Some highlights of Harald Niederreiter’s work

Gerhard Larcher,∗ Friedrich Pillichshammer,† Arne Winterhof‡ and Chaoping Xing§

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 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 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 returned to Austria and served as director of two institutes of the Austrian Academy of Sciences in Vienna, until 1999 of the Institute for Information Processing and then of the Institute of Discrete Mathematics. From 2001 to 2009 he was professor at the National University of Singapore. Since 2009 he is 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).

∗G. Larcher is supported by the Austrian Science Fund (FWF): Project F5507-N26, which is a part of the Special Research Program "Quasi-Monte Carlo Methods: Theory and Applications".
†F. Pillichshammer is supported by the Austrian Science Fund (FWF): Project F5509-N26, which is a part of the Special Research Program "Quasi-Monte Carlo Methods: Theory and Applications".
‡A. Winterhof is supported by the Austrian Science Fund (FWF): Project F5511-N26, which is a part of the Special Research Program "Quasi-Monte Carlo Methods: Theory and Applications".
§C. Xing is supported by Singapore Ministry of Education Tier 1 grant 2013-T1-002-033

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

- (with L. Kuipers) Uniform distribution of sequences. Pure and Applied Mathematics. Wiley-Interscience, New York-London-Sydney, 1974; reprint, Dover Publications, 2006.

- (with R. Lidl) Finite fields. Encyclopaedia of Mathematics and its Applications, 20. Addison-Wesley Publishing Company, Advanced Book Program, Reading, MA, 1983; 2nd ed., Cambridge University Press, 1997.

- (with R. Lidl) Introduction to Finite Fields and Their Applications, Cambridge University Press, 1986; revised ed., Cambridge University Press, 1994.

- Random number generation and quasi-Monte Carlo methods. CBMS-NSF Regional Conference Series in Applied Mathematics, 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, 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

- (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, 233, Cambridge University Press, 1996.

- (with P. Hellekalek, G. Larcher und P. Zinterhof) Monte Carlo and Quasi-Monte Carlo Methods 1996, Springer-Verlag, 1998.

- (with C. Ding und 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 Publishing, 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 Publishing, 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.

It follows an excerpt of his honors and awards:

• 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 is 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, USA (1994)

• Salzburg, Austria (1996)

• Claremont, USA (1998)

• Hong Kong (2000)

• Singapore (2002)

• Juan-Les-Pins, France (2004)
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.

2 Uniform distribution theory and number theory

When we scroll over the more than 350 scientific articles of Niederreiter which appeared in such renowned journals like "Mathematika", "Duke Mathematical Journal", "Bulletin of the AMS", or "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 these articles deal with problems and solve open questions, or initiate a new field of research in the theory of uniform distribution of sequences. So also the later sections on Harald’s work on coding theory, algebraic curves and function fields, on pseudorandom numbers, on finite fields, and on quasi-Monte Carlo methods in this overview in a certain sense will deal with number-theoretical aspects.

Let us give just one example: The analysis and the precise estimation of exponential sums \( \sum_{k=0}^{N-1} e^{2\pi i f(k)} \), or, in particular, of character sums plays an essential role in many different branches of mathematics and especially in number theory. So particularly it plays a basic role in many questions concerning uniform distribution, discrepancy theory, in quasi-Monte Carlo methods, in pseudorandom number analysis, in 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 various most important techniques.

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

In the first years after finishing his PhD thesis on "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 of the 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 uses 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 analogue 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 discrepancy of sequences is the inequality of Koksma-Erdős-Turán which bounds the discrepancy of a sequence by a weighted sum of the values of its Weyl sums. In the joint paper “Berry-Esseen bounds and a theorem of Erdős and Turán on uniform distribution mod 1” [29] with Walter Philipp - this paper appeared in the Duke Mathematical Journal in 1973 - a much more general result about distances of functions is shown that contains the one-dimensional Koksma-Erdős-Turán inequality as a special case. The given theorem is an analogue 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 modulo one” [37] which appeared in Matematika in 1985. It is shown there 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 $\inf_{n \neq m} |b_n - b_m| > 0$.

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

\[((\{na_1\}/N), \ldots, \{na_s\}/N))_{n=0,\ldots,N-1}\]

in the $s$-dimensional unit-cube, one often is 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 $a/N$ are bounded by $c$. Indeed it is conjectured that $c = 5$ satisfies this property.

Niederreiter in “Dyadic fractions with small partial quotients” [14] proved that this result is true even with $c = 3$ if $N$ is a power of 2. He proves the conjecture of Zaremba also 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 now for example it can be deduced that for all $N = 2^m$ there exists an integer $a$ such that the lattice point set

\[((\{n/2^m\}, \{na/2^m\}))_{n=0,\ldots,2^m-1}\]

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

The investigation of certain types of digital $(t,m,s)$-nets and of digital $(T,s)$-sequences (see also Section 5 of this article) 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 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 is shown that these methods also can be applied to estimating sums of multiplicative characters as well. As a consequence, results are obtained in this paper about 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

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

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 in [40].

