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 2018:

B. Kaltenbacher (Univ. Klagenfurt):
Vorsitzende
J. Wallner (TU Graz):
Stellvertretender Vorsitzender
C. Fuchs (Univ. Salzburg):
Herausgeber der IMN
M. Ludwig (TU Wien):
Schriftführerin
M. Haltmeier (Univ. Innsbruck):
Stellvertretender Schriftführer
B. Lamel (Univ. Wien):
Kassier
P. Grohs (Univ. Wien):
Stellvertretender Kassier
E. Buckwar (Univ. Linz):
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)
G. Helmberg (Univ. Innsbruck)
H. Heugl (Wien)
W. Imrich (MU Leoben)
M. Koth (Univ. Wien)
C. Krattenthaler (Univ. Wien)
W. Müller (Univ. Klagenfurt)
H. Niederreiter (ÖAW)
W. G. Nowak (Univ. Bodenkultur)
W. Schachermayer (Univ. Wien)
K. Sigmund (Univ. Wien)
H. Sorger (Wien)
R. Tichy (TU Graz)
H. Zeiler (Wien)

Vorsitzende von Sektionen und Kommissionen:

W. Woess (Graz)
H.-P. Schröcker (Innsbruck)
C. Pötzsche (Klagenfurt)
F. Pillichshammer (Linz)
V. Bögelein (Salzburg)
I. Fischer (Wien)
H. Humenberger (Didaktikkommission)
W. Müller (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 bei der Bank Austria–Creditanstalt (BIC-Code BKAUATWW).

Internationale Mathematische Nachrichten

International Mathematical News

Nouvelles Mathématiques Internationales

Nr. 238 (72. Jahrgang) **August 2018**

Inhalt

Alexander Bors: On Dynamical Aspects of Finite Group Endomorphisms and Beyond 1

Christoph Ableitinger, Hans Humenberger, Michael Oberguggenberger: Kurze Replik auf einen Aufsatz von R. Winkler: Zentralmatura in der Sackgasse? 23

Ernst Stadlober, Robert Tichy: Ulrich Dieter 1932–2018 33

Reinhard Winkler: Das TU Forum Mathematik in Wien – Gedanken zur Popularisierung von Mathematik 45

Buchbesprechungen 59

Nachrichten der Österreichischen Mathematischen Gesellschaft 63

Neue Mitglieder 65

Die Zahl auf der Titelseite gibt die größte derzeit bekannte Primzahl wieder. Es handelt sich um die Mersennesche Primzahl $M_{77232917} = 2^{77232917} - 1$ mit 23 249 425 Ziffern. Die Primzahl wurde im Rahmen von GIMPS (Great Internet Mersenne Prime Search) durch einen Rechner von Jonathan Pace am 26. Dezember 2017 gefunden. Der Fund wird mit einem Preisgeld von $ 3.000 belohnt. Der Nachweis der Primalität benötigte dabei sechs Tage durchgehender Computerrechnungen auf einem PC mit einer Intel i5-6600-CPU. Mit dieser Primzahl ist man dem nächsten großen Ziel, nämlich eine Primzahl mit mindestens hundert Millionen Stellen zu finden, wieder einen Schritt näher gekommen. Weitere Informationen findet man unter *https://www.mersenne.org/primes/*. In Zeiten von Bitcoin und Co. sind solche aufwendigen Rechnungen, wie etwa auch im Rahmen des SETI-Projekts, leider mittlerweile in Gefahr.

Internat. Math. Nachrichten
Nr. 238 (2018), 1–22

On Dynamical Aspects of Finite Group Endomorphisms and Beyond

Alexander Bors

The University of Western Australia

*The aim of this article is to give a self-contained overview, suitable for a general mathematical audience, of the main results from the author's PhD thesis (for which he was awarded the 2017 Studies Prize (*Studienpreis*) of the ÖMG) and of related more recent results achieved by the author in his ongoing Erwin Schrödinger Fellowship (FWF project J4072-N32). Section 1 provides some motivation and background, and in Sections 2 and 3, we discuss the author's results.*

1 Motivation and background

1.1 Studying the *mapping behavior* of homomorphisms

When S_1 and S_2 are algebraic structures *of the same kind* (e.g., two vector spaces over the same field, or two groups), then by a basic algebraic fact, every homomorphism $\varphi : S_1 \to S_2$ is already determined by its restriction $\varphi_{|M}$ to any given generating subset M of S_1. Therefore, algebraists usually identify φ with $\varphi_{|M}$, thus specifying homomorphims in a *compressed form*. A typical example which every mathematician encounters during their studies is the specification of homomorphisms between K-vector spaces by matrices over K.

However, knowing $\varphi_{|M}$ does not necessarily mean that one understands the function $\varphi : S_1 \to S_2$ as a whole, just as knowing the set

The author is supported by the Austrian Science Fund (FWF), project J4072-N32 *Affine maps on finite groups*.

ISSN 0020-7926

$$\{\varphi_{|M} \mid \varphi : S_1 \to S_2 \text{ a homomorphism}\}$$

of all *compressions* of homomorphisms $S_1 \to S_2$ (which algebraists usually equate with *understanding the set* $\mathrm{Hom}(S_1, S_2)$ *of homomorphisms* $S_1 \to S_2$) does not necessarily mean that one can easily answer questions about the possible *mapping behaviors* of homomorphisms $S_1 \to S_2$, such as the following:

- Given a function $f : S_1 \to S_2$, do there exist permutations σ_1, σ_2 on S_1 and S_2 respectively such that $\sigma_2 \circ f \circ \sigma_1$ is a homomorphism $S_1 \to S_2$?
- In case $S_1 = S_2 =: S$ is a *finite* structure, does there exist an automorphism α of S (i.e., a bijective homomorphism $S \to S$) such that α, viewed as a permutation on S, admits a cycle of length larger than $\frac{1}{2}|S|$?

In his PhD thesis, the author studied these and similar questions under the assumption that $S_1 = S_2 = G$ for a finite group G, and he continues to study problems of a similar flavor in his current Erwin Schrödinger project. One can view these as fundamental theoretical questions of intrinsic interest, but they also have connections with certain concepts (finite dynamical systems, pseudorandom number generators) and problems (constructing efficient pseudorandom number generators of high quality) from applied mathematics, which originally served as an additional motivation and inspiration to study such theoretical questions. In the next subsection, we give some more details on these applied concepts and their connections with the author's PhD results. We note that the results discussed in Subsection 3.2, which are part of the author's ongoing project, are also motivated and inspired by a concept from applied mathematics (the concept of nonlinearity from cryptography), as will be explained in more detail at the beginning of that subsection.

1.2 Background: Finite dynamical systems and pseudorandom number generation

By definition, a *finite dynamical system* (henceforth abbreviated by *FDS*) is just a finite set S of so-called *states* (S itself is also called the *state space* of the system) together with a function $f : S \to S$, called the *transition function* of the system. The idea behind this terminology is that in applications, S is the collection of states which some complex system (such as a cell organism) can potentially attain over the course of time and that this system is studied time-discretely, with f describing the transition of the system states as time progresses by one step (so if s is the state at which the system is at time t, then $f(s)$ is its state at time $t+1$). This practical application explains the fact that people studying FDSs (S, f) are usually interested in the behavior of f under iteration (corresponding to the evolution of

the system over the course of time); typical basic questions asked in this context are:

- How many periodic points does f have (i.e., for how many $s \in S$ does there exist some positive integer l such that $f^l(s) = f(f(\cdots f(s)\cdots)) = s$?)?
- Can it be efficiently decided whether, for a given pair $(x,y) \in S^2$, y lies in the *orbit of x under f*, i.e., whether $y = f^l(x)$ for some non-negative integer l (with $f^0(x) := x$)?

Of course, without further assumptions, the concept of an FDS is too general to allow for nontrivial things to be said about it, so people studying FDSs restrict their attention to special cases by introducing some further structure on the set S and only considering transition functions f that are in some way related to that structure. Some examples:

1. A *linear FDS* is a finite vector space V together with a vector space endomorphism φ of V. The study of these FDSs dates back to a 1959 paper of Elspas [13], and Hernández-Toledo in [15] gave an extensive discussion of them using linear algebra.
2. A *polynomial FDS* consists of a Cartesian power K^n of some finite field K together with a polynomial function

   $$f : K^n \to K^n, (x_1, \ldots, x_n) \mapsto (f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n))$$

   with $f_1, \ldots, f_n \in K[X_1, \ldots, X_n]$ (i.e., polynomials over K in the n formal variables $X_1, \ldots, X_n$). This generalizes the notion of a linear FDS (think of the case when $f_1, \ldots, f_n$ are linear polynomials with vanishing constant term), but polynomial FDSs are much less understood in general than linear FDSs, and there are still many interesting open problems concerning them, see [8, Section 3], for example.
3. A *group FDS* (or *finite dynamical group*, abbreviated *FDG*, a term used by the author in his PhD thesis) is a finite group G together with a group endomorphism φ of G. These were the main objects of study in the author's PhD thesis. Just like polynomial FDSs, they can be seen as a generalization of linear FDSs.
4. *Finite generalized cellular automata*: This example shows that the additional structure on S is not always an algebraic one. Here, the state space is M^V, the set of all functions $V \to M$, where V is the vertex set of some finite graph Γ (which may be directed or undirected), and M is a finite set whose

elements are called *vertex states* (not to be confused with the system states). In order to define the transition function $f : M^V \to M^V$, one first fixes, for each vertex $v \in V$, a so-called *vertex function* $g_v : M^{\mathrm{N}_1(v)} \to M$, where $\mathrm{N}_1(v)$ is the 1-*neighborhood of* v *in* Γ (i.e., the subset of V consisting of v itself and all vertices that are connected to v by an edge of Γ). f itself is then defined via $f(s)(v) := g_v(s_{|\mathrm{N}_1(v)})$ for $s \in S := M^V$ and $v \in V$. As the name suggests, this concept encompasses all *standard* cellular automata such as Conway's famous *Game of Life*.

Besides their application in modeling complex systems in science, FDSs are also used in pseudorandom number generation. Let us also explain what this is and how FDSs come into play. Nowadays, one often wants to produce a random output on a deterministic device such as a computer, for example when simulating experiments with random components or when playing a game of chance (such as any popular board game involving dice throwing) against the computer. However, there is a fundamental problem with that: A deterministic device is by its nature unable to produce *truly random* outputs. One therefore works around this problem by letting the device produce a sequence of outputs according to a deterministic procedure such that this sequence *looks like a random sequence* to someone who does not know how it is produced; one speaks of *pseudorandom number generation*. There are several precise definitions of this *looking like a random sequence*, leading to different quality criteria for pseudorandom number generators, see [23, Section 7.2], for example.

A classical and still popular way of producing pseudorandom sequences is the following (see e.g. [21, Definition 1]): Let (S, f) be an FDS, and let g be a function $S \to U$, where U is a set consisting of all potential members of the pseudorandom sequence to be output (for example, U is often chosen to be $[0,1]^d$, the compact d-dimensional unit cube, for some positive integer d, or the finite set $\{0,\ldots,m-1\}$ for some positive integer m). g is also called an *output function*. In order to start the production of a pseudorandom sequence in U, one first chooses an element $s_0 \in S$, called the *seed*. The procedure for choosing s_0 must of course also be deterministic, but it is usually *of chaotic nature*, depending on certain device parameters that are uncontrollable and can be considered *random for practical purposes* (for example, when $S = \{0,1,\ldots,9\}$, one could let s_0 be the fourth post-comma decimal digit of the device's system run-time (in seconds) at the moment the user issues the command to produce the sequence). After s_0 has been picked, the sequence that is output is $(g(s_0), g(f(s_0)), g(f(f(s_0))), \ldots)$, i.e., the translation under g of the *orbit sequence* $(s_0, f(s_0), f(f(s_0)), \ldots)$ of s_0 in (S, f).

Of course, (S, f) and g must be chosen carefully in order for the associated pseudorandom number generator to satisfy some of the aforementioned quality criteria. A classical (and well-studied) example are *(matrix) pseudorandom vector generators* (see [23, Section 10.1]), where $S = (\mathbb{Z}/m\mathbb{Z})^d$, the d-fold direct power of the

ring $\mathbb{Z}/m\mathbb{Z}$ of integer residue classes modulo m for some positive integers m and d, and $f : S \to S$ maps

$$\begin{pmatrix} x_1 + m\mathbb{Z} \\ \vdots \\ x_d + m\mathbb{Z} \end{pmatrix} \mapsto M \cdot \begin{pmatrix} x_1 + m\mathbb{Z} \\ \vdots \\ x_d + m\mathbb{Z} \end{pmatrix} = \begin{pmatrix} \sum_{j=1}^{d} a_{1,j} x_j + m\mathbb{Z} \\ \vdots \\ \sum_{j=1}^{d} a_{d,j} x_j + m\mathbb{Z} \end{pmatrix}$$

for some fixed $(d \times d)$-matrix $M = (a_{i,j} + m\mathbb{Z})_{i,j=1}^{d}$ over $\mathbb{Z}/m\mathbb{Z}$. Moreover, $g : S \to [0,1]^d$ is defined to map

$$(x_1 + m\mathbb{Z}, \ldots, x_d + m\mathbb{Z}) \mapsto (\frac{x_1}{m} \bmod 1, \ldots, \frac{x_d}{m} \bmod 1)$$

for all $x_1, \ldots, x_d \in \mathbb{Z}$. For $d = 1$, these are also called *multiplicative congruential generators*. We note that the underlying FDSs (S, f) of pseudorandom vector generators are group FDSs.

Certainly, not all choices of (m, M) in the above example lead to a *good* pseudorandom number generator, but which such pairs constitute a *good choice* has been extensively studied, see [23, Section 7.3] for an overview of and some more references on the case $d = 1$, and [23, Section 10.1] for more information on the general case. One necessary (and by far not sufficient) condition is that the associated FDS $((\mathbb{Z}/m\mathbb{Z})^d, v \mapsto Mv)$ admit a *large* orbit, i.e., that for at least one $v \in (\mathbb{Z}/m\mathbb{Z})^d$, the orbit $\{v, Mv, M^2v, \ldots\} \subseteq (\mathbb{Z}/m\mathbb{Z})^d$ is *large* (for example, of size at least $\rho \cdot m^d = \rho |(\mathbb{Z}/m\mathbb{Z})^d|$ for some given $\rho \in (0,1]$, such as $\rho := \frac{1}{2}$ or $\rho := \frac{1}{10}$ (the precise value of ρ then being a matter of convention)), see [23, Section 7.2, p. 164].

There are also computational aspects to consider for the applicability of an FDS (S, f) in pseudorandom number generation: One should be able to compute each of the function values of f efficiently and store f as a whole economically (using only little storage space) on a computer. These criteria are fulfilled e.g. for the polynomial FDSs described above (assuming that the arithmetic of the finite field K is efficient and that only *sparse* polynomials, say with $O(\log^C |K|)$ (Landau notation, meaning at most $D \cdot \log^C |K|$ for some positive constant D) many nonzero terms for some positive constant C, are considered), but as also mentioned above, polynomial FDSs are hard to understand in general. On the other hand, assuming that a finite group G allows for efficient *normal form computations* (see Subsection 3.3), these computational requirements hold for every endomorphism φ of G (note that as stated in Subsection 1.1, it suffices to store the values of φ on a generating subset of G, which, as one can show using Lagrange's theorem, only has size at most $\log_2 |G|$). Therefore and given both the large variety of structures of finite groups and the vast knowledge on them, it seemed natural to the author to study group FDSs both theoretically and with regard to potential new examples of

pseudorandom number generators based on such FDSs; this was the starting point of the author's PhD research.

2 On dynamical aspects of finite group endomorphisms: Results from the author's PhD thesis

2.1 Results on the functional graphs of finite group endomorphisms

In this subsection, we discuss the results from Chapter 2 of the author's PhD thesis, published as [2]. An important concept in the general theory of FDSs is the following:

Definition. *Let (S, f) be an FDS. The* functional graph of (S, f) *(or simply of f), denoted Γ_f, is the (finite) digraph with vertex set S and having a directed edge $x \to y$ if and only if $y = f(x)$.*

There is a simple characterization of when a given finite digraph Γ with vertex set V is the functional graph of a suitable function on V: This is the case if and only if Γ is a *finite directed* 1*-forest*, which is a finite digraph that arises from a finite disjoint union of finite directed circles by glueing, onto each vertex on each of the circles, the root of some finite directed rooted tree all of whose edges are oriented toward the root.

It was the author's goal in [2] to gain as good of an understanding as possible of those finite digraphs that arise as functional graphs of finite group endomorphisms. The following three enumeration points provide an overview of this:

1. A consequence of a version of the Fitting lemma for groups (see [9, Theorem 4.2]), which can also be proved directly, is that each endomorphism φ of each finite group G induces a semidirect decomposition (readers not familiar with (internal) semidirect group products, see below) $G = \mathrm{hypker}(\varphi) \rtimes \mathrm{per}(\varphi)$, where

   - $\mathrm{hypker}(\varphi) := \{g \in G \mid \varphi^n(g) = 1_G \text{ for some non-negative integer } n\}$ is the so-called *hyperkernel of* φ, and
   - $\mathrm{per}(\varphi) := \{g \in G \mid \varphi^n(g) = g \text{ for some positive integer } n\}$ is the set of periodic points of φ.

   In more *down-to-earth* terms, this just means that $\mathrm{hypker}(\varphi)$ is a normal subgroup of G, $\mathrm{per}(\varphi)$ is a subgroup of G (not necessarily normal), G is generated by $\mathrm{hypker}(\varphi) \cup \mathrm{per}(\varphi)$ and $\mathrm{hypker}(\varphi) \cap \mathrm{per}(\varphi) = \{1_G\}$ (so the

only difference between internal semidirect and internal direct products is that in the former, only one of the two factors needs to be normal).

A consequence of this is that (just as for direct products) every element $g \in G$ admits a unique factorization $g = h \cdot p$ with $h \in \mathrm{hypker}(\varphi)$ and $p \in \mathrm{per}(\varphi)$. This induces an identification of the *set* G with the Cartesian product $\mathrm{hypker}(\varphi) \times \mathrm{per}(\varphi)$, under which φ corresponds to the componentwise application of $\varphi_{|\mathrm{hypker}(\varphi)}$ and $\varphi_{|\mathrm{per}(\varphi)}$. Consequently, Γ_φ can be decomposed (as a graph tensor product) into the two functional graphs $\Gamma_{\varphi_{|\mathrm{hypker}(\varphi)}}$ and $\Gamma_{\varphi_{|\mathrm{per}(\varphi)}}$, the former of which is the functional graph of a *nilpotent* finite group endomorphism (a finite group endomorphism mapping every element to the neutral element 1 after sufficiently many iterations) and the latter of which is the functional graph of a finite group *auto*morphism. It therefore suffices to study these two special cases, and this also implies that in contrast to general functional graphs, in the functional graph of a finite group endomorphism, the rooted trees whose roots are glued onto the circles as described above are all isomorphic.

2. The finite digraphs that arise as functional graphs of nilpotent finite group endomorphisms were combinatorially characterized by the author in [2, Theorems 2 and 3, and the Proposition at the end of Section 2]. Each such graph arises by glueing a loop to the root of a suitable finite directed rooted tree Δ having each edge oriented toward the root, and the author described the possibilities for Δ through its *branching behavior*, which turned out to be *rigid*, see [2, Definition 1] for the precise definition of this.

3. The problem of characterizing the finite digraphs that arise as functional graphs of finite group automorphisms remains open. Note that each such graph is a disjoint union of directed circles, corresponding to the cycles of the automorphism when viewed as a permutation on the underlying group, and so this is essentially the same as characterizing the possible cycle types (i.e., the information how many cycles of each length there are) of finite group automorphisms, which is considered to be a difficult problem among group theorists, for which there probably is not a *simple and clean* solution as for nilpotent endomorphisms.

2.2 Finite group automorphisms with a large cycle

Given that a complete understanding of the functional graphs of finite group automorphisms in general is probably out of reach, the author then restricted his attention to automorphisms that are *extreme* in the sense that they have a *long* cycle; this was also motivated by the connection to pseudorandom number generators as outlined at the end of Subsection 1.2. The results presented in this subsection are from Chapter 3 of the author's thesis and were published as [1] and [3].

Let us first introduce some notation for a more precise and concise formulation of the results:

Notation. *Let G be a finite group.*

1. *For an automorphism α of G, we denote by $\Lambda(\alpha)$ the maximum cycle length of α (viewed as a permutation on G) and set $\lambda(\alpha) := \frac{1}{|G|}\Lambda(\alpha) \in (0,1]$.*

2. *We define $\Lambda(G)$ as the maximum value of $\Lambda(\alpha)$ where α ranges over the automorphisms of G (so $\Lambda(G)$ is the maximum possible cycle length that can be achieved by some automorphism of G) and set $\lambda(G) := \frac{1}{|G|}\Lambda(G) \in (0,1]$.*

The main achievement of the papers [1] and [3], which will be explained in more detail below, is a complete classification of the pairs (G,α) where G is a finite group and α is an automorphism of G with $\lambda(\alpha) \geq \frac{1}{2}$, split into the cases $\lambda(\alpha) > \frac{1}{2}$ (see [1, Corollary 1.1.8]) and $\lambda(\alpha) = \frac{1}{2}$ (see [3, Theorem 1.1.4]). In particular, this gives a classification of the finite groups G with $\lambda(G) \geq \frac{1}{2}$, and it shows that

- a finite group G with $\lambda(G) > \frac{1}{2}$ is abelian and
- the pairs (G,α) with $\lambda(\alpha) > \frac{1}{2}$ essentially are just those group FDSs long known and used in some classical pseudorandom vector generators (see Subsection 1.2 and also below).

Some further applications of this, which were worked out in [3], are

1. a deterministic algorithm to produce, for each given $\rho \in \left[\frac{1}{2},1\right] \cap \mathbb{Q}$, a finite description of the complete list of pairs (G,α), where G is a finite group, α is an automorphism of G and $\lambda(\alpha) = \rho$, see [3, Subsection 2.3], and
2. some insights concerning topological properties of the subset of $[0,1]$ consisting of all λ-values of all finite group automorphisms, most notably that it is not dense (i.e., that there are nonempty open subintervals of $[0,1]$ that do not contain a single λ-value), see [3, Theorem 1.1.5(b)].

In the rest of this subsection, to give interested readers some impressions, we provide some more background on and a precise formulation of the classification of the (G,α) with $\lambda(\alpha) > \frac{1}{2}$.

