Hors-Série N°1 - Mai 2014

FSMP
Fondation Sciences Mathématiques de Paris

MathsInfos

DES PREUVES ET DES PROGRAMMES

Qu'y a-t-il de commun entre les constructions mathématiques et les développements logiciels? Tout d'abord, le fait d'être souvent très complexes. On parle d'architectures logicielles, mais on pourrait aussi parler de l'architecture d'une preuve telle que celle du théorème de Fermat. Dans les deux cas, on mesure aussi les prouesses selon des critères assez similaires, on parle d'élégance pour une belle preuve ou un beau programme. Dans le monde des langages de programmation, on recherche la *portabilité* et la *réutilisation de code*, concepts qui font sens aussi en mathématiques : l'importance d'une théorie augmente considérablement lorsqu'elle est utilisée avec succès dans une tout autre branche, et des noms de mathématiciens sont souvent associés à des lemmes parfois « bêtes » mais terriblement utiles et utilisés à tout bout de champ.

En mathématiques et en informatique il y a une tension, ou plutôt un va-et-vient entre sens d'une part, et langage formel comme support du sens d'autre part (en linguistique, on parle de sémantique et de syntaxe). Un mathématicien communiquera plus sûrement ses idées et résultats lors d'une présentation au tableau qu'à travers ses articles écrits. Un programme informatique est conçu pour répondre à une spécification (penser par exemple à la régulation des trains, qui de préférence ne doivent pas se percuter), mais est exécuté par une machine à la fois parfaitement stupide et totalement obstinée parce qu'obéissant exactement aux règles qu'on lui a demandé d'appliquer.

Dans les deux mondes enfin, on cherche à être rigoureux : pas le droit à l'erreur, une preuve doit être juste, un programme ne doit pas contenir de bug. Seulement voilà, la liste des bugs informatiques est considérable, avec des coûts associés (financiers ou humains) parfois catastrophiques (pensons en particulier aux bugs d'équipements médicaux informatisés). En mathématiques, les erreurs sont pratiquement inévitables, et sont particulièrement gênantes quand elles sont découvertes longtemps après que d'autres mathématiciens ont utilisé les résultats en question.

Il existe donc un besoin de vérification et de correction : pour pouvoir faire confiance à des calculs, et tant qu'à faire à la preuve tout entière, il faut pouvoir les vérifier formellement. C'est là que peuvent intervenir des assistants de preuves (voir ci-contre), qui ont joué un rôle majeur dans la démonstration de certains théorèmes (voir ci-dessous).

Ce sont toutes ces questions passionnantes qui sont au centre du trimestre *Semantics of proofs and certified mathematics*.

Pierre-Louis Curien
Directeur de recherche CNRS (laboratoire PPS et équipe commune Inria π r²)

Les assistants de preuve

Un assistant de preuve est un logiciel (souvent interactif) qui permet de vérifier d'autres logiciels, ou des preuves mathématiques écrites formellement. On peut citer parmi eux les logiciels Coq, développé par des chercheurs de l'Inria et d'autres institutions, et HOL Light, du mathématicien et informaticien John Harrison (Intel). Le trimestre *Semantics of proofs and certified mathematics* (cf. verso) met ces outils à l'honneur, à travers leur utilisation en mathématiques et en informatique, et cherche aussi à mettre en lumière les développements théoriques en logique et en informatique qui ont permis de les concevoir : la théorie des types et la sémantique des langages de programmation, respectivement. Ces développements en retour, ainsi que les assistants de preuve eux-mêmes, sont à leur tour source d'idées nouvelles, comme celles de la théorie homotopique des types, qui suggère de nouvelles manières d'aborder les fondements des mathématiques, en reconnaissant le rôle prépondérant de la notion d'égalité, puis celle d'égalité entre preuves d'égalité, etc. Ils suggèrent également de nouvelles manières d'exercer l'activité de mathématicien : les assistants de preuve seront bientôt, dans de nombreux domaines des mathématiques, un compagnon aussi naturel que leur éditeur de texte favori (La)Tex ! Ceci va de pair avec le développement d'outils permettant de développer des environnements sûrs pour les développeurs et utilisateurs des logiciels les plus divers.

L'équipe Inria π r²

L'équipe π r² se consacre à l'étude des aspects fondamentaux des preuves formelles et des programmes, ainsi qu'au développement de l'assistant de preuve Coq, dans lequel elle est actuellement l'équipe la plus fortement impliquée. Depuis 2012, elle a également étendu son champ d'application à l'étude de l'homotopie de systèmes de réécriture, qui partage des outils fondamentaux avec de récentes avancées en théorie des types et en sémantique.

Dans la presse

Le thème de la preuve informatique a eu les honneurs du journal *Le Monde* (14 avril 2014) avec un portrait de Georges Gonthier réalisé par Philippe Pajot : *Georges Gonthier, « hacker » de théorèmes*.

