Petit guide à l'usage du promeneur égaré dans l'univers de la Logique

Richard Lassaigne
IMJ/Logique mathématique
CNRS-Université Paris Diderot

Logique, vous avez dit logique?

Epimondes a dit:

« Tous les Crétois sont des menteurs »

Or Epimondes était Crétois

Le barbier du village a une règle d'or:

il rase les habitants du village

qui ne se rasent pas eux-mêmes

Le barbier se rase-t-il?

Livre de R. Smullyan:

Quel est le titre de ce livre?

« The art of correct reasoning with

false or inconsistent hypothesis »

Logique, Mathématique et Informatique

- Naissance

  G. Boole, G. Frege, B. Russell, D. Hilbert, …

  Crise des Fondements (Cantor, Russell)

- Panorama de la Logique mathématique

  Zermelo-Fraenkel, K. Gödel, A. Turing, G. Gentzen,...

  Cohérence, Incomplétude, Indécidabilité, Preuves

- Problèmes et résultats

  K. Gödel, P. Cohen, A. Tarski, L. Henkin,...,Y. Matiyasevich,...

  Indépendance,Théorie des Modèles, Indécidabilité

- Logique et Informatique

  J.Y. Girard, J.L. Krivine, A. Pnueli, S. Cook, R. Karp,..

  Preuves et Types, Vérification, Complexité

Naissance

Le calcul propositionnel (calcul booléen)

G. Boole, The Mathematical Analysis of Logic, 1847

Présentation algébrique du calcul propositionnel

The Laws of Thought, The Mathematical Theories of Logic and Probabilities, 1854

Formalisation du raisonnement

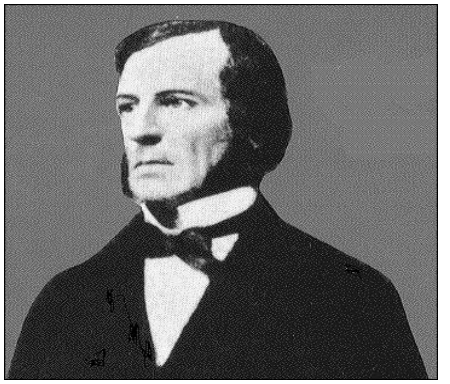
G. Frege, Begriffsschrift, 1879

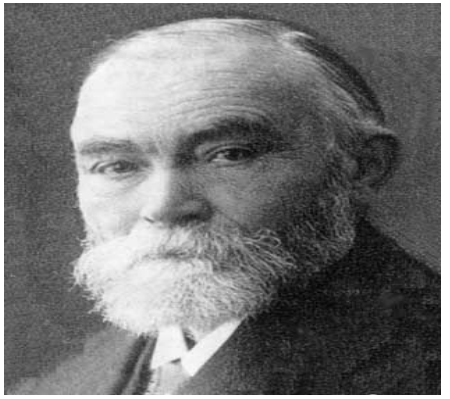
Notion de système formel

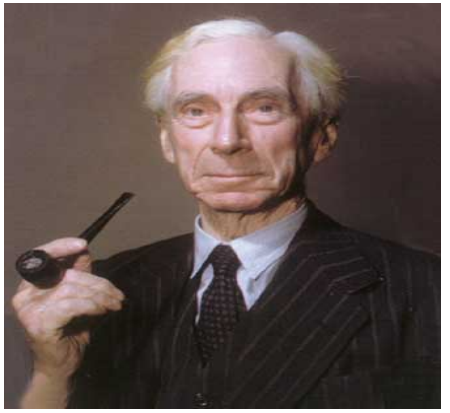
Principles of mathematics

B. Russell, 1903

Rejoint les conclusions de G. Frege







Fondements des mathématiques

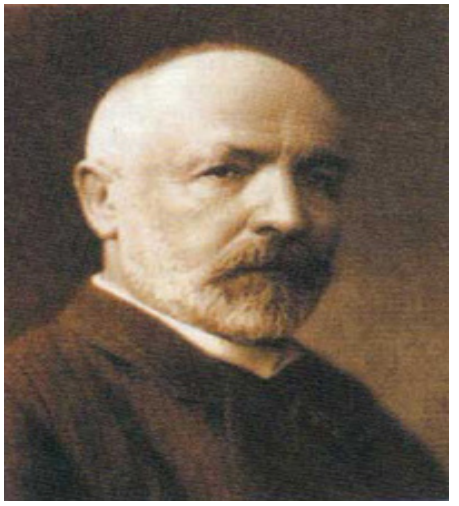
Axiomatisation des mathématiques: 1873-1895

