# La bifurcation de Vladimir Voevodsky. De la théorie de l'homotopie à la théorie des types

Propos recueillis par Gaël Octavia[1]

*Le mathématicien Vladimir Voevodsky nous raconte ici comment il a fait le choix de quitter l'univers des mathématiques pures, qui l'avaient pourtant couronné de succès et lui avaient valu de remporter la médaille Fields en 2002, et d'embarquer pour de tout autres aventures : la logique et les fondements univalents, l'informatique fondamentale et les assistants de preuve. Cet entretien est disponible sous forme filmée à l'adresse suivante :*
*http://www.icm2014seoul-blog.com/videos-en-preambule.html*

Bonjour, je suis Vladimir Voevodsky. Je suis actuellement professeur à l'Institute for Advanced Study à Princeton dans le New Jersey. Je suis en poste là-bas depuis 2002. Pendant la première partie de ma carrière, j'ai surtout fait de la géométrie algébrique. J'ai travaillé sur l'application de diverses méthodes issues de la théorie de l'homotopie à des problèmes de géométrie algébrique. J'ai toujours été fasciné par la puissance de cet outil, à savoir la théorie de l'homotopie. J'ai presque envie de dire que c'est la nouvelle arithmétique. C'est une théorie qui peut être utilisée dans un large spectre de domaines mathématiques et qui peut être un outil de calcul très puissant. J'ai donc appliqué cette théorie à des questions complexes d'algèbre et de géométrie algébrique, en particulier à la *conjecture de Milnor* et à la *conjecture de Bloch-Kato* ; ce sont des conjectures en algèbre pure mais les méthodes utilisées pour les démontrer appartiennent à la géométrie algébrique, avec des intuitions venant de la théorie de l'homotopie. Je trouve que c'est vraiment beau.

*Comment vous êtes-vous intéressé à la théorie des motifs ?*

À l'époque où j'ai commencé à faire des mathématiques de manière professionnelle, disons entre 1987 et 2002, date à laquelle j'ai obtenu la médaille Fields, j'ai construit ma carrière en mathématiques, et à cette époque, cette idée de motifs, introduite par Grothendieck, était un sujet très « tendance » dans la communauté

[1] Fondation Sciences Mathématiques de Paris.

mathématique russe. Alors évidemment, l'ambitieux jeune homme que j'étais a été attiré par ce sujet qui était le plus « tendance », le plus difficile et d'une certaine façon le plus ésotérique parmi les mathématiques de cette époque.

*Pour quels travaux avez-vous remporté la médaille Fields en 2002 ?*

J'ai eu la médaille Fields pour ma preuve de la conjecture de Milnor. J'avais trouvé la démonstration début 1995, j'en avais rédigé l'essentiel fin 1996 et elle a été publiée en 2000. C'était vraiment fascinant de travailler sur ce sujet qui faisait intervenir tant de domaines des mathématiques très en vogue. Je me suis vraiment beaucoup amusé et j'ai beaucoup travaillé aussi ! Ce que dit cette conjecture c'est que pour tout nombre entier naturel $n$ et tout corps $K$ « quelque chose » est vrai, sauf qu'il y a des cas particuliers... Pour certains $K$, cela ne marchait pas pour tous les $n$, et pour certains $n$, cela ne marchait pas pour tous les $K$. Et les démonstrations pour ces divers cas particuliers étaient différentes les unes des autres, il n'était pas possible de les combiner ensemble pour en faire une preuve générale. La preuve du cas particulier le moins trivial était très étrange. Beaucoup de gens avaient du mal à comprendre cette preuve comme la conséquence de principes généraux, ou à voir clairement quels principes généraux il y avait en fait derrière. C'était très mystérieux. Beaucoup de mathématiciens ont essayé d'établir la preuve générale. Beaucoup de conjectures dépendaient de celle-ci ou s'en déduisaient, ce qui fait que quand j'ai été en mesure de la démontrer, cela a permis de développer bien d'autres choses. Je ne passais pas le plus clair de mon temps à travailler spécifiquement sur la conjecture. J'étais en train de développer cette théorie générale de *l'homotopie motivique*, ou théorie de la cohomologie motivique. À un moment, j'ai senti que j'avais une boîte à outils qui contenait des objets nouveaux, alors j'ai cherché quelque chose de spectaculaire à faire, histoire de montrer que ces outils étaient intéressants. Et c'est comme cela que cette conjecture a attiré mon attention, c'était quelque chose à tenter avec mes nouveaux outils. Et quand la preuve a été claire, c'est encore le développement d'outils généraux sous-tendant cette preuve qui a été délicat. Donc le travail sur la conjecture proprement dite a peut-être représenté 20% de mon temps, tandis que 80% de mon temps était consacré au développement des outils généraux pour cet usage particulier qu'était la preuve de cette conjecture.

