THE SERIAL TEST FOR A NONLINEAR PSEUDORANDOM NUMBER GENERATOR

TAKASHI KATO, LI-MING WU, AND NIRO YANAGIHARA

Abstract. Let $M = 2^w$, and $G_M = \{1, 3, \ldots, M - 1\}$. A sequence $\{y_n\}$, $y_n \in G_M$, is obtained by the formula $y_{n+1} \equiv ay_n + b + cy_n \mod M$. The sequence $\{x_n\}$, $x_n = y_n/M$, is a sequence of pseudorandom numbers of the maximal period length $M/2$ if and only if $a + c \equiv 1 \mod 4$, $b \equiv 2 \mod 4$. In this note, the uniformity is investigated by the 2-dimensional serial test for the sequence. We follow closely the method of papers by Eichenauer-Herrmann and Niederreiter.

1. Introduction

For generating uniform pseudorandom numbers (denoted as PRN) in the interval $I = [0, 1)$, the linear congruential methods are commonly used. Recently several nonlinear methods, especially the inversive congruential one, were proposed and investigated. For a modulus $M$, let

$$Z_M = \{0, 1, \ldots, M - 1\} = \mathbb{Z}/M.$$ 

In the linear method, a sequence $\{y_n\}$ in $Z_M$ is generated by

$$y_{n+1} \equiv cy_n + b \mod M, \quad n = 0, 1, \ldots,$$

where $c, b \in Z_M$. The PRN are obtained by the normalization

$$x_n = y_n/M.$$

In the inversive method with power of two modulus, let $M = 2^w$ and

$$G_M = \{1, 3, \ldots, M - 1\} = \{\text{positive odd integers less than } M\}.$$ 

For any $u \in G_M$, there is a unique $\overline{u} \in G_M$ such that $\overline{u}u \equiv 1 \mod M$. Now a sequence $\{y_n\}$ in $G_M$ is generated by the inversive recursion formula

$$y_{n+1} \equiv a\overline{y}_n + b \mod M, \quad n = 0, 1, \ldots,$$

in which $a, b \in Z_M$ are chosen so that $y_n \in G_M$ implies $y_{n+1} \in G_M$.

In a previous note we have proposed another nonlinear method which is given by the following formula, with the modulus $M = 2^w$,

$$y_{n+1} \equiv a\overline{y}_n + b + cy_n \mod M, \quad n = 0, 1, \ldots,$$

in which $a, b, c \in Z_M$ should be such that $y_n \in G_M$ implies $y_{n+1} \in G_M$. The PRN $\{x_n\}$ is defined by (1.2). In [7], we proved the following Theorem A, which shows that the modified inversive method (1.4) bears close resemblance to (1.3):

Received by the editor October 25, 1994.

1991 Mathematics Subject Classification. Primary 65C10; Secondary 11K45.

Key words and phrases. Pseudorandom number generator, the inversive congruential method, power of two modulus, discrepancy, $k$-dimensional serial test, Kloosterman sum.

©1996 American Mathematical Society
Theorem A. Let $M = 2^w, w \geq 3$. Then the PRN $\{x_n\}$ derived from (1.4) is purely periodic with period $M/2$ if and only if

$$a + c \equiv 1 \pmod{4} \quad \text{and} \quad b \equiv 2 \pmod{4}.$$

Now we will study the behavior of these PRN under the 2-dimensional serial test. That is, we will estimate the discrepancy of the PRN. For a dimension $k \geq 2$ and for $N$ arbitrary points $t_0, t_1, \ldots, t_{N-1} \in [0,1)^k$ we define the discrepancy

$$(1.5) \quad D_N(t_0, t_1, \ldots, t_{N-1}) = \sup_J |F_N(J) - V(J)|,$$

where the supremum is extended over all subintervals $J$ of $[0,1)^k$. $F_N(J)$ is $N^{-1}$ times the number of terms among $t_0, t_1, \ldots, t_{N-1}$ falling into $J$, and $V(J)$ denotes the $k$-dimensional volume of $J$. If $\{x_n\}$ is a sequence of PRN in $[0,1)$ with period $p$, then we consider the points

$$x_n = (x_n, x_{n+1}, \ldots, x_{n+k-1}) \in [0,1)^k \quad \text{for} \quad n = 0, 1, \ldots, p - 1,$$

and write their discrepancy $D_p(x_0, x_1, \ldots, x_{p-1})$ as $D_p^{(k)}$.

