Entretien avec Assia Mahboubi

Pouvez-nous présenter votre parcours académique ?

Mon parcours scolaire est à la base un parcours de mathématiques. Après une classe préparatoire, j'ai intégré l'ENS Lyon en mathématiques. Déjà un peu à l'époque je me posais des questions de définition des objets mathématiques. La façon de faire des maths change vraiment du lycée au supérieur et c'est le même seuil quand on passe de la prépa à une école spécialisée. Mais les questions restaient toujours là, même après ce passage. Je me suis intéressée à des cours de logique ou de mathématiques discrètes qui étaient dans le parcours informatique. C'était d'ailleurs encouragé de compléter sa formation dans les cursus d'à côté. Puis via un stage je me suis retrouvé à faire de la formalisation avec Coq que je ne connaissais pas du tout. C'était en master 1. Je me suis rendu compte que c'était vraiment ce qui m'intéressait. J'ai donc fait un M2 cohabité entre Paris 6 et Paris 7 dont le sujet était la théorie de langage de programmation et la logique. J'ai fait ensuite une thèse à Nice à Sofia Antipolis. Je n'ai pas du tout la formation de quelqu'un qui a fait un cursus d'informatique mais par contre j'avais fait cette forme de logique qui était enseignée en informatique (de manière arbitraire). Georges Gonthier avait fini son travail sur le 4CT quand j'ai commencé ma thèse mais il avait besoin de gens pour travailler sur le théorème de Feit Thompson. J'ai eu la chance d'être là au tout début.

Avez-vous eu des oppositions sur la validité de la preuve de Feit-Thompson ?

Pas du tout car l'exemple avait été choisi justement pour ça. **Il y a déjà une controverse sur la preuve du 4CT enfin il y a quand même deux aspects : il y a la découverte de la preuve et sa vérification** et la controverse qui reste actuelle c'est plus la controverse des preuves où il y a encore des parties de calcul qui sont surhumaines et qu'on ne pourrait pas faire à la main. **Je pense le fait de vérifier avec une machine n'est pas trop controversé**. **Le fait que la machine soit plus stupide et donc plus efficace pour la vérification qu'un être humain c'est une idée qui est assez naturelle et qui passe plutôt bien**. Les retours qu'avait eu Georges Gonthier à l'époque sont plus « Ce ne sont pas des vraies maths » pour le dire très grossièrement. C'était très bien mais c'était plus de la vérification de preuve qu'un réel ajout aux mathématiques ce qui n'est pas très honnête car il n'y a quand même plus que des programmes dans cette preuve mais disons que ça n'impressionnait pas forcément des gens d'autres communautés de mathématiques que la combinatoire qui ne pouvaient pas se convaincre sur la base de ce succès que la technologie des bibliothèques digitales de mathématiques vérifiées par assistant de preuve étaient suffisamment mûres pour pouvoir devenir un outil que eux puissent s'approprier. Et donc ce que **George a fait, c'est trouver un exemple qui fasse un peu plus "coup d'éclat" pour les mathématiques**, si tenté qu'il y a eu une notion de mathématiques générales. Un exemple qui soit plus notoirement un résultat de mathématiques récent et qui ait un petit parfum de souffre, de controversé. Je ne sais pas si on vous a déjà mentionné ça mais dans plusieurs disciplines de mathématiques vraiment « pures », c'est à dire qui n'implique pas forcément des calculs à vérifier, le problème c'est qu'il n'y a plus suffisamment de personnes compétentes pour référer les papiers. En fait, de façon

relativement surprenante la façon dont une conjecture devient un théorème est un processus social. Les gens font des exposés, il confronte leurs démonstrations en public, après ils rédigent un article, puis ils le mettent sur un serveur de pré-print pour voir les réactions et/ou ils le soumettent à un journal. Là ça va être relu par des référés anonyme mais en fait l'anonymat est un peu une blague et de toute façon y'a forcément un acte de foi à un moment car personne ne maîtrise la chaîne de résultats de bout en bout qui est convoquée dans un article dans une certaine discipline de mathématiques. Aussi, il y a très peu de gens qui sont en mesure de faire une relecture experte de certain sujet puis il y a la réputation de l'auteur qui entre en compte. Enfin, il y a tout un tas de facteurs qui font qu'il y a plein de faux papiers. Il y a des problèmes difficiles qui ont vu des preuves fausses publiées dans les meilleurs journaux. Et il y a des gens que ça émeut et qui considèrent qu'il faut faire quelque chose. Tout ça pour dire qu'on utilise des ordinateurs pour trouver une solution à cette situation qui n'est pas satisfaisante. Ce n'est pas ça tellement la controverse. Donc pour revenir à la réception de Feit-Thompson, c'est un morceau d'un résultat beaucoup plus gros qui est la classification des groupes finis simples qui sent le souffre en fait, qui fait partie de ces résultats imposant avec une preuve écrite par beaucoup d'auteurs, pas dans un seul volume avec plusieurs papiers qu'il faut mettre bout à bout, où il y a déjà eu des fausses annonces disant que c'était fini. **Donc le fait que quelqu'un s'attaque à la vérification de ce truc là c'était plutôt bien reçu et c'est pour ça que le choix avait été fait.** Donc c'était favorable mais ça avait été décidé en avance pour que si jamais le succès était au bout de l'aventure ça soit convaincant. Convaincant pour un résultat, j'insiste encore une fois, qui est une preuve très importante mais sans calcul. Ce n'est pas le fait qu'il y ait des calculs qui pose un problème sur la nature convaincante ou non de la preuve.

