CONTENTS

The 3rd International Conference on Uniform Distribution Theory, Smolenice, June 25–29, 2012

On the limit distribution of consecutive elements of the van der Corput sequence

Christoph Aistleitner

Abstract

Let $(x_n)_{n\geq 1}$ be the van der Corput sequence. We calculate the limit distribution of the s-dimensional sequence $(x_n, \ldots, x_{n+s-1})_{n\geq 1}$. To obtain our results, we use the connection between the van der Corput sequence and the ergodic von Neumann-Kakutani transformation, which we present in detail.

Hilbert space with reproducing kernel and uniform distribution preserving maps, II

Vladimir Baláž — Jana Fialová — Vassil Grozdanov
Stanislava Stoilova — Oto Strauch

Abstract

In Part I of this series we discuss the relation between a uniform distribution preserving map $\Phi(\mathbf{x})$ and the mean square worst-case error

$$\int_{[0,1]^s} \sup_{\substack{f\in H\\ ||f||\le 1}} \left| \frac{1}{N}\sum_{n=0}^{N-1} f\big(\Phi(\mathbf{x}_n \oplus \boldsymbol{\sigma})\big) - \int_{[0,1]^s} f(\mathbf{x})\mathrm{d}\mathbf{x} \right|^2 \mathrm{d}\boldsymbol{\sigma} \tag{1}$$

in a Hilbert space H with reproducing kernel $K(\mathbf{x},\mathbf{y})$ with respect to a sequence

$$\mathbf{x}_0,\dots,\mathbf{x}_{N-1} \quad \text{shifted to} \quad \Phi(\mathbf{x}_0\oplus\boldsymbol{\sigma}),\dots,\Phi(\mathbf{x}_{N-1}\oplus\boldsymbol{\sigma}).$$

Applying the method of Fourier-Walsh expansion, which was introduced by F. J. Hickernell (2002), we find a partially known formula of the mean square worst-case error (1) in the form

$$\sum_{\substack{\mathbf{k}\in\mathbb{N}_0^s\\ \mathbf{k}\neq\mathbf{0}}} \widehat{K}_1(\mathbf{k},\mathbf{k}) \left| \frac{1}{N}\sum_{n=0}^{N-1} \mathrm{wal}_{\mathbf{k}}(\mathbf{x}_n) \right|^2,$$

where $\widehat{K}_1(\mathbf{k},\mathbf{k})$ are Fourier-Walsh coefficients of $K\big(\Phi(\mathbf{x}),\Phi(\mathbf{y})\big)$.

In Part II, for dimension $s=1$, using Riemann-Stieltjes integration and theory of distribution functions we find (1) in the form

$$\begin{aligned} K\big(\Phi(1),\Phi(1)\big) &- \int_0^1 y\mathrm{d_y}K\big(\Phi(1),\Phi(\mathrm{y})\big) - \int_0^1 \mathrm{x}\mathrm{d_x}K\big(\Phi(\mathrm{x}),\Phi(1)\big) \\ &+ \int_0^1\int_0^1 \left(\frac{1}{N^2}\sum_{m,n=0}^{N-1} g_{m,n}(x,y)\right)\mathrm{d_x}\mathrm{d_y}K\big(\Phi(\mathrm{x}),\Phi(\mathrm{y})\big) \\ &- \int_0^1\int_0^1 K(x,y)\mathrm{dxdy}, \end{aligned}$$

where $\Phi(x)$ is an arbitrary u.d.p. map, $x_0,\dots,x_{N-1}$ be a sequence in $[0,1)$, $\Phi(x\oplus\sigma)$ can be replaced by $\Phi(x+\sigma \bmod 1)$, and $g_{m,n}(x,y)$ is a distribution function $(x_m\oplus\sigma_i, x_n+\sigma_i)$ or $\big(\{x_m+\sigma_i\},\{x_n+\sigma_i\}\big)$, where σ_i, $i=1,2,\dots$ is u.d. in $[0,1)$.

Directional discrepancy

Dmitriy Bilyk

Abstract

It is well known in the theory of irregularities of distribution that the nature of the discrepancy estimates depends crucially on the geometry of the underlying sets. In particular, while the discrepancy with respect to axis-parallel rectangles behaves logarithmically, the discrepancy with respect to rectangles rotated in arbitrary directions is polynomial in the number of points N. In this talk we shall attempt to explore the gap between these two phenomena and study what happens when the rectangles are allowed to be rotated in some partial sets of directions. We consider some particular cases (lacunary sets of directions, Cantor-type sets etc) and derive more general results in terms of the metric entropy of the set of rotations. This is joint work with X. Ma, J. Pipher and C. Spencer.

Spherical nets and their relatives – – optimal order Quasi-Monte Carlo methods on the sphere

Johann S. Brauchart [1]

Abstract

A Quasi-Monte Carlo rule approximates the integral of a function with respect to the uniform measure using the average of function values at well-chosen nodes. In the unit cube digital nets and sequences provide a very efficient method to generate low-discrepancy sequences of such node sets giving an optimal bound for the discrepancy part in the celebrated Koksma-Hlawka inequality.

The study of low-discrepancy sequences suitable for (effective) numerical integration on the unit sphere in, say, the $d+1$ dimensional Euclidean space has to cope with a number of obstacles emerging from the topology and the symmetry of the d-sphere $\mathbb{S}^d$.

Notable is the absence of the notion of "the Koksma-Hlawka inequality" on the sphere. Instead many Koksma-Hlawka like inequalities propose different approaches to "discrepancy" of point sets and struggle with a replacement of "total variation of a function".

The quantification of the irregularity of distribution of a sequence of configurations with respect to test functions from a sufficiently smooth Sobolev space $\mathbb{H}^s$ over $\mathbb{S}^d$ rather than taking test sets like spherical caps leads to the notation of "generalized discrepancy". In fact, since $\mathbb{H}^s(\mathbb{S}^d)$ is also a reproducing kernel Hilbert space for $s > d/2$, the error of numerical integration for the qMC rule Q_N for functions in this space satisfies

$$\left| Q_N(f) - \int_{\mathbb{S}^d} f \, d\sigma_d \right| \leq \operatorname{wce}(Q_N; \mathbb{H}^s(\mathbb{S}^d)) \, \|f\|_{\mathbb{H}^s}$$

and the worst-case error $\operatorname{wce}(Q_N; \mathbb{H}^s(\mathbb{S}^d))$ takes over the role of discrepancy of the integration node set. Perhaps surprisingly, one can find suitable reproducing kernels so that the worst-case error has the following simple closed form for $d/2 + L < s < d/2 + L + 1$ (L an integer ≥ 0):

$$\Big[\operatorname{wce}(Q_N; \mathbb{H}^s(\mathbb{S}^d))\Big]^2 = \frac{1}{N^2} \sum_{j=1}^{N} \sum_{k=1}^{N} (-1)^{L+1} \, |\mathbf{x}_j - \mathbf{x}_k|^{2s-d} - (-1)^{L+1} V_{d-2s}(\mathbb{S}^d),$$

[1] Postdoctoral Fellow School of Mathematics and Statistics at the University of New South Wales

subject to the requirement that for $L \geq 1$ the nodes form a so-called spherical L-design. It is well-known that for optimal sum of distance points with $d/2 < s < d/2+1$ one has $\mathrm{wce}(Q_N; \mathbb{H}^s(\mathbb{S}^d)) \asymp N^{-s/d}$. Spherical t-designs with $N_t \asymp t^d$ points also satisfy such a relation but for every $s > d/2$! This leads to the definition of sequences of approximate spherical designs for $\mathbb{H}^s(\mathbb{S}^d)$; that is, of point sets with worst-case error not worse than spherical designs with optimal number of points. The corresponding qMC rules, thus, provide optimal order numerical integration on $\mathbb{S}^d$. It is interesting to note that all sequences of N-point configurations with low spherical cap discrepancy are approximate spherical designs for $\mathbb{H}^s(\mathbb{S}^d)$ with $d/2 < s < (d+1)/2$.

