

# A Software Implementation of Niederreiter–Xing Sequences

Gottlieb Pirsic

Institute of Discrete Mathematics, Austrian Academy of Sciences, Sonnenfelsgasse 19, A-1010 Vienna, Austria. E-mail address: gottlieb.pirsic@oeaw.ac.at

**Abstract.** In a series of papers, Niederreiter and Xing introduced new construction methods for low-discrepancy sequences, more specifically  $(t, s)$ -sequences. As these involve the rather abstract theory of algebraic function fields — a special case of algebraic geometry and also closely related to function theory and algebraic number theory — for a long time no computer implementation of this new method was given. In this paper we present our efforts in this direction, address the algorithmical problems and give some numerical data obtained from our implementation.

## 1 Introduction

It is known that the minimal order of discrepancy for the first  $N$  points of an  $s$ -dimensional sequence is at most  $\mathcal{O}((\log N)^s/N)$  as  $N$  increases. Sequences that attain this bound are called low-discrepancy sequences. An especially fruitful construction method using digit expansions leads to so-called digital  $(t, s)$ -sequences constructed over  $\mathbb{F}_b$ , where  $b$  is some prime power. The Sobol', Faure and Niederreiter sequences are examples of increasing generality. Well-known low-discrepancy sequences that are not  $(t, s)$ -sequences are the good lattice-points and the Halton sequence.

All of these have a discrepancy upper bound of  $\mathcal{O}((\log N)^s/N)$  (we refer to star discrepancy throughout this section), but differ in the implied constant of the upper bound, whose asymptotic orders with respect to  $s$  are shown in Table 1. The quantity  $t$  is an integer parameter that describes the distribution

Sequence	Discrepancy bound constant
Good Lattice Points	$2^s$
Halton sequence	$s!$
$(t, s)$ -sequence constr. over $\mathbb{F}_b$	$\frac{b^s b^t}{s!(2 \log b)^s} \approx b^{t(s) - s \log_b s}$

**Table 1.** Comparison of constants

quality of a given  $(t, s)$ -sequence.

It should be noted that in a preprint, Atanassov [1] showed that the constant for the Halton sequence is of the smaller order  $\mathcal{O}((2^s \log s)^{-1})$ .

An important application of low-discrepancy sequences is in the quasi-Monte Carlo method of very high-dimensional numerical integration. Therefore the asymptotic behaviour of the discrepancy upper bound constants with respect to the dimension  $s$  is of interest. The behavior of  $(t, s)$ -sequences depends on the quality parameter  $t$ , which is an increasing function in  $s$ . For the best previously known construction method, the Niederreiter sequences,  $t(s)$  is of the order  $\mathcal{O}(s \log_b s)$ . This has been dramatically improved by Niederreiter and Xing in a series of papers, where they obtain  $t(s) \in \mathcal{O}(s)$  by use of algebraic geometry. The ensuing constant hence is of order  $\mathcal{O}((b/s)^s)$ , which even improves Atanassov's bound for the Halton sequence. For this reason Niederreiter-Xing (NX-)sequences can be considered as the currently optimal low-discrepancy sequences.

Note that not only the low constant implies the practical relevance of NX-sequences, but also the fact that there is a fixed base  $b$  for increasing dimension  $s$ , which is not the case if we employ Faure sequences. For fixed  $b$ , there are better bounds on the integration error of certain function classes (Korobov classes with respect to Walsh functions) and also computer implementation can benefit from a fixed base, especially if  $b$  equals a power of 2.

In the next section we are going to introduce some notions of function field theory that we need to describe the algorithmic issues of a computer implementation in Section 3. Following that, some numerical results are given in Section 4, and a brief outlook to further developments in Section 5.

## 2 Definitions

### 2.1 Function field theory

In the following paragraphs we are going to describe some concepts of algebraic function field theory in a very brief and not altogether rigorous manner. The strict definitions and proofs of the statements can be looked up, e.g. in [2,3] (see also [13]).

An *algebraic function field*  $F/K$  is a finite algebraic extension  $K(x, y)$  of the field of rational functions  $K(x)$ . Here we will always assume that  $K$  is some finite field  $\mathbb{F}_b$ .

