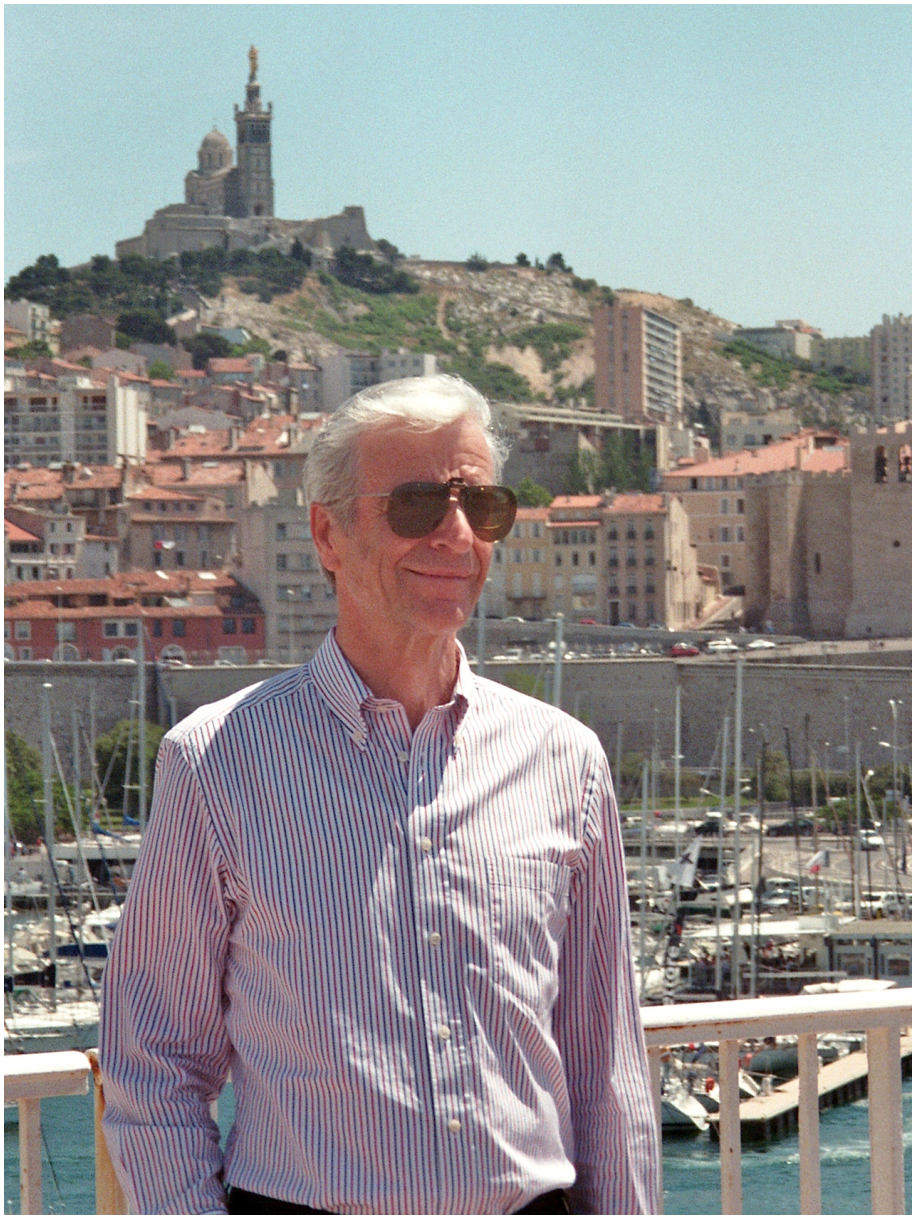
Workshop on the Occasion of

Harald Niederreiter's 70th Birthday:

Applications of Algebra and Number Theory

June 23-27, 2014



Harald Niederreiter in Marseille

	Monday	Tuesday	Wednesday	Thursday	Friday
08:15 – 08:55	Registration				
	Chair: Winterhof	**Chair:** Pillichshammer		**Chair:** Xing	**Chair:** Hofer
09:00 – 09:30	Wozniakowski	Sloan		McGuire	Mullen
09:30 – 10:00		Lécot	Coffee	Topuzoğlu	
10:00 – 10:30	Coffee	Coffee		Coffee	Coffee
10:30 – 11:00	Sarközy	Leobacher	**honary doctorate for H. Niederreiter +Lunch** **REP C, Uni-Center**	Ostafe	Mauduit
11:00 – 11:30	Gyarmati	Faure		Meidl	Pilz
11:30 – 12:00	Merai	Göttfert		Gomez	Hellekalek
12:00 – 12:30	Lunch	Photo/Lunch		Lunch	Lunch
12:30 – 13:30					
	Chair: Hellekalek	**Chair:** Leobacher	**Chair:** Larcher	**Chair:** Kritzer	
13:30 – 14:00	Rivat	Fleischner		Vielhaber	
14:00 – 14:30	Keller	Lisonek	Tichy	Iacò	
14:30 – 15:00	Cools/Nuyens	Coffee	Coffee	Coffee	
15:00 – 15:30	**Reception**	Pausinger	**Hiking Tour**	Kawakita	
				Dinner 19:30	

"*Discrepancy bounds for low-dimensional point sets*"
Henri Faure Institut de Mathématiques de Marseille, France

Abstract

In this talk, we will present the latest results given in our survey paper written jointly with Peter Kritzer on the occasion of Harald Niederreiter's 70th birthday. Then, we will review a range of pending open questions and problems concerning low-dimensional point sets in irregularities of distribution; some of them for about forty years, when appeared two founding publications that have been the support of a considerable number of studies in number theory and numerical analysis: the book "Uniform distribution of sequences" (1974) and the paper "Quasi-Monte Carlo methods and pseudo-random numbers" by Harald (Bull. Amer. Math. Soc, 1978, that foreshadowed his book in the CBMS-NSF Series in 1992).

"*Reducing an arbitrary fullerene to the dodecahedron*"
Herbert Fleischner TU Vienna, Austria

Abstract

Fullerenes are carbon molecules, the most prominent one being C60, also sometimes called the 'football' because of its representation on a soccer football. Speaking in terms of graph theory, a fullerene is a planar 3-regular graph all of whose faces are either pentagonal or hexagonal. It follows from Euler's polyhedron formula that every fullerene has exactly 12 pentagonal faces; and it is known that for every $n > 1$ there exist fullerenes with n hexagonal faces (the dodecahedron is a fullerene with $n = 0$ hexagonal faces).

The aim of this presentation is to show that there are several reduction steps (one global, the others local reductions) by which one can obtain the dodecahedron starting from an arbitrary fullerene. It also becomes clear that the application of these reduction steps gives rise to a polynomial time algorithm.

"*Estimating the keystream length for the general combination generator relative to correlation attacks.*"
Rainer Göttfert Infineon Technologies AG Neubiberg, Germany

Abstract

Consider a combination generator that consists of several binary possibly nonlinear feedback shift registers producing sequences of distinct periods. The sequences are combined by some Boolean combining function to form one sequence, called the keystream. We investigate the following problem: How much keystream material is required in order to determine the states of the involved feedback shift registers using correlation attacks.

"*On the linear complexity and lattice test of nonlinear pseudorandom number generators*"
Domingo Gómez-Pérez University of Cantabria, Spain

Abstract

One of the main contributions which Harald Niederreiter made to mathematics is related to pseudorandom sequences theory. In this paper we study several measures for asserting the quality of pseudorandom sequences, involving generalizations of linear complexity and lattice tests and relations between them.

This is joint work with Jaime Gutierrez.

"*Generation of further pseudorandom binary sequences (blowing up a single sequence)*"
Katalin Gyarmati Eötvös Loránd University Budapest, Hungary

Abstract

The present talk is based on a joint paper with C. Mauduit and A. Sárközy. Assume that a binary sequence is given with strong pseudorandom properties. Here an algorithm is presented and studied which prepares many further binary sequences from the given one. It is shown that if certain conditions hold, then each of the sequences obtained in this way also possesses strong pseudorandom properties. Moreover, I will show that certain large families of these sequences also posses strong pseudorandom properties.