Vous parliez du fait que la preuve implique un phénomène social, il y a une relecture de papiers, enfin comme dans toutes les sciences d'ailleurs. Mais est-ce que les preuves informatiques ne posent pas un problème dans le sens où tout n'est pas vérifiable non plus humainement au niveau de la réalisation de la preuve ? Pour pouvoir ensuite la présenter en papier ce serait plus difficile que si ça avait été fait entièrement à la main parce que ce n'est pas dans un langage naturel.

Si vous êtes en train de dire est ce qu'un jour on se passera de papier, ce n'est pas ça que je dis pour l'instant.

Plutôt, est-ce que le langage des preuves informatiques ne rend pas la chose plus difficile pour être présentée aux pairs ?

C'est vraiment une très bonne question que vous posez là. J'imagine que maintenant vous êtes familiers avec le fonctionnement d'un assistant de preuve. **C'est un logiciel avec deux composants, le « gendarme » qui vérifie la preuve et le « gentil » qui aide l'utilisateur à formaliser c'est à dire à représenter ses énoncés et théorèmes.** Le code est idéalement séparé et il y a un jeu interactif entre la vérification et le développement. Une fois que la preuve est complètement écrite et qu'elle est validée par ordinateur c'est quand même très fiable, ça il n'y a pas de problème. Par contre vous avez totalement raison, **il y a une chose que l'assistant de preuve ne vérifie pas c'est que l'on a bien formalisé ce qu'on avait l'intention de formaliser**. Vous avez raison ici, là il y a un **œil humain irremplaçable qui doit se convaincre**

que ce qui a été écrit dans le langage formel de l'assistant de preuve correspond bien à l'intuition et à la définition communément admise par la communauté mathématique qui a travaillé pendant longtemps sur son tableau et sur son papier. Ici **l'humain est irremplaçable et il n'y aura jamais par essence possibilité d'automatiser cette chose-là**. C'est une question de langage, il faut être d'accord que l'on parle de la même chose. Ça arrive régulièrement dans les articles de preuve formelle que quelqu'un prétende avoir fait une théorie formalisée de je ne sais quel objet et en fait le rapporteur du papier de preuve formelle dise non, ce que je trouve dans vos fichiers c'est pas la notion mathématique usuelle et donc vous avez fait une théorie du vide. L'humain est irremplaçable mais au moins sur le papier on peut laisser un flou artistique sur ce qu'on appelle un chat alors qu'en fait on parle d'un violon et cela peut être une source de problème en fait. Le jour où quelqu'un gratte et se rend compte qu'on a prétendu qu'on a mis deux pièces de puzzle ensemble mais en fait elles ne s'emboîtent pas parce que si on gratte on n'a pas exactement le même vocabulaire pour que ça s'emboîte bien. Alors que moi sur machine c'est précis et donc on ne pourra pas mettre deux pièces du puzzle ensemble si elles parlent pas exactement de la même chose.

Il n'y a pas tellement de débat sur l'assistant de preuve. Il y a plein de sujet de recherche pour le rendre plus utilisable et plus ergonomique. On n'est probablement pas au stade où il peut être utilisé par des gens qui ne sont pas experts. La question reste celle de l'utilisateur, comment a-t-il posé ses définitions ? Le problème c'est que lorsqu'on lit un papier de mathématiques, même des papiers de cours ou des bouquins, sans s'en rendre compte on lit des choses qui avec très peu de symboles contiennent beaucoup d'informations et beaucoup d'informations implicites en fait. C'est ce qu'on apprend dans les premières années de mathématiques : tous les appareils de notation, de convention qui sont propres à chacune des sous-disciplines de mathématiques car il y a des usages répétés d'arguments similaires qu'on va condenser dans une notation bien appropriée, dans un vocabulaire qui pourra subtilement avoir un sens différent selon le contexte et qui justement couvrira tous les cas d'usage sans qu'il y ait besoin de recourir à des astuces absconses, brutes et qui obscurcissent le discours. Sur le papier aussi il y a des choses un peu floues sauf que normalement les gens reposent sur des notions de culture partagée de mathématiques et il faut être sûr que ces choses-là ont bien été transcrites dans l'assistant de preuve également, ce qui n'est pas évident, c'est aussi un des sujets de recherche. Il faut transposer ces notions de notation. Ça pose des problèmes d'informatique d'arriver à rendre ça fiable et programmable.

