AAECC **13**, 499–508 (2003)

AAECC
Applicable Algebra in
Engineering, Communication
and Computing

Lattice Structure and Linear Complexity Profile of Nonlinear Pseudorandom Number Generators

Gerhard Dorfer[1,2], **Arne Winterhof**[2,3]

[1] Department of Algebra and Computational Mathematics, Vienna University of Technology, Wiedner Hauptstr. 8–10/118, 1040 Vienna, Austria
(e-mail: g.dorfer@tuwien.ac.at)
[2] Institute of Discrete Mathematics, Austrian Academy of Sciences, Fleischmarkt 20–22/2, 1010 Vienna, Austria
(e-mail: gerhard.dorfer@oeaw.ac.at, arne.winterhof@oeaw.ac.at)
[3] Temasek Laboratories, National University of Singapore, 10 Kent Ridge Crescent, Singapore 119260, Republic of Singapore (e-mail: tslwa@nus.edu.sg)

Received: October 4, 2002; revised version: January 10, 2003

Abstract. We extend a generalized version of Marsaglia's lattice test for sequences over finite fields to segments of sequences over an arbitrary field and show that linear complexity profile and this lattice test provide essentially equivalent quality measures for randomness.

Keywords: Pseudorandom number generator, Nonlinear method, Linear complexity profile, Marsaglia's lattice test.

1 Introduction

Nonlinear methods for pseudorandom number generation provide an attractive alternative to linear methods (see the surveys in [5], [14, Chapter 8], [15], and [18]). Initially, nonlinear pseudorandom numbers were defined as periodic sequences over finite prime fields $\mathbb{F}_p$. More recently, nonlinear methods over arbitrary finite fields $\mathbb{F}_q$ were introduced (see e. g. [6], [10], and [19]). The present paper deals with not necessarily periodic sequences (η_n) over an arbitrary field $\mathbb{K}$. However, finite fields are a natural area of applications.

There is no formal definition for a good pseudorandom number generator, but there are certain characteristic features that we have in mind when we talk about such a generator. In particular, we do not want to have an imbedded low dimensional lattice structure, we require good equidistribution properties and statistical independence of successive pseudorandom numbers. The present paper deals with criteria for a desirable lattice structure. For earlier work on lattice tests we refer to the surveys [15] and [3].

For given $s \geq 1$ and $N \geq 2$ we say that (η_n) passes the *s-dimensional N-lattice test* if the vectors $\{\underline{\eta}_n - \underline{\eta}_0 \mid 1 \leq n \leq N-s\}$ span $\mathbb{K}^s$, where

$$\underline{\eta}_n = (\eta_n, \eta_{n+1}, \ldots, \eta_{n+s-1}), \quad 0 \leq n \leq N-s.$$

If (η_n) passes the s-dimensional N-lattice test then it passes all s'-dimensional N-lattice tests for $s' \leq s$ and if (η_n) fails the s-dimensional N-lattice test then it fails all s'-dimensional N-lattice tests for $s' \geq s$. The greatest s such that (η_n) satisfies the s-dimensional N-lattice test is denoted by $S((\eta_n), N)$. Moreover, we put

$$S(\eta_n) = \sup_{N \geq 2} S((\eta_n), N).$$

The s-dimensional lattice test investigated in [21] is passed if and only if $s \leq S(\eta_n)$. A slightly different lattice test for $\mathbb{K} = \mathbb{F}_q$ has been introduced in [20]. For congruential generators modulo a prime p, both lattice tests coincide and this test was proposed by Marsaglia [11].

