Preuves à divulgation nulle

Avi Wigderson

Avi Wigderson : Je vais essayer d'expliquer ce que sont les preuves à divulgation nulle et peut-être, pourquoi de telles preuves sont utiles.

Eh bien, nous pouvons commencer par une preuve - vous savez que la preuve est la base des mathématiques. La façon dont nous savons que quelque chose est absolument vrai est de le prouver. Comme vous le savez, et comme nous le savons tous, la somme des angles d'un triangle est égale à 180 degrés, nous pouvons le prouver et nous savons alors que cela est vrai pour chaque triangle que nous rencontrons, et même pour des triangles auxquels nous n'avons pas eu affaire.

Les preuves sont ce qui fait que nous sommes certains de certains faits mathématiques. Qu'est-ce qui fait qu'ils sont certains ? C'est qu'ils ont été démontrés selon des règles logiques telles que, vous savez, toute personne qui veut vérifier la preuve peut simplement en suivre les étapes et être convaincu que c'est bien vrai. À quelqu'un qui ne saurait pas à l'avance que telle assertion est vraie - appelons ce type un vérificateur de la preuve, il existe un moyen de vérifier même s'il ne connaît pas de preuve à vérifier étant donné qu'elle est correcte, et en général, c'est beaucoup plus simple de vérifier une preuve que de prouver qu'un théorème est juste.

Le prouveur, le gars qui l'a prouvé, peut être un génie, on n'en connaît qu'un par vie, comme Wiles, qui a prouvé le dernier théorème de Fermat, mais une fois qu'il l'a fait, il a écrit une preuve et puis les gens, vous savez, peut-être avec un peu de travail, mais en n'ayant pas besoin de beaucoup d'ingéniosité, pourraient vérifier que c'est correct. C'est donc une preuve.

Et maintenant, qu'est-ce qu'une preuve à divulgation nulle ? Les preuves à divulgation nulle, comme leur nom l'indique, sont des preuves qui ne révèlent absolument aucune information au vérificateur. Donc encore une fois, nous avons un prouveur qui connaît une certaine vérité et une preuve de celle-ci peut-être un théorème mathématique. Un vérificateur, quelqu'un qui voudrait peut-être être convaincu de cette vérité, mais qui ne se laisserait pas berner par un non-sens.

Le processus dans une preuve à divulgation nulle doit être convaincant d'une part si l'affirmation est vraie et ne doit pas être convaincant si l'affirmation est fausse - donc si je n'ai pas de preuve pour l'affiration.

Alors disons que je veuille vous convaincre. On a cette conversation entre nous, et à la fin vous ne savez rien de plus qu'avant sauf que vous savez que l'affirmation que j'ai

---

Lien vers la vidéo Numberphile : https://www.yout-ube.com/watch?v=5ovdoxnfFVc
Reprise de la traduction Google des sous-titres downsub et mise en forme Latex :
Denise Vella-Chemla, novembre 2021.

faite était vraie. Il n'y a aucune information sur la preuve dans cette conversation. Il n'y a aucune information sur quoi que ce soit en fait que vous ne saviez pas déjà... et pourtant il n'y a aucun moyen de vous tromper et vous serez convaincu. Je ne peux pas vous tromper en vous faisant croire quelque chose d'incorrect ou quelque chose dont je n'ai pas de preuve...

Brady : *(in a surprised tone)* Vous dites qu'après m'avoir convaincu par une preuve à divulgation nulle, je n'ai pas de nouvelle information à l'exception de l'information que XYZ est vrai ? ?

Avi Wigderson : Oui. Alors peut-être donnons-nous un exemple. C'est une histoire que j'aime bien raconter bien qu'elle semble montrer que les mathématiciens peuvent être paranoïaques.

Alors c'est encore toi et moi, mais disons que je suis un jeune professeur de mathématiques et que vous êtes le Président de mon université. Peut-être que nous sommes tous les deux des théoriciens des nombres, et je viens vers toi et je vous dis "regardez, vous savez que je viens de prouver l'hypothèse de Riemann". Donc, pour le public, c'est peut-être le problème le plus célèbre en mathématiques - c'est le Saint Graal.

Et je viens à vous et je vous dis "regardez, je l'ai prouvée, puis-je obtenir un poste ?". Et vous dites "bien sûr, montre-moi la preuve". Nous sommes tous les deux des théoriciens des nombres... Dans une conversation normale entre mathématiciens, vous savez que je vais commencer à utiliser le tableau ou du papier kraft ou un support quelconque et vous savez que je vais commencer à vous montrer les lemmes et les preuves et toute la séquence peut-être prendra une heure, peut-être cela prendra-t-il un jour ou peut-être cela prendra-t-il un an, mais vous savez que si j'ai la preuve, vous serez finalement convaincu. Et quel est le problème dans ce processus, je veux dire qu'il n'y a pas de problème, c'est comme ça que fonctionnent les mathématiciens.

Mais il y a quelques histoires dans l'histoire des mathématiques - vous en connaissez peut-être déjà certaines - où cela ne s'est pas aussi bien passé, lorsqu'un chercheur senior, ayant entendu la preuve, s'est dépêché de la publier.

Brady : Il l'a volée...

Avi Wigderson : Oui, vous savez donc que c'est arrivé. Ce n'est pas que ça arrive souvent, mais c'est arrivé. Alors peut-être que le chercheur junior, vous savez, moi à sa place, j'aimerais un peu de protection. Ce serait bien mieux pour moi si je pouvais vous convaincre complètement que j'ai une preuve, que je connais une preuve de l'hypothèse de Riemann sans vous donner la preuve elle-même (en vous donnant un brin d'évidence de la preuve).

Et alors, avec une preuve à divulgation nulle, vous savez que c'est vrai. Et le fait de savoir que la personne a la preuve, même en n'ayant pas entendu cette preuve, c'est

toute la valeur d'une preuve à divulgation nulle.

C'est un exemple, alors maintenant vous devriez vous demander quelles déclarations mathématiques, ou quelles déclarations tout court, ont de telles preuves ? Peut-être que certaines déclarations ont une telle preuve, peut-être qu'aucune déclaration n'a une telle preuve, il semble contre-intuitif de dire qu'il y en aura peu, parce que nous associons en quelque sorte la conviction au transfert d'informations... Je veux dire qu'il n'y a rien, si je n'ai rien appris de nouveau et que je ne savais pas que c'était vrai.