*Pouvez-vous nous en dire plus sur ces théories ?*

C'est difficile pour des non-spécialistes, et d'ailleurs le fait que ce soit difficile à expliquer est une des raisons qui m'ont poussé à changer de sujet de recherche. C'était extrêmement frustrant de me dire qu'il n'y avait que 10 personnes au monde à qui je pouvais raconter mon travail, et que pour toutes les autres, je devais utiliser des analogies très primaires, sans pouvoir expliquer ce que je faisais. Cette frustration a joué un grand rôle dans mon choix de ce que j'allais faire ensuite : je ne voulais plus d'un sujet aussi ésotérique. Par ésotérique, j'entends réservé à une toute petite communauté.

Mais on peut partir de là pour en venir à ce que je fais maintenant. J'ai eu des idées générales susceptibles de me permettre d'étendre cette boîte à outils de la théorie de l'homotopie motivique. Mais cela requerrait l'utilisation systématique de ce qu'on appelle les 2-catégories. Et j'étais très frustré par le fait que je ne voyais pas très clairement comment expliquer mes raisonnements à propos de ce genre d'objets. C'est une chose que de faire des diagrammes et de réfléchir à ces 2-catégories d'un point de vue purement algébrique, mais c'est tout à fait différent de les utiliser comme outils pour calculer d'autres choses. Il y avait des parties de mon raisonnement où je sentais qu'il fallait en faire plus, mais je ne pouvais pas expliquer pourquoi. Cela n'avait pas de sens dans une approche classique du raisonnement mathématique. J'étais incapable d'expliquer pourquoi telle chose devait être faite de cette façon-ci, et surtout pas de cette façon-là. À ceci s'est rajoutée une autre frustration : celle de rédiger des articles remplis de raisonnements complexes dans un domaine où très peu de gens avaient les compétences pour vérifier si ce que j'avais fait était juste. La vérification de mes démonstrations pouvait prendre des années. Et j'ai senti que si j'amenais encore plus d'abstraction, de complexité, de constructions de haut niveau dans tout cela, il deviendrait tout simplement impossible à quiconque de contrôler ce qui se passait ! De plus, il m'était devenu difficile d'amener de nouvelles idées, car j'étais sans cesse préoccupé par la question de savoir si ceci était juste, si je pouvais m'appuyer sur cela. Comme je n'avais personne pour vérifier ce que je faisais ou ce que j'avais fait, c'était vraiment désagréable. C'est avant tout pour cela que j'ai arrêté la théorie de l'homotopie motivique, ce que j'ai fait effectivement après que mon dernier article sur la conjecture de Bloch-Kato a été accepté.

Je me suis vraiment dit : terminé, je vais faire autre chose. Il y avait en fait plusieurs possibilités. Je pouvais faire quelque chose qui fasse un lien entre mathématiques pures et appliquées, ou faire quelque chose autour de la vérification de preuves par ordinateur et les assistants de preuve. J'avais donc deux possibilités et dans un premier temps j'ai pensé que faire le lien entre mathématiques pures et appliquées était plus simple. J'ai donc essayé, et à un moment j'ai réalisé que j'avais perdu mon temps à faire n'importe quoi. Je me suis donc tourné vers la question de la vérification de preuves et là, cela a commencé à être fructueux. Et donc à partir de 2009, je me suis consacré entièrement à ce travail sur les assistants de preuve.

*Comment cette question de la possibilité d'une erreur (surtout quand un résultat n'est compris que par très peu de collègues) est-elle appréhendée par les mathématiciens ?*

