Tenure Track 2012 – 2015 : Bilan et perspectives

Olivier Hermant
Centre de recherche en informatique
Commission de la recherche, 18 juin 2015

Parcours

Thèse (3 ans) :

- 2002-2005 : doctorat (G. Dowek, Inria et École polytechnique)

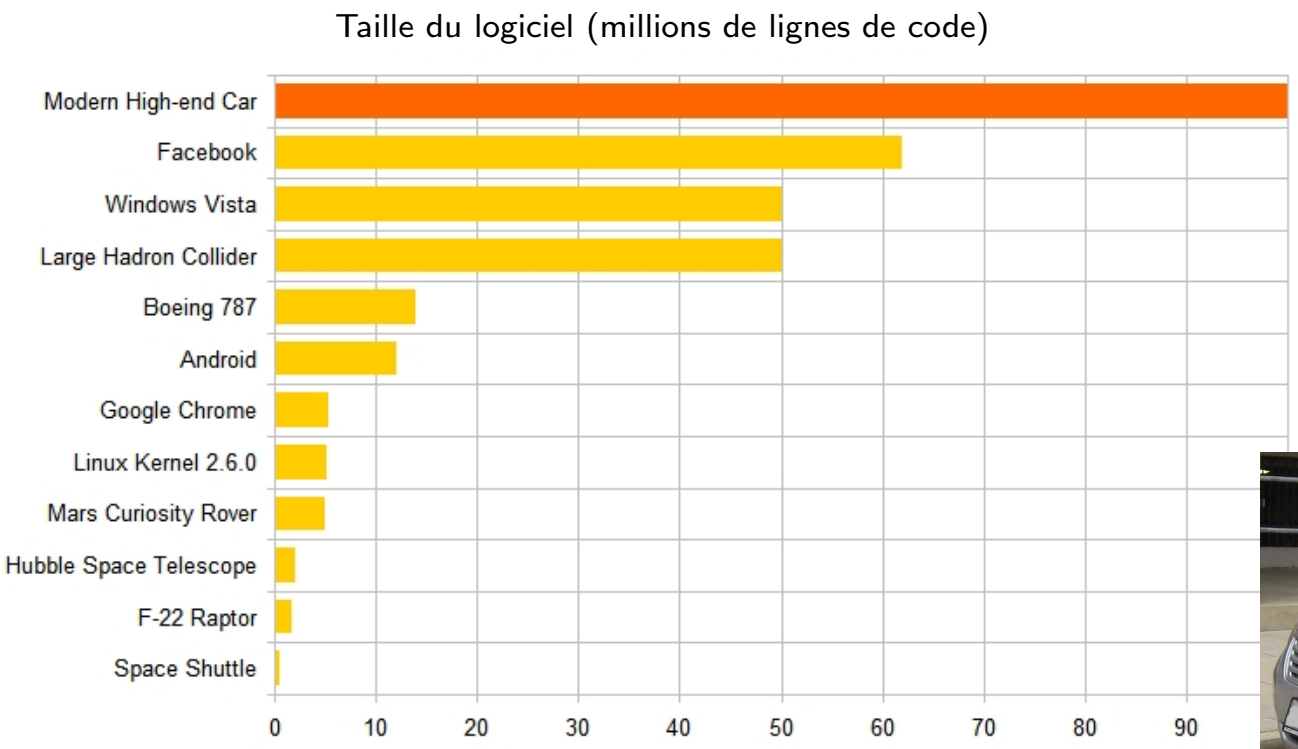
Séjours post-doctoraux (3 ans) :

- 2005-2007 : ATER (Paris VI et Paris VII)
- 2007-2008 : post-doc (U. Complutense, Madrid)

Enseignant-chercheur (7 ans) :

- 2008-2012 : ISEP (CTI), Paris, 275h/an (enseignement)
- 2012-2015 : CRI, MINES ParisTech

Domaine : méthodes formelles



- jusqu'à 100 millions de lignes
- code critique
- coût d'un bug

Questions de recherche :

- qualité du logiciel ?
- sécurité et sûreté ?
- respect des spécifications ?

