La logique en Informatique

Christian Retoré

LIRMM Univ Montpellier

La logique est elle sulfureuse?

Lucifero: "Forse tu non pensavi ch'io LOICO fossi. Dante Alighieri (1265-1321) Comedia, Inferno XXVII

Une traduction pourrait être: Lucifer: « *Sans doute ne savais tu pas que j'étais aussi bon logicien.* »

Il y eut des tensions entre les logiciens et les autorités religieuses.

Avant la logique « moderne »

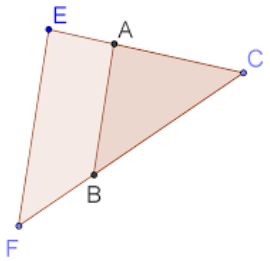
Aristote

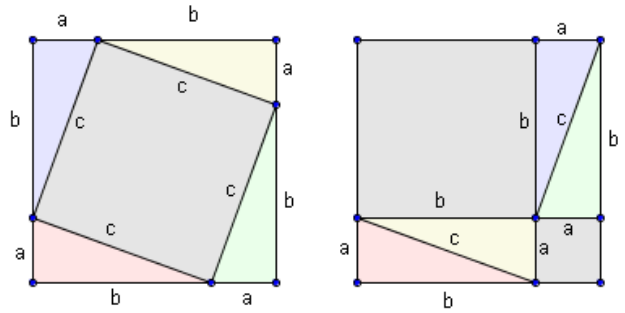
L'antiquité après Aristote

Le Moyen-Âge et la scolastique

La logique algébrique (XVIIe XVIIIe XIXe)

La logique

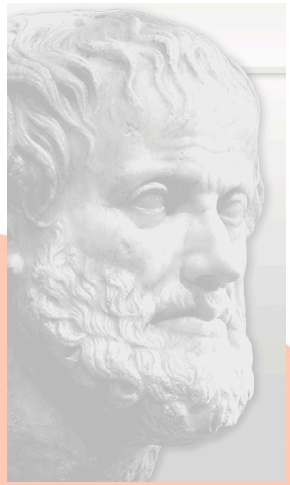




- Art de raisonner correctement
- Avec la rigueur des raisonnements mathématiques (Thalès, Pythagore,… VIIe siècle av. J.C)
- Dériver correctement des énoncés

  …mais à partir de quels axiomes?
- Etude de la vérité
  dans une situation particulière,
  mais cela est plus récent.

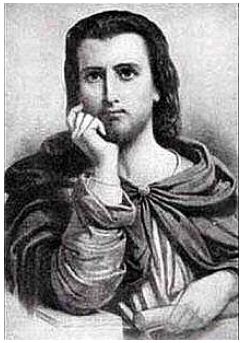
Aristote (III av JC) l'antiquité & la scolastique (moyen âge)



- 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)

La scolastique (Antiquité et Moyen-Âge)

- 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*



Pierre Abélard (1079-1142)

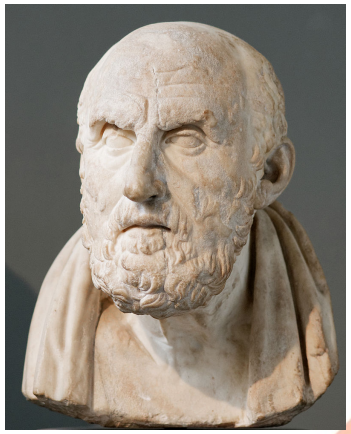
Principes (Aristote, Avicenne)

Avicenne ibn Sina (980-1037)

- Identité: Tout A est A
- Non contradiction NON (G et NON G) *"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 brulé n'est pas la même chose que ne pas être brûlé"* Avicenne (980-1037) en réponse à des religieux souhaitant accommoder ce principe.
- Tiers exclus: pour tout énoncé G on a (G ou NON G) **(tertium non datur)**

Principes (Stoïciens)

- Stoïciens (calcul propositionnel)
- Modus ponens:
  - Si A alors B
  - Or A
  - Donc B.
- Modus tollens:
  - Si A alors B.
  - Or NON B.
  - Donc NON A.
- **Ex falso quodlibet sequitur**



Chrysippe de Soles
logicien stoïcien
(280—206 av. JC, Anatolie).