Je pense que l'on comprend dans la communauté mathématique que c'est un problème, mais que c'est quelque chose dont on n'aime pas tellement parler. On se sent impuissant face à cela. C'est comme quand on n'a pas de remède à une maladie, on préfère ne pas mentionner cette maladie. Et puis il suffit qu'on trouve un remède pour que tout le monde se mette à en parler. C'est un peu pareil avec cette question des preuves et des erreurs en mathématiques. De même, publier un résultat intéressant, et voir que personne n'y réagit, parce que personne ne peut le comprendre, ou bien parce que tout le monde est occupé à faire publier ses propres résultats, pose problème. Les mathématiciens connaissent très bien ce phénomène d'absence de résonance d'un résultat que l'on publie. J'aimerais pourtant pouvoir en savoir plus sur les choses formidables que font d'autres mathématiciens. Le problème, c'est que quand je commence à lire un article, je n'arrête pas de tout vérifier. Donc lire un article devient quelque chose de fastidieux. On ne peut pas juste lire et faire confiance, apprécier. Et c'est pourquoi je pense que quand on aura établi une culture dans laquelle chaque résultat sera certifié par ordinateur, alors on pourra juste lire, faire confiance, apprécier, au lieu de douter, de trouver ça fastidieux, voire de ne pas lire du tout.

*Qu'est-ce que la théorie des types ?*

Il y a quelque chose d'une grande complexité derrière cette appellation de « théorie des types ». À l'origine, l'expression apparaît probablement dans l'œuvre de Russell, dans la première décennie du XX$^{e}$ siècle. Et à cette époque, l'idée des types était quelque chose qui servait à traiter, à éviter les paradoxes au sein de divers systèmes de logique formelle, c'était perçu comme quelque chose de contraignant[2]. Nous aurions adoré faire nos mathématiques dans le monde merveilleux des prédicats sans contraintes, en considérant que le monde entier est constitué d'objets et qu'il y a des prédicats qui sont en gros les propriétés de ces objets. En manipulant les prédicats de manière logique, nous aurions pu tout décrire, et plus particulièrement en mathématiques. Sauf qu'il y avait les paradoxes. C'est pourquoi on a introduit les types. Les types sont a priori restrictifs de par leur nature. Ils interdisent de faire certaines choses, et ces interdits, nous les intégrons dans notre manière de penser, sans quoi on produirait des paradoxes. Cela a été longtemps ainsi...

À quel moment exactement les types sont-il passés d'un dispositif qui restreint à un dispositif qui ouvre des possibilités ? À un moment donné, dans les années 1960, je pense, les *types inductifs* ont été introduits dans les langages de programmation pour exprimer des concepts comme le filtrage. À la fin, les types sont devenus des dispositifs qui permettent de faire des choses. Il y a eu la théorie des types de Russell, puis la théorie des types de Church dans les années 1940, et enfin la théorie des types de de Bruijn et Martin-Löf des années 70 jusqu'au début des années 1980. Donc vous pouvez voir que le développement a été extrêmement lent. C'est ce qui s'est passé en 100 ans. Si on fait la comparaison avec le développement des mathématiques, avec la complexité, la variété, et la beauté des structures qui ont été découvertes en trois décennies, on peut dire que la théorie des types a rampé par rapport à l'extraordinaire prospérité des mathématiques. Mais elle a quand même fait du chemin. Elle est devenue un dispositif puissant pour combiner le raisonnement logique et l'informatique. Maintenant, avec l'idée de théorie des *types homotopiques*, une nouvelle dimension s'ajoute qui ne consiste plus simplement à combiner la logique et l'informatique, mais qui consiste aussi à faire ces deux choses dans le royaume des structures mathématiques en grandes dimensions, comme les catégories. On n'a pas encore trouvé de système complètement satisfaisant pour une telle synthèse, mais on a parcouru pas mal de chemin ces cinq dernières années pour se rapprocher de ce qui était alors un rêve lointain. Nous avons maintenant un système dans lequel travailler, système qui n'est pas parfait, mais qui est quelque chose de tangible.

*Comment expliquer ce projet de « fondements univalents » sur lequel vous travaillez ?*

Le projet des *fondements univalents* a été pour moi quelque chose d'inattendu. Je ne m'attendais pas à ce qu'un tel projet puisse devenir réel si rapidement.

[2] Voir en particulier le paragraphe 2.1 de l'article de A. Pelayo et M. A. Warren.

Le point de départ est probablement l'article FOLDS de M. Makkai [3]. Makkai y examine l'idée de quelque chose qu'il appelle les « fondements univalents ». Dans ce cadre, l'univers n'est pas l'univers des ensembles dans lequel les mathématiciens travaillent, mais l'univers des $\infty$-*catégories*. Pour travailler avec des objets dans cet univers, nous avons besoin non pas de la logique du premier ordre, mais d'une logique à types dépendants, parce que nous voulons pouvoir parler de morphismes entre deux objets, plutôt que de parler de morphismes dont la source est égale au premier objet et dont la cible est égale au second objet[4].

