Internationale Mathematische Nachrichten
International Mathematical News
Nouvelles Mathématiques Internationales

Die IMN wurden 1947 von R. Inzinger als „Nachrichten der Mathematischen Gesellschaft in Wien“ gegründet. 1952 wurde die Zeitschrift in „Internationale Mathematische Nachrichten“ umbenannt und war bis 1971 offizielles Publikationsorgan der „Internationalen Mathematischen Union“.

Von 1953 bis 1977 betreute W. Wunderlich, der bereits seit der Gründung als Redakteur mitwirkte, als Herausgeber die IMN. Die weiteren Herausgeber waren H. Vogler (1978–79), U. Dieter (1980–81, 1984–85), L. Reich (1982–83), P. Flor (1986–99), M. Drmota (2000–2007) und J. Wallner (2008–2017).

Herausgeber:

Österreichische Mathematische Gesellschaft, Wiedner Hauptstraße 8–10/104, A-1040 Wien. email *imn@oemg.ac.at*, *http://www.oemg.ac.at/*

Redaktion:

C. Fuchs (Univ. Salzburg, Herausgeber)
H. Humenberger (Univ. Wien)
R. Tichy (TU Graz)
J. Wallner (TU Graz)

Bezug:

Die IMN erscheinen dreimal jährlich und werden von den Mitgliedern der Österreichischen Mathematischen Gesellschaft bezogen.

Jahresbeitrag: € 35,–

Bankverbindung:
IBAN AT83-1200-0229-1038-9200 bei der Bank Austria-Creditanstalt (BIC-Code BKAUATWW).

Eigentümer, Herausgeber und Verleger: Österr. Math. Gesellschaft. Satz: Österr. Math. Gesellschaft. Druck: Weinitzendruck, 8044 Weinitzen.

ISSN 0020-7926

Österreichische Mathematische Gesellschaft

Gegründet 1903
http://www.oemg.ac.at/
email: *oemg@oemg.ac.at*

Sekretariat:

Alpen-Adria-Universität Klagenfurt,
Institut für Mathematik
Universitätsstraße 65-67
A-9020 Klagenfurt
email: *oemg@oemg.ac.at*

Vorstand des Vereinsjahres 2022:

J. Wallner (TU Graz): Vorsitzender
M. Ludwig (TU Wien):
Stellvertretende Vorsitzende
C. Fuchs (Univ. Salzburg):
Herausgeber der IMN
H. Egger (JKU Linz):
Schriftführer
M. Haltmeier (Univ. Innsbruck):
Stellvertretender Schriftführer
P. Grohs (Univ. Wien):
Kassier
D. Smertnig (KFU Graz):
Stellvertretender Kassier
V. Fischer (Univ. Wien):
Beauftragte für Frauenförderung
C. Heuberger (Univ. Klagenfurt):
Beauftragter f. Öffentlichkeitsarbeit

Beirat:

A. Binder (Linz)
M. Drmota (TU Wien)
H. Edelsbrunner (ISTA)
H. Engl (Univ. Wien)
H. Heugl (Wien)
W. Imrich (MU Leoben)
M. Kim (MathWorks)
M. Koth (Univ. Wien)
M. Kraker (Graz)
C. Krattenthaler (Univ. Wien)
W. Müller (Univ. Klagenfurt)
H. Niederreiter (ÖAW)
W. G. Nowak (Univ. Bodenkultur)
M. Oberguggenberger (Univ. Innsbruck)
W. Schachermayer (Univ. Wien)
K. Sigmund (Univ. Wien)
H. Sorger (Wien)
R. Tichy (TU Graz)
K. Unterkofler (FH Dornbirn)
H. Zeiler (Wien)

Vorsitzende von Sektionen und Kommissionen:

W. Woess (Graz)
H.-P. Schröcker (Innsbruck)
C. Heuberger (Klagenfurt)
F. Pillichshammer (Linz)
S. Blatt (Salzburg)
I. Fischer (Wien)
H. Humenberger (Didaktikkommission)
E. Aichinger (Verantwortlicher für Entwicklungszusammenarbeit)

Die Landesvorsitzenden und der Vorsitzende der Didaktikkommission gehören statutengemäß dem Beirat an.

Mitgliedsbeitrag:

Jahresbeitrag: € 35,–

Bankverbindung: IBAN AT83-1200-0229-1038-9200

Internationale Mathematische Nachrichten

International Mathematical News

Nouvelles Mathématiques Internationales

Nr. 248 (75. Jahrgang) **Dezember 2021**

Inhalt

Die Titelseite zeigt die epidemiologische Kurve von Covid-19 in Österreich im ersten Jahr der Pandemie. Die Daten stammen vom Dashboard der AGES. In diesem Jahr wurde “flatten the curve” zu einem viel zitierten Schlagwort, die effektive Reproduktionszahl, die 7-Tage-Inzidenz und andere Kennwerte sind einer informierten Öffentlichkeit nun bestens vertraut, exponentielles Wachstum ist für alle greifbarer geworden. In der Krise haben Mathematikerinnen und Mathematiker wichtige Sichtweisen beigesteuert und gemeinsam mit anderen Expertinnen und Experten somit einen wesentlichen Input für die Entscheidungen der Politik geliefert. Die Krise hat – so wie in allen Bereichen des Lebens – auch in der mathematischen scientific community für etliche Änderungen gesorgt. Videokonferenzen haben unseren Austausch geprägt. Offenbar geht es doch auch ohne Tafel, wenngleich die Diskussion und die Vermittlung von Ideen dabei gelitten hat!

Internat. Math. Nachrichten
Nr. 248 (2021), 1–15

How to Keep Your Secrets in a Post-Quantum World

Kristin Lauter
Facebook AI Research

1 Cryptography

Cryptography is the science of keeping secrets. But it is more than that. It is now a flourishing branch of mathematics that, in addition to encryption, also provides other tools to protect security and privacy of individuals, enterprises, data, systems, and transactions. Cryptographic protocols enable us, for example, to create secure communication channels, to guarantee the confidentiality and integrity of messages and data, to authenticate the identity of the sender of a message or the endpoint in a transaction. Cryptography is the foundation of secure e-commerce in the world today, providing the trustworthy systems that allow enterprises and consumers to transact business online. Digital signatures and key exchange are two important building blocks for public-key cryptography, in addition to encryption. Cryptographic systems are often built on the premise that certain math problems are very hard to solve, in the sense that known solutions require enormous computational time and resources. Many of these problems, such as factoring certain types of large numbers, have been studied by mathematicians for many decades. In fact, mathematicians often estimate the projected security of cryptographic systems by plotting the evolution in "running time" and "space requirements" of the best-known attacks. These predictions work well, but only in the absence of major

ISSN 0020-7926 — Österr. Math. Gesellschaft

disruptions: new algorithms or technologies that drastically improve the expected running time of attacks.

2 What Do We Mean by "Hard Math Problem"?

In practical applications of cryptography, we have a relatively well-agreed-upon meaning for the term "hard math problem": if the input is represented by m bits, then the best-known attack on the system runs in

$$\textit{exponential time} \text{ in } m, \ e.g., O(2^m) \text{ time}$$

or

$$\textit{subexponential time} \text{ in } m,$$
$$\text{e.g.,} L(\frac{1}{3}, c) = O(e^{c \cdot m^{\frac{1}{3}} (\log m)^{\frac{2}{3}}}) \text{ time, where } c \text{ is a constant.}$$

For example, to factor the number $n = p \cdot q$ where $m = \log n$, trial division takes *exponential time*. This is with respect to classical algorithms, which are represented on today's computers with circuits and with inputs and outputs given in terms of "classical" bits, i.e., sequences of 0s and 1s. *Polynomial time* algorithms run in time that is a *polynomial* in m, which often means in practice that an attack based on a polynomial time algorithm will succeed in a realistic amount of time and render the cryptographic system insecure.

3 Cryptographic Standards

There is a complex process for deploying new cryptographic protocols, especially when based on new hardness assumptions in mathematics. First, the research community needs to reach consensus on the above described process of modeling and giving precise, concrete cost estimates for the best-known attacks that solve the underlying math problem. Second, detailed standards are created through community or government processes such as:

1. a government agency like NIST (National Institute of Standards and Technology) in the United States runs a multiyear, open, international competition, e.g., the block cipher competition that standardized AES or the hash function competition that standardized SHA-3;

2. a professional society such as IEEE (Institute of Electrical and Electronics Engineers) or IETF (Internet Engineering Task Force) convenes a working

group or a committee to develop a draft standard, which is updated and revised over time, e.g., the IEEE P1363 that provided a foundational standard for elliptic curve cryptography (ECC);

3. a consortium consisting of researchers from a collection of interested parties in industry, government, and academia works together to publish a draft standard for reference, e.g., the PKCS standards governing the deployment of the RSA system or the new draft standard for Homomorphic Encryption HES 1.0 [1].

There can be substantial overlap in these first two stages of standardization. Once draft standards have been developed, there is a regulatory layer that is often developed requiring the deployment or adherence to various standards. Specialized standards are often developed for protocols to be used in vertical segments of the economy, such as when ANSI (American National Standards Institute) produced the X9.62 and X9.63 ECC standards for using elliptic curve key exchange and digital signature protocols in the financial services industry. Other examples of protocol-level standards include specifications for secure browser sessions (https: SSL/TLS); signed, encrypted email (S/MIME); virtual private networking (IPSec); and authentication (X.509 certificates).

Finally, there may be an ecosystem of third-party vendors that spring up to respond to the need to verify compliance with regulations. This is the current process for establishing public trust in the cryptographic systems we deploy. It is important that much of this process be public so that everyone can see that the systems were not cooked up in a back alley with some secret trapdoors or weaknesses built in.

The possibility of new, sometimes unexpected, attacks on fundamental cryptographic problems in mathematics, combined with the lengthy and complex standardization process, leaves us in a difficult and sometimes precarious position. Recent advances and substantial new investment in the development of quantum computers represent such a potential threat to our currently widely deployed public key cryptographic systems. This is due to the existence of a polynomial time quantum attack [19] on practically all of our currently deployed public key cryptosystems, which will be feasible to implement once a quantum computer can be built at a large enough scale. In response, NIST has launched a new, multiyear process to standardize post-quantum cryptography (PQC)[1]: i.e., cryptographic systems based on hard math problems for which we do not currently know *polynomial time quantum attacks*. The NIST PQC competition was launched in November 2017, and the twenty-six submissions for key exchange and digital signatures that have advanced to the second round were announced in January 2019.[2] Round 2 is expected to be a 12–18-month process. There may be a third round before NIST announces the post-quantum algorithms that will be recommended.

[1] https://csrc.nist.gov/Projects/Post-Quantum-Cryptography

[2] https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions

4 Pre-quantum (Classical) Systems

The NIST PQC selection process aims to identify candidates to supplement or replace three standards considered to be most vulnerable to a quantum attack: FIPS 186–4,[3] which specifies how to use digital signatures, and NIST SP 800–56A[4] and NIST SP 800–56B[5], which are specifications for key exchange. These currently widely deployed systems are based on "classically" hard problems, for which we do not know any classical polynomial time algorithms: RSA, Diffie–Hellman, and ECC. The RSA cryptosystem for encryption was proposed in the 1970s and is based on the hardness of factoring large integers that are the product of two prime numbers of equal size. Diffie–Hellman key exchange is based on the hardness of solving the discrete logarithm problem in the multiplicative group of integers modulo a large prime number. Elliptic curve cryptosystems are based on the hardness of solving ECDLP, the discrete logarithm problem in the abelian group of points on an elliptic curve over a finite field. Although there is a rich and beautiful mathematical theory of elliptic curves, developed over the course of more than one hundred years by mathematicians, cryptographers often think of an elliptic curve as simply the set of solutions to an affine equation in a finite field F_q. In characteristic not equal to 2 or 3, this equation is given in short Weierstrass form:

$$E: y^2 = x^3 + ax + b,$$

where a and b are constants in the base field F_q. The set of affine solutions, along with a "point at infinity" that can be seen in the projective version of the equation, forms a group where the point at infinity is the identity element. The group law can be described with concrete rational functions and has been widely implemented in industry to enable cryptographic systems, starting with Windows Vista and OpenSSL in 2005.

For RSA and Diffie–Hellman systems, classical subexponential attacks are known: the number field sieve and the index calculus attack; see the *Notices* article by Pomerance [16] for the history. Current key sizes for ECC systems are much smaller than for RSA or Diffie–Hellman because there are no known subexponential classical attacks on ECDLP for generic, ordinary elliptic curves. In 2006, the NSA published the Suite B algorithms, which provided guidance recommending adoption of ECC and mandated it for systems used by government contractors. In 2016, new guidance was released, recommending larger key sizes for ECC: 384 bits minimum instead of a 256-bit minimum. The revised guidance on the bit size raises the bar on the size of a quantum computer required to mount a successful quantum attack on ECC.

[3] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

[4] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar2.pdf

[5] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Br1.pdf

5 An Emerging Threat: The Quantum Computer

Many researchers, industrial labs, and governments are actively working on developing a quantum computer that can handle large-scale computation, such as the work at Station Q,[6] Microsoft's quantum computing headquarters. While classical computers – phones, tablets, laptops, servers, and so on – store and process information in the form of bits (strings of zeros and ones), quantum computers will process quantum bits, which are two-state quantum mechanical systems called qubits. In contrast to a classical bit, a qubit can simultaneously hold all values between zero and one, with each value having a specified probability. Then, when measured, the state of the qubit collapses to either zero or one. Small-scale quantum computers already exist, and estimates vary as to how many years it will take before researchers and engineers succeed in building a quantum computer that can handle computations involving thousands of qubits. However, when that day arrives, the consequences for the world's e-commerce and security infrastructure will be enormous.

Basic arithmetic on a quantum computer is different than on a classical computer. Computation on qubits is specified via quantum circuits consisting of quantum gates. Quantum logic gates are represented by unitary matrices. It remains to be seen which quantum gates and architectures will be achieved and scaled up in practice.

In 1994, Shor [19] introduced a quantum algorithm that can factor large integers in polynomial time, given a quantum computer that can accurately process those computations on a large enough number of qubits. A variant of this idea also allows polynomial-time quantum attacks on all of the other currently widely deployed public key cryptosystems used in industry and government today. Shor's algorithm for factoring on a quantum computer runs in $4m^3$ time and requires $2m$ qubits, where m is the number of bits required to represent the number to be factored ([17]). The current standard minimum for RSA moduli is $m = 2048$ bits. The Proos–Zalka estimates for attacking the elliptic curve discrete logarithm problem were updated in [18] to $9n + 2\log_2 n + 10$ qubits using a quantum circuit of at most $448n^3 \log_2 n + 4090n^3$ Toffoli gates for an ordinary elliptic curve over F_q where $n = \log_2 q$. The conclusion is that 2048-bit RSA and elliptic curve cryptography for $n = 256$ or 384 will not be resistant to quantum attacks once a quantum computer exists at scale.

[6] https://news.microsoft.com/stories/stationq/index.html

6 Post-Quantum Cryptography

The NIST Post-Quantum Cryptography (PQC) competition aims to select post-quantum cryptosystems that are not currently known to be breakable in polynomial time by a full-scale quantum computer. The following are the four main types of proposals for post-quantum systems based on hard math problems, in order of when the hard problem was first proposed in cryptography. Code-based cryptography has been studied for more than four decades, for example, whereas supersingular isogeny graphs have been studied for only about fifteen years. There are trade-offs in size, performance, and security for each proposal.

1. Code-based systems are based on the difficulty of decoding random linear error-correcting codes. McEliece introduced these cryptosystems in [12] using binary Goppa codes. Decoding Goppa codes efficiently is possible due to an algorithm of Patterson ([14]). The security of the schemes also relies on disguising the Goppa code as a general linear code.

2. Multivariate cryptosystems are based on the difficulty of solving systems of many nonlinear equations in many variables over a finite field F_q. Imai and Matsumoto introduced the C^* scheme in [11], and variants were introduced by Patarin and others in follow-up work. Although many proposed multivariate cryptographic systems have been broken, there are still viable proposals that have been submitted to the NIST PQC competition, such as Rainbow for signature schemes.

3. Lattice-based systems are based on the hardness of finding short vectors in lattices. Lattice-based cryptography was introduced in the mathematics community in 1996, when Hoffstein, Pipher, and Silverman ([8]) proposed the system called NTRU. NTRU can be interpreted as a lattice-based system that is especially efficient because of its description in a special kind of number ring.