Voyons un autre exemple : supposons que nous soyons tous les deux face à un casse-tête sudoku, vous voyez ce que c'est, c'est trop dur pour vous mais imaginons que je sais comment le résoudre, et je vous dis "Regardez, Brady, je peux le faire, celui-ci" et vous dites "je ne vous crois pas". Très bien, donc une preuve, dans ce cas, est très simple, d'accord, c'est quelque chose : je remplis juste les blancs, vous les cochez, c'est un type de preuve très simple. Il y a un moyen pour moi de vous convaincre complètement que je peux le faire sans avoir à écrire quoi que ce soit, c'est un processus différent

Brady : Donc je ne connais pas votre algorithme, mais je sais que vous dites la vérité.

Avi Wigderson : Vous ne connaissez pas l'algorithme, vous ne savez rien de plus que ce que vous saviez avant, sauf que maintenant vous me croyez, vous croyez que je peux remplir la grille de sudoku, oui. Nous parlons d'objets finis donc la preuve que je peux résoudre le sudoku, c'est juste de remplir les cases avec des nombres. Prenons la preuve qu'il y a une infinité de nombres premiers, je peux en écrire une. Si j'avais la preuve de l'hypothèse de Riemann, je m'attends à ce que cette preuve soit finie et je pourrais la publier directement.

Alors comme je l'ai dit, vous pouvez vous demander quel genre de déclarations peuvent avoir de telles preuves à divulgation nulle ? Cette question a été soulevée dans le cadre de la cryptographie par Goldwasser et Micali et Rackoff, au milieu des années 80, et environ un an plus tard, avec Oded Golreich et Silvio Micali, nous avons prouvé que chaque déclaration qui a une preuve a une preuve à divulgation nulle, d'accord, toutes.

Donc on peut le faire avec le sudoku, on peut le faire avec l'hypothèse de Riemann, chaque énoncé qui a une preuve a également une preuve à divulgation nulle.

Mais je veux juste dire que cette preuve à divulgation nulle sera légèrement différente de celle, vous savez, écrite dans un cadre normal : pour une preuve normale, vous ne faites que l'écrire ; pour une preuve à divulgation nulle, nous devons interagir, vous devez me poser des questions et, vous savez, c'est une interaction, d'accord, alors les preuves à divulgation nulle sont interactives, il faut que vous me posiez des questions, ces preuves nécessitent une interaction.

Brady : Comment puis-je interagir avec vous sans augmenter votre quantité de connaissance ?

Avi Wigderson : Il y a deux questions distinctes. Tout d'abord, vous pouvez interagir avec moi et je peux refuser de répondre à toutes les questions que vous voulez et alors vous n'obtiendrez pas d'information.

Donner des preuves dans un cadre interactif est aussi, vous le savez, naturel. Vous dites "oh, expliquez-moi ça, je n'ai pas compris" ou "montre-moi un exemple" ou quoi que ce soit d'autre. Les preuves interactives sont donc un objet naturel. Comment pouvons-nous donc prouver que quelque chose n'a donné aucune information ? Je veux dire que vous pourriez vous poser des questions sur cette affirmation. Comment peut-on prouver une telle affirmation ?

La manière de prouver une telle assertion est que quelqu'un d'autre qui n'a pas connaissance de la preuve pourrait avoir généré la conversation que nous venons d'avoir. Si quelqu'un, ou vous-même, pouvait générer la conversation que nous avons eue, si vous-même aviez pu générer la conversation que nous avons eue, vous n'auriez pas besoin de moi - vous utiliseriez seulement les connaissances que la vérité de la déclaration aurait pu générer la conversation que nous avons, cela signifierait que vous n'avez rien appris.

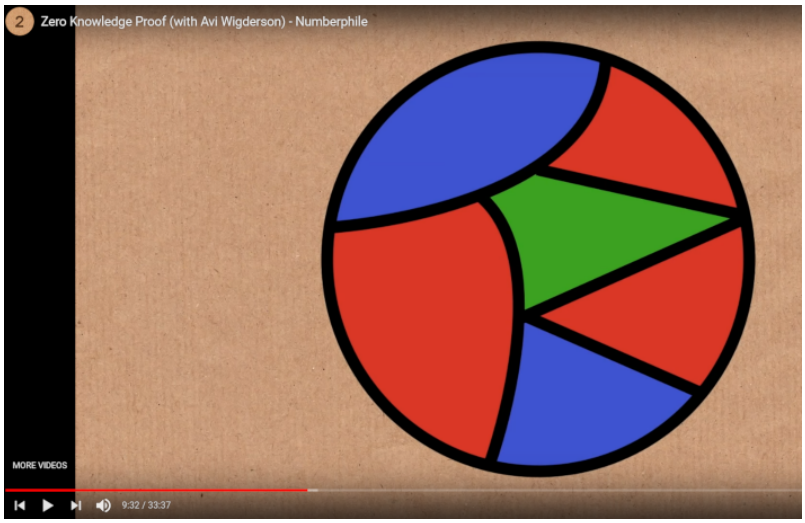
C'est ainsi que vous prouvez que la preuve est à divulgation nulle. La façon dont nous prouvons que chaque énoncé a une preuve à divulgation nulle était en deux parties : d'abord, nous avons prouvé qu'un certain type de déclarations, ce qui est très imagé, ont une preuve de connaissance nulle - d'accord, c'est une déclaration sur le coloriage de cartes, qui, vous le savez, se rapporte au célèbre problème qu'est le théorème des quatre couleurs, du coup je le mentionne.

Nous avons donc prouvé que ces types d'énoncés sur la capacité de colorier des cartes ont des preuves à divulgation nulle.

Et après, nous avons fait appel à un résultat général sur la NP-complétude de ce problème. J'ai donné un exposé au sujet de la NP-complétude, c'est un concept très important de la théorie de la complexité de calcul, et nous l'avons utilisé pour en déduire que tout énoncé qui a une preuve a également une preuve à divulgation nulle.

