# On the Distribution of Counter-Dependent Nonlinear Congruential Pseudorandom Number Generators in Residue Rings

Edwin D. El-Mahassni
Department of Computing, Macquarie University
North Ryde, NSW, 2109
edwinelm@ics.mq.edu.au
&
Intelligence, Surveillance and Recoinnaissance Division
Defence Science & Technology Organisation
P.O. Box 1500, Edinburgh, SA 5111, Australia
Edwin.El-Mahassni@dsto.defence.gov.au

**Abstract**

Nonlinear congruential pseudorandom number generators can have unexpectedly short periods. Shamir and Tsaban introduced the class of counter-dependend generators which admit much longer periods. In this paper, using a technique recently developed by Niederreiter and Shparlinski, we present discrepancy bounds for sequences of $s$-tuples of successive pseudorandom numbers generated by counter-dependent generators modulo a composite $M$.

## 1 Introduction

In this paper we study some distribution properties of *counter-dependent nonlinear congruential pseudorandom number generators* introduced by [26]

and defined by a recurrence congruence modulo an integer $M$ of the form

$$u_{n+1} = f(u_n, n) \pmod{M}, \quad 0 \le u_n \le M-1, \qquad n = 0, 1, \dots, \tag{1}$$

with some *initial value* $u_0$, where $f(X, Y) \in \mathbb{Z}_M[X, Y]$ is a polynomial over the residue ring $\mathbb{Z}_M = \mathbb{Z}/M\mathbb{Z}$.

It is obvious that the sequence (1) eventually becomes periodic with some period $t \le M^2$. Throughout this paper we assume that this sequence is *purely periodic*, that is, $u_n = u_{n+t}$ beginning with $n = 0$, otherwise we consider a shift of the original sequence.

In the case that $f(X, Y) = h(X) \in \mathbb{Z}_M[X]$ does not depend on the second variable we get the well-studied *nonlinear congruential pseudorandom number generators*, see [5, 7, 10, 18] for the distribution of the elements and for power distribution in prime fields see [22].

However, in this case the period $t$ is at most $M$ and it is possible that the generated sequences have unexpectedly short period.

In the case that $f(X, Y) = g(X) + Y \in \mathbb{Z}_M[X, Y]$ we get the *counter-assisted nonlinear congruential pseudorandom number generators* defined in [26]. These generators are special *nonlinear congruential pseudorandom number generators of order* 2 defined by

$$u_{n+1} = F(u_n, u_{n-1}) \pmod{M}, \quad 0 \le u_n \le M-1, \qquad n = 1, 2, \dots$$

where $F(X, Y) = g(X) - g(Y) + X + 1$ with some special initial values $u_0$ and $u_1$ satisfying $u_1 = g(u_0) + 1$. When the order is greater than two, only in the case $M = p$ is a prime, have been analyzed in [9, 11, 28].

Distribution and structural properties of general counter-dependent nonlinear congruential generators over finite fields have first been analyzed in [6, 22]. Here, we establish results about the distribution about residue rings using a technique recenlty introduced in [18]. We start this article introducting some notations and stating known theorems. In Section 3 we prove results about the distribution of the points

$$\Big(\frac{u_n}{M}, \dots, \frac{u_{n+s-1}}{M}\Big) \tag{2}$$

in the $s$-dimensional unit cube $[0, 1)^s$ in terms of a discrepancy bound, where $n$ runs through a part of the period, $n = 0, \dots, N-1$, $1 \le N \le t$.

A uniform distribution of these points, i.e., a low discrepancy, is a desirable feature for pseudorandom numbers in quasi-Monte Carlo methods, see e.g. [15, 17, 21, 29].

Finally, in Section 4, we show how for some $M$, we obtain improvements on these distribution results.

# 2 Definitions and Auxiliary Results

Through this article log represent the logarithm base 2. Given an integer $M$, we define $\omega(M)$ is the number of distinct prime divisors of $M$ and $\tau(M)$ is the number of divisors of $M$.

**Lemma 1.** *For every sufficiently large $M$, the bounds*

$$\tau(M) = O(M^{\frac{1}{\log\log M}})$$

*and*

$$\omega(M) = O(\log M/\log\log M)$$

*hold.*

*Proof.* The bound for $\tau(M)$ follows directly from Theorem 317 in [12], and noting that $2^{\omega(M)} \leq \tau(M)$, then the bound for $\omega(M)$ also follows. □

These bounds hold for suffiently large $M$, but for most values of $M$ we can get improvements.