   A lattice is a linear space generated by a choice of basis vectors. One can imagine it in Euclidean space, where a random set of linearly independent vectors is specified and the lattice consists of all points that are integer linear combinations of these vectors. Given an arbitrary basis with very long vectors in very large dimensions, it is a hard problem to find the shortest vector in the lattice. The best-known algorithms for solving the shortest vector problem run in exponential time in n, the dimension of the lattice. There are well-known polynomial time algorithms ([9]) for finding approximate solutions, but the ratio of the length of the approximate vector to the length of the shortest vector is exponentially bad.

4. Supersingular isogeny graph (SIG) systems were introduced in [4] based on the hard problem of finding paths between random vertices in large,

random-looking graphs. In particular, Charles, Goren, and Lauter proposed and implemented cryptographic hash functions based on supersingular isogeny graphs and presented it at the 2005 NIST Hash Function Workshop.

For more information on the first three proposed approaches and hard problems, see the NIST PQC website or the *IEEE Security and Privacy* magazine issue on post-quantum cryptography, which has short articles on each proposed candidate [3].

The rest of this article is devoted to explaining the mathematics of supersingular isogeny graphs and their applications in cryptography. Although this is the newest proposal among the four main approaches and thus requires further study to gain confidence in the security, the mathematics is interesting and compelling enough to merit exposition.

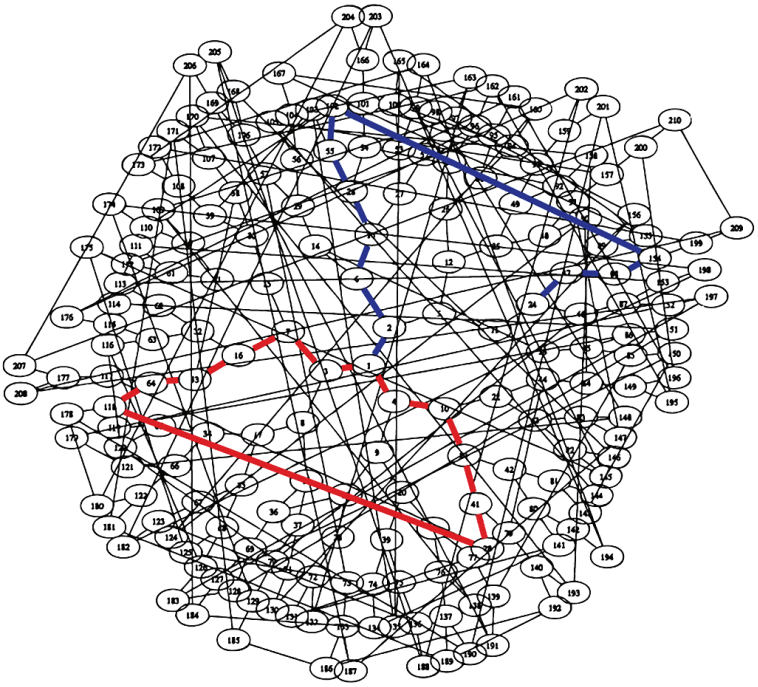

Fig. 1: Supersingular isogeny graph for $p = 2521$

7 Supersingular Isogeny Graphs

Supersingular isogeny graphs (SIG) were introduced as a hard problem into cryptography by Charles, Goren, and Lauter at the NIST Hash Function competition in 2005. The hard problem is *routing* in these graphs; i.e., given two nodes or

vertices in the graph, find a path between them (or find a path of a *certain length* between them).

We will define these graphs precisely later, but first, Figure 1 is a picture of a very small SIG, which we produced to appear in *Science* magazine in 2008 [10]. To get a feel for the hard problem underlying this proposal, pick two random points in the graph and try to find a path between them. Then try to imagine this same problem in a graph that has 10^{75} times as many vertices as this one.

8 Definition of Supersingular Isogeny Graphs

8.1 Supersingular elliptic curves

Let p and ℓ be two distinct prime numbers. For our cryptographic applications, p will be the characteristic of a finite field, which is a very large prime of cryptographic size, while ℓ will be the degree of a map and very small, typically $\ell = 2$ or 3. Elliptic curves were described above, and since the characteristic of the finite field is not equal to 2 or 3, we can work with the short Weierstrass equation for the elliptic curve: $E\colon y^2 = x^3 + ax + b$.

An elliptic curve over a finite field of characteristic p is *supersingular* if it has no p-torsion over its base field or any extension field. It is known that each isomorphism class of supersingular elliptic curves modulo p has a representative over the finite field of p^2 elements. Elliptic curves that are not supersingular are called ordinary. The *j-invariant* is an isomorphism invariant of an elliptic curve, and it can be easily computed as a rational function of the coefficients of the curve equation:

$$j(E) = 1728\frac{4a^3}{4a^3 + 27b^2}.$$

An *isogeny* between two elliptic curves is a morphism that preserves the group structure. The degree of a separable isogeny is the size of its kernel, so to construct an isogeny of degree ℓ from one elliptic curve E to another, take a subgroup C of size ℓ, and take the quotient E/C. In our setting, the prime ℓ is different from p, so the isogenies are all separable. Explicit formulae for isogenies of degree ℓ and the equation for E/C were given by Velu [21].

8.2 The graphs

Define the supersingular isogeny graph $G(p,\ell)$ to have vertex set equal to the set of isomorphism classes of supersingular elliptic curves over the algebraic closure of the finite field with p elements. The number of vertices of $G(p,\ell)$ is the Eichler

class number, which is roughly $\frac{p}{12}$ and depends on the congruence class of p modulo 12 ([20]). Vertices are labeled with their j-invariants, which can be computed directly from the curve equation.

The edges of the graph $G(p,\ell)$ are the isogenies of degree ℓ between elliptic curves, up to composing with an automorphism of the target curve. Since ℓ is prime and not equal to p, the number of distinct edges coming out of each vertex is $\ell+1$, because there are $\ell+1$ distinct subgroups of order ℓ of the ℓ-torsion of E. To make the graph undirected, we can associate an isogeny in one direction with its dual isogeny in the opposite direction. If we impose the congruence condition $p \equiv 1 \pmod{12}$, then there is no ambiguity and we can consider the graphs to be undirected [15, 4].

9 Expansion and Ramanujan Properties of the Supersingular Isogeny Graphs

We now summarize the basic properties of $G(p,\ell)$. These are connected graphs (see [13] or a special case of [5, Theorem 4.1]) with roughly $\frac{p}{12}$ vertices [20, Theorem 4.1]. If $p \equiv 1 \pmod{12}$, then they are undirected and $l+1$–regular, with vertices labeled by j-invariants.

In the next section we will describe cryptographic applications of these graphs. In particular [4] defined a hash function based on random walks on the graphs $G(p,\ell)$ for which the output should be as close to uniformly distributed as possible. But first we must define the concept of an expander graph and its expansion constant, which are closely correlated to this property. An *expander graph* with vertex set V and N vertices has expansion constant $c > 0$ if for any subset U of V of size

$$|U| \leq \frac{N}{2},$$

the boundary (neighbors of U not in U) satisfies

$$|\Gamma(U)| \geq c|U|.$$

The adjacency matrix of an undirected graph is symmetric, and therefore all its eigenvalues are real. For a connected k-regular graph, the largest eigenvalue is k, and all others are strictly smaller:

$$k > \mu_1 \geq \mu_2 \geq \cdots \geq \mu_{N-1}.$$

The expansion constant c can be expressed in terms of the eigenvalues as follows:

$$c \geq 2\frac{k-\mu_1}{3k-2\mu_1}.$$

Therefore, the smaller the eigenvalue μ_1, the better the expansion constant, and the distance between the first and second eigenvalues, $k - \mu_1$, is referred to as the *spectral gap*. A theorem of Alon–Boppana says that for an infinite family of connected, k-regular graphs, X_m, indexed by m, with the number of vertices in the graphs tending to infinity,

$$\liminf_{m\to\infty} \mu_1(X_m) \leq 2\sqrt{k-1}.$$

We define a *Ramanujan graph* to be a k-regular connected graph with optimal expansion properties in the sense that it satisfies

$$\mu_1 \leq 2\sqrt{k-1}.$$

A random walk on an expander graph mixes very fast, so the output of the hash function will be roughly uniform, provided the walk is long enough. The output of a random walk on an expander graph with N vertices tends to the uniform distribution after roughly $O(\log(N))$ steps, where the exact distance from the uniform distribution depends in a precise way on the expansion constant.

Supersingular isogeny graphs $G(p,\ell)$ are optimal expander graphs when $p \equiv 1 \pmod{12}$ in the sense that they are Ramanujan graphs (see [15, Prop. 4.7] or a special case of [5, Theorem 4.2]). The Ramanujan property of this graph follows from the fact that the adjacency matrix (called the Brandt matrix) gives the action of a Hecke operator on the space of weight 2 cusp forms of level p. So the bound on the eigenvalues follows from the corresponding result for modular forms (the Ramanujan–Petersson conjecture).

10 Applications

10.1 Cryptographic hash functions

A *hash function* maps bit strings to bit strings:

$$h\colon \{0,1\}^n \to \{0,1\}^m.$$

A hash function h is said to be *collision resistant* if it is computationally infeasible to find two distinct inputs, x, y, that hash to the same output, $h(x) = h(y)$. It is *preimage resistant* if, given any output of h, it is computationally infeasible to find an input, x, that hashes to that output. To be useful in cryptographic applications and protocols, hash functions should have at least the following properties: they should be easy to compute, unkeyed (do not require a secret key to compute output), collision resistant, and preimage resistant, with an approximately uniformly distributed output.

The cryptographic hash function proposed in [4] based on hardness of routing in supersingular isogeny graphs was defined as follows. A fixed vertex in the graph is specified as the starting point. The input bit string is divided into blocks and used as directions for walking around the graph. At each step in the walk, the choice of the next edge to follow is determined by the next block of bits of the input. No backtracking is allowed, since that would allow for trivial collisions of walks that go forward and backward along an edge at two different steps in the walk! The output of the hash function is the label for the final vertex of the walk. A family of hash functions can be defined by allowing the starting vertex to vary. For a k-regular expander graph with $k-1=2^e$ being a power of 2, the bits are read off in chunks of length e. For example, if $k=3$, then $e=1$ and bits are processed one at a time.

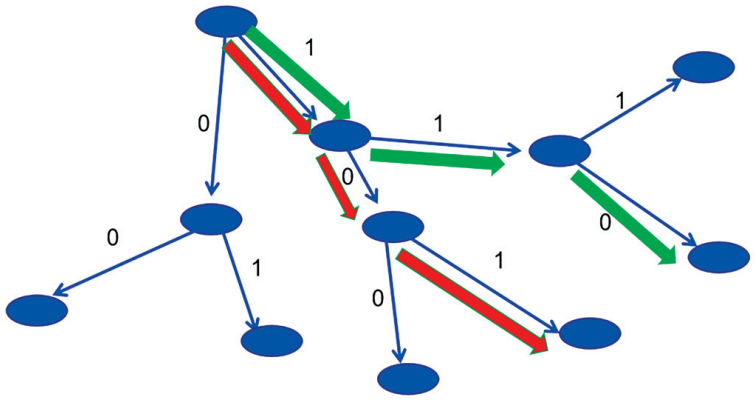

Fig. 2: Walk on a 3-regular graph: 110 is the green path and 101 is the red path

In order to avoid collisions in cryptographic hash functions based on isogeny graphs, it is best if the graph has no short cycles. Charles, Goren, and Lauter show in [4] how to ensure that isogeny graphs do not have short cycles by carefully choosing p to satisfy various congruence conditions. For example, they compute that a 2-isogeny graph does not have double edges (i.e., cycles of length 2) when working over F_p with $p \equiv 1 \pmod{420}$.

The security of the hash function relies on the hardness of finding paths, or *routing*, in this graph. If you can find a path between two given vertices of this graph, then you have found a *preimage* for the hash function specified by that starting point. Collisions and preimages can be found in the graph using the generic *birthday attack*, which involves randomly walking around the graph from two different starting points until a collision is detected. The birthday attack runs in time proportional to the square root of the size of the graph, $O(\sqrt{p})$. No better classical attacks are currently known. To achieve 128-bits of security against the birthday attack, in practice we pick p so that $\log p \approx 256$. The best-known quantum algorithm for computing isogenies between supersingular elliptic curves runs in time $O(p^{1/4})$, ignoring log factors [2].

10.2 Key exchange

One of the fundamental public key protocols being standardized in the NIST post-quantum cryptography competition is key exchange. Key exchange refers to a protocol for two parties to: 1. specify their public parameters; 2. each pick a secret; 3. publicly exchange information with each other; and 4. compute a common key that only the two parties know. The following key exchange protocol was proposed in [7].

Let E be a supersingular elliptic curve defined over the finite field with p^2 elements, where

$$p = \ell_A^m \ell_B^n \pm 1$$

and ℓ_A and ℓ_B are distinct small primes and m and n are balanced. In practice $\ell_A = 2$ and $\ell_B = 3$. In that case, m and n are roughly equal to $\frac{1}{2}\log_2 p$ and $\frac{1}{2}\log_3 p$, respectively.

Suppose two parties, A (for Alice) and B (for Bob), wish to engage in a key-exchange protocol with the goal of establishing a shared secret key by communicating via a (possibly) insecure channel. Alice and Bob generate their public parameters: Alice picks two points P_A and Q_A that generate the ℓ_A^m-torsion, and Bob picks two points P_B and Q_B that generate the ℓ_B^n-torsion.

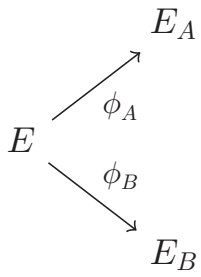

Fig. 3: First stage of supersingular isogeny key exchange

Alice then secretly picks two random positive integers m_A and n_A, which will be her secret parameters. She then computes the isogeny Φ_A from E to another curve E_A, which corresponds to taking the quotient of E by the subgroup generated by $m_A P_A + n_A Q_A$. Bob does the same and secretly picks two random positive integers m_B and n_B. He then computes the secret isogeny Φ_B by taking the quotient of E by the subgroup generated by $m_B P_B + n_B Q_B$.

So far, Alice and Bob have constructed the diagram shown in Figure 3.

In the next stage of the exchange protocol, Alice computes $\Phi_A(P_B)$ and $\Phi_A(Q_B)$ and sends $\{\Phi_A(P_B), \Phi_A(Q_B), E_A\}$ to Bob. Similarly, Bob computes and sends $\{\Phi_B(P_A), \Phi_B(Q_A), E_B\}$ to Alice. Both players now have enough information to construct the diagram shown in Figure 4, where $E_{AB} = E/\langle m_A P_A + n_A Q_A, m_B P_B + n_B Q_B \rangle$. Alice can use the secret information m_A and n_A to compute the isogeny Φ'_B

by taking the quotient of E_B by the subgroup generated by $m_A\Phi_B(P_A)+n_A\Phi_B(Q_A)$ to obtain E_{AB}. Bob can use the secret information m_B and n_B to compute the isogeny Φ'_A, taking the quotient of E_A by the subgroup generated by $m_Bn_A(P_B)+n_B\Phi_A(Q_B)$ to obtain E_{AB}. A separable isogeny is determined by its kernel, and so both ways of going around the diagram from E result in computing the same elliptic curve E_{AB}. Alice and Bob can both compute the curve E_{AB} and use its j-invariant as a shared secret.

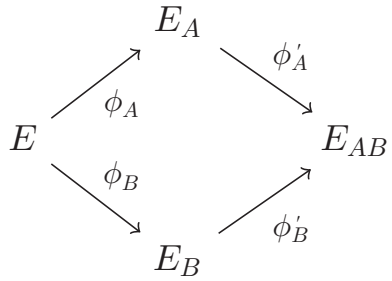

Fig. 4: Completion of supersingular isogeny key exchange

11 A Security Reduction

The security of the supersingular isogeny key-exchange protocol (SIKE) is based on a hardness assumption stated in [7], called the supersingular computational Diffie–Hellman (SSCDH) problem. However, the connection with the path-finding problem introduced in [4] was not published until the paper by Costache, Feigon, Lauter, Massierer, and Puskas [6], which showed that the SSCDH problem is no harder than the CGL-path-finding problem, and it is entirely possible that it is easier to solve, given that there is more auxiliary information available in the SSCDH problem.

Theorem ([6])**.** *Assume as for the key exchange setup that $p=\ell_A^m\ell_B^n\pm 1$ is a prime of cryptographic size, i.e.,* $\log p \geq 256$*, ℓ_A and ℓ_B are distinct small primes, and m and n are balanced so that ℓ_A^m is approximately ℓ_B^n. In practice $\ell_A=2$ and $\ell_B=3$. Given an algorithm to solve the CGL path-finding problem in supersingular isogeny graphs, it can be used to break the supersingular key exchange with overwhelming probability. The failure probability is roughly $\frac{1}{\sqrt{p}}$.*

12 Conclusion

While mathematicians have been researching the hard problem of factoring large integers for centuries, we are now faced with the prospect that our future security may depend on the hardness of mathematical problems that have been studied

by mathematicians for only a matter of decades. This disconcerting fact is made worse by the fact that there is an urgent need to understand both the classical and the quantum security of these new proposals. So the current answer to the question in my title is "We don't know yet!" It is clear, though, that there are very interesting mathematical problems that could serve as the basis of the next generation of post-quantum secure cryptosystems–we just need more mathematicians working on them to understand the security!