Question du langage et la thèse de Zimmerman sur l'interface avec Coq : partir de la preuve en Coq et faire un fichier en Latec et partir du fichier en Latec et faire une preuve Coq avec.

Ça c'est très important. Pointé et faire un pont entre ce qu'il y a écrit sur le papier. C'est vrai que même si on connaît Coq c'est très difficile de lire une preuve en Coq. On est au début, il y a tout un travail d'interface de recherche, de chose comme ça. On fait des choses incroyables avec des moteurs de recherche web et l'interface et les outils de recherche qu'on a pour naviguer dans ces développements formels c'est la préhistoire. En fait c'est parce que ce n'est pas les mêmes sujets de recherche, c'est un peu compliqué d'avoir des gens qui s'intéressent à ça avant d'avoir des développements substantiels qui aient été fait pour montrer que vraiment ça vaut le coup.

C'est vrai qu'il y a toujours un souci, c'est ce que nous expliquait Théo Zimmermann : à chaque fois qu'on rajoute des couches pour rendre ça plus intuitif, on multiplie les sources d'erreurs car le noyau va toujours donner de bons résultats mais les intermédiaires font que l'on pouvait prouver quelque chose qui fait que ce n'est pas ce qu'on voulait faire.

Certaines personnes lors des conférences de Gonthier posaient des questions sur la présence de bugs. Avez-vous déjà eu des bugs ?

Bien sûr qu'il y a des bugs dans Coq, évidemment. C'est un peu provocateur mais on s'en fiche en fait. Enfin, pour qu'il y ait un problème il faudrait qu'il y ait non seulement un bug et que ce bug soit exploité de sorte que l'on prouve quelque chose d'invalide, ce qui est très peu probable dans ce cadre d'application. Nous on est de bonne foi. On est convaincu que la preuve qu'on essaye de vérifier marche et on essaye de la faire marcher. C'est plutôt dans l'autre sens souvent qu'on tape dans les bugs. C'est à dire, on sait qu'il y a un truc qui marche et y'a un bug qui fait qu'il ne veut pas l'avaler. Ça arrive régulièrement. **Mais par contre le contraire c'est à dire qu'on ait réussi à prouver quelque chose de faux grâce à un bug, je ne dis pas que ça arrive pas mais bon**… Coq c'est un assistant de preuve qui est très généraliste et auquel on recourt dans une grande variété d'utilisation. Il y a des gens pour lesquels ça pourrait être un problème si on se met à garantir des propriétés de sécurité, de programmes critiques avec Coq, possiblement attaqués par des gens malveillants. Je peux imaginer des contextes dans lesquels c'est grave qu'il y ait un bug et que ce soit important qu'il y ait plusieurs vérificateurs qui puissent être appliqués pour augmenter la confiance. Mais dans ce contexte mathématique dont on est en train de parler, je ne pense pas. On a des ordres de grandeur plus confiants qu'avec n'importe quelles relectures humaines, c'est clair même si la question doit être posée.

Au début de l'entretien, vous avez dit que les preuves par informatiques ne posaient pas problème aux mathématiciens mais plus après aux sociologues et philosophes. Partagez-vous ce point de vue ?

J'ai peut-être répondu à côté de vos premières questions car j'ai eu l'impression que vous parliez de la place de l'ordinateur dans les mathématiques. Cette place apparaît à plusieurs endroits en fait. C'est clair qu'à partir des années 60-70, les gens s'aperçoivent qu'ils peuvent confier à l'ordinateur des tâches mécaniques routinières comme des calculs et ça transforme les mathématiques complètement mais ça les transforme à plusieurs titres :

- Le fait qu'on puisse "boucher" des preuves qui auparavant n'étaient pas atteignables car la force de calcul nécessaire était trop grosse.
- Il y a des formes de mathématiques qui sont suscitées par l'ordinateur : les questions d'algorithmique qui sont vraiment très mathématiques par moment. Rendre les algorithmes plus efficaces c'est un problème mathématique qui avait moins d'importance tant qu'on n'avait pas accès à des machines de façon standard comme maintenant.