We remark that for $s = (d+1)/2$ ($s = (d+1)/2 + L$) the worst-case error above equals a constant multiple of the spherical cap $\mathbb{L}_2$-discrepancy (or a generalization for integers $L \geq 1$). This is in analogue to Warnock's formula for the unit cube.

One way to obtain good numerical integration nodes is to minimize above energy functional. This is a highly non-linear optimization problem. One would like to have explicit constructions of good node sets. A straightforward approach is to lift digital nets or sequences to the d-sphere using an area preserving map. This leads to spherical nets and sequences and also to spherical lattice rules (spherical Fibonacci rules). A discussion of theoretical and numerical results for these constructions will round off the talk.

Bases with small representation function

Artūras Dubickas

Abstract

Let A be a subset of the set of nonnegative integers $\mathbf{N} \cup \{0\}$, and let $r_A(n)$ be the number of representations of $n \geq 0$ by the sum $a + b$ with $a, b \in A$. Then $\left(\sum_{a \in A} x^a\right)^2 = \sum_{n=0}^{\infty} r_A(n) x^n$. The set $A \subseteq \mathbf{N} \cup \{0\}$ is called a *basis* of $\mathbf{N} \cup \{0\}$ if $r_A(n) \geq 1$ for each $n \geq 0$. A conjecture of Erdős and Turán asserts that $\limsup_{n \to \infty} r_A(n) = \infty$ if A is a basis of $\mathbf{N} \cup \{0\}$. By an old result of Erdős (1954), there exists a basis A of $\mathbf{N} \cup \{0\}$ for which $r_A(n) \leq c \log n$ with some positive constant $c > 0$. We show that this result holds with the constant $2e$, namely, that there exists a basis A of $\mathbf{N} \cup \{0\}$ whose representation function $r_A(n)$ satisfies $r_A(n) < (2e + \varepsilon) \log n$ for each sufficiently large integer n. Towards a polynomial version of the Erdős-Turán conjecture we prove that for each $\varepsilon > 0$ and each sufficiently large integer n there is a set $A \subseteq \{0, 1, \ldots, n\}$ such that the square of the corresponding Newman polynomial $f(x) := \sum_{a \in A} x^a$ of degree n has all of its $2n+1$ coefficients in the interval $[1, (1 + \varepsilon)(4/\pi)(\log n)^2]$.

The correct order of growth for $H(f^2)$ of those *reciprocal* Newman polynomials f of degree n whose squares f^2 have all their $2n + 1$ coefficients positive is $\sqrt{n}$. More precisely, if the Newman polynomial $f(x) = \sum_{a \in A} x^a$ of degree n is reciprocal, i.e., $A = n - A$, then $A + A = \{0, 1, \ldots, 2n\}$ implies that the coefficient for x^n in $f(x)^2$ is at least $2\sqrt{n} - 3$. In the opposite direction, we explicitly construct a reciprocal Newman polynomial $f(x)$ of degree n such that the coefficients of its square $f(x)^2$ all belong to the interval $[1, 2\sqrt{2n} + 4]$.

Best possible lower bounds for the star discrepancy of $(0,1)$-sequences

Henri Faure

Abstract

In this communication, we will present best possible lower bounds for the star discrepancy of several sub-classes of $(0,1)$-sequences, which are one-dimensional versions of (t,s)-sequences as introduced by Niederreiter. Originally, this study was motivated by a best possible lower bound on the star discrepancy of digitally shifted van der Corput sequences in base 2 as shown in [2, Corollary 4] and the question: "Is it true that the constant $1/(6\log 2)$ is also best possible for any digitally shifted NUT (nonsingular upper triangular) digital $(0,1)$-sequence in base 2?" Quickly, it appeared that for this problem the case of base 2 with digital shifts is not simpler than the general case of arbitrary bases with linear digit scramblings. Further, we found it is even possible to deal with arbitrary permutations acting in place of the diagonal entries of generating matrices.

For short we consider sequences $X_b^{\Sigma,C}$ in base b generated by strict upper triangular matrices C with entries in $\mathbb{Z}_b$, completed on the diagonal by sequences of permutations $\Sigma = (\sigma_r)_{r\geq 0} \in \mathfrak{S}_b^{\mathbb{N}}$. (A precise definition will be given in the talk.) Essentially, our results read as follows

Let $\mathcal{C}_{SUT}$ be the set of strict upper triangular matrices, let $\sigma \in \mathfrak{S}_b$ such that $D^*(S_b^\sigma) = D(S_b^\sigma)$ and define $\tau \in \mathfrak{S}_b$ by $\tau(k) = b-k-1$. Then

$$\inf_{\substack{\Sigma\in\{\sigma,\tau\circ\sigma\}^{\mathbb{N}}\\ C\in\mathcal{C}_{SUT}}} \limsup_{N\to\infty} \frac{D^*(N, X_b^{\Sigma,C})}{\log N} = \frac{\alpha_b^\sigma}{2\log b}, \text{ where } \alpha_b^\sigma \text{is effectively computable.}$$

In the special case of identity id, with the same notations, we obtain

$$\inf_{b\geq 2} \inf_{\substack{\Sigma\in\{\mathrm{id},\tau\}^{\mathbb{N}}\\ C\in\mathcal{C}_{SUT}}} \limsup_{N\to\infty} \frac{D^*(N, X_b^{\Sigma,C})}{\log N} = \frac{1}{4\log 3} = 0.2275\ldots$$

And for digitally shifted NUT digital $(0,1)$-sequences in base 2, denoted $Z_2^{\Delta,C}$, we answer the original question

$$\inf_{\substack{\Delta\in\mathbb{Z}_2^{\mathbb{N}}\\ C\in\mathcal{C}_{NUT}}} \limsup_{N\to\infty} \frac{D^*(N, Z_2^{\Delta,C})}{\log N} = \frac{1}{6\log 2} = 0.2404\ldots$$

References

[1] Faure, H.: *Discrepancy and diaphony of digital* $(0,1)$*-sequences in prime bases*, Acta Arith. **117** (2005), 125–148.

[2] Kritzer, P. — Larcher, G. — Pillichshammer, F.: *A thorough analysis of the discrepancy of shifted Hammersley and van der Corput point sets*, Ann. Mat. Pura Appl. **186** (2007), 229–250.

Notes on a family of preimage-resistant functions

János Folláth

Abstract

Cryptographic hash functions are important building blocks for most of the protocols and play a fundamental role in verifying passwords and creating digital signatures. Their use is important for constructing cryptographically secure pseudo-random-number generators. An important property of cryptographic hash functions is preimage-resistance. In [1] the authors proposed a new Family of Preimage-Resistant Functions.

