On the linear complexity profile of explicit nonlinear pseudorandom numbers

Wilfried Meidl, Arne Winterhof *

Institute of Discrete Mathematics, Austrian Academy of Sciences, Sonnenfelsgasse 19, 1010 Vienna, Austria

Received 31 January 2002; received in revised form 24 May 2002

Communicated by H. Ganzinger

Abstract

Bounds on the linear complexity profile of a general explicit nonlinear pseudorandom number generator are obtained. For some special explicit nonlinear generators including the explicit inversive generator these results are improved.

© 2002 Elsevier Science B.V. All rights reserved.

Keywords: Linear complexity profile; Explicit nonlinear pseudorandom number generator; Explicit inversive generator; Computational complexity; Cryptography

1. Introduction

The linear complexity profile \( L(S, N) \) (over the finite field \( F_q \)) of an infinite sequence \( S = (\sigma_n)_{n=0}^{\infty} \) of elements of \( F_q \) is the function which for every integer \( N \geq 2 \) is defined as the least order \( L \) of a linear recurrence relation over \( F_q \)

\[
\sigma_{n+L} = \gamma_{L-1}\sigma_{n+L-1} + \cdots + \gamma_0\sigma_n,
\]

\( 0 \leq n \leq N - L - 1, \) which is satisfied by this sequence, with the convention that \( L(S, N) = 0 \) if the first \( N \) terms of \( S \) are all 0 and \( L(S, N) = N \) if \( \sigma_0 = \sigma_1 = \cdots = \sigma_{N-2} = 0 \) and \( \sigma_{N-1} \neq 0 \). The value

\[
L(S) = \sup_{N \geq 1} L(S, N)
\]

is called the linear complexity of the sequence \( S \). For the linear complexity of any periodic sequence of period \( t \) one easily verifies that

\[
L(S) = L(S, 2t) \leq t.
\]

The linear complexity and the linear complexity profile are important cryptographic characteristics of sequences (see the surveys in [2,12,15,21]). 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 [4,13,14,16,17]). Recently, lower bounds on the linear complexity profile of recursively defined nonlinear generators, i.e.,

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

with a nonlinear polynomial \( f(X) \in F_q[X] \) and some initial value \( \sigma_0 \in F_q \), have been obtained by Gutierrez, Shparlinski, and the second author [6]. In the present paper we consider explicit nonlinear generators. Ini-
tially, these generators were defined as \( p \)-periodic se-quences \( Y = (y_n)_{n=0}^{\infty} \) over a finite prime field \( F_p \), i.e.,
\[
y_n = f(n), \quad n = 0, \ldots, p - 1,
y_{n+p} = y_n, \quad n \geq 0,
\]
where \( f(X) \) is a nonlinear polynomial over \( F_p \) of degree at most \( p - 1 \). In this case they belong to the family of nonlinear congruential generators (cf. [13, Chapter 8]). In Section 2 we prove
\[
L(Y, N) \geq \min\left(N - \deg(f), \deg(f) + 1\right) \tag{1}
\]
and in Section 3 we improve this result for some special generators including explicit inversive generators \( Z = (z_n)_{n=0}^{\infty} \) introduced in [3],
\[
z_n = (an + b)p^{-2}, \quad n = 0, \ldots, p - 1,
z_{n+p} = z_n, \quad n \geq 0,
\]
with \( a, b \in F_p, \, a \neq 0, \, \text{and} \, p \geq 5 \). In particular we show
\[
L(Z, N) \geq \begin{cases} 
(N - 1)/3, & 2 \leq N \leq (3p - 7)/2, 
N - p + 2, & (3p - 5)/2 \leq N \leq 2p - 3, 
p - 1, & N \geq 2p + 2.
\end{cases} \tag{2}
\]
More recently, explicit nonlinear generators over an arbitrary finite field \( F_q \), \( q = p^r, \, r \geq 2 \), were defined (see [18,19]) as the \( q \)-periodic sequences \( Y = (\eta_n)_{n=0}^{\infty} \) produced by an explicit nonlinear digital generator \( (\eta_n)_{n=0}^{\infty} \) defined (see [18,19]) as the \( q \)-periodic sequences \( Y = (\eta_n)_{n=0}^{\infty} \) produced by an explicit nonlinear digital generator.
\[
\eta_n = f(\xi_n) \quad \text{for} \, n = 0, 1, \ldots, q - 1,
\eta_{n+q} = \eta_n, \quad n \geq 0.
\]
where \( f(X) \in F_q[X] \) with \( 2 \leq \deg(f) < q \) and for some fixed basis \( \{\beta_1, \ldots, \beta_r\} \) of \( F_q \) over \( F_p \)
\[
\xi_n = n_1\beta_1 + n_2\beta_2 + \cdots + n_r\beta_r,
\]
if \( n = n_1 + n_2 p + \cdots + n_r p^{r-1}, \, 0 \leq n_i < p, \, i = 1, 2, \ldots, r \). In this case they belong to the family of digital nonlinear generators. We will also prove analogs of (1) and (3) for this family of generators.