· Il y a le fait d'utiliser des mathématiques pour la tâche mathématique particulière qui était de vérifier des preuves.

Ça dépend de quelle chose on parle en fait. **Que l'algorithmique soit des mathématiques, je ne suis pas sûr que tout le monde soit d'accord**. Si vous interrogez un géomètre algébriste ou un probabiliste je ne suis pas sûre. Que l'on vérifie des preuves par informatique il n'y a pas trop de controverse sur la réponse que donne l'ordinateur. Maintenant il y a quelque chose qui est un peu au milieu qui est « Est-ce que je fais une preuve quand j'utilise un ordinateur pour faire des calculs ? » et là je pense que les réponses ne sont pas très tranchées.

Il y a des gens qui explorent avec un ordinateur de façon très usuelle dans leur pratique des mathématiques et qui après par contre enlèvent l'échafaudage quand ils écrivent le papier. En vrai, ils ont utilisé des systèmes de calcul pour avoir des idées de la conjecture qu'il fallait formuler ou repérer des motifs qui leur suggèrent un résultat mais après ils abandonnent l'ordinateur et font une démonstration qui n'a pas besoin de l'ordinateur.

Il y a des gens qui acceptent d'avoir des théorèmes prouvés avec un programme et juste un programme. Vous avez parlé des 4 couleurs mais il y en a plein d'autres en fait. Si vous regardez des questions de système dynamique, il y a un résultat dont vous avez peut-être entendu parler qui est l'étrangeté de l'attracteur de Lorentz. Ça c'est un autre exemple beaucoup plus récent. Il y a quelqu'un qui s'appelle (Smeil) qui a proposé une liste de problème fameux et ouvert. Le fait que l'attracteur de Lorentz ait un caractère étrange était l'un d'eux. C'est un problème de système dynamique. On a un paquet d'équations qui régissent un système qui évolue dans le temps et en fait décrire la trajectoire que ce système parcourt dans l'espace par exemple ce n'est pas possible, on ne peut pas trouver de formule. C'est aussi parfois quand le système est trop volatile, qu'il devient difficile de dégager son comportement quantitatif. C'est ça être étrange. La question était est-ce-que ce système décrit par ces équations a un caractère étrange ? Et c'est très difficile car ça implique typiquement des calculs qui entraînent des erreurs d'arrondi. C'est difficile à attaquer mais il y a quelqu'un qui l'a montré dans les années... Je vais dire une bêtise mais la personne qui a résolu ce problème s'appelle W.Tucker et je pense que c'est un résultat du début des années 1990. Et là le statut de ces démonstrations n'est pas clair. **Je pense qu'il y a encore des gens qui considèrent que si l'on sait démontrer quelque chose qu'avec des gros calculs, à la main ou avec un ordinateur, c'est qu'on a raté un truc, qu'il y a encore quelque chose à creuser. C'est pour ça que les gens vont chercher plus avant même s'ils considèrent que le résultat est valable.**

Justement avec cette question on rejoint un peu la question de l'élégance. Pour vous qu'est-ce que l'élégance dans une preuve mathématique ?

C'est une question éminemment subjective. C'est le même problème que pour la mode. Si vous demandez à quelqu'un ce que c'est qu'être élégant chacun va venir avec sa définition de la classe. **Il me semble qu'il y ait un critère esthétique. Et je pense que peu de gens trouvent esthétique une longue série de calculs qui n'a pas de structure**. Il y a des outils de preuve automatique qui s'appellent les SAT Solver ou les SLT Solver qui sont des outils qui résolvent des outils très simple. Ça vous dit quelque chose la logique propositionnelle, les booléens ? Vous écrivez une équation X ou Y = ? et vous cherchez des solutions pour X et Y. C'est facile