There are two well-known classes of examples of group FDSs (G,α) such that α is an automorphism of G and $\lambda(\alpha) > \frac{1}{2}$. The first class has an underlying group G of the form $\mathbb{Z}/p^k\mathbb{Z}$ for some prime $p > 2$ and some positive integer k. Recall that the automorphism group of $\mathbb{Z}/p^k\mathbb{Z}$ is isomorphic with $(\mathbb{Z}/p^k\mathbb{Z})^*$, the group

of units of the ring $\mathbb{Z}/p^k\mathbb{Z}$, which is of order $\phi(p^k) = p^{k-1}(p-1)$ (Euler totient function) and cyclic (a fact usually proved in a first number theory or algebra lecture), so there always is an $a \in \mathbb{Z}$ which is a *primitive root modulo* p^k, i.e., of the maximum possible multiplicative order modulo p^k, $\phi(p^k)$. So if we let the automorphism α of $\mathbb{Z}/p^k\mathbb{Z}$ be the (modular) multiplication by a primitive root, then α will have order $\phi(p^k)$, but it will also have a cycle of that length, namely the cycle of $1 + p^k\mathbb{Z}$ (or of any other generator of the additive group $\mathbb{Z}/p^k\mathbb{Z}$). Hence $\lambda(\alpha) = \frac{\phi(p^k)}{p^k} = 1 - \frac{1}{p} > \frac{1}{2}$.

For the second class, we will first recall the notion of a Frobenius companion matrix and some related theory. Let K be a field, and let $P(X) = a_0 + a_1X + a_2X^2 + \cdots + a_dX^d \in K[X]$, that is, $P(X)$ is a univariate polynomial in the variable X over the field K. Assume that $P(X)$ is *monic*, i.e., $P(X) \neq 0$ and a_d, the leading coefficient of $P(X)$, is 1_K. Then the *Frobenius companion matrix of* $P(X)$, which we denote by $\mathrm{Comp}(P(X))$, is the following $(d \times d)$-matrix over K:

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{d-1} \end{pmatrix}.$$

$\mathrm{Comp}(P(X))$ can also be defined as the representation matrix of the multiplication by X modulo $P(X)$ on the d-dimensional K-vector space $K[X]/(P(X))$, the quotient ring (algebra) of the polynomial ring (algebra) $K[X]$ by the principal ideal generated by $P(X)$, with respect to its *standard* K-basis $1 + (P(X)), X + (P(X)), X^2 + (P(X)), \ldots, X^{d-1} + (P(X))$. From this equivalent definition, it follows that $\mathrm{Comp}(P(X))$ is invertible if and only if $P(0) = a_0 \neq 0$ and that if K is finite and $\mathrm{Comp}(P(X))$ is invertible, its order is just what finite field theorists call the *order of* $P(X)$: the smallest positive integer o such that $P(X) \mid X^o - 1$. This also entails that (still for finite K and $\mathrm{Comp}(P(X))$ invertible) the K-vector space automorphism of K^d represented by $\mathrm{Comp}(P(X))$ has a cycle of length equal to its order, corresponding to the cycle of $1 + P(X)$ under the modular multiplication by X.

The order of a monic polynomial $P(X)$ over a finite field K and with $P(0) \neq 0$ can be computed as follows (see also [22, Section 3.1, pp. 84ff.]): First, recall that the ring $K[X]$ is factorial, so its elements, like integers, admit an *essentially unique factorization into prime elements*. Consider the factorization $P(X) = Q_1(X)^{k_1} \cdots Q_r(X)^{k_r}$ of $P(X)$ into powers of pairwise distinct prime (equivalently, irreducible) monic polynomials $Q_1(X), \ldots, Q_r(X) \in K[X]$. Then the order of $P(X)$ is the least common multiple of the orders of the $Q_i(X)^{k_i}$, and the order of $Q_i(X)^{k_i}$, in turn, is $\lceil \log_p(k_i) \rceil \, \mathrm{ord}(\xi_i)$, where $\lceil x \rceil$ denotes the smallest integer in $[x, \infty)$, ord denotes the multiplicative order and ξ_i is any of the roots of the ir-

reducible polynomial $Q_i(X)$ in the algebraic closure $\overline{K}$ of K. (Recall that a basic field-theoretic fact states that if $R(X)$ is an irreducible polynomial over K and L is the *splitting field of* $R(X)$ *over* K, i.e., the smallest extension field of K containing all the roots of $R(X)$ in $\overline{K}$, then for any two of these roots, say ξ and θ, there is a field automorphism α of L such that $\alpha(\xi) = \theta$; in particular, if $R(0) \neq 0$, then all roots of $R(X)$ in $\overline{K}$ must have the same multiplicative order.)

Therefore, if $K = \mathbb{F}_p$, the finite field with p elements (which is isomorphic to the ring $\mathbb{Z}/p\mathbb{Z}$), and if $P(X)$ is chosen as the minimial polynomial over $\mathbb{F}_p$ of a generator of the cyclic unit group $\mathbb{F}^*_{p^d}$, so that $\mathrm{ord}(P(X))$ attains the maximal possible value $p^d - 1 = p^{\deg P(X)} - 1$ (such polynomials are also called *(monic) primitive irreducible*), then the automorphism of $\mathbb{F}_p^d \cong (\mathbb{Z}/p\mathbb{Z})^d$ represented by the matrix $\mathrm{Comp}(P(X))$ has a cycle of length $p^d - 1$ and thus of proportion $1 - \frac{1}{p^d}$ (which is greater than $\frac{1}{2}$ provided that $p^d > 2$) within the entire vector space. Another example of a companion matrix achieving a long cycle is $\mathrm{Comp}((X - a)^2)$ acting on $\mathbb{F}_p^2$, where $a \in \mathbb{F}_p^*$ has order $p - 1$; this matrix has order (and thus maximum cycle length) $p(p-1) = (1 - \frac{1}{p})p^2 > \frac{1}{2}p^2$.

Both classes of examples of finite group automorphisms with a long cycle given above play an important role in our classification, for a more concise formulation of which we introduce the following notation (see also [1, Definition 1.1.6]):

Notation.

1. *Let $m \in \mathbb{N}^+ := \{1, 2, 3, \ldots\}$ and $a \in \mathbb{N} := \{0, 1, 2, \ldots\}$. We denote by $\mathrm{M}(m, a)$ the group FDS $(\mathbb{Z}/m\mathbb{Z}, \mu_a)$, where μ_a is the multiplication by a modulo m.*

2. *Let $m \in \mathbb{N}^+$ and let A be a $(d \times d)$-matrix over $\mathbb{Z}/m\mathbb{Z}$ for some $d \in \mathbb{N}^+$. We denote by $\mathcal{V}(m, A)$ the group FDS $((\mathbb{Z}/m\mathbb{Z})^d, \mu_A)$, where μ_A is the function on $(\mathbb{Z}/m\mathbb{Z})^d$ that maps $v \mapsto Av$ for each $v \in (\mathbb{Z}/m\mathbb{Z})^d$ (matrix-vector multiplication).*

3. *Let p be a prime, and let $P(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_d X^d \in \mathbb{F}_p[X]$, that is, $P(X)$ is some univariate polynomial in the variable X with coefficients from $\mathbb{F}_p$. Assume that $P(X)$ is monic, i.e., $P(X) \neq 0$ and $a_d = 1$. We set $\mathcal{V}(P(X)) := \mathcal{V}(p, \mathrm{Comp}(P(X)))$.*

We note that $\mathrm{M}(m, a)$ can be viewed as $\mathcal{V}(m, (a))$, where the second argument is the (1×1)-matrix with entry a. The notation $\mathrm{M}(m, a)$ is derived from *multiplicative congruential generator*, and $\mathcal{V}(m, A)$ from *pseudorandom vector generator*. Our analysis of examples above gives us the following *basic* examples of group FDSs (G, α) where α is an automorphism of G (such group FDSs will henceforth be called *periodic*) and $\lambda((G, \alpha)) := \lambda(\alpha) > \frac{1}{2}$:

1. For each $k \in \mathbb{N}^+$ with $k \geq 2$ and each monic primitive irreducible polynomial $P(X) \in \mathbb{F}_2[X]$ of degree k: $\mathcal{V}(P(X))$, of (underlying group) size 2^k and

with Λ-value $2^k - 1$ and λ-value $1 - \frac{1}{2^k}$.

2. For each prime $p > 2$, each $k \in \mathbb{N}^+$ and each $a \in \{1, \ldots, p^k - 1\}$ that is a primitive root modulo p^k: $\mathrm{M}(p^k, a)$, of size p^k and with Λ-value $\phi(p^k) = p^{k-1}(p-1)$ and λ-value $1 - \frac{1}{p}$.

3. For each prime $p > 2$, each $k \in \mathbb{N}^+$ and each monic primitive irreducible polynomial $P(X) \in \mathbb{F}_p[X]$ of degree k: $\mathcal{V}(P(X))$, of size p^k and with Λ-value $p^k - 1$ and λ-value $1 - \frac{1}{p^k}$.

4. For each prime $p > 2$ and each $a \in \{1, \ldots, p-1\}$ that is a primitive root modulo p: $\mathcal{V}((X-a)^2)$, of size p^2 and with Λ-value $p^2 - p$ and λ-value $1 - \frac{1}{p}$.

In the below formulation of the author's classification theorem, we use the notation $\prod_{i=1}^m (G_i, \alpha_i)$ to denote the *product of the group FDSs* $(G_1, \alpha_1), \ldots, (G_m, \alpha_m)$, which is the group FDS with underlying group $\prod_{i=1}^m G_i$ (direct product) and with transition function

$$(g_1, \ldots, g_m) \mapsto (\alpha_1(g_1), \ldots, \alpha_m(g_m)).$$

We also use the notion of *isomorphic group FDSs* (G, α) *and* (H, β), which just means that there is a group isomorphism $\psi : G \to H$ such that $\psi \circ \alpha = \beta \circ \psi$. As usual, we write $(G, \alpha) \cong (H, \beta)$ for (G, α) *and* (H, β) *are isomorphic*.

Theorem. *(B., 2016, [1, Corollary 1.1.8]) Let* (G, α) *be a periodic group FDS. The following are equivalent:*

1. $\lambda(\alpha) > \frac{1}{2}$.

2. *For some* $m \in \mathbb{N}$*, there are periodic group FDSs* $(G_1, \alpha_1), \ldots, (G_m, \alpha_m)$ *with* $(G, \alpha) \cong \prod_{i=1}^m (G_i, \alpha_i)$ *and such that each of the following holds:*

   (a) *For* $i = 1, \ldots, m-1$, $(G_i, \alpha_i) = \mathcal{V}(P_i(X))$ *for some monic primitive irreducible polynomial* $P_i(X) \in \mathbb{F}_2[X]$*, say of degree* $t_i \geq 2$.

   (b) *Either*

   - $(G_m, \alpha_m) = \mathcal{V}(P_m(X))$ *for some monic primitive irreducible polynomial* $P_m(X) \in \mathbb{F}_2[X]$*, say of degree* $t_m \geq 2$*, or*
   - (G_m, α_m) *is one of the odd order* basic *examples listed above (in enumeration points 2–4).*

(c) *The positive integers* $\Lambda(\alpha_1), \ldots, \Lambda(\alpha_m)$ *are pairwise coprime (note that if* $i, j \in \{1, \ldots, m\}$ *are such that* $(G_i, \alpha_i) = \mathcal{V}(P_i(X))$ *and* $(G_j, \alpha_j) = \mathcal{V}(P_j(X))$ *for some monic primitive irreducible polynomials* $P_i(X), P_j(X) \in \mathbb{F}_2[X]$*, then* $\gcd(\Lambda(\alpha_i), \Lambda(\alpha_j)) = \gcd(2^{t_i} - 1, 2^{t_j} - 1) = 2^{\gcd(t_i, t_j)} - 1$*, and so* $\Lambda(\alpha_i)$ *and* $\Lambda(\alpha_j)$ *then are coprime if and only if* t_i *and* t_j *are coprime).*

(d) $\prod_{i=1}^{m} \lambda(\alpha_i) > \frac{1}{2}$.

2.3 Finite group automorphisms whose order is *of positive proportion*

The two classes of examples of periodic group FDSs (G, α) such that α has a cycle of length more than $\frac{1}{2}|G|$ studied in the previous subsection both had the property that the largest cycle length of α, $\Lambda(\alpha)$, coincides with the order of α, $\mathrm{ord}(\alpha)$ (by which we mean the order of α as an element of the automorphism group $\mathrm{Aut}(G)$; equivalently, $\mathrm{ord}(\alpha)$ is the least common multiple of all cycle lengths of α). This is not a coincidence:

Theorem. *(Horoševskiĭ, 1974, [19, Corollary 1]) For every finite nilpotent group* G *and every automorphism* α *of* G*, we have that* $\Lambda(\alpha) = \mathrm{ord}(\alpha)$.

For readers unfamiliar with the notion of a nilpotent group, we note that nilpotent groups are a certain generalization of abelian groups (and that this notion has nothing to do with the concept of a nilpotent group endomorphism discussed in Subsection 2.1). In particular, Horoševskiĭ's theorem applies to all finite *abelian* groups G, and so in the studied examples, it was *a priori* clear that this would happen. However, Horošeskiĭ in [19, text passage between Corollaries 1 and 2] also gave examples of automorphisms α of finite groups G such that $\Lambda(\alpha) < \mathrm{ord}(\alpha)$, and, even worse, the quotient $\mathrm{mao}(G)/\Lambda(G)$, where $\mathrm{mao}(G)$ denotes the maximum automorphism order of G, can in general be arbitrarily large (this result was omitted from the author's published paper [4], but it can be found as Proposition 3.1 in an online preprint with the same title, available under https://arxiv.org/abs/1509.04607). So the condition that $\mathrm{mao}(G) \geq \rho|G|$ for some given $\rho \in (0, 1]$ is in general weaker than the condition that $\lambda(G) \geq \rho$.

As an extension of the results from Chapter 3, the conditions $\mathrm{mao}(G) \geq \rho|G|$ were studied by the author in Chapter 5 of his thesis, and the results of this investigation were published as [4]. The first insight, which (using the classification of periodic group FDSs (G, α) with $\lambda(\alpha) > \frac{1}{2}$ as well as results from Horoševskiĭ's paper [19]) only requires about one page of argumentation, is the following:

Theorem. *(B., 2017, [4, Theorem 1.1.1(1)]) An automorphism* α *of a finite group* G *satisfies* $\mathrm{ord}(\alpha) > \frac{1}{2}|G|$ *if and only if it satisfies* $\lambda(\alpha) > \frac{1}{2}$.

In particular, the classification result given at the end of the previous subsection is actually a classification of the periodic group FDSs (G,α) with $\mathrm{ord}(\alpha) > \frac{1}{2}|G|$.

The remaining main results of [4] are concerned with general conditions of the form $\mathrm{mao}(G) \geq \rho|G|$, $\rho \in (0,1]$, and with the related, weaker conditions that G admit a *bijective affine map* (i.e., a permutation on G of the form $\mathrm{A}_{t,\alpha} : G \to G$, $x \mapsto t\alpha(x)$ for some fixed $t \in G$ and $\alpha \in \mathrm{Aut}(G)$) of order at least $\rho|G|$. Before we state them, we give some group-theoretic background information.

There is an interesting distinction in the theory of finite groups between so-called solvable and semisimple (or Fitting-free) groups. Solvable groups are a generalization of abelian groups, and many results about finite abelian groups still apply to finite solvable groups (for example the existence of so-called Hall π-subgroups for all sets π consisting of primes (see [25, Section 9.1, introduction and result 9.1.7]), a stronger version of the existence (valid for all finite groups G) of Sylow p-subgroups for all primes p). On the other hand, finite semisimple groups are a generalization of the nonabelian finite simple groups and, just like the nonabelian finite simple groups themselves, often behave very differently from finite solvable groups. The author's theorem given below is one of the many manifestations of this vague statement.

Studying these two sort-of contrary classes of finite groups is also often fruitful for proving results on finite groups in general. This is because, while *not* every finite group is either solvable or semisimple, every finite group can be written as what group-theorists call an *extension of a finite semisimple group by a finite solvable group* (see [25, p. 122]). This means the following: Every finite group G has a normal subgroup N such that N is solvable and the quotient group G/N is semisimple. Actually, this normal subgroup N is unique and is the largest solvable normal subgroup of G, called the *solvable radical of* G, denoted by $\mathrm{Rad}(G)$. One may view the index $[G : \mathrm{Rad}(G)] = \frac{|G|}{|\mathrm{Rad}(G)|}$ as a measure for *how far G is from being solvable* (it is 1 if and only if G is solvable).

In this vein, statement (2) in the author's theorem below, which is concerned with finite groups G such that $\mathrm{mao}(G) \geq \rho|G|$ for a given $\rho \in (0,1]$, states that such groups are always *close to being solvable* in the sense that their radical index is bounded in terms of ρ:

Theorem. *(B., 2017, [4, Theorems 1.1.1(2,3) and 1.1.3(1,2)]) Let G be a finite group. The following hold:*

1. *If $\mathrm{mao}(G) > \frac{1}{10}|G|$, then G is solvable.*
2. *For any $\rho \in (0,1]$: If $\mathrm{mao}(G) \geq \rho|G|$, then $[G : \mathrm{Rad}(G)] \leq \rho^{-1.78}$.*
3. *If G has a bijective affine map of order larger than $\frac{1}{4}|G|$, then G is solvable.*
4. *For any $\rho \in (0,1]$: If G has a bijective affine map of order at least $\rho|G|$, then $[G : \mathrm{Rad}(G)] \leq \rho^{-5.91}$.*

3 Beyond: Results from the author's current research project

3.1 Finite groups with an automorphism orbit of positive proportion

This subsection is about results from the author's recent preprint [7], which is currently submitted to a journal. As explained at the beginning of Subsection 2.3, for each $\rho \in (0,1]$, the condition on finite groups G that G has an automorphism of order at least $\rho|G|$ (i.e., that $\mathrm{mao}(G) \geq \rho|G|$) is at most as strong as the assumption that G have an automorphism with a cycle of length at least $\rho|G|$ (i.e., that $\lambda(G) \geq \rho$). Recently, the author studied a different weakening of the condition $\lambda(G) \geq \rho$, as we will explain now.

For every group G and every subgroup A of the automorphism group $\mathrm{Aut}(G)$, one can define an equivalence relation $\sim_A$ on G via $g \sim_A h$ if and only if there is an automorphism $\alpha \in A$ such that $\alpha(g) = h$. The equivalence classes of this equivalence relation are called the *A-orbits on G*, and the cardinality of an orbit is also called its *length*; $\mathrm{Aut}(G)$-orbits on G are also simply called *automorphism orbits on G*. Now for each $\alpha \in \mathrm{Aut}(G)$, since the cyclic subgroup $\langle \alpha \rangle$ of $\mathrm{Aut}(G)$ generated by α consists just of the powers/iterates of α, the $\langle \alpha \rangle$-orbits on G correspond to the cycles of α, and $\lambda(\alpha) \geq \rho$ is equivalent to the existence of a $\langle \alpha \rangle$-orbit on G of length at least $\rho|G|$.

In view of this, a natural weakening of the condition $\lambda(G) \geq \rho$ (which just means that there is a cyclic subgroup A of $\mathrm{Aut}(G)$ achieving an orbit of length at least $\rho|G|$ on G) is the condition that the full automorphism group $\mathrm{Aut}(G)$ achieves an orbit of length at least $\rho|G|$ on G. It is precisely this condition which the author studied in his paper [7]. Before stating the precise results achieved in [7], we give some more group-theoretic background.

The reason why finite simple groups have received (and continue to receive) so much attention among finite group theorists is that they are in some sense the *basic building blocks* of finite groups, somewhat similarly to how prime numbers may be viewed as the *basic building blocks* of positive integers (built from them via multiplication). This is made precise by the so-called *Jordan-Hölder-Schreier theorem*, by which every finite group G can be written as an iterated extension (in the sense detailed in Subsection 2.3) of finite simple groups in at least one way, and the multiplicity with which each finite simple group S occurs in such a decomposition only depends on G and S (and not on the decomposition itself). The finite simple groups that occur at least once in some (hence any) such decomposition of G are called the *composition factors of G*. The aforementioned contrast between solvable and semisimple groups also manifests itself on the composition factor level, as one can show that a finite group is solvable if and only if all its

composition factors are abelian, whereas nontrivial finite semisimple groups do not just always contain nonabelian composition factors, but are actually closely related to direct products of nonabelian finite simple groups, see [25, Section 3.3, particularly result 3.3.18] (though in general, finite semisimple groups may have abelian composition factors).

One can show that for finite groups G, having a constant upper bound on the radical index $[G : \mathrm{Rad}(G)]$ is equivalent to having a constant upper bound on both the maximal order and the maximal multiplicity of a nonabelian composition factor of G. Since, as explained above, the assumption that G has an automorphism orbit of length at least $\rho|G|$ is weaker than the assumption $\lambda(G) \geq \rho|G|$, one may conjecture that the restrictions on the nonabelian composition factors of G which one can give under the former assumption are not as strong as the ones from the Theorem in Subsection 2.3, and this is indeed the case:

Theorem. *(B., 2018+, [7, Theorem 1.1.2]) Let G be a finite group, and denote by* $\mathrm{maol}(G)$ *the quotient of the maximum automorphism orbit length on G by $|G|$ (so* $\mathrm{maol}(G)$*, like $\lambda(G)$, is always an element of $(0,1]$). Then the following hold:*

1. *If* $\mathrm{maol}(G) > \frac{18}{19}$*, then G is solvable.*

2. *For any $\rho \in (0,1]$, if* $\mathrm{maol}(G) \geq \rho$*, then the orders of the nonabelian composition factors of G are at most $g(\rho)$ for some absolute (not depending on G or ρ) function $g : (0,1] \to (0,\infty)$.*

3. *For any nonabelian finite simple group S, there is a constant $c(S) \in \left(0, \frac{18}{19}\right)$ such that among finite groups G with* $\mathrm{maol}(G) \geq c(S)$*, S occurs as a composition factor with arbitrarily large multiplicity.*

So while the orders of the nonabelian composition factors of G can still be bounded in terms of ρ under the assumption $\mathrm{maol}(G) \geq \rho$, the same is not true in general for their multiplicities in G.

