÉ: CALCUL PROPOSITIONNEL

- Une interprétation:
  - On fixe la valeur, vrai ou faux de chaque proposition élémentaire
  - On en déduit la valeur dans cette interprétation des propositions complexes par les tables de vérités
- Validité:
  - Une proposition dérivable (par exemple  $p \rightarrow p$ ) vaut vrai dans toute interprétation
- Complétude:
  - Si une proposition vaut vrai dans toute interprétation, alors elle est dérivable (Bernays, 1926)



# MODÈLE, VÉRITÉ: CALCUL DES PRÉDICATS

1/2

- La même chose, en plus compliqué:
  - Ensemble (domaine) par exemple les gens
  - Interprétation des constantes, des relations, ...
    - Dort: ensemble de personnes
    - Connaît: ensemble de couples
  - On peut vérifier dans un modèle donné que, par exemple:
    - Pour tout x il existe y, x connaît y et y dort;
- Il y a des formules vraies dans TOUT modèle:
  - SI il existe X tel que pour tout Y  
X soit en relation R avec Y  
ALORS pour tout Y il existe un X  
tel que X soit dans la relation R avec Y
  - C'est-à-dire  $\exists x \forall y P(x,y) \Rightarrow \forall y \exists x P(x,y)$
-

# MODÈLE, VÉRITÉ: CALCUL DES PRÉDICATS

$\frac{1}{2}$

- Validité
- Toute formule dérivable est vraie dans tout modèle,.
- **Complétude (Gödel, 1929) : Toute formule vraie dans tout modèle est dérivable**

# LUITZEN EGBERTUS JAN BROUWER (1881-1966) ET L'INTUITIONNISME

- Rejet du tiers exclus:
  - A ou non A
  - Différent de non (A et non A)
  - « ou » intuitionniste: plus exigeant
- Même chose pour le « il existe »
  - Existe  $x$   $P(x) = P(0)$  ou  $P(1)$  ou  $P(2)$  ...
  - Ne se déduit pas de NON pour tout X non  $P(x)$
- Raisonnement qui construit la solution
- Ex. théorème des valeurs intermédiaires
- Paradoxe du buveur:
  - Il existe X tel que si X boit alors tout le monde boit.

# KURT GÖDEL (1906-1978)

- Complétude de la logique du premier ordre
- Compatibilité de l'axiome du choix
- Compatibilité de l'hypothèse du continu
- Incomplétude de l'arithmétique
  - Il existe des formules de l'arithmétique qui ne sont ni démontrable ni réfutables
  - En particulier la cohérence de la théorie qui peut s'exprimer dans la théorie n'est pas démontrable.

## EN RÉSUMÉ: FONDAMENTAUX

- Preuves
- Modèles
- Théorie des ensembles, ordinaux, cardinaux
- *Lowenheim Skolem:*  
*une théorie qui admet un modèle infini en admet de toute cardinalité infinie*
- Complétude de la logique du premier ordre
- *Compacité:*  
*étant donné une famille de formules dont chaque partie finie admet un modèle, toute la famille admet un modèle*
- Incomplétude de l'arithmétique de Peano.



# INFORMATIQUE

Et calculabilité

22

# POURQUOI LA SCIENCE INFORMATIQUE EST ELLE AUSSI LIÉE À LA LOGIQUE

- Informatique? Science? technologie ?
  - Données (informatique)
  - Calcul (computer science)
- Mécanisation du raisonnement (et du calcul) dans le programme de Hilbert
- Formalisation, codage,...(cf. Gödel)
- Dès les débuts analyse du langage naturel, test de Turing pour l'intelligence artificielle: berner 30% des humains dans un dialogue.

# MACHINE ABSTRAITE 1936

## ALAN TURING (1912-1954)

- Ruban avec des 0 et des 1 (qui peuvent « tout » représenter via divers codages)
- Tête qui parcourt le ruban
- Etats: 1 initial plusieurs finaux
- Actions
  - lire, écrire (0, 1, rien),
  - déplacer (gauche, droite, rien),
  - Changement d'état
- Instructions:  
si dans tel état si on lit tel caractère  
alors on fait telle écriture,  
on déplace la tête et on va dans tel état.



# MACHINES DE TURING: TERMINE? OU PAS?

- La machine s'arrête quand on atteint un des états finaux
- Le problème de l'arrêt des machines de Turing est indécidable. Il n'y a pas de machine de Turing qui étant donné (sur un ruban):
  - Un entier  $m$  qui code une machine de Turing  $M$  (un texte finit décrit la machine, et il se représente par un nombre entier)
  - Et un entier  $n$
  - Répond 1 si la machine  $M$  s'arrête sur l'entrée  $n$  et 0 sinon.

