THE ABEL PRIZE 2021

La Academia Noruega de Ciencias y Letras ha resuelto conceder el Premio Abel 2021 a

László Lovász

de la Universidad Eötvös Loránd de Budapest, Hungría y

Avi Wigderson

del Instituto de Estudios Avanzados de Princeton, EE. UU.,

«por sus contribuciones fundamentales a la ciencia computacional teórica y a las matemáticas discretas, y su destacado papel en el desarrollo como campo central de las matemáticas modernas».

La ciencia computacional teórica (TCS por sus siglas en inglés) es el estudio del poder y las limitaciones de la computación. Sus orígenes se remontan a los trabajos fundamentales de Kurt Gödel, Alonzo Church, Alan Turing y John von Neumann, lo que llevó al desarrollo de auténticos ordenadores físicos. La TCS se compone de dos subdisciplinas complementarias: el diseño de algoritmos que desarrollan métodos eficientes para una gran variedad de problemas computacionales y la complejidad computacional que muestra las limitaciones inherentes en la eficiencia de los algoritmos. El concepto de algoritmos de tiempo polinómico presentado en los años sesenta por Alan Cobham, Jack Edmonds y otros, y la famosa conjetura P≠NP de Stephen Cook, Leonid Levin y Richard Karp tuvieron gran impacto en este campo y en el trabajo de Lovász y Wigderson.

Además del enorme impacto en las ciencias de la computación en general y en la práctica, la TCS proporciona la base de la criptografía y actualmente tiene una creciente influencia en muchas otras ciencias, lo que lleva a adoptar nuevas perspectivas con el «empleo de una lente computacional». Estructuras discretas, como los grafos, las secuencias y las permutaciones, son fundamentales para la TCS y, de forma natural, las matemáticas discretas y la TCS han estado estrechamente vinculadas. Mientras estos dos campos se han beneficiado en gran medida de áreas de las matemáticas más tradicionales, también ha habido una creciente influencia en la dirección opuesta. Las aplicaciones, los conceptos y las técnicas de la TCS han dado lugar a nuevos retos, han permitido nuevos enfoques de investigación y han resuelto importantes problemas abiertos en las matemáticas puras y aplicadas.

László Lovász y Avi Wigderson han liderado estos avances durante las últimas décadas. Sus trabajos se entrelazan en muchos sentidos y, en particular, los

dos han contribuido en gran medida a entender la aleatoriedad en computación y a explorar los límites de la computación eficiente.

De la mano de Arjen Lenstra y Hendrik Lenstra, László Lovász desarrolló el algoritmo de simplificación de retículos LLL. Para un retículo entero en dimensiones altas, el algoritmo LLL produce una buena base casi ortogonal. Además de tener varias aplicaciones, como un algoritmo para factorizar polinomios de coeficientes racionales, el algoritmo LLL es una herramienta preferida en criptoanálisis, rompiendo con éxito otros sistemas de encriptación. Sorprendentemente, el análisis del algoritmo LLL también se utiliza para diseñar y garantizar la seguridad de los criptosistemas más recientes basados en retículos que parecen resistir a ataques incluso de ordenadores cuánticos. Para algunas encriptaciones exóticas primitivas, como la homomórfica, las únicas construcciones conocidas son a través de estos criptosistemas basados en retículos.

