



THE ABEL PRIZE 2021

قررت الأكاديمية النرويجية للعلوم والآداب
منح جائزة أبيل لعام ٢٠٢١ إلى

و السيد آفي ويجدرسون Avi Wigderson
معهد الدراسات المتقدمة، برينستون، الولايات المتحدة
الأمريكية

السيد لزلو لوفاز László Lovász، جامعة
جامعة أوتفوش لوراند Eötvös Loránd
بودابست، المجر

تكريماً "لمساهمتهما التأسيسية في علوم الحاسوب النظرية والرياضيات المتقطعة، ودورهما الرائد في تشكيل هذه الميادين
في المجالات المركزية للرياضيات الحديثة"

تحديات جديدة، وفتحت اتجاهات جديدة للبحث، وحلّت مشاكل مفتوحة
مهمة في الرياضيات البحتة والتطبيقية.

قاد "لزلو لوفاز László Lovász" و"آفي ويجدرسون Avi Wigderson" القوى
في هذه التطورات على مدى العقود الماضية. يتقاطع عملهما في نواح عديدة،
وعلى وجه الخصوص، قدّم كلاهما مساهمات أساسية لفهم العشوائية في
الحوسبة وفي استكشاف حدود كفاءة الحوسبة.

جنباً إلى جنب مع "أرجن لينسترا Arjen Lenstra" و"هنريك لينسترا Hendrik
Lenstra"، طور "لزلو لوفاز László Lovász" خوارزمية LLL لتقليل الشبكية.
بالنظر إلى شبكية (شبكة) ذات أبعاد عالية، تجد هذه الخوارزمية أساساً لطيفاً
متعامداً تقريبياً. بالإضافة إلى العديد من التطبيقات مثل خوارزمية لتحليل
منطقي متعدد الحدود، فإن خوارزمية LLL هي الأداة المفضلة لمحللي التشفير،
حيث نجحت في كسر العديد من أنظمة التشفير المقترحة. من المثير للدهشة
أن تحليل خوارزمية LLL يُستخدم أيضاً لتصميم وضمان أمان أنظمة التشفير
الأحدث القائمة على الشبكية والتي يبدو أنها تصمد أمام الهجمات حتى
بواسطة أجهزة الحاسوب الكمومية (Quantum computers). بالنسبة لبعض
بدائل التشفير الغريبة، مثل التشفير المتماثل الشكل، فإن التركيبات الوحيدة
المعروفة هي عبر أنظمة التشفير المستندة إلى الشبكية.

تعد خوارزمية LLL واحدة فقط من بين العديد من مساهمات "لوفاز Lovász"
البصيرة. لقد أثبت أن برهان ليما المحلي Local Lemma، أداة فريدة لإظهار

علم الحاسوب النظري (TCS) هو دراسة قوة وحدود الحوسبة. تعود جذورها
إلى الأعمال التأسيسية "لكورت جودل Kurt Gödel"، و"ألونزو تشرتش
Alonzo Church"، و"ألان تورينج Alan Turing"، و"جون فون نيومان John
von Neumann"، مما أدى إلى تطوير أجهزة حاسوب مادية حقيقية. يحتوي
علم الحاسوب النظري (TCS) على اثنين من التخصصات الفرعية التكميلية:
تصميم الخوارزمية الذي يطور طرقاً فعالة للعديد من مشكلات الحوسبة؛
وتعقيد الحوسبة، الذي يظهر قيوداً متأصلة في كفاءة الخوارزميات. كان مفهوم
الخوارزميات ذات الزمن المتعدد الحدود التي طرحها "ألان كوبهام Alan
Cobham" و"جاك إدموندز Jack Edmonds" وآخرين في الستينيات من القرن
الماضي، وحداثة $P \neq NP$ الشهيرة لـ"ستيفن كوك Stephen Cook" و"ليونيد
ليفين Leonid Levin"، و"ريتشارد كارب Richard Karp" تأثيراً قوياً على
المجال وعلى عمل "لوفاز Lovász" و"يجدرسون Wigderson".

بصرف النظر عن تأثيره الهائل على علوم وممارسات الكمبيوتر الأوسع نطاقاً،
يوفر علم الحاسوب النظري (TCS) أسس التشفير، وله الآن تأثير متزايد على
العديد من العلوم الأخرى مما يؤدي إلى رؤى جديدة فيها من خلال "استخدام
عدسة حوسبة" "Employing a computational lens". تعتبر الهياكل المنفصلة
مثل الرسوم البيانية والأوتار والتباديل أساسية بالنسبة لعلم الحاسوب النظري
(TCS)، والرياضيات المتقطعة بشكل طبيعي وعلم الحاسوب النظري (TCS)
مجالات متحالفة بشكل وثيق. بينما استفاد كلا المجالين بشكل كبير من
مجالات الرياضيات التقليدية، كان هناك تأثير متزايد في الاتجاه العكسي أيضاً.
لقد حفزت تطبيقات ومفاهيم وتقنيات علم الحاسوب النظري (TCS) ظهور

مماثلة؛ علاوة على ذلك، فإن إلغاء العشوائية هو عام وعالمي، دون الاعتماد على التفاصيل الداخلية للخوارزمية العشوائية.

هناك طريقة أخرى للنظر إلى هذا العمل وهي المقايضة بين الصلابة مقابل العشوائية: إذا كانت هناك مشكلة صعبة بدرجة كافية، فيمكن محاكاة العشوائية بواسطة خوارزميات حتمية فعالة. يثبت العمل اللاحق لـ "Wigderson" مع "إمباجليازو Impagliazzo" و"فالنتين كابانيتس Valentine Kabanets" العكس: الخوارزميات الحتمية الفعالة حتى بالنسبة لمشاكل محددة مع الخوارزميات العشوائية المعروفة قد تعني أنه لا بد من وجود مثل هذه المشكلة الصعبة.

