Assistants de preuve

MPRI - 2006-2007

3- Architecture des assistants de preuve

Les principaux assistants de preuve

ACL2, PVS, HOL, HOL-Light, Mizar, Isabelle, Twelf, Coq

PhoX, Matita, Agda/Alfa, Epigram, MetaPrl, Minlog, ...

Frontière parfois floue avec

- prouveurs automatiques de théorèmes (Automatic Theorem Provers) (cf Otter, Simplify, CVC, Vampire, ...)

- système de calcul formel (Computer Algebra System) (cf Maple, Mathematica, Magma, Axiom, MuPad, Maxima, ...)

- vérificateur de modèle (Model Checker) (cf Spin, Uppaal, SMV, ...) (liste hautement non exhaustive)

Critères d'analyse des assistants de preuve

- critère de de Bruijn : la correction des preuves repose-t-elle sur un petit ensemble de lignes de code bien délimité

- critère de Poincaré : une notion de calcul est-elle intégrée ? (typiquement $2+2=4$ nécessite-t-il une preuve ou une simple vérification calculatoire)

- statut des preuves : termes de preuves, arbres de tactiques, ou pas de représentation des preuves ?

- interactivité : méthode procédurale (tactiques) ou déclarative (déclarations d'énoncés prouvés automatiquement)

- automatisation : étendue de la décision automatique
  - décision de théories particulières
    - systèmes d'inéquations linéaires, systèmes d'équations polynomiales, systèmes d'inéquations polynomiales,
    - équations polynomiales, équations entre fractions polynomiales,
    - résolution, unification, induction automatique ...
  - décision ou semi-décision de logiques particulières (calcul propositionnel, calcul des prédicats, ...)
  - traitement du calcul et des égalités
  - combinaison de l'automatisation (Schostak, Nelson-Oppen, ...)

- logique : logique spécifique ou méta-logique ("logical framework")

- robustesse, passage à l'échelle, modularité, notations, macros...

Panorama des assistants à la preuve

Systèmes à diffusion large

- ACL2 : suite des systèmes NqThm et Pc-NqThm de Boyer-Moore et de Kaufmann, s'utilise dans Lisp, calcul dans Lisp, implémente l'arithmétique, excellente automatisation, largement utilisé pour la preuve de hardware, pas d'objet preuve, déclaratif

- HOL : suite de LCF, logique d'ordre supérieur de Church, écrit en SML, largement utilisé pour la preuve de hardware, preuves sous formes de tactiques, procédural

- HOL-Light : logique d'ordre supérieur de Church, en O'Caml, utilisé pour la preuve de hardware et la formalisation des mathématiques, preuves sous formes de tactiques, procédural

- PVS : logique d'ordre supérieur, en Lisp, excellente automatisation, appliqué à différents types de preuves de programme, pas d'objet preuve, interactif

- Isabelle/HOL : logique d'ordre supérieur, en ML, bonne automatisation, objets preuves, applications diverses, procédural et déclaratif

- Coq : logique d'ordre supérieur avec inductifs et et types dépendants, en O'Caml, bonne automatisation, objets preuves, procédural et déclaratif, applications surtout mathématiques

- Mizar : théorie des ensembles de Tarski-Grothendieck, en Pascal, dédié à la formalisation des mathématiques, journal de mathématiques formelles, déclaratif, pas d'objet preuve

-Twelf : méta-logique, suite de LF et de ELF, offrant unification d'ordre supérieur dans un langage avec lieurs d'ordre supérieur (Higher-Order Abstract Syntax)

Panorama des assistants à la preuve (suite)

Systèmes à diffusion restreinte

- PhoX : arithmétique d'ordre 2, en O'Caml, utilisé dans l'enseignement, Chambéry
- Matita : Calcul des Constructions Inductives, O'Caml, récent, Bologne
- Agda/Alfa : méta-logique de Martin-Löf, Haskell, preuves données comme des programmes, Göteborg
- Epigram : théorie des types observationnelle, Haskell, bonne gestion des inductifs dépendants, Nottingham
- MetaPrl : méta-logique de Martin-Löf, extraction, Cornell
- Minlog : arithmétique, extraction en logique classique, Munich

Autres systèmes: Omega, Theorema, Metamath, IMPS

Ceci est une présentation sommaire, plus d'infos par exemple dans "The Seventeen Provers of the World" de Freek Wiedijk.