- Analyse -------> Arithmétique Weierstrass, Dedekind,Cantor, Bolzano
- Arithmétique Dedekind, Frege, Peano,...
- Ensembles Cantor
- Géométrie euclidienne D. Hilbert, 1899

Théorie cantorienne :

Cardinalité des ensembles de réels

Etude mathématique de l'infini



Crise des Fondements

Paradoxes:

Burali-Forti 1897, Cantor 1899, Russell 1901

Richard 1905

« le plus petit nombre non définissable en moins de douze mots »

Zermelo (1904): Tout ensemble peut être bien ordonné

En réaction à cette crise, naissance de 3 projets...

Projets

- Logiciste:

  Réduction des mathématiques à une logique cohérente

  Principia Mathematica Russell, Whitehead 1910-1913

- Formaliste:

  Application des mathématiques à leur propre langage

  Programme de Hilbert, 1904

- Intuitionniste:

  Objections aux conceptions ensemblistes (Baire, Lebesgue, Borel)

  Poincaré

  et aux procédés non constructifs (thèse de Brouwer, 1907)

Logique et fondements des mathématiques

Quelques échantillons du programme de D. Hilbert (1904)

- Problème n°1: Démonstration de l'hypothèse du continu (HC)

  Tout sous-ensemble infini de R qui n'est pas équipotent à N

  est équipotent à R

- Problème n°2: Démonstration de la cohérence de l'Arithmétique

- Problème n°10: Décidabilité des problèmes diophantiens

  Existe-t-il un algorithme permettant de déterminer

  si un polynôme à coefficients dans Z possède des racines?

Panorama de la Logique mathématique

Origine: Formalisation et Fondements

- Théorie des Ensembles:

  Axiomatisation, ZF, problèmes de non contradiction relative

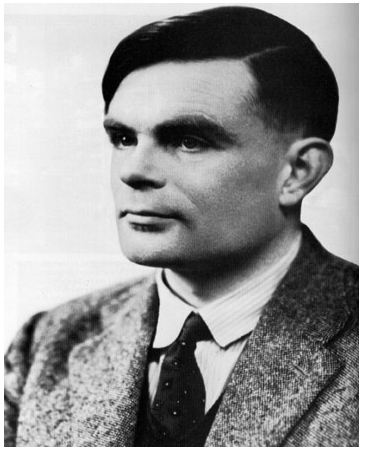
  Cantor, Zermelo, Fraenkel, Von Neumann, Skolem,... 1908-1920

- Théorie de la Calculabilité:

  Fonctions récursives, calculables sur machine,

  lambda-calcul

  Gödel, Church, Kleene, Markov, Post, Turing,... 1936



- Décidabilité et Indécidabilité: Church, Rösser, Tarski
- Théorie de la Démonstration:

  Calcul des séquents, déduction naturelle

  Gentzen 1935, Heyting

Premiers résultats

- Théorie des Ensembles:

  Zermelo-Fraenkel et Skolem (1920) ZF

  J. Von Neumann (1925), Bernays, Gödel NBG

- Ebauche de langage du 1er ordre Lowenheim (1915)

  Point de vue modèle Skolem (1923)

  Point de vue preuve J. Herbrand

- Thèse de Gödel (1930):

  Complétude et compacité

Premiers résultats (suite)

Théorie de la démonstration:

- G. Gentzen (1935) Calcul des séquents

  1e démonstration de cohérence de l' Arithmétique (1936)