An important property of cryptographic hash functions is the strict avalanche criterion [2]. Although the functions in question do not possess the avalanche criterion in the strict sense, a slightly weaker statement holds.

Theorem 1. *Let us define* $f \in \mathbb{F}_{2^k}[x_1, \ldots, x_m]$ *as*

$$f(x_1, \ldots, x_m) = \sum_{i=1}^{m} \alpha_i x_i^n + \sum_{i=1}^{m} \beta_i x_i,$$

where $n = 2^l + 1$ *such that* $(l, k) = 1$. *Then*

$$\begin{aligned}(1 - q\varepsilon)^{m-1} \left(\frac{1}{q} - \varepsilon\right) \leq & P\big(f(x_1, \ldots, x_m) - f(x_1 + \delta_1, \ldots, x_m + \delta_m) = \gamma\big) \\ \leq & (1 + q\varepsilon)^{m-1} \left(\frac{1}{q} + \varepsilon\right),\end{aligned}$$

where $0 \leq \varepsilon \leq (q - n)q^{-\frac{3}{2}}$.

The implementation discussed in [1] is reconsidered, and improvements have been made. The avalanche criterion of the implemented version have been tested and the results visualized.

References

[1] Bérczes, A. — Folláth, J.— Pethő, A.: *On a family of preimage-resistant function*, Tatra Mt. Math. Publ. **47** (2010), 1–13.

[2] Webster, A. F. — Tavares, S. E.: *On the Design of S-Boxes*. In: Crypto '85 proceedings, Advanced in Cryptology, Springer, New York, 1986.

On the weighted $(\mathcal{W}(b);\gamma)-$diaphony of the generalized van der Corput sequence and the Zaremba-Halton net

Vassil S. Grozdanov

Abstract

In this talk, we will present a new weighted $b-$adic version of the diaphony, the so-called weighted $(\mathcal{W}(b);\gamma)-$ diaphony, as a numerical measure for irregularity of distribution of sequences in the $s-$dimensional unit cube. The exact order $\mathcal{O}\left(\frac{1}{N}\right)$ of the $(\mathcal{W}(b);\gamma)-$diaphony of the generalized Van der Corput sequence is obtained. For an arbitrary integer $\nu \geq 3$ the exact order $\mathcal{O}\left(\frac{\log N}{N^2}\right)$ $(N = b^{\nu})$ of the $(\mathcal{W}(b);\gamma)-$diaphony of the generalized Zaremba-Halton net is obtained. Also the exact constant in this exact order is shown. These orders are smaller than the corresponding orders of the classical $b-$adic diaphony. This is a joint work Vesna Dimitrievska-Ristovska, Dora Mavrodieva, Stanislava Stoilova.

On the correlation of subsequences

Katalin Gyarmati

Abstract

In 1997 Sárközy and Mauduit introduced the well-distribution measure (W) and the correlation measure of order ℓ (C_ℓ) of binary sequences E_N as measures of their pseudorandomness. For a truly random binary sequence these measures are small ($\ll N^{1/2}(\log N)^c$ for a sequence of length N). Several constructions have been given for which these measures are small, namely they are $\ll N^{1/2}(\log N)^c$, thus the sequence E_N has strong pseudorandom properties. But in certain applications, e.g., in cryptography, it is not enough to know that the sequence has strong pseudorandom properties, it is also important that the subsequences E_M (where E_M is of the form $\{e_x, e_{x+1}, \dots, e_{x+M-1}\}$) also have strong pseudorandom properties for values M possibly small in terms of N. In this talk I will deal with this problem in case of M values $M \gg N^{1/4+\varepsilon}$.

Function systems in the theory of u.d. mod 1

Peter Hellekalek

Abstract

Any construction method for finite or infinite sequences ω of points in $[0,1)^s$ will have to employ arithmetical operations like addition, on some suitable domain D.

For the analysis of the equidistribution behavior of such sequences it is necessary to employ function systems $\mathcal{F}$ that possess several properties.

$\mathcal{F}$ should be convergence determining, i.e., a Weyl criterion for $\mathcal{F}$ should hold.

$\mathcal{F}$ should be suitable for the type of addition that is used on D. If D is a compact abelian group, then there is a natural choice for $\mathcal{F}$, namely the dual group of D.

In this talk, this observation will be our starting point. For several types of addition, like addition of digit vectors over $\mathbb{F}_2$ without or with carry, we will discuss the associated function systems. We will present the appropriate variants of the Weyl criterion and of the inequality of Erdös-Turán-Koksma. Further, we will derive the related version of diaphony and of the spectral test. Finally, we will exhibit a general concept behind these uniform distribution measures, the Weyl array.

In the last part of the talk, we will extend our technique to hybrid sequences.

References

[1] Hellekalek, P.: *A general discrepancy estimate based on p-adic arithmetics*, Acta Arith. **139** 2009, 117–129.

[2] Hellekalek, P.: *A notion of diaphony based on p-adic arithmetic*, Acta Arith. **145** 2010, 273–284.

[3] Hellekalek, P.: *Hybrid function systems in the theory of uniform distribution of sequences* (L. Plaskota and H. Wozniakowski, eds.), in: *Monte Carlo and Quasi-Monte Carlo Methods in Scientific Computing*, Warsaw, 2010, Lecture Notes in Statist., Springer, New York, 2012.

[4] Hellekalek, P.: *On Weyl arrays and the* **b***-adic spectral test*, 2012, (unpublished).

[5] Hellekalek, P. — Kritzer, P.: *On the diaphony of some finite hybrid point sets*, 2011, (submitted).

[6] Hellekalek, P. — Niederreiter, N.: *Constructions of uniformly distributed sequences using the b-adic method*, Unif. Distrib. Theor. **6** 2011, 185–200.

Construction of uniformly distributed linear recurring sequences modulo powers of 3

Tamás Herendi

Abstract

Linear recurring sequences are among the earliest and most widely studied methods to generate pseudo random number sequences. In [1] the theoretical background is developed for proving uniform distribution property of linear recurring sequences modulo prime powers. Here it is shown, that if a linear recurring sequence is uniformly distributed modulo p^s, where p is a prime and s is bound depending only on the order of the recurrence relation, then the sequence is uniformly distributed modulo p^t, for any t. In [2] we develop the theory of construction of linear recurring sequences which are uniformly distributed modulo 2^n for any $n \in \mathbb{N}$ and give an algorithm based on the results. The constructed sequences has arbitrary large period length depending only on the computational power of the used machine.

In the present work the results of [2] are modified to be able to apply for the case, when the base prime of the modulus is 3.

Corresponding to some more general results, it is assumed that the generating polynomial of the candidate sequence contains a factor of $(x+1)^2$. First, it is shown, that if the period length of the observed sequence is large enough, then it is uniformly distributed modulo 3. Obviously, this is a necessary condition for the targeted result.

Then, applying the methods of [1], it is proven, that the chosen sequence has some strict periodicity properties. As a consequence, one can determine a small set of recurrence relations, such that one of them have the required uniform distribution property.

Based on the proofs, an algorithm is given for the construction (selecting from the previously determined set) of the suitable recurring sequence.