Finally, we note that the condition $\mathrm{maol}(G) \geq \rho$ also has connections to pseudorandom number generation, since some authors have considered the possibility to generate pseudorandom sequences not through iterated application of a single function on a state space, but through successive applications of functions from a given pool of functions on the state space, where in each step, the choice of function to be applied from the pool is (pseudo)random (see, for example, [12]). So one way to look at statement (1) of the theorem is the following: Finite groups G such that some random walk on G via applications of automorphisms of G visits more than $\frac{18}{19}|G|$ many elements of G are necessarily solvable.

3.2 Endomorphic and affine approximability of general functions on finite groups

Consider the following general concepts:

Definition. *Let X and Y be finite sets, $\mathcal{F}$ a family of functions $X \to Y$, and g a single function $X \to Y$.*

1. *For any function $f : X \to Y$, the* Hamming distance between f and g *is the number* $\operatorname{dist}(f,g) := |\{x \in X \mid f(x) \neq g(x)\}|$ *of arguments on which f and g disagree.*
2. *The* Hamming distance of g to $\mathcal{F}$ *is defined as* $\operatorname{dist}_{\mathcal{F}}(g) := \min_{f\in\mathcal{F}}\{\operatorname{dist}(f, g)\}$*, the minimum Hamming distance between g and an element of $\mathcal{F}$.*

Special cases of this general notion of Hamming distance are studied in several mathematical disciplines. For example, a fundamental problem in coding theory is to find large function families (*codes*) $\mathcal{F}$ for $X := \{1,\ldots,l\}$ and $Y := \{0,1\}$ such that for all functions $g : X \to Y$, the Hamming distance $\operatorname{dist}_{\mathcal{F}\setminus\{g\}}(g)$ is large (enabling the code to correct or detect many errors). Cryptographers are particularly interested in the case $X := \mathbb{F}_2^d$ for some positive integer d and $Y := \mathbb{F}_2$ (*Boolean functions*) and want functions $f : \mathbb{F}_2^d \to \mathbb{F}_2$ with large *nonlinearity*, i.e., large Hamming distance to the family of affine functions $\mathbb{F}_2^d \to \mathbb{F}_2$ (to resist so-called *linear attacks*); see also [10, Introduction] for some more quality criteria for Boolean functions in cryptography.

Inspired by this (particularly the second, cryptographical problem), in his preprint [6] (which is also currently submitted to a journal), the author studied the maximum Hamming distance $\operatorname{maxdist}(\mathcal{F})$ of a function $X \to Y$ from $\mathcal{F}$ in the special case where $X := Y := G$ for a finite group G and $\mathcal{F}$ is either chosen as $\operatorname{End}(G)$, the family (monoid) of endomorphisms of G or $\operatorname{Aff}(G)$, the family (monoid) of *affine maps on G*, i.e., functions $G \to G$ of the form $\mathrm{A}_{t,\varphi} : x \mapsto t\varphi(x)$ for fixed $t \in G$ and $\varphi \in \operatorname{End}(G)$. Since both these families $\mathcal{F}$ of functions on G are rather small and limited in their mapping behavior, it is to be expected that $\operatorname{maxdist}(\mathcal{F})$ is large for them, i.e., close to $|G|$, and so it is more natural to work with the complementary notion

$$\begin{aligned}\operatorname{app}(\mathcal{F}) &:= |G| - \operatorname{maxdist}(\mathcal{F}) = \min_{g:G\to G}\max_{f\in\mathcal{F}}(|G| - \operatorname{dist}(f,g)) \\ &=: \min_{g:G\to G}\max_{f\in\mathcal{F}}(\operatorname{app}(f,g))\end{aligned}$$

of the *minimum $\mathcal{F}$-approximability* of a function $G \to G$. We set $\operatorname{endapp}(G) := \operatorname{app}(\operatorname{End}(G))$ (the *minimum endomorphic approximability of (a function on) G*)

and $\mathrm{affapp}(G) := \mathrm{app}(\mathrm{Aff}(G))$ (the *minimum affine approximability of (a function on) G*). The following theorem, which is the main result of [6], gives information on the asymptotic behavior of $\mathrm{endapp}(G)$ and $\mathrm{affapp}(G)$ as $|G| \to \infty$:

Theorem. *(B., 2017+, [6, Theorem 1.1.4]) In the following three enumeration points, the variable G ranges over all finite groups.*

1. *For all nontrivial finite groups H, we have that*

$$0 \leq \mathrm{endapp}(H) \leq (\frac{1}{\log 2} + \frac{1}{\log |H|}) \log^2 |H|$$

   and

$$1 \leq \mathrm{affapp}(H) \leq (\frac{1}{\log 2} + \frac{2}{\log |H|}) \log^2 |H|.$$

   In particular, we have that $\mathrm{endapp}(G) \leq \mathrm{affapp}(G) \in \mathrm{o}(|G|)$ *as* $|G| \to \infty$ *(Landau notation, meaning that the quotients of these quantities by* $|G|$ *converge to* 0 *as* $|G| \to \infty$*).*

2. *There is an infinite class of finite groups H such that* $\mathrm{endapp}(H) \geq \log_2 |H|$ *and* $\mathrm{affapp}(H) \geq 1 + \log_2 |H|$. *In particular, we have that* $\limsup_{|G| \to \infty} \mathrm{endapp}(G) = \limsup_{|G| \to \infty} \mathrm{affapp}(G) = \infty$.

3. *There is an infinite class of finite groups H such that* $\mathrm{endapp}(H) = 0$ *and* $\mathrm{affapp}(H) = 1$. *In particular, we have that* $\liminf_{|G| \to \infty} \mathrm{endapp}(G) = 0$ *and* $\liminf_{|G| \to \infty} \mathrm{affapp}(G) = 1$.

The general upper bounds on $\mathrm{endapp}(H)$ resp. $\mathrm{affapp}(H)$ from statement (1) in the above theorem can be derived with a purely combinatorial argument, only using that H has *few* endomorphisms resp. affine maps (more precisely, that $|\mathrm{End}(H)| \leq |H|^{\log_2 |H|}$ resp. $|\mathrm{Aff}(H)| \leq |H|^{1+\log_2 |H|}$), see [6, Lemma 3.1 and its proof]. This argument, while not constructive, i.e., not yielding an explicit example of a function $H \to H$ with low endomorphic resp. affine approximability, does show that with probability converging to 1 as $|H| \to \infty$, a randomly chosen function $H \to H$ has affine (and thus also endomorphic) approximability in $O(\log^2 |H|)$.

Concerning statement (3) of the above theorem, we note that for finite *abelian* groups H, one always has $\mathrm{endapp}(H) \geq 1$ and $\mathrm{affapp}(H) \geq 2$ (see [6, Corollary 2.5]), so the statement shows that in nonabelian groups, one can in general achieve slightly lower minimum endomorphic and affine approximabilities than what is possible in the abelian setting (in which cryptographers usually work). The finite groups H given in [6, Section 4] as examples to prove statement (3) also

have another interesting property: They are nonabelian groups with commutative endomorphism monoid (in particular with abelian automorphism group), see [6, Lemma 4.2 and the paragraph after it].

3.3 Efficient algorithms for the computation of orders and cycle lengths of automorphisms of finite solvable groups

Inter alia due to the significance of FDSs for practical applications, algorithmic problems concerning them are widely studied. They can be roughly divided into two classes:

1. Global problems, asking for a property of the system itself, not depending on a particular tuple of states. For example:

   - Do all periodic states of the system have cycle length 1 (i.e., are fixed states)? This problem is studied e.g. in [11] for polynomial FDSs over $\mathbb{F}_2$, where each of the coordinate polynomials is a monomial, and in [26] for linear FDSs over finite commutative rings. In both cases, the respective paper shows that the problem can be solved in polynomial time.
   - Does there exist a fixed state? The complexity of this is studied e.g. in [18] for a generalization of graph FDSs (as defined in Subsection 2.1) with common vertex state set $\{0,1\}$, where not all vertices need to update their state at every discrete time step.

2. Local problems, asking for a property of a particular state of the system, or of a finite tuple of states. For example:

   - Is a given state periodic, and if so, what is its cycle length?
   - Do the orbits of two given states intersect?

   Both of these questions are studied e.g. in [24] for some subclasses of graph FDSs (as defined in Subsection 2.1) with common vertex state set $\{0,1\}$.

Given that by the results of Subsection 2.3, the periodic group FDSs (G,α) that may be suitable for applications in pseudorandom number generation (more precisely, where α has a cycle of length at least $\rho|G|$ for some fixed $\rho \in (0,1]$) are *close to being solvable*, it seems natural to study algorithmic problems on periodic group FDSs (G,α) where the underlying group G is solvable. In his recent preprint [5], also currently submitted to a journal, the author developed and analyzed efficient algorithms for the following two problems on such FDSs:

1. Compute the order of α, i.e., find the least common multiple of all the cycle lengths of α – a global problem.

2. Given $g \in G$, compute the length of the cycle of g under α – a local problem.

For this, it is assumed that the finite solvable group G is given through a so-called *refined consistent polycylic presentation*. For readers unfamiliar with group presentations, we note that a *presentation of a group H* is essentially a way to represent H in terms of a generating subset and the relations that hold between them, expressed through equations where both sides are (possibly empty) products of formal letters and their inverses, and each formal letter stands for an element of the generating set. For example, $\langle x, y \mid x^2 = 1, y^2 = 1, xy = yx \rangle$ is a presentation of the Klein four group $(\mathbb{Z}/2\mathbb{Z})^2$, because that group is generated by two elements $x := (\overline{1}, \overline{0})$ and $y := (\overline{0}, \overline{1})$ such that the three specified relations for x and y hold (note that these relations are given in multiplicative notation, whereas $(\mathbb{Z}/2\mathbb{Z})^2$ is usually written as an additive group) and such that any valid relation between the generators x and y in $(\mathbb{Z}/2\mathbb{Z})^2$ is a *formal consequence* of these three relations. (We will not go into detail here about what precisely this means.)

In certain cases, one can derive from a presentation of a group H, say with formal generator set X and denoting the set of formal inverses of the elements of X by X^{-1}, an effective *normal form representation* of the elements of H over the alphabet $X \cup X^{-1}$, along with the corresponding version of the group multiplication on normal forms. For instance, with regard to the above example of a presentation of the Klein four group, one can write each element of the group in a unique way as $x^{e_1}y^{e_2}$ with $e_1, e_2 \in \{0, 1\}$, and the group multiplication of H corresponds to the binary operation $x^{e_1}y^{e_2} \cdot x^{f_1}y^{f_2} := x^{(e_1+f_1) \bmod 2}y^{(e_2+f_2) \bmod 2}$. This is often useful for computational purposes, as it provides one with a concrete way of implementing the group on a computer.

A well-studied example of group presentations and associated normal form representations with computational applications are the so-called *refined consistent polycyclic presentations*. Every finite solvable group has such a presentation, and it allows to express each group element in a unique way as $x_1^{e_1} \cdots x_n^{e_n}$ where $x_1, \ldots, x_n$ are the formal generators and for $i = 1, \ldots, n$, $e_i \in \{0, \ldots, p_i - 1\}$ for some prime p_i associated with the presentation and called the *relative order of x_i*. The above presentation of $(\mathbb{Z}/2\mathbb{Z})^2$ is actually (up to a slight rewriting of the third relation into an equivalent form) a refined consistent polycyclic presentation of it. So as a set, one may represent each finite solvable group on a computer simply by $\mathbb{Z}/p_1\mathbb{Z} \times \cdots \times \mathbb{Z}/p_n\mathbb{Z}$, but the group operation is usually more complicated than just component-wise modular addition, and unfortunately, while refined consistent polycyclic presentations and the associated normal forms are considered the most efficient currently known way to deal with computational problems on finite solvable groups (see [17, introduction to Chapter 8, pp. 273f.]), no general polynomial-time algorithms are known for multiplication of normal forms of such

presentations; multiplication algorithms with subexponential (in the group order) worst-case complexity are known, though, see [16].

Since one can hardly expect to solve a computational group-theoretic problem without performing a single multiplication in the respective groups, one therefore has to accept that *efficient* in the context of algorithms on finite solvable groups G can only mean *of time-complexity subexponential in* $\log|G|$, not *of time-complexity polynomial in* $\log|G|$. Another fundamental problem that cannot be circumvented at the moment is that many basic algorithmic tasks in algebra, such as computing the order of an invertible matrix over the finite field $\mathbb{F}_p$ (which is a special case of our problem of computing the order of an automorphism of a finite solvable group), involve integer factorization, for which the most efficient currently known method is the General Number Field Sieve, which is not deterministic, but a so-called Las-Vegas-algorithm (on each input, it terminates eventually with probability 1, outputting the correct answer) and has *expected* time-complexity subexponential in the logarithm of the integer to be factored. This does not make much of a difference for the application of these algorithms in practice, but it means that the best theoretical complexity result to reasonably expect on, say, the computation of the order of an automorphism of a finite solvable group G, is to have a Las-Vegas-algorithm with expected time-complexity subexponential in $\log|G|$. And indeed, this is the case:

Theorem. *(B., 2017+, [5, Theorem 1.2.2]) There are Las-Vegas-algorithms with expected run-time subexponential in* $\log|G|$ *for computing the order of an automorphism* α *of the finite solvable group* G *and for computing the cycle length under* α *of a given element* $g \in G$ *respectively.*

Of course, this is not just a purely existential statement; explicit examples of such algorithms are given in [5, Subsection 1.4], and they were also implemented by the author in GAP [14], the corresponding source code being available from the author's website under https://alexanderbors.wordpress.com/sourcecode/pcautord/. We note that such algorithms had never been implemented before; the algorithms for these two tasks currently used by the core GAP system are based on simple iteration of α, which leads to a worst-case time-complexity exponential in $\log|G|$.

4 Concluding remarks

We now provide a few concluding thoughts on the discussed results.

1. The results may be viewed as examples of how conditions motivated from potential practical applications (such as that a finite dynamical system be able to produce a *large* orbit) may lead to interesting theoretical problems when formulated for suitable abstract models (in our case, groups).

2. Except for the results from Subsections 2.1 (which are of a qualitative nature) and 3.3 (which belong to computational group theory), the common tenor behind the results discussed in this article may be referred to as *quantitative group theory*: relating the structure of a (finite) group G with assumptions on G of a quantitative nature. The conclusions reached from these assumptions may be qualitative (*G is abelian if it has an automorphism of order larger than $\frac{1}{2}|G|$, G is solvable if it has an automorphism orbit of length more than $\frac{18}{19}|G|$*) or quantitative themselves (*the radical index $[G : \mathrm{Rad}(G)]$ is at most $\rho^{-1.78}$ if G has an automorphism of order at least $\rho|G|$*).

3. This quantitative approach to group theory allows lots of interesting questions to be asked; of particular interest are quantitative extensions or generalizations of known qualitative results. As an independent, recent example of this, we mention the fact that for any odd integer o, there is a function $g_o : (0,1] \to (0,\infty)$ such that a finite group G whose elements g satisfy $g^o = 1$ with probability at least ρ has radical index $[G : \mathrm{Rad}(G)] \leq g_o(\rho)$ [20, Theorem 1.10(i)]; for $\rho = 1$, this is an immediate consequence of the celebrated Feit-Thompson theorem, which states that a finite group of odd order is solvable.

References

[1] A. Bors, Classification of Finite Group Automorphisms with a Large Cycle, *Comm. Algebra* **44**(11):4823–4843, 2016.

[2] A. Bors, On the dynamics of endomorphisms of finite groups, *Appl. Algebra Engrg. Comm. Comput.* **28**(3):205–214, 2017.

[3] A. Bors, Classification of finite group automorphisms with a large cycle II, *Comm. Algebra* **45**(5):2029–2042, 2017.

[4] A. Bors, Finite groups with an automorphism of large order, *J. Group Theory* **20**(4):681–718, 2017.

[5] A. Bors, Computation of orders and cycle lengths of automorphisms of finite solvable groups, submitted (2017), preprint available under https://arxiv.org/abs/1707.02368.

[6] A. Bors, Worst-case approximability of functions on finite groups by endomorphisms and affine maps, submitted (2017), preprint available under https://arxiv.org/abs/1709.00734.

[7] A. Bors, Finite groups with a large automorphism orbit, submitted (2018), preprint available under https://arxiv.org/abs/1802.09215.

[8] N. Boston, A. Ostafe, I. Shparlinski and M. Zieve, The Art of Iterating Rational Functions over Finite Fields, final report of the workshop held from May 5–10, 2013, at the Banff International Research Station, http://www.birs.ca/workshops/2013/13w5141/report13w5141.pdf.

[9] A. Caranti, Quasi-inverse endomorphisms, *J. Group Theory* **16**(5):779–792, 2013.

[10] C. Carlet and Y. Tarannikov, Covering sequences of Boolean functions and their cryptographic significance, *Des. Codes Cryptogr.* **25**(3):263–279, 2002.
[11] O. Colón-Reyes, R. Laubenbacher and B. Pareigis, Boolean Monomial Dynamical Systems, *Ann. Comb.* **8**(4):425–439, 2004.
[12] D.A. Dahl, C.L. Atwood and R.A. LaViolette, A random-walk pseudorandom byte generator, *Appl. Math. Modelling* **24**(10):771–778, 2000.
[13] B. Elspas, The theory of autonomous linear sequential networks, *IRE Trans. Circuit Theory* **6**(1):39–60, 1959.
[14] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.9.1* (2018), http://www.gap-system.org.
[15] R.A. Hernández-Toledo, Linear finite dynamical systems, *Comm. Algebra* **33**(9):2977–2989, 2005.
[16] B. Höfling, Efficient multiplication algorithms for finite polycyclic groups, preprint (2004), http://www.icm.tu-bs.de/~bhoeflin/preprints/collect.pdf.
[17] D.F. Holt, B. Eick and E.A. O'Brien, *Handbook of Computational Group Theory*, Chapman & Hall/CRC (Discrete Mathematics and its Applications), Boca Raton, 2005.
[18] C.M. Homan and S. Kosub, Dichotomy results for fixed point counting in boolean dynamical systems, *Theoret. Comput. Sci.* **573**:16–25, 2015.
[19] M.V. Horoševskiĭ, On automorphisms of finite groups, *Math. USSR-Sb.* **22**(4):584–594 (1974).
[20] M. Larsen and A. Shalev, Words, Hausdorff dimension and randomly free groups, to appear in *Math. Ann.*, online version available under https://dx.doi.org/10.1007/s00208-017-1635-y.
[21] P. L'Ecuyer, Uniform random number generation, *Ann. Oper. Res.* **53**(1):77–120, 1994.
[22] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge University Press (Encyclopedia of Mathematics and its Applications, 20), Cambridge, 2nd. ed. 1997.
[23] H. Niederreiter, *Random Number Generation and Quasi-Monte Carlo Methods*, Society for Industrial and Applied Mathematics (CBMS-NSF Regional Conference Series in Applied Mathematics, 63), Philadelphia, 1992.
[24] M. Ogihara and K. Uchizawa, Computational complexity studies of synchronous Boolean finite dynamical systems on directed graphs, *Inform. and Comput.* **256**:226–236, 2017.
[25] D.J.S. Robinson, *A Course in the Theory of Groups*, Springer (Graduate Texts in Mathematics, 80), New York, 2nd. ed. 1996.
[26] G. Xu and Y.M. Zou, Linear dynamical systems over finite rings, *J. Algebra* **321**(8):2149–2155, 2009.

Authors' address:
Alexander Bors
The University of Western Australia
35 Stirling Highway, Crawley 6009, WA
Australia
email alexander.bors@uwa.edu.au

Internat. Math. Nachrichten
Nr. 238 (2018), 23–31

Kurze Replik auf einen Aufsatz von R. Winkler: Zentralmatura in der Sackgasse?

Christoph Ableitinger, Hans Humenberger, Michael Oberguggenberger

Univ. Wien, Univ. Wien, Univ. Innsbruck

Der Aufsatz von Reinhard Winkler in den IMN 237, Winkler (2018), wendet sich expressis verbis auch an die ÖMG (Österreichische Mathematische Gesellschaft). Die Autoren dieser Replik sind eng verbunden mit der ÖMG (Vorsitzender der Didaktikkommission der ÖMG, ehemaliger Vorsitzender der ÖMG), sie fühlen sich deshalb angesprochen und veranlasst zu dieser kurzen Replik. Während es unter den Mitgliedern der ÖMG ein breites Meinungsspektrum zur Zentralmatura gibt – von Zustimmung bis Ablehnung –, hat der (bisherige) Vorstand Untergruppen eingerichtet, die die Maturaaufgaben regelmäßig qualitätssichernd begleiten. Des Weiteren wurden unter breiter Beteiligung Rückmeldungen zum Grundkompetenzkatalog und den Lehrplänen erstellt.

Die Replik gliedert sich in drei Teile: Erstens, Verbesserungsvorschläge bei Formulierungen, die bereits in den erwähnten Rückmeldungen angebracht worden waren (und mit einigen Punkten in R. Winklers Aufsatz übereinstimmen), zweitens, einige Anmerkungen zu Kritikpunkten R. Winklers, bei denen wir ihm teilweise Recht geben, und drittens, eine ausführliche Replik auf R. Winklers Ruf nach einer Art von Rigorosität bzw. Abstraktion, welche unserer Ansicht nach im Mathematikunterricht in dieser Form aus guten Gründen weder durchführbar noch erstrebenswert ist.

Rückmeldungen zur Liste der Grundkompetenzen. Die ÖMG hat schon Anfang 2016 „Rückmeldungen zur Liste der Grundkompetenzen (AHS)“ gegeben. Das war damals nicht unter der Prämisse, Vorschläge zu machen, wie der Katalog der Grundkompetenzen inhaltlich überarbeitet (d.h. erweitert oder reduziert) werden könnte, sondern das Ziel war: Wie sollten – bei praktisch gleichen Inhalten – manche Formulierungen adaptiert werden, sodass sie präziser und weniger

ISSN 0020-7926

missverständlich sind? Dieses Papier wurde bis jetzt leider nicht berücksichtigt. Aber selbst wenn es Berücksichtigung gefunden hätte, wäre das für den Befund von R. Winkler nebensächlich, denn ihm geht es um viel tiefer gehende – aus seiner Sicht nötige – Adaptierungen der Grundkompetenzen, nicht nur um Formulierungen. Wir geben hier nur zwei Beispiele im angesprochenen ÖMG-Papier, die auch im Aufsatz von R. Winkler vorkommen: (1) In WS 3.2 heißt es: „Binomialverteilung als Modell einer diskreten Verteilung kennen . . . ". Hier passt offenbar das Wort „Modell" nicht und sollte durch „Beispiel" ersetzt werden. (2) Bei AN 1.4 heißt es: „das systemdynamische Verhalten von Größen durch Differenzengleichungen beschreiben bzw. diese im Kontext deuten können." Das klingt in der Tat so, als ob es um *Systeme von Differenzengleichungen* (und evtl. sogar um deren *Lösungen*) ginge. Das kann aber nicht gemeint sein. Besser wäre hier: „Diskrete Veränderungen von Größen durch Differenzengleichungen beschreiben bzw. diese im Kontext deuten können." (Diese Formulierung hat übrigens auch Eingang in den neuen Lehrplan gefunden.) Hier ginge es nicht so sehr um Grenzwerte und Lösungen, sondern lediglich darum, entsprechende Rekursionen (z.B. bei Wachstumsprozessen) aufschreiben, involvierte Parameter interpretieren und mithilfe von Tabellenkalkulation grafische Verläufe darstellen zu können. Im Wesentlichen auf dieser Ebene waren die Vorschläge in besagtem Papier der ÖMG.