- K. Gödel (1931-1932)

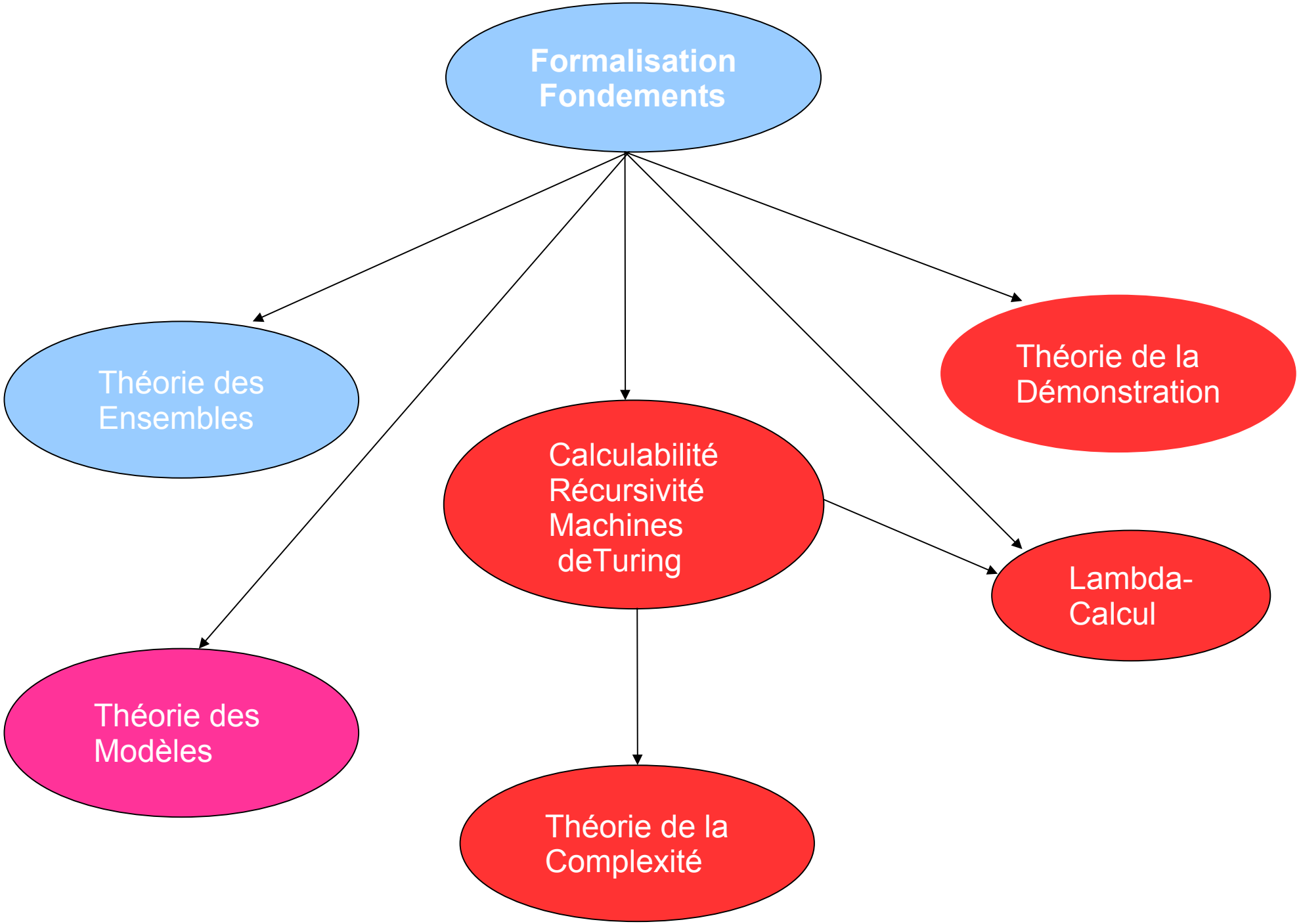
  Interprétation de la logique classique dans la logique intuitionniste