References

[1] T. Herendi: *Uniform distribution of linear recurring sequences modulo prime powers*, Finite Fields and Applications, **10** (2004), 1–23.

[2] T. Herendi: *Construction of uniformly distributed linear recurring sequences modulo powers of 2* (to appear).

Enhanced matrix multiplication algorithm for FPGA

Tamás Herendi — Sándor Roland Major

Abstract

The presented work is based on a previous research done by Herendi [1] on uniformly distributed random number sequences. The fast, efficient and reliable computation of "high quality" random values is an important requirement of many applications, e.g., cryptographic protocols. In [1], an algorithm is given for the construction of uniformly distributed linear recurring sequences with arbitrarily large periods. The most computation demanding step of this algorithm raises large matrices to powers exponentially large in the matrix size (e.g., raising 1000×1000 size matrices to a power in the order of magnitude of 2^{1000}).

While this operation can become very time-consuming on traditional architectures, it can be greatly speed up using the unique options of an FPGA. A previous implementation working on 896×896 size matrices, achieving a speedup factor of ~ 200 compared to a highly optimized PC implementation has already been detailed in [2].

Further research on the algorithm enables new optimization opportunities, leading to a significant restructuring of the FPGA implementation. This new module is currently in development, utilizing the unique architecture of the hardware and special properties of the algorithm. The presented solution manages a speedup factor of ~ 10 over the previous version.

References

[1] Herendi, T: *Construction of uniformly distributed linear recurring sequences modulo powers of 2* (to appear).

[2] Herendi, T.—Major, R.S.: *Modular exponentiation of matrices on FPGA-s*, Acta Univ. Sapientiae, Informatica, **3** (2011), 172–191.

Uniform distribution of generalized Kakutani's sequences of partitions

Markus Hofer

Abstract

We consider a generalized version of Kakutani's splitting procedure where an arbitrary starting partition π is given and in each step all intervals of maximal length are split into m parts, according to a splitting rule ρ. We give conditions on π and ρ under which the resulting sequence of partitions is uniformly distributed.

Constructions and properties of finite-row (t, s)-sequences

Roswitha Hofer

Abstract

We consider the special class of digital (t, s)-sequences, where the generator matrices are finite-row matrices, that are $\mathbb{N} \times \mathbb{N}$-matrices satisfying that each row consists of only finitely many nonzero entries. We discuss different ways of constructing such finite-row generating matrices and identify certain interesting properties of these matrices and the corresponding low-discrepancy sequences.

Lattice point problems in the plane and their relationship to uniform distribution methods

Martin Huxley

Abstract

To find the area of a shape S by "counting squares", we put a sheet of transparent squared paper over S, and count the squares inside. Some squares cross the boundary. For these, we pick a representative point (u, v) in the unit square, and count a square when the corresponding point in it lies in S. The error can be analysed in terms of the boundary arcs of S reduced modulo the unit square. This leads to problems of uniform distribution.

On normal numbers

Imre Kátai

Abstract

In a series of paper written jointly with Jean-Marie De Koninck we constructed normal numbers based on classification of prime divisors of integers, one example of which is the next assertion.

Let $q \geq 2$, $q \in \mathbb{N}$, $\mathcal{A}_q := \{0, 1, \cdots, q-1\}$. Given $n = p_1^{e_1} \dots p_{k+1}^{e_{k+1}}$ with primes $p_1 < \cdots < p_{k+1}$ and positive exponents $e_1, \dots, e_{k+1}$ we define the arithmetic function $H(n) = c_1(n) \cdots c_k(n)$ ($H(n)$ is a word over $\mathcal{A}_q$, where

$$c_j(n) = \left\lfloor \frac{q \log p_j}{P \log p_{j+1}} \right\rfloor \ (j = 1, \dots, k).$$

Let

$$\xi = 0, H(2)H(3) \dots,$$

ξ is the real number the q-ary expansion of which is the infinite sequence standing on the right hand side. Then ξ is a normal number.

On congruences with products of variables and double character sums [1]

Sergei V. Konyagin

Abstract

The talk is based on a joint paper of the speaker with J. Bourgain, M. Z. Garaev and I. E. Shaprlinski.

For a prime p, let $\mathbb{F}_p$ be the field of residues modulo p. For positive integers h and ν and an element $s \in \mathbb{F}_p$, we denote by $K_\nu(p,h,s)$ the number of solutions of the congruence

$$\begin{gathered}(x_1+s)\dots(x_\nu+s) \equiv (y_1+s)\dots(y_\nu+s) \not\equiv 0 \pmod p,\\ 1 \le x_1,\dots,x_\nu,\ y_1,\dots,y_\nu \le h.\end{gathered} \tag{1}$$

Clearly, $K_\nu(p,h,s) \ge h^\nu$. We prove the inequality

$$K_\nu(p,h,s) \le h^\nu \exp\left(c(\nu)\frac{\log h}{\log\log h}\right)$$

if $3 \le h \le p^{\alpha_\nu}$, where $\alpha_\nu = 1/\max(\nu^2-2\nu-2, \nu^2-3\nu+4)$ and $c(\nu)$ depends only on ν.

Also, for $\nu = 2$ we estimate from above the number of solutions of congruences similar to (1) with additional restrictions on variables and prove several applications of our estimates. In particular, we establish nontrivial estimates for a double character sum

$$\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{A}}\chi(a+b),$$

where χ is a non-principal multiplicative character modulo a prime p, $\mathcal{A} \subset [M, M+A]$ for some integer M, $A \le p^{1/2}$ and $\#\mathcal{A} > p^{9/20+\varepsilon}$ for some $\varepsilon > 0$.

[1]The research of Sergei Konyagin was partially supported by Russian Fund for Basic Research, Grant N. 11-01-00329.

On the distribution properties of hybrid point sets [1]

Peter Kritzer

Abstract

Quasi-Monte Carlo (QMC) methods are important tools in numerical integration. For the point sets serving as the integration nodes in QMC algorithms, it is advantageous if they are evenly spread in the integration domain. A recent topic in this field of research is that of hybrid QMC point sets, which are finite or infinite sequences of points in the unit cube, the components of which stem from two or more different other QMC point sets. Studying the distribution properties of such point sets is a challenging problem, and in many cases it is not clear if or under which conditions the hybrid point sets are uniformly distributed.

In this talk, we discuss recent findings on two special types of hybrid point sets, namely:

- point sets based on Halton sequences and lattice points,
- point sets based on (t, s)-sequences and lattice points.

We present results that guarantee the existence of such hybrid point sets with excellent distribution properties, where we use the recently introduced hybrid diaphony as a way of measuring uniformity of distribution.

This talk is based on joint work with P. Hellekalek (Salzburg) and F. Pillichshammer (Linz).

[1] P. Kritzer gratefully acknowledges the support of the Austrian Science Fund (FWF), Project P23389-N18.