**Lemma 2.** *The bounds*

$$\tau(M) \leq (\log M)^2 \quad \textit{and} \quad \omega(M) \leq 3\log\log M$$

*hold for most values of $M$.*

*Proof.* From Hardy and Ramanujan (see [14]), we note that for most $M$,

$$\tau(M) = (\log M)^{\log 2 + o(1)}.$$

Further, since

$$2^{\omega(M)} \leq \tau(M),$$

then $\omega(M) \leq 3\log\log M$ for most values of $M$. □

For a sequence of $N$ points

$$\Gamma = (\gamma_{1,n}, \dots, \gamma_{s,n})_{n=1}^{N} \tag{3}$$

of the half-open interval $[0,1)^s$, denote by $\Delta_\Gamma$ its *discrepancy*, that is,

$$\Delta_\Gamma = \sup_{B \subseteq [0,1)^s} \left| \frac{T_\Gamma(B)}{N} - |B| \right|,$$

where $T_\Gamma(B)$ is the number of points of the sequence $\Gamma$ which hit the box

$$B = [\alpha_1, \beta_1) \times \ldots \times [\alpha_s, \beta_s) \subseteq [0,1)^s$$

and the supremum is taken over all such boxes. For an integer vector $\mathbf{a} = (a_1, \dots, a_s) \in \mathbb{Z}^s$ we put

$$|\mathbf{a}| = \max_{i=1,\dots,s} |a_i|, \qquad r(\mathbf{a}) = \prod_{i=1}^{s} \max\{|a_i|, 1\}. \tag{4}$$

Also, denote by $\gcd(\alpha_0, \dots, \alpha_{N-1})$ the greatest common divisor of the integers $\alpha_0, \dots, \alpha_{N-1}$. We need the *Erdös–Turán–Koksma inequality* (see Theorem 1.21 of [3]) for the discrepancy of a sequence of points of the $s$-dimensional unit cube, which we present in the following form.

**Lemma 3.** *There exists a constant $C_s > 0$ depending only on the dimension $s$ such that, for any integer $L \geq 1$, for the discrepancy of a sequence of points (3) the bound*

$$\Delta_\Gamma < C_s \left( \frac{1}{L} + \frac{1}{N} \sum_{0 < |\mathbf{a}| \leq L} \frac{1}{r(\mathbf{a})} \left| \sum_{n=1}^{N} \exp\left( 2\pi i \sum_{j=1}^{s} a_j \gamma_{j,n} \right) \right| \right)$$

*holds, where $|\mathbf{a}|$, $r(\mathbf{a})$ are defined by (4) and the sum is taken over all integer vectors*

$$\mathbf{a} = (a_1, \dots, a_s) \in \mathbb{Z}^s$$

*with $0 < |\mathbf{a}| \leq L$.*

The currently best value of $C_s$ is given in [2]. We put

$$\mathbf{e}(z) = \exp(2\pi i z / M).$$

For a polynomial $f(X,Y) \in \mathbb{Z}_M[X,Y]$ of total degree $d$ we define the sequence of polynomials $f_k(X,Y) \in \mathbb{Z}_M[X,Y]$ by the recurrence relation

$$f_{k+1}(X,Y) = f\left(f_k(X,Y), Y+k\right), \qquad k = 0,1,\ldots, \tag{5}$$

where $f_0(X,Y) = X$. It is clear that $\deg f_k \le d^k$ and that

$$u_{n+k} = f_k\left(u_n, n\right). \tag{6}$$

This allows us to state the following lemma which we will also need and can also be found in [6].

**Lemma 4.** *Let $f(X,Y) \in \mathbb{Z}_M[X,Y]$ be a polynomial of local degree in $X$ of value $d_p \ge 2$ modulo every prime divisor $p$ of $M$ and $f_k(X,Y)$ is defined as in (5). Then the local degree in $X$ of $f_k^{(p)}(X,Y) = f_k(X,Y) \pmod p$ equals $d_p^k$, $k = 0,1,\ldots$.*

*Proof.* It is trivial to see that

$$f_k^{(p)}(X,Y) = f^{(p)}(f_{k-1}^{(p)}(X,Y), Y+K-1) \pmod p.$$

So, using a Lemma in the article [6], we have finished □

The following lemma is the 2-dimensional version of Theorem 2.6 in [1] in a slightly weaker form.