The results of this paper provide evidence that nonlinear generators are attractive alternatives to linear generators. In particular the inversive generators seem to be especially suited for applications in Monte Carlo methods.

## 2. Results on general nonlinear generators

To obtain the main result of this section we utilize the following two lemmas. For a proof of the first lemma see [7, Theorem 6.7.4], [9], or [20]. The second lemma was proven by the authors [11] (cf. [1, Theorem 8]).

Lemma 1. If \( L(S, N) > N/2 \) then \( L(S, N + 1) = L(S, N) \). If \( L(S, N) \leq N/2 \), then \( L(S, N + 1) = L(S, N) \). In Section 2 we improve this result for some special generators.

Lemma 2. Let \( F_q \) be a finite field of characteristic \( p \), \( f(X) \in F_q[X] \) be a polynomial of degree \( 1 \leq D \leq q - 1 \), and let \( Y \) be the sequence defined by (4). Then we have
\[
(D + 1 + p - q)\frac{q}{q} \leq L(Y) \leq (D + 1)\frac{p}{q} + q - p.
\]

Theorem 3. The linear complexity profile of a sequence \( Y = (\eta_n)_{n=0}^{\infty} \) produced by an explicit nonlinear digital generator \( (\eta_n)_{n=0}^{\infty} \) of degree \( 1 \leq D \leq q - 1 \) satisfies
\[
\min\left(N + 1 - (D + 1)\frac{p}{q} - q + p, \right.
\]
\[
(D + 1 + p - q)\frac{q}{q} \leq L(Y) \leq \min\left(N, (D + 1)\frac{p}{q} + q - p\right).
\]

### Proof

The upper bound follows immediately by Lemma 2. Since otherwise the lower bound is trivial we may suppose that \( L(Y, N) < (D + 1 + p - q)q/p \). Then due to Lemma 2 there exists an integer \( k \geq 1 \) such that \( L(Y, N) = L(Y, N + 1) = \cdots = L(Y, N + k - 1) \leq L(Y, N + k) \leq L(Y) \) and Lemma 1 yields \( L(Y, N + k) = N + k - L(Y, N) \). If \( L(Y, N) < N + 1 - (D + 1)p/q - q + p \), then
\[
L(Y) \geq L(Y, N + k)
\]
\[
> N + k - \left(N + 1 - (D + 1)\frac{p}{q} - q + p\right)
\]
\[
\geq (D + 1)\frac{p}{q} + q - p
\]
which is a contradiction to Lemma 2. \( \square \)
In the case of an explicit nonlinear digital generator for small \( N \) or small \( D \) Theorem 3 yields just the trivial lower bound. Employing a different method we also obtain nontrivial results for many small \( N \) and \( D \), respectively.

**Theorem 4.** Let
\[
1 \leq D = D_0 + D_1 p + \cdots + D_{r-1} p^{r-1},
\]
\[
0 \leq D_i < p \quad \text{for } 0 \leq i < r,
\]
and suppose that for some integers \( m \geq 0 \) and \( 0 \leq s < r \) we have
\[
D_m = D_{m+1} = \cdots = D_{m+s-1} = p - 1,
\]
where the indices are considered modulo \( r \). Then for \( N > D \) the linear complexity profile of a sequence \( Y = (\eta_n)_{n \geq 0} \) produced by an explicit nonlinear digital generator (4) with a polynomial \( f(X) \in F_q[X] \) of degree \( 1 \leq D \leq q - 1 \) satisfies
\[
L(Y, N) \geq \min \left( \left\lfloor \frac{N}{4D} \right\rfloor + 1, \left\lfloor \frac{q}{2D} \right\rfloor, p^s(D_{m+s} + 1) \right).
\]