Place de la logique en philosophie

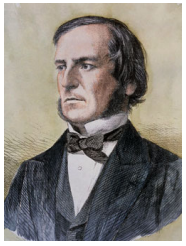
- A étudier en premier pour raisonner correctement (Organon, Catégories,..)
- *« Celui qui souhaite atteindre la perfection humaine doit d'abord étudier la logique, puis les diverses branches des mathématiques dans l'ordre qui convient, puis la physique et enfin la métaphysique. »* (Maimonides, XIIe)

Logique algébrique
Leibnitz et ses successeurs Boole, De Morgan, Pierce

- Précurseur: Leibniz (1646-1716)
- Lois et calculs
- Calcul propositionnel: tables de vérité
  - X → VRAI : VRAI
    (Si Rome est en Chine alors Paris est en France)
  - FAUX → X : VRAI
    (Si Rome est en Chine alors Paris est en Chine)
  - VRAI → FAUX : FAUX
    (si Paris est en France alors Rome est en Chine)

Logique algébrique anglo-américaine Boole, De Morgan, Pierce (XIXe)

- Pour les prédicats des règles parfois fausses
  $\forall x[I(x) -> (F(x) \vee M(x))]$
  $\Leftrightarrow$
  $\forall x(I(x) -> F(x))$ ou $\forall x(I(x) -> M(x))$
  pensez à I=Individu F= femme M=homme …



Le XXe siècle

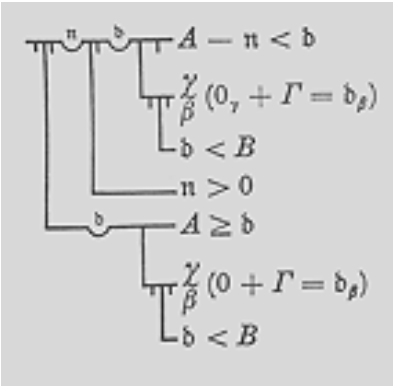
La crise des fondements des mathématiques

Les débuts de la logique mathématique

La logique du premier ordre

Calcul des prédicats (formules quantifiées) Gottlob Frege (1848-1925)

- Formules avec des variables,
- Sur lesquelles on peut quantifier
- Incluent strictement les énoncés A E I O d'Aristote
- *Tout entier est la somme de quatre carrés:*
  pour tout n il existe a b c et d tels que $n=a^2+b^2+c^2+d^2$
- Idéographie: notation pour les formules et les preuves



Formalisation des quantificateurs (Frege)

- Tout x est P: noté (x) P(x) puis ∀x P(x)
  « tout », « tous les », « chaque »
  (et même « un »: « *un homme averti en vaut deux* »)
- Au moins un x est P: noté Ex P(x) puis ∃x P(x)
  « certains » « quelques » « des » « un »
- Problème de formulation: pluriel / singulier
  A-t-elle des enfants? Oui, deux. Oui, un. # Non, un.
  A-t-elle un diplôme de maths? Oui, un. Oui, Deux. # Non, deux.

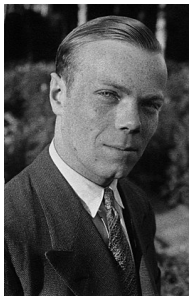
Frege, Hilbert: les quantificateurs des mathématiques usuelles

- Une seule sorte d'individus:
- 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.
  $\exists\ X\ (A(X)$ ET $B(X))$

$\exists x\ \forall y\ P(x,y) \neq \forall y\ \exists x\ P(x,y)$

Règles de déduction Gottlob Frege (1848-1925) David Hilbert (1862-1943), Jacques Herbrand (1908-1931)

- SI on a établi P(x) (sans rien supposer sur x)
  ALORS on a ∀x P(x) sous les mêmes hypothèses
  (règle de généralisation ou d'abstraction formalisation de Aristote)
- SI on a établit ∀x P(x)
  ALORS on a P(t) pour tout terme particulier



Frege, Hilbert, Herbrand,…
Règles de la quantification existentielle

Herbrand à 23 ans, peu avant son fatal accident d'alpinisme.

- SI on a établi P(t) pour un terme particulier,
  ALORS on a établi ∃ x P(x)
- SI P(x) (avec x quelconque) suffit pour obtenir A
  ALORS ∃ x P(x) suffit pour obtenir A.