To apply for NSF funding for research projects in cryptography and cybersecurity, visit the program solicitation for Secure and Trustworthy Cyberspace (SaTC).[7]

References

[1] M. Albrecht, M. Chase, H. Chen, J. Ding, S. Goldwasser, S. Gorbunov, S. Halevi, J. Hoffstein, K. Laine, K. Lauter, S. Lokam, D. Micciancio, D. Moody, T. Morrison, A. Sahai, and V. Vaikuntanathan. Homomorphic Encryption Standard. Cryptology ePrint Archive, Report 2019/939, 2019. https://ia.cr/2019/939.

[2] J.-F. Biasse, D. Jao, and A. Sankar. A quantum algorithm for computing isogenies between supersingular elliptic curves. In *Progress in cryptology–INDOCRYPT 2014*, volume 8885 of *Lecture Notes in Comput. Sci.*, pages 428–442. Springer, 2014.

[3] J. Buchmann, K. Lauter, and M. Mosca. Postquantum cryptography–state of the art. *IEEE Security & Privacy*, 15(4):12–13, 2017.

[4] D. X. Charles, E. Z. Goren, and K. E. Lauter. Cryptographic hash functions from expander graphs. *J. Cryptology*, 22(1):93–113, 2009.

[5] D. X. Charles, E. Z. Goren, and K. E. Lauter. Families of Ramanujan graphs and quaternion algebras. In *Groups and symmetries*, volume 47 of *CRM Proc. Lecture Notes*, pages 53–80. Amer. Math. Soc., Providence, RI, 2009.

[6] A. Costache, B. Feigon, K. Lauter, M. Massierer, and A. Puskas. Ramanujan graphs in cryptography. In *Research directions in number theory–Women in Numbers IV*, volume 19 of *Assoc. Women Math. Ser.*, pages 1–40. Springer, 2019.

[7] L. De Feo, D. Jao, and Jérôme Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *J. Math. Cryptol.*, 8(3):209–247, 2014.

[8] J. Hoffstein, J. Pipher, and J. H. Silverman. NTRU: a ring-based public key cryptosystem. In *Algorithmic number theory*, volume 1423 of *Lecture Notes in Comput. Sci.*, pages 267–288. Springer, Berlin–Heidelberg, 1998.

[9] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261(4):515–534, 1982.

[10] D. Mackenzie. Cryptologists cook up some hash for new 'bake-off'. *Science Magazine*, 319:1480–1481, 2008.

[11] T. Matsumoto and H. Imai. Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. In *Advances in cryptology–*

[7] https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=504709

EUROCRYPT '88 (Davos, 1988), volume 330 of *Lecture Notes in Comput. Sci.*, pages 419–453. Springer, Berlin, 1988.

[12] R. J. McEliece. A Public-Key Cryptosystem Based On Algebraic Coding Theory. *DSN Progress Report*, 44:114–116, 1978.

[13] J.-F. Mestre. La méthode des graphes. Exemples et applications. *Taniguchi Sympos.*, 1986.

[14] N. J. Patterson. The algebraic decoding of Goppa codes. *IEEE Trans. Inform. Theory*, IT-21:203–207, 1975.

[15] A. K. Pizer. Ramanujan graphs and Hecke operators. *Bull. Amer. Math. Soc. (N.S.)*, 23(1):127–137, 1990.

[16] Carl Pomerance. A tale of two sieves. *Notices Amer. Math. Soc.*, 43(12):1473–1485, 1996.

[17] J. Proos and C. Zalka. Shor's discrete logarithm quantum algorithm for elliptic curves. *Quantum Inf. Comput.*, 3(4):317–344, 2003.

[18] M. Roetteler, M. Naehrig, K. M. Svore, and K. Lauter. Quantum resource estimates for computing elliptic curve discrete logarithms. In T. Takagi and T. Peyrin, editors, *Advances in Cryptology – ASIACRYPT 2017*, pages 241–270. Springer International Publishing, 2017.

[19] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997.

[20] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[21] Jacques Vélu. Isogénies entre courbes elliptiques. *C. R. Acad. Sci. Paris Sér. A-B*, 273:A238–A241, 1971.

Author's address:
Facebook AI Research
Seattle, WA, USA
email kristinelauter@gmail.com

Internat. Math. Nachrichten
Nr. 248 (2021), 17–27

σ-Projective Sets of Reals, Cut Elimination, and Large Cardinals

Juan P. Aguilera
Vienna University of Technology

1 Introduction

A set $A \subset \mathbb{R}$ is σ-projective if it belongs to the smallest σ-algebra of subsets of $\mathbb{R}$ which contains the open sets and is closed under continuous images.

Much like the Borel sets, the σ-projective sets can be generated by an inductive procedure of transfinite length. One way of doing this is as follows: inductively define

1. $\Sigma^1_1 =$ the collection of all analytic sets (continuous images of Borel sets);
2. $\Pi^1_\alpha =$ the collection of all complements of sets in Σ^1_α;
3. $\Sigma^1_{\alpha+1} =$ the collection of all continuous images of sets in Π^1_α;
4. $\Sigma^1_\lambda =$ the collection of all unions of countably many sets, each in some Σ^1_α with $\alpha < \lambda$, if λ is a limit ordinal.

Using (a weak version of) the Axiom of Choice, one shows that a set is σ-projective if and only if it belongs to Σ^1_α for some countable ordinal α. An important subcollection of the σ-projective sets is comprised of all sets of the form Σ^1_n, for $n \in \mathbb{N}$; these are the *projective sets*. Projective sets are commonly studied in Descriptive Set Theory because of their logical properties, and the methods employed generalize, in one way or another, to the σ-projective sets. These sets are very interesting from a foundational perspective: even at the low levels of the projective hierarchy many questions (Lebesgue measurability of sets in Σ^1_n, the

ISSN 0020-7926

existence of an uncountable wellordered sequence of reals in Σ^1_n) are independent of ZFC.

The goal of this article is to collect some game-theoretic, proof-theoretic, and set-theoretic principles about σ-projective sets and state theorems whereby these principles are all equivalent to each other, but unprovable within ZFC.

2 Infinite games

We consider infinite two-player, perfect-information games on the real numbers. These can be thought of as follows: the game begins with a set of *rules*; this is a subset A of $\mathbb{R}$ (or just of the unit interval $[0,1]$). Two players, I and II, alternate turns playing digits $x(i) \in \{0,1,2,3,4,5,6,7,8,9\}$. After infinitely many turns, the play leads to the construction of a real number

$$x = \sum_{i=0}^{\infty} \frac{x(i)}{10^{i+1}} \in [0,1].$$

Player I wins if and only if $x \in A$; otherwise, Player II wins. The game is said to be *determined* if one of the players has a winning strategy, in which case we also say that A itself is determined.

Definition 1. *Let Γ be a class of sets of real numbers.* Γ-determinacy *is the assertion that all sets in Γ are determined.*

Determinacy is a kind of master regularity property: if a class of sets Γ is modestly closed, then all sets in Γ enjoy many desirable properties, such as having the property of Baire (Banach and Mazur), being Lebesgue measurable (Mycielski and Świerczkowski), and having the perfect set property (Davis).

The history of determinacy is long and fascinating. A more detailed overview can be found in Larson [12]. Gale and Stewart [8] proved Γ-determinacy when $\Gamma =$ the collection of all open sets. Wolfe [21] improved this result to $\Gamma =$ the collection of all F_σ sets, and Davis [6] to the collection of all $G_{\delta\sigma}$ sets. At this point, the natural expectation arose that all Borel sets are determined. Indeed, a more ambitious – yet vague – suspicion emerged that all "definable" sets of reals should be determined. The principle that *all* sets are determined is called the *Axiom of Determinacy* and was introduced by Mycielski and Steinhaus [18]. It can be disproved using the Axiom of Choice. However, this is necessary: a theorem of Woodin (see [22]) states that ZF with the Axiom of Determinacy is consistent if and only if ZFC is consistent with the existence of infinitely many Woodin cardinals.

Martin [13] proved that all Σ^1_1 sets are determined. However, Martin's proof had an unusual feature: it made use of a *large-cardinal axiom* which transcended ZFC.

Large cardinal axioms are principles asserting the existence of various very large sets. These sets usually satisfy all axioms of ZFC themselves, and so they cannot be proved to exist within ZFC, by Gödel's second incompleteness theorem. Examples of these are inaccessible cardinals, measurable cardinals, and Woodin cardinals. Martin showed that if there is a measurable cardinal, then all Σ^1_1 sets are determined. His proof, however, only made use of a slightly weaker form of measurability, and this hypothesis was proved necessary by Harrington [11].

Motivated by Martin's theorem, Friedman [7] proved a theorem of a very different nature. Regardless of whether Borel determinacy is provable in ZFC, any potential proof of it must make crucial and essential use of all the axioms of ZFC. In particular, if one removes from ZFC either the Powerset axiom or the Replacement axiom, then Borel determinacy cannot be proved. Armed with the knowledge imparted by Friedman's theorem, Martin [14] finally showed that Borel determinacy is indeed provable in ZFC.

Afterwards, the goal became to prove the determinacy of increasingly complex sets, perhaps aided by the use of large-cardinal axioms. Martin and Steel [15] showed that if there are n Woodin cardinals below a measurable cardinal, then all Π^1_{n+1} sets are determined. Woodin (see Müller-Schindler-Woodin [17]) showed that, in a sense, this hypothesis is necessary. Woodin (see [22] for a proof from a stronger hypothesis) showed that if there are infinitely many Woodin cardinals, then classes of sets much larger than the σ-projective sets are determined. The principle of σ-projective determinacy is thus weaker than infinitely many Woodin cardinals, but stronger than all finite amounts of Woodin cardinals.

3 Games of transfinite length

Much like the infinite games of length $\mathbb{N}$, one can consider games of transfinite length. Let us focus on the following class of games of length $\mathbb{N} \times \mathbb{N}$: one begins by fixing a payoff set A in $\mathbb{R}$ as before. This time, one also fixes a bijection

$$\rho : \mathbb{N} \times \mathbb{N} \to \mathbb{N},$$

e.g., $(n,m) \mapsto 2^n \times (2m+1) - 1$. Let us define projection functions π_0 and π_1 for the inverse of ρ, so that

$$\rho^{-1}(i) = (\pi_0(i), \pi_1(i)) \quad \text{for all } i \in \mathbb{N}.$$

In the game, Players I and II alternate infinitely many turns playing digits $x(i)$, producing a real number $x \in [0,1]$ as before. Let us write $x_0 := x$. After this is done, Players I and II alternate infinitely many more turns playing digits $x_1(i)$ and producing a second real number $x_1 \in [0,1]$. This is done infinitely often, so that

eventually infinitely many real numbers

$$x_j = \sum_{i=0}^{\infty} \frac{x_j(i)}{10^{i+1}}$$

are produced. These infinitely many numbers can be re-coded into a single real number by setting

$$x_\omega = \sum_{i=0}^{\infty} \frac{x_{\pi_0(i)}(\pi_1(i))}{10^{i+1}}.$$

Player I wins the game if and only if $x_\omega \in A$.

Longer games are much harder to win compared to short games, if one fixes the complexity of the payoff set. By the Gale-Stewart theorem, open determinacy for short games is true and provable in ZFC and, in fact, many of the axioms of ZFC (such as the Powerset axiom) are not needed for the proof. In contast, open determinacy for games of length $\mathbb{N} \times \mathbb{N}$ is not provable in ZFC and indeed it is strictly stronger than σ-projective determinacy for games of length $\mathbb{N}$. A weakening of open determinacy for long games, however, captures the strength of σ-projective determinacy for short games. Let us say that a set $A \subset \mathbb{R}$ is *clopen* if $A \setminus \mathbb{Q}$ is clopen in the space $\mathbb{R} \setminus \mathbb{Q}$ with the induced topology. For undefined terms in Theorem 1 below, we refer the reader to [5].

Theorem 1. *The following are equivalent over* ZFC*:*

1. σ*-projective determinacy;*
2. *all clopen games of length* $\mathbb{N} \times \mathbb{N}$ *are determined;*
3. *all simple clopen games of length* $\mathbb{N} \times \mathbb{N}$ *are determined; and*
4. *all simple* σ*-projective games of length* $\mathbb{N} \times \mathbb{N}$ *are determined.*

The implications from (2) to (4) and from (3) to (2) were proved jointly with S. Müller and P. Schlicht in [5], where the notion of *simple games* was introduced. The implication from (1) to (2) was later proved in [1]. (The implications from (4) to (3) and (1) are trivial.)

4 Cut elimination

Gödel's second incompleteness theorem states that no consistent, recursively enumerable extension of Peano Arithmetic proves its own consistency. Gödel's theorem gave rise to a re-imagined version of Hilbert's program, whose goal can be vaguely phrased as: *what are the necessary infinitary ingredients of a consistency*

proof of arithmetic? Such program arose from Gentzen's [9] consistency proof of arithmetic. Gentzen's proof proceeded as follows. He devised a syntactic calculus of proofs, where one works with expressions of the form

$$\Gamma \vdash \Delta,$$

where Γ and Δ are finite sets of formulas. The intended interpretation is "if all formulas in Γ are true, then some formula in Δ is true." Gentzen's calculus works with *rules* of the form "from $\Gamma \vdash \Delta$, infer $\Gamma' \vdash \Delta'$". An example of this is

$$\frac{\Gamma \vdash \Delta, A}{\Gamma \vdash \Delta, A \vee B},$$

which captures the principle "under any context, from A, deduce $A \vee B$." The calculus also asserts that some sequents are *axioms* and can be taken to be true, namely, those of the form $A \vdash A$. Gentzen's calculus has the property that every formula which appears in a sequent in a derivation also appears in every sequent following it, with one exception, the *cut* rule:

$$\frac{\Gamma \vdash \Delta, A \quad A, \Gamma \vdash \Delta}{\Gamma \vdash \Delta},$$

which states that if (i) A and Γ imply Δ and (ii) Γ implies either Δ or A, then Γ implies Δ.

Gentzen showed that his calculus precisely captures first-order logic. The *cut-elimination theorem* states that if a sequent $\Gamma \vdash \Delta$ is provable in the calculus, then it is provable without using the cut rule. An immediate consequence is that the calculus is consistent: suppose otherwise, so that a formula A and its negation $\neg A$ are both provable. The rule for introducing negation in the calculus is

$$\frac{\Gamma, \vdash \Delta, A}{\Gamma, \neg A \vdash \Delta.}$$

Thus, if A and $\neg A$ were both provable, then, by applying the negation rule and the cut role, we obtain a derivation of the empty sequent:

$$\frac{\dfrac{}{\vdash A} \quad \dfrac{}{\neg A \vdash}}{\vdash}.$$

However, the cut-elimination theorem now implies that the empty sequent is provable without using the cut rule, which is absurd.

Gentzen's consistency proof for arithmetic followed a similar idea, except that the calculus had to be modified in order that arithmetic be properly embeddable into

it. The cut-elimination procedure then becomes much more involved, enough that it cannot be provably total in arithmetic, and necessarily so – by Gödel's theorem.

Genzen's work was the first landmark result in proof theory and has been expanded in a wide variety of directions ever since, including consistency proofs for stronger systems, methods for abstracting mathematical content from non-constructive proofs, and abstract proof theory for infinitary systems. Let us mention a result in the latter direction.

Takeuti [20] introduced an infinitary proof system for *Determinate Logic*. This system dealt with infinitary formulas. These are built from possibly infinitary *atomic* formulas of the form

$$A(x_0, x_1, x_2, \ldots)$$

by applying negations, conjunctions, disjunctions, implications (as usual), but also infinitary conjunctions and disjunctions, such as

$$A_0 \vee A_1 \vee A_2 \vee A_3 \vee A_4 \vee \ldots,$$

interpreted in the natural way. It also allowed for expressions of the form

$$Q_0 x_0 \, Q_1 x_1 \, Q_2 x_2 \, Q_3 x_3 \ldots A(x_1, x_2, x_3, \ldots),$$

where each Q_i is a quantifier $\exists$ or $\forall$. Takeuti's system is the natural extension of Gentzen's calculus for deriving expressions in this language and it captures the logic of these expressions just like Gentzen's system captures first-order logic. The only other difference worth noting is that the axioms of Determinate Logic impose the restriction that the predicates $A(x_0, x_1, \ldots)$ range over (at most) countable domains.

