Programme

Thursday

9:30-10:00 Arrival & coffee

10:00-11:00 **Anna Frühbis-Krüger (U of Oldenburg)** – Parallel computations in algebraic geometry

11:00-11:30 Coffee break

11:30-12:00 **Jasper van Doornmalen (TU/e)** – Symmetry handling in binary programs through propagation

12:00-12:30 **Mike Daas (UL)** – The symplectic method for solving Diophantine equations

12:30-13:30 Lunch

13:30-14:00 **Martin Lüdtke (RUG)** – Refined non-abelian Chabauty and the S-unit equation

14:00-14:30 **Alex Best (VU)** – Elliptic curves with good reduction outside of the first six primes

14:30-15:00 Coffee break

15:00-15:30 **Berend Ringeling (RUN)** – Critical points of modular forms

15:30-16:00 **Mar Curcó Iranzo (UU)** – Rational torsion of generalized modular Jacobians of level N = p^(r)q^(s)

16:00-17:00 **Lisa Kohl (CWI)** – Correlated Pseudorandom Functions

17:00 – Drinks & dinner

Friday

9:00-9:30 Arrival & coffee

9:30-10:30 **Matthias Walter (UT)** – Polyhedra, representable matroids and graphs: a computational perspective

10:30-11:00 **Lucas Slot (CWI)** – Sum-of-squares hierarchies for polynomial optimization

11:00-11:30 Coffee break

11:30-12:00 **Lawrence Barrott (UL)** – Smoothing Calabi-Yau fibrations

12:00-12:30 **Wessel van Woerden (CWI)** – On the Lattice Isomorphism Problem, Quadratic Forms, Remarkable Lattices, and Cryptography

12:30-13:30 Lunch

13:30-14:00 **Wout Moltmaker (UvA)** – Quantum invariants of biframes knotoids

14:00-14:30 **Jorge Becerra (RUG)** – A categorical approach to the universal tangle invariant

14:30-15:00 Coffee break

15:00-15:30 **Josse van Dobben de Bruyn (TUD)** – Recent progress on the Brill–Noether conjecture for graphs

15:30-16:30 **Julia Wolf (U of Cambridge)** – Efficient structure-randomness decompositions

16:30 – Mastermath discussion

Speakers

Anne Frühbis-Krüger (University of Oldenburg)

Parallel Computations in Algebraic Geometry

While parallel algorithms are a common tool both to numerical analysts and to number theorists (each interpreting the idea in their own way), computational tasks in algebraic geometry have rarely been addressed in this manner -- too daunting was the fact that Groebner Bases withstand naive approaches to parallelization. However, aiming for a very coarse-grained parallelism, there are several recent success stories. We will discuss some of these applications in detail.

Jasper van Doornmalen (TU/e)

Symmetry handling in binary programs through propagation

Symmetries of binary programs are known to dramatically slow down branch-and-bound procedures. A classical approach is to add symmetry handling inequalities that cut off all solutions that are not lexicographically maximal in their symmetry class.
In this talk, we present a propagation-based symmetry handling technique to ensure only lexicographically maximal solutions for permutations and groups acting on binary variables are found. Given certain initial variable fixings, e.g. branching decisions at a node of the branch-and-bound tree, the goal is to find valid additional fixings ensuring that integral solutions are lexicographically maximal in their symmetry class. We devise efficient algorithms that find possible fixings for sets of permutations, and for various classes of symmetry groups. In some cases, we are able to find all possible fixings. Last, we discuss the computational effectiveness of our methods.

Mike Daas (UL)

The symplectic method for solving Diophantine equations

Fermat’s Last Theorem was finally proved after Andrew Wiles had completed his proof of a large part of the modularity theorem. The general recipe for using Wiles’s theorem to actually solve diophantine equations is known as the ”modular method”. After recalling some basic facts about elliptic curves over C, Q and Fp, we briefly state the results on which the method relies, and illustrate it by proving Fermat’s Last Theorem. The so-called ”symplectic method” refines the modular method and can be used when the standard techniques are insufficient. After defining the Weil-pairing, we will give one such symplectic theorem and then illustrate how it can be used to prove that an equation similar to Fermat’s Last Theorem, but with arbitrary factors of 2 and 3 in the coefficients, does not have any non-trivial integer solutions for at least half the primes in most cases.