Theorem 1. Let $M = 2^w (w \geq 6)$ and $a, b, c \in Z_M$. Suppose $a + c \equiv 1 \pmod{4}, b \equiv 2 \pmod{4}$ and $a \neq 0$. Then, for the PRN $\{x_n\}$ in Theorem A, we have

(I) If $c$ is an even number, hence $a$ is odd, then

$$D_{M/2}^{(2)} \leq 2KM^{-1/2} \log M + 1.12M^{-1/2} \log M + 1.35M^{-1/2} + 4/M,$$

with $K = 2/(2^{3/2} - 1)BP(J^2)$.

(II) If $c$ is odd (hence $a$ is even), then writing $a = 2a', a'$ odd, we have

$$D_{M/2}^{(2)} \leq 2^{t/2} M^{-1/2} \{2K \log M \}^2 + (1.12) \log M + 1.35 \} + 4/M + 2L/M^2,$$

with $K = 2/(2^{3/2} - 1)BP(J^2)$ and $L = 2^{24}(2(t - 1)(t + 2)^2 + 14(t + 2)^2)$, assuming that $w \geq t + 6$.

Theorem 2. Let $M = 2^w, w \geq 6$. Let $0 < r \leq 2$ and $A(r) = (4 - r^2)/(8 - r^2)$. Suppose $c \in Z_M$ is given.

If $c$ is even, there are more than $A(r)M/8$ values of $a \in Z_M$ such that $a + c \equiv 1 \pmod{4}$, and for any $b \in Z_M$ with $b \equiv 2 \pmod{4}$, we have

$$D_{M/2}^{(k)} \geq K'M^{-1/2} \quad \text{with} \quad K' = r/(\pi + 2).$$

If $c$ is odd, there are more than $A(r)M/32$ values of $a \in Z_M$ such that $a + c \equiv 1 \pmod{4}$, and for any $b \in Z_M$ with $b \equiv 2 \pmod{4}$, we have

$$D_{M/2}^{(k)} \geq (2K'/3)M^{-1/2} \quad \text{with} \quad K' = r/(\pi + 2).$$

Our proofs of Theorems 1 and 2 are almost the same as in [9, Theorem 2], [6, Theorems 1-2], respectively. The lattice structure of the sequence generated by (1.4) will be studied in another paper.
2. Proof of Theorem 1

We closely follow the method in [9, p.141]. Let $M = 2^w$, $w \geq 6$.
Suppose $m = 2^f$, with a positive integer $f$, be given. For $k \geq 1$, let $C_k(m)$ be
the set of all nonzero lattice points $(h_1, ..., h_k) \in \mathbb{Z}^k$ with $-m/2 < h_j \leq m/2$, for
$1 \leq j \leq k$. We put

$$r(h, m) = \begin{cases} 1 & \text{for } h = 0, \\ m \sin(\pi |h|/m) & \text{for } h \in C_1(m), \end{cases}$$

and for $h = (h_1, ..., h_k) \in C_k(m)$ we define

$$r(h, m) = \prod_{j=1}^{k} r(h_j, m).$$

For real $s$ we write $e(s) = e^{2\pi i s}$. For $x, y \in \mathbb{R}^k$, $x \cdot y$ denotes the inner product.
We put, for integers $u, v$,

$$S(u, v; m) = \sum_{n \in G_m} e((un + v\pi)/m),$$

in which $\pi \in G_m$ denotes the number such that $\pi n \equiv 1 \pmod{m}$. This sum has
the following properties [12, 9]:

(2.1) $S(u, v; m) = S(1, uv; m)$ if $u$ is odd,

(2.2) $S(u, v; m) = 0$ if $u + v \equiv 1 \pmod{2}$,

(2.3) $S(u, v; m) = 2^d S(u/2^d, v/2^d; 2^{f-d})$ if $u \equiv v \equiv 0 \pmod{2^d}$ and $d < f$,

where in (2.2) and (2.3) we assume that $f \geq 2$. Further (see [9, p.140]),

(2.4) $|S(1, v; 8)| = \begin{cases} 4 & \text{if } v \equiv 3 \pmod{4}, \\ 0 & \text{otherwise}, \end{cases}$

(2.5) $|S(1, v; 16)| = \begin{cases} 4\sqrt{2} & \text{if } v \equiv 1 \pmod{4}, \\ 0 & \text{otherwise}, \end{cases}$

(2.6) $|S(1, v; 32)| \leq \begin{cases} 8\sqrt{2} + \sqrt{2} & \text{if } v \equiv 5 \pmod{8}, \\ 0 & \text{otherwise}. \end{cases}$

For $f \geq 6$, we have

(2.7) $|S(1, v; 2^f)| \leq \begin{cases} 2^{(f+3)/2} & \text{if } v \equiv 1 \pmod{8}, \\ 0 & \text{otherwise}. \end{cases}$

The following lemmas are from [9, p.136 and p.140].
Lemma 2.1. Let \( m \geq 2 \) be an integer and let \( y_0, y_1, \ldots, y_{N-1} \in \mathbb{Z}^k \) be lattice points all of whose coordinates are in \([0, m)\). Then the discrepancy of the points \( t_n = y_n/m, 0 \leq n \leq N-1 \), satisfies

\[
D_N(t_0, t_1, \ldots, t_{N-1}) \leq \frac{k}{m} + \frac{1}{N} \sum_{h \in C_1(m)} \frac{1}{r(h, m)} \left| \sum_{n=0}^{N-1} e(h \cdot t_n) \right|.
\]

Lemma 2.2. Let \( m = 2^f \). For \( f \geq 6 \) and \( r \) odd, we have

\[
\sum_{k \in C_1(m), k \equiv r (\text{mod } 8)} \csc \left( \frac{\pi |k|}{m} \right) < \frac{(f + 1)(\log 2)}{4\pi} m + 0.2126m,
\]

and for \( f \geq 3 \) we have

\[
\sum_{k \in C_1(m), k \text{ odd}} \csc \left( \frac{\pi |k|}{m} \right) < \frac{(f + 1)(\log 2)}{\pi} m + 0.3024m.
\]

Now we prove Theorem 1. Since \( \{y_0, y_1, \ldots, y_{M/2-1}\} = G_M \), we have

\[
\{(y_n, y_{n+1}); 0 \leq n \leq M/2 - 1\} = \{(n, an + b + cn); n \in G_M\}.
\]

Lemma 2.1 yields

\[
D_{M/2}^{(2)} \leq \frac{2}{M} + \frac{2}{M} \sum_{h \in C_2(M)} \frac{|S(h)|}{r(h, M)},
\]

where for \( h = (h_1, h_2) \in C_2(M) \) we have

\[
|S(h)| = \left| \sum_{n \in G_M} e \left( \frac{(h_1 + h_2c)n + h_2aM + h_2b}{M} \right) \right| = |S(h_1 + h_2c, h_2a; M)|.
\]

Now \( \gcd(h_1, h_2, M) = 2^d \) with \( 0 \leq d \leq w - 1 \), so splitting up the following sum according to the value of \( d \), we get

\[
\sum := \sum_{h \in C_2(M)} \frac{|S(h)|}{r(h, M)} = \sum_{d=0}^{w-1} T_d
\]

with

\[
T_d = \sum_{h} \frac{|S(h_1 + h_2c, h_2a; M)|}{r(h, M)},
\]

where the last sum is extended over all \( h = (h_1, h_2) \in C_2(M) \) with \( \gcd(h_1, h_2, M) = 2^d \). It follows immediately that

\[
T_{w-1} = 1 + \frac{1}{2M}.
\]
Now consider $0 \leq d \leq w - 2$. Write $k_1 = h_1/2^d$, $k_2 = h_2/2^d$. If one of $k_1$ or $k_2$ is even, then (2.3) and (2.2) imply $S(h_1 + h_2c, k_2a; M) = 0$. Thus it suffices to suppose that both $k_1$ and $k_2$ are odd.

