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) und M. Drmota (2000–2007).

Herausgeber:

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

Bezug:

Die IMN erscheinen dreimal jährlich und werden von den Mitgliedern der Österreichischen Mathematischen Gesellschaft bezogen.
Jahresbeitrag: € 20,–

Bankverbindung: Konto Nr. 229-103-892-00 der Bank Austria–Creditanstalt (IBAN AT83-1200-0229-1038-9200, BLZ 12000, BIC/SWIFT-Code BKAUATWW).

Eigentümer, Herausgeber und Verleger: Österr. Math. Gesellschaft. Satz: Österr. Math. Gesellschaft. Druck: Grafisches Zentrum, Wiedner Hauptstraße 8–10, 1040 Wien.

ISSN 0020-7926

Österreichische Mathematische Gesellschaft

Gegründet 1903

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

Sekretariat:

TU Wien, Institut 104,
Wiedner Hauptstr. 8–10, A 1040 Wien.
Tel. +43-1-58801-11823
email: *sekr@oemg.ac.at*

Vorstand des Vereinsjahres 2011:

M. Drmota (TU Wien): Vorsitzender
M. Oberguggenberger (Univ. Innsbruck): Stellvertretender Vorsitzender
J. Wallner (TU Graz): Herausgeber der IMN
B. Lamel (Univ. Wien): Schriftführer
A. Ostermann (Univ. Unnsbruck): Stellvertretender Schriftführer
G. Larcher (Univ Linz): Kassier
P. Kirschenhofer (MU Leoben): Stellvertretender Kassier
G. Schranz-Kirlinger (TU Wien): Beauftragte für Frauenförderung
G. Teschl (Univ. Wien): Beauftragter f. Öffentlichkeitsarbeit

Beirat:

A. Binder (Linz)
U. Dieter (TU Graz)
H. Engl (Univ. Wien)
P. M. Gruber (TU Wien)
G. Helmberg (Univ. Innsbruck)
H. Heugl (Wien)
W. Imrich (MU Leoben)
M. Koth (Univ. Wien)
C. Krattenthaler (Univ. Wien)
W. Kuich (TU Wien)
W. Müller (Univ. Klagenfurt)
W. G. Nowak (Univ. Bodenkult. Wien)
L. Reich (Univ. Graz)
N. Rozsenich (Wien)
W. Schachermayer (Univ Wien)
K. Sigmund (Univ. Wien)
H. Sorger (Wien)
H. Strasser (WU Wien)
R. Tichy (TU Graz)
W. Wurm (Wien)

Vorstand, Sektions- und Kommissionsvorsitzende gehören statutengemäß dem Beirat an.

Vorsitzende der Sektionen und Kommissionen:

W. Woess (Graz)
G. Kirchner (Innsbruck)
C. Nowak (Klagenfurt)
F. Pillichshammer (Linz)
P. Hellekalek (Salzburg)
C. Krattenthaler (Wien)
H. Humenberger (Didaktikkommission)

Mitgliedsbeitrag:

Jahresbeitrag: € 20,–

Bankverbindung: Konto Nr. 229-103-892-00 der Bank Austria–Creditanstalt (IBAN AT83-1200-0229-1038-9200, BLZ 12000, BIC BKAUATWW).

Internationale Mathematische Nachrichten

International Mathematical News

Nouvelles Mathématiques Internationales

Nr. 220 (66. Jahrgang) **August 2012**

Inhalt

Die Titelseite illustriert eine diskrete Variante der flächentreuen und ergodischen „Katzenabbildung“ $(x,y) \mapsto (2x+y, x+y)$ modulo 1 am Torus $\mathbb{R}^2/\mathbb{Z}^2$, die von V. I. Arnold anhand des Bildes einer Katze illustriert wurde. Die diskrete Abbildung lautet $(i,j) \mapsto (2i+j, i+j)$ modulo N, auf dem Gitter $\mathbb{Z}^2/(N\mathbb{Z})^2$. Für den abgebildeten Fall $N = 150$ hat sie eine Periode von 300 Iterationen. *Illustration:* Claudio Rocchini (ISTI, Pisa), abgelegt in *Wikimedia Commons*.

Internat. Math. Nachrichten
Nr. 220 (2012), 1–27

Topics Related to Character Sums

Arne Winterhof

Austrian Academy of Sciences

Dedicated to the RICAM directorate: Heinz W. Engl, Karl Kunisch, and Ulrich Langer, on the occasion of their 180th birthday.

Abstract. Character sums are important tools in the theory of finite fields and have many application areas including coding theory, wireless communication, Monte Carlo methods, pseudorandom number generation, analysis of algorithms, and quantum physics. This article starts with a short tutorial on character sums and continues with a collection of applications including some classical and well-known ones as the construction of Hadamard matrices or diagonal equations as well as more recent and maybe less known ones as the analysis of nonlinear pseudorandom numbers and mutually unbiased bases for measuring quantum states.

1 Introduction

Finite fields play important roles in many application areas such as coding theory, cryptography, design theory, Monte Carlo methods, pseudorandom number generation, computational algebra, and wireless communication.

Character sums are important tools in the theory of finite fields since they govern the transition of the additive and the multiplicative structure and introduce analytical methods.

After a short tutorial on character sums we mention several applications of finite fields where character sums are involved. Any survey on applications of character sums will be incomplete such that we can present only a small choice including some classical and some new results. We start with applications of a simple character sum identity to

— Hadamard matrices,
— permutations for check digit systems as the ISBN (International Standard Book Number) and the Austrian social security number,
— autocorrelation of sequences,

ISSN 0020-7926

continue with applications of Gauss and Jacobi sums to

— uniform distribution of linear congruential pseudorandom numbers,
— diagonal equations and covering radius,
— the hidden number problem,
— mutually unbiased bases,

and conclude with applications of incomplete character sums to

— factoring of polynomials in finite fields,
— pseudorandom binary sequences,
— nonlinear pseudorandom numbers.

2 A Tutorial on Character Sums

2.1 Group Characters and Orthogonality Relations

Let $(G,\circ)$ be a finite Abelian group. A mapping

$$\chi : G \to U$$

is called a *character* of G if

$$\chi(g \circ h) = \chi(g)\chi(h) \quad \text{for all } g,h \in G,$$

where U is the multiplicative group of complex numbers of absolute value 1. The mapping $\chi_0(g) = 1$ for all $g \in G$ is called the *trivial character*. With the following multiplication of two characters χ and ψ, the set of characters $\hat{G}$ becomes a group, isomorphic to G:

$$\chi\psi(g) = \chi(g)\psi(g), \quad g \in G.$$

If G is a cyclic group of order n with a generator g, then

$$\chi(g^j) = \chi(g)^j, \quad 0 \le j \le n-1, \quad \text{and} \quad \chi(g)^n = 1$$

imply that any element χ_k of $\hat{G}$ can be expressed in terms of the complex nth roots of unity:

$$\chi_k(g) = \exp(2\pi ik/n), \quad 0 \le k \le n-1.$$

We have the following orthogonality relations:

$$\sum_{g \in G} \chi(g) = 0, \quad \chi \neq \chi_0, \tag{1}$$

and

$$\frac{1}{|G|} \sum_{\chi \in \hat{G}} \chi(g \circ h^{-1}) = \begin{cases} 1, & g = h, \\ 0, & g \neq h. \end{cases} \tag{2}$$

Proof. Since $\chi \neq \chi_0$ there exists $h \in G$ with $\chi(h) \neq 1$. We have $G = \{g \circ h : g \in G\}$ and get

$$\sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(g \circ h) = \chi(h) \sum_{g \in G} \chi(g)$$

which implies (1) since $\chi(h) \neq 1$.
Moreover, for any $g \in G$ the mapping $\hat{g}(\chi) = \chi(g)$, $\chi \in \hat{G}$, is a character of $\hat{G}$ and for $g \neq 1$ we get by (1)

$$0 = \sum_{\chi \in \hat{G}} \hat{g}(\chi) = \sum_{\chi \in \hat{G}} \chi(g)$$

which implies (2). □

2.2 Equations and Character Sums

Let $f : G^s \to G$ be a mapping, $S \subseteq G^s$ and $h \in G$. Let $N(h, f)$ be the number of solutions of

$$f(\mathbf{x}) = h, \quad \mathbf{x} \in S.$$

From the orthogonality relation (2) and separating the trivial character we get

$$N(h,f) = \frac{1}{|G|} \sum_{\mathbf{x} \in S} \sum_{\chi \in \hat{G}} \chi(f(\mathbf{x}) \circ h^{-1}) = \frac{|S|}{|G|} + \frac{1}{|G|} \sum_{\chi \neq \chi_0} \chi(h^{-1}) \sum_{\mathbf{x} \in S} \chi(f(\mathbf{x})) \quad (3)$$

and thus

$$\left| N(h,f) - \frac{|S|}{|G|} \right| < \max_{\chi \neq \chi_0} \left| \sum_{\mathbf{x} \in S} \chi(f(\mathbf{x})) \right|.$$

2.3 Characters of Finite Fields

Let $q = p^r$ be the power of a prime p. In the finite field $\mathbb{F}_q$ of q elements we naturally have two kind of characters: *additive characters*, corresponding to $(G, \circ) = (\mathbb{F}_q, +)$, and *multiplicative characters*, corresponding to $(G, \circ) = (\mathbb{F}_q^*, \cdot)$, where $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. We get all additive characters by

$$\psi_a(x) = \exp(2\pi i \operatorname{Tr}(ax)/p), \quad a, x \in \mathbb{F}_q,$$

where

$$\operatorname{Tr}(x) = x + x^p + \ldots + x^{p^{r-1}} \in \mathbb{F}_p, \quad x \in \mathbb{F}_q,$$

is the *trace function*, and all multiplicative characters by

$$\chi_k(g^j) = \exp(2\pi i jk/(q-1)), \quad 0 \leq k, j \leq q-2,$$

where g is a *primitive element of* $\mathbb{F}_q$ ($\mathbb{F}_q^* = \{g^j : 0 \leq j \leq q-2\}$).

In particular, if q is odd, the character $\chi_{(q-1)/2}(g^j) = (-1)^j$ is called *quadratic character* and is in the case $q = p$ often represented by the *Legendre symbol* $\chi_{(p-1)/2}(x) = (\frac{x}{p})$, $x \in \mathbb{F}_p$. We use the convention $\chi_k(0) = 0$ for $k \neq 0$ and $\chi_0(0) = 1$.

2.4 Complete and Incomplete Character Sums

Let $f, g : \mathbb{F}_q \to \mathbb{F}_q$ be any functions, χ be a multiplicative character, and ψ be an additive character of $\mathbb{F}_q$. A sum of the form

$$S(\chi, \psi, f, g) = \sum_{x \in \mathbb{F}_q} \chi(f(x))\psi(g(x)),$$

where x ranges over all elements of $\mathbb{F}_q$, is called a *complete character sum*. For $X \subset \mathbb{F}_q$, a sum of the form

$$S(\chi, \psi, f, g, X) = \sum_{x \in X} \chi(f(x))\psi(g(x))$$

is an *incomplete character sum*. Since the summands are either zero or roots of unity we have the *trivial bound*

$$|S(\chi, \psi, f, g, X)| \leq |X|.$$

2.5 Weil Bound

For complete sums with polynomials we have the following *Weil bound*: Let $f, g \in \mathbb{F}_q[X]$, χ be a multiplicative character and ψ be an additive character of $\mathbb{F}_q$. If χ is nontrivial of order $s > 1$ and f is not of the form $f = au^s$, $a \in \mathbb{F}_q^*$, $u \in \mathbb{F}_q[X]$, or ψ is nontrivial and g is not of the form $g = h^p - h + c$, $c \in \mathbb{F}_q$, $h \in \mathbb{F}_q[X]$, then we have

$$|S(\chi, \psi, f, g)| \leq (\deg(f) + \deg(g) - 1)q^{1/2}.$$

Note that the condition on f is fulfilled if $\gcd(\deg(f), s) = 1$ and the condition on g if $\gcd(\deg(g), q) = 1$. We provide the proof of the Weil bound, for the convenience of the reader, in two special cases in the next section. For a proof of the general case see [63].

2.6 Gauss Sums

Let χ be a multiplicative and ψ be an additive character of $\mathbb{F}_q$. Then

$$G(\chi, \psi) = \sum_{c \in \mathbb{F}_q^*} \chi(c)\psi(c)$$

is called a *Gauss sum (of type I)*.
If χ and ψ are both nontrivial, we have

$$|G(\chi,\psi)| = q^{1/2}. \tag{4}$$

Proof. We have

$$\begin{aligned}|G(\chi,\psi)|^2 = G(\chi,\psi)\overline{G(\chi,\psi)} &= \sum_{c,d\in\mathbb{F}_q^*} \chi(\underbrace{cd^{-1}}_{u})\psi(c-d) \\ &= \sum_{u\in\mathbb{F}_q^*}\chi(u)\sum_{c\in\mathbb{F}_q^*}\psi(c(1-u^{-1})) = -\sum_{u\neq 0,1}\chi(u)+q-1 = q\end{aligned}$$

by (1). □

If χ or ψ is trivial, we have

$$\begin{aligned} G(\chi_0,\psi) &= -1, \quad (\psi\neq\psi_0),\\ G(\chi,\psi_0) &= 0, \quad (\chi\neq\chi_0),\\ G(\chi_0,\psi_0) &= q-1.\end{aligned}$$

A sum of the form

$$S_n(\psi) = \sum_{c\in\mathbb{F}_q^*}\psi(c^n), \quad n|q-1,$$

is also called *Gauss sum (of type II)*. Let χ be a multiplicative character of order n, then we have

$$\frac{1+\chi(x)+\chi^2(x)+\ldots+\chi^{n-1}(x)}{n} = 1$$

if and only if $\chi(x)=1$ or equivalently $x=c^n$ for some $c\in\mathbb{F}_q^*$ and 0 otherwise. This implies the following bound on Gauss sums of type II:

$$|S_n(\psi)| = \left|\sum_{j=0}^{n-1} G(\chi^j,\psi)\right| \leq (n-1)q^{1/2}. \tag{5}$$

We note that the bound on $|S_n(\psi)|$ is only nontrivial if $n<q^{1/2}$. If $q=p$ is a prime, bounds which are nontrivial for $n\leq p^{2/3-\varepsilon}$ and $n\leq p^{1-\varepsilon}$ are given in [8, 32] (see also [7] for an improvement), respectively.

2.7 Jacobi Sums

Let $\chi_1,\ldots,\chi_k$ be $k\geq 2$ multiplicative characters of $\mathbb{F}_q$. The sum

$$J(\chi_1,\ldots,\chi_k) = \sum_{c_1+\cdots+c_k=1}\chi_1(c_1)\ldots\chi_k(c_k),$$

where the summation is extended over all $(c_1,\dots,c_k) \in \mathbb{F}_q^k$ such that $c_1+\cdots+c_k = 1$, is a *Jacobi sum*. Gauss sums and Jacobi sums are closely related by

$$J(\chi_1,\dots,\chi_k) = \frac{G(\chi_1,\psi)\cdots G(\chi_k,\psi)}{G(\chi_1\cdots\chi_k,\psi)}$$

if all involved characters are nontrivial. For background on Gauss and Jacobi sums see [3] or [45, Chapter 5]. In particular, we have (if all characters are nontrivial)

$$|J(\chi_1,\dots,\chi_k)| = q^{(k-1)/2}. \tag{6}$$

2.8 Incomplete Sums Over Intervals

In this section we consider incomplete multiplicative character sums over a finite prime field $\mathbb{F}_p$. The main tool for estimating an incomplete character sum is first transforming it to a complete sum and then using a known bound for a complete sum. The following result is proved by using a method which can be traced back to Polya and Vinogradov, see for example [38, Section 12.2], and the Weil bound. Generalizations to certain incomplete character sums over arbitrary finite fields are given in [18, 76, 79, 80].

Let χ be a nontrivial multiplicative character of $\mathbb{F}_p$. Then we have for $N < p$

$$\left|\sum_{n=0}^{N-1}\chi(n)\right| = O(p^{1/2}\log p).$$

Proof. From the orthogonality relation (2) and the Weil bound we get

$$\left|\sum_{n=0}^{N-1}\chi(n)\right| = \left|\sum_{n=0}^{N-1}\sum_{x\in\mathbb{F}_p}\chi(x)\frac{1}{p}\sum_{\psi}\psi(x-n)\right| \le \frac{1}{p}\sum_{\psi}\underbrace{\left|\sum_{x\in\mathbb{F}_p}\chi(x)\psi(x)\right|}_{\le p^{1/2}}\left|\sum_{n=0}^{N-1}\psi(n)\right|.$$

Combining this with Vinogradov's inequality

$$\begin{aligned}\sum_{\psi\neq\psi_0}\left|\sum_{n=0}^{N-1}\psi(n)\right| &= \sum_{a=1}^{p-1}\left|\frac{\exp(2\pi iaN/p)-1}{\exp(2\pi ia/p)-1}\right| \ll \sum_{a=1}^{p-1}\frac{1}{\sin(\pi a/p)} \\ &\ll p\sum_{a=1}^{p-1}\frac{1}{\min\{a,p-a\}} \ll p\int_1^p\frac{dx}{x} = p\log p\end{aligned} \tag{7}$$

we get the result. □

Actually, the same method gives also a bound on incomplete character sums with polynomials.

Theorem 1 (Polya-Vinogradov-Weil bound)**.** *Let χ be a nontrivial multiplicative character of order s of $\mathbb{F}_p$ and $f \in \mathbb{F}_p[X]$ with $d > 0$ different zeros such that f is not, up to a constant multiple, an s-th power. Then we have*

$$\left| \sum_{n=0}^{N-1} \chi(f(n)) \right| \leq dp^{1/2} \log p, \quad 1 \leq N < p.$$

3 Applications of a Simple Character Sum Identity

In this section we present applications of the following well-known character sum identity.

Proposition 1. *Let χ denote a nontrivial multiplicative character of $\mathbb{F}_q$. Then we have*

$$\sum_{x \in \mathbb{F}_q} \chi(x+a)\overline{\chi(x+b)} = -1, \quad a,b \in \mathbb{F}_q, \quad a \neq b.$$

Proof. Since $\chi(u)\overline{\chi(v)} = \chi(uv^{-1})$, $v \neq 0$, and the mapping

$$-b \neq x \mapsto (x+a)(x+b)^{-1} \neq 1$$

is injective, we get

$$\sum_{x \in \mathbb{F}_q \setminus \{-b\}} \chi((x+a)(x+b)^{-1}) = \sum_{1 \neq z \in \mathbb{F}_q} \chi(z) = -\chi(1) = -1$$

by (1). □

3.1 Hadamard Matrices

A *Hadamard matrix of order n* is an $n \times n$ matrix H with entries from $\{-1,+1\}$ satisfying $HH^T = nI_n$, where I_n denotes the $n \times n$ identity matrix. The following construction is due to Paley [60].

Theorem 2 (Paley)**.** *Let q be the power of an odd prime, η the quadratic character of $\mathbb{F}_q$ and $\mathbb{F}_q = \{\xi_1, \ldots, \xi_q\}$ any fixed ordering of $\mathbb{F}_q$. For $q \equiv 3 \bmod 4$ there exists a Hadamard matrix $H = (h_{ij})$ of order $n = q+1$ defined by*

$$\begin{aligned} h_{i,n} &= h_{n,i} = 1 && (i = 1, \ldots, n), \\ h_{j,j} &= -1 && (j = 1, \ldots, n-1), \\ h_{i,j} &= \eta(\xi_j - \xi_i) && (i,j = 1, \ldots, n-1,\ i \neq j). \end{aligned}$$

Proof. The inner product of the last row of H with the ith row, $1 \leq i < n$, is

$$\sum_{j=1}^{n-1} \eta(\xi_j - \xi_i) + h_{i,i} + h_{i,n} = \sum_{x \in \mathbb{F}_q} \eta(x) = 0$$

by (1). The product of the ith and kth row for $1 \leq i < k < n$ is

$$\sum_{j=1}^{n-1} \eta(\xi_j - \xi_i)\eta(\xi_j - \xi_k) - \eta(\xi_i - \xi_k) - \eta(\xi_k - \xi_i) + 1 = -\eta(\xi_i - \xi_k) - \eta(\xi_k - \xi_i)$$

by Proposition 1 and thus zero if and only if $\eta(-1) = -1$ or equivalently $q \equiv 3 \bmod 4$. □

Paley also presented a similar, but slightly more complicated construction for Hadamard matrices of order $n = 2(q+1)$ if $q \equiv 1 \bmod 4$.

Theorem 3 (Paley)**.** *Let $q \equiv 1 \bmod 4$ be the power of a prime, $S = (s_{i,j})$ be the $(q+1) \times (q+1)$ matrix defined by $s_{0,0} = 0$, $s_{0,i} = s_{i,0} = 1$, $i = 1, \ldots, q$, and $s_{i,j} = \eta(\xi_j - \xi_i)$, $i, j = 1, \ldots, q$. Then the matrix*

$$H = \begin{pmatrix} S + I_{q+1} & S - I_{q+1} \\ S - I_{q+1} & -S - I_{q+1} \end{pmatrix}$$

is a Hadamard matrix of order $n = 2(q+1)$.

The Hadamard conjecture proposes that a Hadamard matrix of order $n = 4k$ exists for every positive integer k. The smallest order n for which no Hadamard matrix of order $n = 4k$ has been constructed is $n = 668$. The last progress known to the author was the construction of a Hadamard matrix of order $n = 428$ by [39].

For a monograph on Hadamard matrices and applications see [34]. In particular, Hadamard matrices can be used to construct good error correcting codes [44]. For relations between Hadamard matrices and designs see [4].

