The FWF-Special Research Area "Quasi-Monte Carlo Methods: Theory and Applications"

Gerhard Larcher, Michael Drmota, Peter Grabner,
Peter Hellekalek, Roswitha Hofer, Peter Kritzer,
Gunther Leobacher, Friedrich Pillichshammer, Robert Tichy,
Arne Winterhof

1 Introduction

In December 2013 the FWF (the Austrian science fund) granted a special research area (SFB) on the topic "Quasi-Monte Carlo Methods: Theory and Applications". This SFB—which is intended for two four-year periods and which started work in February 2014—is coordinated by Gerhard Larcher (speaker) and Friedrich Pillichshammer (co-speaker), both from the Johannes Kepler University Linz. It connects ten research projects, led by Michael Drmota (TU Vienna), Peter Grabner and Robert Tichy (both TU Graz), Peter Hellekalek (Paris Lodron University Salzburg), Roswitha Hofer, Peter Kritzer, Gerhard Larcher, Gunther Leobacher, Friedrich Pillichshammer (all Johannes Kepler University Linz), and by Arne Winterhof (RICAM, Austrian Academy of Sciences). The SFB funds make it possible to finance about 20 new Postdoc and PhD positions.

The work in this research project will be accompanied and monitored by an international advisory board of highly renowned experts in quasi-Monte Carlo (QMC) methods. The chair of the advisory board is Harald Niederreiter, who is a central figure in the field of QMC methods. In his research, he has frequently cooperated with the project leaders for many years, and he will thus play a central role in this SFB.

There is a variety of "big open problems" in QMC, problems partly arising from theory, partly arising from applications. It is the aim of this SFB to

efficiently exchange the skills of the participating research groups, to analyze the new modern techniques in QMC and integrate them into the joint work, to develop powerful new methods and so to contribute in an essential way to solutions of the most challenging problems in the field. Further it will create a center of excellence for the theory and the application of QMC-methods to be visible world-wide.

"Quasi-Monte Carlo methods" include all methods in which most carefully chosen quasi-random-point sets are used to carry out simulations in the framework of sophisticated and highly developed modeling environments, for obtaining quantitative information in different branches of applications. The study and development of QMC methods requires

- the generation, investigation, and analysis of distribution properties of finite or infinite sequences in all kinds of regions;
- the development, investigation, and analysis of suitable theoretical models on which the applications of the QMC methods are based, and in particular the derivation of error bounds for QMC methods in these models;
- the efficient implementation of the theoretical models and of the algorithms for the generation of the (sometimes very large and high-dimensional) quasi-random point sets, and the development of sophisticated software;
- the concrete application of the QMC methods in different areas, the discussion of the implications and of the performance of the applied QMC methods.

Consequently, many different branches of mathematics are involved in the comprehensive investigation and development of QMC methods, most notably number theory, discrete mathematics, combinatorics, harmonic analysis, functional analysis, stochastics, complexity theory, theory of algorithms, and numerical analysis. Furthermore, profound knowledge of the branches of applications in which the QMC methods are intended to be used is necessary. The theory and application of QMC methods is a modern and extremely lively branch of mathematics. This is demonstrated by an enormous output of research papers on this topic over the last decades, and by the great and growing success of the series of the biannual international conferences

on "Monte Carlo and Quasi-Monte Carlo Methods in Scientific Computing" (MCQMC), which started in 1994 in Las Vegas and was most recently held in Sydney in 2012 and in Leuven (Belgium) 2014.

It is the aim of this article to give a short insight into some of the most relevant topics in QMC which will be investigated by the research groups participating in this SFB. In Section 2 we give a very brief introduction to the basic facts on and techniques used in QMC. In the remaining Sections 3–12 we give examples of some of the main concrete research topics studied in the SFB.

2 Quasi-Monte Carlo methods: Basic facts and techniques

Many quantitative problems in various fields of applications (e.g., finance, engineering, economics, physics, medicine, biology, ...) involve the task of approximately evaluating (sometimes very high dimensional) integrals. This is particularly often the case when one has to calculate the expected value or the variance of a random variable whose value depends on many random sources.

The basic (quasi-) Monte Carlo approach to evaluate such integrals (say of a function f over an s-dimensional unit-cube $[0,1]^s$), is, to choose N points $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_N$ in $[0,1)^s$ and to approximate the integral by the average value of f at these sample points, i.e.,

$$\int_{[0,1]^s} f(\boldsymbol{x})\,\mathrm{d}\boldsymbol{x} \approx \frac{1}{N}\sum_{n=1}^{N} f(\boldsymbol{x}_n).$$

In the pure Monte Carlo approach the N sample points are chosen (pseudo-) randomly. In this case the expected [!] error (i.e., the difference between the true integral value and the approximation) is essentially given by a constant depending on f times $1/\sqrt{N}$.

In QMC methods the sample point sets are chosen deterministically such that the point sets show certain well-distribution properties, and sometimes further structural properties, depending on the class of integrands we are dealing with. In this case the basic error estimate is the fundamental Koksma-Hlawka inequality (see, for example, [13, 18, 27, 30, 36]):

$$\left| \int_{[0,1]^s} f(\boldsymbol{x})\,\mathrm{d}\boldsymbol{x} - \frac{1}{N}\sum_{i=1}^{N} f(\boldsymbol{x}_i) \right| \le V(f) D_N^*(\{\boldsymbol{x}_1,\ldots,\boldsymbol{x}_N\}),$$

where $V(f)$ denotes the variation of f (in the sense of Hardy and Krause) and $D_N^*(\{\boldsymbol{x}_1,\ldots,\boldsymbol{x}_N\})$ denotes the star-discrepancy of the point set $\{\boldsymbol{x}_1,\ldots,\boldsymbol{x}_N\}$. The star-discrepancy is defined as

$$D_N^*(\{\boldsymbol{x}_1,\ldots,\boldsymbol{x}_N\}) = \sup_B \left| \frac{A_N(B)}{N} - \lambda(B) \right|, \tag{1}$$

where the supremum is taken over all axis-parallel boxes B in $[0,1)^s$ anchored at the origin (i.e., which are of the form $B = \prod_{j=1}^{s}[0,t_j)$), where by $A_N(B)$ we denote the number of indices $n \in \{1,\ldots,N\}$ for which $\boldsymbol{x}_n$ is contained in B, and where λ is the s-dimensional Lebesgue measure.

