

Rapport sur la thèse présentée par

Mircea-Dan Hearnest

Extraction de programmes efficaces à partir de preuves (non-constructives) par l'interprétation Dialectica (monotone)

L'installation de l'informatique au centre de notre société au cours des trois dernières décennies a mis au premier plan la question du développement de programmes certifiés. Question apparemment simple, mais qui, dès qu'on la regarde de près, se révèle extrêmement compliquée, aussi bien au plan pratique que théorique, et pose en fait le problème fondamental - et à ce jour non encore entièrement résolu - de la relation entre preuves et programmes. Cette question a redonné une actualité à celles posées dès les premières décennies du siècle dernier concernant le contenu constructif des preuves, la différence étant que cette fois l'enjeu n'est plus seulement celui des fondements des mathématiques, mais l'extraction de véritables programmes à partir de preuves.

La correspondance entre preuves et programmes, au travers de ce qu'on appelle l'isomorphisme de Curry-Howard, est ainsi devenu un sujet central aux confins des mathématiques et de l'informatique. Les nombreux travaux qui y ont été consacrés, ont été sources de progrès importants dans la compréhension, la définition et l'implantation des langages de programmation typés. Plus récemment, ils ont conduit à une relecture des démonstrations mathématiques elles-mêmes, sous l'angle des programmes qu'elles contiennent.

L'isomorphisme de Curry-Howard n'est cependant pas l'unique voie d'accès aux programmes contenus dans les preuves. Diverses notions d'interprétation, en particulier la réalisabilité modifiée de Kreisel et l'interprétation Dialectica de Gödel, peuvent aussi être utilisées.

L'interprétation Dialectica de Gödel, qui véhicule souvent une image ésotérique, a été peu étudiée dans ce contexte. Kohlenbach l'a remise au premier plan ces dernières années au travers de son programme de "proof mining" qui a fourni une quantité impressionnante de résultats. Lui-même et ses étudiants ont utilisé l'interprétation Dialectica dans plusieurs domaines des mathématiques, pour produire des bornes effectives nouvelles de théorèmes classiques.

L'objet des travaux de Dan Hearnest est d'appliquer ce programme de "proof mining" non pas à la recherche de bornes, mais à l'extraction de programmes efficaces à partir de preuves - le mot "efficace" étant ici le mot déterminant. Disons d'emblée qu'il s'agit d'un sujet ambitieux et difficile, qui mérite à l'évidence d'être exploré complètement.

La thèse s'ouvre sur un résumé étendu (en Français) de 18 pages, qui reprend essentiellement les introductions de chacun des chapitre de la thèse et fournit ainsi une présentation synthétique des résultats obtenus et des principaux choix méthodologiques et théoriques qui ont été fait. La présence de ce résumé est tout à fait judicieuse.

Le chapitre 1, qui introduit de façon détaillée les différents systèmes utilisés, n'est pas de la même facture. Il illustre assez bien l'adage selon lequel pour accéder aux belles choses, il faut souffrir. Il est difficilement accessible au lecteur extérieur. Il y a à cela des raisons objectives liées aux particularités des systèmes utilisés, mais pas seulement. La présentation est elle aussi en cause : l'introduction de nombreuses variantes, pas toujours indispensables à ce qui sera dans la suite le coeur de la thèse,

l'accumulation de notations et d'abréviations (souvent codées sur trois lettres) rend la mémorisation en première lecture impossible et l'absence d'index complique dans la suite les nécessaires retours en arrière.

Le chapitre 2 est le coeur de la thèse : on y trouve la définition et la correction de l'interprétation *Dialectica* légère, qui affine l'interprétation *Dialectica* de Gödel. Malheureusement, l'auteur suppose que l'interprétation *Dialectica* originale de Gödel est bien connue du lecteur, ce qui limite le nombre de lecteurs potentiels. Une page d'explications sur ce qui en fait la particularité et la difficulté - l'interprétation du connecteur \rightarrow - n'aurait pas été superflue.

L'interprétation *Dialectica* légère se présente comme une optimisation de l'interprétation *Dialectica* de Gödel au moyen de quantificateurs sans contenu calculatoire. Le résultat principal est la correction des termes extraits par cette méthode. Sa preuve est rédigée en détail et occupe pas moins de 10 pages du chapitre 2. La pertinence de la méthode, en égard notamment à l'objectif d'efficacité des programmes extraits, est justifiée par les exemples développés aux chapitres 4 et la comparaison avec la méthode d'extraction de Berger-Buchholz-Schwichtenberg qui y figure.

