Nederlands Mathematisch Congres 2022

19 - 20 April
Van der Valk Hotel
Utrecht

April 19 - 20, 2022
NMC Scientific Days
9.00 - 17.30 u
[Van der Valk Hotel, Utrecht]

Shafi Goldwasser
Massachusetts Institute
of Technology

Helmut Hofer
Institute for Advanced Study
Princeton

March 24, 2022
Speed dates with industry
[online]

Nataša Jonoska
University of South Florida

Joris van der Hoeven
French National Centre
for Scientific Research, Paris

information & registration
www.mathematischcongres.nl

Organisation under the auspices of

NWO

KWG

platform wiskunde nederland

Sponsors

The organisers gratefully acknowledge support from:





Cover designed by Dick van der Toorn (NWO)

NMC 2022

Programme Booklet

Van der Valk Hotel Utrecht, The Netherlands

Local organising committee:

Joanna Ellis-Monaghan (University of Amsterdam)

Barry Koren (president Koninklijk Wiskundig Genootschap)

Marieke Kranenburg (University of Amsterdam)

Nada Mitrovic (Centrum Wiskunde & Informatica)

Olivia Muthsam (NWO)

Wil Schilders (director Platform Wiskunde Nederland)

Oliver Tse (TU Eindhoven)

Scientific organising committee:

Joanna Ellis-Monaghan (University of Amsterdam, chair)

Jeanine Daems (University of Applied Sciences Utrecht)

Federica Pasquotto (Leiden University)

Frank Redig (TU Delft)

Jacques de Swart (PwC and Nyenrode Business University)

Rob van der Vorst (Free University Amsterdam)

KWG-PhD prize committee:

Gerard van der Geer (University of Amsterdam)

Svetlana Dubinkina (VU Amsterdam, on behalf of NDNS+)

Nelly Litvak (University Twente, on behalf of STAR)

Berry Schoenmakers (TU Eindhoven, on behalf of DIAMANT)

Maarten Solleveld (RU Nijmegen, on behalf of GQT)

Word of Welcome

Dear participants,

Welcome at the Netherlands Mathematical Congress (NMC), which is held onsite again! In 2020, NMC had to be cancelled very shortly before its intended start. In 2021, NMC was held fully online in a series of nine events spread over nine months.

After two years of pandemic perils, overall, mathematics is doing very well in The Netherlands. Student inflow numbers remain to be good. The Delta Plan and Sector Plan have brought staff growth and extra dynamics. Let's keep this up!

After the last onsite congress – NMC 2019 in Veldhoven – the request from many mathematicians was to organize NMC on a more central location in The Netherlands. The NMC organization has responded to this by moving the congress to Utrecht.

The two-day congress is still held on the Tuesday and Wednesday after Eastern, but is called the *NMC Scientific Days* now. The *NMC Speed Dates with Industry* event, which used to be part of the two-day congress, appeared to be very successful in its 2021 online version. It will be held online again, as part of the NMC, but on another date than the NMC Scientific Days.

The NMC Scientific Days 2022 offer a program with interesting sessions, prize winning events, opportunities to speak with colleagues from other fields of mathematics and other institutes, a joint dinner, and more!

We wish you a fruitful and joyful congress!

Marieke Kranenburg (chair Organizing Committee NMC)
Barry Koren (chair Royal Dutch Mathematical Society)
Wil Schilders (director Platform Wiskunde Nederland)

General Information

Venue: Van der Valk Hotel Utrecht

Winthontlaan 4-6, 3526 KV Utrecht

With this new location we cater to the wishes of the visitor with respect to travel time to the conference. Just off the A12 motorway and within walking distance of a bus and tram stop, the hotel is easily accessible both by public transport and by car.

By public transport

From Utrecht CS (about 10 minutes)

- Bus lines: 65, 74 and 77 (every 5 minutes)
- Express tram lines 60 and 61

By car

Van der Valk Hotel Utrecht is located on the A12. Take exit 17 (Utrecht / Jaarbeurs / Kanaleneiland). Parking is possible at a reduced rate in our parking garage.

Food and beverages

Lunches are included in the registration fee, as is the conference dinner. *Continue fill in further*

Registration desk

Should you have any questions or encounter any problems, please contact the registration desk which will be open during early mornings and the breaks. The hotel registration desk is open full time for non-conference-related questions.

Stands

On the first floor In the foyer there will be stands of the following organisations:

- Epsilon Uitgaven
- Vierkant voor Wiskunde
- Optische Fenomenen
- NWO
- Platform Wiskunde Nederland
- de Nederlands Vereniging van Wiskundeleraren


Oudegracht 3
Oudegracht 2
Oudegracht 1
Foyer
Lift 1
Coffeecorner
Lift 2
Lift 3
Lift 4
Lift 5
Herentoilet
Damestoilet
Live Cooking
Coffeecorner
Nieuwegracht 1
Bar
Nieuwegracht 2
Lift 6