We divide the proof into two cases (I) and (II):

(I) $c$ is an even number, hence $a$ is odd. In this case, (2.3) and (2.1) yield

$$S(h_1 + h_2c, k_2a; M) = 2^d S(1, (k_1 + k_2c)k_2a; 2^{w-d}).$$

Thus we obtain

$$T_d = 2^d \sum_{k_1, k_2 \in C_1(2^{w-d}) \atop k_1, k_2 \text{ odd}} \frac{|S(1, (k_1 + k_2c)k_2a; 2^{w-d})|}{r(k_1 2^d, M)r(k_2 2^d, M)}.$$

For $0 \leq d \leq w - 6$, we use (2.7) to get

$$T_d \leq 2^{(w+d+3)/2} \sum_{k_1, k_2 \in C_1(2^{w-d}) \atop k_1, k_2 \text{ odd}} \{r(k_1 2^d, M)r(k_2 2^d, M)\}^{-1},$$

with the sum over odd numbers $k_1, k_2 \in C_1(2^{w-d})$ such that $(k_1 + k_2c)k_2a \equiv 1 \pmod{8}$, that is, $k_1 + k_2c \equiv k_2a \pmod{8}$, i.e.,

$$k_1 \equiv k_2(a - c) \pmod{8}.$$

Thus we have

$$T_d \leq 2^{(w-3w+d+3)/2} \sum_{k_2 \in C_1(2^{w-d}) \atop k_2 \text{ odd}} \csc\left(\frac{\pi k_2}{2^{w-d}}\right) \sum_{k_1 \in C_1(2^{w-d}) \atop k_1 \equiv k_2(a - c) \pmod{8}} \csc\left(\frac{\pi k_1}{2^{w-d}}\right).$$

Together with (2.8) and (2.9), this yields

$$T_d \leq 2^{(w-3w+d+3)/2} \left\{ \frac{(w - d + 1) \log 2}{4\pi} + 0.2126 \right\} \left\{ \frac{(w - d + 1) \log 2}{\pi} + 0.3024 \right\} < 2^{(w-3w+d+3)/2} \left\{ \frac{(\log M)^2}{4\pi^2} + 0.127 \log M + 0.1401 + 0.0122d^2 \right\}.$$

Therefore, as in [9, p.142],

$$\sum_{d=0}^{w-6} T_d < M^{1/2} \left\{ K(\log M)^2 + 0.56 \log M + 0.675 \right\} - \frac{876}{M},$$

with $K = 2/\{(2^{1/2} - 1)\pi^2\}$. 

For $d = w - 5$, we get from (2.6) and (2.13)

$$T_{w-5} \leq 2^{-w-2} \sqrt{2 + \sqrt{2}} \sum_{k_2 \in C_1(32) \atop k_2 \text{ odd}} \csc\left(\frac{\pi k_2}{32}\right) \sum_{k_1 \in C_1(32) \atop k_1 \equiv 5k_2(a - c) \pmod{8}} \csc\left(\frac{\pi k_1}{32}\right).$$
in which we note that, in the second sum, \( k_1 \equiv k_2(5a - c) \equiv 5k_2(a - c) \mod 8 \), since \( c \) is even. As in [9, p.142], by distinguishing the cases \( a - c \equiv 1 \) or \( a - c \equiv 5 \mod 8 \), we have

\[
(2.17) \quad T_{w-5} < 240/M.
\]

Similarly, using (2.4), (2.5) and (2.13), we get

\[
(2.18) \quad T_{w-4} < 60/M, \quad T_{w-3} < 14/M.
\]

Since \(|S(1, v; 4)| = 2\) for \( v \) odd, it follows from (2.12) that

\[
(2.19) \quad T_{w-2} = \frac{4}{M}.
\]

By combining (2.11) and (2.16, 17, 18, 19), we get

\[
\sum_{d=0}^{w-1} := \sum_{d=0}^{w-1} T_d < M^{1/2} \{ K(\log M)^2 + 0.56 \log M + 0.675 \} + 1,
\]

with the constant \( K \) in (2.16). The desired result follows from (2.10).