Takeuti's system also features the cut rule (defined exactly the same as before). It then becomes a natural question whether one can prove an analogue of Gentzen's cut-elimination theorem. Takeuti essentially showed that the cut-elimination theorem can be proved if, and only if, the Axiom of Determinacy holds. In particular, one cannot prove the cut-elimination theorem for Determinate Logic if the Axiom of Choice holds.

The next question is how much the Axiom of Choice can be reconciled with the cut-elimination theorem for Determinate Logic. It turns out that – without changing any of the rules of the calculus – a simple modification to the *language* suffices. Namely, it suffices to demand that atomic formulas be finitary, i.e., all of the form

$$A(x_0, x_1, x_2, \ldots, x_n).$$

Infinite conjunctions and quantifier strings are still allowed. Indeed not only is the cut-elimination theorem consistent with the Axiom of Choice, but one obtains the following equivalence:

Theorem 2. *The following are equivalent over* ZFC*:*

1. *σ-projective determinacy; and*

2. *Takeuti's Determinate Logic satisfies the cut-elimination theorem for languages all of whose atomic formulas are finitary.*

A proof of the theorem can be found in [4].

5 Large cardinals and inner models

We have mentioned before that σ-projective determinacy lies in strength between infinitely many Woodin cardinals and all finite amounts of Woodin cardinals. Logically speaking, this means that of the three systems:

1. ZFC + {"there are n Woodin cardinals": $n \in \mathbb{N}$}[1];

2. ZFC + σ-projective determinacy;

3. ZFC + "there are infinitely many Woodin cardinals";

each proves the consistency of the previous one. [This situation is possible because of the compactness theorem: suppose the theory (1) were inconsistent, so that there is a proof of a contradiction from the axioms. Such a proof is necessarily finite, so it can only make use of finitely many axioms. Hence, in order to prove that (1) is consistent, one needs only prove, for each n, that the theory ZFC + "there are n Woodin cardinals" is consistent. This alone does not suffice to conclude that (3) is also consistent.]

Typically, there is nothing to be found between all finite quantities and infinity, so it might not be immediately clear how to describe the strength of σ-projective determinacy in terms of Woodin cardinals. The solution is to speak in terms of *inner models*. This is a technique that goes back to Gödel's [10] consistency proof for the Axiom of Choice and the Generalized Continuum Hypothesis. The idea is to consider structures which satisfy the axioms of set theory (and possibly more) and are, in a way, *minimal*.

[1] This is a set of infinitely many axioms, indexed by natural numbers.

Gödel's model L is constructed by transfinite recursion as follows:

$$\begin{aligned} L_0 &= \varnothing; \\ L_{\alpha+1} &= L_\alpha \cup \text{ every subset of } L_\alpha \text{ that can be defined from elements of } L_\alpha; \\ L_\lambda &= \bigcup_{\alpha<\lambda} L_\alpha \quad \text{ at limit stages;} \\ L &= \bigcup_{\alpha\in\mathsf{Ord}} L_\alpha. \end{aligned}$$

Gödel showed that L satisfies the axioms of ZFC together with the Generalized Continuum Hypothesis (this was his consistency proof).

By a theorem of Scott, however, L cannot have any measurable (and hence any Woodin) cardinals, so it is inadequate for our purposes. However, the models we will need are obtained in a similar, though more involved, way. They are obtained much like L, except that they make use of a certain external predicate E. The reader might think of this as analogous to the notion of computability relative to an oracle (if he or she is familiar with it). More precisely, the successor clause in the definition of L is replaced by allowing definability which makes reference to E. The resulting model is called $L[E]$. The predicates E to be used are certain type of *extender sequences*, and their description is lengthy. They were introduced in their current incarnation by Mitchell and Steel [16], though their story begins earlier.

By choosing the predicate E appropriately, one arrives at certain canonical models, which are minimal with respect to several properties. Rather than iterating the recursive construction through all ordinals, it will often suffice to stop at a certain countable stage and obtain analogues of L_α. Letting $M = L[E]$, let us write

$$M|\alpha = L_\alpha[E].$$

For a given $n \in \mathbb{N}$, the (countable) model $M_n^\sharp$ is obtained this way. This is a very important model of set theory with the property that there exist

$$\delta_1, \delta_2, \ldots, \delta_n \in M_n^\sharp \cap \mathsf{Ord}$$

such that for each i, we have

$$M_i^\sharp \models \text{“}\delta_i \text{ is a Woodin cardinal.”}$$

ZFC alone does not suffice to prove the existence of $M_n^\sharp$, but it can be proved to exist if there are n Woodin cardinals and a measurable cardinal greater than them (this is a theorem of Steel [19]). A theorem of Woodin (see Müller-Schindler-Woodin [17]) states that projective determinacy holds if and only if $M_n^\sharp$ exists for

all $n \in \mathbb{N}$. Thus, the strength of projective determinacy is captured by the existence of the elements of the sequence

$$M_0^\sharp, M_1^\sharp, M_2^\sharp, \ldots,$$

as is the strength of all finite amounts of Woodin cardinals. In order to describe the strength of σ-projective determinacy, we need to extend this sequence to the transfinite and form a certain sequence

$$N_0^\sharp, N_1^\sharp, N_2^\sharp, \ldots, N_\omega^\sharp, N_{\omega+1}^\sharp, \ldots.$$

Without defining them precisely, let us describe the models $N_\alpha^\sharp$. The models $N_i^\sharp$ will be the same as $M_i^\sharp$ for $i \in \mathbb{N}$. The model $N_\omega^\sharp$ is a sort of "sum" of the $N_i^\sharp$s. It has the property that for each $n \in \mathbb{N}$ one can find $\alpha_n \in \mathsf{Ord} \cap N_\omega^\sharp$ and ordinals $\delta_1^n, \delta_2^n, \delta_3^n, \ldots, \delta_n^n$ such that for each i, we have

$$N_\omega^\sharp | \alpha_n \models \text{“}\delta_i^n \text{ is a Woodin cardinal.”}$$

However, we will have

$$N_\omega^\sharp \not\models \text{“}\delta_i^n \text{ is a Woodin cardinal.”}$$

Thus, some initial segment of $N_\omega^\sharp$ will think that δ_i^n is a Woodin cardinal, but $N_\omega^\sharp$ will contain some additional information letting it know that δ_i^n is not in fact one. Indeed, δ_i^n will not even be a cardinal in $N_\omega^\sharp$ – there will be some bijection $f : \omega \to \delta_i^n$ with $f \in N_\omega^\sharp$, but (naturally) $f \notin N_\omega^\sharp | \alpha_n$.

$N_{\omega+1}^\sharp$ will relate to $N_\omega^\sharp$ as $N_{i+1}^\sharp$ relates to $N_i^\sharp$. It will have one single Woodin cardinal δ and it will resemble $N_\omega^\sharp$ above δ.

In general, as α increases, the models $N_\alpha^\sharp$ will have a more and more complicated structure of ordinals which various initial segments think are Woodin cardinals and others do not. The way these initial segments are configured yield higher and higher consistency strength for $N_\alpha^\sharp$.

Eventually, for large enough α one runs into trouble attempting to define $N_\alpha^\sharp$, and the reason for this comes from the fact that the candidate model for $N_\alpha^\sharp$ thinks that α is a cardinal (while in reality it is countable). The solution for this is to replace the use of $N_\alpha^\sharp$ by a *relativized* version $N_\alpha^\sharp(x)$, where $x \in \mathbb{R}$. This is a structure of the form $L_\gamma[E](x)$ which has access to both E and x as oracles. The theorem is:

Theorem 3. *The following are equivalent over* ZFC*:*

1. σ*-projective determinacy;*

2. *for each countable ordinal* α*,* $N^{\sharp}_{\alpha}(x)$ *exists for some* $x \in \mathbb{R}$*;*

3. *for each countable ordinal* α*,* $N^{\sharp}_{\alpha}(x)$ *exists for almost all* $x \in \mathbb{R}$*.*

A proof (joint with S. Müller and P. Schlicht) of the implication from (2) to (1) can be found in [5]. A different proof of this implication, as well as a proof of the implication from (1) to (3), can be found in [2]. (The remaining implication is trivial.)

6 Acknowledgements

Aside from the cited articles, the theorems mentioned herein appeared in the author's PhD dissertation [3] (Chapters 4,5,7, and 13), written under the advice of M. Baaz and W. H. Woodin. The work surveyed in this article was partially supported by FWF grants P31955 and P31063. The typing of this article was partially supported by FWF grant I4513N and FWO grant 3E017319.

References

[1] J. P. Aguilera. Shortening clopen games. *J. Symbolic Logic*. In press, doi:10.1017/jsl.2021.2.

[2] J. P. Aguilera. σ-Projective Determinacy. Forthcoming.

[3] J. P. Aguilera. *Between the Finite and the Infinite*. 2019. Ph.D. Thesis, Vienna University of Technology.

[4] J. P. Aguilera. Determinate logic and the axiom of choice. *Ann. Pure Appl. Logic* 171:102745, 2020.

[5] J. P. Aguilera, S. Müller, and P. Schlicht. Long games and σ-projective sets. *Ann. Pure Appl. Logic* 172:102939, 2021.

[6] M. Davis. Infinite games of perfect information. In *Advances in Game Theory*, pages 85–101. Princeton University Press, 1964.

[7] H. M. Friedman. Higher set theory and mathematical practice. *Ann. Math. Logic*, 2(3):325 – 357, 1971.

[8] D. Gale and F. M. Stewart. Infinite games with perfect information. In H. W. Kuhn and A. W. Tucker, editors, *Contributions to the Theory of Games*, volume 2, pages 245–266. Princeton University Press, 1953.

[9] G. Gentzen. Die Widerspruchsfreiheit der reinen Zahlentheorie. *Math. Ann.*, 112:493–565, 1936.

[10] K. Gödel. The consistency of the axiom of choice and the generalized continuum hypothesis. *Proc. Nat. Acad. Sci. USA*, 25:556–557, 1938.

[11] L. Harrington. Analytic Determinacy and $0^{\#}$. *Journal of Symbolic Logic*, 43:685–693, 1978.

[12] P. B. Larson. A brief history of determinacy. In A. S. Kechris, B. Löwe, and J. R. Steel, editors, *Large Cardinals, Determinacy, and Other Topics: The Cabal Seminar, Volume IV*. Cambridge University Press, 2020.
[13] D. A. Martin. Measurable cardinals and analytic games. *Fund. Math.*, 66:287–291, 1970.
[14] D. A. Martin. Borel Determinacy. *Ann. Math.*, 102(2):363–371, 1975.
[15] D. A. Martin and J. R. Steel. A proof of projective determinacy. *J. Amer. Math. Soc.*, 2:71–125, 1989.
[16] W. J. Mitchell and J. R. Steel. *Fine structure and iteration trees*. Lecture notes in logic. Springer-Verlag, Berlin, New York, 1994.
[17] S. Müller, R. Schindler, and W. H. Woodin. Mice with Finitely many Woodin Cardinals from Optimal Determinacy Hypotheses. *J. Math. Logic* 20:1950014, 2020.
[18] J. Mycielski and H. Steinhaus. A Mathematical Axiom Contradicting the Axiom of Choice. *Bull. Acad. Pol. Sci. Ser. Math. Astr. Phys.*, 10:1–3, 1962.
[19] J. R. Steel. Inner models with many Woodin cardinals. *Ann. Pure Appl. Logic*, 65:185–209, 1993.
[20] G. Takeuti. *Proof Theory*. 1975.
[21] P. Wolfe. The strict determinateness of certain infinite games. *Pacific J. Math.*, 5:841–847, 1955.
[22] W. H. Woodin. Supercompact cardinals, sets of reals, and weakly homogeneous trees. *Proc. Natl. Acad. Sci. USA*, 85(18):6587-6591, 1988.

Authors' address:
Institute of Discrete Mathematics and Geometry, Vienna University of Technology. Wiedner Hauptstraße 8–10, 1040 Vienna, Austria
Department of Mathematics, University of Ghent. Krijgslaan 281-S8, B9000 Ghent, Belgium
email aguilera@logic.at

Internat. Math. Nachrichten
Nr. 248 (2021), 29–39

Bemerkungen über Pseudozufallszahlen und deren Anwendung zur Komposition von Walzern

Robert F. Tichy und Reinhard Winkler†
TU Graz und TU Wien

Dieser Artikel ist erstmals vor 30 Jahren in den Sitzungsberichten der Österreichischen Akademie der Wissenschaften *(„Bemerkungen über Pseudozufallszahlen und deren Anwendung zur Komposition von Walzern", Robert Tichy und Reinhard Winkler, Sitzungsberichte d. Österr. Akad. d. Wiss., Abt. II, Math.-Nat. Klasse 200, Nr. 1–10 (1991), 53–63) erschienen. Der Nachdruck erfolgt mit freundlicher Erlaubnis von Robert Tichy und des Verlags der ÖAW.*

Vorwort von Robert Tichy (Graz) zum Nachdruck: Als ich Reinhard Winkler näher kennenlernte – er hatte bei mir an der TU Wien dissertiert und war dann Mitarbeiter von Edmund Hlawka in der Kommission für Mathematik der Österreichischen Akademie der Wissenschaften –, konnte ich mit ihm viele anregende Gespräche über unterschiedliche Themen führen: Philosophie, Kunst, Politik und natürlich über Mathematik. Dabei wurde deutlich, dass Reinhard eine „kunstaffine" Herangehensweise an Mathematik hatte: Ihr ästhetischer Wert und die Vermittlung der Schönheit der Mathematik war ihm stets ein Anliegen. Aus solchen Gesprächen mit Reinhard ist die nachfolgende Arbeit entstanden: eine kleine Note über zahlentheoretische Simulationsverfahren, die in schöner Weise seine beiden großen Interessen verbindet: Mathematik und Musik.

ISSN 0020-7926

(Vorgelegt in der Sitzung der math.-nat. Klasse am 20. Juni 1991 durch das w.M. PETER GRUBER)

Herrn Prof. Dr. E. Hlawka zum 75. Geburtstag gewidmet

Eine klassische Anwendung von Zufallszahlen sind sogenannte Monte-Carlo-Methoden, etwa zur numerischen Integration. Dabei approximiert man zum Beispiel das Integral einer auf dem s-dimensionalen Einheitswürfel $U_s = [O,1)^s$ definierten Funktion f durch das arithmetische Mittel der Funktionswerte $f(p_1),\dots,f(p_N)$, wobei die Punkte $p_1,\dots,p_N$ „zufällig“ $U_s = [0,1)^s$ entnommen werden. E. HLAWKA und I. KOROBOV (vgl. [9], [10], [13] und [14]) haben unabhängig voneinander eine deterministische Simulation solcher Monte-Carlo-Methoden gefunden und zahlentheoretische Verfahren entwickelt, um solche Punktfolgen zu konstruieren. Der Approximationsfehler kann nach oben durch den Wert $V(f)D_N(p_n)$ abgeschätzt werden, wobei $V(f)$ die Totalvariation von f im Sinne von HARDY und KRAUSE und

$$D_N(p_n) = \sup_I \left| \frac{1}{N} |\{n \le N : p_n \in I\}| - \lambda(I) \right| \tag{1}$$

die Diskrepanz der Punktfolge bezeichnet; das Supremum läuft über alle Intervalle $I \subseteq U_s$ mit Lebesgueschem Inhalt $\lambda(I)$. Man benötigt also Folgen mit kleiner Diskrepanz, d. h. Folgen, die in U_s gut verteilt liegen. Dazu sind mehrere Konstruktionen bekannt:

1. Gute Gitterpunkte (HLAWKA-KOROBOV): Es wird ein Modul $m \ge 2$ und ein Gitterpunkt $g \in \mathbb{Z}^s$ betrachtet. Bei geeigneter Wahl von g hat die Folge der komponentenweise genommenen gebrochenen Anteile

$$p_n = \left\{ \frac{n}{m} g \right\} \text{ eine Diskrepanz } D_N(p_n) \le c_s \frac{(\log m)^s}{m}$$

mit einer nur von s abhängigen Konstanten c_s. Im Falle der Dimension $s = 2$ können solche guten Gitterpunkte leicht mittels Kettenbruchentwicklungen konstruiert werden, für höhere Dimensionen gibt es ausführliche Tabellen (vgl. [11]).