source: https://www.linkedin.com

Approche : la preuve

Correspondance formelle

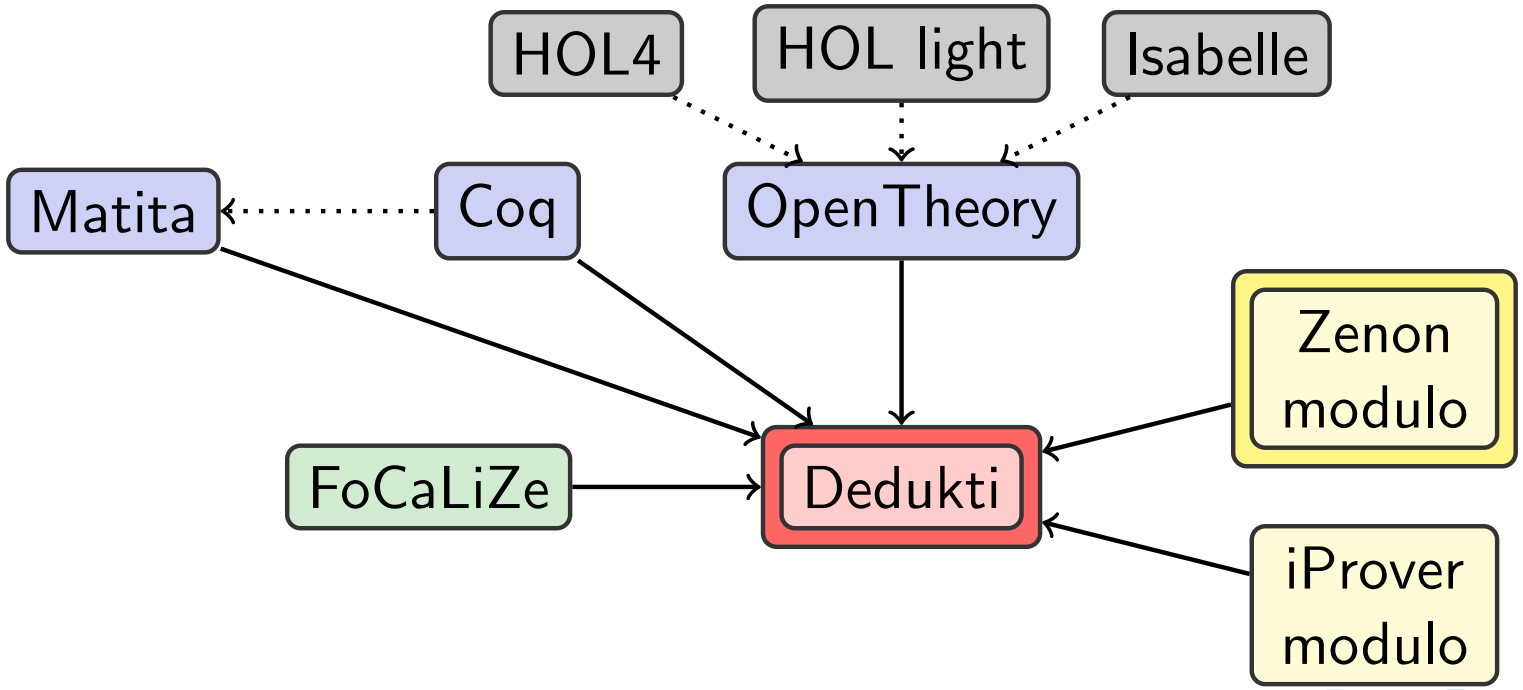
Informatique	$\longleftrightarrow$	Mathématiques
Spécification	$\longleftrightarrow$	Théorème
Programme	$\longleftrightarrow$	Preuve

Contributions

- assistant de preuve : Dedukti
- preuve automatique : Zenon Modulo
- fondements mathématiques des langages de programmation