Programme NMC 2022

Tuesday 19 April 2022

Time	Location	Activity
9:00-10:00	Nieuwegracht 1+2	Registration & coffee
10:00-10:10	Nieuwegracht 1+2	Opening session: Barry Koren (chair KWG) Arian Steenbruggen (director NWO Domain Science) Richard Boucherie (chair PWN)
10:10-11:10	Nieuwegracht 1+2	Keynote lecture: Helmut Hofer (Institute for Advanced Study) *chair: Federica Pasquotto*
11:10-11:30		Break
11:30-12:30	Nieuwegracht 1+2	AIM and Committee Innovation *chair: Tristan van Leeuwen*
12:30-13:30		Lunch KWG Annual Meeting
13:30-15:00	Oudegracht 1 Oudegracht 2 Oudegracht 3 Oudegracht 4	Parallel sessions: STAR DIAMANT QSC 4TU.AMI and PWN Committee Innovation
15:00-15:30		Coffee break
15:30-16:00	Nieuwegracht 1+2	Stieltjes Prize 2020-2021: Jan-Willem van Ittersum *chair: Odo Diekmann*
16:00-17:00	Nieuwegracht 1+2	Beeger lecture: Shafi Goldwasser (Massachusetts Institute of Technology) *chair: Serge Fehr*
17:00-18:00	Nieuwegracht 1+2	European Women in Mathematics, The Netherlands *chair: Maria Vlasiou*
18:00-19:00		Drinks
19:00-21:00		Dinner
21:00-23:00		Bar open

Wednesday 20 April 2022

Time	Location	Activity
8:30-10:00	Nieuwegracht 1+2	Registration & coffee
9:00-10:00	Nieuwegracht 1+2	What's cooking? * Platform Wiskunde Nederland (Richard Boucherie) * Math4NL (Vivi Rottschäfer) * Research Assessment Mathematics (Erik Koelink) * Nederlandse Vereniging van Wiskundeleraren (Heleen van der Ree) * eScience Center (Ncolas Renaud) * Koninklijk Wiskundig Genootschap (Barry Koren)
10:00-11:00	Nieuwegracht 1+2	Ceremony N.G. de Bruijn medal: Joris van der Hoeven *chair: Jan van Neerven*
11:00-11:30		Break
11:30-13:00	Oudegracht 1 Oudegracht 2 Oudegracht 3 Oudegracht 4	Parallel sessions: NETWORKS GQT NDNS+ History of Mathematics
13:00-14:00		Lunch
14:00-15:00	Nieuwegracht 1+2 Oudegracht 1	KWG PhD Prize Pythagoras Prize
15:00-15:30		Break
15:30-16:30	Nieuwegracht 1+2	Keynote lecture: Nataša Jonoska (University of South Florida) *chair: Joanna Ellis-Monaghan*
16:30-17:00		Prize giving ceremony
17:00-18:00		Drinks

Tuesday, April 19

Keynote Lecture 10:10-11:10

Helmut Hofer (Institute for Advanced Study, Princeton)

A Short History of Symplectic Dynamics

Although it is difficult to give a precise definition of the emerging field of Symplectic Dynamics, it is not difficult to give examples demonstrating how ideas from Dynamical Systems and Symplectic Geometry/Topology come together to answer nontrivial questions. The modern theory of Dynamical Systems and the field of Symplectic Geometry emerged from Poincaré's integrated viewpoint of Mathematics. He combined ideas from Geometry, Topology and Dynamical Systems to study Hamiltonian Dynamics. After Poincaré, the theory of Dynamical Systems and Symplectic Geometry developed almost independently, and the latter even gave birth to the new field of Symplectic Topology. In the last twenty years we have seen breakthroughs on a variety of dynamical system problems using integrated ideas, which result from the merger of viewpoints coming from the different fields. These developments point to a new fruitful direction of research, which we call Symplectic Dynamics. In this talk for a general mathematical audience we shall describe some of the ideas and how they came about.

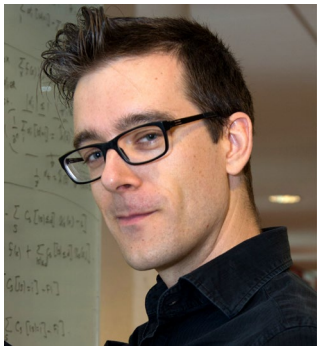
Matthias Möller (TU Delft)

IgaNets: Physics-Informed Machine Learning Embedded Into Isogeometric Analysis

Many engineering problems of practical interest are modelled by systems of partial differential equations equipped with initial and boundary conditions and complemented by problem-specific constitutive laws. For decades, numerical methods like the finite element method have been the method of choice for computing approximate solutions to problems that cannot be solved analytically. Starting with the seminal paper on physics-informed neural networks (PINNs) a new paradigm has entered the stage: learning the behavior of the differential operator instead of discretizing it and solving the resulting linear(ized) systems of equations brute-force. Next to PINNs, several alternative approaches like DeepONets and Fourier neural networks have been proposed in recent years. Their ease of implementation and fast response time, once training is completed, makes learning-based methods particularly attractive for engineering applications as they offer the opportunity to combine computer simulations with real-world data, e.g., stemming from measurements of real physical systems.