Alors laissez-moi vous expliquer à propos du coloriage d'une carte, que vous connaissez, on a une carte telle qu'une carte géographique et vous pouvez penser que ce que nous voyons sont des pays, donc vous voudriez colorier les pays pour que les pays qui sont voisins auront des couleurs différentes.

Alors peut-être que nous colorons celui-ci en bleu - si nous colorons ce bleu, cela signifie que nous ne pouvons colorier aucun de ceux-là en bleu, alors peut-être qu'avec du rouge, et alors, cela nous ne pouvons pas le colorier en rouge ainsi qu'en bleu, donc il doit être d'une autre couleur - vert -, et celui-ci, je suppose qu'il doit être colorié en rouge.



Avi Wigderson : Voyons si on peut le faire avec trois couleurs, oui, parce que ça nous pouvons aussi le colorier en rouge, à droite - donc seuls les pays qui partagent une frontière, ne peuvent pas être coloriés avec la même couleur - et alors nous pouvons je suppose colorier celui-ci en vert ou bleu, ce que vous voulez. Cette carte particulière peut donc être colorié avec trois couleurs.

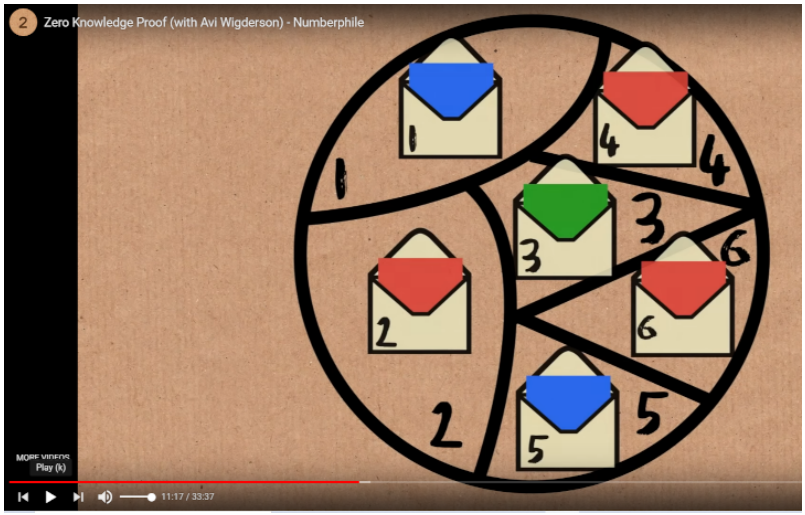
C'est un théorème très célèbre en mathématiques qui dit que chaque carte planaire comme celle-ci peut - peu importe le nombre de pays qu'elle possède - peut être coloriée avec quatre couleurs. Ou si j'ai besoin de vous convaincre que je peux colorier une carte planaire avec quatre couleurs, vous n'avez pas besoin d'être convaincu, sachez qu'il existe un article faisant cela pour n'importe quelle carte planaire, mais toutes les cartes planaires ne peuvent pas être coloriées avec trois couleurs comme celle-ci peut l'être. Regardez cette carte oui, alors c'est aussi un pays, d'accord, donc nous avons quatre pays et ils se touchent tous, ils ont tous des bordures entre eux, donc cela nécessite quatre couleurs... Toute carte ne peut pas être coloriée par trois couleurs.

Alors maintenant, c'est une chose intéressante à prouver : admettons que je prétende qu'une carte peut être coloriée avec trois couleurs, d'accord, supposons que je fasse cette affirmation, et que vous ne me faites pas confiance, et que vous disiez que vous voulez la preuve ?

D'accord, je peux vous donner un 3-coloriage comme je l'ai donné ici, d'accord, vous vérifiez les limites et vous dites d'accord, oui, ça, c'est légitime, je vous crois. Et le défi maintenant est de fournir la preuve à divulgation nulle. Ainsi, la première partie de notre article montre qu'une assertion de ce type - cette carte est tricolore - a une preuve à divulgation nulle.

Brady : Mais la façon dont je peux voir que vous pouvez le prouver, c'est juste en le faisant, en le montrant, en accomplissant l'acte.

Avi Wigderson : C'est vrai - ce n'est donc pas le seul moyen... ce n'est pas le seul. Dessinons à nouveau la même carte. Alors je veux vous convaincre que je sais comment on peut colorier cette carte et au lieu de vous dire les couleurs qui révéleraient des informations que je ne veux pas révéler, à la place, on peut par exemple associer des chiffres à ces pays et ici au lieu d'écrire la couleur, je vais mettre une enveloppe. Bon alors, je vous dis "Brady, cette carte est 3-coloriable et j'ai un 3-coloriage de cette carte et voici ma preuve : je vais mettre la couleur dont j'ai besoin pour chaque pays à l'intérieur de cette enveloppe - chaque enveloppe est comme un engagement une fois que je l'ai mise sur la table - et ce sont de vraies enveloppes. Considérez-les comme de vraies enveloppes - je veux dire, si nous les avions, je peux le faire. Il y a des enveloppes et à l'intérieur de chacune se trouve le nom de la couleur que je vais utiliser pour tel ou tel pays.



Brady : Donc si j'ouvre une enveloppe, ça va dire rouge ou bleu.

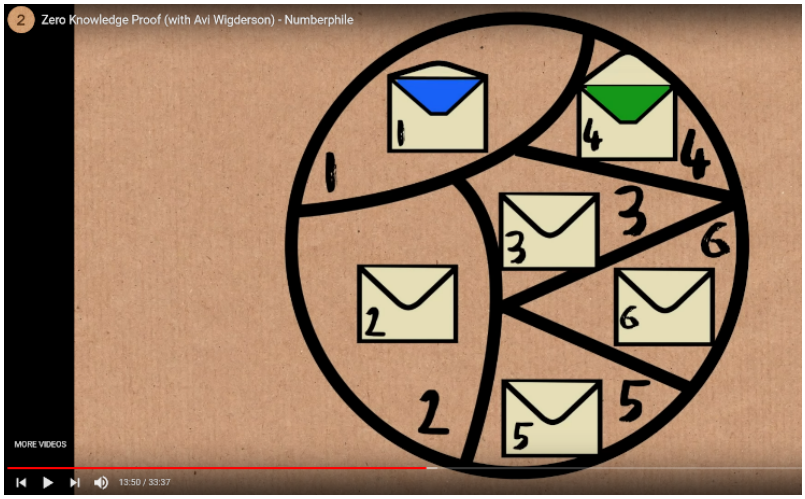
Avi Wigderson : Oui, donc tout d'abord si vous ouvrez une enveloppe - disons que la promesse est que non seulement le coloriage est tricolore mais tricolore avec ces couleurs - rouge vert et bleu - donc si vous ouvrez une enveloppe et que vous voyez du violet,

vous me jetez, vous dites que vous ne me croyez pas.