- A. Heyting (1930) 1e formalisation de l'Intuitionnisme
- A. Kolmogorov (1925) V. Glivenko (1929) A. Markov

  Constructivisme

Théorie de la Calculabilité: A. Turing (1936)

Fonctions calculables sur machine, problèmes indécidables


Formalisation
Fondements
Théorie des
Ensembles
Théorie de la
Démonstration
Calculabilité
Récursivité
Machines
deTuring
Lambda-
Calcul
Théorie des
Modèles
Théorie de la
Complexité

Panorama de la Logique mathématique (suite)

Développement de nouvelles branches (ou de nouvelles méthodes)

- Théorie des Modèles:

  Sémantique, construction de modèles

  A. Tarski 1931, L. Henkin, A. Robinson, Mal'cev, M. Morley, R. Vaught

- Théorie des Ensembles:

  Méthode du Forcing

  P. Cohen 1962, R. Solovay, J. Silver, D. Martin, R. Jensen

- Théorie de la Complexité:

  SAT, P=NP?, problèmes NP-complets, complexité descriptive

  S. Cook 1971, R. Karp, R. Fagin, N. Immermann

Résultats

- Théorie des Modèles:

  Constitution en tant que branche à part entière (Tarski, 1950)

  Méthodes de construction de modèles

  Résolution de la conjecture de Los par Morley (1963)

  Congrès international de Berkeley (1963)

  Concept de théorie stable (S. Shelah)

- Théorie des Ensembles:

  Méthode du Forcing

  P.J. Cohen Médaille Fields (1964)

  Réponse inattendue au 1er problème de Hilbert

Calculabilité et Arithmétique

- Problème n°1:

  Approche mathématique pour

  Calculabilité et Décidabilité

- Problème n°2:

  Existe-t-il une axiomatisation

  des propriétés vraies dans l'Arithmétique?

- Problème n°3:

  Existe-t-il un algorithme pour

  décider les propriétés vraies dans l'Arithmétique?

- Problème n°4:

  Qu'est-ce qu'un algorithme efficace?

Résultats

- Thèse de A. Church:

  Calculabilité = Récursivité = Turing-Calculabilité

  = lambda-définissabilité = …

- Indécidabilité et Incomplétude de l'Arithmétique:

  K. Gödel, 1931

- Indépendance de l'axiome du choix et

  de l'hypothèse du continu:

  K. Gödel, 1938, P.J. Cohen, 1962

  Indécidabilité des problèmes diophantiens:

  M. Davis, J. Robinson, Y. Matijasevich , 1970

- Théories catégoriques, théories stables:

  M. Morley, R. Vaught, S. Shelah, 1976...

Résultats (suite)

- Développement considérable de la théorie des ensembles

  R. Solovay, R. Jensen, J. Silver, D. Martin

- Exemples de phénomènes d'incomplétude en Arithmétique

  J. Paris, L. Harrington, 1977, L. Kirby, J. Paris, 1982

Complexité du problème SAT S. Cook, 1971

Réduction entre pb (difficiles) R. Karp, 1972

Problème ouvert:

- P=NP?

  Complexité descriptive?

Exemple de correspondance (sans courrier électronique…)

Lettre de Von Neumann à Gödel (1930):

- Affirme qu'il a une démonstration du 2e théorème d'incomplétude
- Comme Gödel joint à sa réponse une prépublication de ce résultat, Von Neumann ne publie pas la sienne

Lettre de Gödel à Von Neumann (1956):

- S'inquiète de la santé de Von Neumann, puis formule une question mathématique:
- "One can obviously easily construct a Turing machine, which for every formula F in first order predicate logic and every natural number n, allows one to decide if there is a proof of F of length n (length = number of symbols). Let ψ(F,n) be the number of steps the machine requires for this and let φ(n) = maxF ψ(F,n). The question is how fast φ(n) grows for an optimal machine. One can show that φ(n) ≥ k ק n. If there really were a machine with φ(n) Ґ k ק n (or even Ґ k ק n2), this would have consequences of the greatest importance."
- Formulation implicite de la conjecture P=NP (explicitée dans les années 70…)