vous écrivez X = ? et Y = n'importe quoi ou Y = ? et X = n'importe quoi. Vous écrivez des grosses formules avec des ET des OU des NON et vous cherchez une solution dans 1/0. C'est un problème débile mais très difficile. On ne sait pas trouver des algorithmes. Il y a de fortes chances pour qu'un algorithme très efficace n'existe pas. Par contre vérifier qu'une solution est bonne c'est très facile il suffit de calculer. Il y a des outils de preuve automatiques spécialisés qui s'appellent les SAT solver dont le boulot c'est de faire ça, c'est de trouver des solutions avec des heuristiques, des choses comme ça. On peut encoder dans ce truc là plein de problèmes exprimés dans un langage potentiellement beaucoup plus expressif. Donc on a un problème qu'on comprend très bien et puis on va l'encoder dans ce langage très pauvre. À la fin si je vous montre l'encodage sans le problème dont vous êtes parti vous êtes incapables de reconnaître le problème. Par contre du coup vous pouvez le donner à manger à ces outils de preuve automatique qui vont potentiellement vous cracher une solution. Si vous lisez la solution du problème encodé vous avez une réponse à votre problème initial mais je pense que personne ne trouvera ça élégant. Donc je ne saurais pas vous définir l'élégance mais je peux vous donner des exemples de ce qui n'est pas élégant. Là ça va donner un exemple d'exploration typiquement, « ici la conjecture à l'air valable » maintenant on ne va pas s'arrêter là, on va essayer de comprendre ce qui dans la structure des objets mathématiques qui interviennent dans l'énoncé explique le fait que cette propriété soit valable. **Il me semble que l'élégance c'est quand on a compris quelque chose de plus sur les objets qui sont en jeux**.

D'ailleurs à ce sujet nous avons fait un entretien avec un philosophe des sciences qui nous disait qu'après qu'une preuve ait été prouvée un second travail d'amélioration de la preuve commençait. La meilleure preuve est celle qui donne le plus de compréhension de l'objet.

Parler de la meilleure preuve me gêne un peu car il peut y avoir plusieurs critères. Ça c'est du vécu, ça m'est arrivé à l'oral de l'agrégation. Lors de l'agrégation, il faut faire une leçon, proposer un plan et faire un zoom sur une ou plusieurs questions et le jury choisi la question. Donc le jury était en train de rédiger le zoom au tableau et je me suis vu reprocher le fait que j'utilisais une méthode probabiliste pour démontrer un résultat alors que ce résultat n'a pas besoin de la théorie des probabilités pour être justifié. J'avais une raison personnelle de trouver ça élégant d'invoquer un outil externe au problème et le jury estimait que ce n'était pas approprié car rien qu'en exploitant la structure des objets présents dans le problème on pouvait arriver à comprendre cette propriété là et on n'avait pas besoin d'aller chercher plus loin. Mais les deux se défendent dans ce cas précis. Ils avaient certainement raison que pédagogiquement c'était discutable d'aller chercher cette autre théorie si les autres étudiants devaient comprendre que ça n'avait rien à voir avec les probabilités. Et pourtant ça dit quelque chose aussi sur le fait qu'en probabilité cette nature d'argument ça explique telle nature de phénomène comme illustré dans cette preuve. On peut se perdre dans ce genre de recherche de l'élégance.

Pourquoi selon vous il y a toujours des gens qui essayent de prouver le 4CT avec un papier et un crayon ?

Encore une fois **il y a deux aspects. La lecture d'une preuve qui existe et la découverte et ce n'est pas du tout la même chose**. **Les gens qui ont choisi de faire de la recherche en mathématiques, c'est parce qu'ils aiment la partie créative** et ce n'est pas parce qu'ils aiment bien relire des papiers en général. C'est vrai que ça fait partie du boulot aussi et c'est vrai qu'on peut avoir de grand plaisir en lisant des bouquins qui racontent une théorie mathématique qu'on ne connaît pas. C'est souvent comme ça qu'on est arrivé à aimer les mathématiques et qu'on continue après. **Par contre, si on passe le cap d'essayer de faire de la recherche c'est parce qu'on aime bien se poser des questions et essayer de jouer avec les constructions mathématiques pour faire avancer les choses et là, à mon avis, tous les outils sont permis.** Vous allez avoir plein de profils de gens et peut être ça dépend des moments aussi. Personnellement, je fais un peu de mathématiques aussi au sens d'essayer de répondre à des questions pour lesquelles on n'a pas de réponse *a priori*. Je pense que ça dépend des questions. **Il y a des questions pour lesquelles je vais passer des heures devant un tableau et c'est le meilleur outil et il y a des moments où l'exploration informatique a du sens.** Pour moi, il n'y a pas de règle mais je n'imagine pas faire uniquement des mathématiques par ordinateur. Il y a une phase de réflexion sur un support où on écrit à la main, où on fait des dessins. Enfin ça sera peut-être une tablette j'en sait rien mais je veux dire ce n'est pas un truc de programmation.

Sachant qu'on ne peut prévoir les développements à venir au niveau des intelligences artificielles (IA), c'est un sujet que nous avons abordé avec Théo Zimmermann, est-ce qu'on pourrait voir un jour des IA, ou des algorithmes qui pourraient créer des preuves, c'est-à-dire pourvus du côté créatif lui-même, et qu'on pourrait croire sur parole ou bien est-ce qu'il sera toujours nécessaire de passer quand même par un processus de vérification a posteriori ?
Cela reste tout de même de la science-fiction.

