THE ABEL PRIZE 2021

Det Norske Videnskaps-Akademi har besluttet å gi Abelprisen for 2021 til

László Lovász

ved Eötvös Loránd University i Budapest, Ungarn og

Avi Wigderson

ved Institute for Advanced Study, Princeton, USA,

"for deres grunnleggende bidrag til teoretisk datavitenskap og diskret matematikk, og deres ledende rolle i å gjøre dem til sentrale felt i moderne matematikk."

Teoretisk datavitenskap er studiet av hvilke muligheter og begrensninger som ligger i moderne informasjonsteknologi. Disiplinens røtter går tilbake til det grunnleggende arbeidet til Kurt Gödel, Alonzo Church, Alan Turing og John von Neumann, som førte til utviklingen av virkelige, fysiske datamaskiner. Datavitenskap omfatter to kompletterende underdisipliner: algoritmedesign, som utvikler effektive metoder for en mengde forskjellige informatikkproblemer, og datakompleksitet, som viser iboende begrensninger for algoritmenes effektivitet. Ideen om polynomiske tidsalgoritmer som ble fremsatt i 1960-årene av Alan Cobham, Jack Edmonds og andre, og den berømte P≠NP-formodningen til Stephen Cook, Leonid Levin og Richard Karp, fikk stor innflytelse på feltet og på arbeidene til Lovász og Wigderson.

Ved siden av den enorme innflytelsen den har på datavitenskap og datapraksis i videre forstand, danner teoretisk datavitenskap grunnlaget for kryptografi, og har nå en økende innflytelse på flere andre vitenskaper der det oppnås ny innsikt ved studere problemer ut fra et algoritmisk perspektiv.

Diskrete strukturer som grafer, strenger og permutasjoner er sentrale i datavitenskapen, og diskret matematikk og datavitenskap har naturlig vært nært relaterte disipliner.

Begge disse feltene har hatt stor nytte av mer tradisjonelle områder innen matematikken, men det har også vært en økende innflytelse i den motsatte retningen. Anvendelser, begreper og teknikker fra datavitenskapen har motivert nye utfordringer, åpnet opp nye retninger for utforskning og løst viktige åpne problemer innen ren og anvendt matematikk.

László Lovász og Avi Wigderson har vært ledende krefter innen denne utviklingen de siste tiårene. Deres arbeid er på mange måter sammenvevd, og særlig har de begge gitt fundamentale bidrag til å forstå tilfeldighet i informatikken og i utforskingen av grensene for effektiv databehandling.

Sammen med Arjen Lenstra og Hendrik Lenstra utviklet László Lovász gitterreduksjonsalgoritmen LLL. For et høydimensjonalt heltallsgitter finner denne algoritmen en pen, nesten-ortogonal basis. I tillegg til flere anvendelser, som en algoritme for å faktorisere rasjonale polynomer, er LLL-algoritmen et favorittredskap for kryptoanalytikere, idet den er i stand til å knekke flere foreslåtte kryptosystemer. Forbløffende nok brukes analyse av LLL-algoritmen også til å designe og garantere sikkerheten til nyere, gitterbaserte kryptosystemer som synes å kunne motstå angrep selv fra kvantedatamaskiner. For enkelte eksotiske kryptografiske primitiver, som homomorf kryptering, går de eneste konstruksjonene som er kjent, via disse gitterbaserte kryptosystemene.