In a rational function field (the field of rational functions), a valuation can be defined for each irreducible polynomial (recall that an integer function  $v(\cdot)$  is called a *valuation* iff  $c^{v(\cdot)}$  is a norm for an arbitrary  $c \in (0, 1)$ ): for a rational function  $f \in K(x)$  and an irreducible polynomial  $p \in K[x]$ , the integer  $v_p(f)$  shall be defined as the exponent of  $p$  in the unique factorization of  $f$  into integer powers of irreducible polynomials (as special case,  $v_p(0) := \infty$ ). Then the function  $v_p$  is a valuation of  $K(x)$ . Apart from the  $v_p$ , only one further valuation exists, namely  $v_\infty(f) := \deg(f_{\text{den}}) - \deg(f_{\text{num}})$ , where  $f_{\text{num}}/f_{\text{den}}$  is the unique representation of  $f$  as a fraction of coprime polynomials.

In an algebraic function field, for each valuation  $v_p$  of  $K(x)$  (also for  $v_\infty$ ) there are only finitely many extensions  $v_{P_1}, \dots, v_{P_r}$  to  $F/K$ , where an *extension*  $v_{P_i}$  of a valuation  $v_p$  is a valuation of  $F$  such that  $v_{P_i}(f) = e_i \cdot v_p(f)$  for all  $f \in K(x)$  (for some positive integer  $e_i$ ). Set  $v_P = v_{P_i}$  for some  $i$ . Note that  $O_P := \{f \in F : v_P(f) \geq 0\}$  is a subring of  $F$  and that  $P := \{f \in F : v_P(f) > 0\}$ , called a *place of  $F$* , is a maximal ideal of  $O_P$ . So  $O_P/P$  is a field, in fact it is a finite extension of the field  $K[x]/(p(x)) \cong \mathbb{F}_b^{\deg(p)}$ . The degree over the field  $K = \mathbb{F}_b$  of this extension,  $[O_P/P : \mathbb{F}_b] =: \deg P$ , is called the *degree of the place  $P$* . Note that places  $P$  of degree one can only come from linear polynomials  $p$  (or  $v_\infty$ , which is a special case).

In  $K(x)$ , for each nonzero rational function  $f$  there are only finitely many irreducible polynomials  $p$  such that  $v_p(f) \neq 0$ . The same is true in  $F$ : for nonzero  $f \in F$ , the following formal sum over all places  $P$ ,  $\sum_P v_P(f)P =: (f)$ , called a *canonical divisor*, is a finite sum. Any general formal sum over all places,  $D = \sum_P v_P(D)P$ , where almost all integers  $v_P(D)$  are 0, is simply called a *divisor*. The degree function on places is extended to divisors by linearity:  $\deg D := \sum_P v_P(D) \deg(P)$ .

For any divisor  $D$ , we define a set  $\mathcal{L}(D)$  by

$$\mathcal{L}(D) := \{f \in F^* : v_P(f) + v_P(D) \geq 0, \text{ for all places } P\} \cup \{0\}$$

(An analogy of this set in function theory would be the set of all meromorphic functions that are holomorphic outside finitely many specified points on the Riemann sphere and whose pole orders at these places are not to exceed prescribed bounds.) It can be shown that  $\mathcal{L}(D)$  is a finite-dimensional vector space over  $\mathbb{F}_b$ . We denote its dimension by  $\dim D$  (abbreviated for  $\dim_{\mathbb{F}_b} \mathcal{L}(D)$ ). In fact, the dimension  $\dim D$  of a divisor  $D$  is always at most  $1 + \deg D$ , for all  $D$  with  $\deg D \geq 0$ . But also  $\deg D + 1 - \dim D$  is at most some integer  $g \geq 0$  that depends on the extension  $F/K$ . This quantity  $g = g(F)$  is called the *genus of  $F$* .

Finally, the concept of Laurent series expansions of rational functions also extends to algebraic functions. For any place  $P$  of degree one,  $z \in F$  such that  $v_P(z) = 1$  and an arbitrary nonzero function  $f \in F$ , there are  $a_i \in K$  such that

$$v_P \left( f - \sum_{i=v_P(f)}^m a_i z^i \right) > m,$$

for any  $m \in \mathbb{Z}$ . Such an expansion is called a *local expansion at  $P$  with the local parameter  $z$* .

## 2.2 The construction

Now we are ready to give the description of NX-sequences, which is based on the construction given in [4]. The only difference is that we fix parameters

that were left free to choice in the original paper, i.e. we consider a special case.

Consider a function field  $F/\mathbb{F}_b$  with genus  $g$  and at least  $s + 1$  places of degree one, call them  $P_\infty, P_1, \dots, P_s$ . In the implementation, we choose the distinguished place  $P_\infty$  among those that come from the polynomial  $p(x) = x \in K(x)$ . Define the divisor  $D := 2g(F)P_1$ , i.e. set  $v_{P_1}(D) = 2g$  and  $v_P(D) = 0$  for all other places  $P$ .