For an infinite sequence $\mathcal{S} = (\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots)$ of points in $[0,1)^s$ we denote by $D_N^*(\mathcal{S})$ the star-discrepancy of the point set consisting of the first N elements of the sequence. The sequence is called uniformly distributed if and only if $\lim_{N\to\infty} D_N^*(\mathcal{S}) = 0$.

So obviously one of the main tasks in the theory of QMC methods is to analyze the discrepancy of point sets and point sequences, and to provide point sets or point sequences with low discrepancy in a (sometimes very high-dimensional) unit-cube. These tasks—which often lead to deep problems in fields like number theory or combinatorics—are in the center of interest of the SFB and in particular of the projects which will be described in short in Sections 3, 5, 6, 8, 10 and 11 below. It is known that in every dimension s and for all N there exist point sets $\{\boldsymbol{x}_1,\ldots,\boldsymbol{x}_N\} \subseteq [0,1)^s$ with star-discrepancy $D_N^*(\{\boldsymbol{x}_1,\ldots,\boldsymbol{x}_N\}) \ll_s \frac{(\log N)^{s-1}}{N}$.

Depending on the class of functions one is dealing with the particular integration problem. However, sometimes not only distribution properties of the point sets, but also further structural properties may play a crucial role. To give but one example: Assume that we know that the integrand f is periodic with period one in each coordinate and that all its partial mixed derivatives up to order α exist and are continuous. Then it can be shown that it is of advantage to use so-called good-lattice point sets for numerical integration. These are point sets of the form

$$\boldsymbol{x}_n = \left(\left\{ n\frac{a_1}{N} \right\}, \ldots, \left\{ n\frac{a_s}{N} \right\} \right) \quad \text{with} \quad n = 0,1,\ldots,N-1, \tag{2}$$

with given integers $a_1, \ldots, a_s$. QMC algorithms based on good-lattice point sets are also known as lattice rules, and they were introduced independently by Hlawka and Korobov by the end of the 1950s.

It is known, that for all dimensions s and all N there exist $a_1, \ldots, a_s \in \{1, \ldots, N\}$, such that the integration error for functions of the above form is of order $O((\log N)^{s\alpha}/N^{\alpha})$.

This is just one classical and well-known result in this direction, and—of course—there exists a magnitude of much more subtle integration rules in the modern theory of QMC-methods. With the analysis and the development of such efficient integration- (and also approximation-) rules especially the projects described in Sections 4, 7, 8, 9 and 10 will be concerned.

Finally, the application of QMC-methods in concrete problems in most cases needs a suitable adaptation of the methods to the problem. For example, the integration region might not be a unit-cube but a more general manifold (e.g., the sphere), or certain variance and variation reduction methods might have to be applied, or the special simulation problem needs point sets with additional pseudo-random properties. With such problems especially the projects described in Sections 4, 9, 11 and 12 will be concerned. When dealing with concrete applications in this SFB, then in almost all cases we will work with show-case problems from mathematical finance.

In the following we will highlight some of the main topics of our research in the SFB.

3 Subsequences of automatic sequences and uniform distribution

This project part is led by Michael Drmota and it aims at constructing uniformly distributed sequences with the help of proper subsequences of automatic sequences.

Automatic sequences are sequences $t(n)$ on a finite alphabet that are the output of a finite automaton. The Thue-Morse sequence $T(n) = s_2(n) \bmod 2$ is one of the most prominent examples of an automatic sequence. (Here and in what follows $s_q(n)$ denotes the q-adic sum-of-digits function).

One of the main motivations for the research in this project part is the recent progress on the so-called Gelfond problems [19] on the prime values and on polynomial values of the sum-of-digits function modulo m. Gelfond

conjectured that the subsequence $s_q(p)$, where p runs through all primes, as well as subsequences of the form $s_q(P(n))$, where P is a polynomial of degree greater than 1, are uniformly distributed on the residue classes modulo m. (The cases of primes and squares of these 40 year old conjectures have been solved by Mauduit and Rivat [32, 33], and there is a partial solution for polynomials by Drmota, Mauduit and Rivat [17]). Furthermore, Drmota, Mauduit and Rivat [16] recently proved that the subsequence $T(n^2) = s_2(n^2) \bmod 2$ of the Thue-Morse sequence is actually a normal sequence, that is, every possible 0-1-block appears with the correct asymptotic frequency. Consequently this sequence can be used to generate a Quasi-Monte-Carlo sequence. Since automatic sequences (like the Thue-Morse sequence) can be efficiently generated this gives rise to a completely new efficient construction of Quasi-Monte-Carlo sequences.

Therefore the **first overall goal** of this sub-project is to provide a more systematic treatment to these kinds of problems and to characterize the distributional behaviour of subsequences of automatic sequences $t(n)$ of the form $t(P(n))$ for polynomials P of degree greater than 1, $t(\lfloor n^c \rfloor)$ (for $c > 1$), and $t(p)$ for primes p. It is certainly too ambitious to expect a complete solution in the general case, nevertheless we will work on (at least) the following questions: to study $t(n^2)$, to study $t(\lfloor n^c \rfloor)$ for specific non-integer $c > 1$, to improve results on $s_q(P(n))$ for polynomials, and to study $t(p)$ for special (e.g. invertible) automatic sequences.