There are several generalizations of Hadamard matrices to matrices with entries which are complex mth roots of unity. The earliest was introduced by Butson [11]. A *Butson-Hadamard matrix* H of order n with complex mth roots of unity satisfies $H\overline{H}^T = nI_n$. If $m = p$ is prime, $n = p^r$, and ψ a nontrivial additive character of $\mathbb{F}_{p^r}$, then $H = (h_{i,j})$ with $h_{i,j} = \psi(\xi_i \xi_j)$ is a Butson-Hadamard matrix of order p^r with complex pth roots of unity by (2). For some non-existence results on Butson-Hadamard matrices see [78]. In particular, if $m = p^r$ is a power of a prime p, a Butson-Hadamard matrix of order n can only exist if n is divisible by p. Moreover, if $p \equiv 3 \bmod 4$ is prime, $n = p^b a^2 s$ is odd with a square-free s and $\gcd(s, p) = 1$, and there exists a prime $q | s$ with $(\frac{q}{p}) = -1$, then there is no Butson-Hadamard matrix with $m = p^r$ or $m = 2p^r$.

3.2 Cyclotomic Complete Mappings and Check Digit Systems

In this section we study certain permutations which are linear on cyclotomic cosets and can be used to define check digit systems which detect all single errors and neighbor transpositions.

Let n be a positive divisor of $q-1$ and γ a primitive element of $\mathbb{F}_q$. Then the sets

$$C_i = \left\{\gamma^{jn+i} : j = 0,1,\ldots,(q-1)/n-1\right\}, \quad i = 0,1,\ldots,n-1, \tag{8}$$

are *cyclotomic cosets of order n*. For $a_0,a_1,\ldots,a_{n-1} \in \mathbb{F}_q^*$ we define a *cyclotomic mapping* $f_{a_0,a_1,\ldots,a_{n-1}}$ *(of index n)* by $f_{a_0,a_1,\ldots,a_{n-1}}(0) = 0$ and

$$f_{a_0,a_1,\ldots,a_{n-1}}(\xi) = a_i\xi \quad \text{if } \xi \in C_i, \quad i = 0,1,\ldots,n-1.$$

Proposition 2 [26, Theorem 3.7]**.** *The mapping $f_{a_0,a_1,\ldots,a_{n-1}}$ is a permutation of $\mathbb{F}_q$ if and only if $a_iC_i \neq a_jC_j$ for all $0 \leq i < j \leq n-1$.*

Proof. The function $f_{a_0,a_1,\ldots,a_{n-1}}$ is injective on each coset C_i, hence, it is not a permutation if and only if there exists $0 \leq i < j < n$, $x \in C_i$, and $y \in C_j$ with $a_ix = a_jy$ which is possible if and only if $a_iC_i = a_jC_j$ for some $0 \leq i < j < n$. □

Corollary 1. *For $n \geq 2$ let j be an integer with $0 \leq j < n$, χ a multiplicative character of $\mathbb{F}_q$ of order n, and $a,b \in \mathbb{F}_q$ with $a \neq b$. If $a_j = a$ and $a_i = b$ for $i \neq j$, then $g_{a,b} = f_{a_0,a_1,\ldots,a_{n-1}}$ is a permutation if and only if $\chi(a) = \chi(b)$.*

A permutation f of $\mathbb{F}_q$ is a *complete mapping* of $\mathbb{F}_q$ if $f(x)+x$ is also a permutation of $\mathbb{F}_q$.

Complete mappings are pertinent to the problem of constructing orthogonal Latin squares [45, Section 9.4]. A $q \times q$ array (a_{ij}) is called a *Latin square* over $\mathbb{F}_q$ if each row and each column contains every element of $\mathbb{F}_q$ exactly once. Two Latin squares (a_{ij}) and (b_{ij}) are said to be *orthogonal* if the q^2 ordered pairs (a_{ij},b_{ij}) are all different. If $f(X)$ is a complete mapping, (a_{ij}) with $a_{ij} = \xi_i + \xi_j$ and (b_{ij}) with $b_{ij} = f(\xi_j) - \xi_i$ are orthogonal Latin squares.

Substituting $b = ac$ we see that $g_{a,b}$ is a complete mapping if and only if $\chi(c) = 1$ and $\chi(a+1) = \chi(ac+1)$ and the number N of complete mappings $g_{a,ac}$ with $c \neq 1$ is

$$N = \sum_{c \in \mathbb{F}_q^*,\ \chi(c)=1,\ c\neq 1} \frac{1}{n} \sum_{i=0}^{n-1} \sum_{a \in \mathbb{F}_q^* \setminus \{1,c^{-1}\}} \chi^i(a+1)\overline{\chi^i(a-c^{-1})}$$

and Proposition 1 implies the following theorem [56, Theorem 3].

Theorem 4. *Let $n \geq 2$ be a divisor of $q-1$ and $j \in \{0,1,\ldots,n-1\}$. Then the number N of ordered pairs $(a,b) \in \mathbb{F}_q^* \times \mathbb{F}_q^*$ with $a \neq b$ such that the cyclotomic*

mapping $g_{a,b} = f_{a_0,a_1,\ldots,a_{n-1}}$ *with* $a_j = a$ *and* $a_i = b$ *for* $i \neq j$ *is a complete mapping of* $\mathbb{F}_q$ *equals*

$$N = \frac{(q-n-1)(q-2n-1)}{n^2}.$$

A *check digit system* over $\mathbb{F}_q$ consists of s permutations $p_1, \ldots, p_s$ of $\mathbb{F}_q$ and a symbol $c \in \mathbb{F}_q$ such that each word $a_1 \ldots a_{s-1} \in \mathbb{F}_q^{s-1}$ is extended by a *check digit* a_s such that $p_1(a_1) + \cdots + p_s(a_s) = c$.

All *single errors* are detected since all p_i are permutations. Another frequent family of errors are *adjacent transpositions* $\ldots ab \ldots \to \ldots ba \ldots$ which are all detected if $p_{i+1}(x)p_i^{-1}(x) - x$ are also permutations for $i = 1, \ldots, s-1$. A permutation f such that $f(x) - x$ is also a permutation is an *orthomorphism*. Since f is an orthomorphism whenever $-f$ is a complete mapping, the number of orthomorphisms and complete mappings of the form $g_{a,b}$ is the same and the probability that a random choice of the parameters (a,b) gives an orthomorphism is asymptotically n^{-2} by Theorem 4.

Examples. An International Standard Book Number (ISBN-10) consists of a string of 10 digits $x_1x_2x_3x_4x_5x_6x_7x_8x_9 - x_{10}$. The digits $x_1, \ldots, x_9$ consist of three consecutive blocks, a language identifier, a publisher identifier (both issued by the international ISBN agency), and a serial number issued by the publisher. The digit x_{10} is a check digit. A correct ISBN satisfies

$$x_1 + 2x_2 + 3x_3 + 4x_4 + 5x_5 + 6x_6 + 7x_7 + 8x_8 + 9x_9 + 10x_{10} = 0 \in \mathbb{F}_{11},$$

that is, $p_i(x) = ix$, $i = 1, \ldots, 10$, and $p_{i+1}p_i^{-1}(x) = (i^{-1}+1)x$, $i = 1, \ldots, 9$, which are all orthomorphisms. For example here is a list of books and their ISBNs:

— H. W. Engl: Integralgleichungen [24]. ISBN: 3-211-83071-5
— H. T. Banks, K. Kunisch: Estimation techniques for distributed parameter systems [2]. ISBN: 0-8176-3433-9
— C. C. Douglas, G. Haase, U. Langer: A tutorial on elliptic PDE solvers and their parallelization [22]. ISBN: 0-89871-541-5

The Austrian social security number consists of 10 digits as well. The first three digits $x_1x_2x_3$ are any given number and the last six $x_5x_6x_7x_8x_9x_{10}$ describe the birthday in the form *ddmmyy*. The missing digit x_4 is calculated such that

$$3x_1 + 7x_2 + 9x_3 + 10x_4 + 5x_5 + 8x_6 + 4x_7 + 2x_8 + x_9 + 6x_{10} = 0 \in \mathbb{F}_{11},$$

that is, $p_i(x) = 3 \cdot 2^{1-i}$, $i = 1, \ldots, 10$, and $p_{i+1}p_i^{-1}(x) = 2^{-1}x$, $i = 1, \ldots, 9$, which are also all orthomorphisms.

The detection of several other types of frequent errors is only guaranteed if $p_1, \ldots, p_n$ satisfy additional conditions. The frequencies of several error types are given in [74]. Besides single errors

$$\mid \ \ldots\ a\ \ldots\ \mid \rightarrow \mid \ \ldots\ b\ \ldots\ \mid$$

and adjacent transpositions

$$\mid \ \ldots\ ab\ \ldots\ \mid \rightarrow \mid \ \ldots\ ba\ \ldots\ \mid$$

the most frequent errors are *jump transpositions*

$$\mid \ \ldots\ acb\ \ldots\ \mid \rightarrow \mid \ \ldots\ bca\ \ldots\ \mid$$

twin errors

$$\mid \ \ldots\ aa\ \ldots\ \mid \rightarrow \mid \ \ldots\ bb\ \ldots\ \mid$$

and *jump twin errors*

$$\mid \ \ldots\ aca\ \ldots\ \mid \rightarrow \mid \ \ldots\ bcb\ \ldots\ \mid.$$

We consider the case when $p_i = f^{(i)}$ for $i = 1,\ldots,n$ is the ith composition of a fixed permutation f of $\mathbb{F}_q$. Single errors are detected since f is a permutation. Adjacent transpositions are detected if and only if $f - id$ is a permutation, i.e., f is an orthomorphism. Twin errors, jump transpositions and jump twin errors are detected whenever $f + id$, $f^{(2)} - id$ and $f^{(2)} + id$, respectively, is a permutation, i.e., f is a complete mapping, $f^{(2)}$ is an orthomorphism or a complete mapping, respectively, see for example [64].

For example, the mapping induced by the polynomial $f(X) = aX \in \mathbb{F}_q[X]$ for a in $\mathbb{F}_q$ satisfies all five (not necessarily different) conditions if $a \notin \{0,-1,1, \sqrt{-1},-\sqrt{-1}\}$. The number of $a \in \mathbb{F}_q$ such that all five conditions are satisfied is $q-2$ if q is even, $q-5$ if $q \equiv 1 \bmod 4$ and $q-3$ if $q \equiv 3 \bmod 4$ since -1 is a square in $\mathbb{F}_q$ if and only if $q \equiv 1 \bmod 4$ and $1 = -1 = \pm\sqrt{-1}$ if q is even.

Again the number of pairs (a,b) such that $g_{a,b}$ satisfies all five conditions can be expressed in terms of character sums and an asymptotic formula for this number is given in [66].

3.3 Autocorrelation of Cyclotomic Generators

Put $\varepsilon_n = \exp(2\pi i/n)$. Let (s_k) be a T-periodic sequence over $\mathbb{Z}_n$. The *(periodic) autocorrelation* of (s_k) is the complex-valued function defined by

$$A(t) = \frac{1}{T}\sum_{k=0}^{T-1} \varepsilon_n^{s_{k+t}-s_k}, \quad 1 \le t < T.$$

Sequences with low autocorrelation have several applications in wireless communication, cryptography, and radar, see the monograph [28].

Let p be a prime and $n > 1$ be a divisor of $p-1$. The p-periodic sequence (s_k) over $\mathbb{Z}_n$ defined by $s_0 = 0$ and $s_k = j$ if $k \in C_j$ for $0 \le j < n$, $1 \le k < p$, where C_j denotes the jth cyclotomic coset of order n defined by (8), is a *cyclotomic generator of order n*. Its autocorrelation function is

$$A(t) = \frac{1}{p}\left(\overline{\chi(-t)} + \chi(t) + \sum_{k=0}^{p-1} \chi(k+t)\overline{\chi(k)}\right),$$

where χ is a multiplicative character of $\mathbb{F}_p$ of order n. Proposition 1 implies the exact values of the autocorrelation function of the cyclotomic generator of order n, see [47] for the proof of a generalization to arbitrary finite fields.

Theorem 5. *The autocorrelation function $A(t)$ of the cyclotomic generator of order n is given by $A(t) = (-1 + \varepsilon_n^j + \varepsilon_n^{-j-k})/p$ if $t \in C_j$ and $-1 \in C_k$.*

The (periodic) autocorrelation reflects global randomness of a sequence whereas the *aperiodic autocorrelation* function

$$A(t,a,b) = \frac{1}{T}\sum_{k=a}^{b} \varepsilon_n^{s_{k+t}-s_k}, \quad 1 \le a,b,t < T$$

reflects local randomness. For the cyclotomic generator of order n the value $A(t,a,b)$ is essentially an incomplete multiplicative character sum and can be bounded by Theorem 1. See also [47] for a generalization.

4 Applications of Gauss and Jacobi Sums

Now we mention some applications of Gauss and Jacobi sums.

4.1 Distribution of Linear Congruential Pseudorandom Numbers

From now on, for a prime p, we identify $\mathbb{F}_p$ with the integers $\{0,1,\ldots,p-1\}$. The sequences

$$x_{n+1} = ax_n + b, \quad n \ge 0,$$

where $x_0, a, b \in \mathbb{F}_p$ with $x_0, a \ne 0$, and $a \ne 1$ are *linear congruential pseudorandom number generators*.

If $a \ne 1$, they can also be given explicitly by

$$x_n = a^n x_0 + \frac{a^n - 1}{a-1}b, \quad n \ge 0. \tag{9}$$

The sequence (x_n) is T-periodic if $b \neq (1-a)x_0$, where T is the order of a.

Let Γ be a sequence of N elements $(\gamma_n)_{n=1}^N$ in the unit interval $[0,1)$. The *discrepancy* $D_N(\Gamma)$ is defined by

$$D_N(\Gamma) = \sup_{B \subseteq [0,1)} \left| \frac{T_\Gamma(B)}{N} - |B| \right|,$$

where the supremum is taken over all subintervals $B = [\alpha, \beta) \subseteq [0,1)$, and $T_\Gamma(B)$ is the number of elements of Γ inside B.

The discrepancy is a measure for the uniform distribution of Γ and a small discrepancy is a desirable feature for Monte Carlo integration, see [49]. The problem of estimating the discrepancy can be reduced to the problem of estimating certain exponential sums.

For example, for any sequence $\gamma_n = u_n/p$, $n = 0, 1, \ldots, N-1$, derived from a sequence $u_0, u_1, \ldots, u_{N-1}$ of elements of $\mathbb{F}_p$ and any interval of the form $[a/p, b/p)$ with integers a, b we get with $f(x) = x$ and $S = \{u_0, u_1, \ldots, u_{N-1}\}$ by (3)

$$T_\Gamma(B) = \sum_{h=a}^{b-1} N(h,f) = \frac{(b-a)N}{p} + \frac{1}{p} \sum_{\psi \neq \psi_0} \sum_{h=a}^{b-1} \psi(-h) \sum_{n=0}^{N-1} \psi(u_n)$$

and thus by Vinogradov's inequality (7)

$$\left| \frac{T_\Gamma(B)}{N} - |B| \right| \ll \frac{\log p}{N} \max_{\psi \neq \psi_0} \left| \sum_{n=0}^{N-1} \psi(u_n) \right|,$$

where the maximum is taken over all nontrivial additive characters of $\mathbb{F}_p$.

In general, the Erdős-Turan inequality reduces the problem of estimating the discrepancy to the problem of estimating exponential sums.

Proposition 3 (Erdős-Turan inequality, cf. [23, Theorem 1.2.1])**.** *Let Γ be a sequence $(\gamma_n)_{n=1}^N$ in $[0,1)$. We have for any integer $H \geq 1$,*

$$D_N(\Gamma) \ll \frac{1}{H} + \frac{1}{N} \sum_{h=1}^{H} \frac{1}{h} |S_N(h)|, \quad \textit{where } S_N(h) = \sum_{n=0}^{N-1} \exp(2\pi i h \gamma_n).$$

For the sequence (x_n/p), $n = 0, 1, \ldots, T-1$, in $[0,1)$ derived from a linear pseudorandom number generator (x_n), we have with the additive character $\psi(x) = \exp(2\pi i h x_0 x/p)$ of $\mathbb{F}_p$,

$$|S_T(h)| = \left| \sum_{n=0}^{T-1} \psi(a^n) \right| = \frac{T}{p-1} \left| \sum_{x \in \mathbb{F}_p^*} \psi\left(x^{(p-1)/T}\right) \right| \leq p^{1/2}$$

by (5). A discrepancy bound for parts of the period can be easily obtained by combining Proposition 3 with the corresponding bound for incomplete Gauss sums of type II.

Theorem 6 [48, Theorem 1]**.** *For the sequence* $\Gamma = \{x_n/p : n = 0,\ldots,N-1\}$, *where* x_n *is defined by* (9)*,* $N < T$ *and* T *is the order of* a*, we have* $D_N(\Gamma) \ll N^{-1}p^{1/2}(\log p)^2$.

Although linear generators can be certainly used for many applications they have some well-known deficiencies which can be disastrous for some particular applications. For example, they have a coarse lattice structure. Nonlinear methods have become attractive alternatives to linear generators which don't have such undesirable features, see [15, 19, 20, 21, 54, 55, 57, 61].

A particularly nice nonlinear generator is the *digital explicit inversive pseudorandom number generator* over $\mathbb{F}_q$ defined as follows. Let $\{\gamma_1,\ldots,\gamma_r\}$ be an ordered basis of $\mathbb{F}_q$ over $\mathbb{F}_p$, where $q = p^r$. Then we define an ordering $\{\xi_0,\ldots,\xi_{q-1}\}$ of $\mathbb{F}_q$ by

$$\xi_n = n_1\gamma_1 + n_2\gamma_2 + \ldots + n_r\gamma_r$$

if

$$n = n_1 + n_2 p + \ldots + n_r p^{r-1}, \quad 0 \le n_1,\ldots,n_r < p.$$

The pseudorandom number generator, i.e. a sequence over $\mathbb{F}_q$ from which we can derive pseudorandom numbers, is

$$\rho_n = (\alpha\xi_n + \beta)^{-1}, \quad n = 0,1,\ldots,q-1, \quad \xi_n \neq -\alpha^{-1}\beta$$

and $\rho_n = 0$ if $\xi_n = -\alpha^{-1}\beta$ for some $\alpha,\beta \in \mathbb{F}_q$ with $\alpha \neq 0$. If

$$\rho_n = c_{n,1}\gamma_1 + c_{n,2}\gamma_2 + \cdots + c_{n,r}\gamma_r$$

with all $c_{n,i} \in \mathbb{F}_p$, we derive rational pseudorandom numbers in the interval $[0,1)$ by defining

$$y_n = \sum_{j=1}^{r} c_{n,j}p^{-j}, \quad n = 0,1,\ldots.$$

Discrepancy bounds on these pseudorandom numbers are given in [14, 52]. In particular, we note that in contrast to many other nonlinear generators these sequences can be rather efficiently generated using the *Itoh-Tsujii algorithm* [36] for inverting elements in a finite field and they are also suitable for parallelization [53].

For more information on pseudorandom number generation we refer to the monograph [49] and the survey [73].

4.2 Diagonal Equations, Waring's Problem in Finite Fields, and Covering Radius of Certain Cyclic Codes

A *diagonal equation* over $\mathbb{F}_q$ is an equation of the type

$$c_1x_1^{k_1} + \cdots + c_sx_s^{k_s} = b \tag{10}$$

for any positive integers $k_1,\dots,k_s$, $c_1,\dots,c_s \in \mathbb{F}_q^*$, and $b \in \mathbb{F}_q$. We denote by N_b the number of solutions in $\mathbb{F}_q^s$ of (10) which can be represented in terms of Jacobi sums and multiplicative characters.

Theorem 7 [45, Theorem 6.34]**.** *The number N_b of solutions of (10) for $b \in \mathbb{F}_q^*$ is*

$$N_b = q^{s-1} + \sum_{j_1=1}^{d_1-1} \cdots \sum_{j_s=1}^{d_s-1} \chi_1^{j_1}(bc_1^{-1}) \dots \chi_s^{j_s}(bc_s^{-1}) J(\chi_1^{j_1},\dots,\chi_s^{j_s}),$$

where χ_i denotes a multiplicative character of order $d_i = \gcd(k_i, q-1)$.

We note that N_b can also be expressed in terms of Gauss sums of type II.

Let $g(k,q)$ be the smallest s such that every element $b \in \mathbb{F}_q$ can be written as a sum of at most s summands of k-th powers in $\mathbb{F}_q$. The problem of determining or estimating $g(k,q)$ is *Waring's problem in $\mathbb{F}_q$*.

We note that $g(k,q) = g(d,q)$ if $d = \gcd(k, q-1)$ and we may restrict ourselves to the case that $k \mid (q-1)$. Combining Theorem 7 (with $k_1 = \cdots = k_s = k \mid q-1$ and $c_1 = \cdots = c_s = 1$) with the result on the absolute value of Jacobi sums (6) we get immediately

$$N_b \geq q^{s-1} - (k-1)^s q^{(s-1)/2}$$

which implies the following bound [77].