(II) \( c \) is an odd number; hence \( a (\neq 0) \) is even, \( a \in \mathbb{Z}/M \). Put \( a = 2^t a', a' \) odd.

Consider some \( T_d \) for \( 0 \leq d \leq w-2 \).

We always assume that both \( k_j = h_j/2^d, j = 1, 2 \), are odd. Put \( 2^s = \gcd(k_1 + k_2c, a, 2^{w-d-1}) \), and \( r_1 = (k_1 + k_2c)/2^s, r_2 = k_2a/2^s \).

(II-1) Suppose \( t \geq w - d - 1 \). If \( s < w - d - 1 \), then

\[
S(h) = S(h_1 + h_2c, h_2a; M) = 2^{d+s} S(r_1, r_2; 2^{w-d-s}) = 0
\]

by (2.2), since \( r_1 \) is odd and \( r_2 \) is even. If \( s = w - d - 1 \), then

\[
S(h) = 2^{d+2w-d-1} S(r_1, r_2; 2) = 2^{w-1} = M/2.
\]

If \( w - d \geq 3 \), then

\[
T_d = \frac{M}{2} \sum_{\substack{k_1 + k_2c \equiv 0 \mod 2^s - d \atop k_1, k_2 \text{ odd}}} \frac{1}{r(k_1 2^d, M)r(k_2 2^d, M)}
\]

\[
= \frac{1}{2M} \sum_{k_2 \in C_1(2^{w-d})} \frac{\csc(\pi |k_2|/2^{w-d})}{k_2 \text{ odd}} \sum_{k_1 \in C_1(2^{w-d})} \frac{\csc(\pi |k_1|/2^{w-d})}{k_1 \equiv -k_2 \mod 2^{w-d-1}}
\]

\[
\leq \frac{1}{2M} \left\{ \frac{(w - d + 1) \log 2}{\pi} + 0.3024 \right\} 2^{2(w-d)}
\]

by Lemma 2.2. Since \( 3 \leq w - d \leq t + 1 \), we have

\[
T_d \leq \frac{2^{2t+1}}{M} \left\{ \frac{(t + 2) \log 2}{\pi} + 0.3024 \right\}^2.
\]
If \( w - d = 2 \), then
\[
T_{w-2} \leq 4 \frac{\csc^2(\pi/4)}{2M} = \frac{4}{M}.
\]
Hence,
\[
(2.20) \quad \sum_{w-2 \leq d \leq w-t-1} T_d = T_{w-2} + \sum_{w-3 \leq d \leq w-t-1} T_d \\
\leq 4 \frac{w}{M} + \frac{(w-1)2^{t+1}}{2M} \left( \frac{(t+2)\log 2}{\pi} + 0.3024 \right)^2,
\]
in which the second term does not appear if \( t = 1 \).

(II-2) Now suppose \( 1 \leq t \leq w - d - 2 \).

We define \( s \) and \( r_1, r_2 \) as above. Obviously, \( s \leq t \), hence \( w - d - 1 - s \geq 1 \). Thus one of \( r_1 \) or \( r_2 \) must be odd. If one of \( r_1 \) or \( r_2 \) is even,
\[
S(h) = S(h_1 + h_2c, h_2a; M) = 2^{d+s}S(r_1, r_2; 2^{w-d-s}) = 0.
\]

Hence both \( r_1 \) and \( r_2 \) must be odd, which implies \( s = t \).