Oui c'est vraiment de la projection mais est-ce que de telles preuves pourront-elles être acceptées selon vous ou est ce qu'on les prendra comme des preuves humaines qu'il faudra vérifier ?

Je ne vois pas pourquoi on leur ferait plus confiance qu'à un être humain. Je ne vois pas non plus pourquoi il n'y aurait pas de nécessité de relecture de ces mêmes preuves. Après pourquoi pas ? Il existe déjà des ordinateurs qui découvrent des preuves, et ce sans IA, c'est juste que l'on imagine un autre passage à l'échelle ou une autre nature de découvertes. Cela me paraît sans doute concevable mais au-delà, je ne sais pas… Ça me parait un peu trop être de la science-fiction. **Pour l'instant, je ne crois pas que la créativité mathématique sera supplantée, en tout cas, s'il pourra exister une autre forme de créativité (des ordinateurs), mais elle ne la remplacera pas et fera des choses différentes**.

En fait, au moment de la preuve de 1976, il y a eu des craintes parce que l'informatique était assez méconnue. Maintenant on cerne mieux ses capacités réelles, ainsi ces craintes se sont estompées. Pour Théo Zimmermann, ce genre de preuves pourraient

être une réalité car il existera des IA ou des programmes qui créent des preuves mais il faudra leur appliquer de la vérification basique de preuves avec des logiciels comme Coq ou autre au même titre qu'une preuve humaine d'ailleurs.

C'est vrai qu'il existera toujours des personnes qui essaieront de comprendre mieux qu'elles sont ces preuves, ce qu'elles suggèrent. En fait, je ne pense pas que le travail de l'intelligence artificielle soit de bâtir des théories et des abstractions. Explorer et donner des chemins inattendus sans doute … Mais telle que je le conçois et peut être que je peux me tromper, j'imagine que le rôle des IA sera plutôt donner des indications de "partie immergée des Icebergs" mais pour comprendre le tout, la théorie abstraite, qui justifient ces découvertes potentiellement non-humaines, je ne le vois pas pour tout de suite.

C'est vrai qu'il y a une distinction entre faire une preuve et la comprendre pour appréhender la logique qui se cache derrière.

Et cela n'est d'ailleurs pas propre aux preuves informatiques, c'est déjà un phénomène observé. En effet, il y a des domaines scientifiques, où les gens ont leur "boîte à outil rouge" et leur collègues ont la " boîte à outil bleue" et quand les "rouges" essaient de démontrer un théorème, les "bleus" essaient aussi sans utiliser les outils "rouges" juste pour voir si cela relève de leur spectre d'outil ou non : il n'y absolument rien de calculatoire là-dedans.

Donc cela dépend des axiomes que l'on choisit ?

En fait, c'est moins une question d'axiomes. De fait, est ce que vous avez besoin de pures mécaniques ou absolument d'électronique pour résoudre un problème ? Je ne dis pas cela dans l'optique d'opposer modernité contre anciens temps (image de la mécanique contre l'électronique), mon propos n'est pas celui-là. En fait, il y a par exemple des méthodes où l'on a recours qu'à de la combinatoire : j'ai un objet et des axiomes et des opérations commutatives, associatives et l'objectif est simplement en comptant mes objets et en comparant des comptages, d'arriver à trouver des propriétés sur ces objets. Puis on change de monde, et là ces objets peuvent être utilisés dans des matrices, où là on a une autre nature d'outils qui est l'algèbre linéaire. Et dans ce monde, on des notions nouvelles comme les fonctions : c'est un univers complètement différent. Et potentiellement cela me donne plus d'outils : Il y a des choses que j'ai dans l'algèbre linéaire que ne voyais pas dans mon monde combinatoire et il y a aussi des choses que j'ai perdu en passant dans ce monde d'algèbre linéaire. Cet exemple est vraiment un cas de ce que l'on peut trouver en théorie des groupes finis. Et donc la preuve de Feit-Thompson c'est aussi une étape dans les groupes finis car c'était le premier résultat d'envergure qui demandait la combinaison de ces deux "boîtes à outils rouges et bleue". Et on arrivait vraiment à avancer en restant dans une seule "boîte à outil" monochrome. C'est un exemple de démarcation où les gens cherchent à comprendre s'il est nécessaire de rester en combinatoire ou il est obligatoire de passer en algèbre linéaire, et si l'on arrive toujours à relire même en étant dans le monde de l'algèbre linéaire ce qu'on avait avant. Il s'agit vraiment d'une question mathématique d'intérêt. Ce n'est pas simplement une "guéguerre" entre "*ce que je sais faire*" et "*ce que tu sais faire*".

