Jérôme Germoni
12/9/2013.

Formalisation de la preuve du Th de Feit-Thompson : 5-10 ans de travail

- Qu'est-ce qu'une preuve formelle ?

Revue de presse sur France Inter : jurer de faire / jurer de mauvaise foi.

- pas d'erreurs en maths ! méthode hypothético-déductive.

Avis : erreur de Poincaré : prix du roi Oscar de Norvège.

→ sur l'instabilité du système solaire : il avait commencé à montrer la stabilité !

→ erreur de Wiles (très bête mais bien cachée)

→ Amnon Neeman : "A counterexample to a 1961 'theorem'"

Trois exemple de formalisation.

- Bhargava : figure
- Texte en français.
- Russell - Whitehead.

"Il reste toujours de l'implicite : sinon, c'est ingérable".

- Fondements de la géométrie de Hilbert.

→ hiérarchie des types de Russell-Whitehead.
impossibilité de fonder en ayant une tour infinie.

→ vocabulaire qui parle du langage math.

- La science et l'hypothèse de Poincaré (1902)

- "rêve" de Hilbert : algorithme universel.
- démontrabilité / complétude et incomplétude. (Gödel 1931)

Tentative de Bourbaki (1940) : L'usage exclusif des assemblages conduisait à des difficultés insurmontables.

Preuve = suite d'arguments acceptés par un interlocuteur ou une communauté.

c'est un phénomène social qui dépend de l'époque, du contexte (cours oral / recherche écrit), du pays, de la discipline.

Bourbaki Perelman. géométrie algèbre.

Confiance du système logiciel fondée sur des tests.

certification : _bug de la division du Pentium : Intel a investi dans la certification.
_explosion d'Ariane 5.

Ex : certification de l'algorithme d'Euclide

Produire à la fois une preuve et un certificat de preuve

Coq : _ "Calculus of constructions" "assistant de preuve"
- introduit par Thierry Coquand.
- cours de Coq pour enseigner la preuve aux étudiants en info.
- usages industriels : Java Card, Gérard Berry - Esterel - aéronautique de Nice.

Écrit en OCaml : langage fonctionnel : λ-calcul (Church).

c'est la "revanche de Russell" (Gonthier) : basé sur la th. des types.

Preuve en direct de : ∀A, B assertions, (A et (A ⇒ B)) ⇒ B.

[le modus ponens] Coq < Lemma tt :

Coq < forall A B : Prop, (A ∧ (A -> B)) -> B.

1 subgoal

tt < intros.

1 subgoal

A : Prop
B : Prop
H : A ∧ (A → B)

B

tt < destruct H

1 subgoal

A : Prop
B : Prop
H : A
H0 : A → B

B

tt < apply H0

1 subgoal

A : Prop
B : Prop
H : A
H0 : A → B

A et

A et parmi les hypothèses.

Coq est content !

Coq < Qed tt

...

< Print tt

λ A B. ⌊⌋

c'est la correspondance de Curry Howard

Langage formel :

le connecteur regroupement tous à => et la constante ⊥ "faux"

Substitut à ∀ : l'abstraction

λx f(x) ou mieux λ(x:A).(f(x):B).

↑ type de x ↑ type de f(x)

λ calcul de Church | λ-calcul typé. type de f(x)

Correspondance preuve-programme de Curry-Howard.

énoncé = type
preuve = programme

preuve d'un énoncé = tous deux type, l'énoncé.

en info : déf. inductive des types.
on part de types atomiques,
puis on construit A → B.
c'est une fonction qui à a : A associe (complète/totale)
t(a) : B.

Donc à une preuve a de A, elle associe une preuve t(a) de B.

Preuve par l'absurde = séquence d'échappement
" on sort du programme

Certifié : Bézout, Gödel, Jordan, nombres premiers : et pourtant basé sur l'analyse complexe.

- Th 4 couleurs
- Feit Thompson

} certifié par Gonthier-Werner Gonthier

À certifier : la conjecture de Kepler.

La preuve de Hales de la conj. de Kepler : non certifiée par les rapports d'Annals of maths : ils ne savent pas exclure l'erreur.

Donc Hales : certifié !

Or "toutes les 500 lignes de code il y a un bug".

Coq est construit autour d'un cœur de 500 lignes
sauté et testé dans de nbreuses situations.
Le cœur peut certifier le reste.

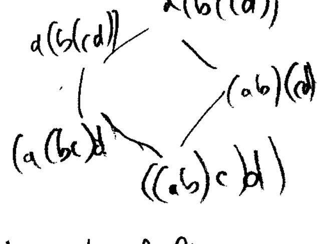
MAIS : il faut croire à la th. de la démo ; que Coq l'implémente,
au langage OCaml ; au microprocesseur...

Pb : preuve formelle = 1,5 × preuve classique.
Feit Thompson = 6 ans pour 5-10 personnes.
intuition : on n'a pas d'alternative : 4 couleurs, Kepler, FT
Cela transforme la preuve en un objet math.

Univalent foundations of maths : IAS (Princeton).
+ Voevodsky - Awodey : empreinte forte du catégoricien.

Gonthier : mise en place de types qui prennent en compte pls registres

égalité : égalité stricte / à qqch près
pb : le corps à 4 éléments ... isomorphismes
associativité : ds les catégories tensorielles.



→ comment l'implémenter ?
sur cette Q : th. de cohérence de MacLane : on obtient le même résultat quel que soit le chemin sur le graphe.

Le th. de FT : tout groupe fini simple de cardinal impair est abélien
+ Si G groupe fini et $|G| \equiv 1 [2]$, alors G est résoluble.
+ Si G est simple non abélien alors $|G| \equiv 0 \ [2]$.

Q : OCaml
- licence
- associa...

Question : Coq va-t-il populariser la th. de types ? voir Assia Mahboubi ; HoTT : livre pour...