The **second overall goal** of this sub-project is to study similar questions for more general digital expansions like the Zeckendorff expansion that is based on Fibonacci numbers. The Zeckendorff sum-of-digits funcion $s_Z(n)$ is the (minimal) number of Fibonacci numbers that are needed to represent n. It is well known that $s_Z(n)$ is uniformly distributed modulo m and that $\alpha s_Z(n)$ is uniformly distributed modulo 1 for irrational α. However, nothing is known on $s_Z(n^2)$ or $s_Z(p)$. It should be mentioned that $s_Z(n) \bmod m$ is not an automatic sequence, nevertheless it is expected that $s_Z(n)$ has similar distributional properties as $s_q(n)$, also regarding its subsequences.

4 Distributing points on spheres and manifolds: minimal energy and designs

This project part led by Peter Grabner aims for a more detailed investigation of point sets of minimal energy and spherical designs. Especially, estimates for the discrepancy of such point sets are of interest; quantifying the distribution properties of such point sets is necessary for applying them to numerical integration.

Minimal energy point sets

For a given compact manifold $M \subset \mathbb{R}^{d+1}$ and a set of N distinct points $X_N = \{x_1, \dots, x_N\} \subset M$, the Riesz s-energy is defined as $E_s(X_N) = \sum_{i \neq j} \|x_i - x_j\|^{-s}$. A configuration X_N, which minimizes E_s among all N-point configurations, is called a minimal energy configuration. Several questions are of interest in this context:

- the asymptotic behavior of the minimal energy for $N \to \infty$
- the (weak-*) limiting distribution of the measures $\nu_N = \frac{1}{N} \sum_{i=1}^{N} \delta_{x_i}$
- the discrepancy between these discrete measures and the limiting measure.

One motivation for studying this question is quite classical: how do N mutually repelling particles distribute on a surface?

- For $s = 1$, $d = 2$ these are particles under a Coulomb potential on a surface.
- For $s \to \infty$ this optimization problem becomes the problem of best packing (cf. [8]).
- The resulting point distributions for moderately large N occur in biology (optimal phyllotaxis, viral morphology).

The case $s < \dim(M)$ can be studied by methods from classical potential theory (cf. [29]). The distribution of minimal energy point sets approaches the equilibrium measure. For $s \geq \dim(M)$ the situation changes completely. The corresponding energy integral diverges for all probability measures. Techniques from geometric measure theory could be applied in [21] to show that the limiting distribution $\mu_M^{(s)}$ of the minimal energy distributions is normalized $\dim(M)$-dimensional Hausdorff measure on M, if M is rectifiable.

In [21] it was shown that for $s > d$ the minimal energy of an N point subset X_N on a d-dimensional rectifiable manifold behaves like

$$\frac{C_{s,d}}{H_d(M)^{s/d}} N^{1+s/d},$$

where H_d denotes the d-dimensional Hausdorff measure. For s tending to infinity, $C_{s,d}^{1/s}$ has a limit that is related to the best-packing constant.

Spherical designs

A spherical t-design is a finite set of points $X \subset S^d$ such that

$$\frac{1}{\#X} \sum_{x \in X} p(x) = \int_{S^d} f(x)\, d\sigma(x)$$

for all polynomials p of degree $\leq t$, where σ denotes the normalized surface measure on S^d (cf. [10]). In [10] a lower bound of order t^d could be given, which was shown to be only attained for small values of t. Only recently, it could be shown that $O(t^d)$ points suffice to obtain a t-design (cf. [4]).

5 Arithmetic primitives for uniform distribution modulo 1

The setting underlying this subproject led by Peter Hellekalek is the following. We are given three mathematical objects: X, ω, and f, where X is a nonempty set, $\omega = (x_n)_{n \geq 0}$ is a sequence in X, and $f : X \to \mathbb{C}$ is a function on X. Suppose that X and f are such that $I(f) = \int_X f$ is defined. It is a fundamental property of any notion of uniformly distributed (u.d.) sequences in X that, for a given u.d. sequence ω, the *sample means* $S_N(f, \omega) = (1/N) \sum_{n=0}^{N-1} f(x_n)$ converge to the *expectation* $I(f)$ if the sample size N increases to infinity, for all functions f in a suitable function class $\mathcal{F}$ defined on X.

The above notions call for an appropriate structure on X. Integration requires a measure space structure on X. The concept of u.d. sequences in X leads to the need for construction methods for such sequences, which, in their turn, demand arithmetics on X. If we also want to use some kind of harmonic analysis to study the difference between $S_N(f, \omega)$ and $I(f)$, a short

study of [25] will convince the reader that a *(compact abelian) topological group* X is a suitable mathematical environment.

In this subproject of the SFB, we start our research on the s-dimensional torus $(\mathbb{R}/\mathbb{Z})^s$, which we represent by the compact abelian group $X = [0,1)^s$ with addition modulo one. For a given sequence ω in $[0,1)^s$, it is clearly important to measure the uniform distribution of ω. The best known *figures of merit* employed for this task are *discrepancy* and *diaphony* (see [18, 27, 36]). During the recent years, many other figures of merit for u.d. sequences have been developed and relations to extremal integration errors in certain function spaces have been established (see, for example, [12, 13]).

The first goal of this project is to find a unifying general concept for these figures of merit. We will study a generalized version of the *spectral test*, which is a concept based on so-called *convergence determining classes* of functions. Examples are the trigonometric functions and the Walsh functions. The methods and results developed in [9, 22, 23, 24] will serve as starting points.

The second goal concerns the construction of finite and infinite sequences on the s-torus with good uniform distribution behavior. We will employ the arithmetical structure of the b-adic numbers $\mathbb{Q}_b$ in a new construction method that is related to the method of *good lattice points* (see [36, 46]) and to some duality principles (see [37, 45]).