Grundsätzliches zur Kritik R. Winklers. R. Winklers Aufsatz ist ein Aufzeigen der aus seiner Sicht beträchtlichen fachlichen Schwachstellen des Katalogs der sogenannten Grundkompetenzen (GK), wie er für die AHS nun schon seit einigen Jahren existiert. (Auch für die BHS gibt es einen Katalog der Grundkompetenzen, der aber nicht Gegenstand seines Aufsatzes ist.) Das spiegelt seine persönliche Sichtweise wider, eine Sichtweise, die stark von der Universitätsmathematik[1] beherrscht wird und dem dringenden Wunsch, möglichst viel *präzise*, in einem gewissen Sinn *höhere* Mathematik im Schulunterricht (speziell im Grundkompetenzen-Katalog[2]) zu verorten. Dieser Wunsch wird sich in dem Umfang, wie er es vorgeschlagen hat, nicht realisieren lassen: Denn der Mathematikunterricht hat nicht nur die Funktion, auf ein mögliches späteres Mathematikstudium vorzubereiten, auch andere Schüler/innen müssen dem Mathematikunterricht folgen können. Und da kann man das *Abstraktionsniveau* nicht so weit heben. (Die *New Math*-Bewegung in den 70er-Jahren ist u.a. daran gescheitert.) Generell muss gesagt werden, dass es einen gravierenden Unterschied zwischen einem GKK und einem Lehrbuch gibt: Während es bei einem GKK darum geht, solche GK zu formulieren, aus denen sich konkrete mögliche *Prüfungsaufgaben* für die Zentralmatura (also für alle Schüler/innen!) ergeben, können/sollen in einem Lehrbuch auch weitergehende Präzisierungen, Definitionen, Begründungen, Abstraktionen, etc.

[1] Der Begriff *Universitätsmathematik* müsste genauer als *aktuell vorherrschendes Paradigma der Lehre im Mathematikstudium* umschrieben werden und steht nicht für an Universitäten gelehrte Mathematik schlechthin.

[2] In weiterer Folge mit „GKK" abgekürzt.

vorhanden sein. Natürlich hat ein GKK auch Einfluss auf den tatsächlich stattfindenden Unterricht, aber daraus die Konsequenz zu ziehen, dass sich alle im Aufsatz von Winkler erwähnten mathematischen Inhalte auch im GKK widerspiegeln sollen, ist u.E. nicht angemessen.

Ein Schlüssel zum Zugang R. Winklers liegt u.E. in einem Satz auf S. 52, wo er bedauert, dass man sich abgewöhnt habe, Fragen zu stellen, die mit „Was ist ein(e) . . .“ beginnen. Dieses Bedauern drückt die Position aus, dass jedem mathematische Begriff eine strenge, formale Definition zugrunde gelegt werden muss, bevor man damit operieren darf. Demgegenüber steht die in den Naturwissenschaften weit verbreitete Position, die stattdessen fragt „Was mache ich korrekterweise mit einer(m) . . . “, also mathematische Objekte von ihren operativen Eigenschaften her versteht. Viele Kritikpunkte R. Winklers lösen sich auf, wenn man letztere Position einnimmt. Dies wird besonders augenscheinlich bei der Frage, wie Wahrscheinlichkeit und Statistik im Unterricht vermittelt werden soll.

Bevor wir auf ausgewählte Punkte seiner Kritik, bei denen wir die Lage gänzlich anders sehen, auf einer eher grundsätzlichen Ebene eingehen, beginnen wir mit einigen Punkten, bei denen wir ihm (zumindest) teilweise Recht geben.

1. Es ist nur schwer nachzuvollziehen, warum nur bei Potenzfunktionen und bei der Quadratwurzelfunktion die vertikale Verschiebung des Funktionsgraphen eine Rolle spielen soll ($f(x) = a \cdot x^z + b$), horizontale und vertikale Streckungen nur bei der Sinusfunktion ($f(x) = a \cdot \sin(b \cdot x)$). Denn diese Phänomene („Transformationen“) spielen schon eine Rolle, wenn man die allgemeine Form einer quadratischen Funktion f mit $f(x) = ax^2 + bx + c$ in der Scheitelpunktform $f(x) = a \cdot (x - x_S)^2 + y_S$ schreibt. (Dabei ist $S = (x_S|y_S)$ der Parabelscheitel.) Lernende sollten also ganz allgemein die Veränderung des Graphen einer Funktion f beschreiben können, wenn man von $f(x)$ zu $c \cdot f(x)$, $f(x) + c$, $f(x + c)$ und $f(c \cdot x)$ übergeht.

2. Ein anderer verständlicher Wunsch von R. Winkler ist (S. 34), dass das Wort *verstehen* öfter vorkommen sollte, denn dieser Begriff ist zentral für mathematische Bildung. Dem können wir zustimmen. Das Problem daran ist allerdings, dass *verstehen* keine von allen geteilte und generell gültige Definition hat: Was genau bedeutet es, einen Begriff zu *verstehen*? Darauf gibt es sehr viele mögliche Antworten und „Niveaustufen“ (exemplarisch für den Funktionsbegriff vgl. Vollrath 1994, S. 118ff). Dieses Problem hat man nicht, wenn man Formulierungen verwendet „irgendetwas kennen oder können“. Da der *Kompetenzkatalog* naturgemäß *kompetenzorientiert* formuliert sein muss (ob das Prinzip der Kompetenzorientierung gut oder schlecht ist, ist eine ganz andere Frage!), werden diese Formulierungen bevorzugt. Trotzdem soll es gelingen, dem *Verständnis* mehr Raum zu geben, auch ohne genaue Definition dafür.

3. Auch wir sind der Meinung, dass Begriffe wie *Umkehrfunktionen* und *Verkettung von Funktionen* nicht aus dem Kompetenzkatalog ausgespart bleiben sollten. Dazu müssen aber nicht die Begriffe *injektiv* und *surjektiv* ins Zentrum des GKK kommen. Der Begriff der *bijektiven* Funktion reicht, und den gibt es auch in Schulbüchern, nur nicht im GKK. Man kann sicher auch darüber diskutieren, ob der Inhaltsbereich *Funktionale Abhängigkeiten* evtl. besser *Reelle Funktionen und funktionale Abhängigkeiten* heißen sollte. Darüber hinaus wird in Zukunft sicher eingehend zu diskutieren sein, ob der *Logarithmus* weiterhin aus dem GKK ausgespart werden soll.

Replik auf R. Winklers Hauptkritikpunkte. Nun zu jenen Punkten, bei denen wir glauben, dass R. Winkler deutlich überschätzt, was in einem allgemeinbildenden Schulunterricht im Fach Mathematik von *allen* Maturanten/innen möglich und sinnvoll zu verlangen ist (GKK, zentrale Prüfungen). Wir gehen dabei nicht auf Details ein, sondern versuchen uns dabei auf eher grundsätzliche Aspekte zu beschränken.

1. Beim Inhaltsbereich „Funktionale Abhängigkeiten“ (S. 36) bedauert R. Winkler, dass man im GKK den allgemeineren Begriff der *Relation* nicht findet – eine *Funktion* ist dann ja eine *spezielle Relation* (z.B. mit *linkstotal* und *rechtseindeutig* zu charakterisieren). Das war in Lehrplänen in Zeiten der von Bourbaki geprägten Strukturmathematik auch tatsächlich der Fall. In guter Absicht hat man damals geglaubt: Man muss schon möglichst früh möglichst *allgemein, abstrakt, strukturbetont, etc.* Mathematik unterrichten, dann trägt der Unterricht reiche Früchte. Heute weiß man, dass das nicht funktioniert, denn das *Lernen von Mathematik* ist eben nicht gleichzusetzen mit der Mathematik schlechthin. Das waren auch die Zeiten, in denen im Schulunterrricht Begriffe wie *Gruppe, Ring, Körper,* etc. unterrichtet wurden. Nach der zugehörigen Einsicht, dass Lernende die Bedeutung dieser Abstraktionen kaum verstanden, sind diese Dinge wieder aus den Schulbüchern und Lehrplänen gestrichen worden.

2. Zum Abschluss seiner Betrachtungen zum Inhaltsbereich „Funktionale Abhängigkeiten“ (S. 39) bringt R. Winkler bekannte *Funktionalgleichungen* ins Spiel. Diese spielen aber im Schulunterricht nicht nur zufällig praktisch keine Rolle[3], sondern deswegen, weil das ein auf Schulniveau kaum zugängliches Gebiet der Mathematik ist. (Dabei sind gewissermaßen die Funktionen die interessierenden „Variablen“.) Das *Wachstumsverhalten von Funktionen* spielt dort sehr wohl eine Rolle. Daher ist es nur folgerichtig, dass nicht die Funktionalgleichungen ins Zentrum gerückt werden, sondern – bei verschiedenen Funktionen f – die entsprechenden Fragen: Wie entsteht $f(x+1)$ aus $f(x)$? Das sind die zugehörigen wichtigen, aus der

[3]Nur in M-Olympiade-Kursen.

Sichtweise des Wachstumsverhaltens typischen Fragestellungen, das ist mit *charakteristisch* gemeint. Um sicherzugehen, dass niemand die angegebenen Beziehungen zwischen $f(x+1)$ und $f(x)$ jeweils als *charakterisierend* ansieht, wäre vielleicht eine Bemerkung angebracht, dass solche Beziehungen mutatis mutandis nicht nur für $f(x+1)$, sondern allgemein für $f(x+c),\ c \in \mathbb{R}$ gelten.

3. Im Inhaltsbereich Analysis schlägt R. Winkler vor, dass GKen beim Grenzwertbegriff begriffliche Klarheit einfordern sollen (S. 40). Ihm ist „auf der Grundlage eines intuitiven Grenzwertbegriffes“ zu wenig, er fragt, was das heißen soll[4]. Eine mögliche Antwort darauf bei Grenzwerten der Form $\lim\limits_{x\to\infty} f(x)$: Das ist jener Wert, dem sich die Funktionswerte beliebig nähern, wenn x über alle Schranken wächst. Bei Grenzwerten der Form $\lim\limits_{x\to a} f(x) = g$: Wenn x gegen den Wert a strebt, dann strebt $f(x)$ gegen den Wert g. Schon präziser, aber immer noch rein sprachlich ausgedrückt: Man kann erreichen, dass $f(x)$ dem Wert g *beliebig nahe* kommt, wenn nur x hinreichend nahe bei a liegt. Mit dieser Vorstellung kommt man praktisch durch die ganze Differentialrechnung. Natürlich ist der Grenzwertbegriff so wichtig, dass seine exakte Definition den Schülern/innen nicht vorenthalten werden soll, er kann als „krönender Abschluss“ der Differentialrechnung in einem Präzisierungskapitel im Nachhinein thematisiert werden. Das formale Fassen des Grenzwertbegriffs war eine historische Leistung, die auch von Schülern/innen gewürdigt werden soll. Immerhin hat die Mathematik jahrhundertelang darum gerungen, aber er ist u.E. kein *Arbeits*begriff in der Schule, um den herum viele Aufgaben (insbesondere in zentralen Prüfungen) geschart werden sollten.

4. Mit dem Inhaltsbereich *Wahrscheinlichkeit und Statistik* (WS) liegt seiner Meinung nach besonders viel im Argen. R. Winkler beklagt, dass man „in der *Schulstochastik* keinen Anlass zu sehen scheint, Nutzen aus den großen Freiheiten zu ziehen, die uns Kolmogorow eröffnet.“ Das ist in der Tat so, und u.E. auch gut so. Den Lernenden bringt es nur sehr wenig, wenn man ihnen sagt, dass $\mathbb{P}$ nichts anderes als ein normiertes Maß auf Ω ist (selbst wenn man diesen Satz aufschlüsselt in die drei bekannten Axiome).

   Hier zeigt sich deutlich das Spannungsfeld zwischen den beiden oben erwähnten Richtungen („Was ist ein(e) . . .“ bzw. „Was mache ich korrekterweise mit einer(m) . . .“). Muss gesagt werden, was eine Wahrscheinlichkeit oder eine Zufallsvariable *ist* – ein als existierend imaginiertes Objekt, das letztlich aus den Axiomen der Mengenlehre abgeleitet wird, oder arbeitet man mit der Zufallsgröße als nicht näher definiertem Grundbegriff,

[4] Vielleicht wäre hier der Begriff „propädeutisch“ besser als „intuitiv“? Jedenfalls geht es darum, zu Beginn einen formalen Grenzwertbegriff zu vermeiden.

der durch seine Verteilungsfunktion formal vollständig charakterisiert ist? Es sei hier erwähnt, dass die Kolmogorow-Axiome keineswegs die einzige Möglichkeit darstellen, die Wahrscheinlichkeitstheorie zu begründen, siehe etwa das Werk von Fine (1973), das im Titel *Theories of Probability* bewusst die Mehrzahl verwendet (und je nach Zählung mindestens sieben Zugänge abhandelt). Mit der Zufallsgröße und deren Verteilungsfunktion kommt man in der wahrscheinlichkeitstheoretischen Modellierung und Statistik sehr weit, jedenfalls weiter, als in der Schule und in den meisten fachwissenschaftlichen Anwendungen nötig (und wie seit Jahrhunderten vor und nach Kolmogorow erfolgreich bewiesen).

In den 70er-Jahren bzw. Anfang der 80er-Jahre standen die Kolmogorow-Axiome sogar in Schulbüchern (z.B. Laub u.a. 1980), aber dieses „Experiment“ ist gescheitert, sie kamen wieder heraus, weil das für den Schulunterricht zu abstrakt erschienen ist. Lernende in der Schule sollen eher wissen, wie man *Wahrscheinlichkeiten* interpretieren kann (Stichwort *Grundvorstellungen*), und wie man damit rechnet. Natürlich ist es sinnvoll, den Lernenden zu sagen, dass in der Wahrscheinlichkeitsrechnung *Ereignisse gewissen Teilmengen von* Ω entsprechen und dass durch eine Wahrscheinlichkeit(-sfunktion) diesen Teilmengen so etwas wie eine *relative Größe* bzw. ein *relatives Maß* (bezogen auf die Gesamtmenge Ω selbst) zugeordnet wird. Aber das dann in ausgebauter Form als *Definition des Wahrscheinlichkeitsbegriffs* anzusehen, ist höchstens besonders interessierten Schülern/innen zumutbar, nicht allen (GKen, Zentralmatura).

5. R. Winkler findet es seltsam („Sowohl mathematisch als auch didaktisch[5] höchst unglücklich“), dass *Additionsregel und Multiplikationsregel* nur durch das Wort *und* verknüpft in einem Atemzug präsentiert werden (S. 46). Das eine (Additionsregel) sei „Bestandteil des Grundbegriffs“ (Additivität als eines der von Kolmogorow geforderten Axiome), und das andere (Multiplikationsregel) eine Eigenschaft . . . (gemeint ist die Unabhängigkeit von Ereignissen). Dazu sind zwei Dinge zu sagen:

   - Wenn man dem Wahrscheinlichkeitsbegriff die Kolmogorow-Axiome zugrundelegt, dann ist in der Tat die Additionsregel Teil der Definition. Aber das geschieht ja im Schulunterricht nicht. Aus der Perspektive der Kolmogorow-Axiome mag selbst der Name „-Regel“ befremdlich wirken. Im Schulunterricht – dort ist der Wahrscheinlichkeitsbegriff eben nicht schon vorher durch irgendwelche Additivitätsaxiome festgelegt – ist das aber tatsächlich eine Regel, weil sie klärt, wie man Wahrscheinlichkeiten der Art $\mathbb{P}(A \cup B)$ berechnet (als Ereignisse: A oder B).

[5] Warum hier auch die Didaktik bemüht wird, erschließt sich uns nicht.

- Mittels der Multiplikationsregel kann man dann entsprechend Wahrscheinlichkeiten der Art $\mathbb{P}(A \cap B)$ berechnen (als Ereignisse: A und B). Die Multiplikationsregel ist *nicht* die Definition der Unabhängigkeit! Diese Regel meint in ihrem Anfangsstadium nichts anderes, als dass in einem (zunächst zweistufigen) Baumdiagramm die Wahrscheinlichkeit eines Pfades als „Produkt der Einzelwahrscheinlichkeiten" berechnet werden kann. Gemeint sind Situationen der Art: Eine Urne enthält 4 rote und 6 weiße Kugeln, man zieht zweimal ohne Zurücklegen. Wie groß ist die Wahrscheinlichkeit, dass bei beiden Ziehungen eine rote Kugel gezogen wird? Sie beträgt $\frac{4}{10} \cdot \frac{3}{9}$. Diese Zusammenhänge können gut an Baumdiagrammen veranschaulicht und plausibel gemacht werden. Formal ausgedrückt, besagt diese Regel: $\mathbb{P}(A \cap B) = \mathbb{P}(A) \cdot \mathbb{P}(B|A)$. In der Universitätsmathematik ist das eine einfache Konsequenz aus der Definition bedingter Wahrscheinlichkeiten. In der Schule wird oft auf eine formale Definition bedingter Wahrscheinlichkeiten verzichtet, es wird sozusagen in die andere Richtung gearbeitet: Die Multiplikationsregel wird anhand paradigmatischer Beispiele (siehe oben) plausibel gemacht, und daraus erhält man dann eine Formel, mit der man bedingte Wahrscheinlichkeiten ausrechnen kann. Die Abfolge, zunächst die Additions- und Multiplikationsregel einzuführen und dann erst das Konzept einer (bedingten) Wahrscheinlichkeit, ist im Übrigen nicht nur in der Schule verbreitet, sondern auch der Weg, der im Rahmen der *logischen Wahrscheinlichkeit* beschritten wird, etwa von Jaynes (2003).

6. Im Zusammenhang mit *WS 2.2 relative Häufigkeit als Schätzwert von Wahrscheinlichkeit verwenden und anwenden können* schreibt R. Winkler (S. 45): „Was spricht dagegen, eine Aussage der folgenden Art zu unterrichten?: ‚Für eine Folge unabhängiger Zufallsgrößen (die alle dieselbe Verteilung haben und nicht zu sehr schwanken dürfen) konvergieren die arithmetischen Mittel mit Wahrscheinlichkeit 1 gegen den gemeinsamen Erwartungswert.'" Aus der Sicht der Universitätsmathematik mag das kurz[6] und kompakt „einen beträchtlichen Teil dessen ausdrücken, worum es in der Stochastik geht" (S. 45). R. Winkler plädiert somit dafür, das sogenannte *Starke Gesetz der großen Zahlen* im Schulunterricht zu lehren, aber da steckt wieder sehr viel höhere Mathematik dahinter, über die Lernende i.A. nicht verfügen: Folgen (reeller Zahlen) haben im Schulunterricht nicht mehr den Stellenwert wie früher[7], Folgen von Zufallsgrößen kommen im Schulunter-

[6] Uns ist nicht klar, warum hier gefordert wird: „nicht zu sehr schwanken dürfen", denn es wird ja ohnehin „iid" gefordert, und so scheint uns der zweite Teil der Forderung überflüssig zu sein. Es soll zwar auf dieses Detail hier nicht wirklich ankommen, aber vielleicht ist es ein zusätzlicher Hinweis, dass diese Formulierung für den Schulunterricht nicht geeignet ist.

[7] Das spiegelt sich natürlich auch im GKK wider, denn dort gibt es sie praktisch nicht mehr; im

richt gar nicht vor, Unabhängigkeit von *Zufallsgrößen* wird im Schulunterricht auch kaum unterrichtet – meist nur Unabhängigkeit von *Ereignissen*. Es gibt darüber hinaus bei Folgen von Zufallsgrößen verschiedene Konvergenzbegriffe[8], die meist nicht einmal in einem Lehramtsstudium thematisiert werden. Es ist uns nicht klar, wie man so eine Forderung aufstellen kann, wenn man auch noch möchte, dass Lernende mit *Verständnis* bei der Sache sein sollen (und R. Winkler betont ja an vielen Stellen, dass ihm *Verständnis* wichtig ist, auch für Lernende). Der von R. Winkler vorgeschlagene Satz ist schlicht *unverdaulich* für Lernende in der Schule, und selbst wenn es einzelne Schüler/innen geben sollte, die diesen Satz verstehen, für die Zentralmatura und Grundkompetenzen (d.h. für *alle* Maturanten/innen sozusagen als „Pflichtprogramm“) ist er mit Sicherheit ungeeignet[9].

Resümee: Wir möchten zum Abschluss betonen, dass wir das Engagement von R. Winkler, das er in der früheren Lehramtsausbildung an der TU-Wien, in der Didaktikkommission der ÖMG, etc. an den Tag legt, schätzen. Er hat auch recht, wenn er sagt, dass die momentan im GKK stehenden GKen nicht bis zum „Jüngsten Gericht“ gleich bleiben sollen, keine Frage! Und manche seiner Vorschläge halten wir auch für sinnvoll. Aber in der Einschätzung, welcher Abstraktionsgrad im Mathematikunterricht an AHS für die Allgemeinheit zumutbar ist (sodass es bei zentralen Prüfungen eine Rolle spielen sollte), unterscheidet sich unser Standpunkt doch beträchtlich.