Also in the present Harald Niederreiter is still an utmost creative and productive researcher in the field of number theory and uniform distribution of sequences. We want to confirm this fact by giving two last quite 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 is 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] is 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 $(x_n)_{n \geq 0}$ of a certain type and a $t$-dimensional sequence $(y_n)_{n \geq 0}$ of another type and combine them to an $(s+t)$-dimensional hybrid sequence, i.e., with some abuse of notation,

$$(z_n)_{n \geq 0} := ((x_n, y_n))_{n \geq 0}.$$

Well known examples of such sequences are Halton-Kronecker sequences (generated by combining Halton sequences with Kronecker sequences) or Halton-Niederreiter sequences (a combination of digital $(t,s)$-sequences or of digital $(T,s)$-sequences in different bases). The investigation of these sequences again leads to challenging problems in number theory. For example with his papers [22, 23, 24, 25, 26] Niederreiter essentially influences the direction of research in this topic.
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 great attention of the 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 5). Then he realized that the construction can be generalized to global function fields \([43, 44]\). From this point, Harald Niederreiter has extensively investigated 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 genus. If we use \(g(F)\) and \(N(F)\) to denote genus and number of rational places of \(F/\mathbb{F}_q\), the well-known Hasse-Weil bound says that

\[
|N(F) - q - 1| \leq 2g(F)\sqrt{q}. \tag{1}
\]

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 game 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., \(N_q(g) = \max\{N(F) : F/\mathbb{F}_q\ \text{has genus} \ g\}\). Apparently, it follows from the Hasse-Weil bound that

\[
|N_q(g) - q - 1| \leq 2g\sqrt{q} \tag{2}
\]

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. Finding lower bounds on \(N_q(g) \geq N\) is through either explicit construction or showing existence of global function fields of genus
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, 51, 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 asterisk in the above table are the exact values of $N_q(g)$, while the entries without asterisk in the above table 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

$$A(q) := \limsup_{g \to \infty} \frac{N_q(g)}{g}.$$  \hspace{1cm} (3)

It is immediate from the Hasse-Weil bound that $A(q) \leq 2\sqrt{q}$. Sergei G. Vlăduț and Vladimir G. Drinfeld refined this bound to $A(q) \leq \sqrt{q} - 1$. Yasutaka Ihara first showed that $A(q) \geq \sqrt{q} - 1$ 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 in this topic. 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 on this problem was finding a new bound on $A(2)$ and an improvement on $A(q^m)$ for odd $m$. More precisely, he proved the following result in [52, 53].

**Theorem 1** One has $A(2) \geq \frac{81}{317} = 0.2555...$.

**Theorem 2** One has the following bounds:

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

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

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

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

Harald Niederreiter has been also working on applications of algebraic curves over finite fields. These applications include low-discrepancy sequences, coding theory and cryptography, etc. For the details on application of algebraic curves over finite fields to low-discrepancy sequences, we refer to Section 5.

For applications of algebraic curves over finite fields 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 following table, $[n, k, d]_q$ means a $q$-ary code of length $n$, dimension $k$ and minimum distance $d$. 




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

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 \([33, 56]\).

It is easy to see that \( f(X) = aX \) is a complete mapping whenever \( a \notin \{−1, 0\} \).

Complete mappings are pertinent to the construction of orthogonal Latin squares, see \([10]\), which can be used to design some agricultural experiments. However, here we will describe another application of complete mappings, namely, check digit systems.

A check digit system (defined with one permutation polynomial over \( \mathbb{F}_q \)) consists of a permutation polynomial \( f(X) \in \mathbb{F}_q[X] \) and a control symbol \( c \in \mathbb{F}_q \) such that each word \( a_1, \ldots, a_{s−1} \in \mathbb{F}_q^{s−1} \) of length \( s−1 \) is extended by a check digit \( a_s \in \mathbb{F}_q \) such that

\[
\sum_{i=0}^{s−1} f(i)(a_{i+1}) = c,
\]

where \( f(i) \) is recursively defined by \( f(0)(X) = X \) and \( f(i)(X) = f(f(i−1)(X)) \) for \( i = 1, 2, \ldots \).

