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

En biografi over Avi Wigderson

Da Avi Wigderson begynte sin akademiske karriere i slutten av 1970-årene, var teorien om "datakompleksitet" – som befatter seg med algoritmers hastighet og effektivitet – bare i sin barndom. Det kan hevdes at Wigderson har bidratt mer til å gjøre dette feltet både bredere og dypere enn noen annen enkeltperson, og det som en gang var et nytt emne, er nå et etablert felt både innen matematikken og i teoretisk datavitenskap. Datakompleksitet har også blitt uventet betydningsfullt fordi det utgjør det teoretiske grunnlaget for Internettsikkerhet.

Wigderson er født i Haifa, Israel, i 1956. Han begynte ved Technion – Israeli Institute of Technology – i 1977, der han tok en BSc. i datavitenskap i 1980. Han flyttet til Princeton for sine videregående studier, og fikk sin Ph.D i 1983 for avhandlingen *Studies in Combinatorial Complexity*, med Richard Lipton som sin veileder. I 1986 dro Wigderson tilbake til Israel for å begynne i en stilling ved Hebrew University i Jerusalem. Der fikk han fast ansettelse året etter og et fullverdig professorat i 1991.

I 1970-årene utformet datateoretikere visse fundamentale ideer om arten av databehandling, særlig i begrepene P og NP. P er det settet av oppgaver som datamaskiner kan løse enkelt, kanskje i løpet av noen få sekunder, mens NP også omfatter oppgaver som datamaskiner har vanskelig for å løse, på den måten at de kjente metodene kanskje bare kan finne svaret etter noen millioner år. Spørsmålet om hvorvidt alle disse vanskelige oppgavene kan reduseres til enklere problemer, altså hvorvidt P = NP eller ikke, er det grunnleggende spørsmålet innen datakompleksitet. Faktisk er det nå ansett som et av de viktigste uløste spørsmålene i all matematikk.

Wigderson gjorde oppsiktsvekkende fremskritt på dette området ved å undersøke hvilken rolle tilfeldighet spiller som støtte for databehandlingen. Enkelte vanskelige problemer kan forenkles ved hjelp av algoritmer der datamaskinen treffer tilfeldige valg, "slår mynt og krone", under behandlingen. Men hvis en algoritme avhenger av tilfeldige valg, er det alltid en mulighet for at en feil kan snike seg inn i løsningen. Wigderson viste,

først sammen med Noam Nisan og senere med Russell Impagliazzo, at for enhver rask algoritme som kan løse vanskelige problemer ved å slå mynt og krone, finnes det en nesten like rask algoritme som ikke gjør dette, forutsatt at visse vilkår er oppfylt.

Wigderson har drevet forskning på alle større åpne problemer innen kompleksitetsteori. På mange måter har feltet vokst frem rundt ham, ikke bare på grunn av hans brede interessefelt, men også på grunn av hans åpne personlighet og hans entusiasme for samarbeidsprosjekter. Han har medforfattet artikler med godt over 100 andre, og har vært veileder for et stort antall unge kompleksitetsteoretikere. "Jeg anser meg som utrolig heldig som lever i denne epoken," sier han. "[Datakompleksitet] er et ungt felt. Det er et svært demokratisk felt. Det er et svært vennlig felt, det er et felt som er veldig samarbeidsvillig, noe som passer min natur. Og det er avgjort smekkfullt av intellektuelle problemer og utfordringer."

I 1999 begynte Wigderson ved Institute of Advanced Study (IAS) på Princeton, der han har vært hele tiden senere. Ved et arrangement for å feire Wigdersons sekstiårsdag i 2016, uttalte IAS' direktør Robbert Dijkgraaf at han hadde startet en gullalder innen teoretisk datavitenskap ved instituttet.

Wigderson er kjent for sin evne til å se forbindelser mellom tilsynelatende ubeslektede områder. Han har gjort forbindelsene mellom matematikk og datavitenskap dypere. Et eksempel på dette er hans "sikksakk-graf", som han utviklet sammen med Omer Reingold og Salil Vadhan. Dette produktet knytter sammen gruppeteori, grafteori og kompleksitetsteori og har overraskende anvendelser, som hvordan du best kommer ut av en labyrint.

Den viktigste anvendelsen for datakompleksitet i dag er innen kryptografi, som brukes for å sikre informasjon på internett, som kredittkortnumre og passord. Folk som designer kryptosystemer må for eksempel passe på at oppgaven med å avkode systemet deres er et NP-problem, altså at det ville ta en datamaskin millioner av år å klare det. Tidlig i sin karriere kom Wigderson med fundamentale bidrag til et nytt konsept i kryptografien i form av "zero-knowledge"-beviset, som nå, over 30 år senere, brukes i blokkjedeteknologi. I et "zero-knowledge"-bevis, eller kunnskapsløst bevis, må to mennesker bevise en påstand uten å avsløre noen kunnskap utover gyldigheten av påstanden, som i eksempelet med de to millionærene som vil bevise hvem som er rikest av dem uten at noen av dem avslører hvor mye penger de har. Sammen med Oded Goldreich og Silvio Micali viste Wigderson at slike kunnskapsløse beviser kan brukes til å bevise, i hemmelighet, ethvert offentlig resultat om hemmelige data. Si for eksempel at du vil demonstrere overfor noen at du har bevist et matematisk teorem, men du vil ikke avsløre noen detaljer om hvordan du gjorde det. Et kunnskapsløst bevis lar deg gjøre dette.

I 1994 ble Wigderson tildelt Rolf Nevanlinna-prisen for datavitenskap, som deles ut av Den internasjonale matematikkunionen hvert fjerde år. Blant hans mange andre utmerkelser er Gödel-prisen i 2009 og Knuth-prisen i 2019.

Wigderson er gift med Edna, som han traff ved Technion, og som arbeider i dataavdelingen ved Institute of Advanced Study. De har tre barn og to barnebarn.

Kilde til sitatet: Heidelberg Laureate Foundation Portraits, intervju med Avi Wigderson, 2017.