The third goal is about *arithmetic primitives*. In the construction principles behind cryptographic primitives and behind pseudo-random number generators, the iteration of a given *update function* $f : S \to S$ on a *finite* state space S plays a central role. We are interested in the question of how to describe the long-term behavior of the orbits $x, f(x), f^2(x) = f(f(x)), f^3(x), \ldots$ of a given point $x \in S$ in dependence of certain properties of f. What are the appropriate mathematical models to rate different update functions with respect to their (bit-) mixing behavior? Due to the finiteness of S, there is no asymptotics. Two different approaches to this kind of question can be found in the survey papers [26, 44].

6 Finite-row digital sequences and related hybrid sequences

One main aim of this project part (which is led by Roswitha Hofer) is to deepen the study of hybrid sequences with at least one digital component-

sequence. Hybrid sequences are built by concatenating the components of two or more different types of low-discrepancy sequences or in the original idea of Spanier [48] by combining low discrepancy sequences with pseudo-random sequences. The intentions are multiple: combining the different structures and/or advantages of the component sequences, providing new types of sequences, discovering new types of low-discrepancy sequences, etc. The difficulty we face when studying the distribution of hybrid sequences is to work out proper methods which can handle the different structures of the component sequences. Hybrid sequences with one or more digital component sequences appear as particularly hard-to-study. Digital sequences are constructed by the digital method introduced in [35]. The digital method is an algorithm that generates the nth point of the s-dimensional sequence $(\boldsymbol{x}_n)_{n\geq 0}$ by operating on the digits of n in base q and at whose heart are s doubly infinite generating matrices. It should be emphasized here that the distribution of the sequence is mainly determined by the specific choice of the generating matrices and the main computational effort of the algorithm lies in the multiplication with those matrices. In particular, for hybrid sequences so called finite-row digital sequences, which are generated by matrices satisfying that each matrix-row contains only finitely many nonzero entries, seem to be promising.

This project part contains partial problems which are relevant for the investigation of hybrid sequences with at least one digital component-sequence and which are interesting as number-theoretical problems per se. An interesting problem is to determine specific relations between special generating matrices, which for example yield certain correlations between the components of the generated digital sequence. This problem seems to be related to combinatorial objects such as binomial type sequences of polynomials and generalized versions. Thereof such relations between generating matrices are not only interesting for the investigation of hybrid sequences but may also be interesting for efficient construction algorithms of digital sequences. Furthermore, the current methods for investigating hybrid sequences need information on the distribution of specific subsequences of the component sequences. As a part of this project we want to deepen recent investigations of subsequences of digital sequences.

7 Approximation of integrals and functions by new types of quasi-Monte Carlo algorithms

In this project part, led by Peter Kritzer, we consider recent trends in the theory of QMC algorithms applied to problems of integration and approximation over suitably chosen function spaces. A particular emphasis is laid on high-dimensional problems where it is necessary to control how the error of an algorithm depends on the dimension of the problem.

A prominent topic in this project part is that of function approximation by means of QMC (and, more generally, linear) algorithms. The basic problem is to study classes of functions defined on a domain $D \subseteq \mathbb{R}^s$ which usually can be represented by an expansion of the form

$$f(\boldsymbol{x}) = \sum_{\boldsymbol{k}} \widehat{f}(\boldsymbol{k}) e_{\boldsymbol{k}}(\boldsymbol{x}),$$

where the $e_{\boldsymbol{k}}$ form an orthonormal function system and where the coefficients $\widehat{f}(\boldsymbol{k})$ are given by $\widehat{f}(\boldsymbol{k}) = \int_D f(\boldsymbol{x}) \overline{e_{\boldsymbol{k}}(\boldsymbol{x})} \mathrm{d}\boldsymbol{x}$.

The approximation algorithms considered in this project frequently work as follows. We first choose a finite set $\mathcal{A}$ of indices $\boldsymbol{k}$ corresponding to the typically large coefficients $\widehat{f}(\boldsymbol{k})$ of the functions considered. Then, the coefficients $\widehat{f}(\boldsymbol{k})$ are approximated by a suitably chosen QMC algorithm $Q_{N,s}(f, \boldsymbol{k})$ using N integration nodes. That is, we approximate f by

$$A_{N,s}(f)(\boldsymbol{x}) := \sum_{\boldsymbol{k} \in \mathcal{A}} Q_{N,s}(f, \boldsymbol{k}) e_{\boldsymbol{k}}(\boldsymbol{x}),$$

which makes it necessary to control both the error of a QMC integration rule and the error of truncating the series expansion of f. The error of an approximation algorithm $A_{N,s}$ is measured in, most notably, the L_2 or L_∞ norm. If the function class we consider is a normed space, we frequently use the so-called worst-case error (i.e., the supremum of the error over the unit ball of the space) as a quality criterion for approximation algorithms.

In our error analysis, we study how the error of an approximation algorithm depends on two quantities: the number N of integration nodes used in the QMC algorithm for approximating the coefficients $\widehat{f}(\boldsymbol{k})$, and the dimension s of the problem. It is crucial to also include the dependence on

the dimension, as our algorithms should ideally work for high-dimensional problems and we would like to avoid a curse of dimensionality, i.e., we would like to achieve an approximation error that does not depend exponentially on s. If the latter situation occurs, we say that we can achieve tractability, a concept that has been introduced by Woźniakowski in [52]. As outlined in the seminal paper [47] by Sloan and Woźniakowski, one can achieve tractability of multivariate algorithms in certain weighted function spaces, where the influence of different groups of variables is modeled by weights.

So far, there have been numerous results on function approximation based on QMC or related algorithms for functions in certain weighted reproducing kernel Hilbert spaces, as for example in [11] and [28]. In these and in related papers, functions defined on the s-dimensional unit cube $[0,1]^s$ that can be represented as Fourier or Walsh series are considered.

For many of the previous results, one had to make rather restrictive assumptions on the function classes considered, such as smoothness or periodicity assumptions. It is one of the main goals of this project to develop approximation algorithms that also work for more general function classes and to relax some of the restrictions we had to make until now. As first examples, it is intended to study cosine spaces of non-periodic functions defined on $[0,1]^s$ and Hermite spaces of functions defined on $\mathbb{R}^s$.