Als Beispiel für eine u.E. zukünftig nötige Änderung wollen wir nur eines anklingen lassen, das bei R. Winkler nicht vorkam: Momentan hat die Normalverteilung im GKK die einzige Funktion: Approximation einer Binomialverteilung. Die Normalverteilung selbst als eigenständige Verteilung kommt gar nicht vor. In Zeiten von Technologie (z.B. der *Wahrscheinlichkeitsrechner* in GeoGebra) wird aber genau der Aspekt des Ersetzens der Binomialverteilung durch die Normalverteilung immer unwichtiger, weil alles quasi auf Knopfdruck auch mit der Binomialverteilung gerechnet werden kann. Für das Testen von Hypothesen mittels Binomialverteilung (auch für andere Verteilungen) gibt es im Wahrscheinlichkeitsrechner von GeoGebra eigene automatisierte Umgebungen, auch für klassische Konfidenzintervalle für einen unbekannten Anteil p. (Dabei wird allerdings die Approximation der Binomialverteilung durch die Normalverteilung benutzt.) Aber mittels „Probierverfahrens“ oder durch näherungsweises Lösen bestimmter Gleichungen

Lehrplan und in den Schulbüchern gibt es sie aber weiterhin.

[8] In der Formulierung von R. Winkler ist wohl die *fast sichere Konvergenz* angesprochen.

[9] Im Übrigen kann man gegen die Aussagekraft des *Starken Gesetzes des Großen Zahlen* durchaus auch inhaltliche Einwände vorbringen, Fine (1973), Abschnitt IVD. Selbst in der fachlichen Ausbildung für Lehramtsstudierende begnügt man sich oft mit dem *Schwachen Gesetz der großen Zahlen*, aus dem dann unmittelbar eine Präzisierung der Aussage „relative Häufigkeiten pendeln sich mit wachsendem n i.A. bei p ein“ folgt (gemeint ist das *Bernoulli'sche Gesetz der großen Zahlen*).

kann man auch heutzutage schon rein bei der Binomialverteilung bleiben beim Problem eines Konfidenzintervalls für einen unbekannten Anteil p. Bei einer der nächsten Versionen von GeoGebra gibt es auch dafür sicher ein automatisiertes Tool. Es wäre also vielleicht angebracht, bei den GKen genau auf diese Verbindung zwischen Binomial- und Normalverteilung zu verzichten und stattdessen der Normalverteilung eine eigene Daseinsberechtigung zu verschaffen.

So wie der obige Absatz ein Vorschlag ist, gibt es von anderen Fachleuten sicher andere/weitere Vorschläge, die irgendwann einmal zu einem neuen GKK führen werden. Auch aus unserer Sicht wäre eine Diskussion darüber sehr zu begrüßen.

Literatur

[1] Fine, T. (1973): Theories of Probability: An Examination of Foundations. New York: Academic Press.

[2] Jaynes, E. T. (2003): Probability Theory: The Logic of Science. Cambridge: Cambridge University Press.

[3] Laub, J. u.a. (1980): Lehrbuch der Mathematik, 3. Band. Wien: Hölder-Pichler-Tempsky.

[4] Vollrath, H.-J. (1994): Algebra in der Sekundarstufe. Mannheim: BI-Wissenschaftsverlag.

[5] Winkler, R. (2018): Zentralmatura in der Sackgasse? In: IMN 237, 27–58.

Adressen der Autoren:

Christoph Ableitinger, Hans Humenberger
Universität Wien
Fakultät für Mathematik
Oskar-Morgenstern-Platz 1
A-1090 Wien
email christoph.ableitinger@univie.ac.at, hans.humenberger@univie.ac.at

Michael Oberguggenberger
Universität Innsbruck
Arbeitsbereich für Technische Mathematik
Technikerstraße 13
A-6020 Innsbruck
email michael.oberguggenberger@uibk.ac.at

Internat. Math. Nachrichten
Nr. 238 (2018), 33–43

Ulrich Dieter 1932–2018

Ernst Stadlober, Robert Tichy

TU Graz

Ulrich Dieter hat uns am 25.1.2018 im 86. Lebensjahr nach längerer Krankheit für immer verlassen. Wir trauern um einen originellen Wissenschaftler, Kollegen und Freund, der uns fehlen wird. Unsere aufrichtige Anteilnahme gilt seiner Ehefrau Claire und der gesamten Familie. Nach seiner Biographie folgen einige persönliche Erinnerungen und Erlebnisse mit ihm, welche die umfangreichen Facetten seiner einzigartigen Persönlichkeit beleuchten. Der Nachruf schließt mit einer Würdigung des Wirkens und der Verdienste Ulrich Dieters sowie mit einem Schriftenverzeichnis.

Ulrich Dieter im Jahr 2010

1. Biographie

Ulrich Dieter wurde am 21.10.1932 in Kiel als zweiter Sohn des Ehepaars Dr. Walter Dieter und Charlotte, geb. v. Rumohr, geboren. Sein Vater stammte aus Württemberg und seine Mutter aus einem bekannten norddeutschen Adelsgeschlecht. 1934 erfolgte der Umzug nach Breslau, wo der Vater als Professor an

ISSN 0020-7926

der Augenklinik wirkte. Am 20.1.1945 in den Endwirren des Zweiten Weltkriegs flüchtete die Familie nach Preetz/Holstein. Es folgte der Besuch der Kieler Gelehrtenschule mit Abitur 1952 und am 1.5.1952 der Beginn des Studiums der Mathematik und Physik mit den Stationen Tübingen, München, Kiel, Bonn, Göttingen und wieder Kiel. Das Studium wurde 1958 mit der Dissertation *Zur Theorie der Dedekindschen Summen*, einem zahlentheoretischen Thema, abgeschlossen. Dafür erhielt er den Fakultätspreis. Sein Doktorvater war der berühmte Geometer Friedrich Bachmann. Nach einigen Jahren als Assistent in Kiel (bei Prof. Bachmann und später bei Prof. H. Schubert) hat er sich dann im Rahmen eines DFG Forschungsstipendiums der Optimierungstheorie zugewandt.

1965 erfolgte die Habilitation für Mathematik an der Universität Kiel mit der Arbeit *Theorie der Optimierungsaufgaben in topologischen Vektorräumen*. In seiner Antrittsvorlesung kommt erstmals eine statistische Fragestellung vor, die sequentielle Analysis. In dieses Jahr fällt auch die Heirat mit Klara Christa Mähler. 1966 führt der erste Aufenthalt in die USA, an die Eliteuniversitäten Stanford und Berkeley in Kalifornien. Ende 1966 tritt er eine Stelle als Wissenschaftlicher Rat am Institut für Mathematische Statistik der TH Karlsruhe (Vorstand Prof. Bierlein) an. 1969 erfolgte der erste von vielen Aufenthalten am Nova Scotia Technical College, Halifax, Kanada, wo er seinen langjährigen Koautor, den ebenfalls aus Kiel stammenden Prof. J.H. Ahrens, besuchte. 1969-1970 trat er die Vertretung des Lehrstuhls von Prof. H.H. Schaefer am Mathematischen Institut der Universität Tübingen an. 1971 erfolgte die Ernennung zum apl. Prof. an der TU Karlsruhe, 1972 war er Gastprofessor an der FU Berlin.

Am 9.4.1973 erfolgte die Ernennung zum o. Univ.-Prof. für Mathematische Statistik am gleichnamigen, neu gegründeten Institut an der TH Graz, mit anfangs 2, später 3 Assistentenstellen, 1980 wurde zusätzlich eine Professur für Angewandte Statistik geschaffen. 1981/82 war Ulrich Dieter im Rahmen eines Forschungsaufenthalts an der Stanford University, Kalifornien. Von 1973–1998, also 25 Jahre, wirkte er als Institutsvorstand am Institut für Statistik in Graz. Seit 1.10.2001 war er dort Emeritus. 5 Habilitationen wurden unter seiner Ägide am Institut abgeschlossen. Er war der Doktorvater von 9 Dissertanten und betreute 38 Diplomarbeiten.

Seine Publikationsliste umfasst mehr als 50 meist umfangreiche Arbeiten, erschienen in renommierten internationalen Journalen und Tagungsbänden; er hat an die 250 wissenschaftliche Vorträge in aller Herren Länder gehalten. Zusammen mit J.H. Ahrens hat er einige bahnbrechende Arbeiten im Bereich der gleichverteilten und nichtgleichverteilten Zufallszahlen verfasst. Die beiden kann man als Pioniere auf diesem Gebiet bezeichnen, deren Arbeiten nach wie vor in Zeitschriftenartikeln und Büchern zitiert werden und deren effizienteste Verfahren und Algorithmen Bestandteil von aktuellen Softwarepaketen sind. Diese bilden die Basis von umfangreichen Simulationen, die darauf angewiesen sind, dass man eine große

Zahl von Zufallsstichproben aus unterschiedlichen Verteilungen am Computer effizient und mit hoher Genauigkeit erzeugen kann.

2. Persönliche Erinnerungen[1]

Ich erlebte Ulrich Dieter erstmals als Student in einer Vorlesung über Optimierungstheorie, wo er gleich von seinen Erlebnissen im fernen Kanada erzählte und mich durch seine unkonventionelle Art einnahm. Es war sozusagen Sympathie auf den ersten Blick. Faszinierend für mich war es, wie er an der Tafel agierte. Er kam sehr schnell zum Kern der Sache und führte uns die kompliziertesten analytischen Herleitungen mit Bravour vor. Dass wir meistens gar nicht verstanden, woher er all die Ingredienzien nahm, war für uns nebensächlich. Viel wichtiger war, dass er in uns das Gefühl hinterließ, wie spannend Mathematik sein kann. Eine andere gut besuchte Vorlesung handelte von der Theorie der Pseudozufallszahlen, die er uns anhand eines 1974 fertiggestellten Buchmanuskripts nahebrachte. Dieses Manuskript hat eine lange Geschichte; dazu nur eine kurze Anmerkung: Es ist wohl eines der bekanntesten und meist zitierten unter jenen Büchern, die nie erschienen sind.

Bei mündlichen Diplomprüfungen war es allgemein üblich, dass man sich als Prüfling mit dem Prüfer auf ein eingegrenztes Fachgebiet einigte. Dies geschah auch mit Prof. Dieter. Bei ihm war man aber nie vor Überraschungen gefeit. Es konnte durchaus sein, dass man z.B. in einer Prüfung über Wahrscheinlichkeitstheorie mit Fragen aus ganz anderen Bereichen konfrontiert wurde wie: *Wie rechnet man eigentlich Kettenbrüche numerisch aus?* Der Fairness halber sollte ich hinzufügen, dass er diesen Zusatzstress nur seinen besten Studenten zumutete.

In den ersten Jahren in Graz hatte Prof. Dieter neben der Wahrscheinlichkeitstheorie und Mathematischen Statistik auch die Optimierungstheorie zu betreuen und numerische Praktika durchzuführen. Meine Diplomarbeit behandelte z.B. eine Fragestellung aus der Optimierung und ich musste als junger Assistent die Übungen zu unterschiedlichen Vorlesungen halten. Eine Geschichte dazu: Mitte der 70er-Jahre kamen die programmierbaren Taschenrechner von Texas Instruments auf, die bis zu 256 programmierbare Speicherplätze hatten. Was ist naheliegender als eine Lehrveranstaltung über Mathematik auf Kleinrechnern anzubieten? Wir programmierten numerische Verfahren zur Nullstellenbestimmung von Polynomen, das Rombergverfahren zur numerischen Integration und natürlich Algorithmen im Zusammenhang mit den Zufallszahlen, wie Abschätzungen für die Diskrepanz bei linearen Kongruenzgeneratoren. Unser Chef war da sehr findig und hat trickreiche Programme entwickelt, die nur manchmal einen kleinen Haken aufwiesen: Sie lieferten nicht das gewünschte Ergebnis, da sich noch irgendein dummer Fehler eingeschlichen hatte. Anfangs quälten wir Assistenten

[1] Diese Erinnerungen stammen vom ersten Autor, der den Großteil seiner akademischen Laufbahn gemeinsam mit Ulrich Dieter am Institut für Statistik der TU Graz verbracht hat.

uns bei der Fehlersuche, aber nach und nach entwickelten wir ein Gespür wie ein Arzt, der das Psychogramm seines Patienten immer besser kennt.

Als Mitarbeiter hatte man bei ihm einen großen Freiraum. Dafür musste aber jeder selbst wissen, wo es langgeht. Dies hatte Vor- und Nachteile. Bis zu meiner Promotion litt ich darunter, da ich zu dieser Zeit mehr Führung gebraucht hätte. Heute würde man sagen, die Führungskompetenz hat gefehlt. Aber er hatte viele andere Vorzüge zu bieten: Er hat uns Forschungsaufenthalte ermöglicht, nahm uns zu Tagungen mit. Wir bekamen Anregungen von interessanten Gastprofessoren, die wir regelmäßig zu Besuch hatten, und er hat von Zeit zu Zeit kleinere Symposien organisiert, wo sein Improvisationstalent zur vollen Entfaltung kam.

In der Optimierung kennt man das Problem des kürzesten Weges. Bei seinen Tagungsreisen wandte er sich einem verwandten Problem zu: dem Problem des verschlungenen Weges, das man wie folgt formulieren kann. Man minimiere die Flugkosten unter Vernachlässigung von Randbedingungen wie Reisedauer, Nächtigungskosten und Kosten von alternativen Transportmitteln, aber unter Berücksichtigung von Orten, wo interessante Mathematiker anzutreffen sind. Zum leichteren Verständnis ein Beispiel.

Zielort ist Çesme, ein Ort an der Westküste der Türkei in der Nähe von Izmir. Der kürzeste Weg dorthin führt per Flugzeug über die Route Graz-Wien-Istanbul-Izmir und dann auf dem Landweg nach Çesme. Gesamte Reisedauer ca. 6 Stunden. Das Problem des verschlungenen Weges haben wir damals, 1986, wie folgt gelöst: Man fahre am Tag 1 um 18 Uhr mit dem Auto von Graz nach Zagreb, treffe dort zum Abendessen mit zwei interessanten Mathematikern zusammen, übernachte im Hotel, stehe am Tag 2 um 5 Uhr in der Früh auf, fliege von Zagreb nach Belgrad und besichtige 12 Stunden lang den schönen Belgrader Flughafen, um am späten Abend den Anschlussflug nach Istanbul zu nehmen. Dort um Mitternacht angekommen, suche man das nächstbeste Hotel. Am Tag 3 fliege man um 8 Uhr nach Izmir, damit man um ca. 12 Uhr Mittag am Zielort Çesme ankommt. Die gesamte Reisedauer beträgt dann zwar ungefähr 42 Stunden, das Siebenfache der klassischen Variante. Was ist das aber im Vergleich zu den spannenden Abenteuern, die einem bei der zweiten Variante meist erwarten.

Ulrich Dieter hatte ein ausgeprägtes Interesse für die Geschichte Mitteleuropas und darüber hinaus. Seine Kenntnisse und sein Gedächtnis, was historische Daten, Personen, Familien- und andere Geschichten betrifft, waren wohl unübertroffen. Ich erinnere mich an eine gemeinsame Fahrt durch die Schweiz Anfang der 90er-Jahre, wo ich von ihm an einem Nachmittag einen Kompaktkurs in Schweizer Geschichte, Geographie und Kultur erhielt, gegen den jeder noch so spannende Unterricht blass wirken muss. Im Laufe der Jahre hatte ich ja gelernt, wie man seinen historischen Wurlitzer anzapfen konnte. Durch die Wahl geschickt eingestreuter Stichworte gelang es mir häufig, eine erschöpfende Auskunft über das von mir gewünschte Thema zu erhalten. Dass sich manche historischen Theorien,

die am Anfang der Diskussion von ihm verbreitet wurden, am Ende ganz anders anhörten, ist wohl eine andere Geschichte.

Szenario Institutsumzug im September 1984 von der Hamerlinggasse im Stadtzentrum in eine schöne Wohnung in der Lessingstraße nahe der Alten Technik. Durch diesen Umzug kam die wissenschaftliche Tätigkeit am Institut für drei Monate zum Erliegen. Diese wurde nämlich ersetzt durch eifrige handwerkliche Tätigkeiten unter der Führung unseres Vorstands. Für die Adaptierung des Instituts war es notwendig, in Eigenregie alle Wände mit Eichenpanelen zu verkleiden und mit Regalen zu versehen. Ich hatte beispielsweise meine Arbeitsmontur im Schrank und meine damalige Haupttätigkeit wurde nur durch lästige Vorlesungen unterbrochen. Kurz vor Weihnachten trat ich dann als Handwerker doch in den Streik. In meinem Zimmer fehlte noch die Verkleidung der beiden Fenster. All sein Charme und seine Überredungskunst fruchteten nichts. Ich blieb standhaft. Als ich aber vom Weihnachtsurlaub zurückkam, wurde ich von ihm schon mit einem verschmitzten Lächeln erwartet und er zeigte mir mein nunmehr vollständig fertiges Zimmer. Ein von ihm angeheuerter Student hatte das Werk vollendet. Mit der Bemerkung "So ist es doch viel hübscher" hat er mich dann endgültig überzeugt.

Nach einiger Zeit in unserem schönen Land entdeckte er auch die Leidenschaft zu unserem Volkssport Nr. 1, dem Skilaufen und besuchte eine Reihe von Skikursen in schönen Skigebieten. Den Feinschliff hat er dann von mir bei einem einwöchigen Intensivkurs auf der Frauenalpe bei Murau in der Obersteiermark, meiner unmittelbaren Heimat, erhalten. Wie bei Skikursen üblich, zog ich als Lehrer die Spur, und er hat versucht, meine Schwünge nachzuzeichnen, um die hohe Kunst des Parallelschwungs zu lernen. Einmal fiel mir auf, dass er immer knapper hinter mir herfuhr, und mir schien auch, dass er zum Überholen ansetzte. So beschleunigte ich mein Tempo, wie es gerade nötig war, um vorn zu bleiben. Unten am Lift angekommen, schwangen wir beide fast gleichzeitig ab. Sein trockener Kommentar von damals klingt mir heute noch in den Ohren: "Sie fahren doch schneller als ich!" Ich möchte ergänzen. Kein Wunder, bei einem Altersunterschied von beinahe 20 Jahren.

Ich erinnere mich auch an die Winter Simulation Conference, Dezember 1989, Washington, D.C. im Hilton Hotel. Es gab da einen Cocktailempfang mit sehr knapp bemessenen Getränken und trockenem Salzgebäck. Nach ca. einer halben Stunde saßen bzwstanden wir im Trockenen. Da lüftete unser Uli die linke Seite seines Sakkos und zum Vorschein kam eine in der Innentasche platzierte Flasche Cognac. Durch einfaches Kippen der Flasche direkt aus der Sakkotasche konnte er uns mit diesem köstlichen Nass versorgen. Die Party war gerettet. So behalte ich meinen Doktorvater, akademischen Lehrer und Freund in lieber Erinnerung.

3. Ulrich Dieter und sein Wirken für die Mathematik[2]

Meine erste Begegnung mit Ulrich Dieter geht auf das Studienjahr 1979/80 zurück, als er meinen akademischen Lehrer Edmund Hlawka in Wien besuchte. Ulrich Dieter interessierte sich Zeit seines Lebens für Zahlentheorie und ihre Anwendungen in Statistik und Numerik. Diese Interessen hatten Dieter und Hlawka gemeinsam, beide originelle, aber sehr unterschiedliche Persönlichkeiten. Dieter hat sehr früh erkannt, dass zahlentheoretische Konzepte wie Kettenbrücke, Gitter, Dedekindsche Summen, etc. für Anwendungen zur statistischen Simulation von grundlegender Bedeutung sind. Stets haben ihn die zugehörigen Algorithmen interessiert; in diesem Sinn war Dieter ein "konstruktiver" Mathematiker. Seine Interessen waren äußerst vielfältig: sie reichten von analytischer Zahlentheorie, zur Funktionalanalysis und Geometrie, zur Kombinatorik, Wahrscheinlichkeitstheorie, Optimierung, Statistik und Numerik. Immer standen konkrete Probleme im Zentrum seiner Interessen und es war ihm ein besonderes Anliegen, die Interaktion von Mathematik und Informatik intensiv zu fördern. Gemeinsam mit Hermann Maurer setzte er in den 1970er-Jahren wesentliche Impulse für den Aufbau der Informatik in Graz.

Von seinen zahlreichen Arbeiten möchte ich nur zwei besonders herausstreichen: Die erste behandelt Dedekindsche Summen (siehe [3] Journal für die reine u. angew. Math., 1959), ist aus seiner Dissertation hervorgegangen und behandelt ein klassisches Thema der analytischen Zahlentheorie. Das Hauptergebnis erweitert die Methode von Rademacher zur Untersuchung des Reziprozitätsgesetzes für die Dedekindsche η-Funktion. Diese Fragen hat er später immer wieder aufgegriffen, etwa auch in einer gemeinsamen Arbeit mit Bruce Berndt ([35], in derselben Zeitschrift 1982) bzw. zwei Jahre später in einer Arbeit im Journal of Number Theory ([38]). Die erstgenannte Arbeit erhielt vielfache Anerkennung und ist an prominenter Stelle im Buch von Donald Knuth, *The Art of Computer Programming*, zitiert. Schließlich möchte ich noch die Arbeit über die Berechnung von kürzesten Vektoren in Gittern ([26] Math. Comp. 1975) hervorstreichen. Diese Arbeit beschäftigt sich mit einer Frage der algorithmischen Zahlentheorie, die durch den berühmten *LLL*-Algorithmus von Lenstra, Lenstra und Lovász ihre endgültige Lösung erfahren hat.

Ulrich Dieter hat auch sehr früh die Bedeutung von mathematischer Software für Forschung und Lehre erkannt. Mitte der 80er-Jahre brachte er von einer deutschen Universität, ich glaube es war Göttingen, ein Magnetband mit. Auf diesem Band befand sich ein Computerprogramm, das er ins EDV-Zentrum der TU Graz brachte und womit er dort zunächst nicht das gebührende Verständnis vorfand. Aufgrund seiner Hartnäckigkeit wurde dieses Programm dann schließlich doch

[2]Dieser Abschnitt wurde vom zweiten Autor während eines Aufenthalts in Berkeley verfasst. Dabei wurden immer wieder Erinnerungen an Ulrich Dieter geweckt, der Kalifornien sehr geschätzt und Berkeley und Stanford oft besucht hat.

installiert. Nun, es war das heute allseits bekannte Programmsystem für symbolisches Rechnen: *Mathematica*. Uli Dieter war weiterhin aktiv auf diesem Sektor, und es dauerte nicht lange, bis auch das Konkurrenzprodukt zu Mathematica, nämlich *Maple*, durch seine Initiative an unserer TU eingeführt wurde. Nicht zu vergessen sind seine missionarischen Bemühungen, TEX, das von Donald Knuth entwickelte System zur Erstellung von mathematischen Texten, bis an die PCs der Sekretärinnen vordringen zu lassen.