2. $n\alpha$-Folgen: Bekanntlich ist die Folge $(\{n\alpha\})$ genau dann gleichverteilt, wenn α irrational ist. Sind die Teilnenner in der Kettenbruchentwicklung von α beschränkt, so gilt

$$D_N(\{n\alpha\}) \le C \frac{\log N}{N}$$

mit einer von α abhängigen Konstanten C. Tatsächlich kann C für die Zahl des goldenen Schnitts

$$\alpha = \frac{1+\sqrt{5}}{2}$$

minimal gehalten werden. Im Mehrdimensionalen kann man ähnliche Ergebnisse erreichen, wenn man von über $\mathbb{Z}$ linear unabhängigen Irrationalzahlen $\alpha_1,\dots,\alpha_s$

ausgeht und die Folge $(\{n\alpha_1\},\ldots,\{n\alpha_s\})$ im s-dimensionalen Einheitswürfel untersucht.

3. Hammersley-Halton-Folgen: Der natürlichen Zahl $n=\sum_{j=0}^{L} a_j b^j$ (Entwicklung zur Basis b) wird die Zahl $g_b(n)=\sum_{j=0}^{L} a_j b^{-j-1}$ zugeordnet. Es entsteht eine Folge in $[0,1)$ mit Diskrepanz

$$\ll \frac{\log N}{N}$$

(Van-der-Corput-Folge zur Basis b). Nimmt man s paarweise relativ prime Basen $b_1,\ldots,b_s$, so erhält man eine Punktfolge $p_n=(g_{b_1}(n),\ldots,g_{b_s}(n))$ mit Diskrepanz

$$\ll \frac{(\log N)^s}{N}$$

(Hammersley-Folge, vgl. [8]). Die Folge

$$p_n=\left(g_{b_1}(n),\ldots,g_{b_{s-1}}(n),\frac{n-1}{N}\right)_{n=1}^{N}$$

hat sogar Diskrepanz $\ll \frac{(\log N)^{s-1}}{N}$ (Halton-Folge, vgl. [7]).

4. Netz-Folgen (SOBOL, FAURE, NIEDERREITER): Die in $\ll$ auftretenden Konstanten hängen superexponentiell von der Dimension s ab. Die obigen Konstruktionen können so verfeinert werden, dass die Konstanten absolut beschränkt sind (vgl. [3], [17]).

5. Rekursive Folgen: Der wichtigste Fall sind hier linear rekursive Folgen

$$y_{n+s}=a_1 y_{n+s-1}+\ldots+a_s y_n$$

mit konstanten Koeffizienten $a_j\in\mathbb{Z}$ und ganzzahligen Startwerten. Bei Vorgabe einer natürlichen Zahl $m\geq 2$ und geeigneter Wahl der Koeffizienten a_j bildet man die modulo m reduzierte Folge $z_n=y_n \mod m$. Die Punktfolge

$$p_n=\left(\frac{1}{m}z_n,\ldots,\frac{1}{m}z_{n+s-1}\right)_{n=0}^{m-1}$$

hat dann Diskrepanz $\ll \frac{(\log m)^s}{m}$ (vgl. [16]).

Neuerdings spielen auch nichtlineare Rekursionen eine größere Rolle (vgl. [18]). Diese zeigen in gewissem Sinne eine viel größere Irregularität als die linearen. Es kann auch ein wesentlich anderes Verteilungsverhalten als das der Gleichverteilung auftreten. Im Folgenden betrachten wir das Beispiel

$$x_n=\left\{\frac{u_{n+1}}{u_n}\right\},$$

wobei die Glieder u_n einer Rekursion der Gestalt

$$u_{n+2} - 2u_{n+1} + (1 - c_n)u_n = 0 \tag{2}$$

genügen und

$$c_n = -d + O\left(\frac{1}{n^\lambda}\right) \tag{3}$$

sowie

$$\sum_{m=n}^{\infty} m|c_{m+1} - c_m| = O\left(\frac{1}{n^\lambda}\right) \tag{4}$$

mit $\lambda > 0$ vorausgesetzt sei. Unser Ziel ist es, die Verteilungsfunktion F der Folge $(\{x_n\})$ zu bestimmen. Im Falle konstanter Koeffizienten $c_n = -d$ liegt die zu (2) gehörige lineare Rekursion

$$u'_{n+2} - 2u'_{n+1} + (1 + d)u'_n = 0$$

vor. Nach [12] besitzt $x'_n = \left\{\frac{u'_{n+1}}{u'_n}\right\}$ die Verteilungsfunktion

$$F_1(x) = x + \frac{1}{\pi}\arctan\left(\frac{\sin 2\pi x}{\exp(\pi\sqrt{-D}) - \cos 2\pi x}\right), \tag{5}$$

wobei $D = -4d < 0$ die Diskriminante von (4) ist und das Argument ω' der charakteristischen Wurzeln von (4) als irrationales Vielfaches von π vorausgesetzt werden muss („non-degenerate case“, d. h. es handelt sich um keine reellen Vielfachen von Einheitswurzeln). Damit ist auch garantiert, dass $u'_n \neq 0$ für $n \geq n_0$ (vgl. [12]). In [19] wird das folgende Resultat bewiesen:

Satz 1. *Erfülle die Rekursion* (2) *mit reellen Startwerten und reellen c_n die Bedingungen* (3) *und* (4) *mit $d > 0$. Weiters erfülle*

$$\theta = \frac{1}{\pi}\arctan\sqrt{d}$$

die Approximationsbedingung

$$|n\theta - k| \geq \frac{C}{n^\tau}$$

für alle $n \geq 0$, $k \in \mathbb{Z}$ und einem geeigneten

$$\tau < \frac{\lambda - 1}{2},$$

wobei die positive Konstante C nur von τ abhängt. Dann besitzen die Quotienten

$$x_n = \frac{u_{n+1}}{u_n} \text{ modulo 1}$$

die Verteilungsfunktion $F = F_1$ von (5).

Bemerkung: Die im Satz an die Folge (c_n) gestellten Voraussetzungen sind zum Beispiel bei

$$c_n = -d + \frac{1}{n^{4+\alpha}}$$

mit einem $\alpha > 0$ und algebraischem, irrationalem θ erfüllt.

Es ist klar, dass man durch geeignete Transformationen aus gleichverteilten Folgen solche mit anderen Verteilungen erzeugen kann. Eingehende Untersuchungen zu diesem Themenkreis findet man in [2]. Wir werden beispielsweise noch mit der Verteilung f von $(z_n) = (x_n + y_n)$ in $[0,2)$ zu tun haben, wobei (x_n) und (y_n) voneinander unabhängig gleichverteilt sind. Durch Faltung erhält man

$$f(z) = \begin{cases} \frac{z^2}{2} & \text{für } 0 \le z \le 1 \\ -\frac{z^2}{2} + 2z - 1 & \text{für } 1 \le z \le 2. \end{cases}$$

Oft ist man an Zufallsfolgen (x_n) auf einer endlichen Menge

$$M = \{a_1, \ldots, a_m\}$$

interessiert. Gibt man jedem $a_i \in M$ die gleiche Wahrscheinlichkeit

$$P(a_i) = \frac{1}{m},$$

so ist der natürliche Gleichverteilungsbegriff gekennzeichnet durch die Forderung

$$\lim_{N\to\infty} \frac{1}{N} |\{n \le N | x_n = a_i\}| = \frac{1}{m}$$

für alle $a_i \in M$. Klarerweise induziert jede im Einheitsintervall im klassischen Sinne gleichverteilte Folge (x_n) eine auf M gleichverteilte Folge (x'_n), wenn man $x'_n = a_i$ setzt, falls

$$\frac{i-1}{m} \le x_n < \frac{i}{m}.$$

Sucht man nach dem diskreten Analogon zur weiter oben betrachteten Summe $z_n = x_n + y_n$ zweier unabhängiger Folgen (wo $((x_n, y_n))$ im Einheitsquadrat gleichverteilt war), so liegt es nahe, $a_i = i$ zu wählen, (x_n), (y_n) als auf M gleichverteilt vorauszusetzen und die durch die diskrete Verteilung von

$$\frac{z_n}{m} = \frac{x_n + y_n}{m}$$

gegebene Vorteilungsfunktion $f^{(m)}$ mit der oben ermittelten Verteilungsfunktion f zu vergleichen. Zu diesem Zwecke wird man zu einer Folge (z''_n) mit Verteilungsfunktion f die induzierte Folge (z'_n) mit $z'_n = i$ für

$$\frac{i-1}{m} < z'_n \le \frac{i}{m},\ i = 1, \ldots, 2m$$

betrachten. Allerdings fällt sofort auf, dass zum Beispiel der Wert 1 unter den z'_n mit relativer Häufigkeit

$$f\left(\frac{1}{m}\right) = \frac{1}{2m^2} > 0$$

auftritt, in der Folge z_n hingegen gar nicht. Also besitzen die beiden Folgen nicht die gleiche Verteilung. Jedoch liegt für $m \to \infty$ in beiden Fällen schwache Konvergenz der induzierten Maße gegen df vor. Für die Folge (z'_n) ist das vollkommen klar. Aber auch für die Verteilungsfunktion $f^{(m)}$ der Folge (z_n) lässt sich durch elementare Rechnungen

$$\sup_{0\le x\le 2} |f(x) - f^{(m)}(x)| = \frac{3}{2m} - \frac{1}{m^2}$$

verifizieren. Klarerweise folgt hieraus die Konvergenzaussage für $m \to \infty$.

Will man sich nicht damit zufriedengeben, dass jedes Intervall mit der richtigen Häufigkeit getroffen wird, und will man auch die Unabhängigkeit aufeinanderfolgender Glieder einer Zufallsfolge simulieren, so führt man für den Fall einer Folge auf der m-elementigen Menge $M = \{a_1, \ldots, a_m\}$ die s-Diskrepanz $D_N^{(s)}(x_n)$ durch

$$D_N^{(s)}(x_n) = \max_{a\in M^s} \left| \frac{m^s}{N} |\{n \le N | (x_n, \ldots, x_{n+s-1}) = a\}| - 1 \right|$$

ein und verlangt $\lim_{N\to\infty} D_n^{(s)}(x_n) = 0$ (s-Block-Gleichverteilung). Gilt dies für alle Blocklängen s, so heißt (x_n) vollständig gleichverteilt. Es ist sogar sinnvoll, die Blocklänge s in Abhängigkeit von N wachsen zu lassen, da (wie man leicht sieht) stets $D_N^{(s)} \le D_N^{(s+1)}$ gilt. Im Falle $\lim_{N\to\infty} D_N^{(s(N))}(x_n) = 0$ spricht man von $s(N)$-G1eichverteilung der Folge (x_n). Eine realistische Größenordnung für das Wachstum von $s(N)$ wird durch folgendes $0-1$–Gesetz ausgesprochen:

Satz 2. *Sei $(s(N))$ eine Folge natürlicher Zahlen, die der Wachstumsbeschränkung*

$$\mathrm{lm} N - \mathrm{lm}\,\mathrm{lm} N - s(N) \to \infty$$

genügt (hier steht lm *für den Logarithmus zur Basis m, $m \ge 2$), so hat die Menge aller auf der m-elementigen Menge M $s(N)$-gleichverteilten Folgen das Maß 1. Gilt jedoch die Beschränktheit von* $\mathrm{lm} N - \mathrm{lm}\,\mathrm{lm} N - s(N)$*, so hat sie das Maß 0.*

Der Beweis wurde in [4] bzw. [6] für $m = 2$ geführt, kann aber für beliebiges $m \ge 2$ übertragen werden. Eine explizite Konstruktion $s(N)$-g1eichverteilter Folgen ist in [5] und [20] beschrieben. Ein einfaches Beispiel einer vollständig gleichverteilten Folge (auf der Ziffernmenge $M = \{0, \ldots, 9\}$) stammt von D. G. CHAMPERNOWNE ([1]):

$$(x_n) = (0123456789101112131415161718192021222324252627282 9\ldots).$$

Anwendung von Pseudozufallszahlen zur Komposition von Mozartschen Walzern

Anlässlich seines zweihundertsten Todesjahres greifen wir eine Idee von Wolfgang Amadeus Mozart auf. Und zwar verfasste der Meister eine sogenannte „Anleitung zum Componiren von Walzern so viele man will vermittelst zweier Würfel ohne etwas von der Musik oder Komposition zu verstehen“, welche im Verlag N. Simrock, Berlin, publiziert wurde. Ein Exemplar dieser Schrift liegt auch bei der Gesellschaft der Musikfreunde im Wiener Musikverein auf. Darin sind Takte enthalten sowie eine Anleitung, wie man sie mittels zweier Würfel zu 16-taktigen Walzern zusammenfügen kann. (Offensichtlich wären a priori 11^{16} verschiedene Walzer möglich. Tatsächlich sind es wegen einiger Wiederholungen etwas weniger, in jedem Fall jedoch eine astronomische Anzahl.)

Diesen Vorgang kann man natürlich mittels Pseudozufallszahlen simulieren. Das soll nun anhand einiger Beispiele, den bisherigen Ausführungen folgend, geschehen. Wir werden uns von jedem Beispiel drei aufeinanderfolgende Walzer komponieren lassen, d. h. wir benötigen jeweils die ersten $3 \times 16 = 48$ Glieder der Würfelfolge. Die gemäß [15] aus den sechs nun folgenden Beispielen resultierenden Walzer sind sowohl in Notenform als auch auf Tonträger beim zweitgenannten Autor zugänglich.

1.) Nach VAN DER CORPUT: Wir wählen als einfachste Basis $b = 2$ und erhalten in Binärdarstellung die Folge

$$(x_n) = (0{,}1;\ 0{,}01;\ 0{,}11;\ 0{,}001;\ 0{,}101;\ 0{,}011;\ 0{,}111;\ \ldots 0{,}111101;\ 0{,}000011).$$

Um daraus auf natürliche Art eine Folge von Augensummen zweier Würfel zu erhalten, setzen wir zunächst naiv $z_n = i + 1$ für

$$x_n \in \left[\frac{i-1}{11}, \frac{i}{11}\right).$$

Das liefert die Folge

$$\begin{aligned}(z_n) = (&7,\ 5,\ 10,\ 3,\ 8,\ 6,\ 11,\ 2,\ 8,\ 5,\ 10,\ 4,\ 9,\ 6,\ 12,\ 2,\\ &7,\ 5,\ 10,\ 3,\ 9,\ 6,\ 11,\ 3,\ 8,\ 5,\ 11,\ 4,\ 9,\ 7,\ 12,\ 2,\\ &7,\ 4,\ 10,\ 3,\ 9,\ 6,\ 11,\ 2,\ 8,\ 5,\ 11,\ 4,\ 9,\ 6,\ 12,\ 2).\end{aligned}$$

Hier wird eine Schwäche mancher gleichverteilter Folgen in Hinblick auf „Zufälligkeit“ offenkundig. Zwar ist (x_n) gleichverteilt, jedoch mit einer Art Periodizität, welche in unserer Anwendung nach sich zieht, dass bei weiterer Fortsetzung nur einige ganz wenige der fast 11^{16} möglichen Walzer überhaupt auftreten, und selbst diese untereinander große Übereinstimmungen aufweisen.

2.) Nach HAMMERSLEY: Wie wir bereits wissen, entspricht die Gleichverteilung nicht der Verteilung der Augensummen von zwei Würfeln, wo ja bekanntlich 7 am

häufigsten auftritt, 2 und 12 am seltensten. Darauf gehen wir nun ein, indem wir die zu den Basen $b = 2$ und $b = 3$ gehörigen Hammersley-Folgen betrachten. Zur Basis 2 können wir die Folge (x_n) von 1.) weiterverwenden, zur Basis 3 erhalten wir in ternärer Darstellung die Folge

$$(y_n) = (0{,}1;\ 0{,}2;\ 0{,}01;\ 0{,}11;\ 0{,}21;\ 0{,}02;\ 0{,}12;\ 0{,}22;\ 0{,}001;\ \ldots 0{,}2021;\ 0{,}0121).$$

z_n ergibt sich durch $z_n = i + j$ für $x_n \in \left[\frac{i-1}{6}, \frac{i}{6}\right), y_n \in \left[\frac{j-1}{6}, \frac{j}{6}\right)$, also

$$\begin{aligned}(z_n) = (&5,\ 6,\ 6,\ 4,\ 9,\ 5,\ 10,\ 7,\ 5,\ 5,\ 10,\ 3,\ 8,\ 8,\ 8,\ 5,\\ &10,\ 3,\ 8,\ 6,\ 6,\ 7,\ 12,\ 3,\ 8,\ 9,\ 7,\ 5,\ 10,\ 4,\ 9,\ 6,\\ &6,\ 6,\ 11,\ 2,\ 7,\ 8,\ 7,\ 4,\ 9,\ 4,\ 9,\ 8,\ 6,\ 6,\ 11,\ 3).\end{aligned}$$

Da in der Summe $z_n = i + j$ die Folge (x_n) aus 1.) wesentlich beteiligt ist, sind jedoch die dort ausgesprochenen Einwände noch nicht vollständig entkräftet.