In this talk we propose a novel approach to embed the PINN paradigm into the framework of Isogeometric Analysis to combine the best of both worlds. IGA is an extension of the finite element method that integrates the simulation-based analysis into the computer-aided geometric design pipeline. In short, the same mathematical formalism, namely (adaptive) B-splines or NURBS, that is used to model the geometry is adopted to represent the approximate solution, which is computed following the same strategy as in classical finite elements.

In contrast to classical PINNs, which predict point-wise solution values to (initial-)boundary-value problems directly, our IGA-PINNs learn solutions in terms of their expansion coefficients relative to a given B-Spline or NURBS basis. This approach is furthermore used to encode the geometry and other problem parameters such as boundary conditions and parameters of the constitutive laws and feed them into the neural network as inputs. Once trained, our IGA-PINNs make it possible to explorer various designs from a family of similar problem configurations efficiently, without the need to recompute every new problem configuration brute force.



Wouter Koolen (Centrum Wiskunde & Informatica)

Pure Exploration Problems: Information theory and Equilibria

Pure exploration is a class of problems in statistical learning theory, focused around the active collection of data for the purpose of hypothesis testing. Pure exploration systems aim to collect only data that are most useful to answer a particular question quickly and confidently.

In this talk we will introduce pure exploration problems in the stylised multi-armed bandit setting, and provide motivation by reviewing the practical examples of best arm, best CVaR arm and arms-better-than-control.

We will then highlight the modern approach for constructing efficient learning algorithms. We will present information-theoretic lower bounds, and the path to matching instance-optimal algorithms by means of sequential saddle point computation.

Erik Bekkers (University of Amsterdam)

Geometric and Physical Quantities improve E(3) Equivariant Message Passing

Including covariant information, such as position, force, velocity or spin is important in many tasks in computational physics and chemistry. In this talk I will introduce Steerable E(3) Equivariant Graph Neural Networks (SEGNNs) that generalise equivariant graph networks, such that node and edge attributes are not restricted to invariant scalars, but can contain covariant information, such as vectors or tensors. This model, composed of steerable MLPs, is able to incorporate geometric and physical information in both the message and update functions. Through the definition of steerable node attributes, the MLPs provide a new class of activation functions for general use with steerable feature fields. We discuss ours and related work through the lens of equivariant non-linear convolutions, which further allows us to pin-point the successful components of SEGNNs: non-linear message aggregation improves upon classic linear (steerable) point convolutions; steerable messages improve upon recent equivariant graph networks that send invariant messages. The effectiveness of our method is demonstrated -with extensive ablation studies- on several tasks in computational physics and chemistry.

Parallel sessions

STAR **13:30-15:00**

Elisa Perrone (TU Eindhoven)

Geometric structure in dependence models for testing positive dependence

The growing availability of data makes it challenging yet crucial to model and detect dependence traits such as tail dependence, non-exchangeability, or positive/negative dependence. Copulas are fascinating mathematical objects that serve as tools for capturing these complex traits and constructing accurate dependence models. In this talk, we explore the geometric properties of copulas to address challenges in applications. First, we study the class of discrete copulas, i.e., restrictions of copulas to grid domains that admit representations as convex polytopes. We draw connections to the popular Birkhoff and transportation polytopes, thereby unifying and extending results from the statistics and the discrete geometry literature. Then, we exploit the geometric representation of discrete copulas as convex polytopes to define a hypothesis test for positive quadrant dependence. Finally, we compare the proposed approach with existing tests in various simulated scenarios and discuss its advantages and limitations.

Odysseas Kanavetas (Leiden University)

Optimal data driven policies under constrained multi-armed bandit observations

After a brief review of the multi-armed bandit (MAB) problem and its online machine learning applications, we present our work on the model with side constraints. The constraints represent circumstances in which bandit activations are restricted by the availability of certain resources that are replenished at a constant rate.

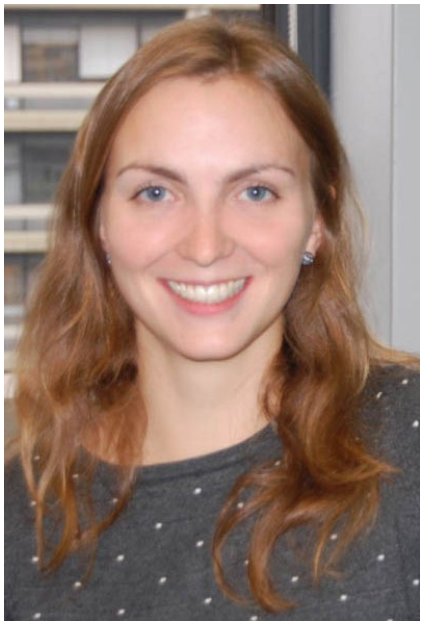
We consider the class of feasible uniformly fast (f-UF) convergent policies, that satisfy sample path wise the constraints. We first establish a necessary asymptotic lower bound for the rate of increase of the regret (i.e., loss due to the need to estimate unknown parameters) function of f-UF policies. Then, under pertinent conditions, we establish the existence of asymptotically optimal policies by constructing a class of f-UF policies that achieve this lower bound.

We provide the explicit form of such policies for the case in which the unknown distributions are Normal with unknown means and known variances.