يرتبط هذا العمل ارتباطاً وثيقاً بتركيبات الكائنات شبه العشوائية (العشوائية المظهر). قامت أعمال "Wigderson" ببناء مولدات شبه عشوائية تقوم بتحويل عدد قليل من البتات العشوائية حقا إلى العديد من البتات شبه العشوائية، والمستخرجات التي تستخرج بتات عشوائية مثالية تقريباً من مصدر غير كامل للعشوائية، ورسوم "رامساي Ramsey" البيانية، والرسوم البيانية الموسعة المتناثرة وما زالت تتمتع بتوصيلية عالية. مع "عمر راينجولد Omer Reingold" و"سالي فادهان Salil Vadhan"، قدم منتج الرسم البياني المتعرج، مما أعطى طريقة أولية لبناء الرسوم البيانية المتوسعة، وألهم إثبات اندماجي لمبرهنة PCP بواسطة "إيريت دينور Irit Dinur" وخوارزمية فعالة للذاكرة لمشكلة اتصال الرسم البياني بواسطة "راينجولد Reingold". يعطي هذا الأخير طريقة للتنقل عبر متاهة كبيرة مع تذكر هوية عدد ثابت فقط من نقاط التقاطع في المتاهة!

تتضمن مساهمات "Wigderson" الأخرى أدلة على عدم المعرفة التي توفر أدلة على الادعاءات دون الكشف عن أي معلومات إضافية إلى جانب صحة المطالبات، وحدود أقل على كفاءة بروتوكولات الاتصال والدوائر وأنظمة الإثبات الرسمية.

بفضل الدور القيادي الذي لعبه "لزلو لوفاز László Lovász" و"آفي ويجدرسون Avi Wigderson"، أصبحت الرياضيات المتقطعة ومجال علوم الحاسوب النظري الصغير نسبياً مناطق مركزية في الرياضيات الحديثة.

وجود كائنات اندماجية نادرة، على عكس الطريقة الاحتمالية القياسية المستخدمة عند وجود الكائنات بكثرة. إلى جانب "مارتن جروتشل Martin Grötschel" و"ليكس شريفير Lex Schrijver"، أظهر كيفية حل البرامج شبه المحددة بكفاءة، مما أدى إلى ثورة في تصميم الخوارزمية. ساهم في نظرية السير العشوائي مع تطبيقات على مسائل المحيط في حساب التغيرات الإقليدية وحسابات الحجم التقريبي للأجسام عالية الأبعاد. أعطت ورقته البحثية مع "يورليل فايج Uriel Feige" و"شافي جولدفاشر Shafi Goldwasser" و"صمويل صافرا Shmuel Safra" و"ماريو سيزيجيدي Mario Szegedy" حول البراهين قابلة التحقق منها عن طريق الاحتمالية والتي أدت إلى وضع نسخة مبكرة من مبرهنة PCP، وهي نتيجة مؤثرة للغاية تظهر أنه يمكن التحقق من صحة البراهين الرياضية بشكل احتمالي، بدرجة عالية من الثقة، من خلال القراءة فقط لعدد قليل من الرموز! بالإضافة إلى ذلك، قام أيضاً بحل مشكلات طويلة الأمد مثل تحديث الرسم البياني المثالي، وحدسية "كنيسر Kneser"، وتحديد قدرة "شانون Shannon" للرسم البياني الخماسي، وفي السنوات الأخيرة، طور نظرية حدود الرسم البياني (في العمل المشترك مع "كريستيان بورجس Christian Borgs"، و"جنيفير شاييس Jennifer Chayes" و"ليكس شريفير Lex Schrijver" و"فيرا سوس Vera Sós" و"بالازس سيزيجيدي Balázs Szegedy" و"كاتالين فيسزترجومبي Katalin Vesztergombi"). يربط هذا العمل بين عناصر نظرية الرسم البياني القصوى، ونظرية الاحتمالات، والفيزياء الإحصائية.

قدم "آفي ويجدرسون Avi Wigderson" مساهمات واسعة وعميقة في جميع جوانب تعقيد الحوسبة، وخاصة دور العشوائية في الحوسبة. الخوارزمية العشوائية هي سحب القرعة برمي العملة المعدنية لحوسبة حل يكون صحيحاً وذات احتمالية عالية. على مدى عقود، اكتشف الباحثون خوارزميات قطعية للعديد من المشكلات التي لم تكن معروفة لها سابقاً سوى خوارزمية عشوائية. تعد الخوارزمية القطعية لاختبار أولية العدد، التي أجراها "أجراوال Agrawal" و"كايال Kayal" و"ساكينا Saxena"، مثلاً صارخاً على مثل هذه الخوارزمية غير العشوائية. تثير نتائج إزالة العشوائية هذه مسألة ما إذا كانت العشوائية ضرورية حقاً. في الأعمال التي جرت مع "لزلو باباي László Babai" و"لانس فورتنوو Lance Fortnow" و"نوام نيسان Noam Nisan" و"راسل إمباجليازو Russell Impagliazzo"، أثبت "Wigderson" أنه من المحتمل أن تكون الإجابة سلبية. بشكل رسمي، أظهروا أن الحدسية الحاسوبية تنطوي على أن $P = BPP$ ، ومماثلةً روحياً لحدسية $P \neq NP$. هذا يعني أن كل خوارزمية عشوائية يمكن فصلها عن العشوائية وتحويلها إلى خوارزمية حتمية ذات كفاءة