1

Some highlights of Harald Niederreiter's work

Gerhard Larcher and Friedrich Pillichshammer
Johannes Kepler University Linz

Arne Winterhof
Austrian Acadamy of Sciences, Linz

Chaoping Xing
Nanyang Techological University, Singapore

Dedicated to our teacher, colleague and friend, Harald Niederreiter, on the occasion of his 70th birthday.

Abstract

In this paper we give a short biography of Harald Niederreiter and we spotlight some cornerstones from his wide-ranging work. We focus on his results on uniform distribution, algebraic curves, polynomials and quasi-Monte Carlo methods. In the flavor of Harald's work we also mention some applications including numerical integration, coding theory and cryptography.

1.1 A short biography

Harald Niederreiter was born in Vienna in 1944 on June 7 and spent his childhood in Salzburg. In 1963 he returned to Vienna to study at the Department of Mathematics of the University of Vienna, where he finished his PhD thesis entitled "Discrepancy in compact Abelian groups" *sub auspiciis praesidentis rei publicae*[1] under the supervision of Edmund Hlawka in 1969. From 1969 to 1978 he worked as scientist and professor in the USA at four different institutes: Southern Illinois University, University of Illinois at Urbana-Champaign, Institute for Advanced Study, Princeton, and University of California at Los Angeles. From 1978 to 1981 he was Chair of Pure Mathematics at the University of the West Indies in Kingston (Jamaica). He

[1] The term "Promotion sub auspiciis praesidentis rei publicae" is the highest possible honor for course achievement at school and university in Austria.

returned to Austria and served as director of two institutes of the Austrian Academy of Sciences in Vienna, of the Institute for Information Processing until 1999 and then of the Institute of Discrete Mathematics. From 2001 to 2009 he was professor at the National University of Singapore. Since 2009 he has been located at the Johann Radon Institute for Computational and Applied Mathematics in Linz. From 2010 to 2011 he was professor at the King Fahd University of Petroleum and Minerals in Dhahran (Saudi Arabia).

Harald Niederreiter's research areas include numerical analysis, pseudorandom number generation, quasi-Monte Carlo methods, cryptology, finite fields, applied algebra, algorithms, number theory and coding theory. He has published more than 350 research papers and several books, including the following.

- (with L. Kuipers) *Uniform Distribution of Sequences*. Wiley-Interscience, 1974; reprint, Dover Publications, 2006.
- (with R. Lidl) *Finite Fields*. Encyclopaedia of Mathematics and its Applications, volume 20. Addison-Wesley, 1983; second edition, Cambridge University Press, 1997.
- (with R. Lidl) *Introduction to Finite Fields and their Applications*. Cambridge University Press, 1986; revised edition, 1994.
- *Random Number Generation and Quasi-Monte Carlo Methods*. CBMS-NSF Regional Conference Series in Applied Mathematics, volume 63. Society for Industrial and Applied Mathematics (SIAM), 1992.
- (with C. P. Xing) *Rational Points on Curves over Finite Fields: Theory and Applications*. London Mathematical Society Lecture Note Series, volume 285. Cambridge University Press, 2001.
- (with C. P. Xing) *Algebraic Geometry in Coding Theory and Cryptography*. Princeton University Press, 2009.

Furthermore he is editor or co-editor of the following proceedings.

- (with P. J.-S. Shiue) *Monte Carlo and Quasi-Monte Carlo Methods in Scientific Computing*. Springer-Verlag, 1995.
- (with S. D. Cohen) *Finite Fields and Applications*. London Mathematical Society Lecture Note Series, volume 233. Cambridge University Press, 1996.
- (with P. Hellekalek, G. Larcher and P. Zinterhof) *Monte Carlo and Quasi-Monte Carlo Methods 1996*. Springer-Verlag, 1998.
- (with C. Ding and T. Helleseth) *Sequences and their Applications*. Springer-Verlag, 1999.