We state some more facts about the dimension of divisors: the dimension of divisors of negative degree is zero and the zero divisor  $0$  (where  $v_P(0) = 0$  for all  $P$ ) has dimension 1. Considering divisors of higher degree, the following holds: for any divisor  $D'$  and a place  $P'$  of degree one the dimension  $\dim(D' + P')$  is at most  $\dim(D') + 1$ . Finally, for divisors  $D'$  of degree at least  $2g - 1$  the dimension equals  $\deg D' + 1 - g$ . (The last statement is a consequence of the Riemann-Roch theorem, a central theorem in this theory.)

Consequently,  $\dim D = \dim(2gP_1) = g + 1$  and  $\dim(D - (2g + 1)P_\infty) = 0$ . Since the dimension of  $2gP_1 - kP_\infty$  increases at most by one as  $k$  decreases, there exist integers  $n_0 = 0 < n_1 < \dots < n_g \leq 2g$  such that  $\mathcal{L}(2gP_1 - n_iP_\infty) \setminus \mathcal{L}(2gP_1 - (n_i + 1)P_\infty)$  is not empty for  $i = 0, \dots, g$ . If we choose  $w_i$  in this set (note that this implies  $v_{P_\infty}(w_i) = n_i$ ), then the set  $\{w_0, \dots, w_g\}$  is a basis of  $\mathcal{L}(D)$ . Additionally, for each  $i = 1, \dots, s$ , and  $m \in \mathbb{N}$ , there is a basis  $\{w_0, \dots, w_g, k_1^{(i)}, \dots, k_m^{(i)}\}$  of  $\mathcal{L}(D + mP_i)$ .

We now consider slightly modified local expansions of the  $k_j^{(i)}$  at  $P_\infty$ . Let  $a_{i,j,n} \in \mathbb{F}_b$  be such that

$$v_{P_\infty} \left( k_j^{(i)} - \sum_{n=v_{P_\infty}(k_j^{(i)})}^m a_{i,j,n} z_n \right) > m,$$

for every  $m \in \mathbb{Z}$  where, if  $z \in F$  is a given local parameter (i.e.  $v_{P_\infty}(z) = 1$ ), the  $z_n$  are defined by  $z_{n_h} := w_h$  for  $h = 0, \dots, g$ , and  $z_n := z^n$  else. Note that  $v_{P_\infty}(k_j^{(i)}) \geq 0$  since  $k_j^{(i)} \in \mathcal{L}(2gP_1 + jP_i)$ , so we can assume that the above sum always starts from  $n = 0$ .

Define matrices  $C_1, \dots, C_s \in \mathbb{F}_b^{\infty \times \infty}$  by

$$C_i = (c_{i,j,n})_{j>0, n \geq 0} := (a_{i,j,n})_{j>0, n \in \mathbb{N}_0 \setminus \{n_0, \dots, n_g\}}, \quad i = 1, \dots, s.$$

Using these as generating matrices for a digital  $(t, m, s)$ -net by [4] we get a  $(g, m, s)$ -net.

### 3 Algorithmic issues

Due to the rather abstract algebraic nature of the described construction, there are several points where it is not obvious how to perform the actual calculations. In fact, some of the arising problems still are research topics. In the following we present our approaches to these problems.

### 3.1 Local expansion

The calculation of the local expansion is an operation that is performed very often, once for each row of each matrix, so it is essential that a sufficiently fast algorithm is used.

Let  $\varphi \in \mathbb{F}_b[x, y]$ ,  $\deg_y \varphi = n$ , and let  $\varphi(x, y) = 0$  be the defining equation of the function field  $F = \mathbb{F}_b(x, y)$ . Since  $F$  is a finite algebraic extension of degree (at most)  $n$  of the rational function field, any  $f \in F$  can be represented as  $f = f_0 + \cdots + f_{n-1}y^{n-1}$ ,  $f_i \in \mathbb{F}_b(x)$ . Let  $z$  be a local parameter at  $P_\infty$ . Then  $F$  can be embedded in the field of Laurent series in  $z$ . (In fact, by simple transformations of the function field, we can in most cases achieve  $z = x$  which simplifies the function field arithmetic basically to polynomial arithmetic over  $\mathbb{F}_b$ .) Therefore it suffices to know the local expansion of  $y$ . From that, we can obtain the expansions of the powers of  $y$ . Any further arbitrary expansion is then simply a linear combination of these in  $\mathbb{F}_b(x)$ .

To now actually find the local expansion of  $y$ , we apply a variant of Newton iteration, which also in the function field case is of quadratic convergence.