La percée qui a vraiment mené les fondements univalents à ce qu'ils sont aujourd'hui, a été de comprendre que le mot $\infty$-catégories pouvait être remplacé par *groupoïdes*, et que ce sont les groupoïdes et les $\infty$-groupoïdes qui sont fondamentaux, là où les catégories, qui sont des structures très utiles sur les groupoïdes, ne sont qu'une sorte de structures utilisables parmi d'autres. Les groupoïdes doivent être compris, non pas comme un cas particulier de catégories, mais comme quelque chose de fondamental, tandis que les catégories doivent être comprises comme des groupoïdes munis d'une structure additionnelle. Avec ce changement de perspective, les fondements univalents sont possibles, car si nous ne savons pas ce qu'est une $\infty$-catégorie, nous savons ce qu'est un $\infty$-groupoïde. C'est juste un type d'homotopie, on le sait grâce à Grothendieck. Nous savons donc ce qu'est cet univers de $\infty$-groupoïdes. C'est la même chose que l'univers des types d'homotopie. C'est beaucoup plus facile à définir précisément. Et de là, j'ai donc vraiment pu établir la construction d'un modèle au sens de la théorie des types de Martin-Löf, où tout est représenté dans la catégorie homotopique. J'ai commencé à m'amuser avec cela avec l'assistant de preuve Coq, car Coq est une implémentation de la théorie des types de Martin-Löf sur ordinateur, qui existe depuis plus de 20 ans. Donc j'ai commencé à jouer avec tout cela en pensant au modèle homotopique, et j'ai réalisé que je pouvais faire tout ce que je voulais faire auparavant, sans que cela ne nécessite plus d'investissement. Je me suis dit que nous avions désormais de nouveaux fondements pour les mathématiques.

*Utilisez-vous la théorie de l'homologie sur laquelle vous travailliez auparavant dans votre travail actuel ?*

De par ma façon de travailler en dessinant des figures, des diagrammes, cela m'est très utile. Je fais cela tout le temps : je formalise en Coq, je fais mes mathématiques en Coq, mais je continue à faire mes dessins sur le tableau noir, mes diagrammes, mes limites homotopiques. Cette intuition qui vient du fait de travailler avec des catégories de modèles, ces catégories homotopiques, m'est extrêmement utile et je continue à m'en servir. Sinon, mes connaissances en géométrie algébrique n'interviennent pas plus que cela jusqu'ici.

---

[3] « First-order logic with dependent sorts, with applications to category theory » `http://www.math.mcgill.ca/makkai/`

[4] Le point de vue traditionnel de la théorie des (multi-)graphes est d'avoir un ensemble de sommets $V$ et un ensemble d'arêtes $E$, et d'indiquer pour chaque arête sa source et son but, ce qui donne deux fonctions « source » et « but » de $V$ dans $E$. Mais le point de vue plus standard en théorie des catégories (qui ne sont rien d'autre que des graphes avec une opération de composition) est de fixer pour chaque paire de sommets $a, b$ dans $V$ un ensemble $\mathrm{Hom}(a, b)$ (les arêtes de $a$ vers $b$).

*Diriez-vous que votre vision des mathématiques, ou de votre métier de mathématicien, a changé ?*

Oui, elle a beaucoup changé, de même que la manière, en pratique, dont je fais des mathématiques. *Ma vision de ce qui est intéressant a changé*. Et les sensations que j'éprouve quand quelque chose marche ou ne marche pas, tout cela a changé !

*Est-ce que vous diriez que vous avez maintenant un point de vue plus constructiviste ?*

Ce qui est remarquable avec les fondements univalents, c'est qu'ils sont naturellement constructivistes. Et ils permettent de faire de manière constructive des choses que l'on ne pouvait pas faire de cette façon auparavant. Il est donc devenu tout à fait réaliste d'envisager des mathématiques constructives intéressantes, sans vouloir offenser les constructivistes. Mais je parle du point de vue de la communauté mathématique, de ceux qui utilisent les mathématiques de manière professionnelle. Je crois que nous avons toujours voulu quelque chose de plus, pouvoir utiliser plus d'objets, plus de constructions mathématiques. Si l'on considère les mathématiques constructives au sens restrictif, c'est-à-dire en empêchant quelqu'un d'utiliser quelque chose, c'est un peu étrange. Mais maintenant, avec les fondements univalents, on peut faire de bonnes mathématiques constructives. Pour moi, la *logique constructive* est beaucoup plus intéressante que la *logique classique* : elle est beaucoup plus proche du comportement réel. Par exemple, en logique classique, comme la double négation équivaut à l'identité, il n'y a aucune différence entre une proposition affirmative et une proposition négative. Nous y sommes habitués. Mais quand vous commencez à disposer de l'option qui consiste à vous dispenser de cette identification, vous comprenez que vous pouvez faire des mathématiques intéressantes dans un monde logique où une proposition positive n'équivaut pas à une proposition négative, et où il y a, de fait, une différence entre les choses positives et les choses négatives. Il me semble que c'est plus proche de la vérité. Maintenant je pense donc qu'il est vraiment très intéressant de faire les choses de manière constructive.