El algoritmo LLL es una de las muchas contribuciones visionarias de Lovász. También es el autor del «Lema local», una herramienta única para demostrar la existencia de objetos combinatorios cuya existencia es poco frecuente, a diferencia del método de probabilidad estándar empleado cuando los objetos existen en abundancia. Junto con Martin Grötschel y Lex Schrijver, mostró cómo resolver programas semidefinidos de forma eficiente, lo que produjo una revolución en el diseño de algoritmos. Contribuyó a la teoría de los paseos aleatorios con aplicaciones a problemas isoperimétricos euclídeos y al cálculo del volumen aproximado de cuerpos de grandes dimensiones. Su trabajo en colaboración con Uriel Feige, Shafi Goldwasser, Shmuel Safra, y Mario Szegedy sobre demostraciones verificables probabilísticamente ofreció una primera versión del teorema PCP, ¡un resultado muy influyente sobre la posibilidad de verificar con alta probabilidad demostraciones matemáticas leyendo únicamente un pequeño número de signos! Además, resolvió antiguos problemas como la conjetura del grafo perfecto, la conjetura de Kneser, determinando la capacidad de Shannon del grafo pentagonal y, en los últimos años, desarrolló la teoría de grafos límite (en colaboración con Christian Borgs, Jennifer Chayes, Lex Schrijver, Vera Sós, Balázs Szegedy, y Katalin Vesztergombi). Este trabajo combina elementos de teoría de grafos extremales, teoría de la probabilidad y física estadística.

Avi Widgerson ha hecho enormes y exhaustivas contribuciones en todos los aspectos de la complejidad computacional, especialmente en el papel de la aleatoriedad en la informática. Un algoritmo aleatorizado es aquel que lanza monedas para calcular una solución correcta con gran probabilidad. Durante décadas, los investigadores descubrieron algoritmos deterministas para varios problemas para los cuales solo se conocía un algoritmo aleatorizado. El algoritmo determinista para pruebas de primalidad de Agrawal, Kayal y Saxena es un llamativo ejemplo de tal algoritmo desaleatorizado. Estos resultados de la desaleatorización plantean la pregunta de si la aleatoriedad es realmente esencial. En trabajos con László Babai, Lance Fortnow, Noam Nisan y Russell Impagliazzo, Wigderson demostró que la respuesta es probablemente negativa. Formalmente, mostraron una conjetura computacional, similar en espíritu al de la conjetura P≠NP, que implica que P=BPP. Esto significa que todo algoritmo aleatorizado puede desaleatorizarse y convertirse en uno determinista de eficiencia comparable; además la desaleatorización es genérica y universal, independientemente de los detalles internos del algoritmo aleatorizado.

Otra forma de interpretar este trabajo es como un equilibrio entre complejidad y aleatoriedad: si existe un problema lo suficientemente complejo, entonces la aleatoriedad se puede simular mediante algoritmos deterministas eficientes. Trabajos posteriores de Wigderson con Impagliazzo y Valentine Kabanets demuestran el recíproco: algoritmos eficientes deterministas incluso para problemas específicos con algoritmos aleatorizados conocidos implican la existencia de tales problemas complejos.

Este trabajo está estrechamente ligado a la construcción de objetos pseudoaleatorios (que parecen aleatorios). Los trabajos de Wigderson han construido generadores pseudoaleatorios que convierten pocos bits realmente aleatorios en muchos bits pseudoaleatorios, extractores que extraen bits casi perfectamente aleatorios de una fuente de aleatoriedad imperfecta, grafos de Ramsey y grafos de expansión dispersos y, aun así, tienen una gran conectividad. Con Omer Reingold y Salil Vadhan introdujo el producto de grafos en zigzag, proporcionando un método elemental para construir grafos de expansión e inspirando la prueba combinatoria del teorema PCP por Irit Dinur y un algoritmo eficiente de memoria para el problema de Reingold de conectividad de grafos. Este último ofrece un método para navegar por un amplio laberinto recordando solamente la identidad de un número constante de puntos de intersección.

Otras contribuciones de Wigderson incluyen las demostraciones de conocimiento cero que presentan verificaciones para enunciados sin revelar ninguna

información adicional aparte de la validez del enunciado, y cotas inferiores de la eficiencia de los protocolos de comunicación, los circuitos y los sistemas de demostraciones formales.

Gracias al liderazgo de Lovász y Wigderson, las matemáticas discretas y el relativamente joven campo de la ciencia computacional teórica se han consolidado como áreas centrales de las matemáticas modernas.