For $N \geq 2$ the linear complexity profile $L((\eta_n), N)$ is the least order L of a linear recurrence relation over $\mathbb{K}$

$$\eta_{n+L} = \alpha_0 \eta_n + \alpha_1 \eta_{n+1} + \ldots + \alpha_{L-1} \eta_{n+L-1}, \quad 0 \leq n \leq N-L-1, \quad (1)$$

which is satisfied by the first N terms of (η_n) (with the additional convention that $L((\eta_n), N) = 0$ if the first N terms of (η_n) are all 0 and $L((\eta_n), N) = N$ if the first $N-1$ terms are 0 and the Nth term of (η_n) is nonzero). The linear complexity $L(\eta_n)$ is defined as

$$L(\eta_n) = \sup_{N \geq 2} L((\eta_n), N).$$

The linear complexity and the linear complexity profile are important cryptographic characteristics of sequences (see the surveys in [2], [7], [9], [13], [16], and [23]). A low linear complexity of a generator has turned out to be undesirable for more traditional applications in Monte Carlo methods as well (see the surveys in [5], [14], [15], [17], and [18]). The main result of [21] proposes the following relation between linear complexity and lattice test. If $\mathbb{K} = \mathbb{F}_q$ is a finite field and (η_n) is periodic with period q then

$$S(\eta_n) = L(\eta_n) - 1.$$

For finite prime fields this result is a combination of [4] and [1, Theorem 8]. For the general case

$$S(\eta_n) = L(\eta_n) - 1 \quad \text{or} \quad S(\eta_n) = L(\eta_n)$$

holds true.

In the following when investigating the relationship between $L((\eta_n), N)$ and $S((\eta_n), N)$ the considered sequence is arbitrary and it is not necessary to stress (η_n) in the notation. Therefore henceforth we write $L(N)$ and $S(N)$ instead of $L((\eta_n), N)$ and $S((\eta_n), N)$ respectively.

As the main result of this paper we prove the following sharp relation between lattice test and linear complexity profile for arbitrary sequences.

Theorem 1 *We have either*

$$S(N) = \min(L(N), N + 1 - L(N))$$

or

$$S(N) = \min(L(N), N + 1 - L(N)) - 1.$$

After some preliminary results in Section 2 we prove Theorem 1 in Section 3 and give an example which shows that all four possibilities in Theorem 1 can occur.

2 Basic Results

The following proposition (cf. [8,Theorem 6.7.4], [12], or [22]) describes the step-growth of the linear complexity profile.

Proposition 2 (i) *If $L(N) > N/2$ then*

$$L(N + 1) = L(N).$$

(ii) *If $L(N) \le N/2$, then*

$$L(N + 1) = L(N)$$

or

$$L(N + 1) = N + 1 - L(N).$$

We add a result which will play an important role in our considerations.

Lemma 3 *In case $L(N) \le N/2$ there is a unique linear recurrence relation of least order satisfied by the first N terms of (η_n), i. e., for $L = L(N)$ the coefficients $\alpha_0, \dots, \alpha_{L-1}$ on the right hand side of* (1) *are uniquely defined.*

Even though this fact is well known we give a short proof. The method used here will be applied in several other instances.

Proof. Put $L := L(N)$. Assume there are two different recurrence relations of the form (1) satisfied by the first N terms of (η_n) with coefficients $\alpha_0, \dots, \alpha_{L-1}$ and $\beta_0, \dots, \beta_{L-1}$, respectively, and put

$$k := \max\{i \mid \alpha_i \neq \beta_i\},$$

so that $0 \leq k \leq L-1$. Comparing the right hand sides in (1) we obtain

$$(\alpha_0 - \beta_0)\eta_n + \ldots + (\alpha_k - \beta_k)\eta_{n+k} = 0, \quad 0 \leq n \leq N-L-1.$$

Since $\alpha_k - \beta_k \neq 0$ this is a linear recurrence relation of order k for the first $N-(L-k)$ terms of (η_n) and hence

$$L(N-(L-k)) \leq k. \tag{2}$$

As a consequence $L(N-(L-k)) < L(N)$ and thus there is a smallest positive index $j \leq L-k$ with $L(N-(L-k)+j) > L(N-(L-k))$. Applying (ii) of Proposition 2 we get

$$L(N-(L-k)+j) = N-(L-k)+j-L(N-(L-k)).$$

Using (2) and the condition $L \leq N/2$ we arrive at

$$L(N-(L-k)+j) \geq N-L+j \geq \frac{N}{2}+j.$$

However, since $N-(L-k)+j \leq N$, we obtain $L(N) = L \geq N/2+j$ contradicting $L \leq N/2$. □

Next we list some properties of the N-lattice test which will be useful in the following.