Petit guide du M2 LMFI

Théorie des modèles:

- Ultraproduits et compacité. Théorèmes de Lowenheim-Skolem
- Théorèmes de préservation. Elimination des quantificateurs

Théorie de la démonstration:

- Théorème de complétude. Calcul des séquents
- Déduction naturelle. Lambda-calcul et types

Théorie des ensembles:

- Arithmétique ordinaux et cardinaux.
- Axiome du choix. Filtres et ultrafiltres.

Calculabilité et incomplétude:

- Fonctions récursives et fonctions calculables par machine
- Arithmétique, indécidabilité et théorèmes d'incomplétude
- Classes de complexité, réductions, complétude, complexité algébrique

Programmation fonctionnelle et preuves formelles en Coq

Petit guide du M2 LMFI
(suite)

Théorie des modèles (2 options):

- Outils classiques (types, théories catégoriques, théories stables,...)
- Géométrie o-minimale

Théorie des ensembles (1 option):

- Constructibles, Forcing et applications (indépendance de AC et HC, itération,...)
- Axiome de Martin et applications

Preuves et Programmes (2 options):

- Outils classiques pour la correspondance preuves-programmes
- Algèbre homotopique et catégories supérieures

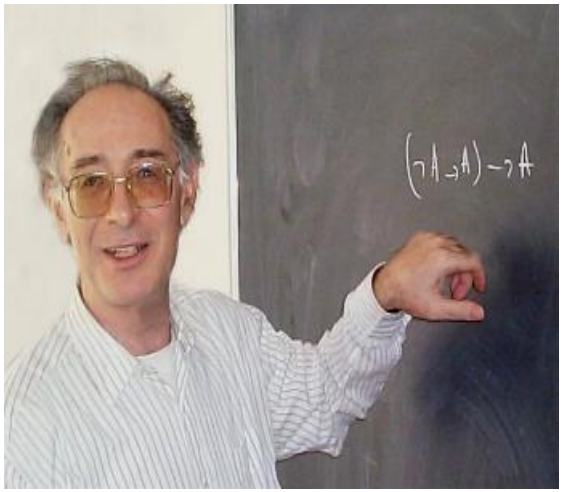
Les jeux en théorie des modèles

Quantification du second-ordre et points fixes en Logique

Complexité (pas d'option en 2023-2024):

- Hiérarchie polynomiale. Classes de comptage.
- Méthodes d'approximation. Vérification probabiliste et complexité

Logique et fondements de l'Informatique



- Preuves et Programmes:
  - Correspondance de Curry-Howard
  - Théorie de la démonstration
  - Systèmes d'aide à la preuve,
  - certification de programmes
- Vérification approchée et Complexité:
  - Preuves interactives et classes de complexité
  - Vérification de circuits, protocoles, systèmes distribués,...
- Complexité et automates:
  - Langages et logiques, complexité descriptive
  - Problèmes de model checking

Preuves et Programmes

Correspondance Types/Formules

Lambda-calcul typé (types simples):

- Types des termes de base
- Règles de construction des termes

  (abstraction, application)

