INFOMAT

MARS 2021

ABELPRISEN FOR 2021 TIL LÁSZLÓ LOVÁSZ OG AVI WIGDERSON

The Norwegian Academy of Science and Letters has decided to award the Abel Prize for 2021 to

László Lovász, Eötvös Loránd University in Budapest, Hungary

and

Avi Wigderson, the Institute for Advanced Study, Princeton, USA,

"for their foundational contributions to theoretical computer science and discrete mathematics, and their leading role in shaping them into central fields of modern mathematics".

INFOMAT kommer ut med 11 nummer i året og gis ut av Norsk Matematisk Forening. Deadline for neste utgave er alltid den 15. i neste måned. Stoff til INFOMAT sendes til

arnebs at math.uio.no

Foreningen har hjemmeside http://www.matematikkforeningen.no/
Ansvarlig redaktør er Arne B. Sletsjøe, Universitetet i Oslo

Matematisk kalender

På grunn av den pågående pandemien kan flere av arrangementene bli utsatt eller avlyst. Følg med på web-sidene.

Mai:
***24.-26.*. Abelpris-uka 2021**, DNVA/UiO <http://www.abelprisen.no/>

Juni:
***7.-11.*MEGA (effective methods in algebraic geometry)**, Tromsø <https://puremath.no/mega2021/>

20.-26.*. *The 8th European Congress of Mathematics (8ECM), Portorož, Slovenia and Online <https://www.8ecm.si/news/79>

27.-3. juli*. *Seminar Sophus Lie, Nordfjordeid <https://www.mathematik.uni-marburg.de/ agricola/SSL2021/>

Nasjonalt matematikermøte, Trondheim [UTSATT TIL SOMMEREN 2021] <https://www.ntnu.no/imf/matematikermote>

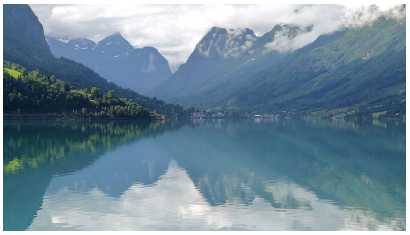
September:
27.-28.Mathematics without Borders, IMU 100 år, Strasbourg

MEGA, Tromsø, 7.-11. juni 2021

MEGA is the acronym for Effective Methods in Algebraic Geometry. This series of biennial international conferences, with the tradition dating back to 1990, is devoted to computational and application aspects of Algebraic Geometry and related topics, over any characteristics.

Plenary speakers:
Alicia Dickenstein, Universidad de Buenos Aires
Ana Romero Ibañez,Universidad de La Rioja
Gleb Pogudin, École Polytechnique
Greg Smith, Queen's University
Gretchen L. Matthews, Virginia Tech
Gunnar Fløystad, Universitetet i Bergen
Kathlén Kohn, KTH
Karin Baur, University of Leeds
Mohab Safey El Din, Sorbonne Universités
Ragni Piene, Universitetet i Oslo

SEMINAR SOPHUS LIE, Nordfjordeid, 27.juni -3. juli 2021



Dear Colleagues.

We are hoping for a good summer 2021, and a possibility for traditional meetings. The Seminar Sophus Lie is no exception. The next meeting of this seminar is June 27 - July 3, 2021, at Nordfjordeid. Recall that Sophus Lie was a famous Norwegian mathematician affiliated for an essential part of his career in Leipzig. It is not a surprise that Seminar Sophus Lie, a biannual meeting of mathematicians, was organized by German colleagues. It is however for the first time that the seminar comes to the Norwegian soil. The venue of the seminar will be the birthplace of Sophus Lie.

The conference center at Norfjordeid allows for meetings with at least 50 participants (with pandemic restrictions, but once these are done the number can be increased). Local expenses will be covered, there are also limited resources to help with travel expenses. Information on the Sophus Lie Conference Center can be found on the conference web page: https://www.mathematik.uni-marburg.de/ agricola/SSL2021/.