**Lemma 5.** *Let $F(X,Y)$ be a polynomial with integer coefficients with the gcd of all of them, except the independent term, is one and total degree $d$ then the bound*

$$\left|\sum_{x,y=1}^{M} \mathbf{e}_M(F(x,y))\right| \le e^{14d} 3^{2\omega(M)} (\tau(M)) M^{2-1/d}$$

*holds.*

This now allows us to state and prove the following Lemma.

**Lemma 6.** *Let $F(X,Y)$ be a polynomial with integer coefficients and total degree $d$. Then the bound*

$$\left|\sum_{x,y=1}^{M} \mathbf{e}_M(F(x,y))\right| \le e^{14d} 3^{2\omega(M/G)} (\tau(M/G)) M^{2-1/d} G^{1/d}$$

*holds, where $G$ is the gcd of all the coefficients of $F$ except the independent term.*

*Proof.* We suppose that $G > 1$ otherwise Lemma 5 applies.

Let $F_G(x,y) = F(x,y)/G$ and $m = M/G$. Then,

$$\left|\sum_{x,y=1}^{M} \mathbf{e}_M(F(x,y))\right| = G^2 \left|\sum_{x,y=1}^{m} \mathbf{e}_m(F_G(x,y))\right| \le G^2 e^{14d} 3^{2\omega(m)} \tau(m) (m)^{2-1/d}. \tag{7}$$

and the result follows. □

Now, we are going to introduce some results about the sequence $f_k(X,Y)$ that we will have to use in the proofs.

**Lemma 7.** *Let $f(X,Y) \in \mathbb{Z}_M[X,Y]$ be a polynomial of local degree in $X$, $d_p \ge 2$ modulo every prime divisor $p$ of $M$ and let*

$$\sum_{j=0}^{s-1} a_j \left(f_{k+j}(X,Y) - f_{l+j}(X,Y)\right) = \sum_{i_1=0}^{D_1} \sum_{i_2=0}^{D_2} B_{i_1 i_2} X^i Y^j.$$

*Then, for any $k \ne l$ we have that these equality*

$$\gcd(B_{10}, B_{01}, \ldots, B_{D_1 D_2}, M) = \gcd(a_0, \ldots, a_{s-1}, M).$$

*holds.*

*Proof.* We put $A_j = a_j/G$, $j = 0, \ldots, s-1$ and $m = M/G$, where $G = \gcd(a_0, \ldots, a_{s-1}, M)$. In particular,

$$\gcd(A_0, \ldots, A_{s-1}, m) = 1. \tag{8}$$

It is enough to show that

$$H(X,Y) = \sum_{j=0}^{s-1} A_j \left(f_{k+j}(X,Y) - f_{l+j}(X,Y)\right)$$

is not a constant polynomial modulo any prime $p|m$.

We take $f^{(p)}$ to be the reduction of $f$ modulo $p$. By our assumption, the local degree of $X$ in $f^{(p)}$ is $d_p \ge 2$. Denoting by $f_k^{(p)}$ the $k$th iteration of $f^{(p)}$ defined similarly to (5) and by $H^{(p)}(X,Y)$ as $H(X,Y) \pmod p$. Thus,

$$H^{(p)}(X,Y) = \sum_{j=0}^{s-1} A_j \left(f_{k+j}^{(p)}(X,Y) - f_{l+j}^{(p)}(X,Y)\right) \pmod p.$$

Let $h$ be the largest $j = 1, \dots, s$ with $\gcd(A_j, p) = 1$ (we see from (8) that such $h$ exists). Then for $k > l$ the polynomial $H^{(p)}(X, Y)$ has local degree in $X$ exactly $d_p^{k+h}$, using lemma 4 and finishing the proof. $\square$

# 3 Discrepancy Bound

Let the sequence $(u_n)$ generated by (1) be purely periodic with an arbitrary period $t$. For an integer vector $\mathbf{a} = (a_0, \dots, a_{s-1}) \in \mathbb{Z}^s$ we introduce the exponential sum

$$S_{\mathbf{a}}(N) = \sum_{n=0}^{N-1} \mathbf{e}\left(\sum_{j=0}^{s-1} a_j u_{n+j}\right).$$

**Theorem 8.** *Let the sequence $(u_n)$, given by (1) with a polynomial $f(X, Y) \in \mathbb{Z}_M[X, Y]$ with $f(X, Y)$ of total degree $d$ and local degree in $X$, at least 2 modulo every prime divisor $p$ of $M$, be purely periodic with period $t$, and $t \geq N \geq 1$, then the bound*

$$\max_{\gcd(a_0, \dots, a_{s-1}, M) = G} |S_{\mathbf{a}}(N)| = O\left(N^{1/2} M (\log\log\log(M/G))^{-1/2}\right)$$