Encore une fois, une preuve normale serait que j'ouvre toutes les enveloppes pour vous, mais cela révélerait le coloriage.

Que va-t-il se passer en cours de preuve : je vous laisserai seulement me demander "Avi, vous savez, je ne vous crois pas, alors peut-être comme je vois que les pays un et quatre sont voisins, je vous défie d'ouvrir l'enveloppe un et l'enveloppe quatre.", et je les ouvre et encore une fois si vous voyez une couleur qui n'est pas un rouge, vert, ou bleu, vous me jetez. Aussi, si vous voyez la même couleur dans les deux, vous me jetez, vous dites que vous croyez que je n'ai pas trouvé de 3-coloriage et lorsque processus se termine.

Il est possible et c'est vraisemblable puisque j'ai fait la preuve et que je n'essaye pas de vous tromper, que vous verrez toujours deux couleurs différentes. Bien sûr, ça seulement ne devrait pas vous convaincre beaucoup parce que vous savez peut-être qu'il existe ce genre de carte à un million de pays.



Brady : Vous auriez pu avoir de la chance.

Avi Wigderson : J'aurais pu avoir de la chance, oui, et donc vous voulez être convaincu convaincu à 99,99999 % que je ne peux pas vous tromper. 100 pour cent, comme je le dis souvent, nous ne pouvons pas l'avoir dans notre monde, donc en fait, dans ce sens, ce n'est pas tout à fait comme une vérité mathématique gravée dans le bronze comme vous l'avez mentionné précédemment. Votre confiance dans le déroulement de la vérification peut être aussi élevée que vous le souhaitez et elle s'approchera de 100 pour cent comme vous le souhaitez simplement en répétant ce processus, mais ce ne sera jamais cent pour cent.

Quoi qu'il en soit, alors, vous pouvez le refaire parce que vous voulez prendre confiance, vous recommencez, et j'ouvre à nouveau les deux, et puis vous recommencez encore une fois, j'ouvre à nouveau, nous le faisons autant de fois que vous le souhaitez.

Mais ça ne peut pas être une preuve à divulgation nulle si je mets vraiment dans ces enveloppes le coloriage que j'avais en tête et si vous les avez finalement toutes ouvertes car alors vous avez tout appris. Voici donc l'astuce pour que ceci ne soit pas possible : après que vous ayez regardé deux enveloppes de deux pays voisins, j'ai remis un coloriage de couleurs différentes dans les deux enveloppes, d'accord ?

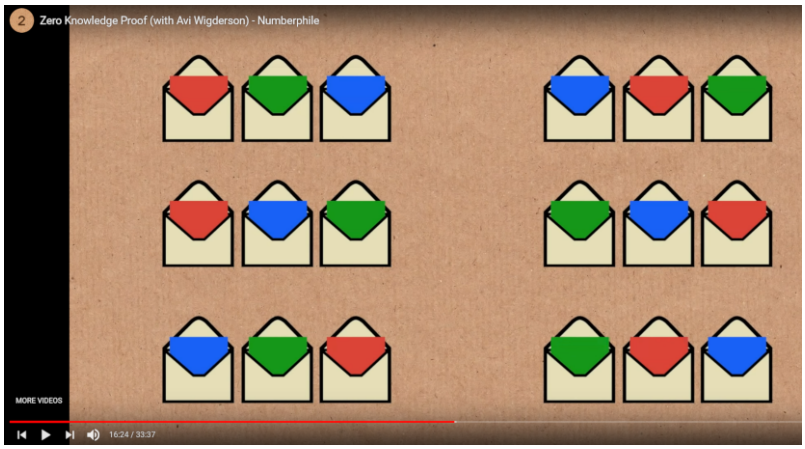
Brady : Mêmes cartes avec des couleurs différentes ?

Avi Wigderson : C'est ça, je vais vous expliquer en quoi le coloriage est différent. Puisque j'ai un coloriage et que vous ne croyez pas qu'il y ait un coloriage, je change la couleur de la paire d'enveloppes, et puis vous me testez sur deux autres et puis le processus continue.

Alors maintenant, on ne sait pas pourquoi cela devrait être convaincant, n'est-ce pas, parce que j'ai changé la couleur d'une paire et on ne sait toujours pas non plus pourquoi ce processus ne donne aucune information parce qu'on ne sait pas... Peut-être qu'il n'y a qu'un seul coloriage, ou bien peut-être qu'il y en a plusieurs - il existe des cartes pour lesquelles un seul coloriage marche.

Alors je dois vous expliquer les 2 choses que je viens de dire. Maintenant, je veux vous convaincre que la façon dont je vais procéder ne révèlera aucune information pour vous, d'accord, et pour cela je dois expliquer comment je récupère, et comment je peux remplir les enveloppes encore et encore, avec les nouvelles couleurs. C'est suffisant d'expliquer le processus sur une carte contenant seulement deux pays - supposons que c'est une carte que vous connaissez. Elle fait partie d'une carte plus grande, d'accord ? Il y a donc beaucoup plus de pays mais nous allons nous concentrer sur deux pays seulement, parce que vous allez me questionner sur ces deux pays - et supposez que j'avais trouvé un certain 3-coloriage de cette carte et en particulier ce pays était vert et ce pays était bleu - et sinon il y avait, vous savez, du bleu ici, du bleu ici et ceux-là rouges et ainsi de suite... Si j'ai un 3-coloriage d'une carte alors j'en ai automatiquement six. Pourquoi ? Je peux toujours renommer les couleurs - je veux dire que vous pouvez savoir que c'est vert à droite,...

Brady : Vous pourriez l'inverser ?