Lie theory has a wide range of applications in different branches of mathematics, and we encourage the Norwegian colleagues to participate in this event. We will try to keep the meeting broad. Therefore we ask everybody who is interested in attending the meeting to send us a noncommittal email saying so. Please use the address: Irina.Markina@math.uib.no. This will help

us to make sure we use the facilities in an optimal way. We also want to give young researchers a chance meet other mathematicians in person and to present/discuss their work.

Sincerely yours.

Boris Kruglikov and Irina Markina.

Abelprisen 2021

FOR THEIR CONTRIBUTIONS ...

(Komiteens begrunnelse for valget av Lovász og Wigderson)

The Norwegian Academy of Science and Letters has decided to award the Abel Prize for 2021 to

László Lovász of Eötvös Loránd University in Budapest, Hungary

and

Avi Wigderson of the Institute for Advanced Study, Princeton, USA,

"for their foundational contributions to theoretical computer science and discrete mathematics, and their leading role in shaping them into central fields of modern mathematics".

Theoretical Computer Science (TCS) is the study of the power and limitations of computing. Its roots go back to the foundational works of Kurt Gödel, Alonzo Church, Alan Turing, and John von Neumann, leading to the development of real physical computers. TCS contains two complementary sub-disciplines: algorithm design which develops efficient methods for a multitude of computational problems; and computational complexity, which shows inherent limitations on the efficiency of algorithms. The notion of polynomial-time algorithms put forward in the 1960s by Alan Cobham, Jack Edmonds, and others, and the famous $\mathbf{P} \neq \mathbf{NP}$ conjecture of Stephen Cook, Leonid Levin, and Richard Karp had strong impact on the field and on the work of Lovász and Wigderson.

Apart from its tremendous impact on broader computer science and practice, TCS provides the foundations of cryptography, and is now having growing influence on several other sciences leading to new insights therein by "employing a computational lens". Discrete structures such as graphs, strings, permutations are central to TCS, and naturally discrete mathematics and TCS have been closely allied fields. While both these fields have benefited immensely from more traditional areas of mathematics, there has been growing influence in the reverse direction as well. Applications, concepts, and techniques from TCS have motivated new challenges, opened new directions of research, and solved important open problems in pure and applied mathematics.

László Lovász and Avi Wigderson have been leading forces in these developments over the last decades. Their work interlaces in many ways, and, in particular, they have both made fundamental contributions to understanding randomness in computation and in exploring the boundaries of efficient computation.

Along with Arjen Lenstra and Hendrik Lenstra, László Lovász developed the LLL lattice reduction algorithm. Given a high dimensional integer lattice (grid), this algorithm finds a nice, nearly orthogonal basis for it. In addition to several applications such as an algorithm to factorize rational polynomials, the LLL algorithm is a favorite tool of cryptanalysts, successfully breaking several proposed cryptosystems. Surprisingly, the analysis of the LLL algorithm is also used to design and guarantee the security of newer, lattice-based crypto-systems that seem to withstand attacks even by quantum computers. For some exotic cryptographic primitives, such as homomorphic encryption, the only constructions known are via these latticebased crypto-systems.

The LLL algorithm is only one among many of Lovász´s visionary contributions. He proved the Local Lemma, a unique tool to show existence of combinatorial objects whose existence is rare, as opposed to the standard probabilistic method used when objects exist in abundance. Along with Martin Grötschel and Lex Schrijver, he showed how to efficiently solve semidefinite programs, leading to a revolution in algorithm design. He contributed to the theory of random walks with applications to Euclidean isoperimetric problems and approximate volume computations of highdimensional

bodies. His paper with Uriel Feige, Shafi Goldwasser, Shmuel Safra, and Mario Szegedy on probabilistically checkable proofs gave an early version of the PCP Theorem, an immensely influential result showing that the correctness of mathematical proofs can be verified probabilistically, with high confidence, by reading only a small number of symbols! In addition, he also solved long-standing problems such as the perfect graph conjecture, the Kneser conjecture, determining the Shannon capacity of the pentagon graph, and in recent years, developed the theory of graph limits (in joint work with Christian Borgs, Jennifer Chayes, Lex Schrijver, Vera Sós, Balázs Szegedy, and Katalin Vesztergombi). This work ties together elements of extremal graph theory, probability theory, and statistical physics.