Martin Lüdtke (RUG)

Refined non-abelian Chabauty and the S-unit equation

The S-unit equation asks for rational numbers x \neq 0,1, such that both x and 1-x contain only prime factors from a given finite set of primes S. In 2005, Kim developed a non-abelian generalisation of the Chabauty method which he used to reprove Siegel’s Theorem, which states that there are only finitely many solutions for each set S. We show how this method can be made explicit in some cases, yielding p-adic analytic functions whose zero set contains the solutions to the equation.

Alex Best (VU)

Elliptic curves with good reduction outside of the first six primes

Elliptic curves are often tabulated by finding the (finite) set of elliptic curves with conductor bounded by some constant. While a natural ordering, it can also be helpful to know explicitly the set of curves with a given set of primes of bad reduction, even if their conductor is larger than existing tables. The Shafarevich conjecture, now proved by work of Faltings, guarantees that the set of elliptic curves over a fixed number field with a given set of primes of bad reduction is finite, but does not give a procedure to determine this set explicitly. We discuss a practical method for finding all elliptic curves over Q with good reduction outside the first set of six primes, some heuristics concerning the completeness of this method, and the properties of the curves found. The method involves finding generators of large height for a set of Mordell curves which may be of independent interest, and makes use of techniques such as 12-descent and computing Heegner points on CM curves.
This is joint work with Benjamin Matschke.

Berend Ringeling (RUN)

Critical points of modular forms

Modular forms are highly symmetric complex analytic functions. They appear in (seemingly) unrelated areas in mathematics and physics, such as number theory, algebraic topology and string theory. By the valence formula, the number of zeros of a modular form within each fundamental domain is known. In recent joint work with Jan-Willem van Ittersum, we generalize these results to the zeros of derivatives of modular forms.

Mar Curcó Iranzo (UU)

Rational torsion of generalized modular Jacobians of level N = p^(r)q^(s)

We consider the generalized Jacobian J_0(N)_m of the modular curve X_0(N) of level N, with respect to the modulus m consisting of all cusps on the modular curve. When N=p^(r)q^(s), for p and q odd prime numbers different from 3, we determine the group structure of the rational torsion of the Jacobian J_0(N)_m up to p- and q-primary torsion. Our results extend known results for squarefree levels and for prime power levels. Our proofs use their techniques, as well as results concerning the study of the rational points on the modular Jacobian and of the rational divisor class group of X_0(N).

Lisa Kohl (CWI)

Correlated Pseudorandom Functions

Correlated randomness is a ubiquitous resource in cryptography. A one-time pad, namely a pair of identical random keys, enables perfectly secure communication. More complex forms of correlated randomness can similarly facilitate protocols for secure multi-party computation that allow two or more parties to jointly compute a function of secret inputs revealing nothing beyond the output. The main challenge, and the core bottleneck of almost all practically oriented protocols for secure multi-party computation, is to design efficient methods to securely generate correlated randomness.

In this work we initiate the study of correlated pseudorandom functions that offer the ability to generate an essentially unbounded amount of correlated pseudorandomness from short correlated keys using only local computation. We present efficient constructions of correlated pseudorandom functions for a broad class of useful correlations from a variable-density variant of the learning parity with noise assumption.
This is joint work with Elette Boyle, Geoffroy Couteau, Niv Gilboa, Yuval Ishai and Peter Scholl.

Matthias Walter (University of Twente)

Polyhedra, Representable Matroids and Graphs: A Computational Perspective

Total unimodularity is an important concept in integer programming and taught in many courses. In the first part of the talk we address the structural viewpoint of this matrix property which is related to questions like “Is a matroid representable over every field?” and “Does the matroid stem from a graph?”. While the main algorithmic question of recognizing totally unimodular matrices was settled in the 80’s, there was no implementation for more than three decades. By now there is an efficient implementation of a polynomial-time recognition algorithm which we sketch in the second part of the talk. Finally, we discuss related open problems that are of practical interest to mixed-integer programming.