### 3.2 $\mathcal{L}$ -space basis calculation

The task of finding basis functions for the vector spaces  $\mathcal{L}(D + kP_i)$  is the most difficult part in the implementation. There exist algorithms for finding them, as for instance implemented in the computer algebra systems Magma or KASH (see e.g. [8,9]), but for our purposes they are a bit too general to be of practical use. Also we would require that the basis for  $\mathcal{L}(D + mP_i)$  is such that a subset of the basis gives a basis for  $\mathcal{L}(D + m'P_i)$  for any  $0 \leq m' \leq m$  (since we need the functions  $k_j^{(i)}$ ), but those algorithms generally do not provide such ‘ascending’ bases.

A small help in this task is the fact that we do not need to calculate new bases for any new  $m$ , but only need the bases for two specific vector spaces by the following simple but effective lemma. (This lemma can be stated in a more general way.)

**Lemma 1.** *Let  $F/\mathbb{F}_b$  be an algebraic function field and  $P, Q, P \neq Q$  be places of degree one of  $F$ . Let  $n_P$  be the smallest number such that  $\dim(n_P P) = 2$  and let  $\{1, \tau\}$  be a basis of  $\mathcal{L}(n_P P)$ . Further let  $\{w_0, \dots, w_g, k_1, \dots, k_{n_P}\}$  be a basis of  $\mathcal{L}(2gQ + n_P P)$ , where  $v_P(k_i) = -i$ . Then an ‘ascending basis’ in the above sense for  $\mathcal{L}(2gQ + mP)$  for any  $m \geq n_P$  is given by*

$$\mathcal{B} := \{w_0, \dots, w_g, \tau^0 k_1, \dots, \tau^0 k_{n_P}, \tau^1 k_1, \dots, \tau^1 k_{n_P}, \dots, \tau^u k_v\},$$

where  $u, v$  are chosen such that  $\mathcal{B}$  has  $g + m + 1$  elements.

*Proof.* For the valuation at  $P$  note that  $v_P(\tau) = -n_P$ , so  $v_P(\tau^i k_j) = -(in_P + j)$ , i.e. the  $\tau^i k_j \in \mathcal{B}$  attain the distinct valuations  $-1, \dots, -m$  at  $P$ . At the place  $Q$  we have  $v_Q(\tau) \geq 0$ , so  $v_Q(\tau^i k_j) \geq -2g$ . At all other places  $P'$  the

valuations stay nonnegative. This shows that  $\mathcal{B}$  is a linearly independent subset of  $g + m + 1$  vectors of  $\mathcal{L}(2gQ + mP)$ . By the Theorem of Riemann-Roch the dimension of  $2gQ + mP$  is also  $g + m + 1$ , so  $\mathcal{B}$  is in fact a basis of  $2gQ + mP$  and everything is proven.

By this lemma we can precompute the two necessary bases and keep the data in a library for reference without the need to compute the bases during runtime.

Another approach is to use function fields, where the  $\mathcal{L}$ -spaces can be found easily and given in a nice form. We use Hermitian function fields, which are function fields over  $\mathbb{F}_{q^2}$  with the defining equation  $y^q + y = x^{q+1}$ . In this paper, however, we restrict ourselves to the binary case (i.e. function fields over  $\mathbb{F}_2$ ) where there is no Hermitian function field available.

### 3.3 Finding appropriate function fields

In the original construction, also places of higher degree than one can be used. However, the error bounds seem to imply that to increase the dimension  $s$  (i.e. to get more matrices) it is preferable to allow a larger genus  $g$  and only use degree one places. So it is necessary to have an extensive table of algebraic function fields with many rational places and a low genus.

A lot of research in this area of looking for such function fields is motivated by coding theory, since there exist very good constructions of linear codes (algebraic Goppa codes, XNL codes) that use function fields as well (see [3], [13, Ch.6]).

In [5] an explicit list of optimal binary function fields is given. We used this list as an input for the implementation.

While this is feasible for low dimensions, where for given  $s$  the optimal choice of function field can be given, in higher dimensions we may employ function fields that are very good but not necessarily optimal with respect to the number of places of degree one in relation to the genus  $g$ . Also we may make use of propagation rules, especially the projection to a lower dimension.

## 4 Results

Implementations were done in the computer algebra system KASH [6] as well as in C++ (using the number theoretic library NTL [7]). Source codes for the programs will be made available at

<http://www.dismat.oeaw.ac.at/pirs/niedxing.html>.

So far only base 2 sequences are available, in dimensions 4 to 16. (In the meantime, this range will have been extended, please refer to above web page for the latest changes.)