In all problems of high-dimensional integration and approximation considered in this project, it is our goal to provide constructive algorithms.

8 Improved discrepancy estimates for various classes of sequences

The aim of this project-part, which is led by Gerhard Larcher, is to give improved discrepancy estimates for several types of point sequences in an s-dimensional unit-cube, but also to give general discrepancy estimates for whole classes of sequences.

It is the so-called "big open problem" in the theory of uniform distribution to determine the best possible order for the discrepancy of point sets in an s-dimensional unit-cube. As already mentioned in Section 2, it is known that in every dimension s and for all N there exist point sets with discrepancy $D_N^* \ll_s \frac{(\log N)^{s-1}}{N}$, and that in every dimension s there exist infinite point sequences with discrepancy $D_N^* \ll_s \frac{(\log N)^s}{N}$ for all N. Let us concentrate on

infinite point sequences in the following. Examples for such sequences are Halton sequences, or digital (t, s)-sequences in the sense of Niederreiter.

However, for $s \geq 2$ it is not known until today whether the order $D_N^* \ll_s \frac{(\log N)^s}{N}$ for the discrepancy of infinite sequences in the s-dimensional unit-cube is the best possible order or not (for $s = 1$ it was shown by W.M. Schmidt in 1972, that the order is best possible). The corresponding best lower bound for $s \geq 2$ currently known was given by Bilyk, Lacey and Vagharshakyan in [3]: There are positive constants c_s and δ_s such that for every sequence $\mathcal{S}$ in $[0, 1)^s$ we have

$$D_N^*(\mathcal{S}) > c_s \frac{(\log N)^{s/2+\delta_s}}{N}$$

for infinitely many $N \in \mathbb{N}$. Here δ_s is a positive, but very small constant which goes to 0 for s tending to infinity.

Indeed, until now even for seemingly very simple types of two-dimensional sequences the correct order of discrepancy is not known. A basic example for such a sequence is the simple 2-dimensional Halton sequence in bases 2 and 3.

The Halton sequence is defined as follows: For a non-negative integer n and an integer $b \geq 2$ let $n = n_r b^r + n_{r-1} b^{r-1} + \cdots + n_1 b + n_0$ be the base b digit representation of n. Define the radical inverse function ϕ_b by

$$\phi_b(n) := \frac{n_0}{b} + \frac{n_1}{b^2} + \cdots + \frac{n_r}{b^{r+1}}.$$

Then the 2-dimensional Halton sequence in bases 2 and 3 is given by

$$\boldsymbol{x}_n = (\phi_2(n), \phi_3(n)) \quad \text{for} \quad n = 0, 1, 2, \ldots.$$

A further example is the really simple hybrid sequence

$$\boldsymbol{x}_n = (\phi_2(n), \{n\sqrt{2}\}) \quad \text{for } n = 0, 1, 2, \ldots.$$

For both of these two simple sequences we do not know the correct order of their discrepancy.

It is the main aim of this project part to improve—and in the best case to find the correct order of—the upper and lower discrepancy bounds of frequently used sequences like Halton sequences, digital (t, s)-sequences in the sense of Niederreiter, and of certain types of hybrid sequences.

9 Adapting QMC algorithms to the simulation problem

The project, which is led by Gunther Leobacher, is located at the interface between QMC methods and applications in finance and natural sciences. Hereby the main questions are how to (re-)formulate a given high-dimensional integration problem to make it more suitable for QMC.

One of the most fruitful approaches known is to express the problem as an expectation of a function depending on independent standard normal variables and concatenate the function with a carefully chosen orthogonal transform. Well known examples of general purpose transforms are provided by the Brownian bridge construction or the principal component analysis construction (PCA)construction of Brownian paths. More specialized orthogonal transforms, which take the form of the integrand into account, exist as well. For very high-dimensional problems another important requirement is that the transform can be computed sufficiently fast, whereby the benchmark is the complexity of the PCA construction for Brownian paths, with computational cost $O(n \log(n))$ for an n-dimensional problem. We call this problem of finding a fast efficient orthogonal transform "FEOT problem".

It is a curious fact that the choice of any orthogonal transform does not make a difference for classical Monte Carlo, since for a standard normal vector X and an orthogonal transform U we have $\mathrm{E}(f(X)) = E(f(UX))$. On the other hand we have that QMC algorithms, originally developed for problems of moderate dimension, become more efficient if the problem can be formulated in a way such that the integrand depends mainly on only few of the input parameters while the others have little influence. And frequently this can be facilitated by simply applying an orthogonal transform.

So we may consider an orthogonal transform U to be effective for the integrand f if only a couple of input parameters of $f \circ U$ are important. A classical concept for measuring the numbers of important parameters is that of "effective dimension", see [6], which relies on the ANOVA decomposition of f resp. $f \circ U$. Thus U could be considered effective, if the effective dimension of $f \circ U$ is much lower than that of f.

A modern alternative to that concept is provided by weighted norms of reproducing kernel Hilbert spaces, as introduced in [47]. Here the integration error of f can be bounded by the norm of f through a Koksma-Hlawka type inequality and thus an orthogonal transform U can be considered to be

effective for the integrand f if the weighted norm of $f \circ U$ is much smaller than that of f.

At the present the project has two main goals: 1. to find and study suitable reproducing kernel Hilbert spaces of functions on the $\mathbb{R}^d$ in which integration is tractable and 2. to find algorithms for the FEOT problem in those spaces. A practical problem occuring is that both effective dimension and weighted norms usually do not depend continuously on the orthogonal transform. Thus we need to find, for example, weighted reproducing kernel Hilbert spaces over the $\mathbb{R}^d$ which are invariant under orthogonal transforms of the $\mathbb{R}^d$. One additional constraint on these spaces is that they should contain interesting functions while at the same time integration should be defined and tractable (in the sense of Section 10).