Dedukti, un vérificateur universel

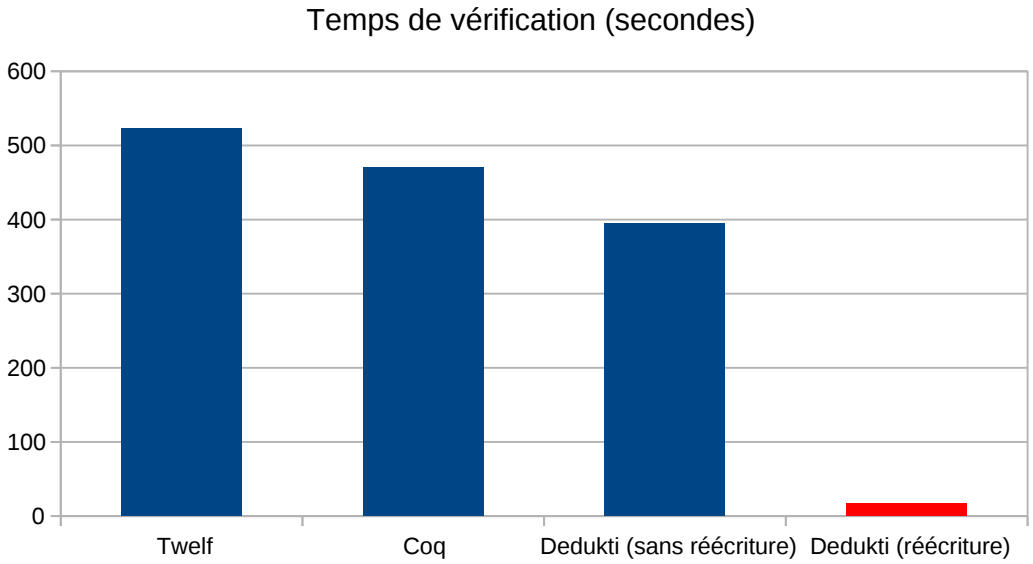
- agnostique, avec une logique paramétrable
- langage universel pour la preuve assistée
- $\lambda\Pi$-calcul avec règle de conversion étendue
- *plongements* qui conservent le calcul (collaboration Inria)
- thèse de Ronan Saillard [2015]



$\lambda\Pi$-calcul modulo

$$\frac{\Gamma \textbf{ wf} \qquad l \text{ et } r \text{ bien typés}}{\Gamma([\Delta]l \hookrightarrow r) \textbf{ wf}}\ \text{(Rewrite)} \qquad \textbf{(Conv)}\ \frac{\Gamma \vdash t : A \qquad \Gamma \vdash B : s \qquad A \equiv_{\beta\Gamma} B}{\Gamma \vdash t : B}$$

$$\textbf{(App)}\ \frac{\Gamma \vdash t : \Pi x^A.B \qquad \Gamma \vdash u : A}{\Gamma \vdash tu : B[x/u]} \qquad \textbf{(Abs)}\ \frac{\Gamma \vdash A : \textbf{Type} \qquad \Gamma(x : A) \vdash t : B \qquad B \neq \textbf{Kind}}{\Gamma \vdash \lambda x^A.t : \Pi x^A.B}$$



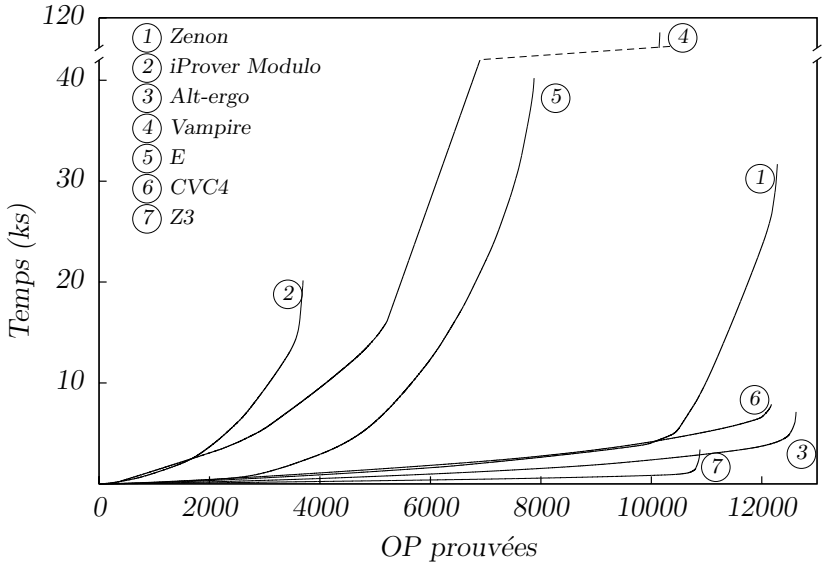
$$2 + 2 \hookrightarrow 4$$
$$map(f, [1, 2, 3]) \hookrightarrow [f(1), f(2), f(3)]$$