**Proof.** Since \( L(Y, N) = L(Y, 2q) \) for \( N \geq 2q \) we may assume that \( N \leq 2q \). Since \( f(X) \) has at most \( D \) zeros and \( N > D \) we have \( L(Y, N) \geq 1 \). Suppose that \( Y \) fulfills the recurrence relation
\[
\eta_{n+L} = \gamma_1 \eta_n + \cdots + \gamma_0 \eta_n,
\]
\[
0 \leq n \leq N - L - 1,
\]
which is equivalent to
\[
f(\xi_{n+L}) = \gamma_1 f(\xi_n + 1) + \cdots + \gamma_0 f(\xi_n) \quad \text{for } 0 \leq n \leq N - L - 1.
\]
Let \( v, l \) and \( 1 \leq N_v, L_l < p \) be the integers defined by
\[
N_v p^v \leq N < (N_v + 1) p^v \quad \text{and}
\]
\[
L_l p^l \leq L < (L_l + 1) p^l.
\]
Since \( p^l \leq L \leq N < p^{v+1} \) we have \( l \leq v \), which yields
\[
N - L - 1 \geq N_v p^v - (L_l + 1) p^l
\]
\[
= \begin{cases} 
(N_v - 1) p^v + p^v - p^l + 1 & \text{if } l < v, \\
(p - 1 - L_l) p^l & \text{if } l = v,
\end{cases}
\]
and
\[
L \leq (L_l + 1) p^l + 1
\]
\[
= L_l p^l + (p - 1)(p^{l-1} + \cdots + 1).
\]
Consequently, if \( l < v \) then the polynomial
\[
F(X) := \sum_{i=0}^L \gamma_i f(X + \xi_i), \quad \gamma_L = -1,
\]
has at least \( N_v(p - L_l)p^{v-l-1} \) distinct zeros if \( N < 2q \), namely \( \xi_k \) with \( k = k_l p^l + k_{l+1} p^{l+1} + \cdots + k_{v-1} p^{v-1} + k_v p^v \), where \( 0 \leq k_1, \ldots, k_{v-1} < p, 0 \leq k_l < p - L_l \), and \( 0 \leq k_v \leq N_v - 1 \) (for those \( k \) we have \( \xi_{k+i} = \xi_k + \xi_l \) for all \( 0 \leq i \leq L \)), and \( (p - L_l)p^{v-l-1} \) zeros if \( N = 2q \). If \( l = v \), then the polynomial \( F(X) \) has at least \( N_v - L_l \) zeros.

First we consider the case that \( F(X) \neq 0 \). If \( l < v \) and \( N < 2q \), then we have
\[
D \geq N_v(p - L_l)p^{v-l-1}
\]
\[
> N_v(p - L_l)L_l N
\]
\[
> (N_v + 1)L_p
\]
\[
\geq (p - 1)N \geq N \geq 4L.
\]
If \( l < v \) and \( N = 2q \), then we have \( D \geq (p - L_l)p^{v-l-1} \geq q/(2L) \).
If \( l = v \) and \( D \geq (N_v + 1)/4 \), then we have \( L \geq p^v > N/(N_v + 1) \geq N/(4D) \).
If \( l = v \) and \( D < (N_v + 1)/4 \), then we have \( L_l \geq N_v - D > N_v - (N_v + 1)/4 \geq N_v/2 \). Thus
\[
L \geq \frac{N_v}{2} p^v \geq \frac{N}{4} \geq \frac{N}{4D}.
\]
Finally we have to consider the case that \( F(X) \equiv 0 \). Let \( f(X) = \sum_{d=0}^D \alpha_d X^d \), then with
\[
f(X + \xi_l) = \sum_{j=0}^D \left( \sum_{d=0}^D \alpha_d \binom{d}{j} \xi_l^{d-j} \right) X^j
\]
we get
\[
F(X) = \sum_{j=0}^D \left( \sum_{d=0}^D \alpha_d \binom{d}{j} \sum_{l=0}^L \gamma_l \xi_l^{d-l} \right) X^j = 0
\]
and thus
\[
S_{D-j} := \sum_{d=0}^D \alpha_d \binom{d}{j} \sum_{l=0}^L \gamma_l \xi_l^{d-l} = 0,
\]
\[
0 \leq j \leq D.
\]
Now we define recursively, \( T_0 := S_0 \) and

\[
T_j := S_j - \alpha_{D-1}^{-1} \sum_{k=0}^{j-1} \alpha_{D-j+k}^{-1} \binom{D}{j} \equiv 0 \mod p
\]

Thus we have

\[
\sum_{i<r} \gamma_i \equiv 0 \mod p.
\]