LLL-algoritmen er bare én blant mange av Lovász' visjonære bidrag. Han beviste Local Lemma, et unikt redskap for å vise eksistensen av sjeldent forekommende kombinatoriske objekter, i motsetning til den vanlige probabilistiske metoden som brukes når objekter finnes i rikelige mengder. Sammen med Martin Grötschel og Lex Schrijver viste han hvordan man effektivt kan løse semidefinitte programmer, noe som førte til en revolusjon innen algoritmedesign. Han bidro til teorien om virrevandringer (random walks) med anvendelser på euklidske isoperimetriske problemer og tilnærmede volumberegninger av høydimensjonale legemer. Hans artikkel sammen med Uriel Feige, Shafi Goldwasser, Shmuel Safra og Mario Szegedy om probabilistisk verifiserbare beviser gav en tidlig versjon av PCP-teoremet, et umåtelig innflytelsesrikt resultat som viste at riktigheten av matematiske beviser kan verifiseres probabilistisk, med stor grad av sikkerhet, ved å lese bare et lite antall symboler! I tillegg løste han også problemer av gammel dato, som formodningen om den perfekte graf, Kneser-formodningen, han bestemte Shannon-kapasiteten til femkantgrafen, og i senere år utviklet han teorien om grafgrenser (i samarbeid med Christian Borgs, Jennifer Chayes, Lex Schrijver, Vera Sós, Balázs Szegedy og Katalin Vesztergombi). Dette arbeidet knytter sammen elementer av ekstremal grafteori, sannsynlighetsteori og statistisk fysikk.

Avi Wigderson har gitt brede og dyptpløyende bidrag til alle aspekter av algoritmekompleksitet, særlig rollen til tilfeldighet i databehandling. En tilfeldig algoritme er en som slår mynt og krone for å beregne en løsning som med stor grad av sannsynlighet er riktig. I løpet av flere tiår har forskere oppdaget deterministiske algoritmer for mange problemer der bare en tilfeldig algoritme var kjent tidligere. Den deterministiske algoritmen for primtallstesting av Agrawal, Kayal og Saxena er et slående eksempel på en slik algoritme. Disse derandomiserte resultatene reiser spørsmålet om hvorvidt tilfeldighet noen gang er essensielt i det hele tatt. I arbeider med László Babai, Lance Fortnow, Noam Nisan og Russell Impagliazzo har Wigderson demonstrert at svaret sannsynligvis er negativt. Formelt viste de at en beregningsformodning, i samme ånd som P≠NP-formodningen, innebærer at P=BPP. Dette vil si at enhver tilfeldig algoritme kan derandomiseres og gjøres om til en deterministisk med tilsvarende effektivitet, og dessuten er derandomiseringen generisk og universell, uten å avhenge av de interne detaljene i den tilfeldige algoritmen.

En annen måte å se på dette arbeidet på, er som en avveining mellom vanskegrad og tilfeldighet: Hvis det finnes et problem som er vanskelig nok, kan tilfeldighet samtidig simuleres av effektive deterministiske algoritmer. Wigdersons påfølgende arbeid sammen med Impagliazzo og Valentine Kabanets beviser et motsatt forhold: at effektive deterministiske algoritmer, selv for spesifikke problemer med kjente tilfeldige algoritmer, ville innebære at det må finnes et slikt vanskelig problem.

Dette arbeidet er nært forbundet med konstruksjoner av pseudotilfeldige (tilfeldighetslignende) objekter. Wigdersons arbeider har konstruert pseudotilfeldige generatorer som gjør noen få virkelig tilfeldige bits til mange pseudotilfeldige bits, ekstraktorer som trekker ut nesten perfekte tilfeldige bits fra en ufullkommen kilde til tilfeldighet, Ramsey-grafer og ekspandergrafer som er glisne og likevel har høy konnektivitet. Sammen med Omer Reingold og Salil Vadhan introduserte han sikksakkgraf-produktet, som gav en elementær metode for å bygge ekspandergrafer, og inspirerte til det kombinatoriske beviset for PCP-teoremet av Irit Dinur og en minneeffekiv algoritme for Reingolds problem om grafkonnektivitet. Det sistnevnte gir en metode for å navigere gjennom en stor labyrint mens man husker identiteten til bare et konstant antall skjæringspunkter i labyrinten!

Wigdersons øvrige bidrag omfatter "zero-knowledge" beviser, der det gis beviser for påstander uten å avsløre noen ekstra informasjon foruten påstandens gyldighet, og nedre grenser for effektiviteten til kommunikasjonsprotokoller, kretser og formelle bevissystemer.

Takket være lederskapet til Lovász og Wigderson er diskret matematikk og det relativt unge feltet teoretisk datavitenskap nå etablert som sentrale områder innen moderne matematikk.