Theorem 8. *For any divisor k of $q-1$ we have $g(k,q) \leq s$ if $q^{s-1} > (k-1)^{2s}$.*

Theorem 8 applies only to $k < q^{1/2-\varepsilon}$. For $q^{3/7}+1 \leq k < q^{1/2}$ we have the improvement $g(k,q) \leq 8$ of [16, Corollary 7]. For larger k the kth powers may fall into some proper subfield of $\mathbb{F}_q$ and $g(k,q)$ may not exist. However, if $g(k,q)$ exists and $k \leq q^{1-\varepsilon}$ for any $\varepsilon > 0$, from [27, Theorem 6] it follows that there is a constant $c(\varepsilon)$ such that $g(k,q) \leq c(\varepsilon)$. If $q = p$ is a prime, we can still extend the range of nontrivial bounds. A very moderate but nontrivial bound on Gauss sums of type II from [41] leads to the bound $g(k,p) \ll (\ln k)^{2+\varepsilon}$ if $k < p(\log\log p)^{1-\varepsilon}/\log p$.

The *covering radius* $\rho(C)$ of a code $C \subseteq \mathbb{F}_q^n$ is

$$\rho(C) = \max_{\mathbf{x} \in \mathbb{F}_q^n} \min_{\mathbf{c} \in C} d(\mathbf{c}, \mathbf{x}),$$

where d is the *Hamming distance*.

Proposition 4 [33, Lemma 1.1]**.** *Let H be the parity check matrix of a linear $[n,k]$-code C over $\mathbb{F}_q$, i.e., $C = \{\mathbf{c} \in \mathbb{F}_q^n : H\mathbf{c}^T = \mathbf{0}\}$. The covering radius is the least integer ρ such that every $\mathbf{x} \in \mathbb{F}_q^{n-k}$ is a linear combination of at most ρ columns of H.*

Let $g \in \mathbb{F}_q[X]$ be the minimal polynomial of an element $\alpha \in \mathbb{F}_q^*$ of order n and r be the order of q modulo n, i.e., $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^r}$. Then the cyclic code $C = (g)$ is

the $[n, n-r]$-code with parity check matrix $H = (1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$, where the elements of $\mathbb{F}_{q^r}$ are identified with r-dimensional column vectors.
Put $N = (q^r - 1)/n$. Then $\alpha = \gamma^N$ for some primitive element γ of $\mathbb{F}_{q^r}$ and the columns of H consist of the nonzero N-th powers in $\mathbb{F}_{q^r}$. By Proposition 4, $\rho(C)$ is the least integer ρ such that any $x \in \mathbb{F}_{q^r}$ can be written as a linear combination of at most ρ N-th powers in $\mathbb{F}_{q^r}$. Hence, we have $\rho(C) \leq g(N, q)$, where we have equality for $q = 2$.

Finally, we note that also Waring's problem with polynomials has been studied [17]. In particular for *Dickson polynomials* very strong results are known [29, 59] which are comparable to the results on monomials mentioned above.

4.3 Hidden Number Problem and Noisy Interpolation

The *(extended) hidden number problem* is defined as follows, see also [5, 6]. Let $\mathcal{T} \subseteq \mathbb{F}_p$. Recover a number $a \in \mathbb{F}_p$ if for many known $t \in \mathcal{T}$ the l most significant bits of at are given.

If l is of order $\log^{1/2} p$ and $\mathcal{T}$ has some uniform distribution property, a lattice reduction technique solves the hidden number problem in polynomial time. The uniform distribution property is fulfilled if the maximum over all nontrivial additive character sums of $\mathbb{F}_p$ over $\mathcal{T}$ is small, i.e.,

$$\max_{\psi \neq \psi_0} \left| \sum_{t \in \mathcal{T}} \psi(t) \right| = O(\#\mathcal{T}^{1-\varepsilon}).$$

If $\mathcal{T}$ is a subgroup of $\mathbb{F}_p^*$ the sums can be reduced to Gauss sums of type II and the desired uniform distribution property is fulfilled by the bounds of [32] and [7, 8] if $\#T \geq p^{1/3+\varepsilon}$ and $\#T \geq p^{\varepsilon}$, respectively. The bound of [41] and ideas reminiscent to Waring's problem solve the problem for smaller $\#T \geq \log p/(\log\log p)^{1-\varepsilon}$ but for larger l of order $\log^4 p$.

The *sparse polynomial noisy interpolation problem*, see [70], consists of finding an unknown polynomial $f \in \mathbb{F}_p[X]$ of small weight from approximate values of $f(t)$ at polynomially many points $t \in \mathbb{F}_p$ selected uniformly at random.

The case $f(X) = aX$ corresponds to the hidden number problem. For more details we refer to the survey [71] and [69, Chapter 30].

4.4 Mutually Unbiased Bases

A maximal set of *mutually unbiased bases*, for short *MUBs*, is given by a set of $n^2 + n$ vectors in $\mathbb{C}^n$ which are the elements of $n+1$ orthonormal bases $\mathcal{B}_h = \{\vec{w}_{h,1}, \ldots, \vec{w}_{h,n}\}$ of $\mathbb{C}^n$ where $h = 0, \ldots, n$. Hence,

$$\langle \vec{w}_{h,i}, \vec{w}_{h,j} \rangle = \delta_{i,j}, \quad \text{where} \quad \delta_{i,j} = \begin{cases} 1, & i = j, \\ 0, & i \neq j, \end{cases}$$

and the defining property is the mutual unbiasedness, given by

$$|\langle \vec{w}_{f,i}, \vec{w}_{g,j} \rangle| = \frac{1}{\sqrt{n}} \tag{11}$$

for $0 \le f,g \le n$, $f \ne g$, and $1 \le i,j \le n$, where $\langle \vec{a}, \vec{b} \rangle = \sum_{u=1}^{n} \overline{a_u} b_u$ denotes the standard inner product of two vectors $\vec{a} = (a_1, \ldots, a_n)$, $\vec{b} = (b_1, \ldots, b_n) \in \mathbb{C}^n$.

Mutually unbiased bases were introduced by Schwinger [65]. They have applications in quantum state determination [37, 82], quantum cryptography [62], quantum error-correcting codes [12, 30] and the mean king's problem [25].

Theorem 9 [40, 82]**.** *Let $n = p^r$ be the power of a prime $p > 2$ and ψ be the additive canonical character of $\mathbb{F}_n = \{\xi_1, \ldots, \xi_n\}$. Then*

$$\vec{w}_{h,k} = \frac{1}{\sqrt{n}} \left(\psi(\xi_h \xi_u^2 + \xi_k \xi_u) \right)_{u=1,\ldots,n}, \qquad h,k = 1, \ldots, n,$$

and $\vec{w}_{0,j} = \left(\delta_{j,u} \right)_{u=1}^{n}$ is a maximal set of MUBs.

The inner products of two vectors from different bases can be easily reduced to Gauss sums (with the quadratic character) and (4) (or (5) with $n = 2$) implies the mutual unbiasedness.

Maximal sets of $n+1$ MUBs in dimension n are only known to exist in any dimension $n = p^r$ which is a power of a prime p. For $n = 2^r$ a construction based on Galois rings is given in [40]. If we relax (11) to

$$|\langle \vec{w}_{f,i}, \vec{w}_{g,j} \rangle| = O\left(n^{-1/2} (\log n)^{1/2} \right)$$

we can construct sets of $n+1$ orthonormal bases for any dimension n, see [72]. Elliptic curves over finite fields can be used to construct sets of $n+1$ orthonormal bases with

$$|\langle \vec{w}_{f,i}, \vec{w}_{g,j} \rangle| = O\left(n^{-1/2} \right)$$

which applies to almost all dimensions n and under some widely believed conjecture about the gaps between primes to all n.

Theorem 10 [72]**.** *Let E be an elliptic curve over a finite field $\mathbb{F}_p$ of prime order $p > 3$ with n points. For $2 \le d \le n-1$ denote by F_d the set of polynomials over E of degree at most d with $f(0,0) = 0$:*

$$F_d = \Big\{ f(X,Y) = u(X) + Y v(X) : \ \ u(X), v(X) \in \mathbb{F}_p[X],\ u(0) = 0,$$
$$\max\{2\deg(u), 2\deg(v) + 3\} \le d \Big\}.$$

Let X denote the character group of E. For $f \in \mathbb{F}_p[E]$ we define the set

$$B_f = \{\vec{v}_{f,\chi} : \chi \in X\},$$

where for a character $\chi \in X$, the vector $\vec{v}_{f,\chi}$ is given by

$$\vec{v}_{f,\chi} = \frac{1}{\sqrt{n}}(\psi(f(P))\chi(P))_{P\in E}$$

where ψ denotes the additive canonical character of $\mathbb{F}_p$. Then the following holds: For $2 \le d \le n-1$ the standard basis and the p^{d-1} sets $B_f = \{\vec{v}_{f,\chi} : \chi \in X\}$, with $f \in F_d$, are orthonormal and satisfy

$$|\langle \vec{v}_{f,\chi}, \vec{v}_{g,\psi}\rangle| \le \frac{2d + (2d+1)n^{-1/2}}{n^{1/2}},$$

where $f, g \in F_d$, $f \neq g$, and $\chi, \psi \in X$.

5 Incomplete Character Sums

In this section we mention some more applications of Theorem 1 as well as an application where the standard techniques for estimating the involved incomplete character sums fail and other methods are used.

5.1 Finding Deterministically Linear Factors of Polynomials

Now we describe an algorithm of Legendre [43] for finding linear factors of polynomials that can be analyzed via incomplete character sums.

Let $f \in \mathbb{F}_p[X]$, p an odd prime, be a squarefree polynomial with $f(0) \neq 0$ which splits over $\mathbb{F}_p$. For $t = 0, 1, \ldots, N$ we compute

$$L_t(X) = \gcd((X+t)^{(p-1)/2} - 1, f(X)) = \gcd(g_t(X) - 1, f(X))$$

via the Euclidean algorithm, where N is the main parameter of the algorithm, hoping that at least one polynomial L_t is nontrivial, that is, is equal to neither 1 nor f. For each t, the polynomial

$$g_t(X) \equiv (X+t)^{(p-1)/2} \bmod f(X), \quad \deg(g_t) < \deg(f)$$

is calculated efficiently using repeated squaring.

Since $x^{(p-1)/2} = 1$ if and only if x is a quadratic residue modulo p, L_t is trivial, i.e. either 1 or f, only if

$$\left(\frac{a+t}{p}\right) = \left(\frac{b+t}{p}\right)$$

for any two distinct roots a, b of f. Therefore, the algorithm does not determine a nontrivial factor of f only if

$$N+1 = \sum_{t=0}^{N} \left(\frac{(a+t)(b+t)}{p} \right) \ll p^{1/2} \log p$$

by Theorem 1. Using another method we can get rid of the log factor, see [68, Theorem 1].

Any polynomial f can be factorized into squarefree polynomials calculating $\gcd(f, f')$. The part of a squarefree polynomial f which splits over $\mathbb{F}_p$ and is not divisible by X is $\gcd(X^{p-1} - 1, f)$.

More details about the factorization of univariate polynomials over finite fields can be found in [42, 75]. Shoup [67] extended Legendre's idea to design a deterministic factoring algorithm for all squarefree polynomials.

5.2 Measures of Pseudorandomness

The following measures of pseudorandomnes were introduced by Mauduit and Sárközy [46]. For a finite binary sequence $E_N = (e_1, \ldots, e_N) \in \{-1, +1\}^N$ the *well-distribution measure* of E_N is defined by

$$W(E_N) = \max_{a,b,M} \left| \sum_{j=1}^{M} e_{a+bj} \right|,$$

where the maximum is taken over all $a, b, M \in \mathbb{Z}$ and $b, M > 0$ such that $1 \leq a + b \leq a + bM \leq N$, and the *correlation measure of order* ℓ of E_N is defined as

$$C_\ell(E_N) = \max_{M,D} \left| \sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} \cdots e_{n+d_\ell} \right|,$$

where the maximum is taken over all $D = (d_1, \ldots, d_\ell)$ and M is such that $0 \leq d_1 < \ldots < d_\ell \leq N - M$.

Let p be an odd prime. The binary sequence $E_p = (1, e_1, \ldots, e_{p-1})$ defined by

$$e_n = \left(\frac{n}{p} \right), \quad 0 \leq n < p,$$

is the *Legendre sequence*.

The sums in the definitions of well-distribution measure and correlation measure of order ℓ for the Legendre sequence are essentially sums of products of Legendre symbols which can be estimated by Theorem 1.

We note that $W(E_N)$ and $C_\ell(E_N)$ of a 'truly random' sequence are up to some logarithmic factor of the order of magnitude $N^{1/2}$, see [1, 13].

Theorem 11 [46]. *For the Legendre sequence E_p we have*

$$W(E_p) \ll p^{1/2}\log p \quad \textit{and} \quad C_\ell(E_p) \ll \ell p^{1/2}\log p.$$

Let $U_N = (u_0,\dots,u_{N-1})$ be a sequence over $\mathbb{F}_q$. The *linear complexity* $L(U_N)$ of U_N (over $\mathbb{F}_q$) is the length L of a shortest linear recurrence

$$u_{n+L} = g_{L-1}u_{n+L-1} + \cdots + g_1 u_{n+1} + g_0 u_n, \quad n = 0,\dots,N-L-1,$$

for some $g_0,\dots,g_{L-1} \in \mathbb{F}_q$.

The linear complexity is a measure for the unpredictability and thus suitability of a sequence in cryptography. For sequences $(u_0,\dots,u_{N-1}) \in \mathbb{F}_2^N$ it is closely related to the correlation measure of order ℓ of the sequence $(e_0,\dots,e_{N-1}) \in \{-1,+1\}^N$ defined by $e_n = (-1)^{u_n}$, $n = 0,\dots,N-1$. Hence, from a suitable upper bound on $C_\ell(E_N)$ up to a sufficiently large ℓ we can derive a lower bound on the linear complexity of (u_n), see [10].

Proposition 5.

$$L(U_N) \geq N - \max_{1\leq \ell \leq L(E_N)+1} C_\ell(E_N).$$

Corollary 2. *For $1 \leq N \leq p$ and the sequence $U_N = (u_0,\dots,u_{N-1}) \in \{0,1\}^N$ derived from the Legendre sequence E_p by $(-1)^{u_n} = e_n$, $n = 0,\dots,p-1$, we have*

$$L(U_N) \gg \frac{N}{p^{1/2}\log p}.$$

We note that the correlation measure of order ℓ is a finer measure of pseudorandomness than autocorrelation and linear complexity. The two-prime generator (v_n) for two given distinct primes p and q is defined by

$$v_n = \left(\frac{n}{p}\right)\left(\frac{n}{q}\right), \quad \gcd(n,pq) = 1,$$

and a suitable choice of v_n if $\gcd(n,pq) > 1$. It can be shown that it has a high linear complexity and a small correlation measure of order ℓ if $\ell = 2$ or ℓ is odd, see [9]. However, choosing the lags $0, p, q, p+q$ we see that the correlation measure of order 4 is close to the length of the sequence.

5.3 Recursive Nonlinear Pseudorandom Number Generators

Finally, we mention an application of incomplete character sums where the standard method of reducing incomplete sums to complete ones fails. We define the

recursive nonlinear pseudorandom number generator (μ_n) of elements of $\mathbb{F}_q$ by the recurrence relation

$$\mu_{n+1} = f(\mu_n), \qquad n = 0, 1, \ldots, \tag{12}$$

with some *initial value* $\mu_0 \in \mathbb{F}_q$. This sequence is eventually periodic with some period $T \le q$. We assume that the sequence (μ_n) is purely periodic. In [50, 58], a method has been presented to study the additive character sums

$$S_{\mathbf{a},N}(f) = \sum_{n=0}^{N-1} \chi\left(\sum_{j=0}^{s-1} \alpha_j \mu_{n+j} \right), \quad 1 \le N \le T,$$

and thus the distribution of such sequences for arbitrary polynomials $f(X)$ where χ is a nontrivial additive character of $\mathbb{F}_q$ and $\mathbf{a} = (\alpha_0, \ldots, \alpha_{s-1}) \in \mathbb{F}_q^s \setminus \{\mathbf{0}\}$, see also the recent survey [81]. More precisely, under some necessary restrictions, say $\gcd(d, p) = 1$, we can prove:

$$S_{\mathbf{a},N}(f) \ll N \left(\log \frac{2q}{N} \right)^{1/2} (\log d)^{1/2} / (\log q)^{1/2}, \quad 1 \le N \le T. \tag{13}$$

Proof. We can assume $N \ge 2q^{1/2}$. We first prove that, for any integer $r \ge 1$ and $\mathbf{0} \ne \mathbf{a} \in \mathbb{F}_q^s$, we have

$$S_{\mathbf{a},N} \ll N r^{1/2} (q/N)^{1/(2r)} (\min\{\log q, r q^{1/(11r)}\})^{-1/2} \tag{14}$$

for $2q^{1/2} \le N \le T$. Since otherwise (14) is trivial, we may assume $r < \log q$.
It is obvious that for any integer $k \ge 0$ we have

$$\left| S_{\mathbf{a},N}(f) - \sum_{n=0}^{N-1} \chi\left(\sum_{j=0}^{s-1} \alpha_j \mu_{n+j+k} \right) \right| \le 2k.$$

Therefore, for any integer $K \ge 1$,

$$K |S_{\mathbf{a},N}(f)| \le W + K(K-1), \tag{15}$$

where

$$W = \sum_{n=0}^{N-1} \left| \sum_{k=0}^{K-1} \chi\left(\sum_{j=0}^{s-1} \alpha_j \mu_{n+j+k} \right) \right|.$$

We consider the sequence of polynomials $f_k(X) \in \mathbb{F}_q[X]$ defined by

$$f_0(X) = X, \quad f_k(X) = f(f_{k-1}(X)), \quad k \ge 1.$$

By the Hölder inequality, using $\mu_{n+k} = f_k(\mu_n)$ and putting

$$F_k(X) = \sum_{j=0}^{s-1} \alpha_j f_{k+j}(X),$$

we obtain

$$\begin{aligned} W^{2r} &\le N^{2r-1} \sum_{n=0}^{N-1} \left| \sum_{k=0}^{K-1} \chi(F_k(\mu_n)) \right|^{2r} \le N^{2r-1} \sum_{x \in \mathbb{F}_q} \left| \sum_{k=0}^{K-1} \chi(F_k(x)) \right|^{2r} \\ &\le N^{2r-1} \sum_{k_1,\ldots,k_{2r}=0}^{K-1} \left| \sum_{x \in \mathbb{F}_q} \chi(F_{k_1,\ldots,k_{2r}}(x)) \right|, \end{aligned}$$

where $F_{k_1,\ldots,k_{2r}}(X) = F_{k_1}(X) + \ldots + F_{k_r}(X) - F_{k_{r+1}}(X) - \ldots - F_{k_{2r}}(X)$. If

$$\{k_1, \ldots, k_r\} = \{k_{r+1}, \ldots, k_{2r}\}$$

as multisets, then $F_{k_1,\ldots,k_{2r}}(X)$ is constant and the inner sum is trivially equal to q. There are at most $r!K^r \le r^r K^r$ such sums. Otherwise note that the degree of $F_{k_1,\ldots,k_{2r}}$ is not divisible by p since $\gcd(d,p) = 1$ and we can apply Weil's bound to the inner sum using $\deg(F_{k_1,\ldots,k_{2r}}) \le d^{K+s-2}$, to get the upper bound $d^{K+s-2}q^{1/2}$ for at most K^{2r} sums. Hence,

$$W^{2r} \le r^r K^r N^{2r-1} q + d^{K+s-2} K^{2r} N^{2r-1} q^{1/2}. \tag{16}$$

Choose

$$K = \min\left\{ \left\lceil 0.4 \frac{\log q}{\log d} \right\rceil, \left\lfloor rq^{1/(11r)} \right\rfloor \right\}.$$

Then it is easy to see that the first term on the right hand side of (16) dominates the second one in terms of the order of magnitude in q, and we get (14) from (15) and (16) after simple calculations. Finally, we choose

$$r = \lfloor \log(q/N) \rfloor + 1$$

and the theorem follows after simple calculations from (14). □

In two special cases of (12), nonlinear generators with small *p-weight degree* [35] and *inversive generators* [51], modifications of the method in the proof of (13) lead to stronger bounds. For other special classes of polynomials, namely for *monomials* and *Dickson polynomials*, an alternative approach, producing much stronger bounds has been proposed, see the survey [81] and references therein. Related results for sequences produced by *Rédei functions* are obtained in [31].

Acknowledgments

The author wishes to thank Domingo Gomez, Gottlieb Pirsic, and Igor Shparlinski for a careful reading of the manuscript and many useful comments.

References

[1] N. Alon, Y. Kohayakawa, C. Mauduit, C. G. Moreira, and V. Rödl. Measures of pseudorandomness for finite sequences: typical values. *Proc. Lond. Math. Soc. (3)*, 95(3):778–812, 2007.

[2] H. T. Banks and K. Kunisch. *Estimation techniques for distributed parameter systems*, volume 1 of *Systems & Control: Foundations & Applications*. Birkhäuser Boston Inc., Boston, MA, 1989.

[3] B. C. Berndt, R. J. Evans, and K. S. Williams. *Gauss and Jacobi sums*. Canadian Mathematical Society Series of Monographs and Advanced Texts. John Wiley & Sons Inc., New York, 1998.

[4] T. Beth, D. Jungnickel, and H. Lenz. *Design theory*. Cambridge University Press, 1986.

[5] D. Boneh and R. Venkatesan. Rounding in lattices and its cryptographic applications. In *Proceedings of the Eighth Annual ACM-SIAM Symposium on Discrete Algorithms (New Orleans, LA, 1997)*, pages 675–681, New York, 1997. ACM.

[6] D. Boneh and R. Venkatesan. Breaking RSA may not be equivalent to factoring (extended abstract). In *Advances in cryptology—EUROCRYPT '98 (Espoo)*, volume 1403 of *Lecture Notes in Comput. Sci.*, pages 59–71. Springer, Berlin, 1998.