"*On an important family of inequalities of Niederreiter involving exponential sums*"
Peter Hellekalek University of Salzburg, Austria

Abstract

The inequality of Erdös-Turán-Koksma is a fundamental tool to bound the discrepancy of a sequence in the s-dimensional unit cube $[0,1)^s$, $s \geq 1$, in terms of exponential sums. In an impressive series of papers, Harald Niederreiter has established variants of this inequality and has proved bounds for the discrepancy for various sequences and point sets, in the context of pseudo-random number generation and in quasi-Monte Carlo methods. These results have been an important breakthrough, because they marked the starting point of a thorough theoretical correlation analysis of pseudo-random numbers. Niederreiter's technique also prepared for the study of digital sequences, which are central to modern quasi-Monte Carlo methods.

In this contribution, we present an overview of these concepts and prove a hybrid version of the inequality of Erdös-Turán-Koksma, thereby extending a recent result of Niederreiter.

"*Ergodic properties of $\boldsymbol{\beta}$-adic Halton sequences*"
Maria Rita Iacò Graz University of Technology, Austria, and University of Calabria, Italy

Abstract

We investigate a parametric extension of the classical s-dimensional Halton sequence where the bases are special Pisot numbers. In a one-dimensional setting the properties of such sequences have already been investigated by several authors. We use methods from ergodic theory in order to investigate the distribution behavior of multidimensional versions of such sequences.
This is joint work with Markus Hofer and Robert Tichy.

"*Certain sextics with many rational points*"
Motoko Kawakita Shiga University of Medical Science, Japan

Abstract

I found Wiman's and Edge's sextics attaining Hasse–Weil–Serre's bound in my previous papers. Wiman's and Edge's sextics have simple defining equations. I investigated the curves obtained by generalising their defining equations, and made computer search. I found new curves with many rational points, some of which attain Hasse–Weil–Serre's bound.

"*Construction of a rank-1 lattice sequence based on primitive polynomials*"
Alexander Keller NVIDIA Berlin, Germany

Abstract

A construction of a rank-1 lattice sequence is introduced. In analogy to the Sobol' sequence, its generator vector is constructed from a sequence of primitive polynomials and is both extensible in the number of dimensions and the number of digits of each component of the generator vector. Some initial numerical evidence is provided by applying the rank-1 lattice sequence to high-dimensional light transport simulation.

This is joint work with Nikolaus Binder and Carsten Wächter.

"*A quasi-Monte Carlo method for the coagulation equation*"
Christian Lécot Université de Savoie, France

Abstract

We propose a quasi-Monte Carlo algorithm for the simulation of the continuous coagulation equation. The mass distribution is approximated by a finite number N of numerical particles. Time is discretized and quasi-random points are used at every time step to determine whether each particle is undergoing a coagulation. Convergence of the scheme is proved when N goes to infinity, if the particles are relabeled according to their increasing mass at each time step. Numerical tests show that the computed solutions are in good agreement with analytical ones, when available. Moreover, the error of the QMC algorithm is smaller than the error given by a standard Monte Carlo scheme using the same time step and number N of numerical particles. This is a joint work with Ali Tarhini, Université Libanaise

"*Even faster CBC construction of lattice rules*"
Gunther Leobacher Johannes Kepler University Linz, Austria

Abstract

Lattice rules and polynomial lattice rules are quadrature rules for approximating integrals over the s-dimensional unit cube. Since no explicit constructions of such quadrature methods are known for dimensions $s > 2$, one usually has to resort to computer search algorithms. The fast component-by-component approach is a useful algorithm for finding suitable quadrature rules.

We present a modification of the fast component-by-component algorithm which yields savings of the construction cost for lattice rules in weighted function spaces. The idea is to reduce the size of the search space for coordinates which are associated with small weights and are therefore of less importance to the overall error compared to coordinates associated with large weights. We analyze tractability conditions of the resulting QMC rules. Numerical results demonstrate the effectiveness of our method.

This is joint work With Josef Dick, Peter Kritzer, and Friedrich Pillichshammer.

"*On double simplex APN permutations*"
Petr Lisoněk Simon Fraser University, Canada

Abstract

Almost perfect nonlinear (APN) functions on finite fields $\mathrm{GF}(2^n)$ are important in cryptography as they provide the optimal resistance of a block cipher to differential attacks. For the purpose of designing block ciphers it is desirable to look for APN functions that are also permutations of $\mathrm{GF}(2^n)$. Many APN permutations are known when n is odd, however their existence in even dimensions $n > 6$ is an open problem. An example of an APN permutation on $\mathrm{GF}(2^6)$ was presented by Browning, Dillon, McQuistan and Wolfe at the conference Fq9 in 2009. Their construction relies on decomposing the related binary linear code as the direct sum of two simplex codes; certain aspects of the construction were regarded as "miracles" by the authors. We show that these results follow easily from considering the number of rational points on a certain family of hyperelliptic curves of genus 2 over $\mathrm{GF}(2^6)$. We discuss the possibility of obtaining similar constructions in higher even dimensions.