# MACHINE DE JOHN VON NEUMAN (1903-1957)

- 1 processeur
- 1 mémoire : données + programme
- Contrôleur qui dicte la séquence des opérations

# CALCULABILITÉ À LA CHURCH (1903-1995)

## LAMBDA CALCUL

- Du point de vue des ensembles, un nombre est la classe des ensemble ayant le même nombre d'éléments.
- On définit le nombre  $n$  comme:  
appliquer  $n$  fois une fonction  $F$  a quelque chose:  
 $S(S(S(0))) : 3$   
 $\text{mère}(\text{mère}(\text{mère}(\text{Jean}))) : 3$   
l'écriture de faire 3 fois une action sur un objet

# CALCULABILITÉ À LA CHURCH

## LAMBDA CALCUL

- En lambda calcul est fonction/action
- 3:  $(\lambda f \lambda x (f(f(f(x)))))$
- S:  $\lambda n \lambda f \lambda x f(n f x)$
- +:  $\lambda n \lambda p n f (p f x)$
- Calculer c'est remplacer la variable par sa valeur...  $(\lambda x. (x+3)) 5 \rightarrow 5+3$  [substitution]
- Quelles fonctions sur les entiers peut on définir?
- Les mêmes que celle de Turing!
- Lambda calcul inventé pour formalisé la logique, pour substituer des formules dans d'autres: axiome appliqué à instance particulière :  $(\lambda p p \Rightarrow p)(A \& B)$  donner  $(A \& B) \Rightarrow (A \& B)$

# THÈSE DE CHURCH TURING (1912-1954)

- La machine de Turing ou le lambda calcul de Church (équivalents) rendent exactement compte de tout ce qui se calcule automatiquement.
- Le lien avec la logique est assez clair: comme on peut coder par des entiers:
  - Les formules
  - Les preuves
  - On peut concevoir une machine qui vérifie par exemple si une formule est prouvable.



# GROS PLAN: DE LA LOGIQUE INTUITIONNISTE AUX PROGRAMMES CERTIFIÉS

Preuves, types et programmes

30

# LA DÉDUCTION NATURELLE

GERHARD GENTZEN (1909-1945),  
DAG PRAWITZ (1936-...)

- Dédutions sous hypothèses
- Des règles simples:
- Bizarrement, la logique sous jacente est intuitionniste et non classique:
- $((a \rightarrow b) \rightarrow a) \rightarrow a$  n'est pas démontrable
- Mais démontrable classiquement:
  - Si a vrai OK
  - Si a faux  $(a \rightarrow b)$  vrai donc  $((a \rightarrow b) \rightarrow a)$  est faux OK

## 23 SIÈCLES APRÈS ARISTOTE DES RÈGLES DE DÉDUCTION SIMPLES

- Axiome  $A \vdash A$
- Modus ponens:  
Si  $\Gamma \vdash A$  et  $\Delta \vdash A \rightarrow B$   
alors  $\Gamma \Delta \vdash B$
- Abstraction:  
Si  $\Delta, A \vdash B$   
Alors  $\Delta \vdash A \rightarrow B$
- Système suffisant pour dériver les propositions intuitionnistes valide (écrites avec  $\rightarrow$ )
- Suffisant pour représenter les entiers!



# LA CORRESPONDANCE DE CURRY HOWARD (1900-1982 & 1926-...)

- Types de données = formule logique  
ex entier:  $(A \rightarrow (A \rightarrow A)) \rightarrow A$
- Donnée de type A = preuve de A
- Type A  $\rightarrow$  B  
fonction de A dans B c'est-à-dire  
fonction des preuves de A dans les preuves de B :  
évidemment: le modus ponens fait le boulot!  
preuve de A, preuve de A  $\rightarrow$  B  
donc preuve de A  $\rightarrow$  B

## L'ENTIER 3 VU SOUS UN ANGLE DIFFÉRENT

- Une preuve de :  $(A \rightarrow (A \rightarrow A)) \rightarrow A$ ?
- Il établir  $A$  sous les hypothèses  $(A \rightarrow A)$  et  $A$   
on part de  $A \mid -A$  (0)  
et de  $A \rightarrow A \mid -A \rightarrow A$  (S) (axiomes)  
par modus ponens on obtient  $A, A \rightarrow A \mid -A$  (1)  
par (1) en utilisant de nouveau (S), on obtient par  
modus ponens  $A, A \rightarrow A, A \rightarrow A \mid -A$  (2)  
par (2) en utilisant de nouveau (S), on obtient par  
modus ponens  $A, A \rightarrow A, A \rightarrow A, A \rightarrow A \mid -A$  (3)
- Par abstraction:  $A \mid - (A \rightarrow A) \rightarrow A$
- Par abstraction encore:  $\mid - A \rightarrow (A \rightarrow A) \rightarrow A$