Proposition 4 (i) $S(N) \leq S(N+1) \leq S(N)+1$.
(ii) $S(N) \leq N/2$.

Proof. (i) If for some positive integer s the s-dimensional vectors $\underline{\eta}_n - \underline{\eta}_0$, $n = 1, \ldots, N-s$, span $\mathbb{K}^s$, then this remains true if we add the vector $\underline{\eta}_{N+1-s} - \underline{\eta}_0$. Thus the first relation of the assertion is clear.

To prove the second inequality put $S := S(N+1)$. The rank of the matrix

$$\begin{pmatrix} \eta_1 - \eta_0 & \cdots & \eta_{N+1-S} - \eta_0 \\ \vdots & & \vdots \\ \eta_S - \eta_{S-1} & \cdots & \eta_N - \eta_{S-1} \end{pmatrix}$$

equals S, so the S rows of this matrix are linearly independent. Consequently also the first $S-1$ rows are linearly independent which shows $S(N) \geq S-1 = S(N+1)-1$ and we are done.

(ii) If $N-s$ vectors span $\mathbb{K}^s$ then $N-s \geq s$. Thus $S(N) \leq N/2$. □

3 N-Lattice Test and Linear Complexity Profile

We start out to compare $S(N)$ with $L(N)$. Firstly, some upper bounds for the N-lattice test in terms of the linear complexity profile are given.

Proposition 5 *We have*

$$S(N) \leq L(N).$$

Proof. Put $L = L(N)$. We may assume $L \leq N/2$ since otherwise the assertion is trivial. Let $\alpha_0, \dots, \alpha_{L-1} \in \mathbb{K}$ such that

$$\eta_{n+L} = \alpha_0\eta_n + \alpha_1\eta_{n+1} + \dots + \alpha_{L-1}\eta_{n+L-1}, \tag{3}$$

$0 \leq n \leq N - L - 1$. We show that (η_n) fails the $(L+1)$-dimensional N-lattice test. For $\underline{\eta}_n = (\eta_n, \dots, \eta_{n+L})$, $n = 0, \dots, N - L - 1$, by (3) we have that $\underline{\alpha} := (\alpha_0, \dots, \alpha_{L-1}, -1) \perp \underline{\eta}_n$ with respect to the standard inner product in $\mathbb{K}^{L+1}$, and hence $\underline{\alpha} \perp (\underline{\eta}_n - \underline{\eta}_0)$, $n = 1, \dots, N - L - 1$. Since $\underline{\alpha} \neq \underline{0}$ we infer that the linear hull of $\{\underline{\eta}_n - \underline{\eta}_0 \mid 1 \leq n \leq N - L - 1\}$ is not $\mathbb{K}^{L+1}$. This completes the proof. □

The following provides a simple characterization when equality holds in Proposition 5.

Proposition 6 *If $L := L(N) \leq N/2$ and*

$$\eta_{n+L} = \alpha_0\eta_n + \alpha_1\eta_{n+1} + \dots + \alpha_{L-1}\eta_{n+L-1}, \quad 0 \leq n \leq N - L - 1, \tag{4}$$

is the linear recurrence relation of least order satisfied by the first N terms of (η_n), then

$$S(N) < L(N)$$

if and only if

$$\alpha_0 + \alpha_1 + \dots + \alpha_{L-1} = 1.$$

Proof. We show the sufficiency of the condition $\alpha_0 + \alpha_1 + \dots + \alpha_{L-1} = 1$. By adding

$$\alpha_0\eta_{n+1} + (\alpha_0 + \alpha_1)\eta_{n+2} + \dots + (\alpha_0 + \dots + \alpha_{L-2})\eta_{n+L-1}$$

on both sides of (4) we obtain

$$\begin{aligned} &\alpha_0\eta_{n+1} + (\alpha_0 + \alpha_1)\eta_{n+2} + \dots + (\alpha_0 + \dots + \alpha_{L-1})\eta_{n+L} \\ &\quad = \alpha_0\eta_n + (\alpha_0 + \alpha_1)\eta_{n+1} + \dots + (\alpha_0 + \dots + \alpha_{L-1})\eta_{n+L-1}. \end{aligned}$$