- (with J. Spanier) *Monte Carlo and Quasi-Monte Carlo Methods 1998*. Springer-Verlag, 2000.
- (with D. Jungnickel) *Finite Fields and Applications*. Springer-Verlag, 2001.
- (with K.-T. Fang and F. J. Hickernell) *Monte Carlo and Quasi-Monte Carlo Methods 2000*. Springer-Verlag, 2002.
- *Coding Theory and Cryptology*. World Scientific, 2002.
- *Monte Carlo and Quasi-Monte Carlo Methods 2002*. Springer-Verlag, 2004.
- (with K. Feng und C. P. Xing) *Coding, Cryptography and Combinatorics*. Birkhäuser-Verlag, 2004.
- (with D. Talay) *Monte Carlo and Quasi-Monte Carlo Methods 2004*. Springer-Verlag, 2006.
- (with A. Keller and S. Heinrich) *Monte Carlo and Quasi-Monte Carlo Methods 2006*. Springer-Verlag, 2008.
- (with Y. Li, S. Ling, H. Wang, C. P. Xing and S. Zhang) *Coding and Cryptology*. World Scientific, 2008.
- (with A. Ostafe, D. Panario and A. Winterhof) *Algebraic Curves and Finite Fields: Cryptography and Other Applications*. de Gruyter, 2014.
- (with P. Kritzer, F. Pillichshammer and A. Winterhof) *Uniform Distribution and Quasi-Monte Carlo Methods: Discrepancy, Integration and Applications*. de Gruyter, 2014.

Some important methods are named after him, such as the Niederreiter public-key cryptosystem, the Niederreiter factoring algorithm for polynomials over finite fields, and the Niederreiter and Niederreiter–Xing low-discrepancy sequences.

Some of his honors and awards are

- full member of the Austrian Academy of Sciences
- full member and former member of the presidium of the German Academy of Natural Sciences Leopoldina
- Cardinal Innitzer Prize for Natural Sciences in Austria
- invited speaker at ICM 1998 (Berlin) and ICIAM 2003 (Sydney)
- Singapore National Science Award 2003
- honorary member of the Austrian Mathematical Society 2012
- Fellow of the American Mathematical Society 2013.

Niederreiter was also the initiator and, from 1994 to 2006, the co-chair of the first seven biennial *Monte Carlo and quasi-Monte Carlo meetings* which took place in

- Las Vegas, NV, USA (1994)
- Salzburg, Austria (1996)

- Claremont, CA, USA (1998)
- Hong Kong (2000)
- Singapore (2002)
- Juan-Les-Pins, France (2004)
- Ulm, Germany (2006)
- Montreal, Canada (2008)
- Warsaw, Poland (2010)
- Sydney, Australia (2012)
- Leuven, Belgium (2014).

In 2006 Harald Niederreiter announced his wish to step down from the organizational role, and a Steering Committee was formed to ensure and oversee the continuation of the conference series.

1.2 Uniform distribution theory and number theory

When we scroll over the more than 350 scientific articles by Niederreiter which have appeared in renowned journals such as *Mathematika*, *Duke Mathematical Journal*, *Bulletin of the American Mathematical Society* and *Compositio Mathematica*, we find that most of these papers have connections to topics from number theory or use techniques from number theory, and many of the articles deal with problems and solve open questions, or initiate a new field of research in the theory of uniform distribution of sequences. The later sections in this overview of Harald's work on coding theory, algebraic curves and function fields, pseudorandom numbers, finite fields, and quasi-Monte Carlo methods in a certain sense will also deal with number-theoretical aspects.

Let us give just one example: the analysis and the precise estimation of exponential sums $\sum_{k=0}^{N-1} \mathrm{e}^{2\pi \mathtt{i} f(k)}$ or, in particular, of character sums plays an essential role in many different branches of mathematics and especially in number theory. In particular, it plays a basic role in many questions concerning uniform distribution of sequences, discrepancy theory, quasi-Monte Carlo methods, pseudorandom number analysis, the theory of finite fields, and many more. In a variety of papers on exponential sums and their applications, Niederreiter has proven to be a leading expert in the analysis of exponential sums and has essentially developed a variety of important techniques.

In this section we want to pick out some of the most impressive of Niederreiter's work on topics in number theory and in uniform distribution theory that will not be described explicitly in subsequent sections.

In the first years after finishing his PhD thesis "Discrepancy in compact Abelian groups" under the supervision of Edmund Hlawka, Niederreiter was concerned with basic questions from the theory of uniform distribution, from discrepancy theory and from metrical uniform distribution theory. We want to highlight three papers of this first phase.

In the paper "An application of the Hilbert–Montgomery–Vaughan inequality to the metric theory of uniform distribution mod 1" [12] which appeared in 1976 in the *Journal of the London Mathematical Society*, Niederreiter used tools from the theory of bounded quadratic and bilinear forms, especially an inequality of Montgomery and Vaughan based on large sieve methods, to establish an analog of Koksma's metric theorem for uniform distribution modulo one with respect to a general class of summation methods.

One of the most powerful tools for estimating the discrepancy of sequences is the Koksma–Erdős–Turán inequality which bounds the discrepancy of a sequence by a weighted sum of the values of its Weyl sums. The joint paper with Walter Philipp, which appeared in the *Duke Mathematical Journal* in 1973, "Berry–Esseen bounds and a theorem of Erdős and Turán on uniform distribution mod 1" [29], gave a much more general result about distances of functions that contains the one-dimensional Koksma–Erdős–Turán inequality as a special case. The given theorem is an analog of the standard Berry–Esseen lemma for $\mathbb{R}^s$.