- dynamique, souple
- comparable aux outils dédiés, plus universalité
- vers l'interopérabilité

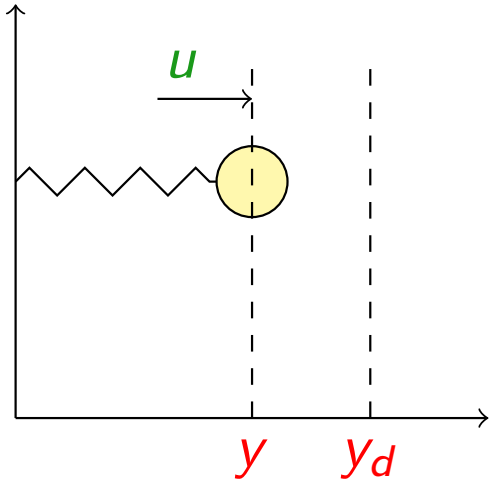
Zenon Modulo : démonstration automatique

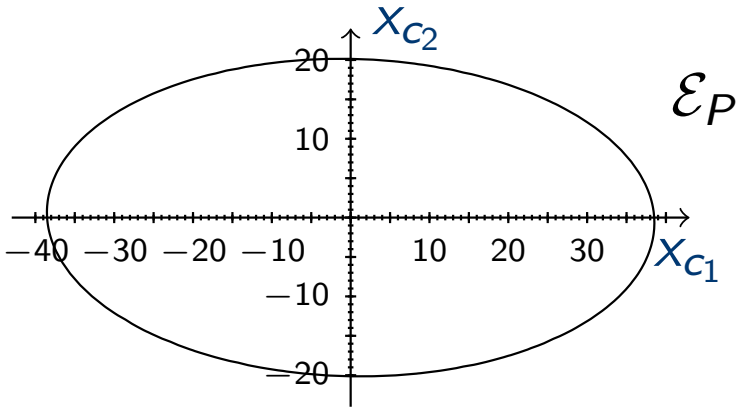
- problématique : méthode B
  $\hookrightarrow$ théorie des ensembles
- raffinement : spécifications haut-niveau
  $\hookrightarrow$ code bas-niveau
- transport automatique
- Ligne 14 : 27000 *obligations de preuve*

- automatisation : plate-forme BWare
- déduction modulo théorie : Zenon modulo
- thèse de Pierre Halmagrand [2016]