An example of a check digit system is the international standard book number (ISBN-10) which consists of a string of 10 digits \( x_1 − x_2 x_3 x_4 x_5 x_6 − x_7 x_8 x_9 − x_{10} \). The first digit \( x_1 \) characterizes the language group, \( x_2 x_3 x_4 \) is the number of the publisher, \( x_5 x_6 x_7 x_8 x_9 \) is the actual book number, and \( x_{10} \) is a check digit. A correct ISBN satisfies

\[
x_1 + 2x_2 + 3x_3 + 4x_4 + 5x_5 + 6x_6 + 7x_7 + 8x_8 + 9x_9 + 10x_{10} = 0 \in \mathbb{F}_{11}.
\]

With the variable transformation \( a_i = x_{2i−1} \mod 11 \) we get a check digit system defined with one permutation \( f(X) = 2X \). Note that \( f(X) = 2X \) and \( −f(X) = 9X \) are both complete mappings of \( \mathbb{F}_{11} \).

For example the ISBN-10 of the monograph on finite fields by Lidl and Niederreiter \([9]\) is \( 0 − 521 – 39231 – 4 \).

Since \( f(X) \) is a permutation polynomial, such a system detects all single errors \( a \mapsto b \). Moreover it detects all

- neighbor transpositions \( ab \mapsto ba \) if \( −f(X) \) is a complete mapping;
- twin errors \( aa \mapsto bb \) if \( f(X) \) is a complete mapping.

Niederreiter and Karl H. Robinson \([33]\) found several nontrivial classes of complete mappings and proved in particular a generalization of the following result:

\[
\begin{array}{|c|c|c|c|c|c|c|}
\hline
108, 25, 44 & 108, 26, 43 & 113, 27, 45 & 130, 29, 53 & 27, 11, 13 & 30, 7, 19 \\
30, 8, 18 & 30, 9, 17 & 36, 7, 23 & 36, 8, 22 & 36, 9, 21 & 36, 10, 20 \\
\hline
\end{array}
\]
Theorem 3 Let \( q \) be odd. Then \( f_b(X) = X^{(q+1)/2} + bX \) is a complete mapping of \( \mathbb{F}_q \) if and only if \( b^2 - 1 \) and \( b^2 + 2b \) are both squares of nonzero elements of \( \mathbb{F}_q \). The number of \( b \) such that \( f_b(X) \) is a complete mapping is \( \frac{q}{4} + O(q^{1/2}) \).

For a survey on (generalizations of) complete mappings and some applications we refer to [58].

Harald Niederreiter also invented a deterministic algorithm based on linear algebra for factoring a univariate polynomial \( f(X) \) over \( \mathbb{F}_q \) which is efficient for small characteristic, see [20] for the initial article and [4] for a survey on factorization. The key step is to find a polynomial \( h(X) \) which satisfies the differential equation

\[
f^q(h/f)^{(q-1)} + h^q = 0,
\]

where \( g^{(k)} \) denotes the \( k \)th Hasse-Teichmüller derivative. Then \( \gcd(f, h) \) is a nontrivial factor of \( f \).

Harald Niederreiter did not only contribute to cryptography via the above mentioned public-key cryptosystem named after him, but also in many other ways. For example he proved several results on the interpolation of the discrete logarithm [17, 39] showing that there is no low degree polynomial \( f(X) \in \mathbb{F}_q[X] \) which coincides with the discrete logarithm on many values, that is for prime \( q \), \( f(g^x) = x \) for many \( x \), where \( g \) is a primitive element of \( \mathbb{F}_q \). Hence, the discrete logarithm problem is not attackable via simple interpolation which is necessary for the security of discrete logarithm based cryptosystems as the Diffie-Hellman key exchange.

Finally, he introduced and studied nonlinear pseudorandom number generators, i.e., sequences over \( \mathbb{F}_q \) of the form

\[
u_{n+1} = f(u_n), \quad n = 0, 1, \ldots
\]

for some initial value \( u_0 \in \mathbb{F}_q \) and a polynomial \( f(X) \in \mathbb{F}_q[X] \) of degree at least 2. These sequences are attractive alternatives to linear pseudorandom number generators which are not suitable for all applications. For example, linear generators are highly predictable and not suitable in cryptography.

As mentioned before in joint work with Igor Shparlinski [34, 35] Niederreiter found a way to prove nontrivial estimates on certain character sums which in the simplest case are of the form

\[
\sum_{n=0}^{N-1} \chi(f(u_n))
\]

where \( \chi \) is any nontrivial additive character of \( \mathbb{F}_q \). For such character sums the standard method for estimating incomplete character sums by reducing them to complete ones and then applying the Weil bound does not work. The method and result of [34] was later slightly improved in [41]. In particular if \( f(X) = aX^{q-2} + b \), i.e. \( f(c) = ac^{-1} + b \) if \( c \neq 0 \), this method yields strong bounds on the exponential sums and leads to very good discrepancy bounds for corresponding sequences in the unit interval. For a survey on nonlinear recurrence sequences see [57].
5 Quasi-Monte Carlo methods