The exact quality parameters  $t$  of the resulting matrices were calculated using the program `tcalc` by Schmid and the author [10].

```

m:\ s: 4 5 6 7 8 9 10 11 12 13 14 15 16
-----
1 : 1 1 1 1 1 1 1 1 1 1 1 1 1
2 : 1 1 1 1 1 2 2 2 2 2 2 2 2
3 : 1 1 2 2 2 2 2 2 2 2 2 2 3
4 : 1 2 2 2 2 2 3 3 3 3 3 3 3
5 : 1 2 2 3 3 3 3 4 4 4 4 4 4
6 : 1 2 2 3 3 3 3 4 4 4 4 4 4
7 : 1 2 3 4 4 4 4 5 5 5 5 5 5
8 : 1 2 3 4 4 5 5 5 5 5 5 6 6
9 : 1 2 3 4 4 5 5 6 6 6 6 6 6
10 : 1 2 3 4 4 5 6 6 7 7 7 7 7
11 : 1 2 3 4 5 6 6 6 7 7 7 8 8
12 : 1 2 3 4 5 6 7 7 8 8 8 8 8
13 : 1 2 3 4 5 6 7 8 8 8 8 8 8
14 : 1 2 3 4 5 6 7 8 9 9 9 9 9
15 : 1 2 3 4 5 6 8 8 10 10 10 10
16 : 1 2 3 4 5 6 8 8 10 10 10 10
17 : 1 2 3 4 5 6 8 9 10 10 10 10
18 : 1 2 3 4 5 6 8 9 11 11 11 11
19 : 1 2 3 4 5 6 8 9 11 11 11 11
20 : 1 2 3 4 5 6 8 9 11 11 12 12
21 : 1 2 3 4 5 6 8 9 11 11 13 13
22 : 1 2 3 4 5 6 8 9 12 12 13 13
23 : 1 2 3 4 5 6 8 9 12 12 13 13
24 : 1 2 3 4 5 6 8 9 12 12 13 13
25 : 1 2 3 4 5 6 8 9 12 12 14 14
26 : 1 2 3 4 5 6 8 9 12 12 14 14
27 : 1 2 3 4 5 6 8 9 12 12 14 14
28 : 1 2 3 4 5 6 8 9 12 12 14 14
29 : 1 2 3 4 5 6 8 9 12 12 15 15
30 : 1 2 3 4 5 6 8 9 12 12 15 16

```

For the dimensions  $s = 4, 5, 6, 7, 8, 9, 10, 11, 14, 16$  we used Examples 1, 2, 3A, 4A, 5A, 6, 8, 9A, 12, and 15 in [5].

In dimensions  $s = 12, 13, 15$  we started from the next higher dimension and used a projection to the first  $s$  coordinates. Further propagation rules have been applied.

The predicted  $t$ -values for each dimension (also using the above projections) are:

```

s: 4 5 6 7 8 9 10 11 12 13 14 15 16
-----
t: 1 2 3 4 5 6 8 9 13 13 13 16 16

```

Using optimal function fields for each dimension gives the following upper bounds (by [5] and [13], Table 4.5.1):

```

s: 4 5 6 7 8 9 10 11 12 13 14 15 16
-----
t: 1 2 3 4 5 6 8 9 10 11 13 15 15

```

We also made some numerical integration experiments, using the Genz test function package [11,12]. We present here the relative errors of numerical integration performed with  $2^{21}$  points. The compared point sets were random, Halton, Niederreiter, and Niederreiter-Xing sequences as well as randomized versions of the last two. The selected functions belong to the function classes named Oscillatory, Product Peak, Corner Peak, Gaussian, Continuous and Discontinuous. In the figures, the relative errors of the random and Halton sequence are not included for the sake of clearer presentation.

We also performed experiments using  $2^{15}$  and  $2^{18}$  points, which showed the same behaviour. The complete numerical data can be obtained at <http://www.dismat.oeaw.ac.at/pirs/netintlog.html>.