## L'ENTIER 3 VU SOUS UN ANGLE DIFFÉRENT

- Notre preuve de :  $(A \rightarrow (A \rightarrow A)) \rightarrow A$   
consiste en 3 applications de  $A \rightarrow A$  à  $A...$   
c'est donc l'entier 3 du lambda calcul de Church
- On peut l'écrire  $(\lambda f:A \rightarrow A \lambda x:A (f(f(f(x)))))$

# CORRESPONDANCE LOGIQUE / CALCUL

## Logique

- Formule A
- Preuve de A
- Normalisation de la preuve (substitution d'une variable par sa valeur)

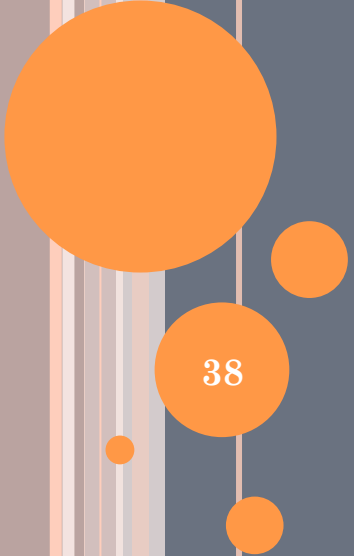

## informatique

- Type A
- Programme de type A
- Evaluation du programme preuve (substitution d'une variable par sa valeur)

# PROGRAMME CERTIFIÉS:

## LES PREUVES VUES COMME DES PROGRAMMES

- Santé, aéronautique, finances, protocoles de connexion...  
**il faut des programme sûrs**
  - Vérification
  - **Extraction de programmes depuis les preuves**
- Procédure:
  1. On écrit la spécification du programme: (équations):
  2. On démontre formellement que pour tout  $x$  il existe un  $y$  tel que  $P(x,y)$  en utilisant les règles de la logique et les équations
  3. On ne garde que la partie propositionnelle
  4. On consrduit le lambda terme
- **Alors il est sûr que le programme obtenu fait exactement ce qu'il est supposé faire.**
- **Programmes peu efficaces mais parfaitement sûrs.**



"CONTRARIWISE, IF IT WAS SO, IT  
MIGHT BE; AND IF IT WERE SO, IT  
WOULD BE; BUT AS IT ISN'T, IT AIN'T.  
THAT'S LOGIC." LEWIS CARROLL  
(1832-1898)

38

Merci de votre attention.

Des questions?

## QUELQUES RÉFÉRENCES GRAND PUBLIC

- **BD LOGICOMIX** de Apostolos Doxiadis, Christos H. Papadimitriou, Alecos Papadatos, and Annie di Donna Vuibert 2010 *Les principaux logiciens du début du XXe sont mis en scène. Pas technique, mais des annexes permettent d'aller plus loin.*
- **Roman** La déesse des petites victoires de Yannick Granne Editions Anne Carrière. 2012 Prix des libraires 2013. *Gödel vu par sa femme. Très bonne reconstitution de la vie scientifique à Vienne puis à Princeton, avec des personnages comme Einstein (l'unique ami de Gödel), von Neuman, Morgenstern,...Très bon roman per se.*
- **BD** Les rêveurs lunaires, quatre génies qui ont changé l'histoire de Cédric Villani et Edmond Baudoin ( Gallimard/ Grasset) 2015 *Science et éthique pendant la 2<sup>nd</sup>e guerre mondiale, avec Turing, les physiciens Heisenberg et Szilard, un général anglais, Hugh Dowding.*
- **Film** de Morten Tyldum avec Benedict Cumberbatch *Imitation games* 2014. *Film populaire sur Turing, aux nombreux prix. (pas encore vu)*

## DEUX OUVRAGES DE VULGARISATION

- **Essai** Les démonstrations et les algorithmes: introduction à la logique et à la calculabilité de Gilles Dowek 2010  
*Très bon ouvrage de vulgarisation.*
- **Essai** Pierre Cassou-Noguès Les démons de Gödel : Logique et folie Seuil 2015 *Toujours sur Gödel, plus scientifique que le roman de Yannick Grannec.*