One of the highlights in this period, and of the work of Niederreiter in metric Diophantine approximation theory certainly, was the solution of a conjecture of Donald Knuth, together with Robert F. Tichy, in the paper "Solution of a problem of Knuth on complete uniform distribution of sequences" [37] which appeared in *Mathematika* in 1985. It was shown that for any sequence $(a_n)_{n\geq 1}$ of distinct positive integers, the sequence $(x^{a_n})_{n\geq 1}$ is completely uniformly distributed modulo one for almost all real numbers x with $|x| > 1$. In the paper "Metric theorems on uniform distribution and approximation theory" [38], again in cooperation with Tichy, this result was even generalized to the following form: the sequence $(cx^{b_n})_{n\geq 1}$ is completely uniformly distributed modulo one for all $c \neq 0$ for almost all real numbers x with $|x| > 1$ whenever $(b_n)_{n\geq 1}$ is any sequence of reals with $\inf b_n > -\infty$ and $\inf_{m\neq n} |b_n - b_m| > 0$.

In the analysis of the distribution properties of sequences and of point sets, especially of Kronecker sequences

$$((\{n\alpha_1\}, \ldots, \{n\alpha_s\}))_{n\geq 0}$$

and of lattice point sets

$$\left(\left(\left\{n\frac{a_1}{N}\right\}, \ldots, \left\{n\frac{a_s}{N}\right\}\right)\right)_{n=0,\ldots,N-1}$$

in the s-dimensional unit cube, one is often led to questions from the theory of Diophantine approximations, of the geometry of numbers or to questions concerning continued fraction expansions. A famous still open problem in the theory of continued fractions is the following conjecture of Zaremba.

There is a constant c such that for every integer $N \geq 2$ there exists an integer a with $1 \leq a \leq N$ and with $\gcd(a, N) = 1$ such that all continued fraction coefficients of $\frac{a}{N}$ are bounded by c. Indeed it is conjectured that $c = 5$ satisfies this property.

In the paper "Dyadic fractions with small partial quotients" [14], Niederreiter proved that this result is true even with $c = 3$ if N is a power of 2. He also proved the conjecture of Zaremba for N equal to powers of 3 and equal to powers of 5. Only quite recently it was shown by Bourgain and Kontorovich that Zaremba's conjecture holds for almost all choices of N.

From Niederreiter's result it can be deduced, for example, that for all $N = 2^m$ there exists an integer a such that the lattice point set

$$\left(\left(\left\{n\frac{1}{2^m}\right\}, \left\{n\frac{a}{2^m}\right\}\right)\right)_{n=0,\ldots,2^m-1}$$

has discrepancy $D_N \leq c' \frac{\log N}{N}$, i.e., has best possible order of discrepancy.

The investigation of certain types of digital (t, m, s)-nets and of digital $(\mathbf{T}, s)$-sequences (see also Section 1.5) in analogy leads to questions concerning non-Archimedean Diophantine approximation and to questions concerning continued fraction expansions of formal Laurent series. Such questions were analyzed, for example, in the papers [7, 8, 16, 21].

In an impressive series of papers together with Igor Shparlinski, powerful methods for the estimation of exponential sums with nonlinear recurring sequences were developed by Niederreiter, see also Section 1.4 below. In the paper "On the distribution of power residues and primitive elements in some nonlinear recurring sequences" [36] which appeared in the *Bulletin of the London Mathematical Society* in 2003, it was shown that these methods can also be applied to estimation of the sums of multiplicative characters. As a consequence, results were obtained in this paper on the distribution of power residues and of primitive elements in such sequences.

So consider a sequence of elements $u_0, u_1, \ldots, u_{N-1}$ of the finite field $\mathbb{F}_q$ obtained by the recurrence relation

$$u_{n+1} = au_n^{-1} + b,$$

where we set $u_{n+1} = b$ if $u_n = 0$. For a divisor s of $q - 1$ let $R_s(N)$ be the number of s-power residues (i.e., the number of $w \in \mathbb{F}_q$ such that there are $z \in \mathbb{F}_q$ with $z^s = w$) among $u_0, u_1, \ldots, u_{N-1}$. Then

$$\left| R_s(N) - \frac{N}{s} \right| < (2.2) N^{1/2} q^{1/4}$$

for $1 \leq N \leq t$, where t is the least period of the recurring sequence. The case of general nonlinear recurrence sequences was studied later [40].