Avi Wigderson has made broad and profound contributions to all aspects of computational complexity, especially the role of randomness in computation. A randomized algorithm is one that flips coins to compute a solution that is correct with high probability. Over decades, researchers discovered deterministic algorithms for many problems for which only a randomized algorithm was known before. The deterministic algorithm for primality testing, by Agrawal, Kayal and Saxena is a striking example of such a derandomized algorithm. These derandomization results raise the question of whether randomness is ever really essential. In works with László Babai, Lance Fortnow, Noam Nisan and Russell Impagliazzo, Wigderson demonstrated that the answer is likely to be in the negative. Formally, they showed a computational conjecture, similar in spirit to the **P** versus **NP** conjecture, implies that **P**=**BPP**. This means that every randomized algorithm can be derandomized and turned into a deterministic one with comparable efficiency; moreover the derandomization is generic and universal, without depending on the internal details of the randomized algorithm.

Another way to look at this work is as a tradeoff between hardness versus randomness: if there exists a hard enough problem, then randomness can be simulated by efficient deterministic algorithms. Wigderson's subsequent work with Impagliazzo and Valentine Kabanets proves a converse: efficient deterministic algorithms even for specific problems with known randomized algorithms would imply that there must exist such a hard problem.

This work is intimately tied with constructions of pseudorandom (random looking) objects. Wigderson's works have constructed pseudorandom generators that turn a few truly random bits into many pseudorandom bits, extractors that extract nearly perfect random bits from an imperfect source of randomness, explicit constructions of Ramsey graphs and expander graphs that are sparse and still have high connectivity. With Omer Reingold and Salil Vadhan, he introduced the zigzag graph product, giving an elementary method to build expander graphs, and inspiring the combinatorial proof of the PCP Theorem by Irit Dinur and a memory efficient algorithm for the graph connectivity problem by Reingold. The latter gives a method to navigate through a large maze while remembering the identity of only a constant number of intersection points in the maze!

Wigderson's other contributions include zero-knowledge proofs that provide proofs for claims without revealing any extra information besides the claims' validity, and lower bounds on the efficiency of communication protocols, circuits, and formal proof systems.

Thanks to the leadership of Lovász and Wigderson, discrete mathematics and the relatively young field of theoretical computer science are now established as central areas of modern mathematics.

BEVIST UTOVER ENHVER TVIL

(En mer folkelig framstilling av komiteens begrunnelse for valget av Lovász og Wigderson)

For å få en domfellelse i retten må straffeskyld være bevist utover enhver rimelig tvil. I matematikk er denne graden av bevis vanligvis ikke akseptert som tilstrekkelig. Et matematisk bevis skal være deterministisk og basert på formal logikk. Pythagoras´ læresetning, som sier at kvadratsummen av de to katetene i en rettvinklet trekant er lik kvadratet til hypotenusen, ble bevist allerede i antikken. Bevisene (det er mange av dem) er deterministiske, siden de lar seg reprodusere og gir det samme resultat hver gang.

Utviklingen av elektroniske datamaskiner utfordret den deterministiske bevis-tradisjonen. Den åpnet også for muligheten til å implementere algoritmer som tidligere var utenfor rekkevidde å gjennomføre for hånd. Nye muligheter åpnet for nye spørsmål. Hva er grensene for det som kan beregnes? Hvor raskt kan vi faktorisere et heltall? Er det mulig å verifisere noe ved å bruke argumenter basert på sannsynlighet?