If \( j = j_0 + j_1 p + \cdots + j_{r-1} p^{r-1} \), \( 0 \leq j_i < p \), then by Lucas' congruence (cf. [5,8,10]) we have

\[
\binom{D}{j} = \binom{D_0}{j_0} \binom{D_1}{j_1} \cdots \binom{D_{r-1}}{j_{r-1}} \mod p,
\]

and thus \( \binom{D}{j} \equiv 0 \mod p \) if and only if \( j_i \leq D_i \) for \( 0 \leq i < r \). The hypothesis \( D_m = D_{m+1} = \cdots = D_{m+r-1} = p - 1 \), yields \( \binom{D}{j} \equiv 0 \mod p \) for \( j = 0, \ldots, p^s(D_{m+s} + 1) - 1 \), then the matrix \( (\xi^m_{ij})_{i,j} \), \( 0 \leq i, j \leq L \), is an invertible Vandermonde matrix and thus we had \( \gamma_L = 0 \) for \( 0 \leq l \leq L \) by (5), which contradicts \( \gamma_L = -1 \). □

**Remark.** If we do not restrict ourselves to the case \( N > D \), then we also might have \( L(Y,N) = 0 \). For instance if \( f(X) = X(X-\xi_1) \cdots (X-\xi_{D-1}) \) then we have \( L(Y,N) = 0 \) for all \( N \) with \( N \leq D \).

### 3. Results on special nonlinear generators

We recall that the nonlinear complexity profile \( NL_m(S,N) \) of order \( m \) of an infinite sequence \( S = (\sigma_n)_{n=0}^{\infty} \) is the function which for every integer \( N \geq 2 \) is defined as the least order \( L \) of a polynomial recurrence relation

\[
\sigma_{n+L} = \Psi(\sigma_{n+L-1}, \ldots, \sigma_n), \quad 0 \leq n \leq N - L - 1,
\]

with a polynomial \( \Psi(X_1, \ldots, X_L) \) over \( F_p \) of total degree at most \( m \), which is satisfied by the sequence. Note, that \( NL_1(S,N) \neq L(S,N) \) is possible because in the definition of \( L(S,N) \) one can use only homogeneous linear polynomials. In general we have \( L(S,N) \geq NL_1(S,N) \geq NL_2(S,N) \geq \cdots \). We present the following results in this general context.

**Theorem 5.** Let \( f(X) \in F_p[X] \) be a polynomial of degree \( D \), suppose that \( 1 \leq b \leq D \) is the number of zeros of \( f(X) \), and let \( Y = (y_n)_{n=0}^{\infty} \) be the sequence defined by \( y_n = f(n)^k \), \( k = p - 1 - c \), \( c \geq 1 \). Then we have

\[
NL_m(Y,N) \geq \min \left( \frac{N-b-cD}{cDm+b+1}, \frac{p-b-cD}{cD+b} \right)
\]

and

\[
L(Y,N) \geq \min \left( \frac{N-b}{cDm+b+1}, \frac{p-b}{cD+b} \right).
\]

**Proof.** Suppose that for \( n = 0, 1, \ldots, N - L - 1 \), the sequence \( Y \) satisfies the recurrence relation

\[
y_{n+L} = \Psi(y_{n+L-1}, \ldots, y_n), \quad 0 \leq n \leq N - L - 1,
\]

with a polynomial \( \Psi(X_1, \ldots, X_L) \) over \( F_p \) of total degree at most \( m \). We may assume that \( L \leq p/b - 1 \). For every zero \( z \) of \( f(X) \) exactly \( L + 1 \) different \( n \) do not fulfill the property \( f(n+i) \neq 0 \) for all \( 0 \leq t \leq L \). Thus at least \( \min(p, N - L) - b(L + 1) \) integers \( n \) fulfill \( 0 \leq n \leq \min(N - L, p) - 1 \) and \( f(n+i) \neq 0 \) for all \( 0 \leq t \leq L \). For those integers \( (6) \) is equivalent to \( f(n+L)^{-c} = \Psi(f(n+L-1)^{-c}, \ldots, f(n)^{-c}) \). Multiplying with \( f(n+L)^c \prod_{i=0}^{L-1} f(n+i)^{cm} \) yields

\[
\prod_{i=0}^{L-1} f(n+i)^{cm} = f(n+L)^c \prod_{i=0}^{L-1} f(n+i)^{cm} \times \Psi(f(n+L-1)^{-c}, \ldots, f(n)^{-c})
\]

for all \( n \) with \( 0 \leq n \leq N - L - 1 \) and \( f(n+i) \neq 0 \) for all \( 0 \leq t \leq L \). Hence the polynomial