Avi Wigderson : Je pourrais, oui, je pourrais les permuter. Si j'ai ce coloriage - il suffit de renommer les couleurs, et j'appelle ça vert et ça rouge et ça bleu et oui, peut-être que je ferai les six - je ne sais pas. Alors si j'avais un coloriage, j'aurais six coloriages parce que je viens de le-renommer je peux le renommer puisque je suis celui qui va remplir les enveloppes et à chaque tour, je vais choisir au hasard l'une de ces 6 possibilités et l'utiliser - donc si j'ai un coloriage, j'en ai six.

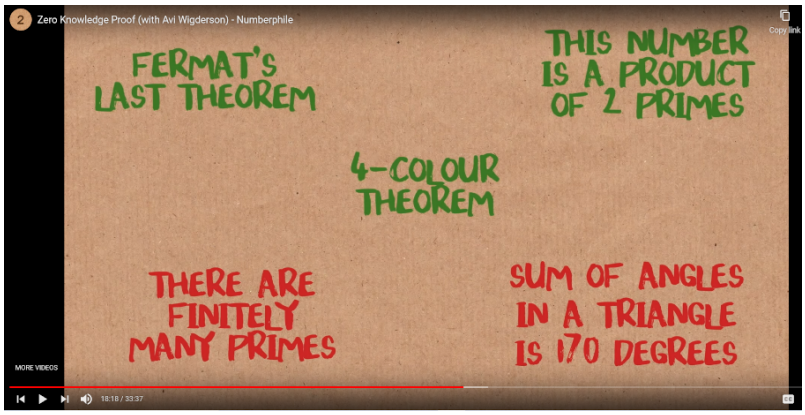
Maintenant regardez ce qui va se passer pour une paire particulière sur laquelle vous pourriez me questionner - dans un coloriage, elle peut avoir été vert et bleu mais si vous regardez le vert et le bleu ici, vous voyez ce qui se produit avec un renommage aléatoire : tout est possible et tout aussi probable si je le choisis au hasard - donc le fait est que dans ce processus, si j'avais une preuve, vous ne verriez pas seulement deux couleurs différentes pour ces deux colonnes, vous verriez deux couleurs différentes au hasard pour ces deux colonnes, vous verriez juste une paire aléatoire de ces colonnes. Mais c'est quelque chose que vous auriez pu faire vous-même - vous n'avez pas besoin de moi pour ça.

Si j'avais une preuve, vous n'apprendrez rien car le processus ne fera que révéler des paires aléatoires de couleurs. Si je n'avais pas de preuve, vous me surprendriez à tricher - c'est tout.

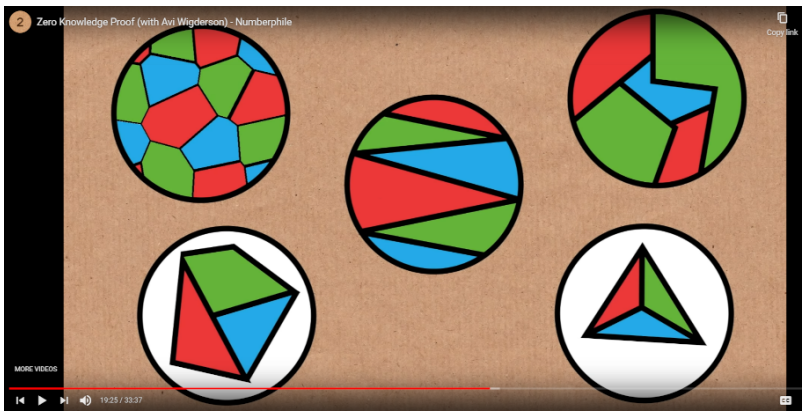
Parlons également de l'article d'Andrew Wiles : comment pourrais-je le convertir en une preuve à divulgation nulle. Il s'avère que la réponse aux deux questions est la même - et cette réponse est la NP-complétude. C'est un type de question qui capture toutes les déclarations mathématiques - l'un des problèmes NP-complet qui est très populaire est celui de savoir si une carte est coloriable avec seulement trois couleurs.

Qu'est-ce que je veux dire par capturer toutes les déclarations mathématiques : si nous avons des énoncés mathématiques - disons le dernier théorème de Fermat, ou qu'un nombre est le produit de deux nombres premiers, ou le théorème des quatre couleurs. Il y a également de fausses déclarations comme il y a un nombre fini de nombres premiers, ou la somme des angles dans un triangle est de 170 degrés ; ce sont de fausses déclarations mais n'importe quel énoncé mathématique formel peut être converti en une carte

et je dois souligner que cette conversion est efficace, il existe un algorithme simple connu de tous... C'est un résultat de la fin des années 70, un résultat fondamental démontré indépendamment par Cook à l'ouest et Levin à l'est - ils ont prouvé essentiellement que tout énoncé mathématique du type que nous venons d'évoquer, n'importe quel énoncé mathématique formel peut être converti en une carte et cela, la traduction de l'énoncé en une carte est très simple, efficace, connue de tout le monde.



Avi Wigderson : Ceci est donc la première partie du théorème et que voulez-vous tirer de cette traduction ? Vous voulez en tirer deux choses (eh bien, nous voudrions en tirer trois choses en fait, mais commençons par les deux qui sont les plus évidentes). Nous voulons que si la déclaration est vraie, la carte peut être coloriée de façon tricolore - et si la déclaration est fausse, la carte n'a pas de coloriage tricolore.



Avi Wigderson : Donc à ce stade, nous pouvons traduire n'importe quelle déclaration en une déclaration sur la 3-colorabilité d'une carte ; ce résultat de Cook et Levin a une propriété supplémentaire qui est très importante : si en plus de la déclaration, j'avais la preuve de la déclaration, le même algorithme qui le traduit en une carte fournit également un 3-coloriage de cette carte. Si c'est une affirmation vraie, alors j'en ai la preuve ; non seulement je peux vous donner une carte, mais j'en connais aussi un 3-coloriage.