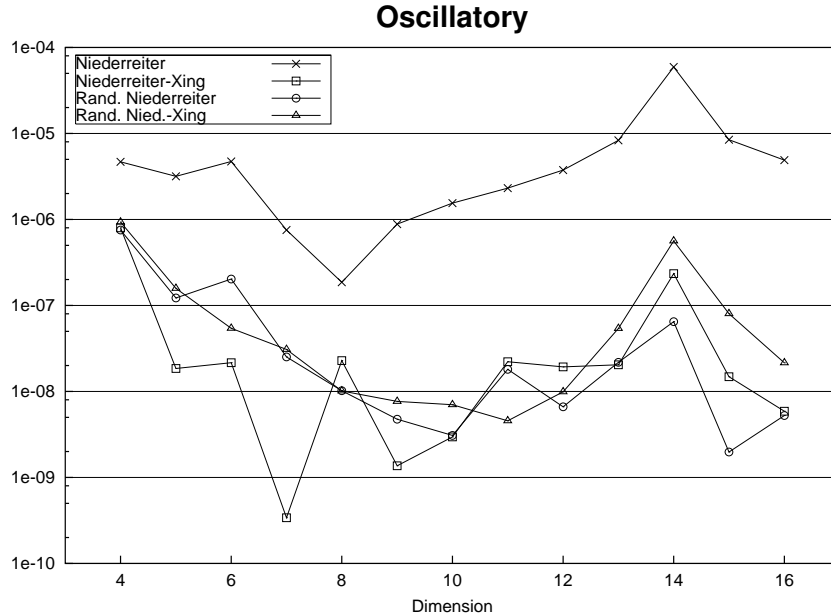


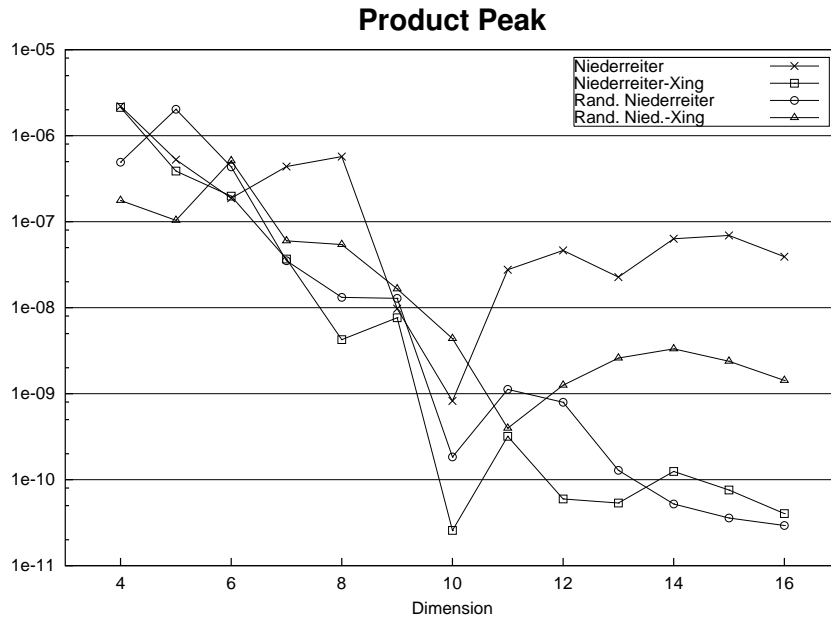
Fig. 1. Relative errors of numerical integration of strongly oscillatory functions

The general trend that can be observed in the figures is that Niederreiter-Xing sequences perform significantly better than Niederreiter sequences and at least as good as randomized Niederreiter sequences. Randomized Niederreiter-Xing sequences, however, generally seem to perform worse than non-randomized ones.

## 5 Outlook

A first attempt at a computer implementation has been made, but much remains yet to be done. The next goal is to extend the range of dimensions  $s$  and to optimize the quality parameters for small dimensions. An extension to function fields with characteristic larger than two is not hard to do and will also follow shortly.

Also, we plan to do further numerical experiments. For instance, we conjecture that the microstructure of the Niederreiter-Xing nets, i.e. the point distribution in intervals smaller than  $b^{t-m}$  of nets obtained from the sequence, is better than in usual nets. This might perhaps even imply qualitatively