Vérité dans un modèle
Préambule: le calcul propositionnel (1/2)

- Suite des travaux de Boole (XIXe)
- 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

Vérité dans un modèle
Préambule: le calcul propositionnel (2/2)

- Validité:
  - Une proposition dérivable
    (par exemple p→ p)
    vaut vrai dans toute interprétation
- Plus tard: Complétude (1926):
  - Si une proposition vaut vrai dans toute interprétation, alors elle est dérivable
    (Bernays, 1988-1977)

Calcul des prédicats: vérité dans un modèle 1/3
Leopold Löwenheim (1878-1957)

- La même chose, en plus compliqué:
  - Ensemble (domaine) par exemple les gens, les nombres,…
  - Interprétation des constantes, des relations, …
    - Dort: ensemble de personnes
    - Connaît: ensemble de couples de personnes
  - On peut vérifier dans un modèle donné que, par exemple:
    - Pour tout x il existe y, x connaît y et y dort;

calcul des prédicats vérité dans un modèle 2/3

- 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 $\exists x \, \forall y \, R(x,y) \Rightarrow \forall y \, \exists x \, R(x,y)$

Calcul des prédicats vérité dans un modèle 3/3

- Validité: Toute formule démontrable formellement est vraie dans tout modèle,.
- **Complétude (Gödel, 1929) : Toute formule vraie dans tout modèle est formellement démontrable:** nous montrerons à la fin de ce cours ce résultat qui relie preuves et modèles.

Cet énoncé dont la signification était peu claire à l'époque découle aussi des travaux de 1923 de Thoralf Skolem (1887-1963), ci-contre, comme Gödel l'avait remarqué.

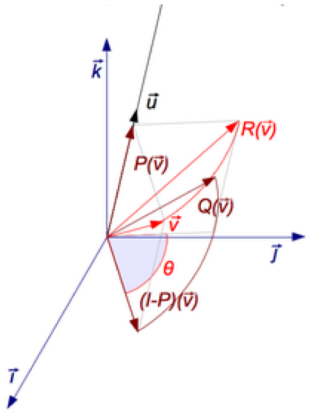
Exemple de modèle

- Un groupe est un ensemble doté d'une opération binaire * satisfaisant:
  - $\forall x \, \forall y \, \forall z. \quad (x * y)*z = x*(y*z)$ [* associative]
  - $\exists e. \quad x*e=x$ et $e*x=x$ [il y a un élément neutre]
  - $\forall x \, \exists y \; x*y=e$ et $y*x=e$ [tout élément a un inverse]
- Exemple de groupes:
  - les rotations du plan,
  - les permutations d'un ensemble,
  - les entiers relatifs avec l'addition,
  - les transformations du Rubik's cube …
- Les axiomes de groupes sont vrais dans tout groupe.

Sens du théorème de complétude

- Une propriété est **vraie dans tous les groupes** si et seulement si cette propriété est **démontrable à partir des axiomes de groupe.**
- Le **théorème de complétude résultat central** de ce cours relie modèles et preuves.

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2



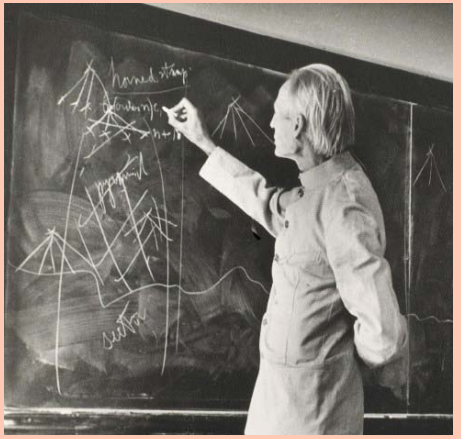
Giuseppe Peano (1858-1932)
Axiomatisation de l'arithmétique

- Esperanto mathématique …
- Arithmétique: symboles: 0,1, +, *, <..
- Axiome évidents sur ces symboles
- Schéma de récurrence.

L.E.J. Brouwer et l'intuitionnisme

Outre ses travaux sur le constructivisme Brouwer a produit un célèbre résultat de topologie en raisonnant par l'absurde, sans aucun argument constructif !!!

- Refus du tiers exclus Av¬A
- Preuve d'existence: nécessite un témoin
- Raisonnement constructif qui calcule ou approche la solution
- Ex. th. des valeurs intermédiaires dichotomies successives (Newton) / absurde)



Kurt Gödel (1906-1978)

- Compatibilité de l'axiome du choix et de l'hypothèse du continu (univers tournants en relativité générale)
- Complétude de la logique du premier ordre et compacité (dans ce cours)
- Incomplétude de l'arithmétique (dans ce cours)
  - Certaines formules de l'arithmétique ne sont ni démontrables ni réfutables
  - En particulier la cohérence de la l'arithmétique (et qui peut s'exprimer dans l'arithmétique) n'est pas démontrable dans l'arithmétique.