In the present, Harald Niederreiter is still a creative and productive researcher in the field of number theory and uniform distribution of sequences. We want to confirm this fact by giving two recent examples of his impressive work in these fields.

In the joint paper "On the Gowers norm of pseudorandom binary sequences" [32] with Joël Rivat, the modern concepts of Christian Mauduit and András Sárközy concerning new measures for pseudorandomness and of William T. Gowers in combinatorial and additive number theory were brought together, and the Gowers norm for periodic binary sequences was studied. A certain relation between the Gowers norm of a binary function f defined on the integers modulo N and a certain correlation measure for the sequence $(f(n))_{n \geq 1}$ introduced in [11] was shown.

A quite new and challenging trend in the theory of uniform distribution of sequences is the investigation of the distribution of hybrid sequences. A hybrid sequence is defined as follows: take an s-dimensional sequence $(\boldsymbol{x}_n)_{n \geq 0}$ of a certain type and a t-dimensional sequence $(\boldsymbol{y}_n)_{n \geq 0}$ of another type and combine them as an $(s+t)$-dimensional *hybrid sequence*, i.e., with some abuse of notation,

$$(\boldsymbol{z}_n)_{n \geq 0} := ((\boldsymbol{x}_n, \boldsymbol{y}_n))_{n \geq 0}.$$

Well-known examples of such sequences are Halton–Kronecker sequences (generated by combining Halton sequences with Kronecker sequences) and Halton–Niederreiter sequences (a combination of digital (t, s)-sequences or of digital $(\mathbf{T}, s)$-sequences in different bases). Investigation of these sequences again leads to challenging problems in number theory. For example, with the papers [22, 23, 24, 25, 26], Niederreiter influenced the direction of research in this topic.

1.3 Algebraic curves, function fields and applications

The study of algebraic curves over finite fields can be traced back to Carl Friedrich Gauss who studied equations over finite fields. However, the real beginning of this topic was the proof of the Riemann hypothesis for algebraic curves over finite fields by André Weil in the 1940s. This topic has attracted the attention of researchers again since the 1980s due to the discovery of algebraic geometry codes by Valerii D. Goppa. This application of algebraic curves over finite fields, and especially of those with many rational points, created a much stronger interest in the area and attracted new groups of researchers such as coding theorists and algorithmically inclined mathematicians. Nowadays, algebraic curves over finite fields is a flourishing subject which produces exciting research and is immensely relevant for applications.

Harald Niederreiter started this topic from applications first. In the late 1980s, he found an elegant construction of (t, m, s)-nets and (t, s)-sequences (see Section 1.5). Then he realized that the construction can be generalized to global function fields [43, 44]. From this point, Harald Niederreiter investigated extensively algebraic curves over finite fields with many rational points and their applications. Algebraic curves over finite fields can be described in an equivalent algebraic language, i.e., global function fields over finite fields. For many of the applications, people are interested in algebraic curves over finite fields with many rational points or, equivalently, global function fields over finite fields with many rational places. Since the global function field language was usually used by Harald Niederreiter, we adopt this language from now onwards in this section.

Let $\mathbb{F}_q$ denote the finite field of q elements. An extension F of $\mathbb{F}_q$ is called an algebraic function field of one variable over $\mathbb{F}_q$ if there exists an element x of F that is transcendental over $\mathbb{F}_q$ such that F is a finite extension over the rational function field $\mathbb{F}_q(x)$. We usually denote by $F/\mathbb{F}_q$ a global function field with the full constant field $\mathbb{F}_q$, i.e., all elements in $F \setminus \mathbb{F}_q$ are transcendental over $\mathbb{F}_q$. A place P of F is called *rational* if its residue field F_P is isomorphic to the ground field $\mathbb{F}_q$. For many applications in coding theory, cryptography and low-discrepancy sequences, people are interested in those function fields with many rational places. On the other hand, the number of rational places of a function field over $\mathbb{F}_q$ is constrained by an important invariant of F, called the genus. If we use $g(F)$ and $N(F)$ to denote the genus and the number of rational places of $F/\mathbb{F}_q$, the well-known Hasse–Weil bound says that

$$|N(F) - q - 1| \leq 2g(F)\sqrt{q}. \qquad (1.1)$$

The above bound implies that the number of rational places cannot be too big if we fix the genus of a function field. Now the problem becomes to find the maximal number of rational places that a global function field over $\mathbb{F}_q$ of genus g could have. We usually denote by $N_q(g)$ this quantity, i.e., $N_q(g) =$

