



Photo credit: Andrea Kane, Institute for Advanced Studies, Princeton, NJ, USA/AbelPrize

السيرة الذاتية لـ "آفي ويجدرسون Avi Wigderson" - المسودة النهائية

مشاكل سهلة، أي ما إذا كانت $P=NP$ أم لا، هذا هو السؤال الأساسي لتعقيد الحوسبة. في الواقع، يعتبر الآن أحد أهم الأسئلة التي لم يتم حلها في جميع الرياضيات.

حقوق © Avi Wigderson 2014. تطورات مذهلة في هذا المجال من خلال البحث عن الدور الذي تلعبه العشوائية في مساعدة الحوسبة. يمكن تسهيل بعض المشكلات الصعبة باستخدام الخوارزميات التي يقوم فيها الحاسوب بسحب القرعة، مثلها تم بقلب العملات المعدنية، أثناة الحوسبة. إذا كانت الخوارزمية تعتمد على تقليب العملة (القرعة)، فهناك دامماً احتمال أن يتسلل خطأ إلى الحل. أظهرت Avi Wigderson، أولًاً مع نوام نيسان Noam Nisan، ولاحقاً مع راسل إمباجيليازو Russell Impagliazzo، أنه بالنسبة لأي خوارزمية سريعة يمكنها حل مشكلة صعبة باستخدام تقليب العملة أي القرعة، توجد خوارزمية سريعة تقريرياً لا تستخدم تقليب العملات، بشرط أن يكون قد تم استيفاء بعض الشروط مسبقاً.

أجرى Avi Wigderson بحثاً في كل مشكلة رئيسية مفتوحة في نظرية التعقيد. من نواح عديدة، تطور المجال حوله، ليس فقط بسبب اتساع اهتماماته، ولكن أيضاً بسبب شخصيته الودودة وحماسه نحو التعاون. شارك في تأليف أوراق مع أكثر من 100 شخص، وأشرف على عدد كبير من منظري التعقيد الشباب. يقول: «أعتبر نفسي محظوظاً بشكل لا يصدق لأنني أعيش في هذا العصر». «[تعقيد الحوسبة] مجال حديث العهد. إنه مجال ديمقراطي للغاية. إنه مجال ودود للغاية، إنه مجال تعاوني للغاية، يتنااسب مع طبيعتي. وبالتالي، إنه مليء بمشاكل والتحديات الفكرية».

عندما بدأ «آفي ويجدرسون Avi Wigderson» مسيرته الأكاديمية في أواخر السبعينيات، كانت نظرية «تعقيد الحوسبة» - التي تهتم بسرعة الخوارزميات وكتفتها - لا تزال في مهدها. يمكن القول إن مساهمة «ويجدرسون Wigderson» في توسيع وتعزيز المجال أكبر من مساهمة أي شخص آخر، وما كان موضوعاً صغيراً أصبح الآن مجالاً راسخاً لكل من الرياضيات وعلوم الحاسوب النظرية. أصبح تعقيد الحوسبة أيضاً موضوعاً مهماً بشكل غير متوقع، حيث أنه يوفر الأساس النظري لأمن شبكة الإنترنت.

ولد Avi Wigderson في مدينة حيفا بإسرائيل عام 1956، والتحق بالجامعةTechnion، المعهد الإسرائيلي للتكنولوجيا، عام 1977. وتخرج بدرجة البكالوريوس. حصل على درجة الدكتوراه في علوم الحاسوب عام 1980. انتقل إلى برينستون Princeton للدراسات العليا، وحصل على درجة الدكتوراه في عام 1983 عن أطروحة دراسات في «التعقيد التوافقي Combinatorial Complexity»، والتي كان ريتشارد ليبتون Richard Lipton يعمل مستشاراً لها. في عام 1986 عاد Avi Wigderson إلى إسرائيل لتولى منصباً في الجامعة العبرية في القدس. تم تعيينه في المنصب في العام التالي وأصبح أستاداً في عام 1991.