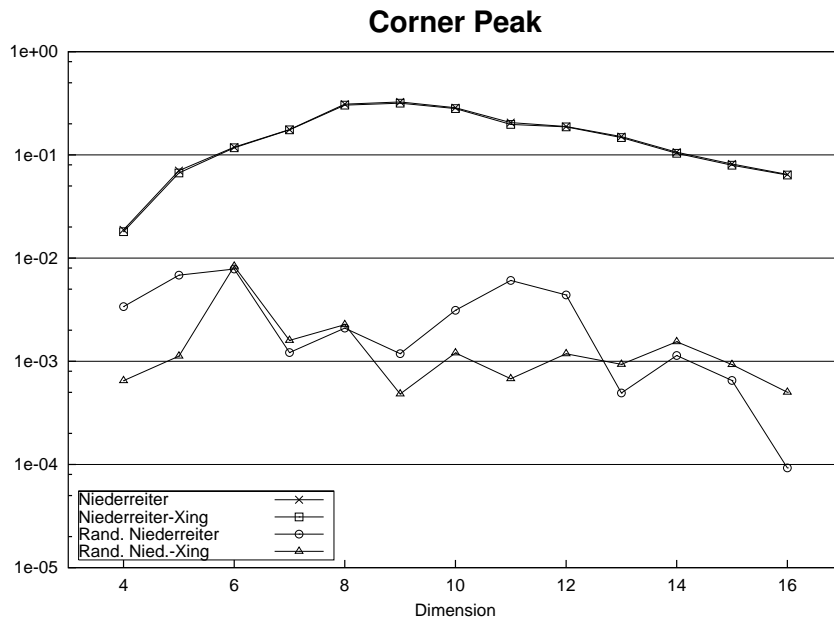


**Fig. 2.** Relative errors of numerical integration of functions with a peak inside the unit cube

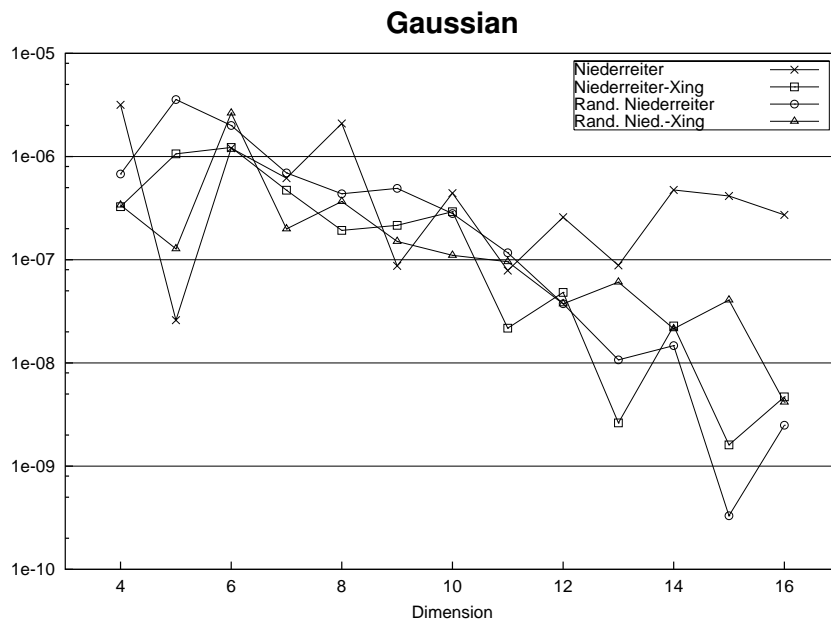
better discrepancy bounds for NX-nets, though it is not yet clear, how this intuitive implication may be put into the form of a proof.

## 6 Acknowledgments

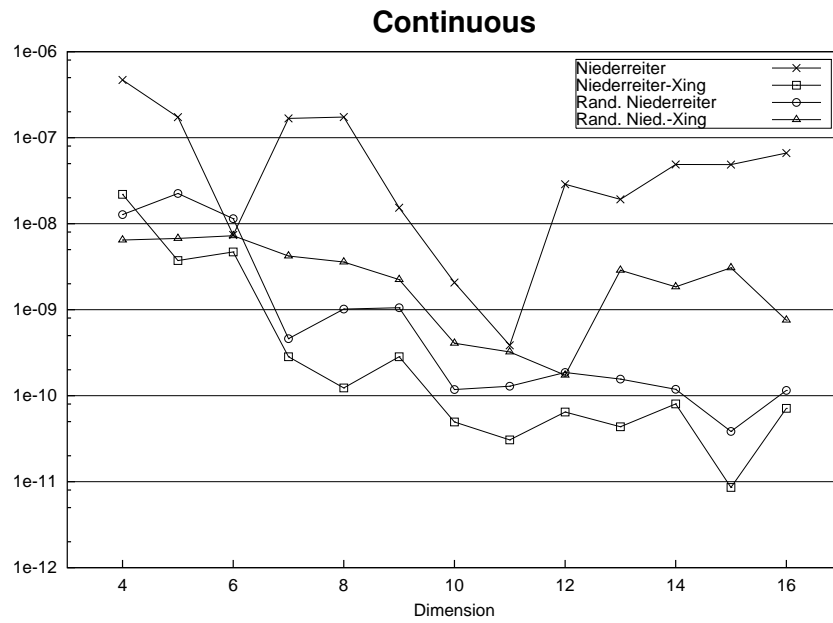
We would like to thank the following persons for their assistance and contributions: Florian Heß (formerly at the KASH group around Prof. Pohst at the TU Berlin), Rudi Schürer (OeNB project 6788) for help with the numerical experiments and Hiren Maharaj, Harald Niederreiter, and Wolfgang Ch. Schmid for support, advice and discussion.