\[
F(X) := - \prod_{i=0}^{L-1} f(X+i)^{cm} + f(X+L)^c \prod_{i=0}^{L-1} f(X+i)^{cm} \times \Psi(f(X+L-1)^{-c}, \ldots, f(X)^{-c})
\]
of degree at most $LcDm + cD$ has at least $\min(p, N - L) - b(L + 1)$ zeros. If we demand that the polynomial $\Psi$ has no constant term as in the case of the linear complexity, then $F(X)$ has degree at most $LcDm$. Suppose that $z_0$ is a zero of $f(X)$ such that $f(z_0 - t) \neq 0$ for $0 < t \leq L$. (Since $L \leq p/b - 1$ the existence of $z_0$ is guaranteed.) Then $F(z_0 - L) = -\prod_{i=1}^{N-1} f(z_0 - t) \neq 0$ yields $F(X) \neq 0$ and $\min(p, N - L) - b(L + 1) \leq LcDm + cD$ or $\min(p, N - L) - b(L + 1) \leq LcD$, respectively, in the case of the linear complexity, which yields the assertions of the theorem. 

Corollary 6. Let $Z$ be a sequence produced by an inversive generator (2). Then $Z$ satisfies

$$NL_m(Z, N) \geq \min\left(\frac{N - 2}{m + 2}, \frac{p - 2}{m + 1}\right)$$

and

$$L(Z, N) \geq \min\left(\frac{N - 1}{3}, \frac{p - 1}{2}\right).$$

Remark. Lemma 1 yields also an upper bound on the linear complexity profile,

$$L(Z, N) \leq \max\left(\frac{2N + 2}{3}, \frac{N - p - 1}{2}\right).$$

For $N \geq (3p - 5)/2$ Theorem 3 yields stronger bounds and we get (3).

Finally we prove a similar result for special digital nonlinear generators including the digital explicit inversive generator introduced by Niederreiter and the second author [18].

Theorem 7. Let $f(X) \in F_q[X]$ be a polynomial of degree $D \geq 1$ with exactly one zero $\rho \in F_q$ and $Y = (\eta_n)_{n=0}^{\infty}$ be the sequence defined by $\eta_n = f(\xi_n)^k$, $k = q - 1 - c$, $c \geq 1$. Then $Y$ satisfies

$$NL_m(Y, N) \geq \min\left(\sqrt{\frac{N}{8(cDm + 1)}}, \frac{q}{4(cDm + 1)}\right).$$

Proof. We proceed as in the previous proofs and may assume that $N < 2q$. Suppose that $Y$ satisfies the recurrence relation $\eta_{n+L} = \Psi(\eta_{n+L-1}, \ldots, \eta_n)$, $0 \leq n < N = L - 1$, with a polynomial $\Psi(X_1, \ldots, X_L)$ over $F_q$ of total degree at most $m$. Then the polynomial

$$F(X) := -\prod_{i=0}^{L-1} f(X + \xi_i)^{c_m}$$

$$+ f(X + \xi_L)^c \prod_{i=0}^{L-1} f(X + \xi_i)^{c_m}$$

$$\times \Psi(f(X + \xi_{L-1} - c, \ldots, f(X - c))$$

of degree at most $LcDm + cD \leq 2LcDm$ has at least $T$ zeros, where $T$ is the number of $0 \leq n < N = L - 1$ with $\xi_{n+L} = \xi_n + \xi_l$ and $\xi_{n+L} \neq \rho$ for all $0 \leq t \leq L$. Since $F(\rho - \xi_L) = -\prod_{i=0}^{L-1} f(\rho - \xi_l + \xi_l)^{c_m} \neq 0$ we have $T \leq 2LcDm$.

Let $v, l$ and $1 < N_v, L_l < p$ be the integers defined by $N_v p^v < N < (N_v + 1) p^v$ and $L_l p^l < L < (L_l + 1) p^l$. If $l = 0$ then we have $l < p > \sqrt{N}$. If $l = v = 0$ then we have $T \geq N - L - l = \geq N - 3L$. If $l < v$ and $N < 2q$ then $T \geq N_v (p - L_l) p^{v-l-1} - L - 1 \geq N/(4L) - 2L$. If $l < v$ and $N = 2q$ then $T \geq (p - L_l) p^{v-l-1} - L - 1 \geq q/(2L) - 2L$. Simple calculations yield the result. 

Acknowledgements

The work was partially supported by the Austrian Science Fund (FWF) under the project S8306-MAT.

References