Group extensions: from old to new results with various applications

Pierre Liardet

Abstract

Let X be a set and let $(\Gamma, .)$ be a group. For given maps $T : X \to X$ and $\varphi : X \to \Gamma$, the map $T_\varphi : X \times \Gamma \to X \times \Gamma$, defined by

$$T_\varphi(x, \gamma) = (Tx, \gamma.\varphi(x)),$$

is called a (φ, Γ)-group extension of base T or a skew product of T with cocycle φ. In the case of topological dynamical systems, X is a compact metrizable space, T is continuous, Γ is a locally compact metrizable group and φ is continuous. In the metric theory of dynamical systems, X is a standard Borel space $(X, \mathcal{B})$ equipped with a σ-finite measure μ, T is an endomorphism of $(X, \mathcal{B}, \mu)$, Γ is a compact (eventually locally compact) metrizable group and φ is measurable. Let ν be the Haar measure of Γ (eventually a right invariant measure).

The case where X and Γ are the one dimensional torus (usually identified to $[0, 1[$ (mod 1), or the unit circle $\mathbf{U}$ as well), was introduced by H. Anzai (1951). Such products and generalizations have been intensively studied into many directions. In this talk, we pay attention to various applications in uniform distribution theory in regard to minimality, ergodicity and spectral properties of skew products.

We will start from examples to exhibit tools that can be used for studying both topological and metrical properties. When T and φ are μ-continuous and $(T_\varphi, \mu \otimes \nu)$ is ergodic (and Γ compact), a useful result says that if x is generic for (T, μ), then (x, γ), with any γ in Γ, is generic for $(T_\varphi, \mu \otimes \nu)$. Consequently, the sequence $n \to \varphi(x).\varphi \circ T(x) \cdots \varphi \circ T^n(x)$ is uniformly distributed in Γ.

Example: let $X = \Gamma = [0, 1[$ and $\varphi(x) = \frac{1}{x+1}$, and let $u = (u_k)$ be a sequence uniformly distributed in X. A rather natural question is to know when the sequence $\Sigma_u : n \mapsto \sum_{n=1}^{n} \frac{1}{u_k+1}$ is uniformly distributed mod 1. We show that the answer is positive if $(u_n)_n$ is completely uniformly distributed mod 1. In that case φ can be replaced by a large family of cocycles. The proof follows easily from a classical characterization of ergodicity for skew products. The answer also is positive for sequences of the form $u_n = n\alpha (\text{mod } 1)$ where α is irrational, but the proof is much more complicated and extension to other cocycles needs extra regular conditions. Statistical independency in between such sequences are discussed. Notice that the uniform distribution of Σ_u is unknown (but positive answer is conjectured) for $u_n = q^n x (\text{mod } 1)$ where q is an integer ≥ 2 and x normal in base q.

The case where T is the Gauss transformation of regular continued fraction on $[0, 1[$ (and more generally when T is an S-expansion in the sense of C. Kraaikamp) leads to a large domain of investigation. For $x \in [0, 1[$, let $p_n(x)/q_n(x)$ be the

sequence of T-convergents of x. We present some generalizations of an old result (1987) we proved, saying that for all generic point x for T the frequency of the $q_n(x)$ which are square free exists and equal to an explicit constant.

Unimodular multiplicative sequences related to numeration systems give rise to interesting skew products and have been intensively studied. We recall some old results and give new ones involving in dependency and spectral properties.

Uniform distribution modulo 1 of ratios of various arithmetic functions

Florian Luca

Abstract

This is a survey talk on various results concerning the uniform distribution modulo 1 of ratios of various arithmetic functions. For example, let $p_a(n),\ p_g(n),\ p_h(n)$ be the arithmetic, geometric and harmonic means of the prime factors of the positive integer n, respectively. All the above sequences are uniformly distributed modulo 1. Furthermore, the arithmetic mean of the first n primes is also uniformly distributed modulo 1. We also present some new results. For example, for an integer $a > 1$ we show that the sequence a^n/n is dense module 1. Finally, we present an amusing application of uniform distribution modulo 1 to the problem of bounding from above the counting function of positive integers n such that F_n is a base 10 palindrome. These results are joint with various colleagues such as W. D. Banks, J. Cilleruelo, J. M. Deshouillers, M. Z. Garaev, I. Kátai, A. Kumchev, J. Rué, I. E. Shparlinski and R. Tesoro.

Quasi-Monte Carlo methods for integration of functions with dominating mixed smoothness

Lev Markhasin

Abstract

In a celebrated construction, Chen and Skriganov gave explicit examples of point sets achieving the best possible L_2-norm of the discrepancy function. We consider the discrepancy function of the Chen-Skriganov point sets in Besov spaces of dominating mixed smoothness and show that they also achieve the best possible rate in this setting. The proof uses a b-adic generalization of the Haar system and corresponding characterizations of the Besov space norm. Results for further function spaces and integration errors are concluded.

On the distribution of the elliptic curve power generator

László Mérai

Abstract

Let $P \in \mathcal{E}(\mathbb{F}_q)$ be a point of order T on a nonsupersingular elliptic curve $\mathcal{E}$. The *elliptic curve power generator* builds a sequence by the rule

$$P_0 = P \quad \text{and} \quad P_n = eP_{n-1} \quad n = 1, 2, \dots$$

with a fixed integer e with $(T, e) = 1$.

An obvious way to compute the elements of the sequence is to compute e which would be the solution of the discrete logarithm problem on this curve. On the other hand to compute an element from the previous part of the sequence one may need to solve the computational Diffie-Hellman problem. Since in general both of these problems are assumed to be hard, the elliptic curve power generator is thought to have good pseudorandom properties.

The distribution of the coordinate sequence $(x(P_n))$ have been widely studied, especially its discrepancy. In this talk results are presented about the distribution of the sequences $(f(P_n))$ where $f \in \mathbb{F}_q(\mathcal{E})$ is a general (not constant) rational function.

The main tool to obtain, for example, discrepancy bound is to prove the following exponential sum estimate

$$\max_{c_1,\dots,c_s} \sum_{P \in \mathcal{H}} \psi\left(\sum_{i=1}^{s} c_i f(k_i P)\right) \ll s \deg f K^2 q^{1/2},$$

where ψ is a non-trivial additive character of $\mathbb{F}_q$, and the bound is uniform in all $1 \le k_1 < \dots < k_s \le K$.

Hausdorff dimension of sets of numbers with prescribed digit densities

Ladislav Mišík — Jan Šustek — Bodo Volkmann

Abstract

For a set A of positive integers $a_1 < a_2 < \dots$ let $\underline{d}(A), \overline{d}(A)$ denote its lower and upper asymptotic density. The gap density is defined as $\lambda(A) = \limsup_{n\to\infty} \frac{a_{n+1}}{a_n}$. We investigate the class $\mathcal{G}(\alpha,\beta,\gamma)$ of all sets A with $\underline{d}(A) = \alpha$, $\overline{d}(A) = \beta$ and $\lambda(A) = \gamma$ for given α,β,γ with $0 \le \alpha \le \beta \le 1$ and $1 \le \gamma \le \frac{\beta}{\alpha}$ if $\alpha > 0$. Using the classical dyadic mapping $\varrho(A) = \sum_{n=1}^{\infty} \frac{\chi_A(n)}{2^n}$, where χ_A is the characteristic function of A, we are interested in the Hausdorff dimension of the ϱ-image set $\varrho\mathcal{G}(\alpha,\beta,\gamma)$. The main result states that

$$\dim \varrho\mathcal{G}(\alpha,\beta,\gamma) = \min\Big\{\delta(\alpha), \delta(\beta), \frac{1}{\gamma} \max_{\sigma\in[\alpha\gamma,\beta]} \delta(\sigma)\Big\},$$

where δ is the entropy function

$$\delta(x) = \frac{x\log x + (1-x)\log(1-x)}{\log\frac{1}{2}}.$$

We also present a general formula for computing the Hausdorff dimension of ϱ-image sets satisfying some conditions.