"*Statistical properties of subsequences of the Thue-Morse sequence*"
Christian Mauduit Institut de Mathématiques de Marseille, France

Abstract

Let $T = t_0 t_1 ... t_n ... \in 0, 1^{\mathbb{N}}$ be the Thue Morse sequence (i.e. the infinite word T obtained as the limit in $0, 1^{\mathbb{N}}$ of the sequence of finite words $(T_k)_{k\in\mathbb{N}}$ defined by the recursion $T_0 = 0, T_0' = 1$ and $T_{k+1} = T_k T_k', T_{k+1}' = T_k' T_k$ for any non negative integer k).

Our talk concerns the study of statistical properties of the subsequences $(T_{u_k})_{k\in\mathbb{N}}$, where $u = (u_k)_{k\in\mathbb{N}}$ is a given increasing sequence of integers. This problem can easily be translated in the study of the representation of elements of the sequence u with an even (or odd) sum of digits in base 2.

We will focus on recent results and open problems concerning the case where u is the sequence of prime numbers or the sequence of square numbers.

This is joint work with Michael Drmota and Joel Rivat.

"*On L-polynomials of curves over finite fields*"
Gary McGuire University College Dublin, Ireland

Abstract

We consider the issue of when the L-polynomial of a curve divides the L-polynomial of another curve. We present a theorem relating this property to the number of rational points on the curves. This is joint work with Omran Ahmadi.

"*Quadratic functions and Artin-Schreier curves*"
Wilfried Meidl Sabancı University Istanbul, Turkey

Abstract

Let p be an odd prime and let $\mathbb{F}_{p^n}$ be the finite field with p^n elements. A quadratic function Q (without linear and constant terms) from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ can be represented in trace form as

$$Q(x) = \mathrm{Tr}_n\Big(\sum_{i=0}^{\lfloor n/2\rfloor} a_i x^{p^i+1}\Big) \quad \text{with } a_0, \ldots, a_{\lfloor n/2\rfloor} \in \mathbb{F}_{p^n}.$$

Its Walsh transform

$$\widehat{Q}(b) = \sum_{x\in\mathbb{F}_{p^n}} \epsilon_p^{Q(x)-\mathrm{Tr}_n(bx)},\ \epsilon_p = e^{2\pi i/p},$$

takes values in $\{0, \zeta p^{(n+s)/2}\}$ for an integer $0 \le s \le n-1$ depending on Q and a fixed $\zeta \in \{\pm 1, \pm i\}$.

We express the number of rational points of the Artin-Schreier cover of the $\mathbb{F}_{p^n}$-projective line given by

$$\mathcal{X} : y^p - y = \sum_{i=0}^{\lfloor n/2\rfloor} a_i x^{p^i+1} \quad \text{with} \quad a_i \in \mathbb{F}_{p^n} \tag{1}$$

by means of the Walsh transform at 0 of $Q(x) = \mathrm{Tr}_n(\sum_{i=0}^{\lfloor n/2\rfloor} a_i x^{p^i+1})$.

We use this to construct classes maximal and minimal Artin-Schreier curves of the form (1), i.e. curves attaining the Hasse-Weil bound on the number of rational points, for various values of s. We completely classify all maximal and minimal curves obtained from quadratic functions of codimension 2, i.e. quadratic functions Q for which $s = n-2$, and coefficients in the prime field $\mathbb{F}_p$.

This is joint work with Nurdagül Anbar.

"*Pseudorandomness of binary threshold sequences derived from linear recursion*"
László Mérai Eötvös Loránd University Budapest, Hungary

Abstract

Let p be a prime number and let (x_n) be a linear recursive sequence in $\mathbb{Z}_p$ defined by

$$x_n = c_1 x_{n-1} + \cdots + c_h x_{n-h}, \quad n > h, \tag{2}$$

with initial values $x_1, \ldots, x_h \in \mathbb{Z}_p$.