- Réduction
- Terme général
- Type d'un terme

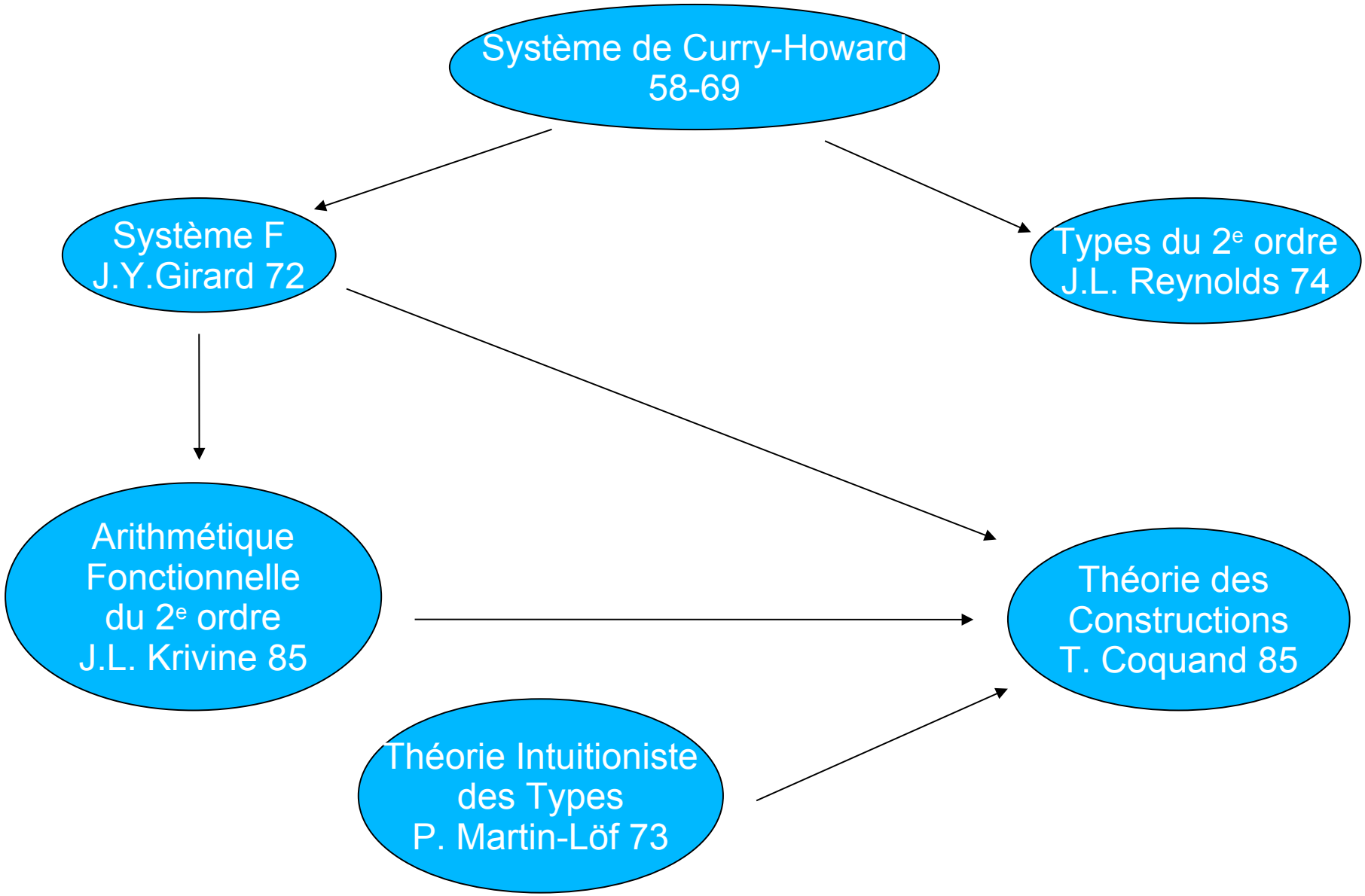
Logique propositionnelle intuitionniste:

- Axiomes Curry
- Règles de déduction concernant l'implication Howard

  (introduction, élimination)