This means that

$$\underline{0} \neq (\alpha_0, \alpha_0 + \alpha_1, \dots, \alpha_0 + \dots + \alpha_{L-1}) \perp (\underline{\eta}_{n+1} - \underline{\eta}_n), \quad 0 \leq n \leq N - L - 1,$$

and (η_n) fails the L-dimensional N-lattice test, i. e., $S(N) < L$, since

$$\left\langle \{\underline{\eta}_n - \underline{\eta}_0 \mid 1 \le n \le N - s\} \right\rangle = \left\langle \{\underline{\eta}_n - \underline{\eta}_{n-1} \mid 1 \le n \le N - s\} \right\rangle,$$

where $\langle M \rangle$ denotes the linear span of M.

Now we prove the converse. Since $S(N) < L$ there exists an L-dimensional vector $(\beta_0, \dots, \beta_{L-1})$ with

$$\underline{0} \ne (\beta_0, \dots, \beta_{L-1}) \perp (\underline{\eta}_{n+1} - \underline{\eta}_n), \quad 0 \le n \le N - L - 1.$$

Firstly we assume $\beta_{L-1} \ne 0$. From the above orthogonality relation we infer a recurrence relation of order L:

$$\eta_{n+L} = \beta_{L-1}^{-1}(\beta_0 \eta_n + (\beta_1 - \beta_0)\eta_{n+1} + \dots + (\beta_{L-1} - \beta_{L-2})\eta_{n+L-1}),$$

$0 \le n \le N - L + 1$. Since for $L(N) \le N/2$ the corresponding (normed) recurrence relation of minimal order is uniquely defined (Lemma 3) we get

$$\alpha_0 + \alpha_1 + \dots + \alpha_{L-1} = \beta_{L-1}^{-1}(\beta_0 + (\beta_1 - \beta_0) + \dots + (\beta_{L-1} - \beta_{L-2})) = 1.$$

Finally we prove that $\beta_{L-1} = 0$ contradicts $L(N) \le N/2$. Let $k := \max\{i \mid \beta_i \ne 0\} < L - 1$. Then, as before, from the orthogonality relation we deduce a recurrence relation of order $k + 1$ for the first $N - (L - 1 - k)$ terms of (η_n) and hence

$$L(N - (L - 1 - k)) \le k + 1 < L.$$

Now we proceed as in the proof of Lemma 3 in the part following (2) and finally arrive at $L(N) = L \ge N/2 + j$ with a positive integer j which contradicts $L \le N/2$. □

As a by-product of the second part of the proof of Proposition 6 we achieved a result we state here for later reference.

Corollary 7 *Put $L := L(N)$. If $S(N) < L \le N/2$ then*

$$\dim \left\langle \{\underline{\eta}_n - \underline{\eta}_0 \mid 1 \le n \le N - L\} \right\rangle = L - 1$$

and $(\eta_L - \eta_{L-1}, \dots, \eta_{N-1} - \eta_{L-1})$ is a linear combination of the vectors

$$(\eta_{i+1} - \eta_i, \dots, \eta_{N-L+i} - \eta_i), \quad i = 0, \dots, L - 2.$$

Proof. The assertion follows immediately from the fact $\beta_{L-1} \ne 0$ for all $(\beta_0, \dots, \beta_{L-1}) \in \left\langle \{\underline{\eta}_n - \underline{\eta}_0 \mid 1 \le n \le N - L\} \right\rangle^{\perp} \setminus \{\underline{0}\}$ obtained in the proof of Proposition 6. □

We continue with another upper bound for $S(N)$ which is effective if the linear complexity is large.