Ces problèmes certifiés sur ordinateur

Le plus célèbre théorème dont la démonstration a été établie en faisant appel à des calculs sur ordinateur est sans doute le *théorème des quatre couleurs* (qui dit que quatre couleurs suffisent toujours pour colorier une carte sans que deux régions adjacentes aient la même couleur). La *conjecture de Kepler*, qui donne la configuration optimale d'un empilement de sphères, en est aussi un exemple. Le besoin de correction est particulièrement important lorsque les preuves comportent des cas et des sous-cas en nombre considérable, dont la vérification est souvent « laissée au lecteur ». Dans d'autres cas, comme pour la classification des groupes finis, c'est la longueur de la démonstration qui pose question : n'a-t-on rien oublié, un lemme un peu faux entraîne-t-il la chute de l'édifice ? La démonstration du *théorème de l'ordre impair* (théorème de Feit et Thompson) fut elle aussi certifiée (par Georges Gonthier) à l'aide du logiciel Coq. En informatique, le projet *CompCert* marque une étape remarquable dans le développement d'outils pour garantir la sûreté des logiciels : pour la première fois, un compilateur complet d'un langage largement utilisé dans l'industrie (C) a été entièrement certifié, c'est-à-dire vérifié, en Coq.

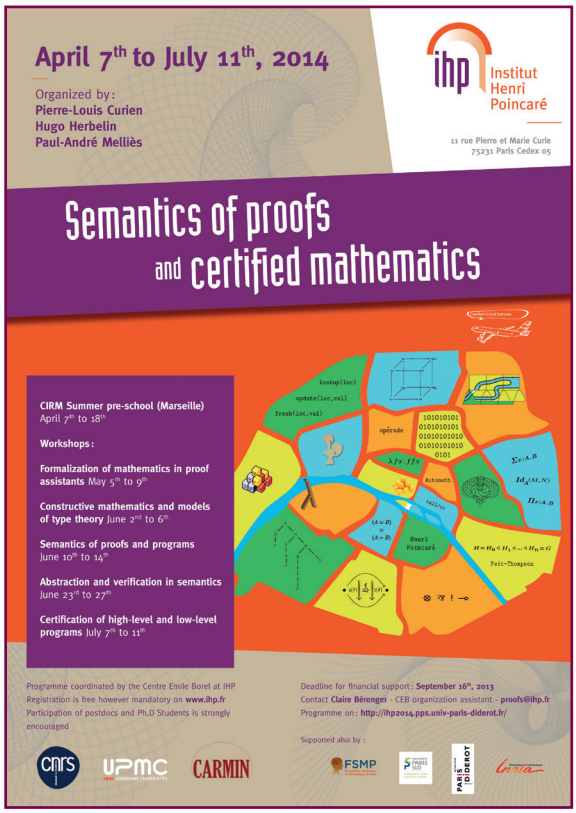
Hors-Série N°1 - Mai 2014

FSMP
Fondation Sciences Mathématiques de Paris

Du 7 avril au 11 juillet 2014 : *Semantics of proofs and certified mathematics*

Le trimestre *Semantics of proofs and certified mathematics*, organisé par Pierre-Louis Curien (PPS), Hugo Herbelin (Inria) et Paul-André Melliès (PPS), se tient à l'Institut Henri Poincaré du 7 avril au 11 juillet 2014, avec le soutien de la FSMP. C'est probablement le premier trimestre IHP dont le thème soit aussi profondément lié à l'informatique. Une après-midi introductive a été proposée le mardi 22 avril, devant un public nombreux, venu écouter les exposés de Georges Gonthier (*Digitizing the Group Theory of the Odd Order Theorem*), Thomas Hales (*Formalizing the proof of the Kepler Conjecture*), Xavier Leroy (*Proof assistants in computer science research*) et Vladimir Voevodsky (*Univalent Foundations - new type-theoretic foundations of mathematic*). La semaine s'est poursuivie, les 23, 24 et 25 avril, par des mini-cours de Gérard Berry (*Constructive semantics, electricity propagation in circuits, 2-adic numbers, and formal verification*) et de Jean-Yves Girard (*Qu'est-ce qu'une réponse ? Qu'est-ce qu'une question ? D'où vient la certitude ?*). Du 28 avril au 2 mai, le cycle d'exposés et de mini-cours a continué avec Per Martin-Löf, Thorsten Altenkirch, Jean-Louis Krivine et François Pottier. L'après-midi du 28 avril était consacré aux méthodes formelles et langages pour le développement de logiciels fiables dans l'industrie, présentés par des docteurs ayant choisi de travailler dans le secteur industriel. Certains de ces exposés et mini-cours ont fait l'objet de captations vidéos qui seront mises en ligne sur le site de l'IHP : **www.ihp.fr**. De nombreux événements liés au trimestre se tiendront également à l'IHP : TYPES, MAP, les journées de la Fédération Mathématique de Paris-Centre, un workshop consacré au thème *Higher Order Computation : Types, Complexity, Applications*, ...

© Institut Henri Poincaré



Les workshops du trimestre

Du 05 au 09 mai :
Formalization of mathematics in proof assistants
Du 2 au 6 juin :
Constructive mathematics and models of type theory
Du 10 au 14 juin :
Semantics of proofs and programs
Du 23 au 27 juin :
Abstraction and verification in semantics
Du 7 au 11 juillet :
Certification of high-level and low-level programs

Bientôt en ligne

Retrouvez prochainement sur le site de la FSMP **www.sciencesmaths-paris.fr** des interviews vidéos liées au thème de la preuve.

Directeur de la publication : Jean Dolbeault
Responsable de la rédaction : Gaël Octavia - Contact : octavia@fsmp.fr
Fondation Sciences Mathématiques de Paris - www.sciencesmaths-paris.fr
IHP, 11 rue Pierre et Marie Curie 75231 Paris Cedex 05
Tél. : +33 (0) 1 44 27 68 03 - Fax : +33 (0) 1 44 27 68 04

Fondateurs
Partenaires scientifiques
LabEx SMP
DIM RDM-ÎdF