Det er generelt vanskelig å faktorisere heltall. Hvis du velger et tilfeldig 1000-sifret heltall og har som mål å primtallsfaktorisere det, kan kanskje en datamaskin finne svaret, men det tar tid. Det kan gå både vinter og vår før beregningen er ferdig. På den annen side, hvis du får oppgitt en forslag til en faktorisering, så er det en enkel oppgave for en datamaskin å sjekke om svaret er riktig. Det er mye vanskeligere å finne en nål i en høystakk enn å bekrefte at det faktisk er en nål du har funnet. Dette er essensen av et berømt matematisk problem, det såkalte **P** versus **NP**-problemet, et av de syv millenniumsproblemene i matematikk.

Abelpris-vinnerne László Lovász og Avi Wigderson har hatt ledende roller i utviklingen av det matematiske grunnlaget for teoretisk computer science og dens to store underdisipliner: algoritmedesign og kompleksitet. Både Lovász og Wigderson har gitt vesentlige bidrag til å forstå betydningen av tilfeldigheter i beregninger og i det å utforske hva som er grensene for effektive beregninger.

Et eksempel på prisvinnernes bidrag innen algoritmedesign er den såkalte LLL-reduksjonsalgoritmen for gittere, oppkalt etter Lovász og Lenstra-brødrene, Arjen og Hendrik. For et høyere-dimensjonalt heltallsgitter finner denne algoritmen en nesten-ortogonal basis, ordnet etter lengde. Algoritmen har blitt et viktig verktøy for kryptoanalytikere, og har med suksess knekt flere kryptosystemer. I tillegg var også algoritmen grunnlaget for å motbevise Mertens-formodningen.

LLL-algoritmen

Mertens-formodningen ble først formulert av Thomas Joannes Stieltjes i 1885 i et brev til Charles Hermite og igjen på trykk av Franz Mertens i 1897. Formodningen dreier seg om den såkalte Möbius-funksjonen μ. Möbius-funksjonen $\mu(n)$ er definert for alle naturlige tall og tar verdien -1, 0 eller 1, avhengig av antall primfaktorer i n; hvis n er delelig med et primtallskvadrat, så er verdien er 0, mens verdien $\mu(n)$ for et kvadratfritt tall n er -1 hvis n har et odde antall primfaktorer og +1 hvis antall primfaktorer er et partall. I Mertens-formodningen summeres $\mu(n)$ for alle positive heltall mindre enn et reelt tall x. Vi kaller denne summen $M(x)$. Mertens-formodningen sier at $M(x)$ er mindre enn $\sqrt{x}$ for ethvert positivt tall x.

Mertens-formodningen er et dypt matematisk resultat. Hvis formodningen var sann, ville det bety at Riemann-hypotesen også var sann. Riemann-hypotesen er et annet av milleniums-problemene i matematikk. Dessverre er det kun en enveis sammenhengen mellom de to formodningene, så Mertens-formodningens fall vil ikke ha noen konsekvenser for statusen til Riemann-hypotesen.

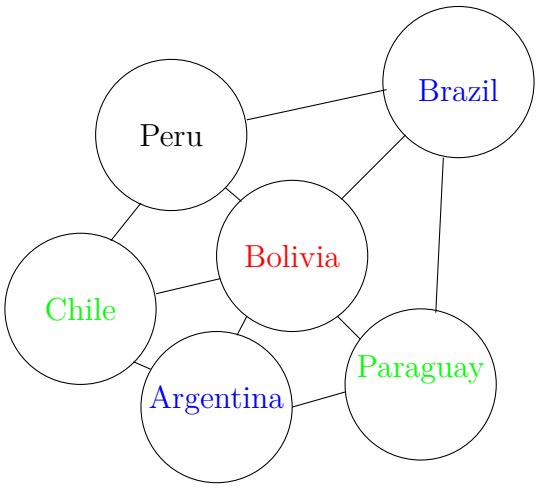
Mertens-formodningen er et godt eksempel på en matematisk formodning som faktisk ikke er riktig, til tross for utallige eksempler som indikerer det motsatte. Etter å ha stått som et åpent spørsmål i nesten et århundre, gjorde LLL-algoritmen det til slutt mulig for Andrew Odlyzko og Herman te Riele å vise at formodningen ikke er riktig.