10 Digital nets and lattice based integration rules

In this project, led by Friedrich Pillichshammer, we analyze QMC rules based on lattice point sets in the sense of Hlawka and Korobov (see (2)) and on digital nets and sequences in the sense of Niederreiter [35]. As the quality criterion we study the worst-case integration error of QMC rules in various function spaces, a concept which comprises the notions of classical and weighted discrepancy. We aim at finding explicit constructions of "good" point sets and sequences and we want to study the dependence of the worst-case error on the dimension of the problem. The following two topics are exemplary:

Extending Roth's general lower bound for the L_2-discrepancy of finite point sets from [43], Proinov [41] showed in 1986 that for any infinite sequence $\mathcal{S}$ in $[0,1)^s$ the L_p-discrepancy[1] with $p \in (1,\infty)$ satisfies

$$L_{p,N}(\mathcal{S}) \geq c_{s,p} \frac{(\log N)^{s/2}}{N} \quad \text{for infinitely many} \quad N \in \mathbb{N}. \tag{3}$$

Recently, together with Dick [14], we found first explicit constructions of infinite digital sequences over the finite field $\mathbb{F}_2$ with L_2-discrepancy of exactly

[1]The star-discrepancy D_N^* given in (1) can be viewed as the L_∞-norm of the local discrepancy $A_N(B)/N - \lambda(B)$. In this sense, the L_p-discrepancy is the L_p-norm of the local discrepancy.

this order of magnitude, which shows that Proinov's lower bound is best possible for $p \in (1,2)$. For arbitary $p > 2$ this problem is still open and it is one aim of this project part to find explicit constructions of infinite sequences whose L_p-discrepancy matches the lower bound (3). (We remark that for *finite* point sets the problem has already been solved by Chen and Skriganov [7] for $p = 2$ and by Skriganov [45] for arbitrary $p \in (1, \infty)$.)

Classical theories study the dependence of the integration error of QMC rules on the number N of underlying integration nodes. Depending on the smoothness of the integrands, described by a certain parameter α, one can typically achieve an error convergence of the form $O((\log N)^{\kappa_{s,\alpha}}/N^{\alpha})$ for finite smoothness or even $O(\mathrm{e}^{-c_s N^{B_s}})$ for infinite smoothness. E.g., for functions on $[0,1]^s$ with finite mixed partial derivatives up to order one, the worst-case integration error is related to the star-discrepancy of the integration nodes which can be of order $O((\log N)^{s-1}/N)$. Such convergence rates are excellent in an asymptotic sense when N grows to infinity. However, if we still consider the star-discrepancy, the function $N \mapsto (\log N)^{s-1}/N$ is increasing for $N \leq \mathrm{e}^{s-1}$. But already for moderately large dimensions s (e.g., in the hundreds) the value e^{s-1} is too large to use point sets of cardinality $N > \mathrm{e}^{s-1}$ in practical applications. This means that we need to analyze the error bounds of QMC rules also with respect to their dependence on the dimension s. This is systematically done by studying the so-called information-complexity $N(\varepsilon, s)$, which is the number of nodes required in order to reduce a certain initial error in dimension s by a factor of ε, where $\varepsilon \in (0,1)$. Problems for which $N(\varepsilon, s)$ grows exponentially in s or ε^{-1} are called intractable and this is exactly what we want to avoid. If, on the other hand, the information-complexity is bounded polynomially in s and ε^{-1}, we speak of polynomial tractability. The subject of tractability for multivariate problems has been introduced by Woźniakowski [52] in 1994. It is a further aim of this project part to study tractability properties for various function spaces and to present explicit constructions of point sets which can achieve tractability. We think that lattice point sets and digital nets and sequences are good candidates for this as well. Following a recent stream of research, we also study the case of infinite smoothness.

11 Diophantine equations, discrepancy and finance

In the analysis of QMC-methods probabilistic methods can be used to investigate the typical behavior of the distribution properties of sequences. An interesting class of sequences, because of its importance in Fourier analysis and in probabilistic number theory, is the class of lacunary sequences $(n_k x)_{k=1}^{\infty}$ for $x \in \mathbb{R}$, where (n_k) is exponentially growing: $n_{k+1}/n_k \geq q > 1$. Answering a question of P. Erdős, Walter Philipp (1975) proved a "bounded" law of the iterated logarithm (LIL) for the discrepancy[2] of such sequences:

$$\frac{1}{8} \leq \limsup \sqrt{\frac{N}{2 \log \log N}} D_N\left(n_k x\right) \leq C(q) \tag{4}$$

for almost all x (in the sense of Lebesgue measure on $\mathbb{R}$) with a constant $C(q)$ depending on the growth rate q; see for instance [18]. Note that if (ξ_k) is a sequence of i.i.d random variables on $(0,1)$ then

$$\limsup_{N \to \infty} \sqrt{\frac{N}{2 \log \log N}} D_N(\xi_k) = \frac{1}{2} \tag{5}$$

with probability one by Chung-Smirnov LIL. It is one aim of this subproject, led by Robert Tichy, to investigate the "probabilistic" behavior of deterministic sequences. This involves various tools, mainly from Fourier analysis, martingale inequalities and methods from Diophantine analysis such as the theory of S-unit equations. It was for instance shown in papers by C. Aistleitner, I. Berkes and R. Tichy [1, 2] that a LIL with constant $\frac{1}{2}$ as in (2) holds for lacunary sequences $(n_k x)$ provided that $n_{k+1}/n_k = \infty$ ("strongly lacunary sequences"). Furthermore, this result is permutation independent, i.e. it remains true for sequences $(n_{\sigma(k)} x)$, where $\sigma : \mathbb{N} \to \mathbb{N}$ is an arbitrary permutation of the positive integers. In the case of "proper" lacunary sequences i.e. $\limsup_{k \to \infty} \frac{n_{k+1}}{n_k} = q > 1$ the situation is completely different: the constant in the LIL depends on the growth rate q and the result is in general not permutation invariant. Within this project the investigation will