- Elimination d'une coupure
- Preuve
- Formule

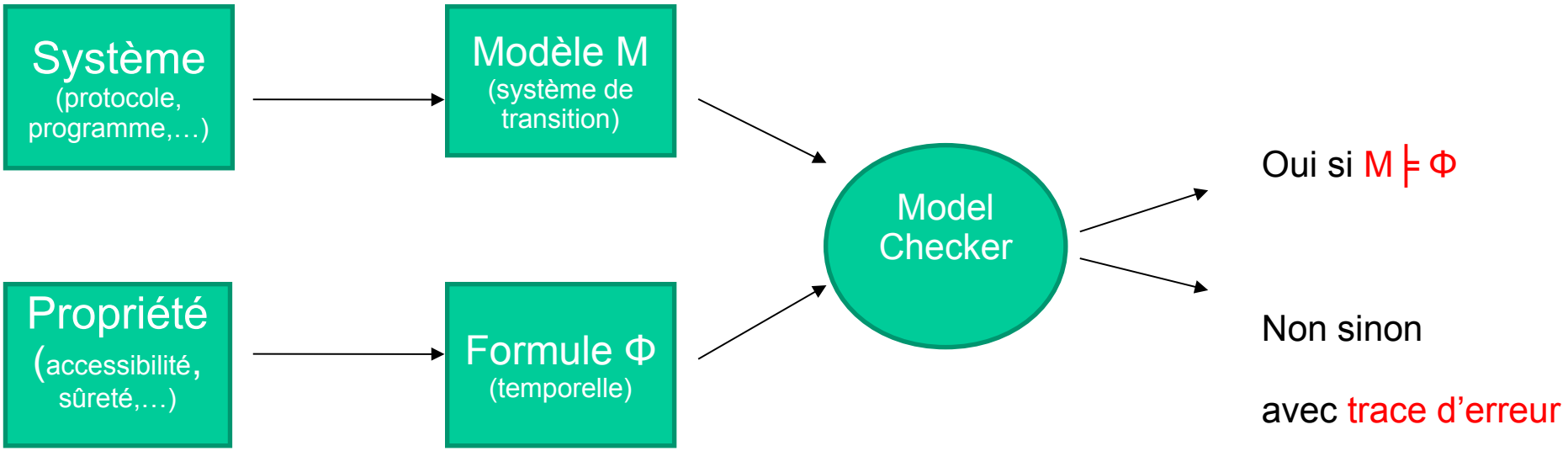
Le paradis (ou l'enfer?) des systèmes de types



Systèmes d'aide à la preuve

Proof Checker	Système de Types
COQ (INRIA, LRI)	Calcul des Constructions (T. Coquand)
PhoX, PML (C.Raffalli, Chambéry)	Arithmétique fonctionnelle du 2e ordre (J.L. Krivine)
Isabelle (L. Paulson, Cambridge) + Theorem Prover	Higher Order Logic (M. Gordon)
PVS (S. Owre,N. Shankar,J. Rushby , Stanford) + Theorem Prover	Théorie des types simples (A. Church)

Vérification par Model Checking



Complexité: linéaire dans la taille du modèle

Problème (modélisation): explosion combinatoire

Remarque: La complexité en espace est bien plus redoutable

(en pratique) que la complexité en temps

Complexité

Un problème célèbre (à 1 million de $): P=NP?

- S. Cook (71): le problème SAT est NP-complet
- R. Karp (72): de nombreux problèmes intéressants

(graphes, optimisation, combinatoire,…) sont NP-complets

Exemple: Pb de 3-coloriage d'un graphe

Entrée: Un graphe G=(E,R)

Question: Existe-t-il une fonction de coloriage f telle que

si (a,b) ε R, alors f(a) ≠ f(b)

Remarque:

- On ne connaît pas d'algorithme en temps polynomial pour ces problèmes
- Un algorithme en temps polynomial pour l'un de ces problèmes résoudrait

P=NP

Complexité descriptive

Question: Peut-on refléter la complexité (structurelle) d'un problème à l'aide de la complexité logique de la formule définissant ce problème?

Exemple: 3-coloriage d'un graphe

il existe une partition des sommets en 3 sous-ensembles t.q.

les extrémités de toute arête soient de 2 couleurs différentes

Théorème (R. Fagin, 74): Pour toute propriété sur les structures finies,

le problème de décision associé est dans NP ssi

elle est définissable par une formule existentielle du 2^e ordre

Théorème (N. Immermann, M. Vardi 82): Sur les structures finies ordonnées,

$$P \equiv FO + TC$$

FO + TC: logique du 1^{er} ordre + opérateur de clôture transitive

Complexité (suite et fin ?...)