Null-kunnskapsbevis

Når du skal overføre penger i banken, er autentisering et viktig begrep. Før de kan utføre en transaksjon må banken være sikker på at du er deg, enten du er fysisk til stede eller om du logger deg inn i banken elektronisk. Når du oppgir din personlige kode, må banken med stor sikkerhet være i stand til å bekrefte at du er den virkelige kontoinnehaveren. Av sikkerhetsmessige grunner ønsker imidlertid ikke banken å lagre din personlige kode. Men er det mulig for banken å bekrefte en kode den ikke har lagret? Svaret er faktisk ja, og her er det null-kunnskapsbevisene kommer inn.

Null-kunnskapsbevis ble først beskrevet i 1985 av Shafi Goldwasser, Silvio Micali og Charles Rackoff. Noen år senere utviklet Oded Goldreich, Silvio Micali og Abel-prisvinneren Avi Wigderson teorien videre og beskrev blant annet et null-kunnskapsbevis for tre-farge-problemet. Dette var et svært viktig resultat siden eksistensen av et slikt bevis garanterer eksistensen av lignende bevis for ethvert annet problem av samme kompleksitet.

Null-kunnskapsbeviset for tre-farge-problemet kan beskrives som følger: Anta at vi har delt et plant område i sammenhengende regioner, slik som f.eks. på et kart. Vår oppgave er å fargelegge hvert land slik at ingen naboland har samme farge. I 1976 fant Kenneth Appel og Wolfgang Haken det første beviset for at uansett hvordan landene ligger i forhold til hverandre, er det alltid mulig å fullføre fargeleggingen med fire farger. Og fire farger er den nedre grensen for å få dette til. Bolivia og nabolandene er et fint eksempel på dette. Bolivia har 5 naboer, Chile, Argentina, Paraguay, Brasil og Peru. De fem naboene omgir Bolivia fullstendig.



Som vi ser i illustrasjonen, hvor forbindelseslinjene symboliserer felles grenser, er ikke tre farger nok.

Men anta nå at vi har et kart som kan fargelegges med kun tre farger. Er det mulig for Alice å overbevise Bob at dette er tilfelle, uten at hun faktisk viser Bob kartet? Wigderson et al. ga et positivt svar; Alice dekker til kartet slik at Bob bare ser landene og grensene, men ingen farger. Bob velger to naboland og ber Alice vise han fargene. Alice gjør som hun blir bedt om og Bob ser med egne øyne at fargene er forskjellige. Alice dekker til fargene igjen og Bob velger et nytt par naboland for fargesjekking. Igjen viser Alice Bob fargene og Bob er fornøyd med det han ser. Så hvorfor får ikke Bob noen kunnskap om fargene på denne måten? Hemmeligheten er at mellom to farge-avsløringer permuterer Alice de tre fargene. Derfor observere kun Bob at de to nabolandene har forskjellige farger, men hvilke farger landene hadde i utgangspunktet forblir en hemmelighet. Etter å ha gjennomført denne prosedyren et passende antall ganger innser Bob at den eneste muligheten for at Alice kan lykkes i hvert forsøk, er at hun faktisk har klart å fargelegge kartet med bare tre farger.

På denne måten har Alice gitt Bob en variant av et null-kunnskapsbevis. Null-kunnskapsbevis baserer seg på sannsynligsbetraktninger, i den forstand at det avgjørende argumentet for Bob er den overveiende sannsynligheten for at Alice har rett. Han godtar Alice's påstand, fordi han finner den bevist utover enhver tvil.

Denne formen for probabilistisk tilnærming har vist seg å gi en vellykket utvidelse av det matematiske universet, gjennom å bidra med en ny type teknikker og strategier. At den har utvidet vår matematiske kunnskap – er bevist utover enhver tvil.