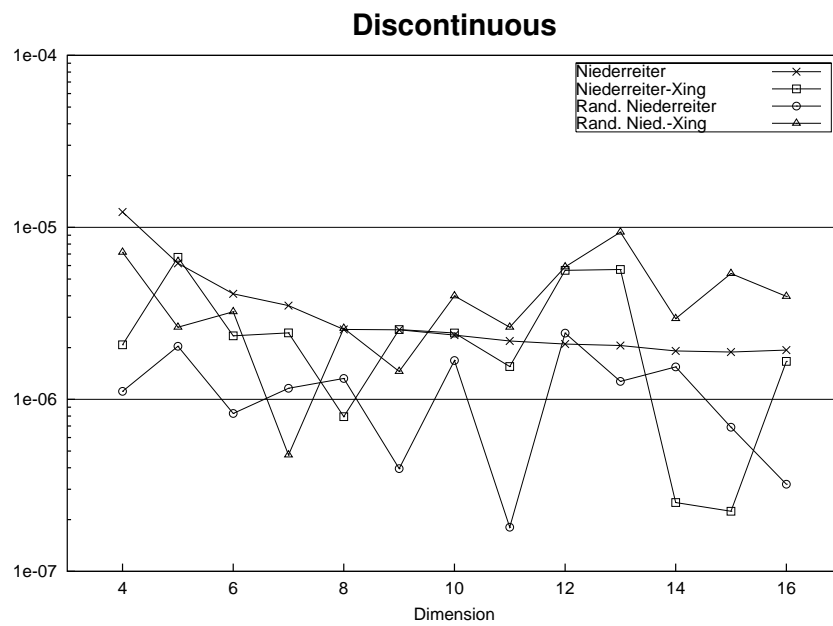
**Fig. 3.** Relative errors of numerical integration of functions with a singularity in a corner of the unit cube



**Fig. 4.** Relative errors of numerical integration of smooth Gaussian (distribution) functions



**Fig. 5.** Relative errors of numerical integration of continuous non-differentiable functions



**Fig. 6.** Relative errors of numerical integration of discontinuous functions

## References

1. Atanassov E.I. (1999) On the discrepancy of the Halton sequences. Preprint, Bulgarian Academy of Sciences, Sofia.
2. Van der Waerden B.L. (1991) Algebra, Volume II, 5th edn. Springer, New York
3. Stichtenoth H. (1993) Algebraic Function Fields and Codes. Springer, Berlin
4. Xing C., Niederreiter H. (1995) A construction of low-discrepancy sequences using global function fields. *Acta Arith.* **73**:87–102
5. Niederreiter H., Xing C. (1996) Explicit global function fields over the binary field with many rational places. *Acta Arith.* **75**:383–396
6. Daberkow M., Fieker C., Klüners J., Pohst M., Roegner K., Schörmig K. and Wildanger K. (1997) KANT V4. *Symbolic Comp.* **24**:267-283.
7. Shoup V. (2001) NTL: A Library for doing Number Theory (version 5.0a). Web site, <http://www.shoup.net/ntl>
8. Heß F. (1999) Zur Divisorenklassengruppenberechnung in globalen Funktionenkörpern [German]. PhD Thesis, TU Berlin, Berlin
9. Schörmig M. (1996) Untersuchungen konstruktiver Probleme in globalen Funktionenkörpern [German]. PhD Thesis, TU Berlin, Berlin
10. Pirsic G., Schmid W.Ch. (2001) Calculation of the quality parameter of digital nets and application to their construction. *Journal of Complexity*, to appear
11. Genz A.C. (1984) Testing multidimensional integration subroutines. In: Ford B., Rault J.C., Thomasset F. (eds) *Tools, Methods and Languages for Scientific Engineering Computation*. North Holland, Amsterdam, 81–94
12. Genz A.C. (1987) A package for testing multiple integration subroutines. In: Keast P., Fairweather G. (eds) *Numerical Integration: Recent Developments, Software and Applications*. D. Reidel, Dordrecht, 337–340
13. Niederreiter H., Xing C.P. (2001) *Rational Points on Curves over Finite Fields: Theory and Applications*. Cambridge Univ. Press, Cambridge