THE ABEL PRIZE 2021

A Norvég Tudományos Akadémia (Norwegian Academy of Science and Letters) úgy döntött, hogy 2021-ben az Ábel-díjat

Lovász Lászlónak

Eötvös Loránd Tudományegyetem, Budapest, Magyarország és

Avi Wigdersonnak

Institute for Advanced Study, Princeton, USA ítéli,

„az elméleti számítástudomány és a diszkrét matematika területén nyújtott alapvető hozzájárulásukért, és az arra irányuló vezető szerepükért, hogy a modern matematika központi területeivé alakítsák őket.”

Az elméleti számítástudomány (Theoretical Computer Science, TCS) a számítástechnika teljesítőképességét és korlátait tanulmányozza. Gyökerei Kurt Gödel, Alonzo Church, Alan Turing és Neumann János alapvető munkásságához nyúlnak vissza, amely a fizikailag valós számítógépek kifejlesztéséhez vezetett. A TCS két egymást kiegészítő altudományágat foglal magában: az algoritmustervezést, amely hatékony módszereket fejleszt ki számos számítástechnikai problémára; és a számítástechnikai komplexitást, amely az algoritmusok hatékonyságának eredendő korlátait mutatja meg. Az 1960-as években Alan Cobham, Jack Edmonds és mások által felvetett polinomiális idejű algoritmusok fogalma, valamint Stephen Cook, Leonid Levin és Richard Karp híres P≠NP-sejtése nagy hatással volt a szóban forgó szakterületre, valamint Lovász és Wigderson munkájára.

A szélesebb értelemben vett számítástudományra és gyakorlatra kifejtett óriási hatása mellett a TCS adja a kriptográfia alapjait, és jelenleg egyre nagyobb befolyással van számos más tudományágra, amelyek terén a „számítógépes lencse (computational lens) alkalmazásával” új felismerésekhez vezet. A diszkrét struktúrák, mint például a gráfok, húrok, permutációk központi szerepet játszanak a TCS területén, a diszkrét matematika és a TCS pedig egymással szoros szövetségben álló területek. Bár mindkét szóban forgó terület rendkívüli előnyt merített a matematika hagyományosabb területeiről, ez fordított arányban is igaz. A TCS-ből származó alkalmazások, fogalmak és technikák új kihívások megjelenését segítették elő, új kutatási irányokat nyitottak meg, valamint fontos, még nyitva álló problémákat oldottak meg a tiszta és alkalmazott matematika terén.

Lovász László és Avi Wigderson az elmúlt évtizedekben vezető szerepet töltött be a fenti területek fejlődésében. Munkájuk számos szempontból egymásba fonódik, konkrétan

pedig mindketten alapvetően hozzájárultak a véletlenszerűség megértéséhez a számítások, valamint a hatékony számítások határainak meghatározása terén.

Arjen Lenstraval és Hendrik Lenstraval, Lovász László kifejlesztette az LLL rácsredukciós algoritmust. Ha adott egy sokdimenziós egész rács, ez az algoritmus szép, majdnem ortogonális bázist talál hozzá. Számos alkalmazás mellett, mint például a racionális polinomok faktorizálására szolgáló algoritmus, az LLL algoritmus a kriptoanalitikusok kedvenc eszköze, amely számos, javasolt kriptorendszert sikeresen feltör. Meglepő módon az LLL algoritmus elemzését az újabb, rácsalapú kriptorendszerek biztonságának tervezésére és garantálására is használják, amelyek, úgy tűnik, ellenállnak akár a kvantumszámítógépek támadásainak is. Néhány egzotikus kriptográfiai primitív, mint például a homomorf titkosítás esetében, az egyetlen ismert konstrukciók e rácsalapú kriptorendszereken keresztül valósulnak meg.