Objectif: Distinguer entre problèmes difficiles (NP-complets, PSPACE-complets)

Méthodes:

- Approximation
- Algorithmes probabilistes

Schéma d'approximation en temps polynomial (FPTAS):

Algorithme A qui pour tout e>0, pour toute entrée x,

fournit une e-approximation A(x) du résultat exact

en temps poly(|x|,1/e)

Optimisation et Approximation

Pb	SAT	VC	CLIQUE	TSP	SAC A DOS
Décision	NP-comp	NP-comp	NP-comp	NP-comp	NP-comp
Optimisation					Pseudo-poly
Approx.					FPTAS
Non-app	FPTAS → P=NP		e-approx → P=NP	e-approx → P=NP	

Algorithmes probabilistes

Classe de complexité probabiliste: la classe RP

Un problème P est dans RP s'il existe un algorithme probabiliste A fonctionnant en temps polynomial t.q. pour toute entrée x,

si P(x), alors Prob[A refuse x] < 1/2,

si non P(x), alors Prob[A accepte x] = 0.

L'espace probabiliste est celui des tirages de l'algorithme.

Classe coRP: problèmes dont le complémentaire est dans RP

Exemple: le problème de primalité est dans coRP

Laboratoires d'accueil

IMJ (B.Velikovic, A.Durand,...)	Théorie des modèles, théorie des ensembles, complexité
IRIF PPS (A.Saurin, H.Herbelin,..)	Preuves et programmes, types
IRIF Algo et Complexité (F.Magniez,M.deRougemont)	Complexité
IRIF (A.Bouajjani, F.Laroussinie,...)	Vérification
LSV ENS-Paris-Saclay (P.Bouyer,...)	Vérification
IML Luminy (L. Régnier,...)	Preuves et programmes, types
VERIMAG Grenoble (J.F.Monin,...)	Vérification
GREYC Caen (E.Grandjean....)	Complexité descriptive
CEA-LIST Saclay (N.Rapin, S.Bardin)	Preuves et vérification
INRIA Projet Deducteam (G. Dowek)	Systèmes de preuves
LIX Palaiseau (O.Bournez)	Théorie des calculs
LIP ENS-Lyon (P.Koiran)	Complexité
ONERA Palaiseau (R.Kervac)	Méthodes formelles,traitement évènements complexes

Références

Générales:

- J. van Heijehoort *From Frege to Gödel* Harvard University Press (1967)
- K. Gödel *Collected Works: I,II,III,IV-V* Oxford University Press (1986-1992)
- J. Barwise *Handbook of Mathematical Logic* North-Holland (1977)
- R. Cori et D. Lascar *Logique mathématique (I et II)* Masson (1993)
- H. Enderton *A mathematical introduction to Logic* Academic Press (1972)
- P. Dehornoy *La théorie des ensembles* *Calvage & Mounet (2017)*

Preuves et systèmes de types:

- D. Prawitz *Natural Deduction* Almqvist et Wiskell (1965)
- J. L. Krivine *Lambda-calcul, types et modèles* Masson (1990)
- J. Y. Girard, Y. Lafont et P. Taylor *Proofs and Types* Cambridge University Press (1990)
- J. Y. Girard *Le Point aveugle (tomes 1 et 2)* *Hermann (2006-2007)*

Références (suite)

Vérification:

- Clarke, Grumberg et Peled *Model Checking* MIT Press (1999)

Complexité:

- M. R. Garey et D. S. Johnsson *Computers and Intractability: A guide to the theory of NP-completeness* Freeman and Co (1979)
- C. Papadimitriou *Computational Complexity* Addison-Wessley (1994)
- M. de Rougemont et R. Lassaigne *Logic and Complexity* Springer (2004)
- R. Motwani et P. Raghavan *Randomized Algorithms* Cambridge University Press (1995)
- M. Mitzenmacher et E. Upfal *Probability and Computing: Randomized Algorithms and Probabilistic Analysis* Cambridge University Press (2005)