Antonis Papapantoleon (TU Delft)

Model-free bounds in finance: a journey through probability, statistics and optimization

Academics, practitioners and regulators have understood that the classical paradigm in mathematical finance, where all computations are based on a single “correct” model, is flawed. Model-free methods, were computations are based on a variety of models, offer an alternative. In this talk, we will discuss model-free methods and bounds, starting from the improved Fréchet-Hoeffding bounds and their applications in option pricing and risk management, and will present how ideas from probability, statistics, optimal transport and optimization can be applied in this field.



Annika Betken (University of Twente)

Time series analysis based on ordinal patterns

In time series analysis, ordinal patterns describe the relative position of consecutive realizations generated by the underlying data-generating stochastic process.
Among other things, we consider estimators for the probabilities of occurrence of ordinal patterns (ordinal pattern probabilities) in time series.

pWe investigate statistical properties of these estimators in discrete-time Gaussian processes with stationary increments.

By means of Rao-Blackwellization, we further improve the estimation of ordinal pattern probabilities.
Moreover, limit theorems that describe the asymptotic distribution of the considered estimators are established.

Depending on the behavior of the data-generating processes' autocorrelation function, these limit distributions differ.

As an application, we discuss the Zero-Crossing estimator for the Hurst parameter which characterizes fractional Brownian motion processes.

Photo credits: Dirk Gillissen

Joanna Ellis Monaghan (University of Amsterdam)

The Tutte Polynomial: From Codes to DNA

William Tutte was one of the most influential mathematicians in combinatorics. He was a code-breaker at Bletchley Park, but his work remained classified long after Turing's story was told. One of the testimonies to his genius is that so many of his ideas proved to be catalysts, triggering further investigations and opening new vistas of mathematics. The Tutte polynomial is one of many such examples in his legacy. Here we will explore the Tutte polynomial, including its universality and multiple definitions, as well as some of its combinatorial and algebraic properties. We will showcase information encoded in the Tutte polynomial as evaluations and specializations, as these inform nearly every aspect of combinatorics and beyond including codes, DNA, and statistical mechanics models in physics and biology.

Léo Ducas (Centrum Wiskunde & Informatica)

Arakelov Random Walks, and Application in Cryptography and in Algorithmic Number Theory

During this presentation, I would like to overview a recent line of work jointly carried with Koen de Boer, Alice Pellet--Mary and Benjamin Wesolowski. The main object of our study is the space of ideal lattices of a given number field, a space known as the Arakelov class group (up to isometries).

Our central result is a fast-mixing theorem for random walks over this group, assuming an Extended Riemann Hypothesis. A first application is a worst-case to average-case reduction for the short-vector problem over ideal lattices (ideal-SVP), a problem of cryptographic interest. But this theorem is also useful for algorithms in Number Theory. For example it allows to formally prove that computing Power Residue Symbols can be done in polynomial time, a result that was previously only heuristic. It should also be useful in eliminating heuristics in sub-exponential algorithms for computing S-unit groups.

Karen Aardal (TU Delft)

Topics on the interface between discrete optimization and machine learning

We treat some topics relevant to machine learning and discrete optimization. The most widely used algorithm for solving discrete optimization problems is the tree search algorithm branch-and-bound (b&b). If a node in the search tree cannot be pruned, one needs to branch. To select the variable on which to branch is a crucial part of b&b as it affects the size of the search tree. We discuss how learning can be used to make selections that can are competitive with state-of-the-art methods. We also discuss how optimization can be used in so-called adversarial learning, and some results on the characterization of functions that are representable by neural networks with certain activation functions.

Lisa Kohl (Centrum Wiskunde & Informatica)

A Compressed Sigma-Protocol Theory for Lattices

Σ-Protocols provide a well-understood and widely-used basis for zero-knowledge proofs, allowing a prover to convince a verifier that a committed vector satisfies a constraint C(x)=0 (captured by an arithmetic circuit) without revealing anything about the (typically long) input vector x, besides the veracity of the claim. Using ideas from secure multi-party computation and from so-called Bulletproofs, it has been shown that the communication of Σ-Protocols for proving general constraint-satisfiability problems can be compressed from linear to (poly)logarithmic in the input length, yielding so-called compressed Σ-protocols. In a recent work, which will be the focus of this talk, we present the first framework for compressed Σ-protocols that can be instantiated from lattice-based assumptions, thereby plausibly withstanding even quantum attacks. This is joint work with Thomas Attema and Ronald Cramer.

Peter Bruin (Leiden University

Hidden shift problems

There has been a lot of interest in possible quantum algorithms for solving the following problem. Suppose we are given an Abelian group ***A***, a set *X* and two injective 'black-box' functions ***f***, ***g***: ***A***\toX such that for

some unknown $s \in \boldsymbol{A}$ (the hidden shift) and all $a \in \boldsymbol{A}$, we have $g(a) = \boldsymbol{f}(a + s)$. How can we efficiently (in terms of both the number of function evaluations and computation time) determine s?
Unlike for the somewhat similar hidden subgroup problem, which is efficiently solved by Shor'salgorithm, no polynomial-time quantum algorithm is known for the hidden shift problem. The best known algorithm for the general problem is Kuperberg's sub exponential algorithm.