Lucas Slot (CWI)

Sum-of-squares hierarchies for polynomial optimization

We consider the problem of minimizing a given polynomial f over a compact set X in R^n. This formulation captures well-known hard optimization problems (including MaxCut and StableSet), even for simple sets X, such as the hypersphere, unit ball or standard simplex. Lasserre introduces several hierarchies of approximations on the minimum of f based on sums of squares of polynomials. These approximations may be computed by solving semidefinite programs of increasing size. It is natural to ask what the relation is between the order of the hierarchy (i.e. the size of the SDPs) and the quality of the resulting approximations. We discuss several recent results estimating the error of Lasserre’s hierarchies in different settings as the order increases. This is based on joint work with Monique Laurent.

Lawrence Barrott (UL)

Smoothing Calabi-Yau fibrations

One prediction from Mirror Symmetry is a connection between Calabi-Yau fibrations and certain types of degenerations. In this talk I'll explain the basic philosophy and recent progress on this problem.

Wessel van Woerden (CWI)

On the Lattice Isomorphism Problem, Quadratic Forms, Remarkable Lattices, and Cryptography

A natural and recurring idea in the knapsack/lattice cryptography literature is to start from a lattice with remarkable decoding capability as your private key, and hide it somehow to make a public key. This is also how the code-based encryption scheme of McEliece (1978) proceeds.

This idea has never worked out very well for lattices: ad-hoc approaches have been proposed, but they have been subject to ad-hoc attacks, using tricks beyond lattice reduction algorithms. On the other hand the framework offered by the Short Integer Solution (SIS) and Learning With Errors (LWE) problems, while convenient and well founded, remains frustrating from a coding perspective: the underlying decoding algorithms are rather trivial, with poor decoding performance.
In this work, we provide generic realizations of this natural idea (independently of the chosen remarkable lattice) by basing cryptography on the lattice isomorphism problem (LIP). The purpose of this approach is for remarkable lattices to improve the security and performance of lattice-based cryptography. For example, decoding within poly-logarithmic factor from Minkowski's bound in a remarkable lattice would lead to an encryption scheme resisting lattice attacks down to poly-logarithmic approximation factor, provided that the dual lattice is also close to Minkowski's bound. Recent works have indeed reached such decoders for certain lattices (Chor-Rivest, Barnes-Sloan), but these do not perfectly fit our need as their duals have poor minimal distance.
In this talk we will discuss the Lattice Isomorphism Problem in a quadratic form perspective and pose some open questions that might be of interest to the DIAMANT community. eprint: https://eprint.iacr.org/2021/1332

Wout Moltmaker (UvA)

Quantum invariants of biframes knotoids

In this talk I will recall the definition of a knotoid, and define several modifications of this definition to obtain 'framed' and 'biframed' knotoids. Afterwards I will give topological spaces whose ambient isotopy classes in 3-space are in one-to-one correspondence with framed and biframed knotoids respectively. Finally I will show how biframed knotoids can be used to construct quantum invariants of knotoids.

Jorge Becerra (RUG)

A categorical approach to the universal tangle invariant

It is known that some types of quantum groups (more specifically, ribbon Hopf algebras) give rise to knot and tangle invariants using the quantum group itself and not its representation theory. By considering a suitable class of tangles, I will present the universal invariant as a monoidal natural transformation. The construction is analogous to considering simplicial set maps as natural transformations between certain functors.

Josse van Dobben de Bruyn (TUD)

Recent progress on the Brill–Noether conjecture for graphs

Around 2006, Matt Baker established an analogy between divisors on curves and chip-firing games on graphs, culminating in a Riemann–Roch theorem for graphs (Baker and Norine, 2007). This has led to a lot of research into the interplay between algebraic geometry, tropical geometry, and graph theory. A key open problem is to determine to which extent Brill–Noether theory also holds for graphs. In this talk, I will discuss two recent developments in this direction (Draisma and Vargas, 2019; Van Dobben de Bruyn, Smit, and Van der Wegen, 2021).

Julia Wolf (University of Cambridge)

Efficient structure-randomness decompositions

Since Szemerédi's seminal work in the 70s, regularity lemmas have proven to be of fundamental importance in many areas of discrete mathematics. This talk will survey some of the classical results in both the graph and the arithmetic context and examine the connections between the two settings. We will then describe recent work under additional assumptions that characterise situations with efficient trade-off between the complexity of the structured part and the degree of randomness achieved.