*Qu'en est-il des logiciels « assistants de preuve » ?*

Les *assistants de preuve* sont au cœur de mon approche des fondements univalents. Ceux-ci ne sont possibles qu'avec les assistants de preuve, ces fondements sont en effet beaucoup plus complexes si l'on ne dispose pas d'ordinateurs qui puissent manipuler les formules dont on a besoin. Mon but initial n'a jamais été de recréer les fondements des mathématiques. Mon but était, et est toujours, de contribuer à la création d'assistants de preuve utilisables pour qu'un jour, peut-être, j'aie la satisfaction de m'asseoir devant mon ordinateur et de me remettre à travailler sur mes théories mathématiques en faisant les choses comme je pense qu'elles devraient être faites, avec un assistant de preuve avec lequel je puisse travailler. Les assistants de preuve sont très importants. La partie la plus connue de leur histoire est probablement celle qui se situe de la fin des années 1960 au début des années 1970. À cette époque, deux assistants de preuve sont développés, *Automath* par de Bruijn, aux Pays-Bas, et *Mizar*, en Pologne. Mizar, qui est toujours en développement, repose sur la théorie des ensembles. C'était donc quelque chose de rassurant pour les mathématiciens habitués à travailler dans ce cadre. Automath reposait sur un socle original que de Bruijn avait inventé. Il y avait aussi LCF. Aujourd'hui, la situation est la suivante : il y a plusieurs assistants de preuve qui sont activement développés, et pour chacun d'entre eux, il y a un groupe de personnes qui s'y consacrent activement. Il y a aussi d'autres assistants de preuve qui apparaissent. Personnellement j'utilise habituellement Coq dans mon travail, et j'essaye d'y contribuer, de suggérer des améliorations inspirées de l'idéologie des fondements univalents. La question est de savoir quel assistant peut bénéficier des nouvelles idées explorées avec les fondements univalents. C'est une question complexe.

*On connaît des théorèmes dont la démonstration a été « certifiée par ordinateur », le théorème des quatre couleurs, par exemple...*

Le théorème des quatre couleurs est un bon exemple illustrant la question de l'intégration du calcul par ordinateur dans l'aide à la preuve. Car ce théorème a été démontré à l'origine en utilisant du calcul par ordinateur et les gens étaient dubitatifs. Ils n'étaient tout d'abord pas sûrs du calcul lui-même, ni du logiciel utilisé. Ensuite, il n'était pas clair qu'un calcul par ordinateur puisse être valable au même titre que le raisonnement logique. Ensuite, G. Gonthier a établi une preuve complète du théorème en Coq ; cette preuve comportait à la fois un raisonnement logique et des calculs par ordinateur, mais le tout était fait en Coq, dans un même système. Cette démonstration a donné naissance à un nombre intéressant que Tom Hales a évoqué, donc je l'ai appelé « nombre de Hales ».

Il existe un nombre nommé « nombre de de Bruijn » qui sert à comparer la longueur d'une preuve formelle à celle d'une preuve écrite en langage humain. Et pour un assistant de preuve, ce nombre est un invariant. Un assistant de preuve est d'autant plus mauvais que ce nombre est grand. Pour le travail le plus long que j'aie effectué sur les fondements univalents, le nombre de de Bruijn est inférieur à 1, donc cela aurait pris beaucoup plus de temps de faire cela à la main que cela n'en a pris sur Coq. Ce nombre est très important du point de vue de l'usage quotidien des assistants de preuve.