D'accord, alors il y a ces trois propriétés. Il est clair maintenant que si Wiles voulait vous prouver avec une preuve à divulgation nulle qu'il a une preuve de son dernier théorème de Fermat, il pourrait le faire, vous pourriez tous les deux le faire, parce que vous pourriez tous les deux le traduire en une carte, parce que vous connaissez aussi le processus. Juste à partir de la déclaration, vous pourriez construire une carte. Alors maintenant, la preuve du dernier théorème de Fermat est devenue la 3-coloriabilité de cette carte que vous connaissez, c'est la carte du théorème de Fermat, puis Wiles vous prouverait en utilisant les enveloppes que je viens de montrer, il vous prouverait que la carte est 3-coloriable et c'est une déclaration équivalente - et vous n'apprenez rien de cela, rien du tout, comme je l'ai dit sur l'exemple précédent.

Brady : Ce processus dont vous me parlez, qui date des années 1970, la NP-complétude, était que vous pouvez convertir... c'est presque comme si vous pouviez prendre n'importe quelle preuve et la montrer à un tiers secret et le tiers vous donnera juste un jeton qui dit "oui, vous l'avez prouvé" et ensuite, vous pouvez juste venir me montrer le jeton, "oui, j'ai le jeton, ce qui veut dire que je l'ai prouvé.".

Avi Wigderson : non, non, non, non, non, non - je veux dire, vous devez toujours être sûr que... nous venons de traduire le théorème de Fermat en la 3-coloriabilité de la carte mais vous voudriez toujours, vous savez, voir le 3-coloriage, n'est-ce pas... On ne fait confiance à personne dans ce business, d'accord, je veux dire que le vérificateur ne fait pas confiance, vous savez.

Brady : Nous faisons confiance à cet algorithme, nous faisons confiance à l'algorithme qui crée.

Avi Wigderson : Vous n'avez pas besoin de lui faire confiance, la preuve est très simple, vous pouvez la lire, je veux dire. Elle est si simple que nous l'enseignons aux étudiants de premier cycle et vous pouvez l'enseigner aux étudiants des lycées ; c'est une preuve très très simple d'un état de fait extrêmement puissant, mais c'est un résultat fondamental, c'est absolument une pierre angulaire de mon domaine - mais cela ne nécessite pas de confiance - d'accord, des choses dont nous avons vu des preuves, nous n'avons pas besoin de confiance, nous l'avons vu, oui, c'est donc une simple déclaration

Brady : Cela passe par ce filtre de la NP-complétude qui nous donne la capacité de faire cela.

Avi Wigderson : Vous savez, j'aurais peut-être pu faire un truc avec des enveloppes directement sur le papier de Wiles, je veux dire que je pourrais *(on voit une page de la preuve de Wiles découpée aux ciseaux en différents morceaux qui vont dans les enveloppes)* - ce serait moins colorié ! J'aurais pu en faire une directement sur le produit de deux nombres premiers. Ce concept de NP-complétude est extrêmement puissant et je ne vais pas entrer ici dans son exposition, bien sûr, je veux dire, c'est mon sujet préféré également.

Brady : Revenons au produit de deux nombres premiers, : si Avi de l'entreprise de cryptographie venait me voir, moi, Brady, et me disait "je veux que vous utilisiez les services de mon entreprise et je vous promets que je sais toujours trouver la factorisation d'un nombre qui est un produit de deux nombres premiers", je vous dirais de me le prouver sans dévoiler les secrets de votre société, et alors que feriez-vous ?

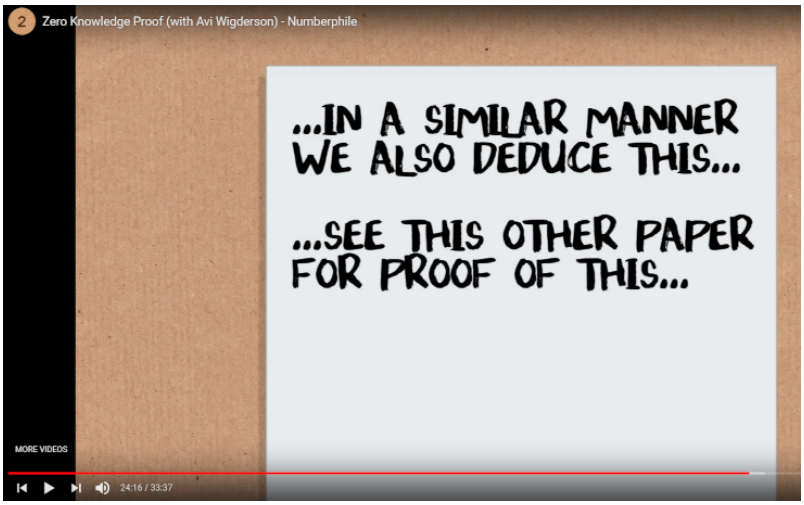
Avi Wigderson : Je traduirais le problème en carte et je vous donnerais une preuve à divulgation nulle que cette carte est 3-coloriable. Et vous sauriez que c'est une déclaration équivalente à la déclaration que j'ai la factorisation de ce nombre qui est le produit de deux nombres premiers.

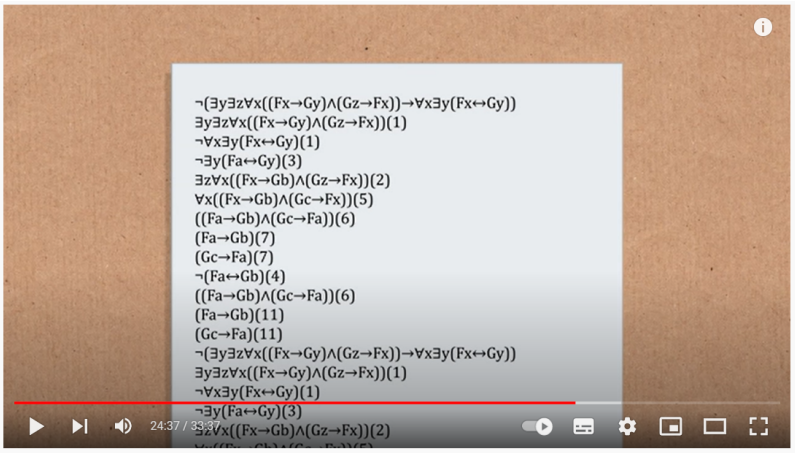
Brady : Mais il faudrait quand même faire la preuve à divulgation nulle de la 3-coloriabilité de la carte, vous ne pouvez pas juste me montrer la carte coloriée avec trois couleurs et me dire "regardez, voici un 3-coloriage de la carte.".