Let \( d \leq w - t - 6 \). We argue as in the case \( d \leq w - 6 \) of (I), with \( w - t \) instead of \( w \); we obtain
\[
T_d \leq 2^{(-3w+d+t+3)/2} \sum_{k_2 \in C_1(2^{w-d})} \csc \left( \frac{\pi k_2}{2w-d} \right) \sum_{k_1 \in C_1(2^{w-d}), k_1 \text{ odd}} \csc \left( \frac{\pi k_1}{2w-d} \right)
\]
\[
= 2^{(-3w+d+t+3)/2} \sum_{k_2 \in C_1(2^{w-d})} \csc \left( \frac{\pi k_2}{2w-d} \right) \sum_{k_1 \in C_1(2^{w-d}), k_1 \text{ odd}} \csc \left( \frac{\pi k_1}{2w-d} \right)
\]
\[
= 2^{(-3w+d+t+3)/2} \sum_{k_2 \in C_1(2^{w-d})} \csc \left( \frac{\pi k_2}{2w-d} \right) \sum_{k_1 \in C_1(2^{w-d}), k_1 \equiv k_2(a-c) \text{ (mod 8)}} \csc \left( \frac{\pi k_1}{2w-d} \right)
\]
\[
\leq 2^{(-3w+d+t+3)/2} \sum_{k_2 \in C_1(2^{w-d})} \csc \left( \frac{\pi k_2}{2w-d} \right) \sum_{k_1 \in C_1(2^{w-d}), k_1 \equiv k_2(a-c) \text{ (mod 8)}} \csc \left( \frac{\pi k_1}{2w-d} \right)
\]
\[
\leq 2^{(-3w+d+t+3)/2} \left\{ \frac{(w - d + 1) \log 2}{4\pi} + 0.2126 \right\} \left\{ \frac{(w - d + 1) \log 2}{\pi} + 0.3024 \right\}
\]
\[
\leq 2^{(-3w+d+t+3)/2} \left\{ \frac{(\log M)^2}{4\pi^2} + (0.127) \log M + 0.1401 + 0.0122d^2 \right\},
\]
since the set \( \{k_1; k_1 \equiv k_2(a-c) \text{ (mod 8 : 2^7)}\} \) is contained in \( \{k_1; k_1 \equiv k_2(a-c) \text{ (mod 8)}\} \). Hence we obtain, as in [9, p.142],
\[
(2.21) \quad \sum_{d=0}^{w-t-6} T_d < 2^{l/2} M^{1/2} \left\{ K(\log M)^2 + 0.56 \log M + 0.675 \right\} - 876/M,
\]
with \( K = 2/((2^{3/2} - 1)\pi^2) \).
For \(d = w - t - 5\), we have as in [9, p.142], with \(r_1\) and \(r_2\) as above,

\[
T_{w-t-5} \leq 2^{-w-2} \sqrt{2 + \sqrt{2}} \sum_{\substack{k_2 \in C_t(2^{2t+5}) \text{ } k_2 \text{ } \text{odd} \}} \csc \left( \frac{\pi |k_2|}{2t+5} \right) \sum_{\substack{k_1 \in C_t(2^{2t+5}) \text{ } k_1 \text{ } \text{odd} \quad r_1r_2 \equiv 5 \pmod{8} \}} \csc \left( \frac{\pi |k_1|}{2t+5} \right)
\]

\[
\leq 2^{-w-2} \sqrt{2 + \sqrt{2}} \sum_{\substack{k_2 \in C_t(2^{2t+5}) \text{ } k_2 \text{ } \text{odd} \}} \csc \left( \frac{\pi |k_2|}{2t+5} \right) \sum_{\substack{k_1 \in C_t(2^{2t+5}) \text{ } k_1 \text{ } \text{odd} \quad k_1 \equiv k_2(5a-c) \pmod{8} \}} \csc \left( \frac{\pi |k_1|}{2t+5} \right)
\]

since \(\{k_1; r_1r_2 \equiv 5 \pmod{8}\} = \{k_1; k_1 + k_2c \equiv 5k_2a \pmod{8 \cdot 2^t}\}\) is contained in \(\{k_1; k_1 \equiv k_2(5a-c) \pmod{8}\}\). Thus we get

\begin{equation}
T_{w-t-5} \leq (t + 6)^2 2^{2t+3}/M.
\end{equation}

Similarly, using (2.4), (2.5), we get

\begin{equation}
T_{w-t-4} < (t + 5)^2 2^{2t}/M, \quad T_{w-t-3} < (t + 4)^2 2^{2t}/M.
\end{equation}