Es war auch in den 80ern, als er bemerkte, dass die Programmierkenntnisse der Studierenden immer weniger für Projekte und Diplomarbeiten ausreichten. So wurde gleich im SS 1986 der nächste Gastprofessor, es war Jo Ahrens, dazu verpflichtet, den Studenten die Programmiersprache C beizubringen. Die Veranstaltung wurde ein voller Erfolg – es war übrigens der erste derartige Kurs, der an der TU Graz angeboten wurde.

Ulrich Dieter war auch wesentlich daran beteiligt, dass der mathematische Fachbereich der TU Graz eine hohe internationale Sichtbarkeit erreicht hat. Er hat durch eine für ihn typische raffinierte Vorgangsweise dazu beigetragen, dass unser Fachbereich auch jetzt noch relativ großzügig mit einem Budget für Gastprofessuren ausgestattet ist. Einer seiner Anträge für eine einsemestrige Gastprofessur wurde mithilfe des damaligen Dekans auf zwei Jahre ausgedehnt. Kurz darauf wurden diese Mittel ins reguläre Budget für Gastprofessuren übernommen, und wir profitieren noch heute davon. Das erleichtert mir mein Leben als gegenwärtiger Dekan durchaus. Er selbst hat übrigens sehr oft hochkarätige Gäste nach Österreich eingeladen. So war Paul Erdős in Graz anlässlich des 50. Geburtstags von Uli, und auch die erste Einladung von Don Zagier nach Österreich geht auf ihn zurück. Noch kurz vor seinem Tod hat er davon gesprochen, Andreas Dress nach Graz einladen zu wollen.

Ulrich Dieter hat sich auch besonders verdienstvoll für die ÖMG engagiert. Er war kurzzeitig Herausgeber der IMN und auf seine Zeit geht die Erstellung eines elektronischen Mitgliederverzeichnisses zurück. Mehrere Jahrzehnte lang war er Mitglied des Beirats der ÖMG und auch an der Ausrichtung zweier ÖMG-Tagungen beteiligt. Ich selbst konnte mit ihm eine “kleine” Tagung in Graz (1999) organisieren, was ich in sehr angenehmer Erinnerung habe.

Als Vortragsbesucher war er gern gesehen. Er ist zwar meist zu spät erschienen, aufgrund seiner raschen Auffassungsgabe konnte er dennoch zumeist problemlos folgen und interessante und originelle Fragen stellen. Bei der Auswahl von Vortragenden legte er hohe Standards an, hatte aber diesbezüglich immer einen guten Geschmack. Als besonderes Anliegen galt Ulrich Dieter die Förderung des akademischen Nachwuchses. Er hat sich stets für begabte Studierende interessiert und ist auf diese persönlich zugegangen. Seinem Interesse für analytische Zahlentheorie ist zu danken, dass er Wolfgang Müller seinerzeit von Wien ans Institut für Statistik nach Graz geholt hat und er war auch daran beteiligt, dass ich im Jahr

1990 nach Graz berufen wurde. Er hat auch als einer der ersten in Österreich das in den 1980er-Jahren entstehende Gebiet der Analyse von Algorithmen wahrgenommen. Dieses auf Donald Knuth zurückgehende Gebiet wurde damals von Philippe Flajolet in Paris zur Hochblüte entwickelt und wurde von Helmut Prodinger nach Österreich gebracht und gemeinsam mit Peter Kirschenhofer in Wien erfolgreich weiterentwickelt. Ulrich Dieter schätzte diese Entwicklungen sehr und stand bis zu seinem Tod mit Helmut Prodinger in engem Kontakt.

Das Engagement für die Mathematik und sein reger Geist waren bis zu seinem Tod aufrecht. Ich erinnere mich noch daran, wie er (schon von Krankheit deutlich gezeichnet) den Berufungsvortrag von Siegfried Hörmann (für die Professur *Angewandte Statistik* im Jahre 2016) besuchte. Er wollte unbedingt dabei sein. Wir werden ihn sehr vermissen.

4. Schriftenverzeichnis

1. Dieter U. (1957a): *Beziehungen zwischen Dedekindschen Summen*, Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg **21**, 109–125.
2. Dieter U. (1957b): *Zur Theorie der Dedekindschen Summen*, Inauguraldissertation, Universität Kiel.
3. Dieter U. (1959): *Das Verhalten der Klein'schen Funktionen* $\sigma_{g,h}(\omega_1,\omega_2)$ *gegenüber Modultransformationen und verallgemeinerte Dedekindsche Summen*, Journal für die reine und angewandte Mathematik **201**, 37–70.
4. Dieter U. (1964): *Theorie der Optimierungsaufgaben in topologischen Vektorräumen*, Habilitationsschrift, Universität Kiel.
5. Dieter U. (1965a): *Dualität bei konvexen Optimierungs- (Programmierungs-) Aufgaben*, Unternehmensforschung **9**, 91–111.
6. Dieter U. (1965b): *Optimierungsaufgaben in topologischen Vektorräumen*, Mimeographierter Vortrag, gehalten auf der Tagung der Deutschen Gesellschaft für Unternehmensforschung (DGU) in Mannheim am 6. Oktober 1965, 10 Seiten.
7. Dieter U. (1966): *Optimierungsaufgaben in topologischen Vektorräumen I: Dualitätstheorie*, Zeitschrift für Wahrscheinlichkeitstheorie und verwandte Gebiete **5**, 89–117.
8. Dieter U. (1967): *Dual Extremal Problems in Locally Convex Linear Spaces* in *Proceedings of the Colloquium on Convexity, Copenhagen 1965*, Kobenhavns Universitets Matematiske Institut, 52–57.
9. Dieter U. (1968): *Dual Extremal Problems in Linear Spaces with Applications in Game Theory and Statistics*, in *Proceed. of the NATO Study Institute on Theory and Appl. of Monotone Operators*, Venice, Italy, 1968, 303–311.
10. Dieter U. (1970a): *Autokorrelation multiplikativ-erzeugter Zufallszahlen*, Operations Research Verfahren **6**, 69–85.
11. Dieter U. and J.H. Ahrens (1970b): *Ein Modell für den Telefonverkehr mit*

wiederholten Versuchen, Operations Research Verfahren **7**, 270–284.
12. Ahrens J.H., U. Dieter and A .Grube (1970c): *Pseudo-Random Numbers: A New Proposal for the Choice of Multiplicators*, Computing **6**, 121–138.
13. Dieter U. and J.H. Ahrens (1971a): *An Exact Determination of Serial Correlations of Pseudo-Random Numbers*, Numerische Mathematik **17**, 101–123.
14. Dieter U. (1971b): *Lösung der Aufgabe 389*, Jahresbericht der Deutschen Mathematiker–Vereinigung **72**, 32–34.
15. Dieter U. (1971c): *Pseudo-Random Numbers: The Exact Distribution of Pairs*, Math. Computation **25**, 855–884.
16. Dieter U. (1972a): *Multiplikativ-erzeugte Pseudo-Zufallszahlen: Statistische Fast-Unabhängigkeit von Paaren*, ZAMM **52**, T 238–240.
17. Dieter U. (1972b): *Statistical Interdependence of Pseudo-Random Numbers Generated by the Linear Congruential Method*, in Proceedings of the Symposium on Applications of Number Theory to Numerical Analysis, Montreal, Canada, September 1971, Academic Press.
18. Dieter U. (1972c): *Properties of Pseudo-Random Numbers*, in Proceedings of the Manitoba Conference on Numerical Mathematics, October 7-9, 1971, University of Manitoba, Winnipeg, 109–116.
19. Ahrens J.H. and U. Dieter (1972d): *Computer methods for sampling from the exponential and normal distributions*, Comm. ACM **15**, 873–883.
20. Ahrens J.H. and U. Dieter (1973a): *Neuere Methoden zur Erzeugung von nicht-gleichverteilten Zufallsvariablen*, ZAMM **53**, T 221–223.
21. Ahrens J.H. and U. Dieter (1973b): *Extension of Forsythe's method for random sampling from the normal distribution*, Math. Computation **27**, 927–937.
22. Dieter U. and J.H. Ahrens (1973c): *A combinatorial method for the generation of normally distributed random numbers*, Computing **11**, 137-146.
23. Ahrens J.H. and U. Dieter (1974a): *Zusammengesetzte Verfahren zur Berechnung von Poisson- und Binomial-verteilten Zufallszahlen*, ZAMM **54**, T 243.
24. Ahrens, J.H. and U. Dieter (1974b): *Computer methods for sampling from gamma, beta, Poisson and binomial distributions*, Computing **12**, 223–246.
25. Dieter U. and J.H. Ahrens (1974c): *Acceptance-rejection techniques for sampling from the gamma and beta distributions*, Dep. Stat., Stanford University.
26. Dieter U. (1975): *How to Calculate Shortest Vectors in a Lattice*, Math. Computation **29**, 827–833.
27. Dieter U. (1979a): *Schwierigkeiten bei der Erzeugung gleichverteilter Zufallszahlen*, in Proceedings in Operations Research **8**, 249–272, Physica Verlag, Würzburg-Wien.
28. Dieter U. (1979b): *Difficulties in the Generation of Uniform Random Numbers on Computers* in Proceedings of the Sixth Conference on Probability Theory, September 10–15, Brasov, Romania 286–288.

29. Ahrens J.H. and U. Dieter (1980): *Sampling from binomial and Poisson distributions: a method with bounded computation times*, Computing **25**, 193–208.
30. Dieter U. (1981a): *Roulette as a Ruin Game*, in *Proceedings of the 5th Symposium on Operations Research*, Köln, 1980 Operations Research–Verfahren **41**, 75–78.
31. Dieter U. (1981b): *The Classical Ruin Problem and Electronic Roulette Machines*, in *Computational Statistics, Festschrift zum 60. Geburtstag von W. Wetzel*, De Gruyter Verlag, Berlin, 55–69.
32. Ahrens J.H. and Dieter, U. (1982a): *Generating gamma variates by a modified rejection technique*, Comm. ACM **25**, 47–54.
33. Ahrens J.H., and U. Dieter (1982b): *Computer generation of Poisson deviates from modified normal distributions*, ACM Trans. Math. Software **8**, 163-179.
34. Dieter U. (1982c): *An alternate proof for the representation of discrete distributions by equiprobable mixtures*, J. Applied Probability **19**, 869–872.
35. Berndt B.C. and U. Dieter (1982d): *Sums Involving the Greatest Integer Function and Riemann-Stieltjes Integration*, Journal für die reine und angewandte Mathematik **337**, 208–220.
36. Ahrens J.H.,K.D. Kohrt and U. Dieter (1983a): *Algorithm 599. Sampling from gamma and Poisson distributions*, ACM Trans. Math. Software **9**, 255–257.
37. Dieter U. (1983b): *Cotangent Sums: Reciprocity and Fast Calculation*, Bericht Nr. 184, Math.-Statist. Sektion, Forschungszentrum Graz.
38. Dieter U. (1984a): *Contangent Sums, a Further Generalization of Dedekind Sums*, Journal of Number Theory **18**, 289–305.
39. Dieter U. and J.H. Ahrens (1984b): *The Prison Rule in Roulette*, Metrika **31**, 227–231.
40. Ahrens J.H. and U. Dieter (1985a): *Sequential random sampling*, ACM Trans. Math. Software **11**, 157–169.
41. Ahrens J.H. and U. Dieter (1985b): *Realistic and Abstract Roulette, A Comparison*, in *Proc. of the 4th Pannonian Symposium on Math. Statist.*, Bad Tatzmannsdorf, 1983, Ed. W. Großmann et. al., Verlag der ungarischen Akademie der Wissenschaften, Budapest.
42. Dieter U. (1986a): *Calculating Shortest Vectors in a Lattice*, Bericht Nr. 244 der Math.-Statistischen Sektion im Forschungszentrum Graz.
43. Dieter U. (1986b): *Probleme bei der Erzeugung gleichverteilter Zufallszahlen*, in *L. Afflerbach und J. Lehn: Zufallszahlen und Simulationen*, Teubner, Stuttgart 7–20.
44. Ahrens J.H. and U. Dieter (1986c): *Effiziente Algorithmen zur Erzeugung nicht-gleichverteilter Zufallszahlen*, in *L. Afflerbach and J. Lehn: Zufallszahlen und Simulationen*, Teubner, Stuttgart.
45. Dieter U. (1986d): *Sequential Analysis: Exact Values for the Bernoulli Dis-*

tribution in *Festschrift für Prof. Eberl*, Teubner, 1987, 50–59.
46. Dieter U. und M. Unger (1987a): *Sequentielle Analysis: Genaue Werte für die Bernoulli-Verteilung*, Österreichische Zeitschrift für Statistik und Informatik **17**, 27–47.
47. Ahrens J.H. and U. Dieter (1987b): *A convenient sampling method with bounded computation times for Poisson distributions*, in *The First International Conference on Statistical Computing*, Izmir, Turkey, March 30–April 2, 1987.
48. Dieter U. (1987c): *Optimal acceptance-rejection envelopes for sampling from various distributions*, in *The First International Conference on Statistical Computing*, Izmir, Turkey, March 30–April 2, 1987.
49. Ahrens J.H. and U. Dieter (1988a): *Efficient Table-free Sampling Methods for the Exponential, Cauchy and Normal Distributions*, Communications of the ACM **31**, 1330–1337.
50. Ahrens J.H. and U. Dieter (1989a): *An Alias Method for Sampling from the Normal Distribution*, Computing **42**, 159–170.
51. Dieter U. (1989b): *Mathematical Aspects of Various Methods for Sampling from Classical Distributions*, Winter Simulation Conference 1989, Washington, D.C. 477–483.
52. Dieter U. (1991): *Principles for Generating Non-Uniform Random Numbers Bootstrapping and Related Techniques*, Proceedings, Trier, Germany, June 4–8, 1990, Lecture Notes in Economics and Mathematical Systems **376**, 3–12.
53. Dieter U. (1992): *Erzeugung von gleichverteilten Zufallszahlen*, Jahrbuch Überblicke Mathematik **1992**, 18 pp.

Adresse der Autoren:

Ernst Stadlober
TU Graz
Institut für Statistik
Kopernikusgasse 24/III
A-8010 Graz
email e.stadlober@tugraz.at

Robert Tichy
TU Graz
Institut für Analysis und Zahlentheorie
Steyrergasse 30/II
A-8010 Graz
email tichy@tugraz.at

Internat. Math. Nachrichten
Nr. 238 (2018), 45–58

Das TU Forum Mathematik in Wien – Gedanken zur Popularisierung von Mathematik

Reinhard Winkler
TU Wien

Am 11. Juni 2018 wurde an der TU Wien das TU Forum Mathematik *eröffnet. Ähnlich dem ehemaligen* math.space*, hat es sich die Aufgabe gestellt, das allgemeine Bewusstsein für die Rolle der Mathematik in der Öffentlichkeit zu fördern. Zunächst soll das vor allem mit allgemeinverständlichen Abendvorträgen und mit einem Schulprogramm an Vormittagen getan werden. Im Hinblick darauf stelle ich im vorliegenden Artikel auch allgemeine Überlegungen an über Anliegen, Schwierigkeiten und Strategien bei der Popularisierung von Mathematik.*

1 Einleitung

Unter sämtlichen Wissensdisziplinen kommt der Mathematik eine besondere Rolle zu. Denn sie befasst sich mit den universellsten Gesichtspunkten, unter denen wir unser Wissen und Verständnis von der Welt zu ordnen und zu vertiefen trachten. Deshalb gibt es kaum einen relevanten Wissensbereich, in den Mathematik nicht mehr oder weniger mächtig hineinwirkt. Selbst Kunst und Kultur stehen in faszinierender Wechselwirkung mit der Mathematik. Gleichzeitig geht die Universalität der Mathematik unweigerlich mit Abstraktionen einher, die schwer zugänglich erscheinen, sofern man nicht tagaus, tagein mit ihnen zu tun hat.

Auf der einen Seite steht also die Relevanz der Mathematik sowohl für den Einzelnen, für die Gesellschaft wie auch für die Menschheit in ihrer Gesamtheit. Auf der anderen Seite genießt die Mathematik den zweifelhaften Ruf einer für den Laien undurchdringlichen Geheimwissenschaft. Eine unüberbrückbare Kluft scheint sich dazwischen aufzutun.

ISSN 0020-7926

Mit dem *TU Forum Mathematik*, kurz *TUForMath*, nimmt die TU Wien ihre Verantwortung gegenüber der Gesellschaft wahr und versucht, einen Beitrag zur Überbrückung dieser Kluft zu leisten. Wie der Erfolg des ehemaligen *math.space* durch eineinhalb Jahrzehnte von Anfang 2003 bis Ende 2017 unter der Leitung von Rudolf Taschner eindrucksvoll gezeigt hat, sind manch wesentliche Aspekte der Mathematik durchaus geeignet, einer interessierten Öffentlichkeit zugänglich gemacht zu werden. Dazu gehören insbesondere auch solche Aspekte, die im Mathematikunterricht an den Schulen oft zu kurz kommen. Studierende, Lehrende und Gäste der TU Wien werden sich im Rahmen des TUForMath dieser Aufgabe stellen.

Der Kernkompetenz einer *Technischen* Universität entsprechend, inkludiert das natürlich die Rolle der Mathematik bei Anwendungen in Technik, Natur- und auch anderen Wissenschaften. Gleichzeitig sieht die TU Wien ihr Paradigma "Technik für Menschen" aber auch als Auftrag, im TUForMath jahrtausendealte Traditionen der Mathematik zu würdigen. In ihnen zeigt sich, dass es zutiefst menschliche Bedürfnisse und Fragen philosophischen, kulturellen und allgemein geistigen Ursprungs sind, denen die Mathematik nicht nur ihren klarsten Ausdruck verleiht, sondern für die sie auch die verlässlichsten Antworten zu bieten hat, die wir überhaupt kennen.

Wie man all diesen hohen Überzeugungen und hehren Anliegen durch ein konkretes Programm gerecht werden kann, verlangt aber durchaus substanzielle Überlegungen, die sich nicht allein mit der Wiedergabe festlich gestimmter Deklarationen wie in dieser Einleitung zufriedengeben dürfen. Die Absicht des vorliegenden Textes ist es, etwas tiefer zu dringen und zu weiteren Gedanken wenigstens anzuregen.

Die nun folgenden Hauptteile des Artikels beschäftigen sich mit den Zielen, die wir mit der Popularisierung von Mathematik generell verbinden, mit den Schwierigkeiten und Tücken, derer wir uns dabei bewusst sein sollten, und mit möglichen Strategien, diese Schwierigkeiten erfolgreich zu bewältigen. Der letzte Abschnitt diskutiert den aktuellen Planungsstand und bringt konkrete Informationen zum TUForMath.

2 Wozu Popularisierung?

Warum soll Wissenschaft generell popularisiert werden, warum insbesondere Mathematik? Mannigfache Antworten bieten sich an. Ich möchte sie unterscheiden und ordnen unter dem Gesichtspunkt, welchen Perspektiven diese Antworten gerecht werden und welchen vielleicht nicht. Daraus werden sich durchaus interessante Konsequenzen ergeben.

In erster Annäherung möchte ich die Situation mit einem Markt vergleichen, an dem Anbieter und Nachfrager teilnehmen. Beginnen wir mit der Perspektive der

Anbieter, also mit der Motivation von uns Wissenschaftlern bzw. Mathematikern; die Perspektive der Nachfrager wird uns im Zusammenhang mit den Schwierigkeiten im nachfolgenden Abschnitt beschäftigen.

Sehr schnell fällt auf, dass auch innerhalb der Anbieter noch weitere Unterscheidungen sinnvoll sind. Denn erstens bildet auch die (vergleichsweise kleine) mathematische Gemeinschaft keine völlig homogene Gruppe, und zweitens agiert jeder einzelne Mathematiker in verschiedenen Rollen, aus denen sich unterschiedliche Motive ergeben. Drei Rollen möchte ich hervorheben: Erstens haben wir jeweils individuelle Vorlieben, Spezialgebiete und Beweggründe, Mathematik zu betreiben. Als Vertreter unserer Wissenschaftsdisziplin wünschen wir uns zweitens materielle Unterstützung und Förderung durch Institutionen wie Schulen, Universitäten und sonstige Einrichtungen des Bildungs- und Wissenschaftssystems und somit durch die Gesamtheit der Steuerzahler. Als Mitglied der Gesellschaft wünschen wir uns drittens, dass die Mathematik ihr volles Potenzial entfaltet, am Wohlergehen möglichst aller mitzuwirken.

Wir dürfen keine dieser drei Rollen geringschätzen. Am einfachsten zu begründen ist das in Hinblick auf die gesamte Gesellschaft. Orientiert man sich an einem kategorischen Imperativ, so ergibt sich der Auftrag zum Bemühen um allgemeines Wohlergehen unmittelbar. In unserem Zusammenhang stellt sich die Frage, inwieweit auch Mathematik dazu beitragen kann. Eine Antwort – wenn auch bei Weitem nicht die einzige – liegt auf der Hand: Für die meisten technischen Errungenschaften, die unseren Alltag im Vergleich zu jenem früherer Generationen unermesslich erleichtern, ist Mathematik in der einen oder anderen Form unverzichtbare Grundlage.

Ist das schon ein hinreichender Grund, Mathematik zu popularisieren? Immerhin müssen wir auf folgenden Einwand gefasst sein: In unzähligen technischen Errungenschaften, die die meisten von uns ständig nutzen, spielen die unterschiedlichsten wissenschaftlichen Erkenntnisse eine Rolle. Sie alle sich anzueignen, wäre eine Aufgabe, die den Einzelnen maßlos überforderte. Er müsste sein ganzes Leben der Weiterbildung unterordnen und ständig populärwissenschaftliche Foren für die unterschiedlichsten Disziplinen aufsuchen.

Wenn also der Möglichkeit, umfassend und detailreich zu vermitteln, *wie* Mathematik in unserer Welt wirkt, Grenzen gesetzt sind, so sollten wir doch die Botschaft vermitteln, *dass* dies so ist und dass deshalb Mathematik auch aus einer ganzheitlichen Perspektive Unterstützung verdient. Damit das gelingt, genügt es aber schwerlich, einen Stehsatz mit dieser Botschaft unablässig zu variieren. Wir müssen die Adressaten unserer Botschaft auch emotional erreichen, das heißt in unserem Fall: tragfähige Assoziationen erzeugen zwischen Mathematik und Gedanken, Ideen, Bildern, Erfahrungen, etc., die in der einen oder anderen Weise als angenehm erlebt werden.