The quasi-Monte Carlo method has its roots in the theory of uniform distribution modulo 1 (see Section 2) and is nowadays a powerful tool in computational mathematics, in particular for the numerical integration of very high dimensional functions, with many applications to practical problems coming from biology, computer graphics, mathematical finance, statistics, etc. Here the integral of a function \( f : [0, 1]^s \to \mathbb{R} \) is approximated by a quasi-Monte Carlo (QMC) rule which computes the arithmetic mean of function values over a finite set of sample nodes, i.e.,

\[
\int_{[0,1]^s} f(x) \, dx \approx \frac{1}{N} \sum_{n=0}^{N-1} f(x_n)
\]

with fixed \( x_0, \ldots, x_{N-1} \in [0,1)^s \). QMC rules can be viewed as deterministic versions of Monte Carlo rules. The fundamental error estimate for QMC rules is the Koksma-Hlawka inequality which bounds the absolute integration error as

\[
\left| \int_{[0,1]^s} f(x) \, dx - \frac{1}{N} \sum_{n=0}^{N-1} f(x_n) \right| \leq V(f) D_N^*(x_0, \ldots, x_{N-1}),
\]

where \( V(f) \) is the variation of \( f \) in the sense of Hardy and Krause and where \( D_N^* \) is the star discrepancy of the underlying sample nodes, see [6].

In the mid of the 1970s Harald Niederreiter started to investigate QMC methods. His first pioneering work was the paper “Quasi-Monte Carlo methods and pseudo-random numbers” [13] published in the Bulletin of the American Mathematical Society in 1978. Today this paper can be seen as the first systematic survey about the theoretical foundations of QMC dealing with Koksma-Hlawka type inequalities and with constructions of point sets for QMC rules such as Halton’s sequence, Sobol’s construction of \( P_\tau \) nets and \( LP_\tau \) sequences, and good lattice points in the sense of Korobov and Hlawka.

The quintessence of the Koksma-Hlawka inequality is that good QMC rules should be based on sample nodes with low discrepancy, informally often called low-discrepancy point sets. Today there are two main streams of constructing low-discrepancy point sets. Both constructions are intimately connected with the name Niederreiter who contributed pioneering works to these topics. The first construction is the concept of lattice point sets and the second one is the concept of \((t,m,s)\)-nets and \((t,s)\)-sequences in a base \( b \).

An \( N \)-element lattice point set (cf. Section 2) is based on an \( s \)-dimensional lattice point \( a = (a_1, \ldots, a_s) \). The \( n \)th element of such a lattice point set is then given as

\[
x_n = \left\{ \frac{n}{N} a \right\} \quad \text{for } n = 0, 1, \ldots, N - 1,
\]

where the fractional part function \( \{ \cdot \} \) is applied component-wise. QMC rules which are based on good lattice point sets are called the method of good lattice points or lattice rules and belong nowadays to the most popular QMC rules in practical applications. Niederreiter analyzed distribution properties and showed the existence of good lattice point sets with low discrepancy. The full power of lattice rules however lies in the integration of smooth one-periodic functions. One reason for this is the following relation: for \( h \in \mathbb{Z}^s \)

\[
\frac{1}{N} \sum_{n=0}^{N-1} \exp \left( 2\pi i \frac{n}{N} a \cdot h \right) = \begin{cases} 
1 & \text{if } a \cdot h \equiv 0 \pmod{N}, \\
0 & \text{if } a \cdot h \not\equiv 0 \pmod{N},
\end{cases}
\]
where \( \cdot \) denotes the usual inner product. Niederreiter studied the worst-case error \( P_\alpha \) for the integration of functions \( f \) which can be represented by absolutely convergent Fourier series whose Fourier coefficients \( \hat{f}(h) \) tend to zero as \( h \) moves away from the origin at a prescribed rate which is determined by the parameter \( \alpha \). His most important contributions to the theory of good lattice point sets are summarized in Chapter 5 of his book “Random number generation and quasi-Monte Carlo methods” [19], which appeared in 1992. Niederreiter’s most recent contributions to the theory of lattice point sets deal with the existence and construction of so-called extensible lattice point sets which have the property that the number of points in the node set may be increased while retaining the existing points (see [5, 30]).