*holds, where the implied constant depends only on $s$ and $d$.*

*Proof.* Select any $\mathbf{a} = (a_0, \dots, a_{s-1}) \in \mathbb{Z}^s$ with $\gcd(a_0, \dots, a_{s-1}, M) = G$. It is obvious that for any integer $k \geq 0$ we have

$$\left| S_{\mathbf{a}}(N) - \sum_{n=0}^{N-1} \mathbf{e}_M\left(\sum_{j=0}^{s-1} a_j u_{n+k+j}\right) \right| \leq 2k.$$

Therefore, for any integer $K \geq 1$,

$$K|S_{\mathbf{a}}(N)| \leq W + K^2,$$

where

$$W = \left| \sum_{n=0}^{N-1} \sum_{k=0}^{K-1} \mathbf{e}_M\left(\sum_{j=0}^{s-1} a_j u_{n+k+j}\right) \right| \leq \sum_{n=0}^{N-1} \left| \sum_{k=0}^{K-1} \mathbf{e}_M\left(\sum_{j=0}^{s-1} a_j u_{n+k+j}\right) \right|.$$

Accordingly, we obtain

$$\begin{aligned} W^2 &\leq N \sum_{n=0}^{N-1} \left| \sum_{k=0}^{K-1} \mathbf{e}_M \left( \sum_{j=0}^{s-1} a_j f_{k+j}(u_n, n) \right) \right|^2 \\ &\leq N \sum_{x,y=1}^{M} \left| \sum_{k=0}^{K-1} \mathbf{e}_M \left( \sum_{j=0}^{s-1} a_j f_{k+j}(x, y) \right) \right|^2 \\ &= N \sum_{k=0}^{K-1} \sum_{l=0}^{K-1} \sum_{x,y=1}^{M} \mathbf{e}_M \left( \sum_{j=0}^{s-1} a_j \left( f_{k+j}(x, y) - f_{l+j}(x, y) \right) \right). \end{aligned}$$

If $k = l$, then the inner sum is trivially equal to $M^2$. There are $K$ such sums. Otherwise, using Lemma 5, the polynomial $\sum_{j=0}^{s-1} a_j \left( f_{k+j}(x, y) - f_{l+j}(x, y) \right)$ is nonconstant and has total degree at most $d^{K+s-2}$. Hence we can apply Lemmas 6 and 7 together with Lemma 1 to the inner sum, obtaining the upper bound

$$e^{c_0 d^{K+s-2}} M^{2-1/d^{K+s-2}+1/\log\log M} G^{1/d^{K+s-2}}$$

for at most $K^2$ sums. Hence,

$$W^2 \leq KNM^2 + K^2 N e^{c_0 d^{K+s-2}} M^{2-1/d^{K+s-2}+1/\log\log M} G^{1/d^{K+s-2}}$$

Now, without too much loss of generality we may assume $d^{K+s-2} \geq 2$. Next we put $K = \lceil c_1 \log\log\log(M/G) \rceil$, for some constant $c_1$ to guarantee that the first term dominates and the result follows. □

Next, let $D_s(N)$ denote the discrepancy of the points given by

$$\left( \frac{u_n}{M}, \ldots, \frac{u_{n+s-1}}{M} \right), \qquad n = 0, \ldots, N-1,$$

in the $s$-dimensional unit cube $[0, 1)^s$. Using the last theorem, we proof the following:

**Theorem 9.** *If the sequence $(u_n)$, given by (1) with a polynomial $f(X, Y) \in \mathbb{Z}_M[X, Y]$ with $f(X, Y)$ of total degree $d$ and local degree in $X$ at least 2 modulo every prime divisor of $M$, is purely periodic with period $t$ and $t \geq N \geq 1$, then the bound*

$$D_s(N) = O\left( N^{-1/2} M (\log\log\log\log M)^s / (\log\log\log M)^{1/2} \right)$$

*holds, where the implied constant depends only on $s$ and $d$.*

*Proof.* The statement follows from Lemma 3, taken with

$$L = \left\lceil N^{1/2} M^{-1} (\log\log\log M)^{1/2} \right\rceil$$

and the bound of Theorem 8, where all occurring $G = \gcd(a_1, \ldots, a_s, M)$ are at most $L$. □

# 4 Improvements on bounds for some $M$

In this section we will show that for some values of $M$, we can improve our bounds. Let $S_{\mathbf{a}}(N)$ and $D_s(N)$ be defined as before.