3.) Nach WEYL: Wir gehen von den auf $[0,1)$ bzw. $[0,1)^2$ gleichverteilten Folgen $(x_n) = (\{n\alpha\})$ und $(y_n) = (y_n^{(1)}, y_n^{(2)})$ mit $y_n^{(1)} = \{n\beta\}$, $y_n^{(2)} = \{n\gamma\}$ aus, wobei wir zum Beispiel

$$\alpha = \frac{\sqrt{5}+1}{2}, \quad \beta = \sqrt{2}, \quad \gamma = \sqrt{3}$$

wählen können. Begnügen wir uns wie in 1.) damit, dass jede mögliche Würfelaugensumme asymptotisch gleich oft auftritt, liegt wieder die Festsetzung $z_n = i + 1$ für

$$x_n \in \left[\frac{i-1}{11}, \frac{i}{11}\right)$$

am nächsten, womit wir zur Folge

$$\begin{aligned}(z_n) = (&8,\ 4,\ 11,\ 7,\ 2,\ 9,\ 5,\ 12,\ 8,\ 3,\ 10,\ 6,\ 2,\ 9,\ 4,\ 11,\\ &7,\ 3,\ 10,\ 5,\ 12,\ 8,\ 4,\ 11,\ 6,\ 2,\ 9,\ 5,\ 12,\ 7,\ 3,\ 10,\\ &6,\ 2,\ 8,\ 4,\ 11,\ 7,\ 3,\ 9,\ 5,\ 12,\ 8,\ 4,\ 10,\ 6,\ 2,\ 9)\end{aligned}$$

gelangen. Legen wir auf eine asymptotisch annähernd richtige Häufigkeit Wert, so können wir uns zunutze machen, dass $(y_n) = (y_n^{(1)} + y_n^{(2)})$ die Verteilungsfunktion f von früher besitzt, sodass die Festsetzung $z_n = i + 1$ für

$$y_n \in \left[2\frac{i-1}{11},\ 2\frac{i}{11}\right), \quad i \in \{2, \ldots, 11\}$$

die Verteilung beim Würfeln mehr oder weniger gut approximiert. Die Folge lautet dann

$$\begin{aligned}(z_n) = (&8,\ 9,\ 4,\ 10,\ 6,\ 6,\ 7,\ 8,\ 9,\ 4,\ 5,\ 11,\ 6,\ 7,\ 8,\ 9,\\ &4,\ 5,\ 11,\ 7,\ 7,\ 3,\ 9,\ 10,\ 5,\ 6,\ 7,\ 8,\ 3,\ 9,\ 10,\ 5,\\ &6,\ 7,\ 8,\ 8,\ 4,\ 10,\ 5,\ 6,\ 7,\ 8,\ 9,\ 4,\ 10,\ 6,\ 6,\ 7).\end{aligned}$$

Hier fällt auf, dass die Werte 2 und 12 unter diesen 48 Gliedern gar nicht auftreten, was durchaus mit der noch geringen Approximationsgüte erklärt werden kann. Die asymptotisch exakte Verteilung erhalten wir natürlich durch die Definition $z_n = z_n^{(1)} + z_n^{(2)}$ mit $z_n^{(j)} = i$ für

$$y_n^{(j)} \in \left[\frac{i-1}{6}, \frac{i}{6}\right), \quad j = 1,2.$$

$$\begin{aligned}(z_n) = (&8,\ 8,\ 4,\ 10,\ 5,\ 6,\ 7,\ 8,\ 9,\ 3,\ 5,\ 11,\ 7,\ 7,\ 8,\ 9,\\ &4,\ 5,\ 12,\ 6,\ 8,\ 2,\ 10,\ 10,\ 5,\ 6,\ 7,\ 7,\ 3,\ 9,\ 11,\ 5,\\ &6,\ 7,\ 7,\ 9,\ 3,\ 10,\ 5,\ 6,\ 7,\ 8,\ 8,\ 4,\ 10,\ 6,\ 6,\ 7).\end{aligned}$$

Es verbleibt aber dennoch ein fast deterministischer Zusammenhang zwischen $z_n^{(j)}$ und $z_{n+1}^{(j)}$, $(j = 1,2)$, was Abhängigkeiten zwischen z_n und z_{n+1} bewirkt. Als Ergebnis erhält man bei weiterer Fortsetzung des Verfahrens daher wieder gewisse Walzer überproportional häufig, eine Unzahl anderer hingegen besitzt überhaupt keine Chance auf ein Erklingen.

4.) Nach CHAMPERNOWNE: Abschließend soll noch ein Beispiel gegeben werden, welches sowohl die exakte Verteilung liefert als auch asymptotisch (natürlich kommt im Falle von 48 Takten diese Asymptotik noch nicht sehr deutlich zum Tragen) die Unabhängigkeit aufeinanderfolgender Würfe simuliert. In unserem Beispiel verwenden wir die vollständig gleichverteilte Champernowne-Folge auf der 36-elementigen Menge $M = \{1,2,3,4,5,6\}^2$, welche wir uns lexikographisch geordnet denken, also

$$\begin{aligned}(x_n) = (&(1,1),\ (1,2),\ (1,3),\ (1,4),\ (1,5),\ (1,6),\ \ldots,\ (6,6),\ (1,2),\ (1,1),\\ &(1,2),\ (1,2),\ (1,2),\ (1,3),\ (1,2),\ (1,4),\ (1,2),\ (1,5),\ (1,2),\ (1,6)).\end{aligned}$$

Die zugehörige Würfelfolge (z_n) lautet demnach

$$\begin{aligned}(z_n) = (&2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 4,\ 5,\ 6,\ 7,\\ &8,\ 9,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11,\ 7,\ 8,\\ &9,\ 10,\ 11,\ 12,\ 3,\ 2,\ 3,\ 3,\ 3,\ 4,\ 3,\ 5,\ 3,\ 6,\ 3,\ 7).\end{aligned}$$

Wir wollen uns hier mit den vorliegenden Beispielen und Bemerkungen zufriedengeben. Es darf sicherlich angenommen werden, dass sich Mozart sehr wohl der wesentlichen Eigenschaften des Glücksspiels und des Zufalls, für welche die moderne Mathematik u. a. die hier erörterten Begriffe geschaffen hat, bewusst war. Ob er sich jedoch bei seiner „Anleitung zum Componiren von Walzern so viele man will vermittelst zweier Würfel ohne etwas von der Musik oder Komposition zu verstehen“ effektiv von diesem Wissen leiten ließ, ja ob Gedanken darüber überhaupt dem Wesen der Musik angemessen seien, vermag selbst nach Vergleich

der oben angeführten Beispiele bestenfalls vielleicht der Musiktheoretiker oder -historiker, sicher jedoch nicht der Mathematiker zu beurteilen.

Schlussbemerkung: Anlässlich des heurigen Mozartjahres ist im Wiener Technischen Museum ein computer-implementierter Zufallsgenerator in Betrieb, mit dem im Mozartschen Sinne komponiert wird. Üblicherweise verwenden solche Generatoren lineare Rekursionen.

Literatur

[1] CHAMPERNOWNE, D. G. The Construction of Decimals Normal in the Scale of Ten. *J. London Math. Soc. 8*, 4 (1933), 254–260.

[2] DEVROY, L. *Non Uniform Random Variate Generation*. Springer, 1986.

[3] FAURE, H. Discrépance de suites associées à un système de numération (en dimension *s*). *Acta Arith. 41*, 4 (1982), 337–351.

[4] FLAJOLET, P., KIRSCHENHOFER, P., UND TICHY, R. F. Deviations from uniformity in random strings. *Probab. Theory Related Fields 80*, 1 (1988), 139–150.

[5] GOLDSTERN, M. Vollständige Gleichverteilung in diskreten Räumen. In *Zahlentheoretische Analysis, II*, vol. 1262 of *Lecture Notes in Math.* Springer, Berlin, 1987, pp. 46–49.

[6] GRILL, K. A note on randomness. *Statist. Probab. Lett. 14*, 3 (1992), 229–233.

[7] HALTON, J. H. On the efficiency of certain quasi-random sequences of points in evaluating multi-dimensional integrals. *Numer. Math. 2* (1960), 84–90.

[8] HAMMERSLEY, J. M. Monte Carlo methods for solving multivariable problems. *Ann. New York Acad. Sci. 86* (1960), 844–874.

[9] HLAWKA, E. Zur angenäherten Berechnung mehrfacher Integrale. *Monatsh. Math. 66* (1962), 140–151.

[10] HLAWKA, E. Uniform distribution modulo 1 and numerical analysis. *Compositio Math. 16* (1964), 92–105.

[11] HUA, L. K., UND WANG, Y. *Number-theoretic methods in Numerical Analysis*. Springer, 1981.

[12] KISS, P., UND TICHY, R. F. Distribution of the ratios of the terms of a second order linear recurrence. *Indag. Math. 48*, 1 (1986), 79–86.

[13] KOROBOV, N. M. Approximate calculation of multiple integrals with the aid of methods in the theory of numbers (Russian). *Dokl. Akad. Nauk SSSR 115* (1957), 1062–1065.

[14] KOROBOV, N. M. The approximate computation of multiple integrals (Russian). *Dokl. Akad. Nauk SSSR 124* (1959), 1207–1210.

[15] MOZART, W. A. *Anleitung zum Componiren von Walzern so viele man will vermittelst zweier Würfel ohne etwas von der Musik oder Komposition zu verstehen*. N. Simrock, Berlin.

[16] NIEDERREITER, H. The performance of *k*-step pseudorandom number generators under the uniformity test. *SIAM J. Sci. Statist. Comput. 5*, 4 (1984), 798–810.

[17] NIEDERREITER, H. Point sets and sequences with small discrepancy. *Monatsh. Math. 104*, 4 (1987), 273–337.

[18] NIEDERREITER, H. *Random number generation and quasi-Monte Carlo methods*, vol. 63 of *CBMS-NSF Regional Conference Series in Applied Mathematics*. Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 1992.

[19] TICHY, R. F. Stability of a class of nonuniform random number generators. *J. Math. Anal. Appl. 181*, 2 (1994), 546–561.

[20] WINKLER, R. Some constructive examples in uniform distribution on finite sets and normal numbers. *Anz. Österreich. Akad. Wiss. Math.-Natur. Kl. 126* (1989), 1–8.

Adresse des Autors:
Institut für Analysis und Zahlentheorie, TU Graz, Steyrergasse 30, 8010 Graz, Österreich
email tichy@tugraz.at

Internat. Math. Nachrichten
Nr. 248 (2021), 41–50

Virtuelle Vernetzung um die ganze Welt: Die gemeinsame Jahrestagung der Deutschen Mathematiker Vereinigung und der Österreichischen Mathematischen Gesellschaft 2021 in Passau

Brigitte Forster-Heinlein

Universität Passau

Vom 27. September bis zum 1. Oktober 2021 fand die Gemeinsame Jahrestagung der Deutschen Mathematiker Vereinigung DMV und der Österreichischen Mathematischen Gesellschaft ÖMG 2021 statt. Gastgeber war die Universität Passau; aufgrund der Pandemie fand die Tagung virtuell statt. Über 700 Wissenschaftlerinnen und Wissenschaftler aus 36 Ländern der Erde fanden sich zusammen. Insgesamt wurden über 420 Vorträge präsentiert.

Für das wissenschaftliche Programm waren elf Kolleginnen und Kollegen aus Österreich und Deutschland gemeinsam verantwortlich: Brigitte Forster-Heinlein (Passau, Hauptorganisatorin der Tagung), Ilka Agricola (Marburg, Präsidentin der DMV), Barbara Kaltenbacher (Klagenfurt, Präsidentin der ÖMG), Tobias Kaiser (Passau, Dekan der gastgebenden Fakultät für Informatik und Mathematik), Friedrich Pillichshammer (Linz), Guido Schneider (Stuttgart), Andreas Schröder (Salzburg), Matthias Brandl, Martin Kreuzer, Ignaz Rutter, Tomas Sauer, Fabian Wirth, and Jens Zumbrägel (alle Passau).

Nach einer musikalischen Eröffnung durch die Passauer Band “Stormy Hill Hot Three” hießen Brigitte Forster und Tobias Kaiser alle Teilnehmerinnen und Teil-

ISSN 0020-7926

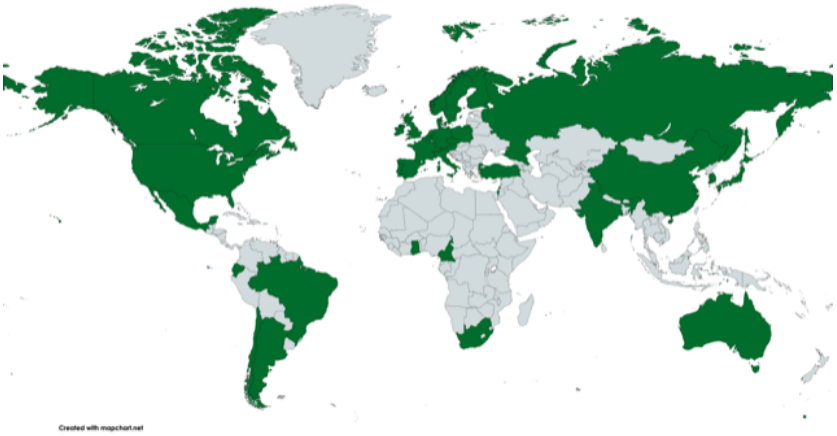

Abbildung 1: Karte aller Nationen, aus welchen Wissenschaftlerinnen oder Wissenschaftler an der Gemeinsamen Jahrestagung teilnahmen.

nehmer herzlich willkommen. Der Präsident der Universität Passau, Ulrich Bartosch, empfing die Gäste mit einem Grußwort, ebenso wie die Präsidentinnen der ÖMG und der DMV, Barbara Kaltenbacher und Ilka Agricola. Anschließend nahm der Archivar der Universität Passau, Mario Puhane, die Gäste mit auf eine virtuelle Tour über den Campus, garniert mit historischen Geschichten zum Schmunzeln.

Highlights des wissenschaftlichen Programms waren die elf Hauptvorträge.

Christian Hesse (Universität Stuttgart) hielt am Dienstagabend den öffentlichen Vortrag über „**Mathematik und Schach**“.

Abstract: *Die Königin der Wissenschaften und das Königliche Spiel: Sie sind Jahrtausende alt und haben weltumspannenden Einzug in alle Kulturen gehalten. Der Vortrag befasst sich mit den Ähnlichkeiten und wechselseitigen Beziehungen zwischen diesen beiden Kulturgütern. Viele Mathematiker:innen haben sich durch das Schachspiel zu tiefen Problemen inspirieren lassen. Und nicht wenige Schachspieler:innen begeistern sich auch für mathematische Probleme. Es gibt schachbezogene Fragestellungen, die mithilfe mathematischer Methoden lösbar sind. Umgekehrt gibt es auch mathematische Fragestellungen, die mit schachlichen Accessoires – also mit Schachbrett und Figuren – gelöst werden können. Besonders das Letztere scheint überraschend. Elegante Beispiele für beide Arten von Problemen sollen besprochen werden. Allgemeinverständlichkeit wird angestrebt.*

Die musikalische Umrahmung für den öffentlichen Vortrag gestaltete die Passauer Band “At the Diners”. Die Veranstaltung war mit über 150 Zuhörerinnen und Zuhörern sehr gut besucht.

Martin Grötschel (Technische Universität Berlin) hielt am Freitag einen öffentlichen Festvortrag mit dem Titel „**Moderne Mathematik**“ anlässlich der Verlei-

hung der Cantor-Medaille, die ihm eine Woche zuvor bei einer Feierstunde in Berlin von Frau Agricola herzlich überreicht worden war.

Abstract: *Der Vortragstitel erscheint ein wenig provokativ. Eine allgemein akzeptierte Definition von Mathematik gibt es nicht. Was soll dann moderne Mathematik sein?*

Das Ziel des Vortrags ist eine Beschreibung von Entwicklungen in der Mathematik. Der Vortrag richtet seinen Fokus auf die letzten fünfzig Jahre und basiert auf Erfahrungen des Vortragenden als Forscher, Hochschullehrer und Wissenschaftsadministrator. Viele Beispiele dienen als Zeugnis signifikanter Veränderungen.