De cette façon, est-ce que les mathématiques seraient entrées dans quelque chose de relatif, où l'on peut avoir des choses vraies selon les outils qu'on utilise ?

Tout le monde est d'accord là-dessus. Il y a un intérêt scientifique de savoir "est-ce que c'est vrai ?" profondément parce qu'on est capable de plonger nos objets dans un autre monde ou est-ce qu'on savait y lire des propriétés axiomatiques. C'est une nature de question qui préexiste d'ailleurs à l'informatique.

Est-ce que la démarche de disjonction de cas qu'emploie Gonthier dans la preuve de 2004 du 4CT est la même que celle qui est utilisé pour le prouver le théorème de Feit-Thompson ? Est-ce que vous pourriez nous expliquer les différences qu'il existe entre la preuve de Gonthier du théorème Feit-Thompson et celle du 4CT ?

En fait il n'y a pas du tout de disjonction de cas et pas de calcul à proprement parler. C'est vraiment une accumulation de livres.

Comment concrètement avez-vous pu procéder alors ?

Il ne faut pas voir cela comme un "superfax" où l'on passe les pages et elles sont directement formalisées. Il faut réussir à transcrire dans la logique les définitions des objets qui sont employées dans les livres. **Le plus dur, ce ne sont pas les théorèmes complexes mais plutôt la définition des objets les plus basiques**, et qu'on utilise dans beaucoup de contextes différents. **Il faut donc les formaliser de telle sorte qu'ils remplissent toutes les fonctions qu'on leur demander.** On est ainsi parti avec les entiers naturels, les listes et ça nous a occupé plusieurs mois pour les entiers mais aussi les nombres premiers, les coefficients binomiaux, c'est-à-dire des choses qu'on voit au lycée ! Et ces définitions doivent être rigoureuses car les objets sont rapidement protéiformes et si on les formalise précisément pour les besoins d'un usage particulier, on va probablement se "tirer une balle dans le pied" le jour où on voudra les voir d'une autre façon.

Il faut donc réfléchir en amont ?
Oui, il faut faire sans cesse des aller-retours et revenir car on ne trouve pas la solution la plus adapter du premier coup.

Ceci est donc en lien avec la théorie de types ?
Oui, complètement.

Car on a vu avec coq, il est nécessaire de définir tous les objets car par exemple celui-ci ne connaît pas la notion d'entier naturel, qui n'est pas a priori défini dans le logiciel. Et ce qui permet des logiques différentes au sein de Coq : on peut avoir des disjonctions de cas comme la preuve de 1976, mais de manière plus formelle, ou cela peut quelque chose de complètement différent comme la simple formalisation d'objet.

En effet, **Coq a cette particularité que l'on peut coder dans la logique**. On peut écrire des fonctions comme vous l'avez indiqué pour faire des calculs aussi garantis dans leur correction que la suite de déduction qui compose une preuve. **C'est quelque chose d'assez spécifique à cette assistant de preuve dans la zoologie des assistants de preuves du marché**. Ce n'est d'ailleurs pas ce qui est utilisé dans la preuve de Feit-Thompson, soit le fait de faire de gros calculs. En revanche, le fait de pouvoir faire ces petits calculs facilite l'automatisation d'une partie de la preuve en séparant certaines étapes trop "bureaucratiques" grâce au calcul. En fait, le gros sujet en mathématiques lié à l'utilisation d'assistant de preuve, c'est le niveau de détail qui apparaît et qui est implicite sur la page. Il faut donc arriver à avoir le moins de "bruits" possible dans la formalisation malgré le fait que l'on parle dans une langue qui est d'un niveau très bas. Et sans rentrer dans les détails, la même notion de calcul qui avait permis de faire la preuve du 4CT avec Coq c'est aussi celle qui de plus petite envergure et qui permet de coder dans le calcul ses étapes de "bureaucratie". Ce trait sous-jacent de la logique de Coq a été utilisé de façons multiples pour ces deux succès.

Oui et la nature de la preuve est donc différente ?

En effet, il y a un cas où l'on doit explorer plein de choses et va concevoir un programme pour cela, et un autre cas où il faut empiler des théories et trouver des moyens pour qu'elles s'empilent bien.

Après le 4CT et Feit-Thompson, est ce que vous voyez des théorèmes qui pourraient être symboliques à prouver de manière informatique et qui pourraient aider à une meilleure acceptation des preuves informatisées ou du moins à une plus grande utilisation de celles-ci ?