Proposition 8 *We have*

$$S(N) \le N + 1 - L(N+1).$$

Proof. Put $S = S(N)$. Then the S-dimensional vectors $\underline{\eta}_1 - \underline{\eta}_0, \dots, \underline{\eta}_{N-S} - \underline{\eta}_0$ span $\mathbb{K}^S$. Thus there are $\alpha_1, \dots, \alpha_{N-S} \in \mathbb{K}$ such that

$$\alpha_1(\underline{\eta}_1 - \underline{\eta}_0) + \dots + \alpha_{N-S}(\underline{\eta}_{N-S} - \underline{\eta}_0) = \underline{\eta}_{N+1-S}.$$

Rearranging the left hand side of this equation as

$$-(\alpha_1 + \dots + \alpha_{N-S})\underline{\eta}_0 + \alpha_1\underline{\eta}_1 + \dots + \alpha_{N-S}\underline{\eta}_{N-S} = \underline{\eta}_{N+1-S}$$

we obtain that $L(N+1) \le N + 1 - S$, or equivalently, $S(N) \le N + 1 - L(N+1)$. □

Remark 9. Since $L(N) \le L(N+1)$ Proposition 8 implies

$$S(N) \le N + 1 - L(N).$$

Now we are going to produce lower bounds for $S(N)$. The next result supplements Proposition 5.

Proposition 10 *If* $L(N+1) \le (N+1)/2$ *then*

$$S(N) \ge L(N+1) - 1.$$

Proof. Put $L = L(N+1)$. Firstly, if (η_n) passes the L-dimensional $(N+1)$-lattice test, i. e., $S(N+1) \ge L(N+1)$, then by Proposition 4 we have $S(N) \ge L(N+1) - 1$.

In case (η_n) fails the L-dimensional $(N+1)$-lattice test, the assumption $L(N+1) \le (N+1)/2$ by Corollary 7 implies that the rank of

$$A := \begin{pmatrix} \eta_1 - \eta_0 & \cdots & \eta_{N+1-L} - \eta_0 \\ \vdots & & \vdots \\ \eta_L - \eta_{L-1} & \cdots & \eta_N - \eta_{L-1} \end{pmatrix}$$

is $L - 1$ and the last row of A is a linear combination of the first $L - 1$ rows. Consequently the rank of the matrix consisting of the first $L - 1$ rows of A is $L - 1$ which means that (η_n) passes the $(L-1)$-dimensional N-lattice test, i. e., $S(N) \ge L(N+1) - 1$. □

Remark 11. (i) The assumption $L(N+1) \le (N+1)/2$ in the last proposition implies $L(N) = L(N+1)$ (cf. Proposition 2), thus the resulting inequality can also be written as

$$S(N) \ge L(N) - 1.$$

(ii) Assuming $L(N) \le N/2$, Proposition 10 implies $S(N-1) \ge L(N) - 1$ and hence we also obtain $S(N) \ge L(N) - 1$.

Corresponding to the upper bound in Proposition 8 we derive the following lower bound.

Proposition 12 *If* $L(N+1) > (N+1)/2$ *then*

$$S(N) \ge N - L(N+1).$$

Proof. Let $L(N+1) = (N+k+1)/2$ with $k \ge 1$. By Proposition 2

$$L(N+1) = L(N+2) = \ldots = L(N+k+1) = \frac{N+k+1}{2}.$$

Due to Proposition 4 we have $S(N) \ge S(N+k) - k$, and since $L(N+k+1) = (N+k+1)/2$ we may apply Proposition 10 to get $S(N+k) \ge L(N+k+1) - 1$. Putting together these inequalities we arrive at

$$\begin{aligned} S(N) \ge L(N+k+1) - k - 1 &= \frac{N+k+1}{2} - k - 1 \\ = N - \left(\frac{N+k+1}{2}\right) &= N - L(N+1). \end{aligned}$$

□

Now we are in position to prove the main result.