Oscillating theorems for irrationality measures

Nikolay Moshchevitin [1]

Abstract

For a real α we consider the irrationality measure function

$$\psi_\alpha(t) = \min_{1\le x\le t,\, x\in\mathbb{Z}} ||x\alpha||$$

(here $||\cdot||$ stands for the distance to the nearest integer).

In [1] it was proved that for any two different irrational numbers α, β such that $\alpha \pm \beta \notin \mathbb{Z}$ the difference function

$$\psi_\alpha(t) - \psi_\beta(t)$$

changes its sign infinitely many times as $t \to +\infty$.

We consider the function $\mu_\alpha(t)$ associated with Minkowski diagonal continued fraction expansion for α (see [3]). The situation with oscillating property of the difference

$$\mu_\alpha(t) - \mu_\beta(t)$$

is quite different. In [2] it is shown that there exist real α and β such that they are linearly independent over $\mathbb{Z}$ together with 1 and

$$\mu_\alpha(t) > \mu_\beta(t),\ \forall t \ge 1.$$

However as it is shown in the same paper [2] for *almost all* pairs $(\alpha, \beta) \in \mathbb{R}^2$ (in the sense of Lebesgue measure) the difference does oscillate as $t \to \infty$.

We will discuss certain results on oscillating properties of differences

$$\int_1^T \psi_\alpha(t)dt - \int_1^T \psi_\beta(t)dt$$

(see [5]) as well as various multidimensional generalizations and related Diophantine spectra [4].

[1]Research is supported by RFBR grant No.12-01-00681-a and by the grant of Russian government, project 11 G.34.31.0053.

References

[1] Kan, I.D.—Moshchevitin, N.G.: *Obtaining Approximations to two real numbers*, Unif. Distrib. Theory **5** (2010), no.2, 79–86.

[2] Kan, I.D.—Moshchevitin, N.G.—Chaika, J.: *On Minkowski diagonal functions for two real numbers*, (M. Amou and M. Katsurada, eds.) in: *The Proceedings Diophantine Analysis and Related Fields 2011'*, AIP Conf. Proc. No. 1385, American Institute of Physics, New York, 2011, pp. 42–48.

[3] H. Minkowski, H.: *Über die Annäherung an eine reelle Grösse durch ratiolale Zahlen*, Math. Ann., **54** (1901), 91–124.

[4] Moshchevitin, N.G.: *On Minkowski diagonal continued fraction*, preprint (2012), available at arXiv:1202.4622v2.

[5] Shatskov, D.O.: *On the irrationality measure function in average*, preprint (2012), available at arXiv:1205.4082v1.

On the metric theory of p-adic continued fractions

Radhakrishnan Nair

Abstract

An analogue of the regular continued fraction expansion for the p-adic numbers for prime p was given by T. Schneider, such that for x in $p\mathbb{Z}_p$, i.e. the open unit ball in the p-adic numbers, we have uniquely determined sequences $(b_n \in \{1, 2, \ldots \ldots, p-1\}, a_n \in \mathbb{N})$ $(n = 1, 2, \ldots)$ such that

$$x = \cfrac{p^{a_0}}{b_1 + \cfrac{p^{a_1}}{b_2 + \cfrac{p^{a_2}}{b_3 + \cfrac{p^{a_3}}{b_4 + \ddots}}}}.$$

A sample result we prove is that if p_n $(n = 1, 2, \ldots)$ denotes the sequences of rational primes, we have

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} a_{p_n}(x) = \frac{p}{p-1},$$

almost everywhere with respect to Haar measure. In the case where p_n is replaced by n this result is due to J. Hirsh and L. C. Washington. The proofs rely on pointwise subsequence and moving average ergodic theorems. This is joint work with J. Hančl (Ostrava), A. Jaššová (Liverpool), and P. Lertchoosakul (Liverpool).

References

[HJLN] Hančl, J.— Jaššová, A. — Lertchoosakul, P. — Nair, R.: *On the metric theory of p-continued fractions*, (manuscript 25 pages).

[HiWa] Hirsh, J. — Washington, L.C.: *P-adic continued fractions*, Ramanujan J. Math. **25**, (2011), no. 3, 389–403.

[SC] Schneider, T.: *Über p-adische Kettenbrche*. In: *Symposia Mathematica*, Vol. **IV**, INDAM, Rome, 1968/69, Academic Press, London, 1970, pp. 181–189.

Omega results for a class of arithmetic functions (On a question of A. Schinzel) [1]

Werner G. Nowak — Manfred Kühleitner

Abstract

The class of arithmetic functions f under consideration is characterized by a generating Dirichlet series

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \zeta^2(s)\zeta(2s-1)(\zeta(2s))^M H(s)\,, \tag{1}$$

where ζ denotes the Riemann zeta-function, M is any fixed integer, and the function $H(s)$ has an Euler product which converges absolutely in a half-plane $\Re(s) > \sigma_0$ for some $\sigma_0 < \frac{1}{2}$.

At the Czech and Slovak Number Theory Conference in fall 2011 in Stará Lesná, an account was given on approaches to derive asymptotics for $\sum_{n\le x} f(n)$, with upper bounds for the error term, culminating in the estimate [1]

$$\sum_{n\le x} f(n) = \mathrm{Res}_{s=1}\left(F(s)\frac{x^s}{s}\right) + O\left(x^{547/832}(\log x)^{26947/8320}\right) \quad \left(\frac{547}{832} = 0.65745\ldots\right).$$

In the discussion following that talk, Professor Schinzel raised the question: *"What can be said about Omega-estimates?"*

Here we give the following general answer [2]:

Theorem 1. *For any arithmetic function f with a generating Dirichlet $F(s)$ according to* (1)*,*

$$\sum_{n\le x} f(n) = \mathrm{Res}_{s=1}\left(F(s)\frac{x^s}{s}\right) + \Omega\left(\frac{\sqrt{x}\,(\log x)^2}{(\log\log x)^{|M+1|}}\right).$$

Special examples of interest are discussed.

References

[1] Krätzel, E. — Tóth, L. — Nowak, W. G.: *On certain arithmetic functions involving the greatest common divisor*, Centr. Europ. J. Math. **10** (2012), no. 2, 761–774.

[2] Kühleitner, M. — Nowak, W. G.: *On a question of A. Schinzel: Omega estimates for a special type of arithmetic functions*, Centr. Europ. J. Math. (to appear).

[1] The authors gratefully acknowledge support from the Austrian Science Fund (FWF) under project Nr. P20847-N18.

Van der Corput sequences and permutation polynomials [1]

Florian Pausinger

Abstract

Generalized van der Corput sequences are one-dimensional, infinite sequences in the unit interval. They are generated from permutations in integer base b and are the building blocks of the multi-dimensional Halton sequences. Motivated by recent progress of Atanassov on the uniform distribution behavior of Halton sequences, we study permutations of the form $P(i) = ai \pmod b$ for coprime integers a and b. We show that multipliers a that either divide $b-1$ or $b+1$ generate van der Corput sequences with weak distribution properties and we relate them to sequences generated from identity permutations. These are, due to Faure, the weakest distributed generalized van der Corput sequences. Furthermore, we discuss distribution properties of sequences generated from a wider class of permutations given by permutation polynomials due to Carlitz.

