Preuves assistées par ordinateur

Hugo Herbelin, Théo Zimmermann

basé sur du matériel d'Alexandre Miquel et Pierre Letouzey

Un peu d'histoire

le développement de la logique mathématique formelle (Boole 1854, Peirce, de Morgan)

- connecteurs : $\wedge$, $\vee$, $\neg$, $\top$, $\bot$, $\Rightarrow$, $\Leftrightarrow$
- quantificateurs : $\forall$, $\exists$
- domaine du discours : x, $f(t,u)$, ...
- propositions, prédicats : $P(t,u)$, $t=u$, ...
- propriétés algébriques : $\neg(A \vee B) \Leftrightarrow (\neg A \wedge \neg B)$, ...
- premier système formel de preuves (Frege 1879) : $\Gamma \vdash A$

les fondations mathématiques

- l'arithmétique de Peano (1889) : $\mathbb{N}$, $0 \neq 1$, induction, ...

- la théorie des ensembles naïve de Cantor (1874), de Zermelo (Z, 1908), de Zermelo-Fraenkel (ZF, 1922) : $t \in u$, $\emptyset$, $\{x|P(x)\}$, $x \mapsto t$, ...

- Principia Mathematica (Russell-Whitehead, 1910)

Un peu d'histoire

La question des fondements (Hilbert, Gödel 1932, Gentzen 1934, ...)

- cohérence (peut-on prouver l'absurde ?) : $\vdash \bot$? ?
  - Gödel met une fin au programme de Hilbert : on ne peut pas prouver la cohérence d'un système arithmétique sans faire appel à un système plus puissant que celui qu'on considère
  - dans tout système logique cohérent, il y a des propositions ni prouvables ni réfutables
  - vérifier une preuve est décidable mais, dès qu'on parle de nombres, l'existence d'une preuve n'est pas décidable
- relations entre langage et métalangage (complétude)
- systèmes axiomatiques (à la Hilbert) : $A \Rightarrow B \Rightarrow A$, Modus Ponens, ...
- déduction naturelle (Gentzen 1934) : $\dfrac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B}$
- calcul « logistique » des séquents (Gentzen 1934) : $\Gamma \vdash \Delta$

La question des fondements (Hilbert, Gödel 1932, Gentzen 1934, ...)

- des modèles universels de calcul :
  - machine de Turing (1935)
  - logique combinatoire (Schönfinkel 1924, Haskell Curry 1930) : K, S et application
  - λ-calcul (Church 1932) : x, $\lambda x.t$, $t\,u$
  - fonctions partielles récursives (Gödel 1934, Kleene) : $T(n,p,q)$, théorème smn, ...
- la théorie des types simples (STT, Church 1940) aussi connue sous le nom de logique d'ordre supérieur (HOL), qui sont des variantes du Système F_ω de Girard

le développement d'un lien entre preuves et programmes

- logique intuitionniste (Brouwer ∼1920, Kolmogorov 1925, Heyting 1930) : $A \vee \neg A$ rejeté

- réalisabilité (Kleene 1945, Gödel 1958, Kreisel 1959) : si on a $\vdash \forall x\, \exists y\, P(x,y)$ alors il existe un programme f tel que pour toute valeur t, on a $\vdash P(t, f(t))$

la correspondance directe entre preuves et programmes

- système axiomatique Automath basé sur le λ-calcul (de Bruijn 1960's)

- système axiomatique = logique combinatoire (Curry 1934)

- déduction naturelle = λ-calcul (Howard 1968)

- théorie des types de Martin-Löf d'abord naïve (**Type** : **Type** en 1970), puis prédicative, un formalisme qui est à la fois une logique et un langage de programmation (MLTT)

autres exemples

- calcul des séquents = machine abstraite

- logique propositionnelle du second ordre = Système F de Girard et Reynolds

- $\perp \Rightarrow A$ = opérateurs d'interruption du flux de contrôle (`return`, `break`, `exit`, ...)

- $A \vee \neg A$ = opérateurs de contrôle (`goto`, `callcc`, ...)

- forcing $\simeq$ mémoire modifiable (`x <- t`)

- modèles syntaxiques $\simeq$ Lisp's `quote` *l'implémentation de logiciels de développement et vérification de preuves (assistants à la preuve, aussi connus comme prouveur de théorèmes interactifs - ITP)*

- Mizar (Białistok), basé sur la théorie des ensembles

- Isabelle/ZF, Isabelle/HOL (Cambridge, Munich 1990-)

- Coq, basé sur le calcul des constructions inductives (CC 1984, puis CIC 1990, étendant MLTT), puis Lego, Matita, Lean

- NuPrl (université de Cornell), Agda (université de Göteborg), basés sur d'autres variantes de MLTT

La question des fondements à la fin du 20e et début du 21e siècle

- la logique linéaire au cœur d'une décomposition des connecteurs (Girard, 1987)

- la théorie des types homotopiques (à partir de 2005) établit de nouveaux liens entre logique et géométrie : $t =_A u$ représente l'ensemble des chemins entre deux points t et u d'un espace A

- la logique polarisée et les adjonctions catégoriques au cœur de la description des effets de bord

- une convergence entre logique, géométrie, informatique, algèbre :
  - théorie des types $=$ topos
  - propositions $\subset$ espaces $=$ types $=$ catégories
  - types inductifs $=$ colimites $=$ types positifs : $\mathbb{N}$, listes, arbres
  - types coinductifs $=$ limites $=$ types négatifs : streams, ...

Les assistants à la preuve en 2021

- de grands projets de certification des programmes :
  - le compilateur C certifié CompCert (Leroy *et al*)
  - le micro-noyau certifié SeL4
  - la logique de séparation IRIS, Fiat, Vellum, ...
  - la chaîne de certification DeepSpec
- de grands succès mathématiques :
  - une preuve formelle exhaustive du théorème des 4 couleurs (Gonthier *et al*, 2005)
  - le théorème de l'ordre impair, dit Feit-Thompson (Gonthier *et al*, 2012)
  - une preuve formelle de la conjecture de Kepler sur l'empilement optimal des oranges sur l'étal du primeur (Hales *et al*, 2014)
  - un intérêt croissant pour la formalisation des mathématiques par les mathématiciens

Un peu de technique

lieurs, substitution, règles d'inférence de la déduction naturelle, représentation des preuves par des programmes, ...