Az LLL algoritmus Lovász látnoki hozzájárulásainak csak egyike. Emellett bebizonyította a lokális lemmát, egy olyan egyedülálló eszközt, amely megmutatja a ritkán létező kombinatorikai objektumok létezését, szemben a normál valószínűségi módszerrel, amelyek a bőségesen létező objektumok esetén használatosak. Martin Grötschellel és Lex Schrijverrel együtt megmutatta, hogyan lehet hatékonyan megoldani a szemidefinit programokat, ezzel forradalmasította az algoritmustervezést. Hozzájárult a véletlenszerű bolyongások elméletéhez az euklideszi izoperimetrikus problémákra való alkalmazásokkal és a magas dimenziós testek hozzávetőleges térfogatszámításaival. Uriel Feigével, Shafi Goldwasserrel, Shmuel Safrával és Mario Szegedyvel együtt a probabilisztikusan ellenőrizhető bizonyításra vonatkozóan publikált tanulmánya a PCP-tétel korai változatát nyújtotta, és ez a rendkívül nagy hatást gyakorló eredmény megmutatta, hogy a matematikai bizonyítékok helyessége probabilisztikusan, magas konfidencia mellett ellenőrizhető, pusztán kisszámú szimbólum olvasásával! Emellett olyan régóta fennálló problémákat is megoldott, mint például a perfekt gráf sejtés, a Kneser-sejtés, az ötszöggráf Shannon-kapacitásának meghatározása, az utóbbi években pedig kidolgozta a gráfhatárértékek elméletét (Christian Borgs, Jennifer Chayes, Lex Schrijver, Sós Vera, Szegedy Balázs és Vesztergombi Katalin együttműködésével). Ez a munka az extremális gráfelmélet, a valószínűségelmélet és a statisztikus fizika elemeit köti össze.

Avi Wigderson minden szempontból széles körűen és mélyrehatóan hozzájárult a számítástechnikai komplexitás elmélet minden aspektusához, különös tekintettel a véletlenszerűségnek a számítástechnikában betöltött szerepére. A randomizált algoritmus lényege, hogy az érmefeldobás módszerével olyan megoldást számít ki, amely nagy valószínűséggel helyes. Az évtizedek során a kutatók számos olyan problémára fedeztek fel determinisztikus algoritmusokat, amelyekről korábban csak randomizált algoritmus volt ismert. Agrawal, Kayal és Saxena determinisztikus algoritmusa, amelynek célja a prímtesztelés, az ilyen derandomizált algoritmus szembetűnő példája. Ezek a derandomizációs eredmények felvetik a kérdést, hogy a véletlenszerűség valóban lényeges-e. Babai Lászlóval, Lance Fortnow-val, Noam Nisannal és Russell Impagliazzóval végzett munkáiban Wigderson bebizonyította, hogy a válasz valószínűleg nemleges lesz. Formálisan megfogalmazva megmutatták, hogy a P≠NP-sejtés szellemiségéhez hasonló számítástechnikai sejtés arra utal, hogy P=BPP. Ez azt jelenti, hogy minden randomizált algoritmus derandomizálható, és hasonló hatékonysággal determinisztikussá alakítható; ráadásul a derandomizáció általános és univerzális, a randomizált algoritmus belső részleteitől függetlenül.

A fenti eredmények megítélésének másik módja az, hogy azokat a nehézség és véletlenszerűség közötti kompromisszumként fogjuk fel: ha létezik elég nehéz probléma, akkor a véletlenszerűség hatékony determinisztikus algoritmusokkal szimulálható. Wigderson későbbi, Impagliazzóval és Valentine Kabanets-szel együtt végzett munkája a fordítottját igazolja: a hatékony determinisztikus algoritmusok létezése még az ismert, randomizált algoritmusokkal rendelkező specifikus problémák esetén is azt jelentenék, hogy léteznie kell ilyen nehéz problémának.

Ez a munka szorosan kötődik a pszeudorandom (véletlenszerű megjelenésű) objektumok konstruálásához. Wigderson művei olyan pszeudorandom generátorokat hoztak létre, amelyek néhány igazán véletlenszerű bitet sok pszeudorandom bitté alakítanak, valamint olyan extraktorokat, amelyek szinte tökéletes véletlenszerű biteket vonnak ki a véletlenszerűség tökéletlen forrásából, a Ramsey-gráfokból és az expander gráfokból, amelyek ritkák, de összefüggőségi

szintjük még mindig magas. Omer Reingolddal és Salil Vadhannal együtt bevezette a cikkcakk gráfszorzatot, amellyel elemi módszert biztosított az expander gráfok konstruálására, továbbá inspirációként szolgált Irit Dinur PCP-tételének kombinatorikus igazolásához, valamint Reingold gráfösszefüggőségét eldöntő memóriahatékony algoritmusához. Ez utóbbi megfelelő módszert ad egy nagy labirintusban történő navigáláshoz, miközben a labirintusban csak az állandó számú kereszteződési pontok azonosságára emlékezik!

Wigderson egyéb hozzájárulásai közé tartoznak az olyan nulla ismeretű bizonyítások, amelyek bizonyítást adnak a megfelelő állításokra anélkül, hogy az állítások érvényessége, a kommunikációs protokollok, áramkörök és formális bizonyítási rendszerek alsó korlátai mellett további információkat fednének fel.

Lovász és Wigderson vezető szerepének köszönhetően a diszkrét matematika és a viszonylag fiatal elméleti számítástudomány területe ma már a modern matematika központi diszciplínáivá lépett elő.