[1]This work is supported by the Graduate School of IST Austria (Institute of Science and Technology Austria).

Recent results for the discrepancy of polynomial lattice point sets [1]

Friedrich Pillichshammer

Abstract

Polynomial lattice point sets (PLPSs) as introduced by Niederreiter in 1992 are polynomial versions of classical lattice point sets due to Korobov and Hlawka. The main difference is that here one uses polynomial arithmetic in $\mathbb{F}_b[x]$ instead of the usual integer arithmetic. PLPSs are special instances of digital (t, m, s)-nets which are among the most widely used classes of node sets for quasi-Monte Carlo integration rules.

For quasi-Monte Carlo rules the integration error is intimately connected with the disrepancy of the underlying node set via the Koksma-Hlawka inequality. In this talk we review recent results for the classical and weighted star discrepancy of PLPSs.

[1]Supported by the Austrian Science Fund (FWF), Project S9609.

On the family complexity of families of binary sequences

András Sárközy

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 to know that our family of "good" binary sequences is large; it can be much more important to know that the family has a "rich", "complex" structure. Thus in 2003 Ahlswede, Khachatrian, Mauduit and Sárközy introduced and studied the notion of family complexity as a quantitative measure of a property of families of binary sequences which plays an especially important role in cryptography. Since that the family complexity of many families of binary sequences with strong pseudorandom properties has been estimated and the notion of family complexity has been extended in various directions. In my talk I will give a survey of all these results.

Additive structures in multiplicative subgroups

Ilya D. Shkredov

Abstract

We investigate various "random" properties of multiplicative subgroups of finite fields such as intersections of such subgroups with its additive shifts, basis properties, representations of subgroups as sumsets, intersections with arithmetic progressions and so on. We give a survey of old and new results in the field.

Some unsolved problems in the theory of distribution functions

Oto Strauch

Abstract

Some functional and some integral equations need to be solved in various parts of the theory of distribution functions (d.f.s) of sequences. In this lecture we will discuss the open problems related to the following equations:

$$g(x/2)+g\big((x+1)/2\big)-g(1/2) = g(x/3)+g\big((x+1)/3\big)+g\big((x+2)/3\big)-g(1/3)-g(2/3), \quad (1)$$

$$g(x)=\sum_{n=1}^{\infty} g\left(\frac{1}{n}\right)-g\left(\frac{1}{n+x}\right), \quad (2)$$

$$x=\sum_{i=0}^{\infty}\left(g\left(\frac{1}{b^i}\right)-g\left(\frac{1}{b^{i+x}}\right)\right) \quad \text{for } x\in[0,1] \quad \text{and d.f.s } g(x), \quad (3)$$

$$\int_0^1\int_0^1 F(x,y)\mathrm{dg(x)dg(y)}=0, \quad (4)$$

$$\int_0^1\int_0^1 F(x,y)\mathrm{dg(x,y)},\ \mathrm{g(x,y)} \text{ take copulas.} \quad (5)$$

- The functional equation (1) connects with the sequence
$$x_n=\xi(3/2)^n \bmod 1, \quad n=1,2,\dots$$
- The functional equation (2) connects with the Gauss-Kuzmin theorem and iterated sequence
$$f(\alpha), f\big(f(\alpha)\big),\dots, \quad \text{where } f(x)=1/x \bmod 1.$$
- The functional equation (3) connecs with Benford law.
- The integral equation (4) is used to find d.f.s of x_n satisfying the limit below
$$\lim_{N\to\infty}\frac{1}{N^2}\sum_{m,n=1}^{N}F(x_m,x_n)=0.$$
- Integrals (5) serve to finding limit points of
$$\frac{1}{N}\sum_{n=1}^{N}F(x_n,y_n), N=1,2,\dots, \text{ where } x_n \quad \text{and} \quad y_n \text{ are } u.d.$$

Any general solutions have not been known in all such cases, see web page http://www.boku.ac.at/MATH/udt/unsolvedproblems.pdf

A new construction of (0,1)-sequences

Shu Tezuka

Abstract

In this talk, we consider the hybridization of van der Corput sequences and polynomial Weyl sequences, which includes the former as one extreme of base polynomial with degree one, and the latter as the other extreme of base polynomial with degree infinity. We show that between these two extremes the hybridization provides one- dimensional low-discrepancy sequences for base polynomial with any positive degree, and thereby leads to a new construction of digital $(0, 1)$-sequences.

Farey fraction spin chains and Gauss-Kuz'min statistics for quadratic irrationals

Alexey Ustinov

Abstract

Farey fraction spin chains were introduced by Kleban and Özlük in [2]. In this model spin configuration

$$\underbrace{\uparrow\uparrow\ldots\uparrow}_{a_1}\underbrace{\downarrow\downarrow\ldots\downarrow}_{a_2}\underbrace{\uparrow\uparrow\ldots\uparrow}_{a_3}\ldots=\uparrow^{a_1}\downarrow^{a_2}\uparrow^{a_3}\ldots$$

has energy

$$E(\uparrow^{a_1}\downarrow^{a_2}\uparrow^{a_3}\ldots)=\log\left(\operatorname{Tr}\left(A^{a_1}B^{a_2}A^{a_3}\ldots\right)\right),$$

where

$$A=\begin{pmatrix}1&0\\1&1\end{pmatrix},\quad B=\begin{pmatrix}1&1\\0&1\end{pmatrix}.$$

Boca (see [1]) proved following asymptotic formula for the number of spin chains with given energy

$$\Psi(N)=\left|\left\{C=A^{a_1}B^{a_2}A^{a_3}\ldots:3\leq\operatorname{Tr}C\leqslant N\right\}\right|=N^2(c_1\log N+c_0)+O_\varepsilon\left(N^{7/4+\varepsilon}\right).$$

In the talk more sharp result will be presented

$$\Psi(N)=N^2(c_1\log N+c_0)+O\big(N^{3/2+\varepsilon}\big).$$

This formula can be generalized for the case of Gauss-Kuz'min statistics and gives a result about quadratic irrationals. Quadratic irrational ω is called to be regular iff it has purely periodic continued fraction expansion.

Let R be the set of all reduced quadratic irrationals. For $\omega\in R$ denote by $\rho(\omega)$ the length of ω (the length of corresponding geodesics on $\mathbb{H}/PSL_2(\mathbb{Z})$) and by ω^* conjugate of ω.

Theorem. For any x, $y\in[0,1]$

$$\sum_{\substack{\omega\in R,\rho(\omega)\leq 2\log N\\ \omega\leq x,-1/\omega^*\leq y}}1\;=\;\frac{\log(1+xy)}{2\zeta(2)}N^2+O(N^{3/2+\varepsilon})$$

In particular this result means that continued fraction expansions of reduced quadratic irrationals have the same statistical properties as continued fraction expansions of almost all real numbers.

References

[1] Boca F. P.: *Products of matrices* $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ *and* $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ *and the distribution of reduced quadratic irrationals*, J. Reine Angew. Math. **606** (2007), 149–165.