Avi Wigderson : Mais cela révèlerait des informations... En fait, le coloriage vous dirait quels sont les 2 nombres premiers. Ce n'est pas ce que vous souhaitez, je veux dire que tout l'intérêt est que vous n'apprendrez rien du processus - si vous connaissez le 3-coloriage d'une carte en trois couleurs que vous ne connaissiez pas auparavant.

Brady : La carte tricolore ici, que nous créons à partir de toutes nos différentes preuves, celle d'Andrew Wiles, celle de la factorisation d'un nombre qui est un produit de deux nombres premiers, c'est une analogie, n'est-ce pas, ou est-ce que vous pouvez réellement... Est-ce réellement...

Avi Wigderson : Non, non, c'est vrai - je veux dire, les cartes vont probablement être énormes, nous aurons des millions ou des milliards de pays à ce stade. Je ne le suggère pas comme un processus efficace, bien que les gens aient travaillé et en aient fait des versions efficaces, comme je l'ai dit avec les monnaies numériques, il semble que le processus sera commercialisé à certaines fins, absolument, il peut être utilisé, mais il ne pourrait pas être utilisé pour les théorèmes mathématiques. Je veux dire en fait, si vous réfléchissez à la façon dont les preuves mathématiques sont écrites, elles ne sont pas complètement formalisées ; elles utilisent des mots anglais comme "de manière similaire, nous en déduisons également ceci" ou "nous nous référons à un autre article", que vous lisez ou pas, et il peut y avoir des parties incomplètes, des boîtes noires non remplies, et vous savez qu'il peut y avoir des erreurs et de toute façon, vous ne lisez pas forcément tout.





Zero Knowledge Proof (with Avi Wigderson) - Numberphile

Avi Wigderson : Les preuves formelles, comme vous le savez, sont des preuves avec des symboles de la logique du premier ordre et elles sont justes des symboles purs déduits des axiomes ; vous énoncez les axiomes au début et ensuite, vous passez par un enchaînement de déductions. Si Wiles écrivait son article dans cette langue formelle - c'est ce que vous voudriez - alors ce ne seraient pas 500 pages, car la preuve couvre maintenant 200 ou 300 pages - ce seraient un million de pages qu'il vous faudrait et c'est ce type de preuve qui devrait être convertie correctement en carte, vous savez que vous devez être formel à ce sujet. Ce n'est pas l'objectif habituel des preuves à divulgation nulle, leur but principal est la cryptographie et mais je dirais que vous savez certainement qu'intellectuellement, c'est une chose incroyable, une chose impossible, que la cryptographie peut faire, et ce n'est qu'une chose parmi tant d'autres que vous connaissez probablement, comme les signatures numériques, jouer au poker sur votre téléphone - peut-être que vous ne le faites pas... les monnaies numériques, ou vous savez, les élections électroniques,..., vous savez, beaucoup de ces choses sont en quelque sorte impossibles à réaliser dans le monde réel, et vous avez besoin des axiomes de la cryptographie et du savoir-faire de la cryptographie pour les faire fonctionner.

Ces preuves à divulgation nulle sont juste un exemple et vous savez que c'est mon exemple préféré parce que c'est si simple et possible, c'est tout.

La NP-complétude est un point fondamental : ça vous permet, quand vous voulez prouver un théorème comme le fait qu'il existe une preuve à divulgation nulle pour chaque déclaration - et en fait cela se produit dans de nombreuses autres situations en théorie de la complexité - d'avoir un problème particulier avec de belles propriétés et qui capture tous les autres problèmes. C'est très pratique, et vous aurez remarqué que dans ce que je viens de vous montrer pour la preuve à divulgation nulle pour colorier les cartes, j'utilise les propriétés des cartes et j'utilise les propriétés des coloriages... On ne dispose pas de cette possibilité pour le dernier théorème de Fermat, on n'en dispose pas non plus dans le cas de la factorisation d'un nombre produit de deux nombres premiers. Et donc avoir un problème NP-complet si élégant, si beau, et si combinatorialement commode, il était essentiel pour nous de concevoir cela - de concevoir cette preuve...

Brady : Donc c'est comme une lingua franca mathématique d'une certaine manière ?

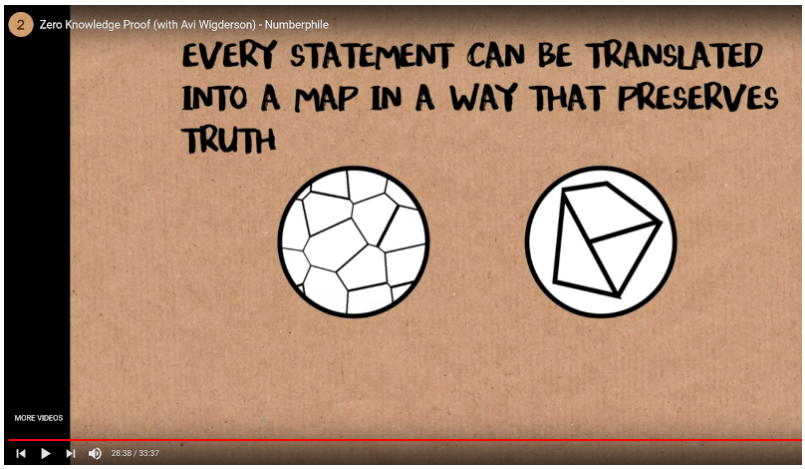
Avi Wigderson : Oui, c'est une langue, absolument, c'est une langue qui est extrêmement utile pour démontrer des choses qui, dans un autre contexte, semblent impossibles. L'utilisation principale de la NP-complétude est juste une démonstration de la difficulté de ce problème - essentiellement ce qu'il dit, il capture tous les autres problèmes, il capture beaucoup de problèmes, des problèmes d'optimisation, donc nous montrons simplement que trouver un 3-coloriage de carte est aussi difficile que de prouver des théorèmes mathématiques en général. Si vous aviez un moyen efficace de 3-colorier toute carte, vous n'auriez pas besoin d'en trouver un pour la preuve du dernier théorème de Fermat par Wiles, vous pourriez simplement exécuter votre traduction de la même façon et exécuter votre algorithme.