Die klassische Mathematik, die durch fachinterne Fragestellungen getrieben das eigene Strukturgebäude immer wieder erneuert und weiter ausbaut, ist höchst aktuell und sehr erfolgreich. Die Verfügbarkeit von leistungsfähigen Rechnern und vielfältige Einflüsse aus der Informatik haben traditionelle mathematische Fächer z. T. neu ausgerichtet. Die unsinnige Aufspaltung der Mathematik in reine und angewandte Fachgebiete ist im Verschwinden begriffen. Mathematisch relevante Fragestellungen aus Industrie, Gesellschaft und anderen Wissenschaftsdisziplinen haben neue mathematische Forschungsthemen generiert. Das vertrauensvolle Zusammenwirken der Mathematik mit anderen Fachdisziplinen hat sich für alle Seiten als äußerst fruchtbar erwiesen. Neue, von politischer Seite aufgelegte, hochdotierte Förderformate haben die interdisziplinäre Zusammenarbeit in den Mittelpunkt gestellt. Bei der Einwerbung derartiger Drittmittel war die Mathematik sehr erfolgreich.

Fazit: Die heutige Mathematik ist eine lebendige Wissenschaft, die ein unverzichtbarer und zentraler Knoten im Netz der Wissenschaften und vieler Anwendungsfelder ist. Sie ist in dem Sinne modern, dass sie ernsthaft und nachhaltig „vielfältige Herausforderungen der Welt“ aufnimmt, zu deren Verständnis durch mathematische Modellierung und konkrete Lösungsvorschläge beiträgt. Hinzu kommt, dass sich das öffentliche Bild der Mathematik – durch erfolgreiche Medienarbeit – sehr positiv gewandelt hat.

Über 200 Personen folgten dem Vortrag von Herrn Grötschel; inzwischen kann das Video dazu auf YouTube angesehen werden:

https://www.youtube.com/watch?v=8RQVmn8Iqjo

Die weiteren Hauptvorträge waren:

Nina Gantert (Technische Universität München): “**Exclusion processes: some new results and open questions**”.

Abstract: *Exclusion processes are interacting particle systems which generalize the basic model of simple random walk. They can model traffic flows or molecules in a low-density gas. Exclusion processes have been investigated intensively in analysis, statistical mechancis as well as in combinatorics. We first explain some*

of the classical questions about such processes: invariant measures, the speed of a tagged particle, the current and its fluctuations. We then turn to more recent results about the convergence of a finite system to its invariant distribution, introducing mixing times and the cutoff phenomenon. The question about cutoff is of independent interest and may be asked for many (sequences of) Markov chains. We present some recent results for a finite system with open boundaries. In the end, we mention open questions about the current and about second class particles. The talks is based on joint work(s) with Nicos Georgiou, Evita Nestoridi and Dominik Schmid.

Stefan Kebekus (Universität Freiburg i. Br.): „Minimale Modelle und die Klassifikation algebraischer Varietäten".

Abstract: *Die Theorie „minimaler Modelle"hat sich in den letzten Jahrzehnten zu einem Kernthema der algebraischen Geometrie entwickelt. Leider steht das Gebiet nicht ganz zu unrecht im Ruf, recht technisch zu sein und es dem Außenstehenden nicht leicht zu machen.*

Der Vortrag erläutert in nicht-technischer Weise die Ziele und die Entwicklung des Programms minimaler Modelle und gibt einen kleinen Einblick in aktuelle Ergebnisse und Forschungsprobleme.

Anke Pohl (Universität Bremen): "**Automorphic functions, transfer operators, and dynamics**".

Abstract: *The interplay of the geometric and the spectral properties of Riemannian manifolds is highly influencial in essentially all areas of mathematics, but far from being fully understood. Some of the recent advancements in understanding this relation could be achieved by means of transfer operators. I shall overview some recent developments in this area with a focus on hyperbolic surfaces, automorphic functions, resonances and the dynamics of the geodesic flow and with an emphasis on insights and heuristics.*

Anita Schöbel (Technische Universität Kaiserslautern): "**Robust optimization: Real-world applications imply a challenging topic**".

Abstract: *Practitioners are often reluctant applying mathematical results. Many reasons for this exist. One is that traditional methods are "stable" and practitioners know how to adapt them to changing requirements. And they are right: Most real-world problems contain parameters which are not known at the time a decision is to be made. Data may not be measurable in the precision needed or may depend on future developments. An optimal solution which does not take such an uncertainty into account often becomes bad or even infeasible for the scenario which is finally realized.*

In robust optimization one specifies the uncertainty as a scenario set and tries to find a solution which is good enough, no matter which scenario occurs. Classical robust optimization aims at finding a solution which minimizes the costs in the

worst case. It is a well-studied concept, but it is known to be very conservative: A robust solution comes with a high price in its nominal objective function value.

This motivated researchers to introduce less conservative robustness concepts. In the first part of this talk, several definitions of robustness will be shown. Two of the less conservative robustness approaches will be discussed in more detail: Light robustness and a scenario-based approach to recovery robustness.

The second part of the talk goes one step further: How to handle uncertain optimization problems in which more than one objective function is to be considered? This yields a robust multi-objective optimization problem, a class of problems only recently introduced. Concepts on how to define robust Pareto solutions will be developed. Mathematical properties will be derived as well as first approaches on how to compute robust efficient solutions.

All concepts will be illustrated on real-world problems which are currently tackled at Fraunhofer ITWM.

Angela Stevens (Universität Münster): "**Mathematics in Epidemiology**".

Abstract: *New infectious diseases emerge regularly, parasites mutate, and often become infectious again for the previously immunized host population. History provides many unfortunate examples. Abel and Riemann died from tuberculosis, C.G.J. Jacobi from smallpox, Kowalewskaja, Kummer and Weierstrass from influenza, and Boole and Descartes died from pneumonia. Fermat fortunately survived the last great outbreak of plague in Toulouse.*

Mathematics itself has successfully played a longstanding and important role in understanding the dynamics of epidemics. Due to the structural similarities of infection processes an abstract approach is natural. This has been realized and exploited a long time ago.

In this talk some of the mathematical tools available for epidemiology are summarized and phenomena like epidemic waves and inter-epidemic periods, heterogeneous populations with variable infectivity, as well as vaccination schemes with subcritical bifurcations are discussed.

Finally we have a look at some actual data.

Gabriele Steidl (Technische Universität Berlin) hielt die diesjährige Emmy-Noether Lecture. Sie sprach zum Thema "**Motion and Deformation in Images**".

Abstract: *Dynamical imaging–the treatment of videos and multimodal images–leads to mathematical modeling by*

- *optical flow,*
- *image metamorphosis, and*
- *optimal transport.*

We present recent adaptations of the three concepts for manifold-valued image

processing. The optimal flow approach is driven by applications in material sciences, in particular electron backscatter diffraction. While metamorphosis can be seen from an optimal control point of view, there is also a geometric concept which endows the space of images with a nonlinear Riemannian structure, which can be used for diffeomorphism estimation by minimizing the path energies of a corresponding geodesics. In optimal transport, we are interested in the multimarginal, unbalanced setting.

Drei der Hauptvorträge wurden von Förderungspreisträgern der ÖMG gehalten.

Julian Fischer (Institute of Science and Technology Austria): "**Interface evolution problems in fluid mechanics and geometry**".

Abstract: *In evolution equations for interfaces, topological changes and geometric singularities often occur naturally, basic examples being the pinch-off of liquid droplets or the shrinkage and disappearance of phases in mean curvature flow. As a consequence, classical solution concepts for such PDEs are naturally limited to short-time existence results or particular initial configurations like perturbations of a steady state. At the same time, the transition from strong to weak solution concepts for PDEs is prone to incurring unphysical non-uniqueness of solutions. In particular, for interface evolution equations not subject to a comparison principle - like multiphase mean curvature flow or fluid-fluid interface evolution problems -, the relation between weak and strong solutions has remained unclear.*

By introducing a novel concept of "gradient flow calibrations", we establish a weak-strong uniqueness principle for multiphase mean curvature flow: Weak (BV) solutions to multiphase mean curvature flow are unique as long as a classical solution exists. In particular, in planar multiphase mean curvature flow, weak (BV) solutions are unique prior to the first topological change. As basic counterexamples show, the uniqueness of evolutions may fail past certain topology changes, demonstrating the optimality of our result. We establish an analogous weak-strong uniqueness principle for the Navier-Stokes equation for two fluids separated by a sharp free interface.

In the last part of the talk, we discuss further applications of our new concept, including the quantitative convergence of diffuse-interface (Allen-Cahn) approximations for mean curvature flow.

Julian Fischer ist Förderungspreisträger der ÖMG des Jahres 2020, Karin Schnass und Joscha Prochno erhielten ihre Förderungspreise im Juli dieses Jahres.

Joscha Prochno (Universität Graz): "**The asymptotic structure of Schatten p-Classes**".

Abstract: *The Schatten p-classes are among the most fundamental operator ideals studied in functional analysis. These matrix spaces are non-commutative versions of classical ℓ_p sequence spaces with which they share several structural characteristics. However, while ℓ_p spaces are quite well understood from an analytic, geo-*

metric and probabilistic point of view, this often cannot be said about the Schatten p-classes. In this talk, we shall present and discuss some recent results concerning their asymptotic structure.

Karin Schnass (Universität Innsbruck): "**Conditioning of random submatrices**".

Abstract: *I will motivate why it is useful to look at random submatrices where each atom is not drawn with the same probability but some atoms are more likely. I will then provide conditions under which such submatrices are well-conditioned with high probability, sketch the proof and show the crux of the proof in more detail. Finally I will give an example application of the results and show how they can be used to decide what a good sensing matrix for compressed sensing is and how we can precondition an pre-determined one. Joint work with Simon Ruetz.*

Neben den gebotenen 14 Sektionen veranstalteten Mathematikerinnen und Mathematiker zusätzlich 28 Minisymposien zu besonderen mathematischen Themen.

Liste der Sektionen:

- **Algebra, Algebraic Geometry and Number Theory**. Clemens Fuchs, Salzburg, und Jörn Steuding, Würzburg
- **Calculus of Variations, Geometric Analysis**. Anna Dall'Acqua, Ulm, und Ulisse Stefanelli, Wien
- **Computer Algebra**. Manuel Kauers, Linz, und Martin Kreuzer, Passau
- **Differential Geometry**. Tomas Sauer, Passau, und Hannes Wallner, Graz
- **Discrete Mathematics**. Clemens Heuberger, Klagenfurt, und Stefan Weltge, München
- **Dynamical Systems**. Josef Hofbauer, Wien, und Timo Reis, Hamburg
- **Functional Analysis; Real, Complex Analysis**. Hartmut Führ, Aachen, und Bernhard Lamel, Wien
- **Geometry and Topology**. Monika Ludwig, Wien, und Thomas Schick, Göttingen
- **History and Didactics of Mathematics**. Gert Kadunz, Klagenfurt, und Ysette Weiss, Mainz
- **Logic**. Vera Fischer, Wien, und Tobias Kaiser, Passau
- **Numerics and Scientific Computing**. Armin Iske, Hamburg, und Dirk Praetorius, Wien
- **Partial Differential Equations**. Klemens Fellner, Graz, und Harald Garcke, Regensburg
- **Statistics**. Sylvia Frühwirth-Schnatter, Wien, und Gernot Müller, Augsburg

- **Stochastics and Financial Mathematics**. Martin Keller-Ressel, Dresden, und Michaela Szölgyenyi, Klagenfurt.

Liste der Minisymposien:

- **Clifford analysis and phase retrieval for image processing**. Swanhild Bernstein, Freiberg, und Bettina Heise, Linz
- **Dynamics, stability and control in infinite dimensions**. Jochen Glück und Andrii Mironchenko, Passau
- **Fractional calculus in cancer modelling**. Mabel Lizzy Rajendran und Christina Kuttler, München
- **Functional analytical approaches to dynamical systems**. Christian Pötzsche, Klagenfurt, und Nils Waterstraat, Halle
- **Large cardinals**. Philipp Lücke, Barcelona, und Sandra Müller, Wien
- **Loop spaces in geometry and topology**. Sebastian Boldt, Leipzig, und Batu Güneysu, Potsdam
- **Massively parallel methods in geometry and applications**. Janko Böhm, Kaiserslautern, und Anne Frühbis-Krüger, Oldenburg
- **Mathematik für die Bildverarbeitung**. Jürgen Frikel, Regensburg, Martin Storath, Schweinfurt, und Brigitte Forster, Passau
- **Mathematische Analyse komplexer Quantensysteme**. Heinz Siedentop, München, und Volker Bach, Braunschweig
- **Meta-learning for randomized optimization heuristics**. Carola Doerr and Martin Krejca, Paris, und Maximilan Moll, München
- **Model order reduction and approximation of coupled systems**. Björn Liljegren-Sailer, Trier, und Benjamin Unger, Stuttgart
- **New trends in algorithmic randomness and computable analysis**. Rupert Hölzl, München, und Christopher Porter, De Moines, USA
- **Nonlocal conservation laws**. Simone Göttlich und Jan Friedrich, Mannheim
- **Optimal transport revisited**. Jonas Hirsch und Tobias Ried, Leipzig
- **PDE models describing interfaces and complex structures**. Patrik Knopf, Regensburg, und Stefan Metzger, Erlangen
- **Recent developments in mathematical fluid dynamics**. Christian Zillinger und Xian Liao, Karlsruhe
- **Signal processing and feature extraction**. Thomas Fink und Florian Heinrich, Passau

- **Structure-preserving computational methods**. Ashish Bhatt, Dhanbad, Indien
- **AIMS-Germany minisymposium on applied mathematics**. Vladimir Shikhman, Alois Pichler, Chemnitz, und Mouhamed Moustapha Fall, Franck Kalala Mutombo, M'Bour, Sénégal
- **Connecting young researchers by networks**. Mechthild Thalhammer, Innsbruck, und Veronika Pillwein, Linz
- **Examining mathematics with electronic systems (E-Assessment)**. Helena Barbas und Julian Großmann, Hamburg
- **Get-together and career advice for young mathematicians**. Hana Dal Poz Kouřimská, Wien, und Teresa Heiss, Wien
- **Historische Aspekte numerischer Methoden in Theorie und Praxis**. Hans Fischer, Eichstätt, und Ysette Weiss, Mainz
- **Mathematical proof in an exam / Mathematischer Beweis in der Klausur**. Thomas Skill, Bochum, und Walther Paravicini, Tübingen
- **Mathematics and arts**. Milena Damrau, Bielefeld, und Martin Skrodzki, Delft
- **Mathematik in der Informatik**. Veronika Böhm, Marion Christl und Bejamin Huber, Passau
- **Ready for MaRDI, am I a digital mathematician?** Karsten Tabelow, Thomas Koprucki, Berlin, und Moritz Schubotz, Olaf Teschke, Karlsruhe
- **Thinking about proofs**. Deniz Sarikaya, Hamburg.

Weitere Informationen, z.B. Webseiten und Abstracts, können unter der folgenden URL nachgelesen werden:
https://www.uni-passau.de/en/dmv-oemg-jahrestagung-2021/

Das Organisationskomitee war sehr angetan von den vielen jungen Forscherinnen und Forschern, die das virtuelle Format der Tagung genutzt haben, um hochrangige internationale Wissenschaftlerinnen und Wissenschaftler in ihre Minisymposien einzuladen. Entsprechend munter waren die fachlichen Diskussionen auf dem Wonder.me-Kanal der Tagung – nicht nur zu den Kaffeepausen.

Das reichhaltige Programm der Jahrestagung umfasste weiter

- den **Lehrer-Mitmach-Tag Online Lehre und GeoGebra** am Dienstag (Martin Kreuzer, Matthias Brandl und Jens Zumbrägel, Passau),
- die **Studierendenkonferenz**, ebenso am Dienstag (Sven Gebauer, Matthias Hanl, Nikolas Kirschstein, Kassian Köck, Barbara Lutz, Maximilian Strohmeier, Passau), mit Vorträgen von Alumni aus der Industrie und von Studierenden über ihre Abschlussarbeiten sowie

- das **Mittagsseminar Mathematik in Industrie und Gesellschaft** (Tomas Sauer, Passau, und Anita Schöbel, Kaiserslautern) mit zwölf spannenden Kurzvorträgen aus der unternehmerischen Forschung zur Anwendung der Mathematik am Donnerstag.

Das Organisationskomitee bedankt sich herzlich bei allen Teilnehmerinnen und Teilnehmern für ihre spannenden Beiträge und ihre Arbeit in den Sektionen und Minisymposia. Besonderer Dank geht an die wissenschaftsunterstützenden Dienste der Universität Passau. Finanziell wurde die Tagung freundlich vom Verein der Freunde und Förderer der Universität Passau e.V. sowie von den Firmen MapleSoft und Springer Nature unterstützt.

Die kommende Jahrestagung der DMV 2022 wird in Berlin stattfinden. Gastgeber der nächsten Gemeinsamen Jahrestagung der DMV und der ÖMG im Jahr 2025 ist Linz.