I will talk about various aspects of quantum algorithms for (special cases of) the hidden shift problem. Parts of this are joint work in progress with Maris Ozols, Arend-Jan Quist and Serge Adonsou.

Maris Ozols (University of Amsterdam)

Quantum telepathy for mathematicians

The goal of this talk is to introduce quantum pseudo-telepathy to a wider audience of mathematicians through the example of quantum nonlocal games. I will try to explain it at three levels of difficulty. First, I will introduce the celebrated Mermin-Peres magic square game and explain why it has no perfect classical strategy but has a perfect quantum strategy. Next, I will discuss an elegant framework by Arkhipov (https://arxiv.org/abs/1209.3819) that characterizes nonlocal games with perfect quantum strategy in terms of graph planarity. Finally, I will mention a recent homotopical extension of Arkhipov's framework due to Okay & Raussendorf (https://arxiv.org/abs/1905.03822).

Clara Stegehuis (University of Twente)

Improving the performance and resilience of 5G wireless networks

In wireless networks, users receive data on their phones, computers or other devices from base stations. Modern 5G networks allow for multi-connectivity, where users in the network can connect to multiple base stations at the same time. As the data then flows through multiple paths, a user can enjoy higher data rates and a higher reliability. These properties are essential for emerging applications such as augmented-reality or surgery robots. In this talk, we will see that while simple forms of multi-connectivity improve resilience and are beneficial from the perspective of a single user, they decrease the performance of the entire network. We then investigate smart strategies to multiconnect users that improve the performance of the entire network.

Sandjai Bhulai (Free University Amsterdam)

Mathematics in healthcare ... it matters!

The relevance of mathematics in healthcare settings cannot be overemphasized. It has been successfully used worldwide to provide a wide range of methodologies that can help healthcare professionals significantly improve their operations. At the same time, many of the traditional problems reappear with

higher complexity due to a more personalized approach due to the availability of data and IT systems. This talk will illustrate the power of mathematics in healthcare systems by highlighting some key examples. Mathematics can help improve healthcare services while balancing resources, quality, and costs. It matters!

John Poppelaars (Doing the Math)

Mathematics for a Better World

Applying mathematics to support big hairy business decisions can be challenging but can be very effective. During the lecture John will use examples from his work as a consultant and illustrate how mathematics was put to work, the challenges encountered and how to resolve those. Can mathematics solve the problem of polluting sewers, improve the safety of gas networks, speed up the energy transition and help reduce our carbon footprint?

About John Poppelaars

John Poppelaars is Founder of Doing the Math, a company focussed on supporting organisations in becoming more sustainable by adopting a data & analytics driven way of decision making. In this role John acts as senior advisor & analytics expert.

John is a passionate proponent of the use of analytics as a key business enabler. Throughout his career, he has applied the business maxim of 'improving decision-making' to numerous projects across a myriad of industries and supported his clients to optimise their businesses with the best suitable analytics techniques. John was awarded the 2012 Franz Edelman Award for this work on the development and enhancement of TNT Express' analytical capabilities which resulted in substantial savings.

Prior to founding his own company, John was employed at BearingPoint and ORTEC. John earned a Master's degree in Econometrics (1990) from the Erasmus University Rotterdam in the Netherlands and is INFORMS Certified Analytics Professional.

Stieltjes Prize 2020-2021 15:30-16:00

Jan-Willem van Ittersum

The jury for the Stieltjes Prize met on Friday 17 December 2021 to award the prize for the best mathematical dissertation published in the academic year 2020-2021. A total of 76 dissertations were assessed this time. External advice was obtained at various stages of the assessment. After an initial selection, a shortlist of 13 dissertations was drawn up.

Once again the jury was impressed by the high level of the dissertations. After the first round of discussion, 4 dissertations remained; all 4 of those candidates would have been worthy winners of the Stieltjes Prize. There was, however, one dissertation out of these four of outstanding quality, written by a PhD student who has shown that he has many other qualities as well. The jury therefore awarded the Stieltjesprijs 2020-2021 to Jan-Willem van Ittersum.

Jan-Willem van Ittersum wrote his thesis “Partitions and quasimodular forms: Variations on the Bloch–Okounkov theorem” at Utrecht University under the supervision of Gunther Cornelissen and Don Zagier (Bonn). In this well-written thesis he investigates how functions of partitions of integers, by way of a statistical physics inspired averaging operation, lead constructively to quasi-modular forms.

The concept of quasi-modular form originates in the work of Ramanujan, but the definition used here is due to Kaneko and Zagier. The thesis addresses three natural fundamental questions:

1. which collections of functions lead to such forms ?
2. which forms do arise in this manner ?
3. when does a classical modular form arise ?

The answers take the form of eight results about properties of such functions and their application. The approach is highly original and far reaching. The results provide new insights in a broad range of subjects, including combinatorics and enumerative geometry. Experts are (pleasantly) surprised by these results. The thesis combines methods from analysis, number theory, algebraic geometry and mathematical physics. A referee wrote: “his thesis is one of the nicest I have ever seen”.