[7] J. Bourgain. Multilinear exponential sums in prime fields under optimal entropy condition on the sources. *Geom. Funct. Anal.*, 18(5):1477–1502, 2009.

[8] J. Bourgain, A. A. Glibichuk, and S. V. Konyagin. Estimates for the number of sums and products and for exponential sums in fields of prime order. *J. London Math. Soc. (2)*, 73(2):380–398, 2006.

[9] N. Brandstätter and A. Winterhof. Some notes on the two-prime generator of order 2. *IEEE Trans. Inform. Theory*, 51(10):3654–3657, 2005.

[10] N. Brandstätter and A. Winterhof. Linear complexity profile of binary sequences with small correlation measure. *Period. Math. Hungar.*, 52(2):1–8, 2006.

[11] A. T. Butson. Generalized Hadamard matrices. *Proc. Amer. Math. Soc.*, 13:894–898, 1962.

[12] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction and orthogonal geometry. *Phys. Rev. Lett.*, 78(3):405–408, 1997.

[13] J. Cassaigne, C. Mauduit, and A. Sárközy. On finite pseudorandom binary sequences. VII. The measures of pseudorandomness. *Acta Arith.*, 103(2):97–118, 2002.

[14] Z. Chen, D. Gomez, and A. Winterhof. Distribution of digital explicit inversive pseudorandom numbers and their binary threshold sequence. In *Monte Carlo and quasi-Monte Carlo methods 2008*, pages 249–258. Springer, Berlin, 2009.

[15] Z. Chen, A. Ostafe, and A. Winterhof. Structure of pseudorandom numbers derived from Fermat quotients. In *Arithmetic of finite fields*, volume 6087 of *Lecture Notes in Comput. Sci.*, pages 73–85. Springer, Berlin, 2010.
[16] J. A. Cipra. Waring's number in a finite field. *Integers*, 9:A34, 435–440, 2009.
[17] T. Cochrane, C. Pinner, and J. Rosenhouse. Bounds on exponential sums and the polynomial Waring problem mod p. *J. London Math. Soc. (2)*, 67(2):319–336, 2003.
[18] H. Davenport and D. J. Lewis. Character sums and primitive roots in finite fields. *Rend. Circ. Mat. Palermo (2)*, 12:129–136, 1963.
[19] G. Dorfer, W. Meidl, and A. Winterhof. Counting functions and expected values for the lattice profile at n. *Finite Fields Appl.*, 10(4):636–652, 2004.
[20] G. Dorfer and A. Winterhof. Lattice structure and linear complexity profile of nonlinear pseudorandom number generators. *Appl. Algebra Engrg. Comm. Comput.*, 13(6):499–508, 2003.
[21] G. Dorfer and A. Winterhof. Lattice structure of nonlinear pseudorandom number generators in parts of the period. In *Monte Carlo and quasi-Monte Carlo methods 2002*, pages 199–211. Springer, Berlin, 2004.
[22] C. C. Douglas, G. Haase, and U. Langer. *A tutorial on elliptic PDE solvers and their parallelization*, volume 16 of *Software, Environments, and Tools*. Society for Industrial and Applied Mathematics, Philadelphia, 2003.
[23] M. Drmota and R. F. Tichy. *Sequences, discrepancies and applications*, volume 1651 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1997.
[24] H. W. Engl. *Integralgleichungen*. Springer Lehrbuch Mathematik. [Springer Mathematics Textbook]. Springer-Verlag, Vienna, 1997.
[25] B.-G. Englert and Y. Aharonov. The mean king's problem: prime degrees of freedom. *Phys. Lett. A*, 284(1):1–5, 2001.
[26] A. B. Evans. *Orthomorphism graphs of groups*, volume 1535 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1992.
[27] A. A. Glibichuk. Sums of powers of subsets of an arbitrary finite field. *Izv. RAN. Ser. Mat.*, (75):35–68, 2011.
[28] S. W. Golomb and G. Gong. *Signal design for good correlation*. Cambridge University Press, 2005.
[29] D. Gomez and A. Winterhof. Waring's problem in finite fields with Dickson polynomials. In *Finite fields: theory and applications*, volume 518 of *Contemp. Math.*, pages 185–192. Amer. Math. Soc., Providence, RI, 2010.
[30] D. Gottesman. Class of quantum error-correcting codes saturating the quantum Hamming bound. *Phys. Rev. A (3)*, 54(3):1862–1868, 1996.
[31] J. Gutierrez and A. Winterhof. Exponential sums of nonlinear congruential pseudorandom number generators with Rédei functions. *Finite Fields Appl.*, 14(2):410–416, 2008.
[32] D. R. Heath-Brown and S. Konyagin. New bounds for Gauss sums derived from kth powers, and for Heilbronn's exponential sum. *Q. J. Math.*, 51(2):221–235, 2000.
[33] T. Helleseth. On the covering radius of cyclic linear codes and arithmetic codes. *Discrete Appl. Math.*, 11(2):157–173, 1985.
[34] K. J. Horadam. *Hadamard matrices and their applications*. Princeton University

Press, 2007.

[35] Á. Ibeas and A. Winterhof. Exponential sums and linear complexity of nonlinear pseudorandom number generators with polynomials of small p-weight degree. *Unif. Distrib. Theory*, 5(1):79–93, 2010.

[36] T. Itoh and S. Tsujii. A fast algorithm for computing multiplicative inverses in GF(2^m) using normal bases. *Inform. and Comput.*, 78(3):171–177, 1988.

[37] I. D. Ivanović. Geometrical description of quantal state determination. *J. Phys. A*, 14(12):3241–3245, 1981.

[38] H. Iwaniec and E. Kowalski. *Analytic number theory*, volume 53 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2004.

[39] H. Kharaghani and B. Tayfeh-Rezaie. A Hadamard matrix of order 428. *J. Combin. Des.*, 13(6):435–440, 2005.

[40] A. Klappenecker and M. Rötteler. Constructions of mutually unbiased bases. In *Finite fields and applications*, pages 137–144. Springer, Berlin, 2004.

[41] S. V. Konyagin. Estimates for Gaussian sums and Waring's problem modulo a prime. *Trudy Mat. Inst. Steklov.*, 198:111–124, 1992.

[42] T. Lange and A. Winterhof. Factoring polynomials over arbitrary finite fields. *Theoret. Comput. Sci.*, 234(1-2):301–308, 2000.

[43] A. M. Legendre. Recherches d'analyse indeterminee. *Memoires Acad. Sci. Paris*, pages 465–559, 1785.

[44] V. Levenshtein. Application of Hadamard matrices to a problem of coding theory. *Problemy Kibernetiki*, 5:123–136, 1961.

[45] R. Lidl and H. Niederreiter. *Finite Fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, second edition, 1997.

[46] C. Mauduit and A. Sárközy. On finite pseudorandom binary sequences. I. Measure of pseudorandomness, the Legendre symbol. *Acta Arith.*, 82(4):365–377, 1997.

[47] W. Meidl and A. Winterhof. On the autocorrelation of cyclotomic generators. In *Finite fields and applications*, pages 1–11. Springer, Berlin, 2004.

[48] H. Niederreiter. On the distribution of pseudo-random numbers generated by the linear congruential method. II. *Math. Comp.*, 28:1117–1132, 1974.

[49] H. Niederreiter. *Random number generation and quasi-Monte Carlo methods*, volume 63 of *CBMS-NSF Regional Conference Series in Applied Mathematics*. Society for Industrial and Applied Mathematics, Philadelphia, 1992.

[50] H. Niederreiter and I. E. Shparlinski. On the distribution and lattice structure of nonlinear congruential pseudorandom numbers. *Finite Fields Appl.*, 5(3):246–253, 1999.

[51] H. Niederreiter and I. E. Shparlinski. On the distribution of pseudorandom numbers and vectors generated by inversive methods. *Appl. Algebra Engrg. Comm. Comput.*, 10(3):189–202, 2000.

[52] H. Niederreiter and A. Winterhof. Incomplete exponential sums over finite fields and their applications to new inversive pseudorandom number generators. *Acta Arith.*, 93(4):387–399, 2000.

[53] H. Niederreiter and A. Winterhof. On a new class of inversive pseudorandom numbers for parallelized simulation methods. *Period. Math. Hungar.*, 42(1-2):77–87,

2001.

[54] H. Niederreiter and A. Winterhof. On the lattice structure of pseudorandom numbers generated over arbitrary finite fields. *Appl. Algebra Engrg. Comm. Comput.*, 12(3):265–272, 2001.

[55] H. Niederreiter and A. Winterhof. Lattice structure and linear complexity of nonlinear pseudorandom numbers. *Appl. Algebra Engrg. Comm. Comput.*, 13(4):319–326, 2002.

[56] H. Niederreiter and A. Winterhof. Cyclotomic R-orthomorphisms of finite fields. *Discrete Math.*, 295(1-3):161–171, 2005.

[57] H. Niederreiter and A. Winterhof. On the structure of inversive pseudorandom number generators. In *Applied algebra, algebraic algorithms and error-correcting codes*, pages 208–216. Springer, Berlin, 2007.

[58] H. Niederreiter and A. Winterhof. Exponential sums for nonlinear recurring sequences. *Finite Fields Appl.*, 14(1):59–64, 2008.

[59] A. Ostafe and I. E. Shparlinski. On the Waring problem with Dickson polynomials in finite fields. *Proc. Amer. Math. Soc.*, 139(11):3815–3820, 2011.

[60] R. Paley. On orthogonal matrices. *J. Math. Phys., Mass. Inst. Techn.*, 12:311–320, 1933.

[61] G. Pirsic and A. Winterhof. On the structure of digital explicit nonlinear and inversive pseudorandom number generators. *J. Complexity*, 26(1):43–50, 2010.

[62] M. Planat, H. C. Rosu, and S. Perrine. A survey of finite algebraic geometrical structures underlying mutually unbiased quantum measurements. *Found. Phys.*, 36(11):1662–1680, 2006.

[63] W. Schmidt. *Equations over finite fields: an elementary approach*. Kendrick Press, Heber City, UT, second edition, 2004.

[64] R.-H. Schulz. Check character systems and anti-symmetric mappings. In *Computational discrete mathematics*, volume 2122 of *Lecture Notes in Comput. Sci.*, pages 136–147. Springer, Berlin, 2001.

[65] J. Schwinger. Unitary operator bases. *Proc. Nat. Acad. Sci. U.S.A.*, 46:570–579, 1960.

[66] R. Shaheen and A. Winterhof. Permutations of finite fields for check digit systems. *Des. Codes Cryptogr.*, 57(3):361–371, 2010.

[67] V. Shoup. On the deterministic complexity of factoring polynomials over finite fields. *Inform. Process. Lett.*, 33(5):261–267, 1990.

[68] I. E. Shparlinski. *Finite fields: theory and computation*, volume 477 of *Mathematics and its Applications*. Kluwer Academic Publishers, Dordrecht, 1999.

[69] I. Shparlinski. *Cryptographic applications of analytic number theory*, volume 22 of *Progress in Computer Science and Applied Logic*. Birkhäuser Verlag, Basel, 2003.

[70] I. Shparlinski and A. Winterhof. Noisy interpolation of sparse polynomials in finite fields. *Appl. Algebra Engrg. Comm. Comput.*, 16(5):307–317, 2005.

[71] I. E. Shparlinski. Playing 'hide-and-seek' with numbers: the hidden number problem, lattices and exponential sums. In *Public-key cryptography*, volume 62 of *Proc. Sympos. Appl. Math.*, pages 153–177. Amer. Math. Soc., Providence, RI, 2005.

[72] I. E. Shparlinski and A. Winterhof. Constructions of approximately mutually unbiased bases. In *LATIN 2006: Theoretical informatics*, volume 3887 of *Lecture Notes*

in Comput. Sci., pages 793–799. Springer, Berlin, 2006.

[73] A. Topuzoğlu and A. Winterhof. Pseudorandom sequences. In *Topics in geometry, coding theory and cryptography*, volume 6 of *Algebr. Appl.*, pages 135–166, Springer, Dordrecht, 2007.

[74] J. Verhoeff. *Error detecting decimal codes*. Mathematical Centre Tracts, No. 29. Mathematisch Centrum, Amsterdam, 1969.

[75] J. von zur Gathen and D. Panario. Factoring polynomials over finite fields: a survey. *J. Symbolic Comput.*, 31(1-2):3–17, 2001. Computational algebra and number theory (Milwaukee, WI, 1996).

[76] A. Winterhof. On the distribution of powers in finite fields. *Finite Fields Appl.*, 4(1):43–54, 1998.

[77] A. Winterhof. On Waring's problem in finite fields. *Acta Arith.*, 87(2):171–177, 1998.

[78] A. Winterhof. On the non-existence of generalized Hadamard matrices. *J. Statist. Plann. Inference*, 84(1-2):337–342, 2000.

[79] A. Winterhof. Incomplete additive character sums and applications. In *Finite fields and applications (Augsburg, 1999)*, pages 462–474. Springer, Berlin, 2001.

[80] A. Winterhof. Some estimates for character sums and applications. *Des. Codes Cryptogr.*, 22(2):123–131, 2001.

[81] A. Winterhof. Recent results on recursive nonlinear pseudorandom number generators (invited paper). In *Sequences and their applications—SETA 2010*, volume 6338 of *Lecture Notes in Comput. Sci.*, pages 113–124. Springer, Berlin, 2010.

[82] W. K. Wootters and B. D. Fields. Optimal state-determination by mutually unbiased measurements. *Ann. Physics*, 191(2):363–381, 1989.

Author's address:

Arne Winterhof
Johann Radon Institute for Computational and Applied Mathematics
Austrian Academy of Sciences
Altenbergerstr. 69, 4040 Linz
email arne.winterhof@oeaw.ac.at

Internat. Math. Nachrichten
Nr. 220 (2012), 29–39

Einige Bemerkungen zum Format von Multiple Choice-Aufgaben: eine Replik

Stefan Götz und Hans-Stefan Siller

Universität Wien, Universität Koblenz-Landau

Im Beitrag von H. Humenberger und G. Kirchner in den IMN *Nr. 217 wird mit einem einfachen Modell nachgewiesen, dass die Wahl des Formats bei Multiple Choice-Aufgaben Einfluss auf die Lösungshäufigkeit bei denselben haben kann. Daher sollen nur mit größter Vorsicht Rückschlüsse auf das Können der Population gezogen werden, die solche Aufgaben bearbeitet hat. Zwei Aspekte zur Begründung dieser Schlussfolgerungen werden dazu diskutiert: die Möglichkeit des Ratens bei Nichtwissen der richtigen Antworten und der geforderte Anteil an richtigen Antworten unter den vorgegebenen. Beide sollen hier im Sinne einer Ergänzung teils bestätigt, teils aber auch relativiert werden. Vor allem aber geht es in dieser Replik darum, die eigentlichen fachdidaktischen Hintergründe und Überlegungen zu dieser Frage oder Problemstellung zu beleuchten.*

1 Einleitung

Zwei wesentliche Neuerungen stehen dem österreichischen Mathematikunterricht bevor: zum einen die Einführung der Bildungsstandards für die achte Schulstufe [8] ab 2011/12, zum anderen die der standardisierten schriftlichen Reifeprüfung, basierend auf sogenannten Grundkompetenzen (vgl. [7], dieses Konzept wurde überarbeitet [1]); sie wird ab 2013/14 österreichweit zentral an AHS gestellt werden. In den eben zitierten Dokumenten finden sich Multiple Choice-Aufgaben, die ebenfalls eine Neuerung darstellen. In Vorbereitung der standardisierten Reifeprüfung ist ein Schulversuch eingerichtet worden, im Zuge dessen die involvierten Klassen nach dem zugrundeliegenden Grundkompetenzenkonzept getestet werden. Vier Pilottestungen und eine Feldtestung sind bereits passiert. Die Aufgabenstellungen sind veröffentlicht worden, ebenso die Lösungshäufigkeiten [12].

ISSN 0020-7926

Im Beitrag von H. Humenberger und G. Kirchner [6] werden nun zwei solche Aufgaben, die sich beide in [12, Testheft A2] befinden, herausgegriffen. Bei der einen aus dem Themenbereich *Quadratische Gleichungen* müssen vier Aussagen durch Ankreuzen als „zutreffend“ oder „nicht zutreffend“ bewertet werden, bei der anderen aus dem Themenbereich *Eigenschaften von Funktionen* stehen fünf Aussagen zur gleichen Beurteilung wie eben durch die Schülerinnen und Schüler an. Ein in [6] diskutierter Unterschied zwischen den beiden Aufgaben liegt nun darin, dass bei der erstgenannten alle vier Kreuze richtig gesetzt werden müssen, um die Aufgabe insgesamt richtig gelöst zu haben, bei der zweiten dagegen nur vier von den fünf. Die Lösungsquote bei den sogenannten Pilotklassen (sie wurden hinsichtlich der Erarbeitung der Grundkompetenzen vom Projektteam [7] betreut, im Unterschied zu den Vergleichsklassen) beträgt bei der ersten Aufgabe ca. 30%, bei der zweiten 74% ([12], dort finden sich auch die Lösungsquoten der Vergleichsklassen, die spielen aber hier keine Rolle). Kann man daraus schließen, dass das Themenfeld *Eigenschaften von Funktionen* besser gekonnt wird als jenes, das *Quadratische Gleichungen* zum Inhalt hat?

Im Folgenden wird nun auf die Argumente und Sichtweisen in [6] im Einzelnen eingegangen, die ebendort im Zuge des Vergleichs dieser beiden Aufgaben angeführt werden.

2 Zur Lösewahrscheinlichkeit von Multiple Choice-Aufgaben

Wenn wir „4 von 4-Aufgaben“ mit „4 aus 5-Aufgaben“ vergleichen, so ist anschaulich klar, dass die erste Forderung schwieriger zu erfüllen ist als die zweite. In [6] wird dies mit einem Binomialmodell noch unterstrichen. Unterstellen wir eine konstante Wahrscheinlichkeit p für das Wissen der richtigen Antwort für jede zu bewertende Aussage innerhalb einer Aufgabe, dann ist $\mathrm{P}(X=4)=p^4=:f(p)$ die Wahrscheinlichkeit, eine „4 von 4-Aufgabe“ richtig zu beantworten. Die Zufallsvariable X zählt dabei die richtigen Antworten bei einer solchen Aufgabe. Analog ist $\mathrm{P}(Y\geq 4)=\binom{5}{4}p^4(1-p)+p^5=:g(p)$ die entsprechende Wahrscheinlichkeit bei einer „4 aus 5-Aufgabe“.

Zuerst halten wir fest, dass $g(p)>f(p)$ ist für alle $p\in(0,1)$. In [6, S. 53] wird dazu der Graph von $f(\frac{1+p}{2})$ mit dem von $g(\frac{1+p}{2})$ verglichen. Das spezielle Argument $\frac{1+p}{2}$ von f bzw. g kommt daher, dass dort noch die Erratewahrscheinlichkeit von $\frac{1}{2}$ zur unterstellten Wissenswahrscheinlichkeit p dazukommt: $p+(1-p)\cdot\frac{1}{2}$ ist dann die Wahrscheinlichkeit, eine bestimmte Aussage richtig zu bewerten. Analytisch sieht man leicht, dass die obige Ungleichung o.B.d.A. *für alle* p aus $(0,1)$ gilt: $5p^4(1-p)+p^5>p^4$ kann mittels elementarer Äquivalenzumformungen zu $p^4>p^5$ vereinfacht werden; diese Ungleichung ist zweifellos richtig.

Weiters sind f und g auf $(0,1)$ streng monoton wachsend, wie man durch Berechnung der ersten Ableitung ebenfalls leicht sieht. Das heißt also zusätzliches Raten

bei Nichtwissen erhöht die Wahrscheinlichkeit, eine Aufgabe richtig zu beantworten. Damit steigt auch der Anreiz, zu raten, wenn falsches Raten nicht sanktioniert wird.

Interessant wird es nun, wenn f und g mit der ersten Mediane verglichen werden. Übersetzt in den inhaltlichen Kontext, bedeutet das natürlich, die Frage zu untersuchen, ob das Aufgabenformat bei gegebenem Wissen p die zugehörige Versuchsperson unterstützt ($f(p)$ bzw. $g(p) > p$) oder hemmt ($f(p)$ bzw. $g(p) < p$). In [6, S. 53] sieht man anhand der dort gezeichneten Funktionsgraphen von f und g, dass „4 aus 5-Aufgaben“ systematisch bevorzugen, die „4 von 4“-Aufgaben dagegen (bis auf sehr kleine p) benachteiligen. Beide Erkenntnisse gelten für eine Lösewahrscheinlichkeit von $\frac{1+p}{2}$ pro Aussage.

Wir wollen nun diese Aussagen analytisch erhärten. Es ist erstens $f(\frac{1+p}{2}) = (\frac{1+p}{2})^4 < p$ genau dann, wenn $p^4+4p^3+6p^2-12p+1<0$ ist. Der Grad der zugehörigen Gleichung kann um eins reduziert werden, wenn wir die Lösung $p_1 = 1$ abspalten. Es bleibt die kubische Gleichung $p^3+5p^2+11p-1=0$ zu lösen. Mittels Cardano und Computeralgebrasystem erhalten wir

$$p_2 = \frac{1}{3}\Big(2\sqrt[3]{3\sqrt{33}+17} - 2\sqrt[3]{3\sqrt{33}-17} - 5\Big) \approx 0.08738.$$

Die anderen beiden Lösungen sind nicht reell. Damit ist die numerische Aussage, für „$p >$ ca. 0.1“ tritt eine systematische Benachteiligung bei den „4 von 4-Aufgaben“ ein [6, S. 53], analytisch verifiziert, wenn wir uns $f(\frac{1+0}{2}) = f(\frac{1}{2}) = \frac{1}{16} > 0$ vor Augen halten.

