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

Avi Wigderson életpályája

Amikor az 1970-es évek végén Avi Wigderson tudományos karrierje elindult, a „számítási bonyolultság” elmélete – amely az algoritmusok sebességével és hatékonyságával foglalkozik – még gyerekcipőben járt. Wigderson alighanem mindenki másnál többet tett e tudományág bővítéséért és elmélyítéséért, és az akkoriban épp csak kialakulóban levő tárgykör mára már a matematika és az elméleti számítógép-tudomány elismert területe. Ráadásul a számítási bonyolultság jelentősége váratlanul megnőtt, és ma már az internetbiztonság elméleti alapjaként tekintünk rá.

Wigderson 1956-ban született az izraeli Haifában. 1977-ben felvételt nyert a Technionba, az Izraeli Technológiai Intézetbe, ahol 1980-ban számítógép-tudományi diplomát szerzett. Posztgraduális tanulmányai miatt Princetonba költözött, PhD fokozatát 1983-ban szerezte a *Tanulmányok a kombinatorikai bonyolultság terén* (*Studies in Combinatorial Complexity*) című disszertációval, konzulense Richard Lipton volt. 1986-ban Wigderson visszatért Izraelbe, és a jeruzsálemi Héber Egyetemen helyezkedett el. A következő évben segédtanári állást kapott, majd 1991-ben egyetemi tanár lett.

Az 1970-es években a számítástudomány elméletével foglalkozó szakemberek alapvető gondolatokat fogalmaztak meg a számítás természetéről, nevezetesen a P és az NP fogalmát. A P az a problémakör, amelyet a számítógépek akár néhány másodperc alatt is könnyedén meg tudnak oldani, míg az NP olyan problémákat is tartalmaz, amelyek alaposan feladják a leckét a gépeknek, vagyis az ismert módszerekkel adott esetben több millió évbe telhet megtalálniuk a választ. A számítási bonyolultság alapkérdése az, hogy ezek a nehéz problémák könnyen megoldhatóvá tehetők-e, azaz igaz-e, hogy P = NP? A matematika világában jelenleg ezt tekintik az egyik legfontosabb, megoldásra váró kérdésnek.

Wigderson óriási előrelépést tett ezen a területen azzal, hogy a véletlenszerűség szerepét vizsgálta a számítás elősegítésében. Egyes nehéz problémák megoldása megkönnyíthető olyan algoritmusokkal, amelyek alkalmazásakor a számítógép „pénzfeldobásra" hagyatkozik a számítás során. Ha azonban egy algoritmus pénzfeldobásra épül, akkor mindig fennáll annak a lehetősége, hogy hiba csúszik a megoldásba. Wigderson először Noam Nisannal, majd később Russell Impagliazzóval kimutatta, hogy minden olyan gyors algoritmus esetében, amely képes pénzfeldobással megoldani egy nehéz problémát, létezik egy majdnem olyan gyors algoritmus, amely bizonyos feltételek teljesülése esetén nem szorul rá a pénzfeldobásos módszerre.

Wigderson kutatásai a bonyolultságelmélet minden jelentősebb, megoldatlan problémáját felölelték. Az ezen a területen elért fejlődés sok szempontból az ő személye köré összpontosult, nemcsak széles körű érdeklődése, de megközelíthető személyisége és az együttműködés iránti lelkesedése miatt is. Jóval több mint 100 tanulmánynál működött közre társszerzőként, és számos fiatal bonyolultságelméleti szakembert mentorált. „Hihetetlenül szerencsésnek tartom magam, hogy ebben a korban élhetek" – állítja. „A [számítási bonyolultság] fiatal terület. Nagyon demokratikus terület. Rendkívül barátságos, együttműködő, a természetemnek megfelelő terület. Ráadásul az is tény, hogy intellektuális problémák és kihívások sokaságát kínálja."

1999-ben Wigderson belépett a princetoni Fejlett Tanulmányok Intézetéhez (IAS), ahol azóta is tevékenykedik. 2016-ban a Wigderson hatvanadik születésnapját ünneplő rendezvényen az IAS igazgatója, Robbert Dijkgraaf úgy fogalmazott, hogy Wigderson érkezésével az elméleti számítógép-tudomány aranykora vette kezdetét az intézetben.

Wigderson arról ismert, hogy képes meglátni az összefüggéseket az egymástól látszólag független területek között is. Elmélyítette a matematika és a számítógép-tudomány kapcsolatát. Ennek egyik példája az Omer Reingolddal és Salil Vadhannal közösen kifejlesztett „cikkcakk-gráfszorzat", amely összekapcsolja a csoportelméletet, a gráfelméletet és a bonyolultságelméletet, és meglepő célokra alkalmazható, így például segíthet meghatároznunk a legjobb módját, hogyan találjunk ki egy labirintusból.

Jelenleg a bonyolultságelmélet legfontosabb alkalmazási területe a kriptográfia, amelyet az interneten tárolt információk, például hitelkártyaszámok és jelszavak biztosítására használnak. A kriptorendszerek tervezőinek például meg kell győződniük arról, hogy a rendszerük dekódolásának feladata NP-probléma, vagyis olyan, amelyet a számítógépek csak évmilliók alatt tudnak megoldani. Pályafutása elején Wigderson meghatározó szerepet játszott a kriptográfia új koncepciója, a nullaismeretű bizonyítás megalkotásában, amelyet most, több mint 30 év elteltével a blokklánc-technológiában alkalmaznak. A nullaismeretű bizonyítás esetében két embernek anélkül kell igazolnia egy állítást, hogy az állítás érvényességén túlmutató bármilyen ismereteket tárnának fel: ilyen eset például a két milliomosé, akik úgy akarják bebizonyítani a másiknak, hogy gazdagabbak nála, hogy közben nem árulják el, mekkora vagyonnal is rendelkeznek valójában. Wigderson Oded Goldreichhel és Silvio Micalival együtt kimutatta, hogy a nullaismeretű bizonyítás segítségével a titkos adatokkal kapcsolatos bármely nyilvános eredmény bizonyítható a titkosság megőrzése mellett. Tegyük fel például, hogy be akarjuk bizonyítani valakinek, hogy bebizonyítottunk egy matematikai tételt, de nem akarunk részleteket elárulni arról, hogyan csináltuk – a nullaismeretű bizonyítással ez is lehetséges.

1994-ben Wigderson elnyerte a számítógép-tudományi Rolf Nevanlinna-díjat, amelyet a Nemzetközi Matematikai Unió négyévente ítél oda. Számos egyéb díja között szerepel a 2009-es Gödel-díj és a 2019-es Knuth-díj.

Wigderson felesége Edna, akivel a Technionban ismerkedett meg, és aki a Fejlett Tanulmányok Intézetének számítástechnikai osztályán dolgozik. Három gyermekük és két unokájuk van.

Forrás: Heidelberg Alapítványdíjasok portréi, interjú Avi Wigdersonnal, 2017.