The theory of \((t,m,s)\)-nets and \((t,s)\)-sequences was initiated by Niederreiter in his seminal paper “Point sets and sequences with small discrepancy” [15] published in the Monatshefte für Mathematik in 1987. The basic idea of these concepts is that if a point set has good equidistribution properties with respect to a reasonable (finite) set of test sets, then the point set already has low star discrepancy at all. The definition of a \((t,m,s)\)-net in base \( b \) can be stated as follows:

**Definition 1 (Niederreiter, 1987)** Let \( s, b, m, t \) be integers satisfying \( s \geq 1, b \geq 2 \) and \( 0 \leq t \leq m \). A set \( P \) consisting of \( b^m \) elements in \([0,1)^s\) is said to be a \((t,m,s)\)-net in base \( b \) if every so-called elementary interval of the form

\[
\prod_{j=1}^{s} \left[ \frac{a_j}{b^{d_j}}, \frac{a_j + 1}{b^{d_j}} \right]
\]

of volume \( b^{-m} \) with \( d_j \in \mathbb{N}_0 \) and \( a_j \in \{0,1,\ldots,b^{d_j} - 1\} \) for \( j = 1,2,\ldots,s \), contains exactly \( b^t \) elements of \( P \).

A \((t,s)\)-sequence in base \( b \) is an infinite version of \((t,m,s)\)-nets.

**Definition 2 (Niederreiter, 1987)** Let \( s, b, t \) be integers satisfying \( s \geq 1, b \geq 2 \) and \( t \geq 0 \). An infinite sequence \( (x_n)_{n \geq 0} \) of points in \([0,1)^s\) is said to be a \((t,s)\)-sequence in base \( b \) if, for all integers \( k \geq 0 \) and \( m > t \), the point set consisting of the \( x_n \) with \( kb^m \leq n < (k+1)b^m \) is a \((t,m,s)\)-net in base \( b \).

In his work [15] Niederreiter presented a comprehensive theory of \((t,m,s)\)-nets and \((t,s)\)-sequences including discrepancy estimates, existence results and connections to other mathematical disciplines such as, e.g., Combinatorics. The fundamental discrepancy estimate for a \((t,m,s)\)-net \( P \) in base \( b \) states that

\[
D_N(P) \leq c_{s,b} b^t \frac{(\log N)^{s-1}}{N} + O_{s,b} \left( b^t \frac{(\log N)^{s-2}}{N} \right)
\]

where \( N = b^m \) and where \( c_{s,b} > 0 \) is independent of \( m \) and \( t \). This estimate justifies the definition of \((t,m,s)\)-nets since it means that for sufficiently small \( t \) one can achieve a star discrepancy of order of magnitude \( O((\log N)^{s-1}/N) \). Many people from discrepancy theory conjecture that this is the best convergence rate at all which can be achieved for the star discrepancy of \( N \)-element point sets in dimension \( s \). For infinite \((t,s)\)-sequences
in base \( b \) one can achieve a star discrepancy of order of magnitude \( O((\log N)^s/N) \) which again is widely believed to be the best rate at all for the star discrepancy of infinite sequences in dimension \( s \).

Most constructions of \((t, m, s)\)-nets and \((t, s)\)-sequences rely on the digital method which was introduced by Niederreiter, also in \([15]\). In the case of \((t, m, s)\)-nets this construction requires \( m \times m \) matrices \( C_1, C_2, \ldots, C_s \) over a commutative ring \( R \) with identity and \( |R| = b \) and, in a simplified form, a bijection \( \psi \) from the set of \( b \)-adic digits \( \mathbb{Z}_b = \{0, 1, \ldots, b - 1\} \) onto \( R \). For \( n = 0, 1, \ldots, b^m - 1 \), let \( n = n_0 + n_1 b + \cdots + n_{m-1} b^{m-1} \) with all \( n_r \in \mathbb{Z}_b \). Then, for \( j = 1, 2, \ldots, s \), multiply the matrix \( C_j \) with the vector \( \mathbf{n} = (\psi(n_0), \psi(n_1), \ldots, \psi(n_{m-1}))^\top \) whose components belong to \( R \),

\[
C_j \mathbf{n} = (y_{n,j,1}, y_{n,j,2}, \ldots, y_{n,j,m})^\top,
\]

and set \( \mathbf{x}_n = (x_{n,1}, x_{n,2}, \ldots, x_{n,s}) \), where

\[
x_{n,j} = \frac{\psi^{-1}(y_{n,j,1})}{b} + \frac{\psi^{-1}(y_{n,j,2})}{b^2} + \cdots + \frac{\psi^{-1}(y_{n,j,m})}{b^m}.
\]

The point set \( \{\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{b^m - 1}\} \) constructed this way is a \( b^m \)-element point set in \([0, 1]^s\) and it is therefore a \((t, m, s)\)-net in base \( b \) for some \( t \in \{0, 1, \ldots, m\} \) which is called a digital \((t, m, s)\)-net over \( R \). In the case of \((t, s)\)-sequences the only difference is that one uses \( \infty \times \infty \) matrices.