في السبعينيات، صاغ منظرو الحاسوب أفكاراً أساسية معينة حول طبيعة الحوسبة، ولا سيما مفاهيم P و NP . إن P هي مجموعة المشكلات التي يمكن لأجهزة الحاسوب حلها بسهولة، على سبيل المثال، في بضع ثوان، بينما يعني NP أيضاً على المشكلات التي يصعب على أجهزة الحاسوب حلها، مما يعني أن الطرق المعروفة لا يمكنها العثور على الإجابة إلا بعد ملايين من السنين على سبيل المثال. مسألة ما إذا كان يمكن اختزال كل هذه المشكلات الصعبة إلى

عن أي معرفة تتجاوز صحة هذا الادعاء، مثل مثال اثنين من أصحاب الملايين اللذين يريدان إثبات من هو الأكثر ثراءً دون أن يخبر أي منها عن مقدار إملاك الذي يمتلكه. أظهر «ويجدرسون Wigderson»، مع أوديد جولدريتش Oded Goldreich و«سيلفيو ميكالي Silvio Micali»، أنه يمكن استخدام براهين الإثبات بلا كشف لإثبات أي نتيجة عامة حول البيانات السرية، سراً. فقط قل، على سبيل المثال، أنك تريدين أن تثبت لشخص ما أنك قد تمكن من إثبات مبرهنة رياضية، لكنك لا تريدين الكشف عن أي تفاصيل حول كيفية قيامك بذلك، سيسمح لك «الإثبات بلا كشف» للإثباتات بلا كشف «Zero-knowledge proofs» بالقيام بذلك.

في عام ١٩٩٤، فاز «ويجدرسون Wigderson» بـ«جائزة رولف نيفانليننا Rolf Nevanlinna Prize» لعلوم الحاسوب، والتي منحها الاتحاد الدولي للرياضيات مرة كل أربع سنوات. ومن بين جوائزه العديدة الأخرى «جائزة Gödel» لعام ٢٠٠٩ و«جائزة Knuth» لعام ٢٠١٩.

«ويجدرسون Wigderson» متزوج من إدنا Edna التي التقى بها في معهد «التخنيون Technion» والتي تعمل في قسم الحاسوب في معهد الدراسات المتقدمة. لديهم ثلاثة أبناء وحفيدان.

مصدر الاقتباس: مؤسسة الفائزين بجائزة هيدلبرج Heidelberg Laureate، مقابلة مع آفي ويجدرسون Avi Wigderson، ٢٠١٧.

في عام ١٩٩٩، انضم «ويجدرسون Wigderson» إلى معهد الدراسات المتقدمة (IAS) في برينستون حيث يعمل منذ ذلك الحين. في حدث الاحتفال بعيد ميلاد «ويجدرسون Wigderson» الستين، في عام ٢٠١٦، قال مدير معهد الدراسات المتقدمة (IAS) روبيت ديجكgraaf Robbert Dijkgraaf إنه قد أطلق عصراً ذهبياً لعلوم الحاسوب النظرية في المعهد.

يُعرف «ويجدرسون Wigderson» بقدرته على رؤية الروابط بين المناطق التي لا علاقة لها فيما بينها في ظاهرها. لقد عمق الروابط بين الرياضيات وعلوم الحاسوب. أحد الأمثلة هو «منتج الرسم البياني المتعرج zig-zag graph product»، الذي طوره مع عمر راينجولد Omer Reingold و«ساليل فادهان Salil Vadhan»، والذي يربط بين نظرية المجموعة ونظرية الرسم البياني ونظرية التعقيد، وله تطبيقات مدهشة مثل أفضل السبل للخروج من الم塔هة.

إن أهم تطبيق في الوقت الحاضر لنظرية التعقيد هو التشفير، والذي يستخدم لتأمين المعلومات على شبكة الإنترنت مثل أرقام بطاقات الائتمان وكلمات المرور. يجب على الأشخاص الذين يصممون أنظمة التشفير، على سبيل المثال، التأكد من أن مهمة فك تشفير نظمهم هي مشكلة NP، أي مشكلة قد تستغرق أجهزة الحاسوب ملايين السنين لتحقيقها. في وقت مبكر من حياته المهنية، قدم «ويجدرسون Wigderson» مساهمات أساسية لمفهوم جديد في التشفير، والإثبات بلا كشف، والذي يتم استخدامه الآن بعد أكثر من ٣٠ عاماً في «تقنية سلسلة التكيل Blockchain technology». في «الإثبات بلا كشف Zero-knowledge proofs»، يجب أن يثبت شخصان ادعاءً دون الكشف