**Theorem 10.** *Let the sequence $(u_n)$, given by (1) with a polynomial $f(X,Y) \in \mathbb{Z}_M[X,Y]$ with $f(X,Y)$ of total degree $d$ and local degree in $X$, at least 2 modulo every prime divisor of $M$, be purely periodic with period $t$ and $t \geq N \geq 1$. Also suppose that*

$$\tau(M) \leq (\log M)^2 \quad \textit{and} \quad \omega(M) \leq 3 \log\log M.$$

*Then the bound*

$$\max_{\gcd(a_0,\ldots,a_{s-1},M)=G} |S_{\mathbf{a}}(N)| = O\left(N^{1/2} M (\log\log(M/G))^{-1/2}\right)$$

*holds, where the implied constant depends only on $s$ and $d$.*

The proof is basically the same, using the bounds given in the theorem instead of Lemma 2.

Recalling lemma 1 we obtain:

**Corollary 11.** *Let the sequence $(u_n)$, given by (1) with a polynomial $f(X,Y) \in \mathbb{Z}_M[X,Y]$ with $f(X,Y)$ of total degree $d$ and local degree in $X$ at least 2 modulo every prime divisor of $M$, be purely periodic with period $t$ and $t \geq N \geq 1$, then for most $M$, the bound*

$$\max_{\gcd(a_0,\ldots,a_{s-1},M)=G} |S_{\mathbf{a}}(N)| = O\left(N^{1/2} M (\log\log(M/G))^{-1/2}\right)$$

*holds, where the implied constant depends only on $s$ and $d$.*

Using Theorem 10

**Theorem 12.** *Let the sequence $(u_n)$, given by (1) with a polynomial $f(X,Y) \in \mathbb{Z}_M[X,Y]$ with $f(X,Y)$ of total degree $d$ and local degree in $X$ at least 2 modulo every prime divisor of $M$, be purely periodic with period $t$ and $t \geq N \geq 1$. Also suppose that $M$ satisfy the inequalities:*

$$\tau(M) \leq (\log M)^2 \qquad \textit{and} \qquad \omega(M) \leq 3 \log\log M.$$

*Then the bound*

$$D_s(N) = O\left(N^{1/2} M (\log\log\log M)^s / (\log\log M)^{1/2}\right)$$

*holds, where the implied constant depends only on $s$ and $d$.*

And again, if we used that for many choices of $M$, the last inequalities holds:

**Corollary 13.** *If the sequence $(u_n)$, given by (1) with a polynomial $f(X,Y) \in \mathbb{Z}_M[X,Y]$ with $f(X,Y)$ of total degree $d$ and local degree in $X$ at least 2 modulo every prime divisor of $M$, be purely periodic with period $t$ and $t \geq N \geq 1$, then for almost all $M$ the bound*

$$D_s(N) = O\left(N^{-1/2} M (\log\log\log M)^s / (\log\log M)^{1/2}\right)$$

*holds, where the implied constant depends only on $s$ and $d$.*

# 5 Open Questions

We remark that the technique used in [23] can not be used here. It would be useful if an improvement using such or a similar method could be found.

# Acknowledgments.

During the preparation of this paper, Domingo Gomez was supported by FWF grant S8313.

# References


[1] G. I. Arkhipov, V. N. Chubarikov, and A. A. Karatsuba, *Trigonometric Sums in Number Theory and Analysis*, de Grutyer Expositions in Mathematics **39**, W.de Grutyer, Berlin, 2004.

[2] T. Cochrane, 'Trigonometric approximation and uniform distribution modulo 1', *Proc. Amer. Math. Soc.*, **103** (1988), 695–702.

[3] M. Drmota and R. F. Tichy, *Sequences, discrepancies and applications*, Springer-Verlag, Berlin, 1997.

[4] J. Eichenauer-Herrmann, E. Herrmann and S. Wegenkittl, 'A survey of quadratic and inversive congruential pseudorandom numbers', *Lect. Notes in Statistics*, Springer-Verlag, Berlin, **127** (1998), 66–97.