The so-called quality parameter \( t \) depends only on the chosen matrices \( C_1, C_2, \ldots, C_s \). Of course \( t \) should be as small as possible, in the optimal case \( t = 0 \). If the base \( b \) is a prime power, then one chooses for \( R \) the finite field \( \mathbb{F}_b \) of order \( b \) which makes life a bit easier and is therefore the most studied case. Then \( t \) is determined by some linear independence property of the row-vectors of the generating matrices \( C_1, C_2, \ldots, C_s \) which provides the link of digital nets and sequences to the theory of finite fields and linear algebra over finite fields.

Niederreiter developed several constructions of generating matrices which lead to good, often even optimal small \( t \)-values. One important construction results in the now so-called \textit{Niederreiter sequences} and is based on polynomial arithmetic over finite fields and the formal Laurent series expansion of certain rational functions over \( \mathbb{F}_b \) whose Laurent coefficients are used to fill the generating matrices. If \( s \leq b \) this leads to an explicit construction of \((0, s)\)-sequences in base \( b \) which in turn implies, for \( s \leq b + 1 \), an explicit construction of a \((0, m, s)\)-net in base \( b \) for every \( m \geq 2 \). It is known that the conditions \( s \leq b \) for sequences and \( s \leq b + 1 \) for nets, respectively, are even necessary to achieve a quality parameter equal to zero. Niederreiter sequences and slight generalizations thereof recover and unify the existing constructions due to Il’ya M. Sobol’ and Henri Faure.

An important subclass of \((t, m, s)\)-nets which was introduced by Niederreiter in the paper “Low-discrepancy point sets obtained by digital constructions over finite fields” \([18]\) is provided by the concept of what we call today \textit{polynomial lattice point sets}. This name has its origin in a close relation to ordinary lattice point sets. In fact, the research on polynomial lattice point sets and on ordinary lattice point sets often follows two parallel tracks and bears a lot of similarities (but there are also differences).

Niederreiter’s early work on \((t, m, s)\)-nets and \((t, s)\)-sequences is well summarized in Chapter 4 of his already mentioned book “Random number generation and quasi-Monte Carlo methods” \([19]\) which appeared in 1992. Since its appearance, this book is \textit{the}
reference book for \((t, m, s)\)-nets and \((t, s)\)-sequences especially and for QMC and random number generation in general.

A disadvantage of Niederreiter sequences in dimension \(s\) is that they can only achieve a \(t\)-value of order \(O(s \log s)\) as \(s\) tends to infinity. This disadvantage was overcome in the next cornerstone of Niederreiter’s work in QMC, the constructions of Niederreiter-Xing sequences. In a series of papers [42, 43, 44, 51, 55] starting in 1995 and based on methods from Algebraic Geometry, Niederreiter developed in collaboration with Chaoping Xing constructions of generating matrices which achieve the currently best known quality parameters of order \(O(s)\) for growing dimensions \(s\). This order is known to be best possible. An introduction into this subject and an overview can be found in the book “Rational points on curves over finite fields” [54] published by Niederreiter and Xing in 2001.

In 2001 Niederreiter developed together with Gottlieb Pirsic [31] a duality theory for digital nets. The basic idea is that the construction of digital \((t, m, s)\)-nets over \(\mathbb{F}_b\) can be reduced to the construction of certain \(\mathbb{F}_b\)-linear subspaces of \(\mathbb{F}_b^{sm}\). Using the standard inner product in \(\mathbb{F}_b^{sm}\) one can define and study the dual linear subspace. If one defines a special weight on \(\mathbb{F}_b^{sm}\), the so-called Niederreiter-Rosenbloom-Tsfasman weight, then the \(t\)-parameter of a digital net is closely related to the weight of the corresponding dual linear subspace. This point of view gives new possibilities for the construction of digital nets, as, for example, cyclic nets or hyperplane nets, and it provides a connection to the theory of linear codes. Later, in 2009, Niederreiter and Josef Dick [1] extended the duality theory for digital nets also to digital sequences which became a convenient framework for the description of many constructions such as, for example, the ones of Niederreiter and Xing or of Niederreiter and Ferruh Özbudak [27, 28] (see also [2]).

Digital nets also have a close connection to other discrete objects such as orthogonal Latin squares or ordered orthogonal arrays. Also these relations were subject of Niederreiter’s research.

Harald Niederreiter’s contributions to the theory of QMC are groundbreaking. He opened new doors and developed comprehensive theories of lattice rules and of \((t, m, s)\)-nets and \((t, s)\)-sequences with many new ideas and facets. Today Niederreiter’s work forms one of the essential pillars of QMC integration.

References
[1] J. Dick and H. Niederreiter: Duality for digital sequences. J. Complexity 25: 406–414, 2009.

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

[3] C. S. Ding, H. Niederreiter and C. P. Xing: Some new codes from algebraic curves, IEEE Trans. IT, 2638–2642, 2000.