Adresse der Autorin:
Universität Passau, Fakultät für Informatik und Mathematik, Innstr. 33, 94032 Passau, Deutschland
email brigitte.forster-heinlein@uni-passau.de

Buchbesprechungen

A. Borel, R. Godement, C. L. Siegel, A. Weil: Arithmetic Groups and Reduction Theory. Edited by L. Ji and translated by W. Globke, L. Ji, E. Leuzinger, and A. Weber. (Classical Topics in Mathematics, Vol. **10**.) A publication of Higher Education Press (Beijing), 2020, 138 S. ISBN 978-7-04-053375-0 H/b $ 59.

Arithmetic groups are generalisations, to the setting of algebraic groups defined over an algebraic number field k, of the subgroups of finite index in the general linear group with entries in the ring of integers of k. Investigations of number theoretical properties of quadratic forms are the historical source for the concept of an arithmetic group. As developed by Gauss, Hermite and Minkowski, among others, the study of reduction of such forms gave a powerful way to select, from the infinitely many forms which are integrally equivalent to a given form, one which is intrinsically characterised by suitable conditions on its entries. Minkowski's works and his geometric point of view influenced Siegel's studies of quadratic, symplectic or Hermitian forms, their associated discontinuous groups, and related reduction theory. Due to the rise of the general theory of linear algebraic groups over fields, nowadays arithmetic groups are viewed as a rich integral extension of this more classical area.

The book under review comprises translations (except in one case) to English of six papers which describe to a certain extent the state of the art at the beginning of the 1960s. Here are the original publications:

- C. L. Siegel, Zur Reduktionstheorie quadratischer Formen, Publ. Math. Soc. Japan, Vol. 5, The Mathematical Society of Japan, Tokyo, 1959
- A. Weil, Réduction des formes quadratiques, d'aprés Minkowski and Siegel, Séminaire Henri Cartan, t. 10, no. 1, exp. 1, 1957-58
- A. Weil, Groupes des formes quadratiques indéfinies et des formes bilinéaires altern'ees, Séminaire Henri Cartan, t. 10, no. 1, exp. 2, 1957-58
- A. Weil, Discontinuous subgroups of classical groups, Lect. Notes, Univ. Chicago, 1958

- A. Borel, Ensembles fondamentaux pour les groupes arithmétiques, Colloq. Théorie des Groupes Algébriques (Bruxelles, 1962), 23-40, Librairie Universitaire, Louvain; GauthierVillars, Paris, 1962

- R. Godement, Domaines fondamentaux des groupes arithmétiques, Séminaire Bourbaki, 1962/63. Fasc. 3, No. 257, 1964.

These historical sources give a reasonable account of certain aspects of reduction theory around 1960. Their publication in English is a valuable addition to the literature. However, a comprehensive critical appraisal of the development of reduction theory at that time and beyond is desirable. In particular, the effect of the papers by Siegel and Godement deserves special attention.

Joachim Schwermer (Wien)

Women in Mathematics

Interview with Monika Ludwig

Monika Ludwig got her PhD from the Technische Universität Wien in 1994. She worked as an Assistant Professor there until 1999 when she moved as an Erwin-Schrödinger Fellow first to University College London and a year later to New York Polytechnic University. She became an Associate Professor at TU Wien in 2001 and was a visiting Professor at the University of Bern for one semester in 2002. In 2007, she moved as full Professor to the Polytechnic Institute of NYU and returned to TU Wien in 2010 as full Professor. She was the first woman who received the Hlawka-Prize of the Austrian Academy of Sciences and the Förderungspreis of the Austrian Mathematical Society. She became a Corresponding Member of the Austrian Academy of Sciences in 2011, a Fellow of the American Mathematical Society in 2012, and a Full Member of the Austrian Academy of Sciences in 2013. She was a plenary speaker at the European Congress of Mathematics in 2021.

(c) Luiza Puiu

Could you tell us about your research in general? What about your current research topic?

I work on questions in geometry and analysis. Presently, I am working on a project that aims at extending geometric valuation theory, that has been very successful

within convex geometry, to function spaces including spaces of convex functions and Sobolev spaces. This can be seen as a part of the larger aim to geometrize analysis.

What are the results you are most proud of?

Let me mention two results, both within geometric valuation theory. About twenty years ago, I was able to give a simple characterization of, first, the classical notion of affine length and, a bit later together with Matthias Reitzner, of classical affine surface area in general dimensions. Much more recently, together with Andrea Colesanti and Fabian Mussnig, I established a version of the classical Hadwiger theorem for convex functions. This is part of an ongoing project.

You have worked at several universities abroad. Are there particular aspects that you liked at those universities and how important are such international experiences?

I enjoyed getting to know new things within mathematics and also in general. For me, it was very valuable to see that there are many different ways to do almost everything, including teaching and administration. It was also very inspiring to have colleagues and collaborators with very different backgrounds and ideas. More specifically, I liked the pragmatism at American universities and the commitment to excellence. I liked the egalitarian approach at Swiss universities and the fortitude and the wit of my British colleagues.

You have supervised quite a few PhD and MSc students. Did you experience any differences in working with female and male students?

There were many differences between my students but the different backgrounds had a much bigger impact than the difference between female and male students. I worked with male students from Austria and from the US and with female students from the US and China. I enjoyed to work with all of them, but, of course, it is easier to work with students who like mathematics a lot and want to make a significant contribution.

How important were mentors for you during your career?

Very important. I would recommend everyone to talk with their colleagues and professors about what it means to be a mathematician. This includes gossip about how other researchers were able to succeed and how they failed. In addition, it is important to get advice on how to do important things, in particular, how to find good research questions, how to establish a research program, how to write a grant proposal and how to publish in good journals. Let me add that it is not easy to be a good mentee. In the end, a good mentor will be demanding and, if necessary, he or she will also criticize your research program. He or she might remind you that you have to become independent in your research, that you have to write grant proposals, that you have to organize events, etc. All this is considered necessary by hiring committees and should not be neglected. But a good mentor should also encourage you and appreciate you and your scientific work.

Austrian universities and Research Institutions like IST Austria are attracting more and more young mathematicians with high scientific potential. Since the number of available academic positions in Austria is quite low, what would you advise them to do once they finished their PhD?

Don't restrict your career options to Austria or to German speaking countries. Mathematics is very international, and working abroad can be a great experience. This is true within academia but also for the wide variety of jobs that a mathematician with a PhD can get nowadays.

Almost any career is facing ups and downs. Did you make such experiences and how did they affect you?

After my habilitation, I was applying for many positions as a professor for quite a few years. It was frustrating when often I was not even invited for an interview (by the way, I don't think that this would happen that often nowadays). In the end, I realized that the restriction to German speaking countries was not wise and moved to New York City when I got an offer from there. I don't think that I would have made this move if I had also got an offer from Germany or Austria. But in the end, my years in the US were very important and rewarding for me.

Interview organized by Sylvia Frühwirth-Schnatter (Vienna University of Economics and Business) and Elena Resmerita (University of Klagenfurt).

Nachrichten der Österreichischen Mathematischen Gesellschaft

Reinhard Winkler 1964–2021

Ao.Univ.-Prof. Dr. Reinhard Winkler ist am 13. Oktober 2021 nach kurzer, aber schwerer Krankheit verstorben. Reinhard Winkler war nicht nur ein hochgeschätzter Kollege mit einem sehr breiten Interessensfeld, sondern auch ein sehr aktives Mitglied der ÖMG, der er seit 1987 als Mitglied angehört hat. Er hat für sehr viele Jahre, nämlich von 2003–2017, in der Redaktion der IMN mitgewirkt und auch in den letzten Jahren immer wieder viel beachtete Beiträge für die IMN verfasst. Zudem war er ein regelmäßiger Verfasser von Beiträgen in der Schriftenreihe zur Didaktik der Mathematik der ÖMG bzw. der Didaktikhefte der ÖMG. Ein ausführlicher Nachruf ist für das nächste Heft geplant.

Redaktioneller Hinweis

Das Protokoll der Generalversammlung vom 19.11.2021 an der Universität Wien wird, zusammen mit den Laudationes zu den Förderungspreisen, im April-Heft der IMN erscheinen.

Neue Mitglieder

Egger Herbert, Univ.-Prof. Dr. – Institut für Numerische Mathematik, JKU, Altenberger Str. 69, 4040 Linz. geb. 1973. Doktorat 2005 an der JKU. Postdoc-Stellen am RICAM in Linz, an der RWTH Aachen, an der TU Graz sowie der KFU Graz. Vertretungsprofessor an der TU Chemnitz. W2-Professor für Scientific Computing von 2011-2012 an der TU München, W3-Professor für Numerische Analysis und Scientific Computing an der TU Darmstadt von 2012-2021. Seit Kurzem Professor für Numerische Analysis an der JKU und Wissenschaftlicher Direktor am RICAM. email *herbert.egger@jku.at*

Ha Nhi Yen – Karl-Löwe Gasse 17-19, 1120 Wien. geb. 2003. Schülerin am BORG 3 in Wien. email *hayennhi31@gmail.com*

Doychev Nikolay – Kollmayergasse 10/2, 1120 Wien. geb. 1996. Physikstudium an der Universität Wien, Mathematikstudium an der JKU sowie an der Fernuni Hagen. email *nikolaydoychev@yahoo.com*

Ettel David – Untere Augartenstr. 38/12, 1020 Wien. geb. 2003. email *david.ettel@gmx.at*

Nicolussi Noema, Dr. – c/o Universität Wien, Fakultät für Mathematik, Oskar-Morgenstern Platz 1, 1090 Wien. geb. 1992. Doktorat an der Universität Wien 2020. Derzeit Erwin-Schrödinger-Stipendiatin des FWF. email *noema.nicolussi@univie.ac.at*

Achleitner Franz, Dr. – c/o TU Wien, Institut für Analysis und Scientific Computing, Wiedner Hauptstr. 8-10, 1040 Wien. geb. 1978. Mathematikstudium und Doktorat an der TU Wien mit Abschluss des Doktorats 2009. Postdoc an der Universität Wien. Derzeit Postdoc an der TU Wien. email *franz.achleitner@tuwien.ac.at* https://www.asc.tuwien.ac.at/ achleitner/

Eisenkölbl Theresia, Dr. – c/o Universität Wien, Fakultät für Mathematik, Oskar-Morgenstern Platz 1, 1090 Wien. geb. 1976. Diplom und Doktorat an der Universität Wien. Universitätsassistentin an der Universität Wien sowie Maitresse de conferences am Institut Camille Jordan an der Université Claude Bernard Lyon 1. Seit Kurzem Leiterin der Begabungsförderung im Projekt „Mathematik macht Freu(n)de“ an der Universität Wien. email *theresia.eisenkoelbl@univie.c.at*

Fischer Julian, Dr. – Am Campus 1, 3400 Korneuburg. geb. 1989. Doktorat an der Universität Erlangen-Nürnberg im Jahr 2013. Postdoc an der Universität Zürich und am MPI in Leipzig. Derzeit Assistenzprofessor am IST Austria, wo er auch ein ERC Starting Grant-Projekt leitet. email *julian.fischer@ist.ac.at* http://j-fischer.eu

Ausschreibung der Preise der ÖMG

Ausschreibung des ÖMG-Förderungspreises 2022

Die Österreichische Mathematische Gesellschaft vergibt auch 2022 wieder ihren jährlichen Förderungspreis. Infrage kommen junge Mathematikerinnen oder Mathematiker, die in überdurchschnittlichem Maße durch ihre mathematische Forschung hervorgetreten sind und welche einen wesentlichen Teil ihrer Arbeiten in Österreich erbracht haben. Dabei soll die Promotion mindestens zwei bis maximal zehn Jahre zurückliegen. (Überschreitungen sind möglich bei Kindererziehungszeiten und bei nachweislichen Präsenz- oder Zivildienstzeiten.)

Die Nominierung muss durch einen zum Zeitpunkt der Nominierung in Österreich an einer Universität oder Forschungseinrichtung beschäftigten habilitierten Mathematiker bzw. eine Mathematikerin erfolgen. Der Vorschlag muss in elektronischer Form *bis spätestens 14. März 2022* beim Vorsitzenden der ÖMG einlangen und folgende Unterlagen enthalten: 1. Beschreibung und Wertung der wissenschaftlichen Leistung; 2. Publikationsliste; 3. Wissenschaftlicher Lebenslauf.

Aus den eingereichten Vorschlägen wählt eine Begutachtungskommission den Preisträger oder die Preisträgerin aus. Der Preis ist mit 1.000 € und einer Ehrenmedaille dotiert. Außerdem wird der Preisträger oder die Preisträgerin eingeladen, beim nächsten ÖMG-Kongress in einem Vortrag über die erzielten Forschungsergebnisse zu berichten. Sollte der Preisträger oder die Preisträgerin noch nicht Mitglied der ÖMG sein, so wird er oder sie auf Wunsch in die ÖMG aufgenommen und vom Mitgliedsbeitrag für das erste Jahr befreit.

Adresse für Einsendungen: Univ.-Prof. Dr. Johannes Wallner, TU Graz. email *oemg@oemg.ac.at*.

Ausschreibung der ÖMG-Studienpreise 2022

Die Österreichische Mathematische Gesellschaft vergibt auch 2022 wieder bis zu zwei Studienpreise. Die Preisträger sollen junge Mathematikerinnen und Mathematiker sein, die in den Jahren 2020 oder 2021 eine Diplom- oder Masterarbeit (im Folgenden als Masterarbeit bezeichnet) bzw. eine Dissertation eingereicht haben.

Voraussetzung für den Studienpreis für Masterarbeiten ist ein Abschluss eines Magister- oder Diplomstudiums an einer österreichischen Universität. Voraussetzung für den Studienpreis für Dissertationen ist entweder der Abschluss des Doktoratsstudiums an einer österreichischen Universität oder, im Falle eines Dokto-

ratsstudiums an einer ausländischen Universität, das Vorliegen eines abgeschlossenen Magister- oder Diplomstudiums an einer österreichischen Universität. Die Nominierung muss durch einen zum Zeitpunkt der Nominierung in Österreich an einer Universität oder Forschungseinrichtung beschäftigten Mathematiker bzw. eine Mathematikerin erfolgen.

Der Vorschlag muss in elektronischer Form *bis spätestens 14. März 2022* beim Vorsitzenden der ÖMG einlangen und folgende Unterlagen enthalten: 1. Ein Exemplar der als besonders hochqualifiziert bewerteten mathematischen Masterarbeit bzw. Dissertation; 2. Zwei begründete Bewertungen dieser Arbeit; 3. Einen Lebenslauf des Kandidaten bzw. der Kandidatin einschließlich einer kurzen Beschreibung des Studienablaufs.

Aus den eingereichten Vorschlägen werden durch eine vom Vorstand der ÖMG eingesetzte Begutachtungskommission die Preisträger ermittelt. Jeder ÖMG-Studienpreis ist mit 500 € dotiert. Jeder Preisträger erhält eine Urkunde. Sollte der Preisträger oder die Preisträgerin noch nicht Mitglied der ÖMG sein, so wird er bzw. sie auf Wunsch in die ÖMG aufgenommen und vom Mitgliedsbeitrag für das erste Jahr befreit.

Adresse für Einsendungen: Univ.-Prof. Dr. Johannes Wallner, TU Graz. email *oemg@oemg.ac.at*.

Ausschreibung der Schülerinnen- und Schülerpreise der ÖMG 2022

Die Österreichische Mathematische Gesellschaft zeichnet herausragende vorwissenschaftliche Arbeiten, die im Schuljahr 2021/22 an österreichischen Schulen entstanden sind und die einen starken Bezug zu Mathematik oder Darstellender Geometrie aufweisen, mit Preisen aus. Diese Arbeiten müssen in elektronischer Form, als PDF-Datei, *bis 10. Juli 2022* bei der ÖMG einlangen und werden von einer Jury begutachtet.

Die Verfasserinnen und Verfasser jener Arbeiten, die im Zuge dieser Begutachtung durch die Jury ausgewählt werden, werden zu einem Kurzvortrag eingeladen, in dem sie ihre Arbeit präsentieren können. Anschließend erfolgt die Preisverleihung. Die Präsentationen und die Preisverleihung der prämierten Arbeiten finden im Herbst 2022 zu einem noch festzusetzenden Termin statt.

Die ÖMG bittet alle ihre Mitglieder sowie die Leserinnen und Leser der IMN, potenziell Interessierte von dieser Einladung zu informieren und Schulen zur Teilnahme zu ermuntern.

Adresse für Einsendungen: Univ.-Prof. Dr. Johannes Wallner, TU Graz. email *oemg@oemg.ac.at*.