Donc les problèmes NP-complets sont des problèmes dont on s'attend à ce qu'ils soient difficiles et P vs NP est la question principale de l'informatique qui consiste à savoir si chacun de ces problèmes a un algorithme efficace - donc en particulier, on peut se demander si prouver des théorèmes mathématiques, disons dans une certaine limite du nombre de pages, c'est facile ou pas ? On ne sait pas que c'est difficile. Il est tout à fait possible qu'il y ait un algorithme vraiment simple, que vous lui donniez une déclaration comme le dernier théorème de Fermat et en une seconde, il crache la réponse "c'est vrai" et fournit même une preuve - c'est la question P vs NP.

Brady : Mais vous m'avez dit précémment que chaque preuve pouvait être convertie...

Avi Wigderson : J'ai dit que si vous aviez une preuve ou un énoncé mathématique, eh bien, je vous ai dit deux choses : que toute déclaration pouvait être convertie en une carte d'une manière qui préserve la vérité - il est donc simplement dit qu'une carte dont on doit trouver un 3-coloriage capture chaque énoncé mathématique, n'est-ce pas, donc pour cette raison prouver une théorie mathématique en général est aussi difficile (ou aussi facile) que trouver le 3-coloriage d'une carte - nous ne savons pas si ce problème

est difficile ou pas. Je vous ai aussi montré que si j'ai un preuve d'un énoncé mathématique, cette preuve peut être traduite en un 3-coloriage de carte.



Brady : Donc n'importe quelle déclaration devient une carte et c'est la preuve qui est un 3-coloriage de la carte.

Avi Wigderson : Oui, si la déclaration est vraie, toute preuve de cette déclaration devient un 3-coloriage de cette carte.

Brady : Donc, si je faisais une fausse déclaration qu'un triangle plat a la somme de ses angles égale à 170 degrés, j'obtiendrais une carte mais mon coloriage serait...

Avi Wigderson : Non, non, il n'y en aurait pas, non, non, il n'y aurait pas de coloriage légal, absolument, oui, s'il n'y avait aucune preuve, il n'y aurait aucun coloriage légal, c'est une traduction bijective, oui.

Brady : C'est une machine incroyable.

Avi Wigderson : C'est une machine incroyable, c'est la NP-complétude, c'est une machine incroyable, c'est le théorème fondamental de Cook-Levin, il date des années 70.

Brady : À quoi ressemble cette machine ? Est-ce que c'est juste une théorie ou est-ce quelque chose ou pas... ?

Avi Wigderson : Une chose géniale, oui ! Non, c'est possible, non, c'est un algorithme, ce n'est pas une équation, c'est un algorithme, ça donne le premier résultat de NP-compétude, donc cela prouve qu'*un* problème, non pas *ce* problème...

Brady : Y a-t-il comme un calculateur ou un programme en ligne dans lequel vous pouvez aller mettre votre déclaration ou votre preuve et appuyer sur un bouton et ça crache...

Avi Wigderson : Oui, c'est ça, vous pouvez le programmer, et ce sera facile, c'est facile à programmer et c'est facile à comprendre. Mais je vais vous dire quelque chose sur sa nature ou sur ce sur quoi cela repose. Pour obtenir un résultat de ce type, vous devez comprendre ce que sont les énoncés mathématiques, ce que sont les preuves mathématiques, quel est le processus de vérification d'une preuve normale. Et la première chose à réaliser est que la vérification est un élément central, ce n'est vraiment pas la preuve mais la vérification de la preuve qui est l'aspect principal des mathématiques.

Brady : Et ici, la vérification était pour moi de faire ouvrir les enveloppes...

Avi Wigderson : Ou même avant, lorsque vous vérifiiez les couleurs si on a laissé les enveloppes ouvertes, oublions temporairement la notion de divulgation nulle, oui. Donc le processus de vérification dans n'importe quel système de preuve en mathématiques est simplement un calcul efficace. C'est un calcul que vous vérifiez : ici, vous vérifiez que les couleurs sont différentes et si c'est écrit logiquement, vous vérifiez que, vous savez, si on a prouvé a et on a prouvé a implique b, on a aussi prouvé b, ce genre de choses, ce sont des choses toutes locales, des choses simples.

Brady : Je pense que c'est une chose très simple mais vraisemblablement en réalité, ces cartes sont gigantesques et trouver deux pays contigus de même couleur pourrait être très difficile à repérer.

Avi Wigderson : non non, mais vous choisissez juste deux pays, ça veut dire que c'est très simple, je veux dire même s'il y a des millions de pays, que je choisis, vous savez, le pays 100 et le pays 273 ou un autre, s'ils ne sont pas voisins, je ne vais pas vous répondre mais s'ils sont voisins, j'ouvrirai les enveloppes, c'est simple, c'est simple même si c'est un grand nombre, il suffit de choisir au hasard les deux nombres ,et ouvrir, maintenant c'est facile mais à nouveau, oubliez juste une seconde les aspects à divulgation nulle, je veux dire parlons juste de NP-complétude, la vérification d'une preuve normale, une preuve mathématique, est un processus de calcul dans lequel le calcul s'effectue localement, il procède par étapes simples qui vérifient que vous connaissez des objets simples ou s'ils savent que vous savez, ils vérifient simplement que deux choses s'ajoutent pour en donner une troisième ou des choses de ce type. Ce que Cook et Levin ont compris, c'est que vous pouvez prendre les processus de vérification des preuves et les convertir - le déclaration et la preuve - et le processus les convertit en ce problème, disons, de 3-coloriage de cartes, qui est un problème simple qui capture tous ces processus et le fait que les calculs soient locaux est un élément essentiel dans cette traduction. Ils partent donc d'une vérification abstraite d'une preuve et ils l'engendrent à partir de cette carte, d'accord ? ! C'est ce que fait l'algorithme - encore une fois, c'est simple, une fois que vous savez ce que vous voulez faire - c'est une excellente idée et un outil incroyablement puissant.

Brady : Est-ce que ces gars gagnent des prix ?

Avi Wigderson : Bien sûr, et ils devraient en gagner davantage.