



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

## Biografía de Avi Wigderson

Cuando Avi Wigderson inició su carrera académica a finales de los años 70, la teoría de la «complejidad computacional», que trata sobre la velocidad y eficiencia de los algoritmos, daba sus primeros pasos. La contribución de Wigderson para ampliar y ahondar en este campo es posiblemente superior a la de cualquier otra persona, y lo que entonces era una materia joven se ha convertido en un campo consolidado tanto de las matemáticas como de la ciencia computacional teórica. La complejidad computacional ha cobrado además una importancia inesperada, al aportar la base teórica para la seguridad en Internet.

Wigderson nació en Haifa, Israel, en 1956. Entró en el Technion, el Instituto Tecnológico de Israel, en 1977 y se graduó en Ciencias de la Computación en 1980. Se trasladó a Princeton para sus estudios de posgrado, doctorándose en 1983 con la tesis *Studies in Combinatorial Complexity* (Estudios de complejidad combinatoria), teniendo como consejero a Richard Lipton. En 1986 Wigderson regresó a Israel para ocupar un puesto en la

Universidad Hebrea de Jerusalén. Obtuvo la plaza en propiedad al año siguiente y se convirtió en profesor titular en 1991.

En la década de 1970, los teóricos computacionales formularon ciertas ideas fundamentales sobre la naturaleza de la computación, en particular las nociones de P y NP. P es el conjunto de problemas que los computadores pueden resolver fácilmente, en unos segundos, mientras que NP incluye también los problemas que los computadores tienen dificultad para resolver, lo que quiere decir que los métodos conocidos tardarían millones de años en encontrar la respuesta. La cuestión de si todos esos problemas difíciles se pueden reducir a problemas fáciles, es decir, si  $P = NP$ , constituye la cuestión fundamental de la complejidad computacional. De hecho, actualmente se considera una de las cuestiones sin resolver más importantes de todas las matemáticas.

Wigderson logró asombrosos avances en este ámbito investigando el papel de la aleatoriedad



como ayuda para la computación. Algunos problemas difíciles pueden hacerse fáciles utilizando algoritmos en los que el ordenador se la juega a cara o cruz durante la computación. No obstante, si un algoritmo se basa en jugársela a cara o cruz, existe siempre la posibilidad de que pueda colarse un error en la solución. Wigderson, primero junto con Noam Nisan y más tarde con Russell Impagliazzo, demostró que, por cualquier algoritmo rápido capaz de resolver un problema difícil a cara o cruz, existe un algoritmo casi igual de rápido que no utiliza el método a cara o cruz, siempre que se cumplan ciertas condiciones.

Wigderson ha desarrollado investigaciones en los principales problemas abiertos en la teoría de la complejidad. En muchos sentidos, este campo ha crecido en torno a él, no solo por la amplitud de sus intereses, sino también gracias a su personalidad accesible y su entusiasmo por las colaboraciones. Ha sido coautor de artículos con más de 100 personas y ha asesorado a un gran número de jóvenes teóricos de la complejidad. «Me considero increíblemente afortunado de vivir en esta época», ha afirmado. «[La complejidad computacional] es un campo joven. Es un campo muy democrático. Es un campo muy amigable, muy colaborativo, que se ajusta bien a mi naturaleza. Y desde luego, está repleto de problemas y retos intelectuales».

En 1999 Wigderson se incorporó al Instituto de Estudios Avanzados (IAS) de Princeton, donde ha permanecido desde entonces. En un acto para celebrar el 60 cumpleaños de Wigderson en 2016, el director del IAS, Robbert Dijkgraaf, declaró que este había inaugurado una edad de oro de la ciencia computacional teórica en el instituto.

Wigderson es conocido por su capacidad para descubrir vínculos entre ámbitos aparentemente no relacionados. Ha profundizado en las conexiones entre las matemáticas y la ciencia computacional. Un ejemplo de ello es el «producto de grafos en zigzag», desarrollado por él junto con Omer Reingold y Salil Vadhan, que vincula la teoría de grupos, la teoría de grafos y la teoría de la complejidad, y que tiene sorprendentes aplicaciones, como el mejor modo de salir de un laberinto.

La aplicación más importante a día de hoy de la teoría de la complejidad es la criptografía, utilizada para proteger información en Internet, como los números de tarjetas de crédito y las contraseñas. Las personas que diseñan criptosistemas, por

ejemplo, deben asegurarse de que la tarea de descodificar su sistema sea un problema NP, es decir, un problema que los computadores tardarían millones de años en resolver. A principios de su carrera Wigderson realizó contribuciones fundamentales a un nuevo concepto en criptografía: la demostración de conocimiento cero, que más de 30 años después se utiliza en la tecnología de cadena de bloques. En una demostración de conocimiento cero, dos personas deben demostrar una afirmación sin revelar ningún conocimiento más allá de la validez de dicha afirmación, como el ejemplo de los dos millonarios que quieren demostrar quién es más rico sin decir ninguno de los dos cuánto dinero tiene. Wigderson, junto con Oded Goldreich y Silvio Micali, demostró que las demostraciones de conocimiento cero pueden servir para demostrar, en secreto, cualquier resultado público sobre datos secretos. Pongamos, por ejemplo, que queremos demostrar a alguien que hemos demostrado un teorema matemático, pero no queremos revelar detalles de cómo lo hemos hecho. Podemos conseguirlo con una demostración de conocimiento cero.

En 1994, Wigderson obtuvo el Premio Rolf Nevanlinna de ciencia computacional, otorgado por la Unión Matemática Internacional cada cuatro años. Entre sus muchos otros premios se encuentran el Premio Gödel 2009 y el Premio Knuth 2019.

Wigderson está casado con Edna, a la que conoció en el Technion y que trabaja en el departamento de computación del Instituto de Estudios Avanzados. Tienen tres hijos y dos nietos.

*Fuente de la cita: Heidelberg Laureate Foundation Portraits, entrevista con Avi Wigderson, 2017.*