Gelingt das, so werden jene Menschen, die als Besucher den Weg in eine Institution wie das TUForMath auf sich nehmen, unsere Botschaft, dass Mathematik in-

stitutionelle Unterstützung braucht, auch weitertragen. Somit agieren wir gleichzeitig als Vertreter unserer Wissenschaft und nicht zuletzt in eigener Sache. Es gilt dabei, glaubhaft zu machen, dass wir dazu legitimiert, ja sogar verpflichtet sind. Denn wer, wenn nicht wir, die Mathematiker selbst, soll unsere Botschaft kompetent formulieren? Um sich das Besondere an unserer Situation besonders deutlich vor Augen zu führen, vergleiche man sie beispielsweise mit der von Ärzten: Es braucht keinen Arzt, um zu erklären, warum Heilkunst segensreich ist. Vermutlich braucht es aber Mathematiker oder wenigstens mathematisch Gebildete, um plausibel zu machen, warum beispielsweise ein grundätzliches Verständnis der Infinitesimalrechnung nicht nur bei Mathematikprüfungen nützlich ist, sondern unser Weltverständnis wesentlich bereichert. Wir sollten uns dabei nicht damit zufriedengeben, die Aufmerksamkeit dieser Menschen für die Dauer einer kurzweiligen Abendveranstaltung an uns zu binden. Darüber hinaus sollten wir unsere Besucher mit Argumenten ausstatten, mit denen sie – in ihrer Rolle als Staatsbürger – selbst Überzeugungsarbeit leisten können bei anderen Menschen, die den Weg zur Mathematik noch nicht gefunden haben. Mit anderen Worten: Wir wollen nicht nur gut unterhalten (das anzustreben, sind wir zweifelsohne gut beraten!), sondern auch aufklären im besten Kantschen Sinne.[1]

Wollen wir unseren Besuchern eine intrinsische Motivation mitgeben, ihre Aufgeklärtheit nicht nur wissend mit sich zu tragen, sondern unsere Botschaft zu verbreiten, so empfiehlt es sich, vor allem rigide akademische Trockenheit zu vermeiden. Das ist leichter gesagt als getan. Denn was dem Mathematiker, der sich tagtäglich damit auseinandersetzt, lebendig, bunt und faszinierend erscheint, wirkt für den Laien, wenn es ihm in der für ihn ungewohnten Terminologie und Formelsprache der Mathematik entgegentritt, intransparent, trocken und leblos. Da helfen auch keine Beteuerungen, wie nützlich unsere geheimnisvollen Objekte für Anwendungen seien. Um über diese zugegebenermaßen recht schlichten Befunde hinauszukommen, ist es an der Zeit, genauer über die Schwierigkeiten der Popularisierung von Mathematik nachzudenken.

3 Schwierigkeiten und Tücken

Bei der Analyse von Chancen und Schwierigkeiten bei der Popularisierung von Mathematik bieten sich zwei Vergleiche an: der mit der Vermittlung von Mathematik in der Schule und der mit der (nicht auf die Schule beschränkten) Popularisierung anderer Fächer und Wissensinhalte. Der Vergleich mit der Schule eröffnet durchaus Chancen auf Strategien, denen wir uns etwas später zuwenden werden.

[1] Zur aufklärerischen Rolle der Mathematik darf ich auch auf meinen Text *Mathematik als zentraler Teil des Projektes Aufklärung auf breiter Front* verweisen, erschienen in: *Mathematik und Gesellschaft. Historische, philosophische und didaktische Perspektiven.* Herausgeber: G. Nickel, M. Helmerich, R. Krömer, K. Lengnink, M. Rathgeb. Springer Spektrum, 2018.

Der Vergleich mit anderen Disziplinen jedoch macht die speziell mit der Mathematik verknüpften Schwierigkeiten deutlich, mit denen wir uns nun beschäftigen wollen.

Warum also ist Popularisierung gerade bei Mathematik so schwierig? Der Vergleich mit dem Beruf des Arztes weiter oben führt uns die besonderen Herausforderungen bereits deutlich vor Augen. Die Vermittlung des Wertes von Mathematik ist offenbar deshalb besonders anspruchsvoll, weil mathematische Phänomene nicht einfach und unmittelbar vor unseren Sinnen auftauchen. Meist setzt nicht erst die Lösung, sondern schon die Wahrnehmung eines mathematischen Problems ein Verständnis begrifflicher Zusammenhänge voraus, das nicht ohne Bereitschaft und Fähigkeit zur Abstraktion möglich ist. Flache Bespaßung mit Mathematik findet deshalb schnell ihre Grenzen. Das spiegelt sich auch in dem Umstand wider, dass sich im Vergleich mit anderen Fachdidaktiken die mathematische mittlerweile zu einer sehr umfangreichen und differenzierten eigenständigen Disziplin entwickelt hat. Unter wissenschaftstheoretischen Gesichtspunkten lässt sich auch sagen, was der international bekannte Zahlentheoretiker Don Zagier ins Zentrum seines Eröffnungsvortrags des math.space am 14. Jänner 2003 gestellt hat und was auch im Vortrag von Karl Sigmund anlässlich der Eröffnung des TUForMath am 11. Juni 2018 als Essenz deutlich wurde: Mathematik stellt im Spektrum sämtlicher Wissenschaften ein Extrem dar, weil sie die allgemeinste und damit notwendig auch die abstrakteste, von Begriffsbildungen am stärksten abhängige Wissenschaft ist.

Zur Illustration der Schwierigkeit, die sich daraus ergibt, will ich auf folgende Erfahrung aufmerksam machen, die – wie ich vermute – jeder Mathematiker schon des Öfteren gemacht hat: Denkt man intensiv über ein mathematisches Problem nach und findet man endlich eine Lösung, so ordnet sich in der Vorstellung alles neu und fügt sich zu wunderschönen, klaren und oft überraschend einfach anmutenden Bildern. Versucht man, diese Bilder in ein Theorem samt lückenlosem, kein Detail übersehendem Beweis zu übersetzen und zu Papier zu bringen, so werden diese klaren Bilder sogleich überwuchert von Formelkram und der das Gesamtbild einengenden Notwendigkeit, alles in eine folgerichtige, methodisch korrekte lineare Argumentation zu pressen. Das ungetrübte ästhetische Erlebnis ist dahin, und der Leser muss Klarheit und Schönheit der Essenz für sich erst wieder mühsam aus dem Niedergeschriebenen rekonstruieren.

Dieses Phänomen ist eine der wesentlichen Schwierigkeiten bei jeder Form von Vermittlung von Mathematik. Mehr als im Mathematikunterricht an Schule oder Universität, wo die Beherrschung des Formalismus Teil des Lehrziels ist und daher nicht einfach umgangen werden kann, plädiere ich bei der Popularisierung von Mathematik abseits von Bildungsinstitutionen im engeren Sinn für mehr Mut zur Metaphorik. Denn es kommt nicht so sehr auf die Korrektheit im technischen Detail an, sondern auf die Stimmigkeit und Überzeugungskraft im Großen, d.h. auf die Wirkungskraft der Botschaft, dass es ein innerer Reichtum ist, von dem Ma-

thematik handelt. Es mag ein Reichtum sein, den man sich in seinen Einzelheiten erst individuell erarbeiten muss; in jedem Fall ist es aber einer, dessen Pflege sich lohnt.

Doch bergen solche Spekulationen die Gefahr, sich in einem fiktiven Bereich zu verlieren, fernab jeglicher realen Möglichkeit, Mathematik zu vermitteln und zu popularisieren. Es ist höchste Zeit, auch die Erwartungshaltung jener ins Auge zu fassen, die wir mit unseren Popularisierungsambitionen erreichen wollen, nämlich die potenziellen Nachfrager – um auf den Vergleich mit einem Markt zurückzukommen.

Ich kenne keine systematischen empirischen Forschungen zur Erwartungshaltung von Nichtmathematikern gegenüber Mathematik. Meine Einschätzung beruht deshalb auf meinen persönlichen Erfahrungen bei Gesprächen mit mehr oder weniger interessierten Laien. Neben recht undifferenzierten Bekenntnissen wie "In der Schule war ich immer schlecht in Mathematik, und ich habe sie gehasst" hört man auch konstruktive Interessensbekundungen. Die meisten davon sind Varianten von zwei Fragen:

1. Auf den Einzelnen bezogen: Welchen praktischen Nutzen hat die Mathematik für mein Leben?

2. Auf die institutionalisierte Wissenschaft bezogen: Was kann man in der Mathematik noch forschen? Ist nicht ohnehin schon alles bekannt?

So sehr jeder Mathematiker geneigt sein mag, spontan mit zahlreichen Antworten zu replizieren, sind doch auch – vom Frager vermutlich nicht beabsichtigte – Tücken zu beachten, die mit diesen beiden Fragen verknüpft sind.

Zur ersten Frage: Ist sie in dem Sinn gemeint, dass unsere alltäglichen Verrichtungen dann leichter von der Hand gehen, wenn wir höhere Mathematik beherrschen, so sollten wir uns eingestehen: Die meisten Menschen haben sich ihr Leben so eingerichtet, dass sie sich (wenigstens subjektiv) auch ohne besondere mathematische Kenntnisse recht gut zurechtfinden. Nur in seltenen Situationen empfinden sie einen Mangel an mathematischer Bildung bewusst als Nachteil. Hinsichtlich eines zu eng verstandenen praktischen Nutzens sollten wir (uns) also nicht zu viel versprechen. Weitet man Frage 1 hingegen vom persönlichen Einsatz mathematischen Wissens aus auf Mathematik, die in unseren Geräten des täglichen Gebrauchs steckt, so scheint das hervorragend zu korrespondieren mit dem zivilisatorischen und vor allem technologischen Nutzen der Mathematik, von dem bereits weiter oben die Rede war. Wie dort bereits festgestellt wurde, sind aber Zweifel angebracht, ob ein Interesse an den mathematischen Hintergründen lange lebendig bleibt, wenn die Zusammenhänge zu komplex werden, als dass ein Verständnis im Detail ohne beträchtliche Mühe erworben werden kann. Bei zu

ungestümer Versenkung in technische Einzelheiten besteht die Gefahr, dass statt Erleuchtung Frustration erzeugt wird, die den überforderten Laien zum Resümee verleitet: “Mathematik ist also doch nichts für mich.” Auch wenn er anzuerkennen bereit ist, dass es ein paar Spezialisten geben sollte, die sich mit solchem Zeug berufsmäßig beschäftigen – aus eigenem Antrieb motivierte Botschafter der Mathematik werden wir so nicht gewinnen. Wir sollten uns fragen, ob da nicht mehr herauszuholen wäre. Bevor wir dem nachgehen, möchte ich aber auch auf die zweite der beiden oben formulierten Fragen, wie sie von interessierten mathematischen Laien sehr oft gestellt werden, eingehen.

Wahrscheinlich ist jeder Mathematiker schon häufig der Einschätzung begegnet, in der Mathematik sei alles schon erforscht und womöglich sogar schon durch das abgedeckt, was üblicherweise in der Schule unterrichtet wird. Den diesbezüglich markantesten Eindruck erhielt ich, als ich mich während meiner eigenen Studienzeit einmal mit einem BWL-Studenten über unsere Studien unterhielt. Er erzählte, dass es in seinem Studium auch eine Mathematikvorlesung gebe. Auf meine Frage, was denn da alles vorkomme, hielt er inne, dachte kurz nach und kam sehr schnell zum Schluss: “Eigentlich eh alles!” Er hatte anscheinend mit dem verglichen, was ihm noch aus seiner Schulzeit in Erinnerung war. Um dieser geradezu rührenden Beschränktheit des Horizonts zu begegnen, ist man als Mathematiker versucht, auf schwierige – gelöste oder ungelöste – mathematische Probleme zu verweisen, die sich leicht formulieren lassen. Sehr oft stammen sie aus der Zahlentheorie; der Fermatsche Satz und seine 350-jährige Geschichte ist ein Musterbeispiel. Doch sehe ich eine Gefahr darin, dass der Laie zwar verstehen kann, worum es bei der Frage nach der Lösbarkeit der diophantischen Gleichung $a^n + b^n = c^n$ für $n \geq 3$ vordergründig geht, dass er jedoch kaum verstehen wird können, was an der negativen Beantwortung dieser Frage durch Andrew Wiles und Richard Taylor im Jahr 1995 denn nun so großartig sein soll. Um das einem Laien (oder auch einem Mathematiker, der wenig mit Zahlentheorie zu tun hat) zu vermitteln, müsste man viel weiter ausholen. Auch bei der zweiten der oben formulierten Fragen ergibt sich nach kurzer Reflexion also das Bedürfnis nach Befriedigenderem, als spontane Antworten es nahelegen mögen.

4 Mögliche Strategien

Wenn ich mich im Folgenden bemühe, konstruktive Vorschläge zu formulieren, auf welche Weise wir uns den mittlerweile recht ausführlich diskutierten Schwierigkeiten bei der Vermittlung von Mathematik stellen könnten, so wäre es natürlich wünschenswert, allfällige Ergebnisse auf den Schulunterricht anzuwenden. Bis zu einem gewissen Grad ist das sicher auch möglich. Ein wesentlicher Unterschied besteht allerdings darin, dass im Schulunterricht über ein aufgeklärtes und emotional positiv besetztes Verhältnis zur Mathematik hinaus auch viel kon-

kretere, inhaltlich spezifizierte Lehrziele erreicht werden sollen. Das bindet den Schulunterricht, während wir in Hinblick auf allgemeine Popularisierung über Freiheiten verfügen, die wir nutzen dürfen, wo immer es Früchte trägt.

Dabei erinnere ich zunächst an unsere drei Rollen: erstens als Personen mit individuellen Vorlieben und Sichtweisen auch die Mathematik selbst betreffend, zweitens als Vertreter unserer Disziplin und der mit ihr verknüpften Institutionen, und drittens als Staatsbürger, die an einer offenen und aufgeklärten Gesellschaft interessiert sind. Es ist erhellend, sich die unterschiedlichen Motivationslagen, die mit diesen drei Rollen verbunden sind, deutlich bewusst zu machen und sie gleichzeitig füreinander zu nutzen. Denn unsere persönliche Begeisterung für Mathematik macht uns in mehrfacher Hinsicht glaubwürdiger: wenn wir das Schöne an der Mathematik verkünden und dass sie das Leben des Einzelnen bereichert; wenn wir das aufklärerische Potenzial unserer Wissenschaft (von dem die Gesellschaft insgesamt profitiert) betonen; und wenn wir daraus die Notwendigkeit ableiten, dass Mathematik im Bildungs- und Wissenschaftssystem mit ausreichenden öffentlichen Mitteln gefördert werde.

Warum also nicht die eigene Faszination möglichst authentisch zum Ausdruck bringen? Die uns Mathematikern wohlvertraute Symbolsprache ist dabei oft nur eine Verkleidung, in der die eigentlichen Inhalte die Bühne der Kommunikation unter Fachleuten betreten. Wir haben uns daran gewöhnt, unsere Protagonisten an dieser Verkleidung sofort zu erkennen. Wer sie aber noch nicht kennt, möchte zuerst sie selbst erfassen und nicht ihre Verkleidung. Doch wie weit ist das überhaupt möglich, wo doch erst die so weit entwickelte Formelsprache der Mathematik die Kommunikation über komplizierte mathematische Sachverhalte ermöglicht? Hier gilt es abzuwägen, was es beim Versuch einer direkteren Kommunikation an Genauigkeit zu verlieren und was es an ganzheitlichem Verständnis zu gewinnen gibt. Eine pauschale Antwort ist nicht zu erwarten. Meiner persönlichen Einschätzung nach liegen aber beträchtliche Potenziale brach, wo eine Emanzipation mathematischer Ideen vom Ballast des Formalismus möglich wäre und damit Mathematik auch gegenüber Laien umfassender als bisher vermittelt werden könnte.

Selbst wenn von einem bestimmten mathematischen Kontext mit realistischem Aufwand kein exaktes und vollständiges Bild des gesamten Sachverhalts gezeichnet werden kann, so gibt es meist wertvolle Alternativen. Entscheidend scheint mir ein großes und vielfältiges Repertoire an Bezügen zu allgemein Vertrautem, das sich weder auf die Welt des technologisch Nützlichen noch auf jene des abstrakt Mathematischen beschränkt. Ein riesiges Reich menschlichen Bewusstseins und menschlicher Erfahrungen, auf das wir uns beziehen können, steht uns offen. An solchen Bezügen ist die Mathematik unermesslich reicher, als die meisten Laien (gar manche Fachmathematiker?) sich in ihrer Schulweisheit träumen lassen.

Um wieder konkreter zu werden, erinnere ich an die Überlegungen zu den Fragen 1 und 2 weiter oben. Dabei fällt eine Gemeinsamkeit der beobachteten Probleme auf: In beiden Fällen wird dem Laien der Glaube an eine Autorität und deren Be-

hauptungen abverlangt. Bei Frage 1 ist es die Behauptung, Mathematik stecke in dieser oder jener Technologie. Bei Frage 2 ist es die Behauptung, die mathematische Strukturtheorie (z.B. hinter einer diophantischen Gleichung) bedeute einen großartigen Erkenntnisfortschritt. Aber gerade Glaube sollte es ja nicht sein, was die Einzigartigkeit und Sicherheit der mathematischen Methode ausmacht, sondern Verständnis durch eigenständigen Vernunftgebrauch. (Ich erinnere nochmals an Kant und an seinen Begriff von Aufklärung.) Erst die berauschende Wirkung eines auf diesem Wege subjektiv und existenziell erfahrenen "Heureka" wird den einzelnen Menschen für das empfänglich machen, was wir vermitteln wollen.

Auch wenn der interessierte und wohlmeinende, vielleicht aber naive mathematische Laie mit Fragen 1 und 2 an uns herantritt, so stehen wir also vor der Aufgabe, ihn zwar dort "abzuholen", wo er die Mathematik vermutet. Die große Herausforderung an uns geht aber darüber hinaus und besteht darin, ihn auch wo "hinzuführen". Mithilfe bescheidener erster Orientierungshilfen, die zu geben unsere erste Aufgabe ist, soll er sich bereits möglichst aus eigenem Antrieb dorthin gezogen fühlen. Zu diesem Zweck müssen wir in ihm das Bedürfnis nähren, sich in eine Richtung zu bewegen, auf die der Blick ihm bislang verschlossen war. Wie kann das gelingen, wenn für den Laien das technische Detail zu kompliziert erscheint und wenn er außerdem die Relevanz großer mathematischer Resultate nicht nachvollziehen kann?

So unspezifisch oder gar pathetisch es auf den ersten Blick auch klingen mag – meines Erachtens geht es darum, der Mathematik, die man vermitteln will, einen *Sinn* zu geben. Wohlgemerkt: Dabei meine ich mit "Sinn" weit mehr als einen Zweck – so wie ein Kunstwerk für uns Sinn haben kann, ohne einem praktischen Zweck dienen zu müssen. Wenn wir ein Kunstwerk nicht nur als schön empfinden, sondern auch "verstehen", dann meinen wir damit vor allem, dass es eingebettet ist in Zusammenhänge, die für uns vertraut oder interessant sind, unsere Aufmerksamkeit erregen, kurz: weil es unsere conditio humana betrifft. Natürlich dürfen dabei auch "Zwecke" im Hinblick auf ein alltägliches, praktisches Anliegen eine Rolle spielen. Die Netze von Assoziationen und gedanklichen Querverbindungen, innerhalb derer wir den gesuchten Sinn suchen, sind aber viel weiter gespannt.

Hier lässt sich ein bemerkenswerter Unterschied in den Traditionen von Mathematik und Naturwissenschaft einerseits und Geisteswissenschaft andererseits ausmachen. Ich halte ihn für eine wesentliche Ursache jener schwer überbrückbaren Kluft, die Hans Magnus Enzensberger in seiner "Außenansicht" unter dem Titel "Zugbrücke außer Betrieb: Die Mathematik im Jenseits der Kultur" so treffend beschreibt.[2] Uns Mathematikern mutet es oft seltsam an, wenn wir von den vielen "Narrativen" und "großen Erzählungen" hören oder lesen, die auf der uns gegenüberliegenden Seite dieser Kluft besungen werden oder deren Verschwinden dort

[2] Hans Magnus Enzensberger. *Drawbridge Up: Mathematics – A Cultural Anathema / Zugbrücke außer Betrieb: Die Mathematik im Jenseits der Kultur* (dt., engl.) Natick, Mass., Peters, 1999.

beklagt wird. Sie erscheinen uns willkürlich im Vergleich mit den Denknotwendigkeiten in unserer eigenen Wissenschaft. Gleichzeitig vergessen wir dabei aber allzu häufig, unsere eigenen "großen Erzählungen" explizit zu machen, die wir eigentlich für den entscheidenden Hintergrund halten, vor dem wir mathematische Errungenschaften erst als bedeutsam wahrnehmen und die in großem Maßstab auch unsere Disziplin vorantreiben.

Um das mit Beispielen zu illustrieren, erwähne ich: die wissenschaftliche Revolution, die um 1600 mit der Mathematisierung der Naturbeschreibung durch Galilei einsetzte und über die Algebraisierung der Geometrie mittels kartesischer Koordinaten durch Descartes auf einen ersten Höhepunkt bei Newton zusteuerte; den erkenntnistheoretischen Einschnitt, den die Entdeckung nichteuklidischer Geometrien bedeutete; die Galoistheorie, die nicht nur den Gruppenbegriff gebar, sondern strukturtheoretische Abstraktion als wesentliche Energiequelle für die gesamte Mathematik entfesselte; die Exaktifizierung des Grenzwert- und Zahlbegriffs, wodurch eine Vision wie das Hilbertsche Programm erst denkbar wurde; oder Gödels Vollständigkeitssatz, mit dem er die logisch-deduktive Methode adelte und somit das moderne, methodisch geprägte Selbstverständnis der Mathematik entscheidend stützte; und schließlich sein Unvollständigkeitssatz als Kontrapunkt, mit dem er schon kurz darauf die Grenzen des Hilbertschen Traums aufzeigte.