Since \(|S(1,v;4)| = 2\) for \(v\) odd, it follows that

\begin{equation}
T_{w-t-2} \leq (t + 3)^2 2^{2t+2}/M.
\end{equation}

By (2.11), (2.20), (2.21), (2.22), (2.23), (2.24), we obtain

\[
\sum_{d=0}^{w-1} T_d < 2^{3/2}M^{1/2}\{K(\log M)^2 + 0.56 \log M + 0.675\} + 1 + L/M,
\]

with \(K = 2/(\{2^{3/2} - 1\}\pi^2)\) and \(L = 2^{2t}\{2(t - 1)(t + 2)^2 + 14(t + 6)^2\}\). Thus, the desired result follows from (2.10).

### 3. Proof of Theorem 2

The proof is almost the same as in [6].

**When \(c\) is an even number.** Calculating as in [6, p.778], putting \(h = (1, 1, 0, \ldots, 0)\), we have

\[
(\pi + 2)MD^{(k)}_{M/2} \geq \left| \sum c\left( \frac{y_n + y_{n+1}}{M} \right) \right| = |S(1 + c, a; M)| = |S(1 + c + a; M)|.
\]

By [6, Lemma 4], there exist more than \(A(r)M/8\) values of \((1 + c)a \in Z_M\) such that \((1 + c)a \equiv 1 \pmod{8}\), and \(|S(1, (1 + c)a; M)| \geq rM^{1/2}\). Then \(a \equiv 1 + c \pmod{8}\), hence \(a + c \equiv 1 + 2c \equiv 1 \pmod{4}\).

**When \(c\) is odd.** If \(c = 1 + 8k\), then put \(h = (3, 1, 0, \ldots, 0)\) and get

\[
3(\pi + 2)MD^{(k)}_{M/2} \geq \left| \sum c\left( \frac{3y_n + y_{n+1}}{M} \right) \right| = |S(3 + c, a; M)|
= 4|S(1 + 2k, a/4; M/4)| \geq 4\sqrt{r(M/4)^{1/2}} = 2rM^{1/2},
\]
for more than \( A(r) M/32 \) values of \((1+2k)a/4\) with \((1+2k)a/4\) \(\equiv 1\), i.e., \(a/4 \equiv 1+2k \mod 8\). Then \( a \equiv 4+8k = 3+c \), hence \(a+c \equiv -3+2a \equiv 1 \mod 4\).

If \( c = 3+4k \), then put \( h = (-1,1,0,...,0) \) and get

\[
(\pi + 2)MD_{M/2}^{(h)} \geq |\sum c(y_{n} + y_{n+1})/M) = |S(c-1,a;M)|
\]

\[= 2|S(1+2k,a/2;M/2)| \geq 2\sqrt{2}rM^{1/2}
\]

for more than \( A(r) M/16 \) values of \((1+2k)a/2\) with \((1+2k)a/2\) \(\equiv 1\), i.e., \(a/2 \equiv 1+2k \mod 8\). Then \( a \equiv 2+4k = c-1 \), hence \(a+c \equiv 1+2a \equiv 1 \mod 4\).

If \( c = 5+8k \), then put \( h = (-1,1,0,...,0) \) and get

\[
(\pi + 2)MD_{M/2}^{(h)} \geq |S(c-1,a;M)| = 4|S(1+2k,a/4;M/4)| \geq 2\sqrt{2}rM^{1/2}
\]

for more than \( A(r) M/32 \) values of \((1+2k)a/4\) with \((1+2k)a/4\) \(\equiv 1\), i.e., \(a/4 \equiv 1+2k \mod 8\). Then \( a \equiv 4+8k = c-1 \), hence \(a+c \equiv 1+2a \equiv 1 \mod 4\).

References

1. J. Eichenauer-Herrmann, Inversive congruential pseudorandom numbers avoid the planes, Math. Comp. 56 (1991), 297–301. MR 91k:65021