Zweitens gelingt es in ganz anderer Weise, die Aussage

$$g\Big(\frac{1+p}{2}\Big) = \frac{1}{16}(1+p)^4(3-2p) > p \quad \text{für alle } p \in (0,1)$$

zu beweisen. Sie ist äquivalent zu

$$j(p) := 3+10p^2-6p-5p^4-2p^5 > 0 \quad \forall\, p \in (0,1)\ .$$

Diese Ungleichung können wir so einsehen:

$$j(p) = 3+10p^2-(2p^5+5p^4+6p) = \underbrace{3+3p^2-6p}_{=3+3p(p-2)>3+3\cdot(-1)=0} + \underbrace{7p^2-2p^5-5p^4}_{>7p^2-2p^2-5p^2=0}\ .$$

Die erste Abschätzung erhalten wir durch Betrachten von $k(p) := p(p-2) < 0$ für alle $p \in (0,1)$. Es ist $k(p) = p^2-2p = p^2-2p+1-1 = (p-1)^2-1$. Jetzt ist klar, dass k für $p = 1$ minimal wird.

Wie ist die Situation aber, wenn wir die Lösungswahrscheinlichkeit p pro Aussage voraussetzen, also die Ratemöglichkeit ignorieren? Für die Funktion f ergibt sich

die zu verifizierende Ungleichung $f(p) = p^4 < p$ für alle $p \in (0,1)$. Hier ändert sich also bis auf das (kleine) Intervall $[0, p_2)$ zumindest qualitativ nichts.

Bei den „4 aus 5-Aufgaben“ ist der Sachverhalt etwas schwieriger zu analysieren: Es ist $g(p) = 5p^4(1-p) + p^5 > p$ gleichbedeutend mit $p^4(5-4p) > p$ und Division durch $p > 0$ liefert schließlich $h(p) := p^3(5-4p) > 1$, wir betrachten $i(p) := p^3(5-4p) - 1$. Wegen $i(1) = 0$ können wir den Linearfaktor $(p-1)$ abspalten und bekommen $j(p) := -4p^3 + p^2 + p + 1$. Noch einmal bemühen wir Cardano und ein Computeralgebrasystem, um

$$p_3' = \frac{1}{12}\left(\sqrt[3]{6\sqrt{1473}+235} - \sqrt[3]{6\sqrt{1473}-235} + 1\right) \approx 0.868877$$

zu berechnen. Das bedeutet also, dass $g(p) > p$ nur für das Intervall $(0.87, 1)$ gilt. (Die beiden anderen Lösungen von $j(p) = 0$ sind nicht reell.) Für den überwiegenden Teil von Lösungswahrscheinlichkeiten p (zwischen null und 0.86) benachteiligen auch die „4 aus 5-Aufgaben“, wenn wir nicht die Ratemöglichkeit berücksichtigen. Die Bevorzugung ist also weniger ein Effekt des Antwortformats (zumindest im engeren Sinn), als der zusätzlichen Möglichkeit, zu raten.

Als kleine Fingerübung überlegen wir uns abschließend, dass im Extremfall „*nur zwei Aussagen, mindestens eine muss richtig angekreuzt werden, um die Aufgabe als richtig zu werten*“, also bei einer „1 aus 2-Aufgabe“, auch ohne Rateoption eine systematische Bevorzugung für alle $p \in (0,1)$ eintritt. Es ist dann $\tilde{g}(p) := p^2 + p(1-p) \cdot 2 = 2p - p^2$. Die Ungleichung $\tilde{g}(p) > p$ ist dann äquivalent zu $p < 1$.

Zusammenfassend können wir also sagen, dass die „n von n-Aufgaben“ jedenfalls systematisch benachteiligen, wenn die Ratemöglichkeit nicht berücksichtigt wird, das heißt $f_n(p) := p^n < p$ für alle $p \in (0,1)$ und $n > 1$.

Ist dagegen die Ratewahrscheinlichkeit $\frac{1}{2}$ pro nicht gewusster Aussagenbewertung mit im Spiel, dann müssen wir im Wesentlichen die Gleichung $f_n(\frac{1+p}{2}) = p$ lösen, was $(1+p)^n = 2^n \cdot p$ bzw. $1 - 2\sqrt[n]{p} + p = 0$ für $n \geq 2$ bedeutet, um die Bevorzugungsintervalle für p von den benachteiligenden Bereichen von p zu trennen. Die folgende Tabelle gibt die oberen Grenzen p_n für $2 \leq n \leq 8$ der Bevorzugungsintervalle näherungsweise an, die untere Grenze ist immer null:

n	2	3	4	5	6	7	8
p_n	1	0.24	0.09	0.04	0.02	0.01	0

.

Wir sehen, dass diese mit wachsendem n immer kleiner werden. Das heißt, je mehr Aussagen in einer Aufgabe zu bewerten sind, desto weniger hilft der Rateeffekt, eine systematische Bevorzugung zu erzielen.

Bei den „$n-1$ aus n-Aufgaben“ ist die Situation komplexer: Für $n = 5$ haben wir gesehen, dass mit Rateoption eine systematische Bevorzugung der Fall ist, ohne

diese nur für ein kleines p-Intervall. Bei $n = 2$ ist systematische Bevorzugung mit oder ohne Ratemöglichkeit gegeben.

Nur der Vollständigkeit halber: Bei „2 aus 3-Aufgaben“ (also $n = 3$) wird systematisch für $p \in (\frac{1}{2}, 1)$ bevorzugt, wenn nicht geraten wird, sonst immer. Last, but not least: Für „3 aus 4-Aufgaben“ (das heißt $n = 4$) wird für $p \in (0, 0.77)$ systematisch benachteiligt, wenn die Ratewahrscheinlichkeit $\frac{1}{2}$ für jede Aussage keine Rolle spielt; sonst wieder systematische Bevorzugung für alle $p \in (0, 1)$. Wir sehen also, dass das Raten als zusätzliche Möglichkeit in den hier diskutierten Fällen jedenfalls eine systematische Bevorzugung bringt. Ohne Raten wird das p-Intervall, das Bevorzugung mit sich bringt, immer kleiner mit wachsendem n ($2 \leq n \leq 5$).

Es zeigt sich somit, dass selbst ein so vereinfachendes Modell wie das in Rede stehende Differenzierungen in sich birgt, die man auf den ersten Blick vielleicht gar nicht vermuten würde. Aus unserer Sicht handelt es sich hierbei um ein Musterbeispiel für eine „eingekleidete“ Aufgabe; das sind solche, die mathematische Probleme in die Sprache des Alltags einbetten (vgl. [9, S. 67]). Dabei gelingt es, die Ergebnisse im ursprünglichen Kontext zu deuten. Paradebeispiel hierfür sind die meisten Extremwertaufgaben, die man in gängigen Schulbüchern findet. In diesem Zusammenhang ist ein neuer Begriff in der Fachdidaktik eingeführt worden: „Inverse Modellierung“; damit werden Aufgaben bezeichnet, bei denen Mathematik bewusst in das Außermathematische übersetzt wird, um mathematische Inhalte deutlicher zu machen.

> „Somit wird nicht die Realität durch die Mathematik, sondern Mathematik durch die Realität mit dem Ziel modelliert, mathematische Sachverhalte in dem Anschauungsraum des Denkenden bzw. Lernenden zu vernetzen [...]“ [10, S. 66].

Genau das ist hier passiert, wobei nicht stochastische Inhalte im Vordergrund standen (sie waren quasi nur Einkleidung „zweiter Ordnung“), sondern eigentlich analytische und algebraische.

Die primäre Intention in [6] ist aber wohl eine andere: Es soll vor der vorschnellen Interpretation von Erfolgsquoten bei einzelnen Aufgaben gewarnt werden. Und davon wird im nächsten Abschnitt die Rede sein.

3 Zum Vergleich von Erfolgsquoten bei Multiple Choice-Aufgaben

In [12] sind die durchschnittlichen Erfolgsquoten der Pilotklassen und der Vergleichsklassen für jede im Schulversuch getestete Aufgabe ausgewiesen, in der Einleitung haben wir diese für die beiden in [6] behandelten Aufgaben angegeben. Ein wesentlicher Punkt in [6] ist nun dieser: Wenn die bekannte Erfolgsquote

q einer Aufgabe gleich $f(\frac{1+p}{2})$ bzw. $g(\frac{1+p}{2})$ gesetzt wird, dann kann die Wissenswahrscheinlichkeit p für jede Aussage innerhalb dieser bestimmten Aufgabe berechnet („geschätzt“) werden. Konkret ergibt sich bei jener über quadratische Gleichungen ein p von ungefähr 0.48 und bei jener über Eigenschaften von Funktionen ein p von circa 0.60. Die Lösewahrscheinlichkeit $\frac{1+p}{2}$ pro Aussage innerhalb einer Aufgabe ist dann 0.74 bzw. 0.8. Das heißt 26% bzw. 20% der richtig angekreuzten Aussagen wurden erraten (allgemein $\frac{1-p}{2}$).

Wenn nun, wird in [6] weiter argumentiert, die Antwortformate der beiden in Rede stehenden Aufgaben vertauscht werden würden, dann ergäbe sich mit $p = 0.48$ eine Erfolgsquote q von 61% bei der Aufgabe über quadratische Gleichungen, die jetzt im „4 aus 5-Format“ getestet werden würde. Die Aufgabe über Eigenschaften von Funktionen hingegen hätte in einem „4 von 4-Format“ eine Erfolgsquote q von nur mehr 41%, wenn $p = 0.60$ unverändert gelassen wird [6, S. 52]. Aus dem Erfolgsquotenpaar $(0.30, 0.74)$ würde also ein Paar $(0.61, 0.41)$. In [6, S. 52] wird von „Umkehr“ gesprochen, daher sagen die Erfolgsquoten q allein wenig über die tatsächlichen Defizite im Mathematikunterricht aus. Das ist die zentrale Botschaft in [6].

Es wird ebendort daraus gefolgert und gefordert, mehr offene Aufgabenformate zu verwenden, um die mathematische Kompetenz einer bestimmten Population in einem gewissen Gebiet der Schulmathematik zu eruieren. Multiple Choice-Aufgaben sollten bei der zentralen schriftlichen Reifeprüfung in Mathematik wegen mangelnder Aussagekraft (Raten, Antwortformat) keine dominierende Rolle spielen, obwohl:

> „Der Druck vonseiten Psychologie, Bildungswissenschaft, Testtheorie, etc. wird da in Zukunft sicher sehr stark sein, Multiple Choice-Aufgaben zu favorisieren; aus fachlicher bzw. fachdidaktischer Sicht sollen diese aber nicht das Hauptgewicht bekommen.“ [6, S. 54]

Aus entsprechenden Publikationen des *bifie* gehen folgende testtheoretische Implikationen hervor:

> „Hauptziel der neuen Reife- und Diplomprüfung ist die Gewährleistung von Objektivität. *Objektivität* ist gewährleistet, wenn die beiden zentralen Kriterien der Reliabilität und Validität erfüllt sind. Die Erfüllung dieser beiden Kriterien ist ein Hauptanliegen der neuen Reifeprüfung.
>
> *Reliabilität* bedeutet Zuverlässigkeit. Das Ergebnis der Prüfung einer Kandidatin/eines Kandidaten soll nicht davon abhängen, wer oder wann und an welchem Ort beurteilt wird. Das Ergebnis soll auch nicht davon abhängen, welche Aufgabe gestellt wurde, sondern soll dasselbe sein, auch wenn eine andere – vergleichbare – Aufgabe gestellt würde.

> *Validität* setzt Reliabilität voraus. Validität ist gewährleistet, wenn die Prüfung jene Fähigkeiten misst, die gemessen werden sollen.“ ([2, S. III], Hervorhebungen im Original).

So weit, so gut. Mittels testtheoretischer Unterstützung werden also im Rahmen der standardisierten schriftlichen Reifeprüfung aus Mathematik stichprobenunabhängige (Aufgaben-)Kennwerte (u.a. die Lösungshäufigkeit jeder einzelnen getesteten Aufgabe) auf Basis der Feldtestungen zur Verfügung gestellt, welche die Qualität der Aufgaben aus Sicht der Testtheorie wiedergeben – insbesondere hinsichtlich der Einschätzung der Schwierigkeit einer Aufgabe.

Das Primat des zugrundeliegenden fachdidaktischen Konzepts bleibt dabei jedoch unangetastet und steht bei den Entscheidungsträgern und Verantwortlichen außer jeglichen Zweifel. Mithilfe eines solchen „Validitätsfilters“ und der zugrundeliegenden bildungstheoretischen Orientierung können innovative Prüfungsaufgaben, welche mehr als das bloße algorithmische Abarbeiten verlangen, gezielt eingesetzt werden.

Aufgaben, welche den fachlichen bzw. fachdidaktischen – allenfalls psychometrischen – Qualitätsansprüchen genügen, bilden somit den Grundstock für die Zusammenstellung von weitestgehend gleich schwierigen Maturaheften pro Jahr(gang). Mit dem Aufgabenformat hat das jedoch wenig bzw. gar nichts zu tun.

Die Entdeckung des „Umkehrphänomens“, welches in [6, S. 52] festgestellt wird, wird ebendort damit motiviert, dass (österreichweite) niedrige Erfolgsquoten q bei einer bestimmten Aufgabe (z.B. „A201 Aussagen zur quadratischen Gleichung.“) einen Nachholbedarf, dieses Thema betreffend, suggerieren könnten, der nicht gerechtfertigt ist. Umgekehrt könnten hohe Erfolgsquoten q bei einer bestimmten Aufgabe (z.B. „A205 Eigenschaften einer Funktion.“) zum (fälschlichen) Schluss führen, dass dort keinerlei Handlungsbedarf notwendig ist.

Niemand wird so eindimensional denken bzw. folgern. Zunächst müssen die Aufgaben und ihre zugehörigen Lösungsquoten für sich bewertet werden, um etwaige Defizite oder auch „Überflüsse“ feststellen zu können. Die in [6, S. 48] „ins Visier“ genommenen Multiple Choice-Aufgaben unterscheiden sich nicht nur durch ihr Aufgabenformat. Monotonieintervalle und Extremwertstellen aus einer vorgegebenen Zeichnung eines bestimmten Funktionsgraphen ablesen zu können, stellt sicher eine weniger hohe Anforderung dar als die doch relativ abstrakte Aufgabe über quadratische Gleichungen, wo nur $ax^2+bx+c=0$, mit $a\neq 0$, $a,b,c\in\mathbb{R}$ gegeben ist und bei der Aussagen über die Anzahl der reellen Lösungen („genau“, „mindestens“, etc.) zu bewerten sind, richtig zu lösen.

Die erhaltenen Lösungsquoten q von 30 bzw. 74% sind u.E. ein nicht überraschendes Spiegelbild des real existierenden Mathematikunterrichts in Österreich – viele Kurvendiskussionen, wenig Theorie, oder in diesem Fall genauer: (zu) wenig Wertlegung auf verbale (aktiv und passiv) mathematisch korrekte Ausdruckswei-

se. In [4, Bd. 7] beispielsweise finden wir 46 Seiten zu Kurvendiskussionen (von der Prominenz ihres Auftretens bei der bisherigen schriftlichen Reifeprüfung ganz zu schweigen), in [4, Bd. 5] acht Seiten zu quadratischen Gleichungen (und ebenfalls insgesamt acht zu den Themen „Ablesen von Eigenschaften einer Funktion aus ihrem Graphen“ und „Zeichnen von Funktionsgraphen aus Wertetabellen“). Auch in der sechsten Klasse werden reelle Funktionen und ihre möglichen Eigenschaften zum Thema gemacht: In [4, Bd. 6] hat das entsprechende Kapitel 32 Seiten. Da der Test, bei dem die in Rede stehenden Aufgaben gegeben worden sind, in siebenten Klassen im Oktober durchgeführt worden ist, ist nicht damit zu rechnen, dass Kurvendiskussionen zu diesem Zeitpunkt schon in aller Ausführlichkeit besprochen worden sind. Dennoch: Neben der unterschiedlichen Quantität muss auch die zeitliche Nähe des einen Stoffgebiets für die Schülerinnen und Schüler im Vergleich zum anderen in Rechnung gestellt werden.

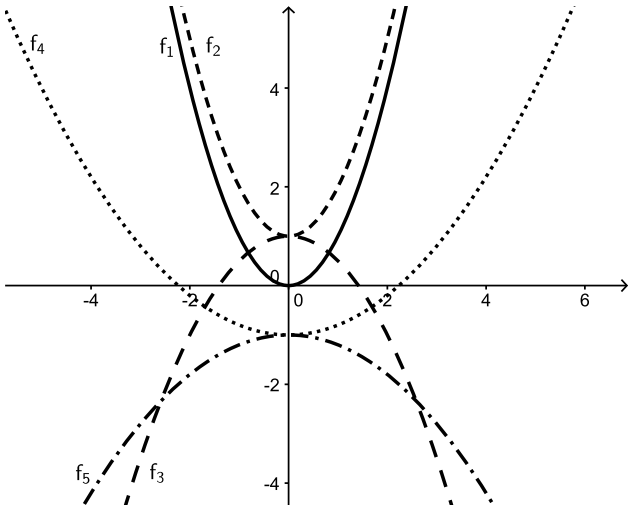
Der in [6, S. 48] geäußerten inhaltlichen Kritik, dass nämlich bei der Aufgabe über die quadratischen Gleichungen zwei Aussagen zu bewerten sind, die logisch das genaue Gegenteil voneinander sind, kann gelassen entgegnet werden: Wenn nur die Schülerinnen und Schüler genau das erkennen und sich so einen Vorteil bei dieser Multiple Choice-Aufgabe verschaffen, dann sei ihnen das von Herzen vergönnt, denn ein wesentliches Ziel des Mathematikunterrichts wäre damit angesprochen, nämlich das korrekte Interpretieren können von mathematischen Texten. Darin liegt aus unserer Sicht der eigentliche Wert von Multiple Choice-Aufgaben im Mathematikunterricht: Das Interpretieren-lernen von mathematischen Statements, die sich auf eine vorgegebene mathematische Situation beziehen.

Wenn, wie es in [7, S. 12] heißt, tatsächlich im zweiten Teil der standardisierten schriftlichen Reifeprüfung Aufgaben gegeben werden, die „eine selbstständige Anwendung der Grundkompetenzen in weniger vertrauten Situationen oder auch weitergehende Reflexionen“[1] erfordern, dann sind die Multiple Choice-Aufgaben eine hervorragende Vorbereitung dafür. Die Situation ist vertraut, aber die Aussagen sind es nicht. Sie müssen modulo der vorgegebenen Bedingungen des gesetzten Rahmens interpretiert, reflektiert werden – ein weniger komplexes Unterfangen als jenes, das das eben angeführte Zitat beschreibt.

Neben den unterschiedlichen Schwierigkeitsgraden verschiedener Aufgaben geben wir noch einen weiteren Grund an, warum Schlussfolgerungen bezüglich inhaltlicher Schwerpunktsetzungen im zukünftigen Mathematikunterricht aufgrund des Vergleichs der zugehörigen Lösungsquoten nicht zulässig sein können. In [8, S. 11f] werden neben den Inhaltsbereichen auch sogenannte Handlungsbereiche definiert: 1.) Darstellen, Modellbilden; 2.) Rechnen, Operieren; 3.) Interpretieren und 4.) Argumentieren, Begründen. Sinngemäß können wir diese Klassifizierung mathematischer Tätigkeiten auch für die in Rede stehenden Aufgaben zur Testung von Grundkompetenzen verwenden. Es ist durchaus vorstellbar, dass eine Aufga-

[1] Im aktuellen Papier [1] ist von *„Aufgaben zur Vernetzung der Grundkompetenzen in definierten Kontexten und Anwendungsbereichen“* die Rede (S. 23).

Abbildung 1: *B211 Quadratische Funktionen.* Im folgenden Koordinatensystem sehen Sie fünf Graphen von quadratischen Funktionen, dabei ist $f_1\colon x \to x^2$.



Aufgabenstellung: Ordnen Sie den unten angeführten Funktionstermen die jeweils zutreffende Funktion zu!

..... $x \to \frac{1}{5} \cdot x^2 - 1$

..... $x \to x^2 + 1$

..... $x \to -\frac{1}{2} \cdot x^2 + 1$

..... $x \to -\frac{1}{5} \cdot x^2 - 1$

be, bei der Begründen (z.B. im Themenkreis *Quadratische Gleichungen*) verlangt wird, wesentlich schlechter ausfällt als eine, bei der operiert werden muss (beispielsweise eine Mittelwertberechnung). Daraus dann zu schließen, Statistik ist im österreichischen Mathematikunterricht gut verankert, während bei den quadratischen Gleichungen noch einiges im Argen liegt, wäre schlicht verfehlt. Das konstruierte Beispiel zeigt lediglich, dass im durchschnittlichen Mathematikunterricht viel operiert und wenig begründet wird.

Tatsächlich hat sich bei einer mathematisch verwandten Aufgabe zum Thema „Quadratische Funktionen“ im zweiten Testheft (B2) eine Erfolgsquote von 77% ergeben [12] – siehe Abb. 1.

Die Leistungsfähigkeit dieser Schülerpopulation zeigt also im Themenfeld *Quadratische Funktionen – Quadratische Gleichungen* ein heterogenes Bild: Einmal steht das Interpretieren im Vordergrund, einmal das Operieren.