Proof of Theorem 1. We show that $\min(L(N), N+1-L(N))$ is an upper bound and $\min(L(N), N+1-L(N)) - 1$ is a lower bound for $S(N)$.

The upper bound is an immediate consequence of Proposition 5, Proposition 8 and Remark 9.

To verify the lower bound we consider two cases.

1. $L(N) \le (N+1)/2$: If $L(N) \le N/2$ then by (ii) of Remark 11 we have $S(N) \ge L(N) - 1$.
   If $L(N) = (N+1)/2$ then $L(N+1) = (N+1)/2$ and our assertion follows from Proposition 10.
2. $L(N) > (N+1)/2$: This implies $L(N) = L(N+1) > (N+1)/2$ and Proposition 12 provides the lower bound $N - L(N)$ for $S(N)$ as desired. □

In case $L(N) = N+1-L(N)$, i. e., $L(N) = (N+1)/2$, there is a definite value for $S(N)$.

Corollary 13 *If* $L(N) = (N+1)/2$ *then* $S(N) = (N-1)/2$.

Proof. The assumption implies $L(N+1) = (N+1)/2$ and by Proposition 10 and Proposition 5 we infer

$$L(N) - 1 \leq S(N) \leq L(N) = (N+1)/2.$$

Since the upper bound is greater than $N/2$ due to Proposition 4 we have $S(N) = L(N) - 1 = (N-1)/2$. □

The following example shows that all the cases appearing in Theorem 1

$$S(N) = \begin{cases} L(N) & \text{(I)} \\ L(N) - 1 & \text{(II)} \\ N + 1 - L(N) & \text{(III)} \\ N - L(N) & \text{(IV)} \end{cases}$$

can occur.

Example. We consider the following sequence (η_n):

$$1\,1\,1 \quad 0 \; -1 \; -1 \quad 0\,1\,0.$$

The first three terms of (η_n) satisfy the relation $\eta_{n+1} = \eta_n$, thus $L(2) = L(3) = 1$ and Proposition 6 yields $S(2) = S(3) = 0$.

Then L increases to $L(4) = \ldots = L(8) = 3$ and the recurrence relation of least order for the first eight terms of (η_n) is $\eta_{n+3} = -\eta_{n+1} + \eta_{n+2}$. Again by Proposition 6 we get $S(6) = S(7) = S(8) = 3$. Since $S(N) \leq S(N+1) \leq S(N) + 1$ (Proposition 4), this implies $S(4) = 1$ and $S(5) = 2$.

Finally, the whole sequence does not satisfy the recurrence relation of order 3, thus $L(9) = 6$ and a simple computation shows $S(9) = 4$.

N	2	3	4	5	6	7	8	9
$L(N)$	1	1	3	3	3	3	3	6
$S(N)$	0	0	1	2	3	3	3	4

To sum up, for $N = 2$ we have case (II), for $N = 4$ case (IV), for $N = 7$ case (I) and for $N = 9$ case (III).

Acknowledgments. The research of the first author is supported by the Austrian Science Fund FWF under grant No. S 8312, the second author is supported by DSTA research grant R-394-000-011-422.

References

1. Blackburn, S.R., Etzion, T., Paterson, K.G.: Permutation polynomials, de Bruijn sequences, and linear complexity. J. Comb. Th. A **76**(1), 55–82 (1996)