Kurt Gödel avec Albert Einstein, son unique ami à Princeton

Un drôle de personnage, mort de faim par crainte d'être empoisonné. Mais aussi un génie auteur de plusieurs théorème clés de la logique athématique, et il inventa la première notion de calculabilité et par là même il est à l'origine de l'informatique.

De la logique à l'informatique (merci à Hilbert et à Gödel!)

Les ordinateurs sont issus de la notion de calculabilité et non l'inverse.

Conservativité (Hilbert)

- CONSERVATIVITÉ: Soient
  - une théorie simple R (dont on ne doute pas)
    par ex. l'arithmétique
  - une théorie I plus complexe que R
    par ex. l'analyse ou théorie des ensembles ou …
- On aimerait qu'il n'y ait pas plus de résultats sur R en passant par I que directement.
  - Par ex avec les réels on n'obtiendra pas 0=1
  - Autre ex: pour x,y,z entiers >0, n>2
    $x^n+y^n \neq z^n$ (grand th de Fermat, Wiles 1994)
    avec de l'analyse complexe, de l'algèbre commutative
    on peut le faire dans l'arithmétique????????

Paradoxe de Russell

$U = \{X / X \notin X\}$

$U \in U$?

$U \notin U$?

Cohérence (Hilbert)

- De là Hilbert est passé à une idée plus forte qui suffit pour avoir la conservativité: LA COHERENCE pas de contradiction dans I en supposant qu'il n'y en a pas dans R ce qui est « évident »
- R démontre que I ne dérive pas de contradiction
- Pas idiot car les formules de I sont finies, les axiomes de I sont finis, les démonstrations sont finies, représentables par des entiers, etc.
- En raisonnant sur les codes des formules et des preuves on devrait pouvoir montrer dans R que I ne démontre pas 0=1
- Cohérence de R => conservativité de R sur I

Patatras! Gödel met fin aux espoirs de Hilbert

- Premier théorème d'incomplétude (Gödel 1930):
  Soit T une théorie (cohérente) contenant l'arithmétique,
  alors il existe une formule F (qui affirme sa non prouvabilité)
  telle que T |-/- F et T |-/- ~F
- Second théorème d'incomplétude (Gödel 1930):
  Soit T une théorie (cohérente) contenant l'arithmétique,
  alors T ne démontre pas la cohérence de T

Cohérence et conservativité envolées

- Second théorème d'incomplétude
  détruit tout espoir de prouver la cohérence de I dans R: si R ne démontre pas la cohérence de R il démontre encore moins la cohérence de I qui est plus riche.
- Premier théorème d'incomplétude
  détruit l'espoir de conservativité
  F est un énoncé réel (sur des codes de preuves et de formules) on peut vérifier dans la construction de F qu'en fait F est vraie et qu'un système I plus riche peut montrer F mais R ne le peut pas

Hilbert → calculabilité ? C'est assez normal.

- Mécanisation du raisonnement
- Décidabilité (calculabilité)
- Idée:
  - Formules finies
  - Preuves finies
  - Codage par des entiers
  - En raisonnant / calculant sur les entiers on montre la cohérence via un codage:
  - $Pr_T(d,a)$: d est le code d'une démonstration de la formule codée par a.
  - Cohérence: $\neg(\exists d\ PR_T(d,\langle 0=1\rangle))$

De cet échec de Hilbert à la calculabilité

- Cadre de la preuve de Gödel:
  - deux théories S et T
  - S simple (arithmétique primitive récursive)
  - T plus compliquée (arithmétique de Peano,)
  - T→S codage
  - S→T S s'interprète dans T
- Fonctions Primitives Récursives
  - Successeur
  - Projections
  - Schéma de récurrence (grosso modo): f(0) donné et f(n) en fonction de f(n-1) par une fonction primitive récursive

Herbrand-Gödel, Church, Kleene

- Fonctions récursives plus générales?
- Par ex. pour inclure Ackermann récursive totale mais pas primitive récursive
- Schémas équationnels plus généraux que la récursion primitive, mais comment calculer avec, comment orienter les équations?
- Solution Kleene 1936, le schéma mu:

$$f : \mathbb{N}^{k+1} \mapsto \mathbb{N}$$
$$\mu(f) : \mathbb{N}^{k} \mapsto \mathbb{N}$$
$$\mu(f)(x_1, \ldots, x_k) : \text{le plus petit entier } n \text{ tel que } f(n, x_1, \ldots, x_k) = 0$$
$$\text{indéfini s'il n'en existe pas.}$$

Gödel fréquente les USA et notamment Princeton à partir de 1930, y expose ses travaux, ses théorèmes d'incomplétude, sur la récursion. Il s'installe aux USA définitivement en après l'Anschluss pour fuir le nazisme.