Je n'en ai aucune idée ...

Par exemple, un collègue de Zimmermann, essaie de formaliser sur Coq le théorème de Banach-Tarski. Mais cela reste tout de même assez difficile.

Oui tout à fait, je pense que cela est possible mais cela ne sera néanmoins pas un "coup de tonnerre" qui convaincra plus de gens. Même si cela reste un très bon travail.

Vous avez raison, mais comme vous l'avez indiqué nous ne sommes encore qu'au balbutiement, les outils sont actuellement très peu développés. Ainsi une telle démarche celle que j'ai évoqué, pourrait permettre de généraliser l'utilisation d'assistant de preuves ?

Cela dépend de la branche des mathématiques à laquelle on s'intéresse. En effet, vous avez évoqué des individus comme Voevodsky, mais au sein d'une telle branche des mathématiques (homotopie) l'usage des assistants de preuves est assez répandu. Et de fait l'usage s'est rapidement généralisé au sein d'une communauté très petite.
Ensuite**, j'ai tout de même l'impression que l'on ait besoin de nouvel exploit de démonstration pour que soit généralisé l'utilisation des assistants de preuves**. Je crois que ce qui fera que ce soient plus utilisés maintenant : c'est vraiment résoudre ces problèmes d'interface, d'utilisabilité, de prise en main. Pour l'instant, c'est très difficile d'utiliser ces systèmes si l'on pas de bagages en théorie des types, une familiarité avec la programmation fonctionnelle, c'est-à-dire des choses qui sont très spécifique à des cursus purement informatiques. Ce n'est pas clair que cela soit nécessaire mais dans l'état actuel des outils et de l'environnement de travail qu'ils proposent c'est difficile de comprendre ce qui se passe et surtout d'appréhender les difficultés que l'on peut rencontrer si on a pas un minimum d'image mentale de ce qui "se passe sous le capot".
Et enfin si vous prenez un système de calcul formel comme Mathematica, Maple : ce sont des gens qui ont pensé très fort l'utilisabilité. En effet, de tels logiciels peuvent être manipulé par des étudiants en première année de math sans problème, et ce n'est pas le cas de Coq. Il y a des personnes qui ont fait l'expérience (de Coq) mais cela reste cantonnés à des cursus purement informatiques. Et je crois que cela qui sera convaincant : des gens qui ne sont pas experts en preuve formelle, parviennent à formaliser peut-être pas de grands théorèmes mais des problèmes relatifs à leur domaines, sans qu'ils aient passé deux ans à se former. Et aujourd'hui je ne connais pas vraiment d'exemple d'une telle situation.

C'est donc rendre plus accessible pour que chacun puisse l'utiliser à son échelle ?

Oui et aussi tous les exemples que vous avez cités, ce sont toutes des personnes qui viennent du domaine des preuves formelles peut-être à l'exception de **Flyspeck et de Thomas Hales** pour la conjecture de Kepler mais ce sont des individus qui ont investis un temps phénoménal et ce n'est pas le vrai travail d'un mathématicien. Je ne pense pas qu'on puisse convaincre les mathématiciens de se former pendant cinq pour faire des preuves assistées par ordinateurs, alors qu'ils n'ont pas besoin de se former cinq ans pour pouvoir écrire leurs documents en Latec, même s'il y a un peu d'investissement à avoir. **Il faudrait que l'on puisse rendre ses outils utilisables après un temps de formation comparable à celui que l'on consacre au fait de se former à un traitement de texte scientifique moderne et actuellement on en est pas là** ! C'est cela qu'il faudra pour qu'il y ait un effet de "seuil" dans la confiance et l'utilisabilité. Maintenant, il y a de grandes figures de mathématicien comme Voevodsky, qui ne sont pas controversées, qui sont clairement reconnu comme de grands mathématiciens, qui disent que c'est possible, que c'est intéressant et que l'on peut faire des choses. C'est plus ça le débat je pense. Et ce qui est plus problématique c'est que les gens téléchargent et essayent de jouer et c'est très dur et ce n'est pas leurs fautes mais c'est celle des systèmes.

Pensez-vous que le théorème que la controverse du 4CT a été largement surévaluée ?

Non, je ne suis pas d'accord, étant dans le côté scientifique, ça occupe beaucoup. J'ai reçu beaucoup de mails de chercheurs qui travaillent dans des laboratoires de mathématiques pour mieux comprendre justement quand la preuve de Feit-Thompson a été publiée et cela reste peu clair du tout pour les gens. En réalité, je pense que c'est le bon moment pour traiter de ces sujets actuels, alors que peut être que dans dix ans …