Jedem Mathematiker werden, je nach persönlichen Vorlieben, weitere "große Erzählungen" dieser Art einfallen. Neben dem Reiz ganz konkreter mathematischer Überlegungen, die anscheinend aber nicht allen Menschen gleichermaßen zugänglich sind, sind es diese Erzählungen, deretwegen wir unser Fach nicht nur lieben, sondern für einen wesentlichen Teil menschlicher Zivilisation und, wegen der immensen erkenntnistheoretischen Relevanz, der conditio humana schlechthin halten.

Dass dieser hohe Rang unserer Wissenschaft immer noch nicht zum anerkannten Allgemeingut geworden ist, schmerzt uns. Dabei hat sich die Lage während der letzten Jahrzehnte zweifellos eher verbessert. In Österreich hat daran sicher Rudolf Taschners ehemaliger math.space einen wesentlichen Anteil. Ich wage die These, dass sein Erfolg vor allem in der großartigen Vermittlung besagter "großer Erzählungen" der Mathematik begründet war. Hierin sollte sich auch das TUForMath ein Vorbild nehmen, damit die Mathematik auf noch größere, ihrer tatsächlichen Bedeutung angemessene Anerkennung hoffen darf. In der Terminologie eines früheren Artikels[3] von mir lässt sich auch sagen: Bleibt der Mathematikunterricht in der Schule mit seinen gedrillten Formalismen leider oft auf der Ebene der mikroskopischen Betrachtungsweise hängen und erweist sich die den Mathematiker besonders interessierende mesoskopische Ebene häufig als zu anspruchsvoll, so hat Popularisierung die Freiheit, auf die makroskopische Ebene auszuweichen.

[3] *Der Organismus der Mathematik; mikro-, makro- und mesoskopisch betrachtet*. Erschienen in: *Mathematik verstehen – philosophische und didaktische Perspektiven.* Herausgeber: Markus Helmerich, Katja Lengnink, Gregor Nickel, Martin Rathgeb. Vieweg + Teubner Verlag, 2011.

Gleichfalls großes Potenzial an breiterer Anerkennung in der Öffentlichkeit liegt im Facettenreichtum der Mathematik, der sich seinerseits unter völlig unterschiedlichen Gesichtspunkten, also wiederum facettenreich zeigt. Unter diesen mannigfaltigen Gesichtspunkten ist die extreme und permanent voranschreitende innere Auffächerung der Mathematik in Teilgebiete unterschiedlichen Charakters nur einer, wenn auch ein ziemlich offensichtlicher. Ein weiterer, sehr überzeugender ergibt sich aus dem Lehrplan der AHS-Oberstufe, in dessen allgemeinem Teil sechs Aspekte der Mathematik als Bildungsziele unterschieden werden: der schöpferisch-kreative, der sprachliche, der erkenntnistheoretische, der pragmatisch-anwendungsorientierte, der autonome und der kulturell-historische. Ohne hier auf jeden von ihnen näher einzugehen, ist es kaum gewagt, zu vermuten, dass sich die Vorstellung von Mathematik in der breiten Öffentlichkeit weitgehend auf sehr bescheidene Teile des pragmatisch-anwendungsorientierten Aspekts beschränkt. Umso größer ist das Betätigungsfeld, das Initiativen wie dem TUForMath offensteht. Auch die Frage nach der Einordnung der Mathematik im Spannungsfeld zwischen Natur- und Geisteswissenschaften, Philosophie, Kunst und Kultur führt uns sofort vor Augen: Die Mathematik hat von alldem etwas, weshalb man ihr gleichzeitig mit keiner einzelnen dieser Zuordnungen allein gerecht wird. Entsprechend viel gibt es über ihr (abermals facettenreiches) Verhältnis zu den anderen Wissenschaften zu sagen. Dem entspricht darüber hinaus eine Vielfalt von möglichen subjektiven Motivationen, aus denen heraus Mathematiker jeweils individuell ihre Wissenschaft betreiben und welche Beziehung des Einzelnen zur Welt sie damit in den Vordergrund stellen. Mit Mathematik kann man nämlich die Welt sowohl besser verstehen (wie in den Naturwissenschaften oder der Nationalökonomie), gestalten (wie in Technik oder wirtschaftlichem Handeln) als auch reflektieren (ähnlich Philosophie und Kunst). Für mathematische Laien besonders überraschend dürften die Antagonismen, Gegensätze, ja scheinbaren (!) Widersprüche innerhalb der Mathematik sein. Diese haben darin nicht nur Platz, sondern stellen sogar essenzielle Elemente dar, aus denen heraus die Mathematik erst ihre große Energie bezieht. Zur Illustration ein paar typische Beispiele solcher Gegensatzpaare: methodische Strenge – inhaltliche Freiheit, formal – anschaulich, abstrakt – konkret, allgemein – exemplarisch, diskret – kontinuierlich, logisch – intuitiv, quantitativ – qualitativ. Schließlich ist dieser Reichtum der Mathematik nicht zuletzt Ergebnis einer jahrtausendelangen historischen Entwicklung, in der die Mathematik zahlreiche Evolutionsschübe erfahren hat, die jeweils neue Gesichtspunkte in den Vordergrund gerückt haben, ohne dabei jedoch die bis dato gesammelten Inhalte in ihrer Substanz entsorgen zu müssen. Denn in der Mathematik wird nicht (im Popperschen Sinne) falsifiziert, wie in den empirischen Wissenschaften, sondern permanent vertieft und verbunden. Altvertrautes erstrahlt in neuen Farben, wobei gleichzeitig oft völlig Neuartiges sichtbar wird.

Dieser Exkurs sollte zeigen, wie groß der Spielraum ist, den die Popularisierung von Mathematik nutzen kann. Will man dem Laien mit einem abendlichen Vor-

trag sowohl Wesentliches als auch Kurzweiliges über Mathematik vermitteln, so ist es also sicher nicht notwendig, ihm die Mühen technischer Details zuzumuten und zu später Stunde außergewöhnliche Konzentration abzuverlangen (wie sie in der mathematischen Forschung natürlich unerlässlich ist). Sympathisierende Anteilnahme an den "großen mathematischen Erzählungen" erzeugt man eher, indem man an vielfältige geläufige Erfahrungen anschließt. Die Wahrnehmung von Sinnzusammenhängen ist ein menschliches Urbedürfnis, das jeden, der die Lust daran einmal erfahren hat, auch für die weitere Vertiefung bisheriger Einsichten empfänglich macht. Wer als Mathematiker im Innersten empfindet, dass mathematische Sinnzusammenhänge im Vergleich zu vielen anderen Disziplinen sogar viel zwingender und weniger willkürlich sind, wird seine Botschaft nur umso überzeugender vermitteln können. Nicht jeder wissenschaftliche Inhalt kann auf ein allgemeinverständliches Niveau "heruntergebrochen" werden, aber zu fast allem gibt es einen lohnenden, weil hinreichend umfassend gewählten Sinnzusammenhang, der sehr wohl vermittelt und in dem auch Schwerverständliches in erhellender Weise eingeordnet werden kann.

5 Das TU Forum Mathematik

Das Auslaufen von Rudolf Taschners math.space mit Jahreswechsel 2017/18 wurde allgemein mit großem Bedauern registriert, nicht zuletzt von uns, der mathematischen Gemeinschaft. Denn der Erfolg, mit dem im math.space die oben diskutierten Schwierigkeiten der Popularisierung von Mathematik überwunden wurden, suchte seinesgleichen. Insbesondere an der Fakultät für Mathematik und Geoinformation der TU Wien wurde die Frage virulent, ob es denn keine Form der Fortsetzung gebe. Auf Initiative der Rektorin Sabine Seidler und des Dekans Michael Drmota wurde eine Möglichkeit gefunden, mit dem TUForMath ein neues Projekt auf die Beine zu stellen, das die durch den math.space begründete Tradition fortsetzt und sich in ähnlicher Weise die Popularisierung von Mathematik zum Ziel setzt.

Einige Rahmenbedingungen haben sich im Vergleich zum math.space geändert. Als Raum wird nicht mehr jener im MuseumsQuartier zur Verfügung stehen, sondern ein von der Wiedner Hauptstraße ebenerdig zugänglicher im Freihaus, jenem Gebäude der TU Wien, in dem auch unsere Fakultät angesiedelt ist. Damit wird der Bezug der Mathematik zur Technik deutlicher sichtbar, als es beim math.space der Fall war. Das soll aber keineswegs bedeuten, dass die kulturellen Aspekte, die im math.space schon durch die Lokalität zum Ausdruck kamen, in Zukunft vernachlässigt werden. Weiters ist das TUForMath durch die TU Wien institutionell verankert und wird von einem Team rund um den Dekan der Fakultät für Mathematik und Geoinformation geleitet. Durch die große Zahl der an unserer Universität tätigen Lehrenden und Studierenden, ergänzt durch Gastvortragende, ist

es möglich, eine thematische wie auch stilistische Vielfalt anzustreben und damit den oben betonten Facettenreichtum der Mathematik sehr breit widerzuspiegeln.

Unser besonderer Dank gilt Karl Sigmund von der Universität Wien, der am 11. Juni 2018 mit seinem eindrucksvollen Vortrag im Festsaal der TU anlässlich der offiziellen Eröffnung von TUForMath allgemeine Begeisterung erntete und die Botschaft verkörperte, dass die Mathematik keine institutionellen Grenzen kennt. Damit bescherte er der als Dauereinrichtung geplanten Serie von Vorträgen für eine interessierte allgemeine Öffentlichkeit einen Einstand, wie er gelungener nicht hätte sein können. Im Wintersemester 2018/19 soll das regelmäßige Vortragsprogramm beginnen, zunächst mit sechs allgemeinverständlichen Vorträgen im Abstand von zumeist zwei Wochen, jeweils an einem Donnerstag ab 18 Uhr. Programme für Schulklassen bilden die zweite Veranstaltungsserie ab Herbst 2018. Sechs hervorragende fortgeschrittene Studierende der Mathematik an der TU Wien werden bis Herbst zunächst zwei Programme entwickeln, eines für die 5. und 6., eines für die 7. und 8. Schulstufe. Mittelfristig ist an eine Ausweitung auch für andere Altersstufen gedacht, insbesondere für Volksschulklassen, außerdem an Diskussionsveranstaltungen zu aktuellen Themen. Eine zusätzliche inhaltliche Bereicherung erhofft sich TUForMath auch von Kooperationen mit Institutionen wie beispielsweise anderen Universitäten, Schulen und Schulverantwortlichen oder Museen, woraus sich Themenschwerpunkte ergeben können, die mehrere Einzelveranstaltungen verbinden.

Abschließend sei noch auf die Möglichkeit hingewiesen, Rückmeldungen zu Veranstaltungen des TUForMath zu geben und auch Wünsche zu äußern. Zu diesem Zweck ist auf der Homepage

`https://tuformath.at`

die sogenannte Wunschbox eingerichtet. Außerdem kann man dort den Newsletter abonnieren und Informationen finden über Aktuelles, und das Programm, so weit es schon feststeht, und über das Team. Dieses besteht zurzeit aus zwölf Personen: den sechs Studierenden, die das Schülerprogramm gestalten, und jenem sechsköpfigen Gründungsteam, welches das Projekt während des Frühjahrs 2018 geplant hat und das es nun ins erste Studienjahr mit regulärem Betrieb führen wird.

Das TU Forum Mathematik dankt seinen zahlreichen wohlwollenden Unterstützern, die mit Rat und Tat geholfen haben und immer noch helfen, das neue Projekt zum Leben zu erwecken. An alle Interessierten richtet sich die Einladung:

Willkommen im TU Forum Mathematik!

Adresse des Autors:
Reinhard Winkler
TU Wien

Wiedner Hauptstr. 8-10
A-1040 Wien
email reinhard.winkler@tuwien.ac.at

Buchbesprechungen

L. Guth: Polynomial Methods in Combinatorics (A. WINTERHOF) 59
T. A. Ivey, J. M. Landsberg: Cartan for Beginners (R. DONNINGER) . . . 60
G. Leoni: A First Course in Sobolev Spaces (R. DONNINGER) 60
J. Justesen, T. Høholdt: A Course In Error-Correcting Codes (A. WINTERHOF) 61
R. C. Gunning: An Introduction to Analysis (R. DONNINGER) 61
M. Eie, S. Chang: A First Course in Linear Algebra (R. DONNINGER) . 62

L. Guth: Polynomial Methods in Combinatorics. (University Lecture Series, Vol. 64.) American Mathematical Society, Providence (USA), 2016, 273 S. ISBN 978-1-4704-2890-7 P/b $ 48.

In recent years several important problems in combinatorial geometry have been solved via a connection with polynomials and algebraic geometry. An emerging collection of such techniques is now called the polynomial method. This book is not only an excellent introduction to this area but also explains some recent progress.

After a short introduction the book presents Dvir's short and elegant proof of the finite field Kakeya problem, which had been considered very difficult before. The author also discusses several problems in incidence geometry related to the distinct distance problem. The book also describes connections between different fields of mathematics. For example, Dvir's proof was motivated by coding theory. Connections to Fourier analysis, number theory and differential geometry are also discussed.

This is a valuable book for both students and researchers who are interested in this very active research area.

A. Winterhof (Linz)

T. A. Ivey, J. M. Landsberg: Cartan for Beginners. Differential Geometry via Moving Frames and Exterior Differential Systems, Second Edition. (Graduate Studies in Mathematics, Vol. 175.) American Mathematical Society, Providence (USA), 2016, 455 S. ISBN 978-1-4704-0986-9 H/b $ 89.

Cartan's approach to differential geometry via moving frames and exterior calculus was crucial for the theoretical development of the field. In addition to its conceptual significance, the Cartan formalism provides efficient methods for computation which makes it important in applications such as general relativity. However, in traditional introductions to differential geometry Cartan's viewpoint is often just mentioned in passing, and modern treatments of the subject are rare. The book under review sets out to fill this gap. It provides a very readable introduction to Cartan's approach which should be accessible to readers with some background in standard differential geometry. The book starts with a number of motivating examples and then moves on to the geometry of submanifolds of Euclidean space and Riemannian geometry. Later chapters cover more advanced topics on projective, Kähler, and conformal geometry. A recurring theme is the application to partial differential equations which makes the book also interesting for experts in PDEs.

R. Donninger (Wien)

G. Leoni: A First Course in Sobolev Spaces. Second Edition. (Graduate Studies in Mathematics, Vol. 181.) American Mathematical Society, Providence (USA), 2017, 734 S. ISBN 978-1-4704-2921-8 H/b $ 94.

This comprehensive book of more than 700 pages provides a somewhat unusual introduction to Sobolev spaces. The approach is primarily measure-theoretic rather than functional-analytic and avoids Fourier methods altogether. In this spirit, the first part of the book consists of a thorough treatment of functions of one variable. Monotone functions, bounded variation, absolute continuity, decreasing rearrangements, curves, Lebesgue-Stieltjes measures, and the Bochner integral are discussed. The second part is devoted to the multi-variable case. Sobolev spaces are introduced, and embeddings, extensions, approximation as well as traces are treated. For the latter purpose there is also a chapter on Besov spaces which are introduced via finite differences (the "Russian school"). Luckily, the author could not resist to redo most of the Besov material using the Littlewood-Paley decomposition in a later section. In summary, the book contains a lot of interesting material on real analysis and Sobolev spaces that is accessible without a background in functional analysis. On the other hand, the technical limitations of the approach made it necessary to omit a number of standard topics, e.g. fractional Sobolev spaces. This means that for many readers the book may indeed comprise a first course on Sobolev spaces but probably not the last one.

R. Donninger (Wien)

J. Justesen, T. Høholdt: A Course In Error-Correcting Codes. Second Edition. (Textbooks in Mathematics, Vol. 19.) European Mathematical Society, Zürich, 2017, 226 S. ISBN 978-3-03719-179-8 H/b EUR 39,50.

This is the updated and enlarged second edition of the book from 2006.

On the one hand, it is a very nice introduction to coding theory and only some familiarity with linear algebra and probability is needed. On the other hand, it also contains material for researchers. It covers codes and decoding methods that are currently of most interest in research, development, and application. A list of problems for each chapter and their solutions make this book especially valuable.

Here is a list of the content: 1. Block Codes for Error Correction; 2.: Finite Fields; 3. Communication Channels and Error Probability; 4. Reed-Solomon Codes and Their Decoding; 5. Cyclic Codes; 6. Frames; 7. Maximum Likelihood Decoding and Convolutional Codes; 8. Combinations of Several Codes; 9. Decoding Reed-Solomon and BCH Codes; 10. Iterative Decoding; 11. Algebraic Geometry Codes.

A. Winterhof (Linz)

R. C. Gunning: An Introduction to Analysis. Princeton University Press, Princeton, 2018, 384 S. ISBN 978-0-691-17879-0 H/b £ 62,95.

Unlike the title suggests, this book is not a traditional introduction to analysis. It grew out of an accelerated honors analysis course at Princeton and contains much more than just an introduction to analysis. Besides the actual topic, analysis, it introduces the key concepts of point set topology and linear algebra. Furthermore, the book goes straight for the multi-dimensional case but still treats the standard one-dimensional results and examples when appropriate. The treatment severely differs from the usual introductory American calculus texts and is more in the European tradition of teaching analysis. The book is mathematically rigorous from the very beginning, the proofs are crystal clear, but the exposition is far from Bourbaki-style and the level of abstraction is moderate. In many respects the book is unusual. For instance, the standard results on series and the elementary functions are introduced only after a thorough discussion of continuity and differentiability. More traditional is the treatment of integration via Riemann's integral – Lebesgue integration is not mentioned. The final chapter treats differential forms, Stoke's theorem, and touches upon more advanced concepts like homology. Needless to say, the structure of the exposition is not compatible with the curricula of most bachelor's programs at European universities, but ideally, every prospective master's student should work through this fantastic book in order to acquire a sound background on the fundamentals of analysis.

R. Donninger (Wien)

M. Eie, S. Chang: A First Course in Linear Algebra. World Scientific Publishing Co., Singapur, 2016, 388 S. ISBN 978-981-3143-11-1 P/b £ 40.

The book is a rather straightforward introduction to linear algebra. It covers most of the standard topics like vector spaces, bases, linear systems of equations, and the canonical forms of finite-dimensional linear operators. The level of abstraction is fairly low, and the book contains a lot of worked out exercises. This makes the material very accessible to beginners. Unfortunately, the treatment of determinants is incomplete. In summary, the book provides a good basis for an introductory course on linear algebra but should ideally be complemented with some slightly more advanced material.

R. Donninger (Wien)

Nachrichten der Österreichischen Mathematischen Gesellschaft

Josef Peter Tschupik 1928–2018

Am 18. März 2018 ist Josef Peter Tschupik, em.o.Univ. Prof. der Leopold-Franzens-Universität Innsbruck, im 90. Lebensjahr verstorben. Josef Peter Tschupik befasste sich mit Geometrie, zudem war er besonders in der geometrischen Bildung und Ausbildung von künftigen Ingenieuren tätig. Er war seit 1965 Mitglied der ÖMG.

Rudolf Fritsch 1939–2018

Am 12. Juni 2018 ist Rudolf Fritsch, em.o.Univ. Prof. der Ludwig-Maximilians Universität München, im 79. Lebensjahr verstorben. Rudolf Fritsch befasste sich mit Topologie, Geometrie und Mathematikdidaktik. Viele interessante Informationen zu seinem wissenschaftlichen Werk findet man unter folgender URL: *http://www.mathematik.uni-muenchen.de/∼fritsch/*. Rudolf Fritsch war seit 1973 Mitglied der ÖMG.

Persönliches

Prof. Herbert Edelsbrunner (IST Austria) hat den Wittgenstein-Preis 2018 erhalten. Der Preis wurde aufgrund seiner exzellenten Forschungen auf dem Gebiet der Computergeometrie und Computertopologie vergeben, die Herbert Edelsbrunner in den vergangenen Jahren erbracht hat. Der jährlich vergebene Wittgenstein-Preis des Wissenschaftsfonds FWF richtet sich an exzellente Forscher/innen aller Fachdiziplinen. Er ist mit 1,4 Millionen Euro dotiert und wird von einer mit internationalen Expert/innen besetzten Jury vergeben. Die Redaktion der IMN gratuliert herzlich. Ein ausführlicher Bericht zum wissenschaftlichen Schaffen des Preisträger ist für das nächste Heft der IMN geplant.

In den *Matematica, Cultura e Societa – Rivista dell'Unione Matiematica Italiana* (Serie I, Vol. 2, N. 3, Dicembre 2017, 291–292) vom Dezember ist ein zweiseitiger Nachruf "Peter Gruber in memoriam – Un ridordo personale" von Enrico

Bombieri erschienen. Auf diese Weise möchte die Redaktion auf diese Würdigung aufmerksam machen, welche den Beitrag aus Heft Nr. 235 der IMN ergänzt.

Neue Mitglieder

Mena Hermann, Assoz.Prof. Dr. – c/o Technikerstr. 13, 6020 Innsbruck. geb. 1979. Studium der Mathematik und Doktorat in Angewandter Mathematik an der Escuela Politecnica Nacional in Quito, Ecuador. Assistent an der Universität Innsbruck von 2013 bis 2016 mit Habilitation im Jahr 2016. Seit 2016 Assoz.Prof. an der Yachay Tech in Ecuador. email *hermann.mena@uibk.ac.at*, http://hermann-mena.org.

Mras Gabriele, ao.Univ.Prof. Dr. – Blumauergasse 23/18, 1020 Wien. geb. 1974. Studium der Philosophie und Logistik an der LMU München und der Universität Wien, Doktorat 1990 mit einer Arbeit über Gottlob Frege und Habilitation 2003 in Philosophie an der Universität Wien. Derzeit ao.Univ.Prof. in Philosophie an der WU Wien. email *gabriele.mras@wu.ac.at*.

Weixlbaumer Elmar – c/o Goldegg Verlag, Mommsengasse 4/2, 1040 Wien. geb. 1967. Unternehmer, Verleger und Buchautor. email *elmar@weixlbaumer.info*.

Piantschitsch Isabell, Dr. – Franzkoglweg 6a, 8010 Deutschlandsberg. geb. 1983. Master in Mathematik 2012 und Doktorat in Astrophysik an der Karl-Franzens-Universität Graz 2018. email *isabell.piantschitsch@gmail.com*.

Nigsch Eduard, Dr. – Oskar Morgenstern Platz 1, 1090 Wien. geb. 1983. Studium der Technischen Mathematik in den Naturwissenschaften, TU Wien, Doktorat in Mathematik und Habilitation für Mathematik an der Universität Wien. Derzeit Postdoc am Wolfgang-Pauli-Institut. email *eduard.nigsch@univie.ac.at*.