Cependant Church depuis 1930 étudie un autre modèle de la calculabilité:

Les lambda termes (purs/non typés) sont des expressions construites ainsi:

- Les variables sont des termes.
- Si t est un terme et x une variable alors $\lambda x.t$ est un terme (la fonction qui associe le terme t à x).
- Si t_1 et t_2 sont des termes alors $t_1(t_2)$ est un terme (t_2 est vu comme une fonction qui est appliquée à t_1.

Quelques lambda termes:

$I = \lambda x.x$
$K = \lambda x.\lambda z.x$
$S = \lambda x.\lambda y.\lambda z.(x, z)(y\, z)$
$0 = \lambda f.\lambda z.z$
$3 = \lambda f.\lambda z.(f(f(f(z))))$

Lambda termes / programmes fonctionnels évaluation= substitution (beta réduction)

$$(\lambda x.t)t' \overset{\beta}{\rightsquigarrow} t[x := t']$$

Exemples:

$(K0)4 = ((\lambda x.\lambda y.x)0)2 \overset{\beta}{\rightsquigarrow} (\lambda y0)2 \overset{\beta}{\rightsquigarrow} 0$

$(\lambda x.(x\,x))(\lambda x.(x\,x)) \overset{\beta}{\rightsquigarrow} (\lambda x.(x\,x))(\lambda x.(x\,x))$

$(\lambda x.((x\,x)x)(\lambda x.((x\,x)x)) \overset{\beta}{\rightsquigarrow} ((\lambda x.((x\,x)x))(\lambda x.((x\,x)x)))(\lambda x.((x\,x)x))$

$(K((K0)2))2 \overset{\beta}{\rightsquigarrow} (K0)2 \overset{\beta}{\rightsquigarrow} 0$

La première notion de « calculable »: le lambda calcul pur (non typé: « le lisp »)

On peut représenter en lambda calcul pur:

- **Les entiers:** $0 = \lambda f.\lambda x x \quad 1 = \lambda f.\lambda x (f\ x) \quad 2 = \lambda f.\lambda x (f (f\ x)) \quad 3 = \lambda f.\lambda x (f (f (f\ x))) \quad \cdots$
- **Les opérations:** le successeur, l'addition, la multiplication, l'exponentiation, la différence tronquée,…
- Les **couples** et n-uplets,
- Les **projections**
- La **composition** de fonction
- Les définitions par récurrence et donc **les fonctions primitives récursives**
- Le **schéma mu** (cf. supra) de la récursion générale,(le plus petit n tel que P(m,n)=0 s'il y en a et sinon le lambda terme ne se normalise pas)

On adonc toutes les fonctions récursives partielles avec comme mécanisme de calcul, la substitution (~programmation fonctionnelle)

Gödel → Church →Turing (+ Kleene)

- Turing ingénieur venu étudier auprès de Church 1937/38
- S'oriente vers un modèle de calcul plus proche des machines et circuits
- Kleene montre en 1936 que les 3 notions suivantes coïncident:
  - Lambda calculable
  - Calculable par une machine de Turing (perfectionné par von Neuman)

  En ramenant les deux notions à:
  - Défini par une fonction récursive de Gödel Herbrand
- Cette notion de calculable (ou pas) reste la même avec les ordinateurs quantiques — même si cela est intéressant « en moyenne » du point de vue de la complexité pour les problèmes NP complets, par ex.

Et l'informatique dans tout ça?

- Informatique? Science? Technologie ?
  - Données (→ informatique)
  - Calcul (→ computer science)
- Mécanisation du raisonnement (et du calcul) issue dans le programme de Hilbert
- Formalisation, codage,…représentation des données (cf. la preuve de Gödel)
- Repose sur le passage de DÉCIDABLE -> CALCULABLE dû à Hilbert.