[2] Kleban, P., Özlük, A. E.: *A Farey Fraction Spin Chain*, Commun. Math. Phys. **203** (1999), 635-647.

Probabilistic star discrepancy bounds for double infinite random matrices

Markus Weimar

Abstract

In 2001 Heinrich, Novak, Wasilkowski and Woźniakowski proved that the inverse of the discrepancy depends linearly on the dimension, by showing that a Monte Carlo point set $\mathcal{P}$ of N points in the s-dimensional unit cube satisfies the discrepancy bound $D_N^{*s}(\mathcal{P}) \leq c_{\text{abs}} s^{1/2} N^{-1/2}$ with positive probability. Later their results were generalized by Dick to the case of double infinite random matrices.

In this talk we give explicit, asymptotically optimal bounds for the star discrepancy of such random matrices, and give estimates for the corresponding probabilities. Using the same techniques we derive similar discrepancy bounds for randomly generated *completely uniformly distributed* (c.u.d.) sequences. Finally, we mention an application of these results to Markov Chain Monte Carlo.

The talk is based on a recent paper which is joint work with C. Aistleitner [1].

References

[1] Aistleitner, C.—Weimar, M.: *Probabilistic star discrepancy bounds for double infinite random matrices*, (submitted manuscript 2012), `http://users.minet.uni-jena.de/~weimar/`

Asymptotic behaviour of average L_p-discrepancies

Heidi Weyhausen

Abstract

We analyse the limit behavior of the average L_p-B-discrepancy for arbitrary $0 < p < \infty$ if the number of sample points n tends to infinity. We present a new proof for a result of Steinerberger who investigated the L_p-star discrepancy and the extreme L_p-discrepancy. The L_p-B-discrepancy involves several types of discrepancy functions studied in the literature, for example L_p-star discrepancy, extreme, centered and periodic L_p-discrepancies. Furthermore, it is also possible to study discrepancy functions based on non-rectangular sets.

To prove our result we use probabilistic methods, namely the central limit theorem, characteristic functions and the dominated convergence theorem. Furthermore, we employ symmetrization techniques to obtain estimates for arbitrary p.

This is joint work with Aicke Hinrichs.

On the digits of squares and the distribution of quadratic subsequences of digital sequences

Heidrun Zellinger [1]

Abstract

Let q be a prime and $\gamma = (\gamma_0, \gamma_1, \gamma_2, \dots)$ be a finite weight sequence with

$$\gamma_i \in \{0, 1, \dots, q-1\} \quad \text{and} \quad \gamma_i = 0 \ \text{ for some } \ i \geq i_0.$$

We study

$$\lim_{N\to\infty} \#\left\{0 \leq n < N | s_{q,\gamma}(n^2) \equiv d \pmod q\right\}/N,$$

where $s_{q,\gamma}(n^2)$ denotes the weighted sum of digits of n^2 in base q.
We will give formulas for the limit above in dependence of the base q, the weight sequence γ and the digit d. Particularly, we analyze in which cases we obtain a fair distribution in the sense that the limit tends to $1/q$.
Finally, we show how these results can be used to classify all digital sequences $(\boldsymbol{x}_n)_{n\geq 0}$ in the sense of Niederreiter, that are generated by matrices with finite rows, for which $(\boldsymbol{x}_{n^2})_{n\geq 0}$ is uniformly distributed.

[1]Recipient of a DOC-FFORTE-fellowship of the Austrian Academy of Sciences at the Institute of Financial Mathematics at the University of Linz (Austria).

Optimality of the width-w non-adjacent form– –a diophanitne inequality

Volker Ziegler

Abstract

Efficient scalar multiplication in Abelian groups (which is an important task in public key cryptography) can be performed using digital expensions. Because the Frobenius endomporphism on elliptic curves fulfils a quadratic equation, imaginary quadratic integer bases are of special interest. One strategy for improving the efficiency is to increase the digit set (at the prize of additional precomputations). A common choice is the width-w non-adjacent form (w-NAF): each block of w consecutive digits contains at most one nonzero digit. Heuristically, this ensures a low weight, i.e., number of non-zero digits, which translates in few costly curve operations. This talk relates the optimality of w-NAF-expansions with properties of lattices, where optimality means minimizing the weight over all possible expansions with the same digit set.

List of participants

Christoph Aistleitner : aistleitner@math.tugraz.ac.at
Vladimír Baláž : vladimir.balaz@stuba.sk
Dimitriy Bilyk : bilyk.dmitriy@gmail.com
Johann Brauchart : j.brauchart@unsw.edu.au
Jozsef Bukor : bukor@selyeuni.sk
Nikolay Mikhaylovich Dobrovolskiy : dobrovol@tspu.tula.ru
Artūras Dubickas : arturas.dubickas@mif.vu.lt
Henri Faure : faure@iml.univ−mrs.fr
János Folláth : follath.janos@inf.unideb.hu
Michael Gnewuch : mig@informatik.uni−kiel.de
Vassil Stankov Grozdanov : vassgrozdanov@yahoo.com
Katalin Gyarmati : gykati@cs.elte.hu,
Peter Hellekalek : peter.hellekalek@sbg.ac.at
Tamás Herendi : herendi@inf.unideb.hu
Markus Hofer : markus.hofer@tugraz.at
Roswitha Hofer : roswitha.hofer@jku.at
Martin Huxley : huxley@cardiff.ac.uk
Maria Rita Iacò : iaco@mat.unical.it
Maria Infusino : infusino@mat.unical.it
Oleg Karpenkov : karpenkov@tugraz.at
Imre Kátai : katai@compalg.inf.elte.hu
Sergei Konyagin : konyagin@ok.ru
Peter Kritzer : peter.kritzer@jku.at
Manfred Kühleitner : manfred.kuehleitner@boku.ac.at
Pierre Liardet : liardet@gmail.com
Florian Luca : fluca@matmor.unam.mx
Sándor Roland Major : major.sandor@inf.unideb.hu
Lev Marghasin : lev.markhasin@uni−jena.de
László Mérai : merai@cs.elte.hu
Ladislav Mišík : ladislav.misik@osu.cz
Nikolay Moshchevitin : moshchevitin@gmail.com
Radhakrishnan Nair : nair@liverpool.ac.uk
Karol Nemoga : karol.nemoga@mat.savba.sk
Werner Georg Nowak : nowak@mail.boku.ac.at
Florian Pausinger : florian.pausinger@ist.ac.at

Friedrich Pillichshammer : friedrich.pillichshammer@jku.at
Štefan Porubský : porubsky@cs.cas.cz
András Sárközy : sarkozy@cs.elte.hu
Ilya Shkredov : ishkredov@gmail.com
Oto Strauch : oto.strauch@mat.savba.sk
Ján Šustek : jan.sustek@osu.cz
Shu Tezuka : tezuka@math.kyushu−u.ac.jp
János Tóth : tothj@selyeuni.sk
Alexey Ustinov : ustinov@iam.khv.ru
Markus Weimar : markus.weimar@uni−jena.de
Heidi Weihausen : heidi.weyhausen@uni−jena.de
Heidrun Zellinger : heidrun.zellinger@jku.at
Volker Ziegler : ziegler@math.tugraz.at