Arithmetic Primitives for Uniform Distribution Modulo 1.

Project Leader: Peter Hellekalek
Project Number: FWF SFB F05504
Funding Period: Feb. 1, 2014 - Jan 31, 2018

This project is about techniques relevant for the theory of uniform distribution modulo 1 (u.d.mod 1) of sequences and its applications in the field of random number generation and quasi-Monte Carlo methods. There is also a connection of this project to applied cryptography.

What do we want to achieve? We will contribute (i) to the question how well a given (finite) sequence is u.d.mod 1, by studying and developing appropriate figures of merit and investigating their relation (keywords: discrepancy, diaphony, spectral test, inequality of Erdös-Turàn- Koksma, inequality of Le Veque), (ii) to new construction methods for so-called low-discrepancy sequences (keywords: b-adic arithmetics, lattice methods), and (iii) to applied cryptography
(keywords: nonlinearity of Boolean functions, bit diffusion).

Where do we start? Any construction method for finite or infinite sequences of points is based on some arithmetical operations like addition or multiplication, on a suitable domain. It is most helpful if the algebraic structure underlying these operations is an abelian group. The choice of this group determines which function systems will be suitable for the analysis of a given sequence, because the construction method is intrinsically related to function systems, via the concept of the dual group. Different types of sequences require different types of function systems for their analysis. It deems us necessary not only to investigate new figures of merit for uniform distribution on [0, 1)s, in an attempt to generalize the so-called spectral test , but also to bring some order to the "zoo" of the numerous notions of such figures of merit. In particular, we will be interested in the inequality of Le Veque, among other goals of research. Hand in hand with the research on the spectral test, we will investigate new methods to generate low-discrepancy sequences, in an approach to complement arithmetics in finite fields by b-adic (p-adic) arithmetics. Finally, we would like to apply our b-adic method to the study of nonlinearity of Boolean functions, like they appear in cryptography, for example in the context of nonlinear filter functions in random bit generation.