2. Cusick, T.W., Ding, C., Renvall, A.: Stream Ciphers and Number Theory. Amsterdam: Elsevier 1998
3. Dieter, U.: Erzeugung von gleichverteilten Zufallsfolgen. Jahrbuch Überblicke Mathematik, pp. 25–44. Braunschweig: Vieweg 1993
4. Eichenauer, J., Grothe, H., Lehn, J.: Marsaglia's lattice test and non-linear congruential pseudo-random number generators. Metrika **35**(3/4), 241–250 (1988)
5. Eichenauer-Herrmann, J., Herrmann, E., Wegenkittl, S.: A survey of quadratic and inversive congruential pseudorandom numbers. In: Niederreiter, H., et al. (eds.) Monte Carlo and Quasi-Monte Carlo Methods 1996. Lecture Notes in Statistics 127, pp. 66–97. New York: Springer 1998
6. Eichenauer-Herrmann, J., Niederreiter, H.: Digital inversive pseudorandom numbers. ACM Trans. Modeling Comp. Simul. **4**(4), 339–349 (1994)
7. Frieze, A.M., Håstad, J., Kannan, R., Lagarias, J.C., Shamir, A.: Reconstructing truncated integer variables satisfying linear congruences. SIAM J. Comput. **17**(2), 262–280 (1988)
8. Jungnickel, D.: Finite Fields: Structure and Arithmetics. Mannheim: Bibliographisches Institut 1993
9. Lagarias, J.C.: Pseudorandom number generators in cryptography and number theory. In: Cryptology and computational number theory. Proc. Sympos. Appl. Math. 42, pp. 115–143. Providence, RI: Amer. Math. Soc. 1990
10. Levin, M.B.: Explicit digital inversive pseudorandom numbers. Math. Slovaca **50**(5), 581–598 (2000)
11. Marsaglia, G.: The structure of linear congruential sequences. In: Zaremba, S.K. (ed.) Applications of Number Theory to Numerical Analysis, pp. 249–285. New York: Academic Press 1972
12. Massey, J.L.: Shift-register synthesis and BCH decoding. IEEE Trans. Inform. Theory **15**, 122–127 (1969)
13. Menezes, A.J., van Oorschot, P.C., Vanstone, S.A.: Handbook of Applied Cryptography. Boca Raton: CRC Press 1997
14. Niederreiter, H.: Random Number Generation and Quasi-Monte Carlo Methods. Philadelphia: SIAM 1992
15. Niederreiter, H.: New developments in uniform pseudorandom number and vector generation. In: Niederreiter, H., Shiue, P.J.-S. (eds.) Monte Carlo and Quasi-Monte Carlo Methods in Scientific Computing. Lecture Notes in Statistics 106, pp. 87–120. New York: Springer 1995
16. Niederreiter, H.: Some computable complexity measures for binary sequences. In: Ding, C., Helleseth, T., Niederreiter, H. (eds.) Sequences and their Applications, pp. 67–78. London: Springer 1999
17. Niederreiter, H.: Design and analysis of nonlinear pseudorandom number generators. In: Monte Carlo Simulation, pp. 3–9. Rotterdam: A.A. Balkema Publishers 2001
18. Niederreiter, H., Shparlinski, I.E.: Recent advances in the theory of nonlinear pseudorandom number generators. In: Fang, K.-T., Hickernell, F.J., Niederreiter, H. (eds.) Monte Carlo and Quasi-Monte Carlo Methods 2000, pp. 86–102. Berlin: Springer 2002
19. Niederreiter, H., Winterhof, A.: Incomplete exponential sums over finite fields and their applications to new inversive pseudorandom number generators. Acta Arith. **93**(4), 387–399 (2000)
20. Niederreiter, H., Winterhof, A.: On the lattice structure of pseudorandom numbers generated over arbitrary finite fields. Appl. Alg. Engrg. Comm. Comp. **12**(3), 265–272 (2001)
21. Niederreiter, H., Winterhof, A.: Lattice structure and linear complexity of nonlinear pseudorandom numbers. Appl. Alg. Engrg. Comm. Comp. **13**(4), 319–326 (2002)
22. Rueppel, R.A.: Analysis and Design of Stream Ciphers. Berlin: Springer 1986
23. Rueppel, R.A.: Stream ciphers. In: Contemporary Cryptology: The science of Information Integrity, pp. 65–134. New York: IEEE Press 1992