Already at an early age Jan-Willem van Ittersum demonstrated extraordinary mathematical intuition and comprehension. Both his bachelor thesis and his master thesis contained original work generalizing results of well-known mathematicians. He converted each into a paper that was accepted right away (i.e., without substantial revision) by a journal.

Jan-Willem shows remarkable independence: he formulated the proposal for the thesis topic himself and managed to win a grant to perform the research. In his research he often went his own way, departing from the road suggested (or even recommended) by his advisors. Alongside the research for his thesis, he initiated collaborations on other topics, which led to yet another publication as well as three almost finished preprints.

Beeger lecture **16:00-17:00**

Shafi Goldwasser, Massachusetts Institute of Technology

The Right to Deny

Plausible deniability seems like the ultimate get-out-of-jail-free card. But how can we make it work when it comes to digital information sent in a public network?

Deniable encryption, defined by Canetti et al (Crypto 1997), suggests a method to achieve deniability by the sender of encrypted messages to overcome this problem. The idea is especially interesting in the context of electronic elections to eliminate the threat of vote buying after a vote has been cast, except that the encryption scheme is not homomorphic, which is necessary for encrypted vote adding, and it achieves only a 1/poly probability of being able to successfully deny unless the ciphertexts are not compact.

I will present two new works on the subject. In the first we define and construct sender Deniable Fully Homomorphic Encryption (FHE) based on the Learning With Errors (LWE) polynomial hardness assumption. Deniable FHE enables storing encrypted data in the cloud to be processed securely without decryption, maintaining deniability of the encrypted data, as well the prevention of vote-buying in electronic voting schemes where encrypted votes can be tallied without decryption. The construction achieves compact ciphertext independently of the level of deniability. Both the size of the public key and the size of the ciphertexts are bounded by a fixed polynomial, independent of the detection probability achieved by the scheme. However, the offline running time of our encryption algorithm depends on the inverse of the detection probability. Thus, the scheme falls short of achieving simultaneously compactness, negligible deniability and polynomial encryption time. The online running time is polynomial. In another work, more recently, we show a sender deniable encryption scheme where the encryption scheme is a quantum algorithm but the ciphertext is classical, which is secure under the LWE polynomial hardness assumption. This scheme achieves for the first time simultaneously compactness, negligible deniability and polynomial encryption time under LWE. Furthermore, it is possible to extend the scheme so that coercion in an election cannot take place when the coercer is able to dictate all inputs to the deniable encryption algorithm even prior to encryption.

Biography

Shafi Goldwasser is Director of the Simons Institute for the Theory of Computing, and Professor of Electrical Engineering and Computer Science at the University of California Berkeley. Goldwasser is also Professor of Electrical Engineering and Computer Science at MIT and Professor of Computer Science and Applied Mathematics at the Weizmann Institute of Science, Israel. Goldwasser holds a B.S. Applied Mathematics from Carnegie Mellon University (1979), and M.S. and Ph.D. in Computer Science from the University of California Berkeley (1984).

Goldwasser's pioneering contributions include the introduction of probabilistic encryption, interactive zero knowledge protocols, elliptic curve primality testings, hardness of approximation proofs for combinatorial problems, and combinatorial property testing.

Goldwasser was the recipient of the ACM Turing Award in 2012, the Gödel Prize in 1993 and in 2001, the ACM Grace Murray Hopper Award in 1996, the RSA Award in Mathematics in 1998, the ACM Athena Award for Women in Computer Science in 2008, the Benjamin Franklin Medal in 2010, the IEEE Emanuel R. Piore Award in 2011, the Simons Foundation Investigator Award in 2012, and the BBVA Foundation Frontiers of Knowledge Award in 2018. Goldwasser is a member of the NAS, NAE, AAAS, the Russian Academy of Science, the Israeli Academy of Science, and the London Royal Mathematical Society. Goldwasser holds honorary degrees from Ben Gurion University, Bar Ilan University, Carnegie Mellon University, Haifa University, University of Oxford, and the University of Waterloo, and has received the UC Berkeley Distinguished Alumnus Award and the Barnard College Medal of Distinction.

Wednesday, April 20

Ceremony N.G. de Bruijn medal 10:00-11:00

Joris van der Hoeven (CNRS)

Fast integer multiplication
(Joint work with David Harvey)

Integer multiplication is one of the oldest mathematical operations and still a central problem for computer arithmetic. The complexities of many other basic operations such as division, base conversion, gcds, computing e and pi, FFTs, etc. can be expressed in terms of the complexity of integer multiplication. In our talk, we will survey a new algorithm for multiplying two n-digit integers in time O(n log n).

NETWORKS 11:30-13:00

Noela Müller (TU Eindhoven)

The full rank condition for sparse random matrices

The presentation is on a sufficient condition for a sparse random matrix with given numbers of non-zero entries in the rows and columns having full row rank. The result covers both matrices over finite fields with independent non-zero entries and {0,1}-matrices over the rationals. The sufficient condition is generally necessary as well. This is joint work with Amin Coja-Oghlan, Pu Gao, Max Hahn-Klimroth, Joon Lee and Maurice Rolvien.