[2]The discrepancy D_N of a sequence is defined in the same way as the star-discrepancy in (1) with the only difference that the supremum is extended over *all* axes-parallel boxes of the form $B = \prod_{j=1}^{s} [u_j, v_j)$ in $[0,1)^s$.

be extended to more general classes of sequences, in particular to the multidimensional situation and to certain sublacunary sequences. In this context so-called Hardy-Littlewood-Polya sequences are well-understood because of their arithmetic structure: in this case (n_k) is given as the multiplicative semigroup generated by finitely many coprime integers and arranged in increasing order. Such sequences were used by H. Furstenberg in the theory of dynamical systems. Later W. Philipp (1994) proved a "bounded" LIL for this class of sublacunary sequences. By Diophantine tools C. Aistleitner, I. Berkes and R.F. Tichy obtained a permutation invariant LIL and it remains open to extend such results to more general classes of sublacunary sequences and to other kinds of distribution measures. It is also one aim of this subproject to apply Diophantine and probabilistic tools to the analysis of models in financial mathematics.

12 On the hierarchy of measures of pseudorandomness

This project part deals with the analysis of pseudorandom numbers in view of several different application areas. It is led by Arne Winterhof.

Pseudorandom numbers are generated by deterministic algorithms and are not random at all. However, in contrast to truly random numbers they guarantee certain randomness properties. Their desirable features depend on the application area. For example, uniformly distributed sequences of pseudorandom numbers are needed for Monte Carlo methods, unpredictable sequences for cryptography, and uncorrelated sequences for wireless communication or radar. Some corresponding quality measures are discrepancy for uniform distribution, linear complexity for unpredictability, and autocorrelation.

The main goal of this project is finding relations between different measures of pseudorandomness. For example, the linear complexity provides essentially the same quality measure as certain lattice tests coming from the area of Monte Carlo methods, see [15, 38]. Moreover, the paper [31] studies links between uniformly distributed pseudorandom sequences (x_n) of real numbers in $[0, 1)$ and the pseudorandom binary sequences (e_n) defined by $e_n = 0$ if $x_n < 1/2$ and $e_n = 1$ otherwise. It is proved that good pseudorandom $[0, 1)$ sequences induce binary sequences that have small correlation

measures. The correlation measure of order k is a rather general measure of pseudorandomness introduced by Mauduit and Sárközy [34]. A relation between linear complexity and the correlation measure of order k is given in [5]. Hence, we may very roughly say that discrepancy is a stronger measure than the correlation measure which is a stronger measure than linear complexity. There are many other related measures of pseudorandomness for sequences, see [20, 42, 49], and we want to analyze their hierarchy. In this hierarchy we may also include measures for cryptographic functions. For example, a small correlation measure of order k of a binary sequence guarantees a high nonlinearity and algebraic degree of a corresponding Boolean function [40], which is necessary to avoid some cryptanalytic attacks.

Moreover, we try to find explicit sequence constructions which separate the hierarchy classes and have excellent behaviour under the strongest measures. A focus is put on uniformly distributed sequences derived from dynamical systems, see the survey [50], hybrid sequences, sequences defined using characters of finite fields, and interleaved sequences. We will also study relations to emergent areas as coding theory, biology, or quantum computing.

Our main tools are from analytic number theory, in particular, exponential sum or character sum techniques. For recent surveys on character sums and their applications see [39, 51]. However, we also use very new techniques for example from additive combinatorics.

References

[1] C. Aistleitner, I. Berkes, and R. F. Tichy. On permutations of Hardy-Littlewood-Pólya sequences. *Trans. Amer. Math. Soc.*, 363(12):6219–6244, 2011.

[2] C. Aistleitner, I. Berkes, and R. F. Tichy. On the asymptotic behavior of weakly lacunary series. *Proc. Amer. Math. Soc.*, 139(7):2505–2517, 2011.

[3] D. Bilyk and M. T. Lacey. On the small ball inequality in three dimensions. *Duke Math. J.*, 143(1):81–115, 2008.

[4] A. Bondarenko, D. Radchenko, and M. Viazovska. Optimal asymptotic bounds for spherical designs. *Ann. of Math. (2)*, 178(2):443–452, 2013.

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

[6] R. Caflisch, W. Morokoff, and A. Owen. Valuation of mortgage-backed securities using Brownian bridges to reduce effectice dimension. *J. Comput. Finance*, 1(1):27–46, 1997.

[7] W. W. L. Chen and M. M. Skriganov. Explicit constructions in the classical mean squares problem in irregularities of point distribution. *J. Reine Angew. Math.*, 545:67–95, 2002.

[8] J. H. Conway and N. J. A. Sloane. *Sphere packings, lattices and groups*, volume 290 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, New York, 1993.

[9] R. R. Coveyou and R. D. Macpherson. Fourier analysis of uniform random number generators. *J. Assoc. Comput. Mach.*, 14:100–119, 1967.

[10] P. Delsarte, J. M. Goethals, and J. J. Seidel. Spherical codes and designs. *Geometriae Dedicata*, 6(3):363–388, 1977.

[11] J. Dick, P. Kritzer, and F. Y. Kuo. Approximation of functions using digital nets. In S. Heinrich, A. Keller, and H. Niederreiter, editors, *Monte Carlo and Quasi-Monte Carlo Methods 2006*, pages 275–297, Berlin, 2008. Springer.

[12] J. Dick and F. Pillichshammer. Diaphony, discrepancy, spectral test and worst-case error. *Math. Comput. Simulation*, 70(3):159–171, 2005.

[13] J. Dick and F. Pillichshammer. *Digital Nets and Sequences. Discrepancy Theory and Quasi-Monte Carlo Integration*. Cambridge University Press, Cambridge, 2010.

[14] J. Dick and F. Pillichshammer. Optimal $\mathcal{L}_2$ discrepancy bounds for higher order digital sequences over the finite field $\mathbb{F}_2$. *Acta Arith.*, 162(1):65–99, 2014.