Die in [6] verlangten „offenen“ Aufgaben erfordern natürlich genaue Korrekturanleitungen (inwieweit sind die offenen Aufgaben dann wirklich noch offen?), um überhaupt aussagekräftige Erfolgsquoten zu erhalten. Nur so können die jeweiligen Bewertungen von Lehrerinnen und Lehrern miteinander verglichen werden. Allerdings konnte schon bei herkömmlichen Schularbeitsbeispielen mangelnde Objektivität bei der Beurteilung festgestellt werden, siehe z.B. [5, S. 175ff]. Umso schwieriger wird es bei den Antworten auf offene Fragestellungen sein, subjektive Einflüsse bei deren Bewertung zu vermeiden. Aber selbst wenn das gelänge, löst ihre Verwendung nicht das Problemfeld, das sich beim Vergleich von zwei ganz unterschiedlichen Aufgaben ergibt. Insofern unterscheiden sie sich nicht von Mul-

tiple Choice-Aufgaben.

Man wird um eine Fehleranalyse nicht herumkommen, wenn man wirklich wissen möchte, warum die eine oder andere Aufgabe diese oder jene Erfolgsquote mit sich gebracht hat, wie das bei den Bildungsstandards in der Erprobungsphase in vorbildlicher Weise passiert ist [11].

Nach der Analyse muss die Therapie erfolgen. Wie ein Unterstützungssystem für Schulen und Lehrerinnen und Lehrer aussehen könnte, dazu gibt es noch wenig ausformulierte Ideen. Erste Überlegungen in diese Richtung, allerdings die Bildungsstandards betreffend, finden sich in [3]. Eines kann von dort jedenfalls übernommen werden: Es wird großer Anstrengungen der österreichischen Fachdidaktik in Mathematik (und nicht nur von ihr!) bedürfen, um den eingangs erwähnten Neuerungen im österreichischen Mathematikunterricht jene Früchte folgen zu lassen, die eigentlich von diesen Konzepten intendiert sind. Überlegungen über Aufgabenformate werden dabei wohl auch eine Rolle spielen, ein Splitter gewiss unter den Balken im Standardisierungsauge, das zurzeit die inhaltlichen Bildungsdebatten in Österreich, aber auch international (siehe etwa die derzeitige Debatte über landesweite Testungen in den USA) prägt.

Literatur

[1] BIFIE Wien (Hrsg.): Die standardisierte schriftliche Reifeprüfung in Mathematik. Inhaltliche und organisatorische Grundlagen zur Sicherung mathematischer Grundkompetenzen (Stand: April 2012). *https://www.bifie.at/system/files/dl/srdp_ma_konzept_2012-05-03.pdf*.

[2] BIFIE Wien: Reifeprüfung neu. Die standardisierte kompetenzorientierte Reifeprüfung im Klausurfach Mathematik, 2010.

[3] S. Götz, W. Peschek: Festlegung von Bildungsstandards – aber was dann? – Versuch über ein Unterstützungssystem. *Mathematik im Unterricht Newsletter* No. 3 (2009), 162–181. *http://www.mathematikimunterricht.at*.

[4] S. Götz, H.-C. Reichel (Hrsg.): *Mathematik 5, 6, 7* von R. Müller und G. Hanisch, unter Mitarbeit von C. Wenzel. öbv, Wien 2010–2011.

[5] G. Hanisch: Problematik der Leistungsfeststellungen durch schriftliche Arbeiten am Beispiel der Mathematik. Habilitationsschrift, Univ. Wien, 1990.

[6] H. Humenberger, G. Kirchner: Der Einfluss des Aufgabenformats bei Multiple-Choice-Aufgaben auf die Lösungshäufigkeit – in einem vereinfachten Modell. *Internat. Math. Nachr.* 217 (2011), 47–54.

[7] Institut f. Didaktik der Mathematik (Hrsg.): Das Projekt „Standardisierte schriftliche Reifeprüfung aus Mathematik“ – Sicherung von mathematischen Grundkompetenzen –. Univ. Klagenfurt, 2009. *http://www.uni-klu.ac.at/idm/downloads/sRP-M_September_2009.pdf*.

[8] Institut f. Didaktik der Mathematik (Hrsg.): Standards für die mathematischen Fähigkeiten österreichischer Schülerinnen und Schüler am Ende der 8. Schulstu-

fe. Version 4/07. Univ. Klagenfurt, 2007. *http://www.uni-klu.ac.at/idm/downloads/Standardkonzept_Version_4-07.pdf*.
[9] G. Kaiser: Realitätsbezüge im Mathematikunterricht – Ein Überblick über die aktuelle und historische Diskussion. In: G. Graumann et al. (Hrsg.): *Materialien für einen realitätsbezogenen Mathematikunterricht, Band 2*. Schriftenreihe der *ISTRON*-Gruppe. Franzbecker Verlag, Bad Salzdetfurth u.a. 1995, 66–84.
[10] S. Nordheimer: Kapitelübergreifende Rückschau: Unterrichtsmethode zum Vernetzen im Mathematikunterricht. In: A. Brinkmann et al. (Hrsg.): *Mathe vernetzt. Anregungen und Materialien für einen vernetzenden Mathematikunterricht 1*. Aulis Verlag, München, 2011, 58–69.
[11] Univ. Klagenfurt: Bildungsstandards, PISA. *http://www.uni-klu.ac.at/idm/inhalt/322.htm*.
[12] Univ. Klagenfurt: Zentralmatura. *http://www.uni-klu.ac.at/idm/inhalt/495.htm*.

Adressen der Autoren:

Stefan Götz
Fakultät für Mathematik, Univ. Wien
Nordbergstraße 15, A-1090 Wien
email *stefan.goetz@univie.ac.at*

Hans-Stefan Siller
Mathematisches Institut, Univ. Koblenz-Landau
Universitätsstraße 1, D-56070 Koblenz
email *siller@uni-koblenz.de*

Internat. Math. Nachrichten
Nr. 220 (2012), 41–50

Mathematicians Take a Stand

Douglas N. Arnold and Henry Cohn

Univ. Minnesota – Microsoft Research and MIT

This article was published in the Notices of the AMS **59** *(2012), 828–833. It is reprinted here with friendly permission by the authors and the publisher.*

Mathematicians care deeply about the mathematical literature. We devote much of our lives to learning from it, expanding it, and guaranteeing its quality. We depend on it for our livelihoods, and our contributions to it will be our intellectual legacy.

It has long been anticipated that technological advances will make the literature more affordable and accessible. Sadly, this potential is not being fully realized. The prices libraries pay for journals have been growing with no end in sight, even as the costs of publication and distribution have gone down, and many libraries are unable to maintain their subscriptions.[1]

The normal market mechanisms we count on to keep prices in check have failed for a variety of reasons. For example, mathematicians have a professional obligation to follow the relevant literature, which leads to inelastic pricing. This situation is particularly perverse because we provide the content, editorial services, and peer review free of charge, implicitly subsidized by our institutions. The journal publishers then turn to the same institutions and demand prices that seem unjustifiable.

Although the detailed situation is complex, the fundamental cause of this sad state of affairs is not hard to find. While libraries are being forced to cut acquisitions, a small number of commercial publishers have been making breathtaking profits year after year. The largest of these, Elsevier, made an adjusted operating profit of $1.12 billion in 2010 on $3.14 billion in revenue, for a profit margin of 36 percent, up from 35 percent in 2009 and 33 percent in 2008.[2] Adding insult to injury, Elsevier has aggressively pushed bundling arrangements that result in libraries

[1] For example, MIT's spending on serials increased by 426 percent over the period 1986–2009, while the number of serials purchased decreased by 16 percent, and the Consumer Price Index increased by only 96 percent.

[2] Reed Elsevier Annual Report 2010, SEC form 20-F (based on data from p. 25 and average exchange rate from p. 6).

ISSN 0020-7926 — Österr. Math. Gesellschaft.

paying for journals they do not want and that obscure the actual costs.[3] They have fought transparency of pricing, going so far as to seek a court injunction in an unsuccessful attempt to stop a state university from revealing the terms of their subscription contract. They have imposed unacceptable restrictions on dissemination by authors. And, while their best journals make important contributions to the mathematical literature, Elsevier also publishes many weaker journals, some of which have been caught in major lapses of peer review or ethical standards. These scandals have done harm to the integrity and reputation of mathematics.

This situation has been extensively analyzed many times before, including in the *Notices*. There have been some high-profile actions, such as mass resignations of entire Elsevier editorial boards over pricing concerns: the *Journal of Logic Programming* in 1999, the *Journal of Algorithms* in 2003, and *Topology* in 2006. These boards have done a valuable service for the community by founding replacement journals, but there has been little relief from the overall trend. As Timothy Gowers wrote in his blog in January, "It might seem inexplicable that this situation has been allowed to continue. After all, mathematicians (and other scientists) have been complaining about it for a long time. Why can't we just tell Elsevier that we no longer wish to publish with them?" Gowers then revealed that he had been quietly boycotting Elsevier for years, and he suggested it would be valuable to create a website where like-minded researchers could *publicly* declare their unwillingness to contribute to Elsevier journals.

Within days, Tyler Neylon responded to this need by creating *http://thecostofknowledge.com*. More than 2,000 people signed on in the first week, and participation has grown steadily since then, to over 8,000 as of early March. Each participant chooses whether to refrain from publishing papers in, refereeing for, or editing Elsevier journals. The boycott is ongoing, and it holds the promise of sparking real change. *We urge you to consider adding your voice.*

The boycott is a true grassroots movement. No individual or group is in charge, beyond Gowers's symbolic position as the first boycotter. However, a group of thirty-four mathematicians[4] (including Gowers and the authors of the present article) issued their best attempt at a consensus statement of purpose for the boycott. It is available online,[5] and we highly recommend it for reading. For reasons of

[3] T. Bergstrom, Librarians and the terrible fix: economics of the Big Deal, *Serials* **23** (2010), 77–82.

[4] Scott Aaronson, Douglas N. Arnold, Artur Avila, John Baez, Folkmar Bornemann, Danny Calegari, Henry Cohn, Ingrid Daubechies, Jordan Ellenberg, Matthew Emerton, Marie Farge, David Gabai, Timothy Gowers, Ben Green, Martin Grötschel, Michael Harris, Frédéric Hélein, Rob Kirby, Vincent Lafforgue, Gregory F. Lawler, Randall J. LeVeque, László Lovász, Peter J. Olver, Olof Sisask, Terence Tao, Richard Taylor, Bernard Teissier, Burt Totaro, Lloyd N. Trefethen, Takashi Tsuboi, Marie-France Vignéras, Wendelin Werner, Amie Wilkinson, and Günter M. Ziegler.

[5] See *http://umn.edu/∼arnold/sop.pdf* or the March 2012 *London Mathematical Society Newsletter*.

space, we will not cover every aspect of that statement here.

Before we proceed, we must address two pressing questions about the boycott. First, why is a boycott appropriate? After all, Elsevier employs many reasonable and thoughtful people, and many mathematicians volunteer their services, helping to produce journals of real value. Isn't a boycott overly confrontational? Could one not take a more collaborative approach? Unfortunately, such approaches have been tried time and again without success. Fifteen years of reasoned discussions have failed to sway Elsevier.[6] Elsevier's leadership seems to be driven only by their fiduciary responsibility to maximize profit for their shareholders. The one hope we see for change is to demonstrate that their business depends on us and that we will not cooperate with them unless they earn our respect and goodwill.

Second, why is the focus solely on Elsevier? Some of the problems we discuss are common among large commercial publishers, and indeed we hope the boycott will help spur changes in the whole industry. But we must start somewhere, and we believe it is more effective to focus on one publisher whose behavior has been particularly egregious than to directly confront an entire industry at once. Many of the successful boycotts in history took the same tack.

Journal Pricing.

Table 1 exhibits prices for three of Elsevier's mathematics journals: *Advances in Mathematics*, the *Journal of Algebra*, and the *Journal of Number Theory*. For comparison, the table includes three more affordable journals.

The *Annals of Mathematics*, published by the Princeton math department and IAS, provides exceptional quality at a rock-bottom price that just covers costs. The other two are highly regarded journals published by the Society for Industrial and Applied Mathematics (SIAM) and by the American Mathematical Society (AMS). Both of these organizations make a profit on their journal publishing operations, which helps to subsidize their other activities. For example, in 2011 SIAM's journal publication costs, including overhead, were 89 percent of their subscription revenues, resulting in an 11 percent profit margin.

Elsevier's recent pricing changes, apparently in response to the boycott, have at times led to multiple conflicting prices on their website. We have listed the prices actually paid by the University of Minnesota in 2012, but the notes after the table indicate the lowest prices we found offered on the Web. We made no attempt to select the highest-priced Elsevier journals, and in fact *Advances in Mathematics*

[6] R. Kirby, Comparative prices of math journals, 1997, *http://math.berkeley.edu/∼kirby/journals.html*; J. Birman, Scientific publishing: a mathematician's viewpoint, *Notices of the AMS* **47** (2000), 770–774; R. Kirby, Fleeced?, *Notices of the AMS* **51** (2004), 181; W. Neumann, What we can do about journal pricing, 2005, *http://www.math.columbia.edu/∼neumann/journal.html*; D. N. Arnold, Integrity under attack: the state of scholarly publishing, *SIAM News* **42** (2009), 2–3; P. Olver, Journals in flux, *Notices of the AMS* **58** (2011), 1124–1126.

Table 1: Summary information for six journals.

Journal	Publisher	Metrics	Price	$/art.	$/page	$/cite
Annals of Mathematics	Princeton	3.7/A*	$447	5.39	0.12	0.06
SIAM J. Appl. Math.	SIAM	1.8/A*	$642	5.95	0.27	0.13
J. of the AMS	AMS	3.6/A*	$300	9.09	0.24	0.13
Advances in Math.	Elsevier	1.6/A*	$3,899	11.53	0.35	0.90
J. of Algebra	Elsevier	0.7/A*	$6,944	13.89	0.75	1.22
J. of Number Theory	Elsevier	0.6/B	$2,745	17.49	1.12	1.91

Metrics are the 2010 5-year impact factor from *Journal Citation Reports* and the 2010 rating by the Australian Research Council (based on expert opinion). A* = top-rated, B = "solid, though not outstanding".

Elsevier prices are the amounts actually paid by the University of Minnesota for electronic-only institutional subscriptions in 2012. The lowest prices we could find on the Elsevier website as of February 29 were $3,555.20, $5,203, and $2,226.40. The *Annals* price is again the actual amount paid by UMN, which is slightly greater than the $435 list price. The SIAM and AMS prices are the list prices, although UMN paid less because of institutional membership.

Columns 5–7 normalize by the most recent data available: the numbers of articles and pages published in 2011 and the number of citations to the journal made in 2010 (as reported in *Journal Citation Reports*).

is among the most affordable. For comparison, the 2011 prices per page of the thirty-six Elsevier journals listed in the AMS journal price survey ranged from $0.33 (*Advances in Mathematics*) to $4.05 (*Mathematical Social Sciences*), with a mean of $1.35 and a median of $0.96.

As shown in the table, the prices of the SIAM and AMS journals are within a factor of two of that of the *Annals*, with differences depending on whether one normalizes the raw journal price by number of articles, pages, or citations. But the Elsevier prices are a different story. The price per page of the *Journal of Algebra*, for example, is triple that of the society journals and six times that of the *Annals*, and the *Journal of Number Theory* is 50 percent more expensive yet.

Moreover, as demonstrated in Table 2, this problem has grown over time. The inflation-adjusted prices per page of the *Journals of Algebra* and *Number Theory* increased by more than 80 percent between 1994 and 2011, compared with much smaller increases for the society journals and a decrease for the *Annals*. It is noteworthy that the recent prices of *Advances in Mathematics*, while still high, have come closer to the prices of the society journals. This supports our belief that Elsevier could offer substantially lower prices and still make a reasonable profit.

We do not mean to suggest that publishing is cheap in the electronic age. True, electronic distribution is very cheap: the arXiv requires just $7 per submission, or

Table 2: Historical prices per page in constant 2012 dollars.

	1994	1997	2000	2003	2006	2009	2010	2011
Annals of Math.	0.19	0.20	0.14	0.15	0.13	0.13	0.09	0.10
SIAM J. Appl. Math.	0.20	0.24	0.23	0.25	0.27	0.24	0.18	0.27
J. of the AMS	0.22	0.26	0.27	0.29	0.30	0.27	0.25	0.24
Advances in Math.	0.65	0.74	0.95	1.01	0.55	0.61	0.44	0.33
J. of Algebra	0.36	0.43	0.50	0.73	0.60	0.77	0.92	0.66
J. of Number Theory	0.57	0.67	0.98	1.01	1.04	0.86	0.95	1.05

Prices are from the AMS journal price survey (*http://www.ams.org/membership/mem-journal-survey*), adjusted using the Consumer Price Index.

1.4 cents per download, in funding.[7] But journal publishing involves significant additional costs, such as IT infrastructure, administrative support, oversight, sales, copyediting, typesetting, archiving, etc. Many of these costs scale roughly with the number of published pages, and some of them benefit from economies of scale (so large publishers like Elsevier should, if anything, achieve lower costs).

Of course, journals are not all the same. A low-circulation journal may need to command a higher price per page to stay afloat. The community might find some such journals too expensive to support, but one viewed as worthy of support might reasonably charge a higher price until more libraries subscribe. Another journal might have extraordinary expenses, for example from translation. But these factors do not apply to the cases we have considered or to many other Elsevier journals.

We see no good reason to pay much more for Elsevier journals than for journals that earn mathematical societies a tidy profit. Even the price targets for mathematics journals that Elsevier announced in response to the boycott – $0.50 to $0.60 per page – would leave their journals costing twice as much as the comparison journals in Table 1. Elsevier's prices have become far out of proportion and have a way to go to return to reasonable.

What's the Big Deal about Bundling?

Bundling refers to grouping together collections of journals and selling access as a single product, discounted from list price. Elsevier commonly negotiates bundles including all the journals to which the library has recently subscribed. The bundles may also include access to nearly all of Elsevier's roughly 2,000 journals. Librarians have termed enormous bundles "the big deal".

[7] *http://arXiv.org/help/support/faq*.

While there is nothing wrong with offering quantity discounts,[8] it is the way in which Elsevier and other large publishers have implemented bundling that is objectionable. They have turned it into a powerful tool for subverting the market forces that would keep prices in check. The then director of Harvard's library summarized it thus: "Elsevier is among a handful of journal publishers whose commercial bundling practices are squeezing library budgets. Their licensing programs require libraries to maintain large, fixed levels of expenditure, without the ability to cancel unneeded subscriptions."[9]

Let us see how this works. While Elsevier has gone to great lengths to keep the details of their bundle contracts secret, some have come to light, thanks to open records laws.[10] Judging by the contracts we have seen and librarians we have consulted, it works essentially as follows.

The university commits to subscribing to the journals it currently receives at a negotiated total price that is typically around the same as they were previously paying and to continuing to subscribe to them for a period of three to five years with annual price increases. Elsevier has called this the "Complete Collection", and it is a large expense. For example, for the University of Minnesota in 2006 it came to $1.8 million (about 18 percent of their total serials budget), and for the University of Michigan in 2007 it was $1.9 million. In both cases, 5 percent yearly price increases were built into the contracts, although the actual rate of inflation for the contract periods was only about 2 percent per year. Cancellation of titles in the Complete Collection is restricted, which makes it difficult or impossible to cut back on the expenditure.

For an additional fee Elsevier offers their "Freedom Collection", which adds deeply discounted access to nearly all of the Elsevier journals to which the library had *not* chosen to subscribe. This option cost the University of Michigan about $19,000 more in 2007, inflating 5 percent a year thereafter. The University of Minnesota elected against it.

Although prices increase quickly inside the bundle, list prices can increase even more quickly, so a university that decides not to renew its bundle may face a steep price increase to hold onto the journals it wants. Because of bundling, ever larger portions of library budgets are locked into Elsevier contracts, budgetary pressures force the cancellation of titles from smaller publishers, and funds for new subscriptions disappear. Furthermore, bundling leads to a lack of clarity on pricing. The discounts on the additional journals in the Freedom Collection can sound impressive, but it is the pricing of the primary subscriptions that drains library budgets.

[8] For example, Mathematical Sciences Publishers offers a bundle of six mathematics journals at a 31 percent discount, bringing their price down to $0.08 per page.

[9] *http://hul.harvard.edu/news/2004_0101.html*.

[10] T. Bergstrom, P. Courant, and R. P. McAfee, *Big Deal Contract Project*.

The constraints imposed by bundles have led some universities to conclude that even paying exorbitant prices for the journals they choose is a better deal. Harvard, MIT, the University of Minnesota, and others have now gone this route. However, many academic libraries remain tied to the big deal.

Price disclosure is necessary for a well-functioning market with competitive pricing, so the lack of transparency in bundling contracts is particularly troubling. As an Elsevier vice president wrote in support of Elsevier's 2009 lawsuit enjoining Washington State University from revealing the prices of their subscriptions, "Elsevier representatives apply pricing formulae and methods which are not generally known (to our competitors or potential customers)" and "disclosure could disadvantage Elsevier in that, if its pricing to customer X was known to customers Y and Z, the latter could demand the same pricing".[11] Elsevier may indeed profit from keeping Y and Z in the dark, but the academic community values sunlight. Without transparency of subscription contracts and costs, the community will remain skeptical of Elsevier's pricing, whatever changes they make to list prices.

Posting Policies.