Viresh Patel (University of Amsterdam)

Computational counting and zeros of graph polynomials

In recent decades there has been a lot of interest in efficient algorithms to (approximately) count fundamental objects in graphs such as independent sets or proper k-colourings. More generally, these counting problems have associated generating polynomials (the independence polynomial for independent sets and the chromatic polynomial for proper k-colourings), and one is also interested in efficient approximation algorithms to evaluate these polynomials at different points. I will give an overview of a relatively recent technique called Taylor polynomial interpolation for designing these counting algorithms. We will see an intimate (but not fully understood) connection between computational complexity of counting problems and the locations of zeros of the associated counting polynomials.

Rajat Hazra (Leiden University)

Spectrum of inhomogeneous Erdős-Rényi random graphs

The talk is on inhomogeneous Erdős-Rényi random graphs. The eigenvalues of the adjacency and Laplacian matrix of the graph are studied. The empirical spectral distribution of the matrix after suitable scaling and centering is shown to have a deterministic limit in probability. Depending on the rank of the inhomogeneity kernel generating the random graph, the largest few eigenvalues have a much higher magnitude than that of the bulk. Assuming the rank to be finite, the second order behaviour of those few eigenvalues, after suitable centring and scaling, is shown to be multivariate Gaussian. We also describe the behaviour of the eigenvectors corresponding to the largest eigenvalue.

Marcello Seri (University of Groningen)

A snaphot of sub-Riemannian Laplacias

The study of intrinsic Laplacians on sub-Riemannian manifolds is still relatively young. In this short presentation, we will introduce the concept and give brief panoramic of the current state of the theory, focusing the attention on some of the many interesting open questions.

Federica Pasquotto (Leiden University)

A differentiable and symplectic point of view on orbifolds

In this talk I would like to discuss recent work with T. Rot which aims at extending basic notions and results in differential topology to the orbifold setting: in particular, the definition of degree of an orbifold map, and properties of the group of orbifold diffeomorphisms.

I also hope to describe how these questions have natural connections with (and extension to) the realm of symplectic topology, where orbifolds naturally arise in the context of symplectic reduction.

Magdalena Kedziorek (Radboud University)

Uniqueness of rational equivariant K-theory

One of the recent themes in algebraic topology concentrates on the different levels of commutative multiplicative structures present in equivariant homotopy theory, i.e. the homotopy theory which takes symmetries given by a group G into account.

I will start this talk by explaining why we should expect different levels of commutativity in equivariant homotopy theory. Working rationally and with a finite group G, one can simplify topological complexity of equivariant stable homotopy theory and produce a purely algebraic model for it. Using this algebraic description, I will discuss a recent result stating that for a finite abelian group G, rational G-equivariant K-theory is unique when considered with the highest level of commutative multiplication.

This is joint work with A.M. Bohmann, C.Hazel, J.Ishak and C.May.

NDNS+ **11:30-13:00**

Karen Veroy-Grepl (TU Eindhoven)

Optimal Experimental Design Strategies for Hyper-Parametrized Inverse Problems

In this talk, we consider the problem of optimal experimental design in the context of inverse problems involving systems governed by parametrised (partial) differential equations. In such inverse problems, the goal is often to infer from measurement data the values of unknown or uncertain parameters and thereby more accurately predict the state. However, when measurements are costly, it is important to choose the most informative data. This task becomes even more challenging when the model contains additional uncertainties and when the data noise is correlated. In this context, I will discuss optimal experimental design strategies for hyper-parametrized families of PDE-constrained inverse problems. With the help of reduced order models, the proposed method iteratively chooses the experiments that increase the stability

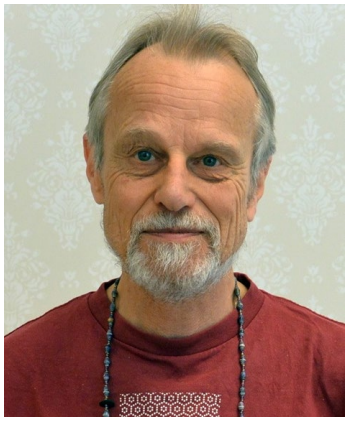
of the inverse problem and decrease the uncertainty in the solution, and is suitable even for large-scale problems with correlated noise.

Wil Schilders (TU Eindhoven)

Mimetic methods within scientific computing

Basic education in scientific computing, also known as numerical analysis, often consists of standard methods that are based upon general principles such as Taylor series expansions. Examples are the large collection of discretisation methods, interpolation techniques such as Lagrange and Hermite, and methods for solving nonlinear systems such as Newton's method. Such methods do not use any information about the underlying problem. Challenges in industry often require robust, fast and efficient scientific computing methods. This can be achieved by using knowledge about the problem and its solution. It is important to teach our students how they can develop and use such methods, and be fully prepared for numerical work in an industrial environment. Such methods are termed mimetic methods, i.e. methods that mimic the behaviour of the underlying problem. When searching the internet, one will observe that most of such methods have been formulated in the area of discretisation. Examples are exponentially fitted discretisation schemes, or numerical methods guaranteeing physical conservation laws and maximum principles. However, the field of mimetic methods is much broader. The well-known method ICCG for iteratively solving large linear systems is a mimetic method. In the area of model order reduction, we have developed index preserving MOR for differential-algebraic systems. Nonlinear systems can be solved using the method of correction transformation, which has been extremely effective for the simulation of semiconductor devices. In the area of port-Hamiltonian systems, special mimetic methods have been developed.