[15] 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.

[16] M. Drmota, C. Mauduit, and J. Rivat. The Thue Morse sequence along squares is normal. manuscript.

[17] M. Drmota, C. Mauduit, and J. Rivat. The sum-of-digits function of polynomial sequences. *J. Lond. Math. Soc. (2)*, 84(1):81–102, 2011.

[18] M. Drmota and R. F. Tichy. *Sequences, discrepancies and applications*, volume 1651 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1997.

[19] A. O. Gel′fond. Sur les nombres qui ont des propriétés additives et multiplicatives données. *Acta Arith.*, 13:259–265, 1967/1968.

[20] K. Gyarmati. Measures of pseudorandomness. In *Finite fields and their applications*, volume 11 of *Radon Ser. Comput. Appl. Math.*, pages 43–64. De Gruyter, Berlin, 2013.

[21] D. P. Hardin and E. B. Saff. Minimal Riesz energy point configurations for rectifiable d-dimensional manifolds. *Adv. Math.*, 193(1):174–204, 2005.

[22] P. Hellekalek. Digital (t, m, s)-nets and the spectral test. *Acta Arith.*, 105(2):197–204, 2002.

[23] P. Hellekalek. Hybrid function systems in the theory of uniform distribution of sequences. In *Monte Carlo and Quasi-Monte Carlo Methods 2010*, Springer Proceedings in Mathematics and Statistics, pages 435–449. Springer, Berlin, Heidelberg, 2012.

[24] P. Hellekalek and P. Kritzer. On the diaphony of some finite hybrid point sets. *Acta Arith.*, 156(3):257–282, 2012.

[25] E. Hewitt and K. A. Ross. *Abstract harmonic analysis. Vol. I*, volume 115 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin-New York, second edition, 1979. Structure of topological groups, integration theory, group representations.

[26] A. S. Jarrah and R. Laubenbacher. On the algebraic geometry of polynomial dynamical systems. In *Emerging applications of algebraic geometry*, volume 149 of *IMA Vol. Math. Appl.*, pages 109–123. Springer, New York, 2009.

[27] L. Kuipers and H. Niederreiter. *Uniform distribution of sequences*. Wiley-Interscience [John Wiley & Sons], New York-London-Sydney, 1974. Pure and Applied Mathematics.

[28] F. Y. Kuo, I. H. Sloan, and H. Woźniakowski. Lattice rules for multivariate approximation in the worst case setting. In H. Niederreiter and D. Talay, editors, *Monte Carlo and Quasi-Monte Carlo Methods 2004*, pages 289–330, Berlin, 2006. Springer.

[29] N. S. Landkof. *Foundations of modern potential theory*. Springer-Verlag, New York, 1972.

[30] G. Leobacher and F. Pillichshammer. *Introduction to quasi-Monte Carlo Integration and Applications. Compact Textbooks in Mathematics*. Birkhäuser, Basel, 2014.

[31] C. Mauduit, H. Niederreiter, and A. Sárközy. On pseudorandom $[0, 1)$ and binary sequences. *Publ. Math. Debrecen*, 71(3-4):305–324, 2007.

[32] C. Mauduit and J. Rivat. La somme des chiffres des carrés. *Acta Math.*, 203(1):107–148, 2009.

[33] C. Mauduit and J. Rivat. Sur un problème de Gelfond: la somme des chiffres des nombres premiers. *Ann. of Math. (2)*, 171(3):1591–1646, 2010.

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

[35] H. Niederreiter. Point sets and sequences with small discrepancy. *Monatsh. Math.*, 104:273–337, 1987.

[36] 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 (SIAM), Philadelphia, PA, 1992.

[37] H. Niederreiter and G. Pirsic. Duality for digital nets and its applications. *Acta Arith.*, 97(2):173–182, 2001.

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

[39] A. Ostafe and A. Winterhof. Some applications of character sums. In Gary L. Mullen and Daniel Panario, editors, *Handbook of finite fields*, pages 170–184. Boca Raton, FL: CRC Press, 2013.

[40] G. Pirsic and A. Winterhof. Boolean functions derived from pseudorandom binary sequences. In *Sequences and their applications—SETA 2012*, volume 7280 of *Lecture Notes in Comput. Sci.*, pages 101–109. Springer, Heidelberg, 2012.

[41] P. D. Proĭnov. On irregularities of distribution. *C. R. Acad. Bulgare Sci.*, 39(9):31–34, 1986.

[42] J. Rivat and A. Sárközy. On pseudorandom sequences and their application. In *General theory of information transfer and combinatorics*, volume 4123 of *Lecture Notes in Comput. Sci.*, pages 343–361. Springer, Berlin, 2006.

[43] K. F. Roth. On irregularities of distribution. *Mathematika*, 1:73–79, 1954.

[44] I. E. Shparlinski. On some dynamical systems in finite fields and residue rings. *Discrete Contin. Dyn. Syst.*, 17(4):901–917, 2007.

[45] M. M. Skriganov. Harmonic analysis on totally disconnected groups and irregularities of point distributions. *J. Reine Angew. Math.*, 600:25–49, 2006.

[46] I. H. Sloan and S. Joe. *Lattice methods for multiple integration*. Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, 1994.

[47] I. H. Sloan and H. Woźniakowski. When are quasi-Monte Carlo algorithms efficient for high dimensional integrals? *J. Complexity*, 14:1–33, 1998.

[48] J. Spanier. Quasi-Monte Carlo methods for particle transport problems. In *Monte Carlo and quasi-Monte Carlo methods in scientific computing*, pages 121–148. Berlin, Springer-Verlag, 1995.

[49] 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.

[50] 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.

[51] A. Winterhof. Topics related to character sums. *Int. Math. Nachr., Wien*, 220:1–27, 2012.

[52] H. Woźniakowski. Tractability and strong tractability of linear multivariate problems. *J. Complexity*, 10:96–128, 1994.