[5] E. D. El-Mahassni, I. E. Shparlinski, and A. Winterhof, 'Distribution of nonlinear congruential pseudorandom numbers for almost squarefree integers, *Monatsh. Math.*, **148** (2006), 297–307.

[6] E. El-Mahassni and A. Winterhof, 'On the distribution and linear complexity of counter-dependent nonlinear congruential pseudorandom number generators', JP Journal of Algebra, Number Theory and Applications (JANTA), Pushpa Publishing House, **6**II (2006), 411–423.

[7] E. D. El-Mahassni and A. Winterhof, 'On the distribution of nonlinear congruential pseudorandom numbers in residue rings', *Intern. J. Number Th.*, **2**(1) (2006), 163–168.

[8] F. Griffin, H. Niederreiter and I. Shparlinski, 'On the distribution of nonlinear recursive congruential pseudorandom numbers of higher orders', Lecture Notes in Comp. Sci., Springer, Berlin, **1719** (1999), 87–93.

[9] J. Gutierrez and D. Gomez-Perez, 'Iterations of multivariate polynomials and discrepancy of pseudorandom numbers', Proc. 14th Symp. Appl. Algebra Algebraic Alg. Error-Correcting Codes. Lecture Notes in Comp. Sci., Springer, Berlin, **2227** (2001), 192–199.

[10] J. Gutierrez, I. Shparlinski and A. Winterhof, 'On the linear and nonlinear complexity profile of nonlinear pseudorandom number-generators', IEEE Trans. Inform. Theory **49**(1) (2003), 60–64.

[11] F. Griffin, H. Niederreiter and I. Shparlinski, 'On the distribution of nonlinear recursive congruential pseudorandom numbers of higher orders', Lecture Notes in Comp. Sci., Springer, Berlin, **1719** (1999), 87–93.

[12] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Clarendon Press, Oxford, UK, 3rd ed., 1979.

[13] R. Lidl and H. Niederreiter, *Finite fields*, Cambridge University Press, Cambridge, 1997.

[14] F. Luca and C. Pomerance, 'On the average number of divisors of the Euler function', *Publ. Math. Debrecen*, to appear.

[15] H. Niederreiter, *Random number generation and Quasi–Monte Carlo methods*, SIAM Press, 1992.

[16] H. Niederreiter, 'New developments in uniform pseudorandom number and vector generation', *Lect. Notes in Statistics*, Springer-Verlag, Berlin, **106** (1995), 87–120.

[17] H. Niederreiter, 'Design and analysis of nonlinear pseudorandom number generators', *Monte Carlo Simulation*, A.A. Balkema Publishers, Rotterdam, 2001, 3–9.

[18] H. Niederreiter and I. E. Shparlinski, 'On the distribution and lattice structure of nonlinear congruential pseudorandom numbers', *Finite Fields and Their Appl.*, **5** (1999), 246–253.

[19] H. Niederreiter and I. E. Shparlinski, 'Exponential sums and the distribution of inversive congruential pseudorandom numbers with prime-power modulus', *Acta Arith.*, **92** (2000), 89–98.

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

[21] H. Niederreiter and I. E. Shparlinski, 'Dynamical systems generated by rational functions', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **2643** (2003), 6–17.

[22] H. Niederreiter and A. Winterhof, 'Multiplicative character sums for nonlinear recurring sequences', Acta Arith. 111, (2004), 299-305 .

[23] H. Niederreiter and A. Winterhof, 'Exponential sums for nonlinear recurring sequences', *Finite Fields and their Applications*, to appear.

[24] H. Niederreiter and A. Winterhof, 'On the distribution of compound inversive congruential pseudorandom numbers', *Monatshefte für Mathematik*, **132** (2001), 35–48.

[25] H. Niederreiter and A. Winterhof, 'Exponential sums and the distribution of inversive congruential pseudorandom numbers with power of two modulus', *Int. J. Number Theory*, **1** (2005), 431–438.

[26] A. Shamir and B. Tsaban, 'Guaranteeing the diversity of number generators', Inform. and Comp., **171** (2001), 350–363.

[27] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, University Press, Cambridge, UK, 1995.

[28] A. Topuzŏglu and A. Winterhof, 'On the linear complexity profile of nonlinear congruential pseudorandom number generators of higher orders', *Applicable Algebra in Engineering, Communications and Computing*, **16** (2005), 219–228.

[29] A. Topuzŏglu and A. Winterhof, 'Pseudorandom Sequences', in Topics in Geometry, Cryptography and Coding Theory, Springer, Berlin, 2006.