In this presentation, we will provide a summary of mimetic methods and identify many areas within scientific computing where such methods have been developed and successfully applied to industrial challenges. In my opinion, mimetic methods are the way forward in scientific computing.



Odo Diekmann

Renewal equations and epidemic models

The first aim of the talk is to highlight the renewal equation formulation of epidemic models as introduced by Kermack and McKendrick in 1927.The second aim is to survey some recently developed tools (pseudo-spectral approximation, time discretization) for analysing this class of delay equations. (Here a delay equation is defined as a rule for extending a function of time towards the future on the basis of the (assumed to be) known past.)

History of Mathematics 11:30-13:00

History of Mathematics of Chess

Theories of chess have a longer tradition, but mathematical theories of the game date back slightly more than a century. None other than the later world champion Max Euwe in 1929 contributed an intuitionist theory of chess. Euwe was one of the respondents in Adriaan de Groot's ground breaking study *Het denken van de schaker*. In a twist of history, the book written as a psychology of chess was re-read as a stepping stone towards an Artificial Intelligence of chess. The session proposes a tour from the history of AI, to the mathematics of chess, and back to an interplay of AI and the psychology of chess.

Nathan Ensmenger (University of Indiana)

From Deep Blue to Alpha Go; Games as the Experimental Organisms AI

For almost fifty years, the possibility of a computer being able to play chess as well as a human being seemed to be the ultimate achievement of artificial intelligence. The pursuit of this goal shaped the agenda

of the discipline for decades. More recently, Go has replaced chess as the game of choice among AI researchers. This paper explores role of games in the history of AI through the concept of the "experimental organism".

Max Laboyrie (University of Amsterdam)

Euwe's best move; Intuitionism in chess

In 1913 Zermelo embarked on a mathematical theory of the game of chess. The result was mathematics, but at the expense of such practicable notions he had wanted to determine as "best move" or "value of a position." In the 1920s König and Kalmár generalised Zermelo's results.
Then came Euwe, with a mathematical treatise on the game of chess, based on the notion of "spread". Brouwer's intuitionist alternative for "set", allowed Euwe to represent a sequence of chess positions in what appeared as a most natural way. Euwe even returned to Zermelo's "best move."
Outside mathematics, Euwe went on to become world champion of chess in 1935.

Han van der Maas

Psychology of chess: from Adriaan de Groot to Apha zero chess

I will first present an overview of the psychological study of chess thinking. Chess research on both expertise and cognition has been strongly influenced by the pioneering work of de Groot (1946/1978). Chess has also been very important in the development of AI. However, programs such as Deep Blue mainly told us how humans do not play chess, as it depended on a brute force computing approach, evaluating 200 million positions per second, that humans are particularly bad at. The renewed interest in AI among psychologists is based on novel techniques that have also revolutionized computer chess in the last five

years. AlphaZero chess (Silver et al., 2018) combines a deep learning network that values positions and predicts next moves, with a reinforcement learning system. Not only does this system plays superior chess, it also provides new insight in human chess thinking.

Keynote lecture 15:30-16:30

Nataša Jonoska (University of South Florida)

From Molecules to Mathematics

DNA self-assembly as a method to construct nanostructures is celebrating its 40 anniversary this year. The field gave impetus to an emerging branch of mathematics, which we coin as 'DNA mathematics'. DNA mathematics models and analyzes structures obtained as bottom-up assembly, as well as the process of self-assembly. We survey some of the mathematical tools that can help advance the science of DNA self-assembly. The theory needed to develop these tools is now driving the field of mathematics in new and exciting directions. In our presentation we focus particularly on the topics related to knot theory and graph theory.

Biography

Nataša Jonoska is a Distinguished Professor at the Department of Mathematics and Statistics at University of South Florida in Tampa, Florida. Her research interests are in theoretical and computational models of molecular self-assembly and molecular biology. She has had extensive research collaborations with experimentalists in molecular biology and structural DNA nano technology. She holds a PhD degree in Mathematical Sciences from the State University of New York in Binghamton NY, USA and since 2014 she is a Fellow of the American Association for the Advancement of Science. Her work on three-dimensional DNA self-assembly as computing models has been awarded with a Rozenberg Tulip Award in DNA Computing and Molecular Programming by the International Society for Nanoscale Science and Computing. Her work has been/is supported by the National Science Foundation (NSF), National Institute of Health (NIH), the W.M. Keck Foundation and for 2022 she is a Simons Fellow in Mathematics. For ten years she served as a Chair of the annual DNA Computing and Molecular Programming conference and co-chaired the annual Unconventional Computing and Natural Computing conference. She also serves on editorial boards of several journals including Theoretical Computer Science, Natural Computing, Computability, International Journal of Foundations of Computer Science, and has edited nine books on these topics. In 2021 the Florida section of Mathematical Association of America awarded her with the MAA award for Distinguished College or University Teaching of Mathematics.