La logique en informatique AUJOURD'HUI en particulier au LIRMM

Principalement:

calculabilité

spécification et vérification

Intelligence artificielle

Mais pas seulement.

Reprenons la classification standard ACM

- Hardware
  - Integrated circuits (en micro électronique)
- Software engineering
  - Formal languages / compilers
  - Software verification

Continuons la classification standard ACM

- Information systems
  - Theory of Data Bases
- Security and privacy
  - Certified programs
- Computing methodology
  - Artificial intelligence
  - Software verification / specification

Finissons la classification standard ACM par THEORY OF COMPUTATION

- Computability
- Formal languages and automata theory
- Computational complexity and cryptography
  - Proof complexity
  - Interactive proof systems
  - Complexity theory and logic
- Semantics and reasoning
- Logic (ci-après)

Détaillons LOGIC dans THEORY OF COMPUTATION

- Logic and verification
- Proof theory
- Modal and temporal logics
- Automated reasoning
- Constraint and logic programming
- Constructive mathematics
- Description logics
- Equational logic and rewriting
- Finite Model Theory
- Higher order logic
- Linear logic
- Programming logic
- Abstraction
- Verification by model checking
- Type theory
- Hoare logic
- Separation logic

Par thème et par équipe

- **AlGCo**
  Paul, Thilikos
- **Escape**
  Durand, Romashchenko
- **GraphiK**
  Carral + presque tout GraphiK
- **Marel**
  Delahaye
- **Smile**
  Gouaich, Kaci
- **Texte**
  Moot, Retoré
- Hors équipe: Legrand
- IMAG: Durand-Guerrier, Saby, Théret (Malgoire?)

- Logique en IA
  - Argumentation
  - Logiques de description
  - Jeux et construction de preuves
  - Sémantique du langage naturel
- Théorie de la démonstration
  - Théorie des types, logique linéaire, programmation fonctionnelle, sémantique dénotationnelle
  - Démonstration automatique (pour GL et IA)
  - Approches dialogiques de LJ, LK, S4,…
- Constructivité, calculabilité et complexité
  - Faisceaux, modèles topologiques, topos (LJ, S4)
  - Ensembles constructibles, ordinaux admissibles
  - Complexité paramétrée

Evénements / projets passés:

- AVANT 2021
  - Workshop Epsilon 2015
  - Action Quanti Projet UM 2017 -> workshop à ESSLLI 2017
  - World Logic Day (UNESCO) 14 janvier 2019 2020
- EN 2021
  - World Logic Day (UNESCO) 14 janvier
  - Réunion de travail Réseaux de démonstration 22 janvier 2021
    (Ehrhard IRIF; Nguyen LIPN; Strassburger, Acclavio INRIA SACLAY; Retoré LIRMM)
  - Journée « Preuves » 4 juin 2021 (Delahaye, Cailler, Catta, Retoré, Moot)

Evénements à venir en 2021:

- MERCREDI 17 NOVEMBRE
  JOURNEE LOGIQUE ET REPRESENTATIONS DES CONNAISSANCES
  (organisée par David CARRAL, GraphiK)
  - Sebastian Rudolph Dresden
  - Jacopo Urban Amsterdam
  - Mickael Tomasso Saclay

- MERCREDI 24 NOVEMBRE
  JOURNEE LOGIQUE ET INTERACTION
  - Michele Abrusci (Rome)
  - Andreas Herzig (Toulouse)
  - Myriam Quatrini (Marseille)

MARDI 23 NOVEMBRE
- HDR Moot Logique et analyse du langage naturel
- Thèse Catta Preuves formelles et sémantiques des jeux

Evénements à venir en 2022

- Nous attendons vos propositions !

Quelques références

J’admets être partial et impressionné par l’œuvre de Gödel

Quelques références légères

- **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 Grannec 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.

Pour aller plus loin

- **Essai:** Pierre Cassou-Noguès Les démons de Gödel : Logique et folie Seuil 2015
  Toujours sur Gödel, plus scientifique que le roman de Yannick Grannec.
- **Article original et commentaires:**
  K. Gödel, E. Nagel, J. Newman, J.-Y. Girard
  Le théorème de Gödel. Seuil 1997
- **Essai:** Gilles Dowek Les démonstrations et les algorithmes: introduction à la logique et à la calculabilité. 2010 Ecole polytechnique.
  Très bon ouvrage de vulgarisation.