Gowers's suggestion of an Elsevier boycott struck a chord in many researchers. Besides pricing and bundling, there are other issues that have contributed to so many researchers' readiness to abandon Elsevier. One of these is Elsevier's policies concerning dissemination. Thanks to the Internet, authors have additional ways of disseminating their work besides the printed journal and journal website. For example, it has become common practice for authors to post a finalized version of their manuscript to a repository such as the arXiv for open dissemination, as allowed by many publishers.[12] Elsevier's actions suggest that they view this development primarily as a threat to their profits, not as an opportunity to advance mathematics or increase their authors' readership. In short, their interests are not aligned with ours.

Elsevier's policies are complex and difficult to understand. In the words of the scholarly communications officer at Duke University, "it seems clear that the intent of these statements, policies and contracts is not to clarify the authors' obligations so much as it is to confuse and intimidate them."[13] Their posting policy[14] specifically prohibits posting an "accepted author manuscript" – the author's own

[11] *http://www. econ. ucsb. edu/∼tedb/Journals/WSUCourtCase/ElsevierStatementbySalesChief. pdf*.

[12] K. Fowler, Do mathematicians get the author rights they want?, *Notices of the AMS* **59** (2012), 436–438.

[13] K. Smith, What a mess!, *Scholarly Communications @ Duke*, July 7, 2011, *http://blogs.library.duke.edu/scholcomm/2011/07/07/what-a-mess/*.

[14] *http://www. elsevier. com/wps/find/authorsview. authors/postingpolicy*, accessed March 3, 2012.

version of a manuscript that has been accepted for publication – on an e-mail list, a subject repository, or even the author's own institutional repository *if* the institution has a posting mandate. The last is not a typo: if your institution mandates posting the accepted author manuscript in its repository, then Elsevier stipulates that you may not, although they permit such posting when there is no mandate!

Fortunately, since hearing complaints from the boycotters about their posting policy, Elsevier has introduced an exception to allow posting to the arXiv. However, that is not enough. There are other non-commercial subject repositories that are important to segments of the community (Optimization Online, the Cryptology ePrint Archive, etc.), and more will undoubtedly be created in the future. Elsevier should allow authors to post accepted manuscripts to any such repository, as well as to university repositories, regardless of whether there is a posting mandate. Furthermore, this right should be guaranteed by the publishing agreement, not just by a posting policy that is subject to change at any time.

Ethics and Peer Review.

Another source of frustration with Elsevier is their history of lapses in peer review and ethics. The case of the journal *Chaos, Solitons & Fractals* (CS&F) has become widely known. This journal published 273 papers by its own editor in chief over eighteen years, 57 of them in a single year. Suspicions that these papers were not subject to peer review are corroborated by the editor's declaration that "senior people are above this childish, vain practice of peer review."[15] Elsevier owes the community an explanation for this and other fiascos. Was there no oversight in place? Have changes been made so this will not happen again? What about the other papers in CS&F? Are there records of peer review? Will any papers that were not peer reviewed be retracted, or otherwise flagged? The current situation leaves the literature in a bad state and compromises the position of authors who submitted manuscripts for peer review in good faith. If Elsevier wants to place this issue behind them, they need to deal with it thoroughly, forthrightly, and transparently.

In another notorious case, for five years Elsevier "published a series of sponsored article compilation publications, on behalf of pharmaceutical clients, that were made to look like journals and lacked the proper disclosures."[16]

There are other incidents in which peer review has failed at Elsevier journals, sometimes in spectacular fashion.[17] For many of us, these call into question El-

[15] C. Whyte, El Naschie questions journalist in Nature libel trial, updated November 16, 2011, *http://www.newscientist.com/article/dn21169*.

[16] Statement from Michael Hansen, CEO of Elsevier's Health Sciences Division, regarding Australia based sponsored journal practices between 2000 and 2005, May 7, 2009, *http://www.elsevier.com/wps/find/authored_newsitem.cws_home/companynews05_01203*.

[17] *http://umn.edu/∼arnold/reasons.html*.

sevier's ability to meet the standards of quality and ethics we require if we are to collaborate with them.

Initial Responses to the Boycott.

On February 27, Elsevier publicly withdrew its support for the Research Works Act, which would have prohibited open access mandates for government-funded research. The bill was declared dead by its sponsors in Congress on the very same day. This victory confirmed the boycott's success in delivering a message where we were never able to get through before.

Further confirmation came that day in an open letter from Elsevier senior vice presidents David Clark and Laura Hassink to the mathematics community.[18] Besides reporting the about-face on the Research Works Act, they announced the target price for "core mathematics titles" that we discussed above. They also stated, correctly, that it would be necessary to address concerns about "large discounted agreements" (bundling) and said that this will come.

Finally, Clark and Hassink announced that free access has been granted to the archives of fourteen core mathematics journals for the years from 1995 through four years before the present day. Access to back issues is indeed critical, and we strongly believe that all research papers should be made freely available long before copyright expires. The shorter the delay the better, of course, but we consider four years a defensible choice, compatible with the subscription model for journal publishing. The AMS's experience with a five-year window shows that such a move is financially viable. We hope that Elsevier's announcement is just the first step and that expansion to the full set of mathematical journals and the period before 1995 will be announced soon.[19] We also hope that this is not just a temporary measure. A binding commitment not to revoke access in the future would be reassuring on that point.

Moving Forward.

While the mathematical literature itself is a treasure, the current system of scholarly publishing is badly broken. Elsevier is the largest and, in our view, the most egregious example of what is wrong. We hope many readers will agree with us that by choosing to withdraw our cooperation from Elsevier, we are sending a valuable message to them and to the scholarly publishing industry more broadly. Please consider joining the movement at *http://thecostofknowledge.com*.

[18] D. Clark and L. Hassink, A letter to the mathematics community, February 27, 2012, *http://www.elsevier.com/wps/find/P11.cws_home/lettertothecommunity*.

[19] All three journals discussed here began publishing in the 1960s. The issues before 1995 are currently available from Elsevier online but remain behind their paywall.

What is our vision for the future? The mathematical community needs a period of experimentation and healthy competition, in which a variety of publishing models can flourish and develop. Possibilities include various approaches to open access publishing,[20] refereed journals tightly integrated with the arXiv or similar servers, increased reliance on non-profit publishers, hybrid models in which community-owned journals subcontract their operations to commercial publishers, commercially owned journals with reasonable prices and policies, etc. It is too early to predict the mix of models that will emerge as the most successful. However, any publisher that wants to be part of this mix must convince the community that they oversee peer review with integrity, that they aid dissemination rather than hinder it, and that they work to make high-quality mathematical literature widely available at a reasonable price.

Let's work together to foster good practices and build better models. The future of mathematics publishing is in our hands.

Douglas N. Arnold is McKnight Presidential Professor of Mathematics at the University of Minnesota. His email address is arnold@umn.edu.

Henry Cohn is principal researcher at Microsoft Research New England and adjunct professor of mathematics at MIT. His e-mail address is cohn@microsoft.com.

[20]For example, based on publication charges or on sponsoring consortia such as SCOAP^3 (*http://scoap3.org*).

Internat. Math. Nachrichten
Nr. 220 (2012), 51–55

Elsevier's Response to the Mathematics Community

Laura Hassink and David Clark
Elsevier

This article was published in the Notices of the AMS **59** *(2012), 833–835.*

During the last months we have spoken to many people in the community about the move by Timothy Gowers and some colleagues to declare their wish not to work with Elsevier and the subsequent boycott movement.

At the end of this article we summarize how we are responding to the feedback from the community and the very specific steps that we are taking. But we would first like to address the concerns raised and some of the arguments. We are the leading journal publisher in scientific publishing and so will attract criticism that is directed at publishing as a whole. While we may disagree with much that has been said, we do recognize that Elsevier has not done a good job communicating what we do and how we support both the peer-review process and the dissemination of work. In particular, we have left authors, editors, reviewers, and board members with the impression that we are focussed on restricting access rather than making their research as widely available as possible.

Helping editors, authors, reviewers, and board members to work easily on journals is central to us. We have systems in place to make it easier for editors to run large journals, some of which are dealing with thousands of submissions each year – something which most smaller publishers are not equipped to do. There will, of course, be people who argue against the involvement of privately owned organizations in academic publishing, but we believe that a mixed economy brings benefits to mathematics.

Professor Gowers's protest is specifically concerned with three issues: the pricing of journals; the practice of offering journals in large "bundles"; and, in particular, Elsevier's support, along with others, of a set of legislation, including the Research Works Act, in the United States.

ISSN 0020-7926 — Österr. Math. Gesellschaft

Pricing

Mathematics journals published by Elsevier tend to be large, with a great many articles published each year. On a price-per-article or price-per-page level, our prices are typically, but not always, lower than those of other mathematics publishers. Our average price increase over the last eight years has been in the lowest quartile of the sector. The Cost of Knowledge statement selects ten (of thirty-eight) Elsevier journals to quote an average 2007 price per page of $1.30 and compares this to prices per page ranging from $0.13 to $1.21 for selected journals from other publishers. However, the average price per page for all thirty-eight Elsevier journals in the AMS dataset for that year is $0.76 per page, with several below $0.50 per page and as low as $0.35 per page. This is below the average for all mathematics journals in the AMS dataset. The document mentions that seven of the top ten most expensive journals are from Elsevier but does not show that the average price per page for those seven Elsevier journals is $0.61.

That said, these figures are five years old, and in recent years we have made moves to reduce or freeze the prices of a number of our mathematics titles, recognizing that this field is not well funded and the articles are used intensively rather than frequently.

Journals such as the *Journal of Algebra*, *Topology and its Applications* and the *Journal of Number Theory* have all seen price reductions in recent years. *Our target is for all of our core mathematics titles to be at or below US$11 per article*[1] *(equivalent to $0.50–$0.60 cents per normal typeset page) by next year*, placing us below most university presses, some societies, and all other commercial competitors. That will lead to a number of our titles seeing further and significant price reductions in their next volumes.

"Bundling"

Most journals are subscribed to as part of large deals or national consortia agreements, and so universities receive access to many more journal titles than they individually subscribe to and thus pay less than the list price described above. Although such packages are offered by virtually all publishers, many mathematicians have expressed dislike for such policies.

To describe this concisely, such agreements involve universities maintaining a core holding of journals and then, depending upon the size of the institution, having the option to subscribe to subcollections, such as in mathematics, or to all of our titles at a discount of the normal journal subscription list price. These collections can be as low as 2.5 percent of the catalogue value of the collection, which is one of the reasons why they have been so popular. A similar arrangement allows

[1] This is calculated by dividing the institutional list price of a journal by the number of articles published.

national consortia of universities to share electronic access to all their subscribed journals amongst themselves, without each university needing to hold an individual subscription.

We therefore disagree with the term "bundling", as it is not mandatory for a customer to enter into such a large deal. Libraries can decide what they want to subscribe to, whether that is individual titles or individual titles within a collection, or to join a national consortium. We do recognize the wish for more choice and flexibility, especially within departments, and we are currently experimenting with new ways of doing this. But switching off such schemes would, in our view, have a detrimental impact on access to the research literature. Because of the introduction of such large agreements, coupled with the simultaneous organization of universities and libraries into large consortia, access to journal content has never been better. However, clearly there are still areas and occasions where access is not at the level where it should be, and we are determined to address this issue.

Access

Later in this response we describe the major new steps that we are taking to ensure substantially wider free access to the mathematics articles that Elsevier publishes, but we'd like to flag two other issues that we think are misunderstood.

First, all of our titles, including our mathematics titles, are available in the poorest countries. We are a founding partner in *Research4Life*, a public/private partnership providing journal content to researchers in the developing world. More than 2,000 Elsevier journals and 6,000 Elsevier e-books are available through Research4Life.

Second, authors in mathematics can post their author manuscripts, including corrections made in peer review and editing, on the arXiv. We have been allowing this for years. Elsevier supplies metadata directly to the arXiv and has for many years. There seems to be some misunderstanding on this point, as Elsevier's policies are no different from other major mathematics publishers in this regard, and we are happy to be able to correct this point. See our article posting policies (*http://www.elsevier.com/wps/find/authorsview.authors/postingpolicy*) for more information.

U.S. Legislation

We are conscious that much of what triggered Professor Gowers's original posting was the support that Elsevier, along with others, gave to proposed U.S. legislation concerned with state mandates for publishing final versions of articles.

Almost all publishers are uncomfortable about laws determining what's published and under what conditions, but the critical feedback on this issue has been very

sobering for many of us and has led to much reflection within the company.

That is why Elsevier announced that we are withdrawing our support for the Research Works Act.

Quality of Journals

The discussion about publishing and large subscription agreements has also highlighted concerns about the quality of particular journals. In the specific case of *Chaos, Solitons and Fractals*, this is a journal which has been rebuilt, with a new set of editors – whose work and commitment we would like to acknowledge – and much involvement from in-house Elsevier staff. We think that we did the right thing to seek to rebuild this journal. This journal has changed and informed the way in which we work on many journals, from our basic editorial contracts with editors to the use of much more formal editorial processes, electronic peer review, clearer statements on ethical issues, and the introduction of additional staff in support of journals.

We have put a great deal of effort in recent years into developing our support for journals, including significant editorial changes. Publishing judgment can go wrong and that will happen in any organization. But we learn from our mistakes and make considerable efforts to address and resolve them.

We do, however, need to be more open about the actions that we have taken when things go wrong. Specifically, we need to develop a better forum for listening to the mathematics community, to hearing specific criticisms, and to jointly developing policies and to hearing critical feedback.

How Elsevier Is Responding to Feedback from the Community

In this article we have responded to some of the concerns raised, but our goal is to do what it takes to ensure that the leading mathematics journals that we publish are as valuable and respected – and contribute as much back to the community – as any journal published by a society or university press. We are therefore taking the following steps now:

1. To make clear our commitment to wider access, we have made the archives of over forty core mathematics journals open for free, from four years after publication back to 1995, the year when we started publishing digitally;
2. On subscription pricing, we will target a price of US$10–US$11 per article (equivalent to $0.50–$0.60 a page) for our core mathematics journals, below that of most of our competitors.
3. On "bundling", we are open to engaging with the mathematics community on how the system could work better, with greater flexibility and choice, and especially for small institutions without access to wider institutional

resources. As a first step we are defining a smaller subcollection of core mathematics titles.
4. We will create an advisory scientific council for mathematics to ensure that we are working in tandem with the mathematics community to address feedback and to give greater control and transparency to the community.
5. We have announced that we are withdrawing our support for the Research Works Act.

We do not regard this as the end of our discussion with mathematicians, but rather as the continuation of our efforts.

We are very open to talking with anyone in the community about what we do and how we do it. Some fair criticism has come to us, which we will address.

More generally, we seek out and welcome the views of any concerned member of the mathematics community.

Laura Hassink is Senior Vice President, Publishing, Elsevier. Her email address is l.hassink@elsevier.com.

David Clark is Senior Vice President, Publishing, Elsevier. His email address is david.clark@elsevier.com.

Internat. Math. Nachrichten
Nr. 220 (2012), 57–60

The Value of Publishing

Klaus Peters

This article was published in the Notices of the AMS **59** *(2012), 741–742.* ©
American Mathematical Society. It is reprinted here with friendly permission.

The recent statement by a large number of prominent mathematicians and other scientists, prompted by a BLOG post from Tim Gowers,[1] inspired me to write down a few comments based on my longtime involvement in publishing and my background as a mathematician. (See also "Why publish mathematics"[2] and "Small independent publishers: Responsible, committed, and flourishing".[3])

As a mathematician and, subsequently, STM[4] publisher for nearly fifty years, I have experienced many changes in the industry. Major changes in publishing started in the mid-seventies when mergers and internal reorganization at larger publishing houses shifted responsibility for final decisions, like pricing, print runs, and the editing process, from editorial departments to financial management. Additionally, the development of TEX, as well as the widespread availability of tools for producing and manipulating images, changed the relationship between the author and the publisher. At the same time, the Internet began to provide archiving and publication options. To be sure, those changes were gradual, but their effect has by now become obvious. I believe, however, that the current developments are more significant and consequential.

As a publisher I appreciate and endorse what I understand to be the broad goals of the protest. I do, however, want to emphasize the importance of the value that used to be – and still should be – *added* by publishers or other services that take their place.

When Gutenberg invented the printing press, publishers were the ones who knew how to produce multiple copies at "reasonable" cost; later the editorial function became important when academic societies became publishers. At the time when I became a publisher in 1964, marketing and distribution became more essential

[1] *http://gowers.wordpress.com/*
[2] Notices of the AMS, Volume 56, Number 7.
[3] Logos, 14/2, Whurr Publishers, 2003.
[4] Scientific, technical, and medical.

ISSN 0020-7926 — Österr. Math. Gesellschaft

functions that were recognized by authors and customers alike. Springer Verlag opened an office in New York to respond to the more global needs. Some years later, direct marketing activities became a function of the editorial department in order to better provide targeted information and thereby optimize the dissemination of books and journals.

Typesetting of technical mathematical texts had become very expensive already by the 1970s, and the quality had gone down from the days of hand-setting. Book prices reflected these increased costs. Donald Knuths monumental development of TEX and his making it publicly available revolutionized the production process for STM publishers. "Typeset" manuscripts replaced camera-ready submissions for publications such as Lecture Notes. Many publishers, driven by economic considerations, took advantage of this without applying classical standards of layout and typography. The important functions of editing and formatting easily became overlooked because manuscripts appeared to be already typeset. Hence, as a result of shifting responsibility, services benefitting authors (and also readers) were largely eliminated.

When the Internet initially provided the opportunity to upload and archive research papers, I had a friendly conversation with a mathematician who strongly championed an exclusive form of electronic publishing that would allow anyone to upload his/her papers to easily accessible servers. My question about quality control was answered by requiring a simple rule: "Whatever you upload, you cant retract. That will prevent any abuse." I knew then, and we all know now, that an established review and editing process is needed to achieve high standards of publication. Unfortunately, "author-pays" open access journals as well as some "reputable" publishers are no longer providing that service. To be very clear and explicit, the broadly accepted math archive[5] has become a standard that should be accepted by publishers. (At A K Peters, after some careful consideration, we accepted submissions to our journals that had been placed on the arXiv server but did not agree to the posting of the final edited and reformatted versions that were available in our printed and electronic journals.)

In my view, publishing should be a service that derives its justification from value added to the process. Publishers need the input and feedback from the scientific community in order to achieve this goal.

When I started in publishing, I "inherited" a group of advisors who were dedicated to the development of a book program that benefitted the community of their peers. They also understood the need for economic sustainability on the part of the publisher. Modest fees were paid to the advisors of the book program to compensate them for time and some administrative expenses.

One of my first encounters with an advisor reminds me of the current protest, although it happened on an individual basis and had an immediate and lasting ef-

[5] *http://arxiv.org/new/math.html*

fect. In 1965, on my first visit to the United States, I met Paul Halmos, one of the major advisors and editor of the series *Ergebnisse der Mathematik*, who became a friend and mentor, and whose understanding of the complex relationship between the publishing industry and the community that it served was at once practical and idea-driven (not idealistic). He opened our first meeting with a blunt statement: "If your company ever again prices a book as high as the recent Homology by Saunders Mac Lane, I will resign." The advice was heeded by the publisher and instilled a deep conviction about the importance of pricing that was later strengthened by experience when I learned more about the relationship between pricing and unit sales.

The situation for journals is quite different, and the current protest seems prompted by the lack of value added by the publisher and the expectation that the scientific community provide their expertise and services without compensation. In my experience, the very autonomous editorial boards of journals did not receive compensation other than for occasional administrative costs, mailing, travel, etc. Their rotating activities were considered a service to the community and did not include detailed editing or tracking, as that was handled by a very experienced staff at the publishing house. With the availability of typesetting programs such as TEX, growing expertise in image manipulation by the authors, and online reviewing tools, publishers have largely abandoned their professional obligation and rely on authors and editors to perform and control many of the publishers responsibilities.

Hand in hand with this reduction in service there was a disproportional price increase, as well as the introduction of the business model of "bundling", which has been deplored by librarians and the scientific community alike. I have checked with a few librarians and found that "bundling" can be prevented or modified but requires tough bargaining and some clout. Journals that used to be considered a self-sustaining, modestly profitable and prestigious part of the publishing program, attracting potential book authors, have become major profit centers as a result of these pricing and bundling policies. (Journal programs were, of course, already a major economic attraction for the publisher due to the cyclic subscription model that generated working capital that would be used over the subscription period.)

Today, new opportunities for self-publishing are evolving rapidly and include tools that were previously exclusively offered by publishers. I strongly believe that these opportunities require procedures that help maintain a desirable level of quality control.

As a mathematician and (former) publisher I would hope to encourage the continued involvement of the community with responsible publishers to be sure that the following essential elements of the process not be destroyed:

- *Technical* reviews should be a joint responsibility of the publisher and the

scientific community to insure quality.

- *Copyediting* is a *sine qua non*. Besides assuring correct spelling and grammar, professional copyediting, a responsibility of the publisher, improves readability by pointing out inconsistency and repetition and by improving the organizational structure of a text where needed.
- *Professional formatting and image handling* are essential functions that the publisher needs to provide.
- *Effective marketing and worldwide distribution* are essential to the widest possible dissemination of a text and should be a major goal of the publisher rather than simply profit maximization.

To navigate the proliferation of information, selectivity and brand recognition are and should remain valuable attributes of a publishing environment, and they can only be achieved through a constructive cooperation between the scientific community and the "publishers" of the future.

Klaus Peters
Founder and former publisher, A K Peters, Ltd.
klauspeters@gmail.com

Buchbesprechungen

V. Cortés (ed.): Handbook of Pseudo-Riemannian Geometry and Supersymmetry. (IRMA Lectures in Mathematics and Theoretical Physics 16.) EMS, Zürich, 2010, xviii+946 S. ISBN 978-3-03719-079-1 H/b € 118,–.