Il y a un autre nombre important qui est le suivant : considérons des calculs faits avec l'ordinateur, que ce soit ceux de la preuve du théorème des quatre couleurs ou ceux de la preuve de la conjecture de Kepler par Tom Hales. Dans les deux cas, une partie de la preuve utilise des calculs avec un logiciel de calcul numérique. Maintenant, prenons tout ce calcul, et au lieu de le lancer avec l'ordinateur, on en fait une partie d'une preuve certifiée. Au lieu de faire du calcul directement, on le fait donc avec un assistant de preuve tout en effectuant la procédure de certification de la preuve. La longueur du calcul fait directement par ordinateur et la longueur du même calcul fait avec l'assistant de preuve peuvent alors être comparées. Quand vous écrivez le code du programme nécessaire pour que l'assistant de preuve fasse un calcul et qu'ensuite vous faites le même calcul, mais en écrivant un programme en C, il y a une différence de temps entre les deux et c'est ce que j'appelle le nombre de Hales. Le nombre de Hales mesure à quel point la programmation avec assistant de preuve est plus lente que la programmation classique. Dans le cas de l'assistant de preuve que Thomas Hales a utilisé pour sa preuve de la conjecture de Képler, le coefficient était de 2000. C'est un nombre très élevé. C'est fâcheux si vous voulez que le calcul certifié devienne la norme en calcul scientifique en général.

Or il me semble important de commencer à utiliser la certification dans les champs d'application des mathématiques, comme la physique, la biologie. Donc ce nombre de Hales va être déterminant dans l'acceptation de la certification. Il faudra réussir à passer de 2000 à un nombre proche de 1. C'est une frontière importante dans le développement des assistants de preuve.

Il reste, de plus, plusieurs problèmes à résoudre, plusieurs portes à ouvrir pour populariser l'utilisation des assistants chez les mathématiciens, leur installation sur un ordinateur pour commencer. Jusqu'à récemment Coq ne pouvait pas s'installer sur Mac OS. Se pose aussi la question des fondements des mathématiques sur lesquels on s'appuie. Par exemple, utiliser Coq suppose de s'appuyer sur quelque chose comme les fondements univalents, à mon avis, parce qu'utiliser Coq avec la théorie des ensembles me semble un peu incongru. Dans le cas de Coq, de mon point de vue, le principal défaut réside dans la faiblesse de la propriété de substitution dans les égalités. Parfois une partie de la démonstration semble évidente et vous vous dites que cela ne devrait pas prendre tant de place et être si complexe.

*Que dire à ceux qui imaginent ces logiciels comme des outils qui à terme « feront » les mathématiques tous seuls, ou remplaceront les mathématiciens ?*

L'idée que les assistants de preuve puissent mener les mathématiciens à être remplacés par les ordinateurs est d'une totale absurdité, de même que l'idée, en général, que les machines puissent remplacer les hommes. Les mathématiques sont un champ de création. Bien sûr, les ordinateurs ont remplacé les gens qui faisaient des calculs, quand le calcul faisait encore partie de grands projets dans les années 1940, par exemple. Les ordinateurs ne peuvent que servir, ils ne peuvent pas développer d'énergie humaine ou sociale par eux-mêmes. Ceci dit, certains mathématiciens sont en effet préoccupés par ces développements, pas du tout parce qu'ils ont peur d'être remplacés par des machines, mais peut-être par peur d'être mis en compétition avec d'autres mathématiciens, et plus particulièrement les mathématiciens plus jeunes, rompus à l'usage des assistants de preuve. Je peux aisément comprendre ce sentiment : on est en train de faire quelque chose que l'on aime faire, et soudain quelqu'un arrive et vous dit que maintenant il faut le faire en utilisant ce nouvel outil, vous devez apprendre à utiliser cet outil, ce qui va ralentir votre travail... Mon espoir est que le bénéfice de ces nouveaux outils sera supérieur au coût. Il y a certes cette tension, mais ce changement finira par être accepté par la communauté mathématique.

*À terme, l'utilisation des assistants de preuve va-t-elle se généraliser ?*

Je l'espère. Les assistants de preuve sont absolument nécessaires. Sinon nous allons rester séparés dans des sous-communautés. La question est d'essayer de ne pas les imposer à tout le monde. Je pense également qu'il est essentiel que l'on puisse disposer de plusieurs assistants de preuve fiables, qu'il n'y en ait pas un seul que tout le monde utilise, et que toute la communauté soit paralysée si quelque chose se passe avec un logiciel ou l'équipe qui le développe. Aujourd'hui il y a de plus en plus de discussions sur plusieurs assistants de preuve confirmés et il y a une certaine communication entre eux. Je suis donc certain que la généralisation de l'usage des assistants de preuve se fera.

Nous remercions Pierre-Louis Curien et Christian Retoré pour leur aide précieuse lors de la préparation de cet entretien.