The aim of the talk is to study the pseudoramndom measures (i.e. well-distribution and correlation measures) of binary sequences derived from (x_n).

Namely, let

$$e_n = \begin{cases} +1 & \text{if } x_n < p/2 \\ -1 & \text{otherwise,} \end{cases} \tag{3}$$

and

$$e'_n = \begin{cases} +1 & \text{if } (x_n)^{-1} < p/2 \\ -1 & \text{otherwise.} \end{cases} \tag{4}$$

Both positive and negative results are proven concerning the pseudoramndom measures of sequences (3) and (4).

"*Value sets of polynomials over finite fields*"
Gary Mullen Pennsylvania State University, USA

Abstract

Given a polynomial over a finite field, we can ask whether the polynomial induces a permutation of the field. More generally, we will discuss the value set (set of distinct images) of the polynomial and its cardinality. Only for a few special kinds of polynomials do we know how to determine the cardinality of the value set. We will also discuss some very recent results concerning value sets of polynomials in several variables over finite fields.

"*Vertex modified lattice rules*"
Dirk Nuyens KU Leuven, Belgium

Abstract

We revisit the idea of vertex modified lattice rules as proposed by Niederreiter & Sloan in 1993 and 1994 where all vertices of the unit cube are added as cubature nodes. A particular case is the so-called "optimal vertex modified lattice rule" which fixes the weights for the vertices of the unit cube in such a way that all multi-linear functions are integrated exactly. We study these rules using the technology of reproducing kernel Hilbert spaces, more specifically, we study the worst-case error in the unanchored Sobolev space of smoothness 1. This is joint work with Ronald Cools.

"*Explicit Hilbert's Nullstellensatz and orbits in polynomial dynamics over finite fields*"
Alina Ostafe University of New South Wales Sydney, Australia

Abstract

We use recent explicit versions of Hilbert's Nullstellensatz to answer several natural questions about reductions of orbits modulo a prime p of polynomial dynamical systems defined over $\mathbb{Z}$. We first show that for sufficiently large primes p, the reduction modulo p of a zero dimensional variety over $\mathbb{Q}$ remains zero dimensional over $\overline{\mathbb{F}}_p$.

We apply these estimates to studying cyclic points and, under a certain natural condition on the intersections of such orbits over $\mathbb{C}$ corresponding to two distinct polynomial systems, we show that intersections modulo p are rare. These results can be considered modulo p versions of recent results of D. Ghioca, T. J. Tucker, and M. E. Zieve in characteristic zero. However the underlying approach and techniques are different.

"*Construction and application of uniformly distributed sequences in the orthogonal group*"
Florian Pausinger IST Klosterneuburg, Austria

Abstract

We present recent progress concerning the explicit construction of uniformly distributed sequences in the orthogonal group. As an application, we show how to approximate certain integral-geometric formulas, yielding various directions for future research.

"*Applications of finite fields to finite fields*"
Günter Pilz Johannes Kepler University Linz, Austria

Abstract

If one starts with a finite field $(\mathbb{F}, +, .)$ and changes the multiplication in skillful way, one obtains a generalized ring (a *planar near-ring*) $(\mathbb{F}, +, *)$ which is the source of numerous ways to create Balanced Incomplete Block Designs. These, in turn, give rise to very efficient experimental designs which are easy to construct. This talk aims to study this connection and to show the use of these experimental designs in (of course, finite) experimental fields in agriculture.

"*On the digits of prime numbers*"
Joël Rivat Institut de Mathématiques de Marseille, France

Abstract

We give general sufficient conditions for a digital function (e.g. Rudin-Shapiro) taken along the sequence of prime numbers to be equidistributed in arithmetic progressions.

This is joint work with Christian Mauduit.

"*On pseudorandomness of families of binary sequences*"
András Sárközy Eötvös Loránd University Budapest, Hungary

Abstract

In cryptography one needs large families of binary sequences with strong pseudorandom properties. In the last decades many families of this type have been constructed. However, in many applications it is not enough if our family of "good" sequences is large, it is more important to know that it has a rich, complex structure. Thus various measures have been introduced and applied for studying pseudorandomness of families of binary sequences: family complexity, collision, distance minimum, avalanche effect and cross-correlation measure. In my talk I will give a survey of all these definitions and results.