Le chapitre 2 introduit aussi deux raffinements de cette méthode : l'interprétation *Dialectica* monotone légère, qui combine les avantages de l'interprétation *Dialectica* légère précédente (destinée à l'extraction de programmes) et de l'interprétation *Dialectica* monotone de Kohlenbach (destinée à l'extraction de bornes), et l'extension de ces interprétations pour permettre l'extraction de programmes à partir de preuves en logique classique.

Outre les contributions précédentes, la thèse contient deux contributions qui méritent d'être notées :

- le chapitre 3 introduit un système pour l'extraction de programmes calculables en temps polynomial ;
- l'annexe A étudie la complexité des algorithmes d'extraction de programmes et bornes fournis par l'interprétation *Dialectica* et l'interprétation *Dialectica* monotone.

Nonobstant les difficultés de lecture précédemment soulignées, je considère le travail de recherche présenté comme étant de très bonne facture. Le sujet choisi, l'extraction des programmes efficaces à partir de preuves au moyen de l'interprétation *Dialectica* de Gödel, est un sujet techniquement difficile qui présente un fort potentiel. L'auteur en a visiblement une parfaite maîtrise et une compréhension profonde. Les résultats présentés sont originaux et significatifs, allant du développement d'une technique nouvelle - l'interprétation *Dialectica* légère - à son application sur des exemples concrets.

L'ensemble des résultats obtenus constituent à l'évidence une très bonne thèse et j'en recommande donc la soutenance.

Paris, le 5 décembre 2006

Michel Parigot

Laboratoire "Preuves, Programmes et Systèmes"

Université Paris 7 - CNRS, UMR 7126

Jean-Pierre Jouannaud
Laboratoire d'Informatique de l'IX

September 29, 2006

Rapport de présentation de la thèse de Mircea Dan Herness

La thèse de Mircea Dan Herness, intitulée "Extraction de programmes efficaces à partir de preuves (non-constructives) par l'interprétation Dialectica (monotone)" s'inscrit dans un courant de recherche très actif concernant l'extraction de programmes à partir de preuves (de logique classique, le cas intuitionniste étant bien maîtrisé), et la complexité du processus d'extraction d'une part et des programmes extraits d'autre part. Le domaine est considéré comme ardu, et l'oeuvre de quelques spécialistes pour la plupart européens. Les résultats nouveaux de la thèse sont de nature essentiellement théorique, mais sont illustrés par quelques exemples non-triviaux. Ils reposent sur une extension de l'interprétation fonctionnelle de Kurt Gödel, comme sous le nom de Dialectica, et de sa variante monotone due à Ulrich Kohlenbach.

La nouvelle technique d'extraction de programmes à partir de preuves est nommée par l'auteur "Dialectica légère" ou "interprétation fonctionnelle légère". Elle a pour caractéristique principale l'élimination, complète dans certains cas, des contractions inutiles apparaissant dans la preuve au cours du processus d'extraction lui-même, plutôt qu'à posteriori. La complexité de l'extraction tout comme celle des programmes extraits peuvent s'en trouver sensiblement réduites. Dans le cas des arithmétiques monotones étudiées par Kohlenbach, l'identification de ces contractions redondantes est assurée par l'ajout des quantificateurs dits "uniformes" ou "sans contenu calculatoire" d'Ulrich Berger. Dans le cadre traité dans la thèse, il faut adapter cet ajout, en particulier en restreignant la règle d'introduction de l'implication. Il s'ensuit que cette nouvelle technique se coule plus facilement dans le moule des preuves pleinement classiques.

Les exemples concrets traités par l'implémentation réalisée sont assez prometteurs dans les cas d'école où ces nouvelles techniques d'extraction s'appliquent réellement. Également encourageante est l'extraction de marges de complexité calculatoire polynomiale par la Dialectica Monotone Légère, ce qui généralise le travail antérieur de Kohlenbach sans toutefois que des exemples adéquats viennent étayer ce gain de généralité.

Enfinement, le chapitre en Annexe présente un travail plus ancien de l'auteur en collaboration avec Ulrich Kohlenbach sur la complexité calculatoire des algorithmes d'extraction eux-mêmes. La faible borne de complexité obtenue (cubique dans le pire cas) s'applique au cas d'une présentation de Dialectica par des systèmes à la Hilbert, mais le résultat peut être facilement adapté, semble-t-il,

Jean-Pierre Jouannaud - Tel: +33 (0)1 69 33 40 70 - jouannaud@lix.polytechnique.fr

aux présentations de type Dédution Naturelle utilisées dans le corps principal de la thèse. La présentation en Dédution Naturelle de l'interprétation fonctionnelle monotone de l'auteur est une adaptation de la présentation due à Joergensen pour la technique d'extraction de Goedel.

Fait à Palaiseau,
Jean-François Jouannaud
Professeur