$\max\{N(F) : F/\mathbb{F}_q$ has genus $g\}$. Apparently, it follows from the Hasse–Weil bound that

$$|N_q(g) - q - 1| \le 2g\sqrt{q} \tag{1.2}$$

for any prime power q and nonnegative integer g. For given q and g, determining the exact value of $N_q(g)$ is a major problem in the study of global function fields. In general it is very difficult to determine the exact value of $N_q(g)$. Instead, it is sufficient to find reasonable lower bounds for most applications. Lower bounds on $N_q(g) \ge N$ are found either by explicit construction or by showing the existence of global function fields of genus g with at least N rational places. Investigation of this problem involves several subjects such as algebraic number theory and algebraic geometry and even coding theory. The method that Harald Niederreiter employed is class field theory in algebraic number theory. He found many record function fields through class field theory, i.e., global function fields with best-known number of rational places. Some of these record function fields are listed below (see [44, 45, 46, 47, 48, 49, 50, 53, 59]).

(q, g)	(2, 23)	(2, 25)	(2, 29)	(2, 31)	(2, 34)	(2, 36)	(2, 49)	(3, 6)	(3, 7)
$N_q(g)$	22	24*	25	27	27	30	36	14*	16*

The entries with an asterisk are the exact values of $N_q(g)$, while the entries without an asterisk are lower bounds on $N_q(g)$.

For a fixed prime power q, to measure how $N_q(g)$ behaves while g tends to infinity, we define the following asymptotic quantity

$$A(q) := \limsup_{g\to\infty} \frac{N_q(g)}{g}. \tag{1.3}$$

It is immediate from the Hasse–Weil bound that $A(q) \le 2\sqrt{q}$. Sergei G. Vlăduţ and Vladimir G. Drinfeld refined this bound to $A(q) \le \sqrt{q} - 1$. Yasutaka Ihara first showed that $A(q) \ge \sqrt{q} - 1$ if q is a square. Thus, the problem of determining $A(q)$ is completely solved for squares q. It still remains to determine $A(q)$ for nonsquare q. Like the case of $N_q(g)$, finding the exact value of $A(q)$ for nonsquare q is very difficult. Although people have tried very hard, so far $A(q)$ has not been determined for any single nonsquare q. In particular, if q is a prime, it is a great challenge to determine or find a reasonable lower bound on $A(q)$.

What Harald Niederreiter did for this problem was to find a new bound on $A(2)$ and an improvement on $A(q^m)$ for odd m. More precisely, he proved the following result [51, 52].

Theorem 1.1 *One has* $A(2) \geq \frac{81}{317} = 0.2555\ldots$.

Theorem 1.2 *One has the following bounds.*

(*i*) *If q is an odd prime power and $m \geq 3$ is an integer, then*

$$A(q^m) \geq \frac{2q+2}{\lceil 2(2q+3)^{1/2} \rceil + 1}.$$

(*ii*) *If $q \geq 8$ is a power of 2 and $m \geq 3$ is an odd integer, then*

$$A(q^m) \geq \frac{q+1}{\lceil 2(2q+2)^{1/2} \rceil + 2}.$$

Harald Niederreiter has also been working on applications of algebraic curves over finite fields. These applications include low-discrepancy sequences, coding theory and cryptography, etc. For details on the application of algebraic curves over finite fields to low-discrepancy sequences, we refer to Section 1.5.

For applications to coding theory, Harald Niederreiter's contribution was the discovery of several new codes via the theory of algebraic curves over finite fields. Some of the new codes discovered by Harald Niederreiter are listed below (see [3]). In the table, $[n, k, d]_q$ is a q-ary code of length n, dimension k and minimum distance d.

$[108, 25, 44]_4$	$[108, 26, 43]_4$	$[113, 27, 45]_4$	$[130, 29, 53]_4$	$[27, 11, 13]_8$	$[30, 7, 19]_8$
$[30, 8, 18]_8$	$[30, 9, 17]_8$	$[36, 7, 23]_8$	$[36, 8, 22]_8$	$[36, 9, 21]_8$	$[36, 10, 20]_8$

Harald Niederreiter has also done some significant work on asymptotic results of coding theory and cryptography via algebraic curves over finite fields.

1.4 Polynomials over finite fields and applications

Now we describe some of Harald Niederreiter's results on polynomials over finite fields and applications. We start with complete mappings and check digit systems.

Let $\mathbb{F}_q$ be the finite field of $q > 2$ elements and $f(X) \in \mathbb{F}_q[X]$ a permutation polynomial over $\mathbb{F}_q$. We call $f(X)$ a *complete mapping* if $f(X) + X$ is also a permutation polynomial. Existence results on complete mappings and their application to check digit systems were discussed in [33, 56].