"*The ANOVA decomposition of a non-smooth function of an infinite number of variables can have every term smooth*"
Ian H Sloan The University of New South Wales, Australia

Abstract

In this joint work with Frances Kuo (UNSW) and Michael Griebel (Bonn) we extend our earlier work motivated by option pricing problems, in which we tried to understand how it is that sparse grid and QMC methods can be applied successfully to option pricing problems, even though the integrands do not live in any mixed derivative smoothness class. The problem derives from the "max function" in the integrand, describing the fact that options are considered worthless if the final value is below the strike price.

In a previous paper (Griebel, Kuo, Sloan, Math. Comp. 82, 383-400, 2013) we showed that if the expected value is expressed as an integral over $\mathbb{R}^d$ then the classical ANOVA decomposition of the integrand for an arithmetic Asian option can have every term smooth

except for the very highest term. That highest ANOVA term has many discontinuities in first partial derivatives, but in most cases is expected to be pointwise very small.

In the present work we consider the ANOVA decomposition of the corresponding continuous problem in the Brownian bridge (or Levy-Ciesielski) formulation, and show that in this case **every term in the (infinite) ANOVA decomposition is smooth.** It may be that this observation will pave the way for an error analysis of the cubature problem for option pricing problem, in which the discrete-time problem is approximated by the continuous problem, and the error analysis then applied to the truncated infinite ANOVA expansion, in which every term is smooth.

"*Uniform distribution and dynamical systems*"

Robert Tichy Technische Universität Graz, Austria

Abstract

The lecture is devoted to van der Corput sets and sets of recurrence. We give new constructions involving equidistribution of sequences of prime powers. This refines and unifies earlier results obtained by Sárkőzy, Furstenberg, Kamae and Mendés France and Bergelson and Lesigne. The proofs heavily depend on analytic machinery involving bounds for exponential sums. In the second part of the lecture we give some new sharp result concerning the probabilistic behaviour of lacunary sequences. In particular we show limit theorems for discrepancy functions and related quantities.

"*On a method of Fu, Niederreiter and Özbudak*"

Alev Topuzoğlu Sabancı University İstanbul, Turkey

Abstract

Fu, Niederreiter and Özbudak developed a method to study the joint linear complexity of multisequences consisting of linear recurring sequences, see FFA, 2009,475–496. We use a variant of their method to enumerate quadratic functions with precribed spectra. Self-reciprocal polynomials enable us to relate these two problems. This is joint work with W. Meidl and S. Roy. We shall also mention the recent work with W. Meidl and C. Kasikci.

"*On the linear complexity of multisequences, bijections between $\mathbb{Z}$ahlen and $\mathbb{N}$umber tuples, and partitions* "

Michael Vielhaber Universidad Austral de Chile / Hochschule Bremerhaven, Germany

Abstract

Stream ciphers employ pseudorandom sequences as a replacement for one-time-pads. Such a cipher is deterministic, but should be indistinguishable from true randomness. A means to assess the quality of such a pseudorandom symbol stream is its linear complexity profile.

This article assembles the known facts about linear complexity of single streams (over $\mathbb{F}_q$) and of multisequences, streams over $\mathbb{F}_q^M$, with M typically a power of two, the wordlength.

We show, how the approaches by Niederreiter and Wang and by Canales and the present author, the BDM, are equivalent.

In the course of modelling the linear complexity of multisequences, we will touch partitions and stochastic infinite state machines. The bijection between both gives rise to a family of bijections between $\mathbb{N}_0^M$ and $\mathbb{Z}^M$.

"*Discrepancy and tractability or how Harald Niederreiter influenced my work*"

Henryk Woźniakowski Columbia University, USA, and University of Warsaw, Poland

Abstract

I will discuss how the paper of Harald Niederreiter "Quasi-Monte Carlo methods and pseudo-random numbers" published in the Bulletin of AMS in 1978 inspired me to work on discrepancy and later on tractability. In particular, it allowed me to solve the conjecture on the minimal average case error of multivariate integration for continuous functions equipped with the Wiener sheet measure. The intriguing factor of $[\log n]^{(d-1)/2}$ in the error bound of the nth minimal error for the d variate case was one of the reasons of tractability studies.