This is a collection of 25 articles by various authors, which are devoted to a wide range of questions of current interest in pseudo-Riemannian geometry. Many of the articles are motivated by or have close connections to theoretical physics, and the collection is intended to be accessible both for mathematicians and for theoretical physicists.

The articles are grouped into 8 parts according to topic. The first four parts, which cover about 580 pages, are devoted to various types of additional geometric structures compatible with a pseudo-Riemannian metric. In particular, this concerns special geometries and their relation to supersymmetry, generalized geometries in the sense of N. Hitchin, geometries with torsion (non-integrable geometries), and para-geometries (like paracomplex and paraquaternionic structures). The remaining four parts deal with more classical pseudo-Riemannian geometry, including holonomy theory, symmetric spaces and spaces of constant curvature, and conformal geometry.

Many of the articles are at least partly of expository character, so the book offers a good opportunity to get some insight into current trends in pseudo-Riemannian geometry. It is less clear to me why it is called a "Handbook".

A. Čap (Wien)

H.-D. Gronau, H.-H. Langmann, D. Schleicher (eds.): 50th IMO – 50 Years of International Mathematical Olympiads. Springer, Berlin, Heidelberg, 2011, xiii+297 S. ISBN 978-3-642-14565-0 P/b € 19,95.

Seit 1959 treffen sich die besten Mathematiker und Mathematikerinnen im Schulalter jährlich zum wissenschaftlichen Wettstreit im Rahmen der Internationalen Mathematischen Olympiade (IMO). Aus ursprünglich sieben teilnehmenden Nationen wurden inzwischen über 100, und im Jahr 2009 hatte Deutschland die Ehre, die Rolle des Gastgebers der 50. IMO in Bremen zu übernehmen. (Aufmerksame Zahlenkundige werden bemerken, dass da etwas mit den Zahlen nicht stimmt, und es ist tatsächlich der Fall, dass ein IMO-Jahr wegen schwerwiegender organisatorischer Probleme ins Wasser gefallen ist.) Aus Anlass des halben Jahrhunderts ließen sich die Gastgeber auch einige Besonderheiten einfallen, und dazu gehört der vorliegende Band.

Neben Informationen über Teilnehmer und Teilnehmerinnen der 50. IMO, Aufgaben und Lösungen des Wettbewerbs und Ergebnislisten findet man hier auch eine Vielzahl von Besonderheiten. An einem denkwürdigen IMO-Nachmittag etwa, hielten Sechs ehemalige IMO-Teilnehmer, heute alle hochangesehene Fachvertreter (Béla Bollobás, Timothy Gowers, László Lovász, Stanislav Smirnov, Terence

Tao und Jean-Christophe Yoccoz), für das speziell geneigte Publikum Kurzvorträge über Aspekte der Mathematik, die sie besonders begeistern. Sie konnten damit die Zusammenhänge der Forschungs- zur Wettbewerbsmathematik auch beeindruckend darstellen, und die Papers ihrer damaligen Darbietungen bilden nun einen faszinierenden Abschnitt dieser Sammlung.

Wie man in den Anhängen nachlesen kann, sind die genannten sechs bei Weitem nicht die Einzigen, die die IMO-Teilnahme als "stepping stone" zur mathematisch-wissenschaftlichen Karriere genutzt haben. Unter den Mathematikern und Mathematikerinnen mit IMO Vergangenheit finden sich etwa nicht weniger als 12 Fieldsmedaillen-Gewinner, aber auch eine Vielzahl von Gewinnern so renommierter Preise wie dem Wolf-Preis oder dem Clay Research Award.

Für alle, die Interesse an mathematischen Wettbewerben im Allgemeinen oder der IMO im Speziellen haben, verspricht dieses Buch eine besonders spannende Lektüre. Besonders aber Wettbewerbsskeptikern sei es dringend ans Herz gelegt, diesem Buch etwas Aufmerksamkeit zu schenken. Die Bedeutung der Internationalen Mathematischen Olympiade für die Entwicklung der modernen Mathematik kann kaum auf eindrucksvollere Weise dargestellt werden als auf diesen Seiten.

R. Geretschläger (Graz)

A. Guerraggio, G. Paoloni: Vito Volterra. Aus dem Italienischen von M. Stern. (Vita Mathematica, Band 15.) Birkhäuser, Basel, 2011, xii+229 S. ISBN 978-3-0348-0080-8 H/b € 82,19.

In der Birkhäuser Serie *Vita Mathematica* ist der Band 15 dem herausragenden italienischen Mathematiker Vito Volterra (1860–1940) gewidmet.

Beim Namen Volterra denkt man natürlich sofort an seine grundlegenden Beiträge zur Biomathematik. Das sehr detailreiche vorliegende Werk zeigt aber auf, dass das nur einen sehr kleinen Teil seines wissenschaftlichen Arbeitens darstellt. Mit großem Interesse habe ich einerseits die Lebensgeschichte dieses Mannes, anderseits aber auch die historische Entwicklung Italiens in dieser Zeit verfolgt.

Diese Buch kann jedem ans Herz gelegt werden, der sich nicht nur für Volterras mathematischen Beiträge, sondern auch für den Menschen dahinter interessiert.

G. Schranz-Kirlinger (Wien)

Q. Han: A Basic Course in Partial Differential Equations. (Graduate Studies in Mathematics, Vol. 120.) American Mathematical Society, Providence, Rhode Island, 2011, x+293 S. ISBN 978-0-8218-5255-2 H/b $ 63,–.

This is one volume in the Graduate Studies in Mathematics of the American Mathematical Society.

It represents an excellent textbook for an introductory graduate course on PDEs. The focus is on linear equations of first and second order. Simple models as the

heat equation, wave equation and Laplace equation are studied in detail. But of course general equations are not forgotten. From the beginning and throughout the book Han emphasizes *a priori* estimates. Such estimates are indispensable tools for proving the existence and uniqueness of solutions of PDEs, being especially important for nonlinear equations.

The book by Han is suitable for students interested in the mathematical theory of PDEs as an overview of the subject or as an introduction leading to further study.

G. Schranz-Kirlinger (Wien)

G. Lukács: Compact-like Topological Groups. (Research and Exposition in Mathematics, Vol. 31.) Heldermann Verlag, Lemgo, 2009, xiv+166 S. ISBN 978-3-88538-231-7 P/b € 28,–.

Kompakte topologische Gruppen sind wohl jene unter den topologischen Gruppen welche am besten studiert sind. Eine Abschwächung der Kompaktheitseigenschaft ist "*c*-compactness". Das Buch ist dem Studium dieses Begriffs gewidmet, insbesondere der Frage, unter welchen zusätzlichen Voraussetzungen *c*-compactness schon „kompakt" impliziert. Neben der Präsentation der Hauptergebnisse enthält das Buch auch eine kleine (zweckgebundene) Einführung zu topologischen Gruppen und einen kurzen Abriss zur Geschichte des diskutierten Begriffs der *c*-compactness.

Das Buch ist eine sehr gelungene und liebevoll verfasste Monographie zu dem – sehr speziellen, aber netten – Thema. Es kann jedem Leser, der mit den Grundlagen der topologischen Gruppen vertraut ist, empfohlen werden.

H. Woracek (Wien)

J. McNeal, M. Mustaţă: Analytic and Algebraic Geometry. Common Problems, Different Methods. (IAS/Parc City Mathematics Series, Vol. 17.) American Mathematical Society, Providence, Rhode Island, 2010, xiv+583 S. ISBN 978-0-8218-4908-8 H/b $ 99,–.

This volume consists of the contributions of the lecturers in the Graduate Program of the 2008 PCMI Summer School in Park City. It starts with a brilliant introduction to things $\overline{\partial}$ by Bo Berndtsson, followed by John D'Angelo's illuminating lectures under the title *Real and Complex Geometry meet the Cauchy-Riemann Equations*. The other interesting lectures are: *Three Variations on a Theme in Complex Analytic Geometry*, by Dror Varolin; *Structure Theorems for Projective and Kähler Varieties*, by Jean-Pierre Demailly; *Lecture Notes on Rational Polytopes and Finite Generation*, by Mihai Paun; *Introduction to Resolution of Singularities*, by Mitrea Mustata; *A Short Course on Multiplier Ideals*, by Robert Lazarsfeld; *Exercises in the Birational Geometry of Algebraic Varieties*, by Janos

Kollar; *Higher Dimensional Minimal Model Program for Varieties of Log General Type*, by Christopher D. Hacon; *Lectures on Flips and Minimal Models*, by Alessio Corti, Paul Hacking, Janos Kollar, Robert Lazarsfeld, and Mitrea Mustata.

The language differences between algebraic and analytic geometry represent a difficulty for students and researchers. These lectures are designed to address this language gulf. In the first four contributions the $\overline{\partial}$-complex plays an important role, whereas in the remaining lectures the focal point was multiplier ideals, a subject of wide current interest. Many illustrative examples and detailed computations open access of the material to students and non-specialists.

F. Haslinger (Wien)

U. Narayan Bhat: An Introduction to Queueing Theory. Modeling and Analysis in Applications. (Statistics for Industry and Technology.) Birkhäuser, Boston, Basel, Berlin, 2008, xii+268 S. ISBN 978-0-8176-4724-7 H/b € 53,39.

Gestützt auf eine 40jährige Erfahrung mit Lehrveranstaltungen über Warteschlangentheorie auf unterschiedlichen Niveaus, erstellte der Autor ein Lehrbuch über die Modellierung mithilfe von Warteschlangen als Basis für eine einsemstrige Veranstaltung auf Master-Niveau, die keine Kenntnisse über stochastische Prozesse voraussetzt. Die notwendigen Grundlagen aus diesem Bereich werden im Zuge der Darlegung des Materials, d.h. der Analyse von Modellen, an entsprechender Stelle erarbeitet. Das Buch richtet sich neben Studierenden der Mathematik und Statistik vor allem an Studierende aus den Anwendungsdisziplinen, wie Informatik, Ingenieurwissenschaften, etc. Für die Darbietung des Materials hat der Autor einen Zugang gewählt, der zwischen tiefer Theorie und reiner Anwendung von Rezepten liegt. Besonderes Augenmerk legte der Autor auch auf die Identifikation von Modellen im Sinne eines modellbasierten Ansatzes. Das Werk gliedert sich in zwölf Kapitel und drei Anhänge, in denen grundlegende Ergebnisse aus den Bereichen des Poisson-Prozesses, der stochastischen Prozesse sowie der Mathematik, wie sie benötigt werden, zusammengefasst sind. Die Darlegung des Materials sowie die formalen Ableitungen erfolgen in gut lesbarem und erfassbarem Stil, an den wichtigsten Stellen ergänzt durch erläuternde und motivierende Beispiele aus den unterschiedlichsten Anwendungsbereichen. Die drucktechnische Hervorhebung der zentralen Ergebnisse hätte zu einer noch besseren Strukturierung des Texts beigetragen. Die wesentlichsten Kapitel werden durch eine Sammlung von Übungsaufgaben abgeschlossen, die es dem Studierenden erlauben, die erworbenen Kenntnisse zu überprüfen. Leider enthält das Werk selbst keine Lösungen oder Lösungshinweise zu den Aufgaben; solche sind aber für Lehrende vom Verlag abrufbar. Zusammenfassend kann gesagt werden, dass die Ziele, die sich der Autor gesteckt hat, durchaus als erreicht angesehen werden können.

G. Haring (Wien)

M. Pitici (ed.): The Best Writing on Mathematics 2011. Princeton University Press, Princeton, Oxford, 2011, xxx+383 S. ISBN 978-0-691-15315-5 P/b $ 19,95.

This booklet is a compilation of mathematical papers from 2011. What they have in common is not a mathematical field or problem. This volume contains various contributions (25, to be exact) from quite a few, pretty different swathes of mathematics. But it is not the variety of topics which deserves being emphasized. There is a lot more to it than that. What makes this booklet stand out is the mere joy at mathematical writing.

A paper on mathematics has many facets. This collection directs the attention to both, the content *and* the presentation. It reminds us that it can well be a piece of literary arts.

The introductory contribution, for one, puts forward the question: "What is mathematics for?" and the answer is not exactly obvious. The mathematical side of M. C. Escher is a quite different subject, though equally intriguing. There are several sections on mathematics education, some of them down-to-earth, others virtually philosophical, but each and everyone sophisticated in its way. I have never before asked myself the question by Chris Budd and Rob Eastaway: "How much math is too much math?" There are so many contributions which would equally deserve being referred to?

Certainly, nobody can prove that the articles – in absolute terms – represent "The best writing on mathematics" of 2011. To my mind, though, there is circumstantial evidence that the contributions in this booklet are pretty close to what the title promises. This volume is the very ticket for any mathematician and – beyond that – for anybody who enjoys a sense of delight in the beauty of writing.

J. Lang (Graz)

E. M. Stein, R. Shakarchi: Functional Analysis. Introduction to Further Topics in Analysis. (Princeton Lectures in Analysis IV.) Princeton University Press, Princeton, Oxford, 2011, xvii+423 S. ISBN 978-0-691-11387-6 H/b $ 85,–.

Der Zusatz zum Titel ist recht treffend. Der Leser sollte nicht eine allgemeine Einführung in die Funktionalanalysis erwarten, sondern vielmehr eine Präsentation ausgewählter Kapitel der Analysis mit funktionalanalytischem Hintergrund. Der hauptsächlicher Fokus liegt auf Funktionenräumen und harmonischer Analysis. Einige Stichworte dazu: L^p-Räume, Hardy-Räume, BMO, Distributionen, Fourierreihen und -Transformation, Hilbert-Transformation. Weiters enthält das Buch ein Kapitel, in dem einige Sätze über analytische Funktionen mehrerer Variabler präsentiert werden, und ein Kapitel über Brownsche Bewegung (davor eine vorbereitende Darstellung einiger Grundlagen der Wahrscheinlichkeitstheorie).

Das vorliegende Buch ist der vierte Teil einer Serie, die aus einer entsprechenden Serie von Vorlesungen entstanden ist. Zielgruppe sind wohl fortgeschrittene Studenten oder Wissenschafter, die sich für eine Einführung in die behandelten Themen interessieren. Der potentielle Leser sollte schon ein gewisses Maß an Wissen aus Analysis mitbringen; aber schließlich ist es ja auch der vierte Teil der Serie. Der Stoff ist solide (manchmal vielleicht ein bisschen trocken) präsentiert, und jedes Kapitel schließt mit *Excercises* und *Problems*. Die Qualität der Aufbereitung geht weit über typische „Lecture Notes“ hinaus, das Werk ist eher in die Kategorie „Lehrbücher über einen gewissen – etwas spezielleren – Themenkreis“ einzuordnen. Es ist zweifelsohne eine Bereicherung der existenten Literatur.

H. Woracek (Wien)

T. Tao: An Introduction to Measure Theory. (Graduate Studies in Mathematics, Vol. 126.) American Mathematical Society, Providence, Rhode Island, 2011, xvi+206 S. ISBN 978-0-8218-6919-2 H/b $ 53,–.

Der vorliegende Text ist eine Print-Version eines Vorlesungsskripts des Autors. Es werden einige Grundlagen aus der Maßtheorie gebracht, wobei spezieller Fokus auf dem Lebesgue-Maß und Zusammenhängen mit der Analysis liegt. Der Text versteht sich auch als Vorbereitung auf das (bedeutend tiefergehende und interessantere) Werk des Autors, „*An epsilon of room*“.

Das Buch ist für Studenten, die mit den Grundlagen der Analysis vertraut sind, lesbar. Die Aufbereitung der Materie ist jedoch weder systematisch noch ausführlich (speziell im zweiten Kapitel). Damit kann man diesen Text wohl nicht als „Lehrbuch“ verstehen; derer gibt es ja aber ohnehin viele ganz ausgezeichnete, die sich auch sehr gut zum Selbststudium eignen.

Als Konklusio kann man vielleicht sagen: Die Vorlesung war sicher toll, aber wozu ein Buch?

H. Woracek (Wien)

D. Varolin: Riemann Surfaces by Way of Complex Analytic Geometry. (Graduate Studies in Mathematics, Vol. 125.) American Mathematical Society, Providence, Rhode Island, 2011, xviii+236 S. ISBN 978-0-8218-5369-6 H/b $ 63,–.

This book provides the basic function theory and complex geometry of Riemann surfaces, both open and compact, using adaptations and simplifications of methods from the theories of several complex variables and complex analytic geometry, as for instance for the Runge approximation theorem and Mittag-Leffler's theorem. The novelty of the book begins in the fourth chapter, where Hermitian holomorphic line bundles and their sections are studied. The finite-dimensionality of spaces of sections of holomorphic line bundles of compact Riemann surfaces and the triviality of holomorphic line bundles over Riemann surfaces are proved.

The main novelty of the book is to use Hörmander's L^2-estimates for the solution of the inhomogeneous Cauchy-Riemann equations to prove the Kodaira and Narasimhan Embedding Theorems for compact and open Riemann surfaces. The final chapters are devoted to the Riemann-Roch Theorem and to Abel's Theorem, which characterizes divisors of meromorphic functions on a compact Riemann surface. The book ends with an interpretation of the Abel-Jacobi Theorem as a classification of all holomorphic line bundles on a compact Riemann surface. In this way the text will be very helpful for those who want to study Riemann surfaces from a differential geometric and PDE viewpoint.

F. Haslinger (Wien)

V. Volpert: Elliptic Partial Differential Equations. Vol. 1: Fredholm Theory of Elliptic Problems in Unbounded Domains. (Monographs in Mathematics, Vol. 101.) Birkhäuser, Basel, 2011, xvii+639 S. ISBN 978-3-0348-0536-6 H/b € 99,95.

The classical theory of elliptic problems has been developed in the case of bounded domains with a sufficiently smooth boundary. In this case, their Fredholm property is provided by the ellipticity condition. In the case of unbounded domains, this condition is no longer sufficient and the Fredholm property may not be satisfied, which is related to the lack of compactness. In order to satisfy the Fredholm property, one needs to impose an additional condition, which characterizes the behavior of the operator at infinity and determines the location of the essential spectrum. This book presents a systematic investigation of general elliptic problems applicable for both bounded and unbounded domains. For this purpose special function spaces are introduced, which are well adapted for problems in unbounded domains. In order to compute the index of an operator a new method is developed based on approximation of unbounded domains by a sequence of bounded domains. The book also contains a treatment of non-Fredholm operators and discrete operators and ends with extensive historical and bibliographical comments.

F. Haslinger (Wien)

Nachrichten der Österreichischen Mathematischen Gesellschaft

Hans Vogler 1935–2012

Professor Hans Vogler ist am 23. April 2012 nach längerer Krankheit in Graz verstorben. Geboren am 7. April 1935 in Wien, absolvierte er das Lehramtsstudium der Darstellenden Geometrie und Mathematik, promovierte 1964 zum Dr.techn. unter der Betreuung von Josef Krames und schloss 1967 die Habilitation ab. Mit 1. Oktober 1972 wurde er an die Lehrkanzel für Geometrie der Technischen Hochschule in Graz berufen. Diese Stelle füllte er bis zu seiner Emeritierung im Jahr 2003 aus. Neben seiner Tätigkeit in Forschung und Lehre war er besonders aktiv in Universitätsverwaltung, Personalvertretung und Standespolitik: 1983–1985 und 1996–2003 als Dekan der technisch-naturwissenschaftlichen Fakutät der TU Graz, 2003–2008 als Universitätsrat der Universität Innsbruck sowie als langjähriges Mitglied des Zentralausschusses der Hochschullehrer. In den Jahren 1978, 1979 war er auch Herausgeber dieser Zeitschrift.

(Johannes Wallner)

Journal of the European Mathematical Society

I am very pleased to announce that the Journal of the European Mathematical Society (JEMS) is now free accessible online to every EMS individual member. Members can get access on *http://www.euro-math-soc.eu/* by going to the member database, logging in, and following the link to JEMS. The username is a 5 digit number printed on your Newsletter address tag.

(Marta Sanz-Solé, EMS President)

Über den am 27.5.2012 verstorbenen "Architekten der modernen Mathematik in Deutschland", Friedrich Hirzebruch, und die Verleihung des Abelpreises an Endre Szemerédi werden im nächsten Heft Beiträge erscheinen. Vgl. den Nachruf auf Friedrich Hirzebruch von Günter Ziegler, erschienen am 30.5.2012 in der *Zeit*: *http://www.zeit.de/wissen/2012-05/nachruf-mathematiker-hirzebruch*.

Neue Mitglieder

Christian Bargetz, Dipl.-Ing. – Univ. Innsbruck. geb. 1984. 2002–2009 Studium der Technischen Mathematik, seit 04/2010 wissenschaftlicher Mitarbeiter an der Univ. Innsbruck. email *christian.bargetz@uibk.ac.at*, *http://www.uibk.ac.at/mathematik/personal/bargetz*.

Karl-Heinz Grass, Mag. – Akademisches Gymnasium Graz. geb. 1986. Lehramtsstudium Mathematik und Chemie an der Karl Franzens-Universität Graz, derzeit dort Doktoratsstudium. email *g.karl@aon.at*.

Benjamin Hackl – Viktring. geb. 1994. Gewinner des Schülerpreises der ÖMG 2011/12. email *benjamin@einfachtoll.com*.

Christoph Temmel, Dipl.-Ing. – TU Graz. geb. 1984. Universitätsassistent am Institut f. mathematische Strukturtheorie der TU Graz. email *temmel@math.tugraz.at*, *http://www.math.tugraz.at/∼temmel*.

Daniel Waschmann – Margarethen am Moos. geb. 1994. Gewinner des Schülerpreises der ÖMG 2011/12. email *da.waschmann@gmail.com*.