[4] J. von zur Gathen and D. Panario: Factoring polynomials over finite fields: a survey. Computational algebra and number theory (Milwaukee, WI, 1996). J. Symbolic Comput. 31: 3–17, 2001.
[5] F.J. Hickernell and H. Niederreiter: The existence of good extensible rank-1 lattices. J. Complexity 19: 286–300, 2003.

[6] L. Kuipers and H. Niederreiter: Uniform Distribution of Sequences. John Wiley, New York, 1974. Reprint, Dover Publications, Mineola, NY, 2006.

[7] G. Larcher and H. Niederreiter: Kronecker-type sequences and non-Archimedean Diophantine approximations. Acta Arith. 63: 379–396, 1993.

[8] G. Larcher and H. Niederreiter: Generalized $(t,s)$-sequences, Kronecker-type sequences, and Diophantine approximations of formal Laurent series. Trans. Amer. Math. Soc. 347: 2051–2073, 1995.

[9] R. Lidl and H. Niederreiter, Finite fields. Second edition. Encyclopedia of Mathematics and its Applications, 20. Cambridge University Press, Cambridge, 1997.

[10] H.B. Mann: The construction of orthogonal Latin squares. Ann. Math. Statist. 13: 418–423, 1942.

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

[12] H. Niederreiter: An application of the Hilbert-Montgomery-Vaughan inequality to the metric theory of uniform distribution mod 1. J. London Math. Soc. 13: 497–506, 1976.

[13] H. Niederreiter: Quasi-Monte Carlo methods and pseudo-random numbers. Bull. Amer. Math. Soc. 84: 957–1041, 1978.

[14] H. Niederreiter: Dyadic fractions with small partial quotients. Monatsh. Math. 101: 309–315, 1986.

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

[16] H. Niederreiter: Rational functions with partial quotients of small degree in their continued fraction expansion. Monatsh. Math. 103: 269–288, 1987.

[17] H. Niederreiter: A short proof for explicit formulas for discrete logarithms in finite fields. Appl. Algebra Engrg. Comm. Comput. 1: 55–57, 1990.

[18] H. Niederreiter: Low-discrepancy point sets obtained by digital constructions over finite fields. Czechoslovak Math. J. 42: 143–166, 1992.

[19] H. Niederreiter: Random Number Generation and Quasi-Monte Carlo Methods. No. 63 in CBMS-NSF Series in Applied Mathematics. SIAM, Philadelphia, 1992.

[20] H. Niederreiter: A new efficient factorization algorithm for polynomials over small finite fields. Appl. Algebra Engrg. Comm. Comput. 4: 81–87, 1993.

[21] H. Niederreiter: Low-discrepancy sequences and non-Archimedean Diophantine approximations. Studia Sci. Math. Hungar. 30: 111–122, 1995.
[22] H. Niederreiter: On the discrepancy of some hybrid sequences. Acta Arith. 138: 373–398, 2009.

[23] H. Niederreiter: A discrepancy bound for hybrid sequences involving digital explicit inversive pseudorandom numbers. Unif. Distrib. Theory 5: 53–63, 2010.

[24] H. Niederreiter: Further discrepancy bounds and an Erdős-Turán-Koksma inequality for hybrid sequences. Monatsh. Math. 161: 193–222, 2010.

[25] H. Niederreiter: Discrepancy bounds for hybrid sequences involving matrix-method pseudorandom vectors. Publ. Math. Debrecen 79: 589–603, 2011.

[26] H. Niederreiter: Improved discrepancy bounds for hybrid sequences involving Halton sequences. Acta Arith. 155: 71–84, 2012.

[27] H. Niederreiter and F. Özbudak: Constructions of digital nets using global function fields. Acta Arith. 105: 279–302, 2002.

[28] H. Niederreiter and F. Özbudak: Matrix-product constructions of digital nets. Finite Fields Appl. 10: 464–479, 2004.

[29] H. Niederreiter and W. Philipp: Berry-Esseen bounds and a theorem of Erdős and Turán on uniform distribution mod 1. Duke Math. J. 40: 633–649, 1973.

[30] H. Niederreiter and F. Pillichshammer: Construction algorithms for good extensible lattice rules. Const. Approx. 30: 361–393, 2009.

[31] H. Niederreiter and G. Pirsic: Duality for digital nets and its applications. Acta Arith. 97: 173–182, 2001.

[32] H. Niederreiter and J. Rivat: On the Gowers norm of pseudorandom binary sequences. Bull. Aust. Math. Soc. 79: 259–271, 2009.

[33] H. Niederreiter and K.H. Robinson: Complete mappings of finite fields. J. Austral. Math. Soc. Ser. A 33: 2, 197–212, 1982.

[34] H. Niederreiter and I.E. Shparlinski: On the distribution and lattice structure of nonlinear congruential pseudorandom numbers. Finite Fields Appl. 5: 246–253, 1999.