Stabilité de Lyapunov : des réels aux flottants



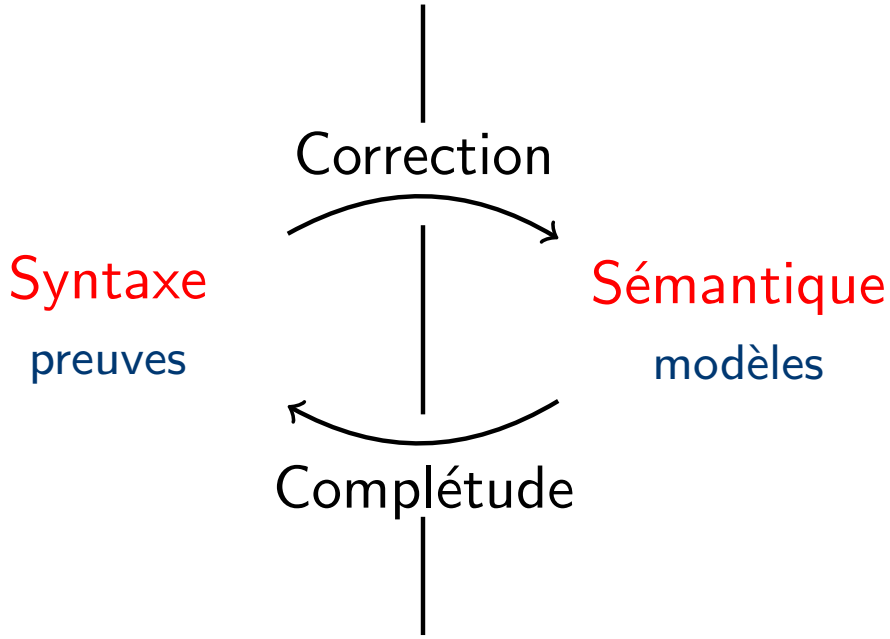



```
while (1)
    % xc ∈ E_P
    yc = max(min(y - yd, 1), -1);
    % xc ∈ E_P, yc^2 ≤ 1
    skip;
    % zc ∈ Q_μ, Q_μ = ( μP  0_{2×1} ; 0_{1×2}  1−μ ), μ = 0.9991
    u = Cc*xc + Dc*yc;
    % zc ∈ Q_μ, u^2 ≤ (Cc Dc) · Q_μ^{-1} · (Cc Dc)^{-1}
    xc = Ac*xc + Bc*yc;
    % xc ∈ E_R, R = [(Ac Bc) · Q_μ^{-1} · (Ac Bc)^T]^{-1},
    % u^2 ≤ (Cc Dc) · Q_μ^{-1} · (Cc Dc)^{-1}
    send(u, 1);
    % xc ∈ E_R
    receive(y, 2); receive(yd, 3);
    % xc ∈ E_R
    skip;
    % xc ∈ E_P
```

- outil LyaFloat
- thèse Vivien Maisonneuve [02/2015]

Étude des formalismes sous-jacents

- les prouveurs sont-ils corrects ?
- peut-on trouver toutes les démonstrations ?



- Et si on applique la correspondance preuves-programmes ?
  - méthode d'évaluation sémantique des langages

Production scientifique

Publications :

- total : 4 journaux, 14 conférences, 7 workshops
- 2012-15 : 1 journal, 8 conférences, 3 workshops

Encadrement :

- 1 post-doc (A. Spiwack), 2 thèses en cours, 2 soutenues
- 4 stages M2

Collaborations :

- international : UFRN (BR, R. Bonichon),
  U. Wesleyan (US, J. Lipton)
- Europe : U. Cambridge (UK, T. Pasquier),
  U. Jacobs (GE, F. Rabe)
- France : Inria Deducteam, Isep (Cloud)

Implication dans l'École

Enseignement :

- adjoint au responsable de l'option MSI
- TC info 1 : groupe 2
- ES informatique fondamentale : 3 séances
- Mastère spécialisé MSIT : 5 thèses professionnelles
- extérieur : ISEP (40h, 3A), MPRI (M2)

Recherche au CRI :

- formalisation des langages : complétude de Turing (Faust)
- contrats : BWare, Feever, PPS, IDCapture

Participation à la vie de l'école :

- gestion des congés
- commission consultative paritaire (cadre de gestion)

Futur

- court terme :
  - soutenance Ronan Saillard [2015]
  - soutenance HDR [2015] : 80 pages rédigées
  - séjour sabbatique Wesleyan (US, [Sep. 2015 – Mai 2016]) : sémantique des langages
- moyen terme :
  - comité scientifique du Groupe de recherche CNRS *Génie de la programmation et du logiciel* [2016]
  - projets & contrats
  - chaire méthodes formelles
  - enseignements : info 1, fondements de l'informatique dans sa totalité
- projets de recherche :
  - assistants de preuves, démonstration automatique
  - application à l'analyse de programmes

Tenure Track 2012 – 2015 : Bilan et perspectives

Olivier Hermant
Centre de recherche en informatique
Commission de la recherche, 18 juin 2015