[35] H. Niederreiter and I.E. Shparlinski: On the distribution of inversive congruential pseudorandom numbers in parts of the period. Math. Comp. 70: 1569–1574, 2001.

[36] H. Niederreiter and I. Shparlinski: On the distribution of power residues and primitive elements in some nonlinear recurring sequences. Bull. London Math. Soc. 35: 522–528, 2003.

[37] H. Niederreiter and R.F. Tichy: Solution of a problem of Knuth on complete uniform distribution of sequences. Mathematika 32: 26–32, 1985.

[38] H. Niederreiter and R.F. Tichy: Metric theorems on uniform distribution and approximation theory. Journées arithmétiques de Besançon (Besançon, 1985). Astérisque No. 147–148: 319–323, 346, 1987.
[39] H. Niederreiter and A. Winterhof: Incomplete character sums and polynomial interpolation of the discrete logarithm. Finite Fields Appl. 8: 184–192, 2002.

[40] H. Niederreiter and A. Winterhof: Multiplicative character sums for nonlinear recurring sequences. Acta Arith. 111: 299–305, 2004.

[41] H. Niederreiter and A. Winterhof: Exponential sums for nonlinear recurring sequences. Finite Fields Appl. 14: 59–64, 2008.

[42] H. Niederreiter and C.P. Xing: Low-discrepancy sequences obtained from algebraic function fields over finite fields. Acta Arith. 72: 281–298, 1995.

[43] H. Niederreiter and C.P. Xing: Low-discrepancy sequences and global function fields with many rational places. Finite Fields Appl. 2: 241–273, 1996.

[44] H. Niederreiter and C.P. Xing: Quasirandom points and global function fields. In: S. Cohen and H. Niederreiter (eds.), Finite Fields and Applications, volume 233 of London Math. Soc. Lecture Note Series, pages 269–296, Cambridge University Press, Cambridge, 1996.

[45] H. Niederreiter, C.P. Xing: Explicit global function fields over the binary field with many rational places. Acta Arith. 75: 383–396, 1996.

[46] H. Niederreiter, C.P. Xing: Cyclotomic function fields, Hilbert class fields and global function fields with many rational places. Acta Arith. 79: 59–76, 1997.

[47] H. Niederreiter, C.P. Xing: Drinfeld modules of rank 1 and algebraic curves with many rational points II. Acta Arith. 81: 81–100, 1997.

[48] H. Niederreiter, C.P. Xing: Global function fields with many rational places over the ternary field. Acta Arith. 83: 65–86, 1998.

[49] H. Niederreiter, C.P. Xing: Algebraic curves with many rational points over finite fields of characteristic 2. In: Proc. Number Theory Conference (Zakopane 1997), de Gruyter, 1999, Berlin, p. 359–380.

[50] H. Niederreiter, C.P. Xing: A general method of constructing global function fields with many rational places. In: Algorithmic Number Theory (Portland 1998), Lecture Notes in Comp. Science 1423, Springer, Berlin, 1998, p. 555–566.

[51] H. Niederreiter and C.P. Xing: Nets, (t,s)-sequences, and algebraic geometry. In: Random and quasi-random point sets, volume 138 of Lecture Notes in Statist., pages 267–302, Springer, New York, 1998.

[52] H. Niederreiter and C.P. Xing: Towers of global function fields with asymptotically many rational places and an improvement on the Gilbert-Varshamov bound. Math. Nachr. 195: 171–186, 1998.

[53] H. Niederreiter and C.P. Xing: Curve sequences with asymptotically many rational points. In: M.D. Fried (ed.), Applications of Curves over Finite Fields, volume 245 of Contemporary Math., pages 3–14, American Math. Society, Providence, RI, 1999.
[54] H. Niederreiter and C.P. Xing: *Rational Points on Curves over Finite Fields. Theory and Applications*. London Mathematical Society Lecture Note Series 285, Cambridge University Press, Cambridge, 2001.

[55] H. Niederreiter and C.P. Xing: Constructions of digital nets. Acta Arith. 102: 189–197, 2002.

[56] R. Shaheen and A. Winterhof: Permutations of finite fields for check digit systems. Des. Codes Cryptogr. 57: 361–371, 2010.

[57] A. Winterhof, Recent results on recursive nonlinear pseudorandom number generators. Sequences and their applications–SETA 2010, 113–124, Lecture Notes in Comput. Sci., 6338, Springer, Berlin, 2010.

[58] A. Winterhof, Generalizations of complete mappings of finite fields and some applications. J. Symbolic Comput., to appear.

[59] C.P. Xing, H. Niederreiter: Drinfeld modules of rank 1 and algebraic curves with many rational points. Monatsh. Math. 127: 219–241, 1999.