MATHEMATICS OF COMPUTATION
Volume 65, Number 214
April 1996, Pages 761–769

THE SERIAL TEST FOR A NONLINEAR PSEUDORANDOM NUMBER GENERATOR

TAKASHI KATO, LI-MING WU, AND NIRO YANAGIHARA

Abstract. Let $M = 2^w$, and $G_M = \{1, 3, ..., M-1\}$. A sequence $\{y_n\}, y_n \in G_M$, is obtained by the formula $y_{n+1} \equiv a\overline{y}_n + b + cy_n \bmod M$. 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 $a + c \equiv 1 \pmod 4$, $b \equiv 2 \pmod 4$. 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

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

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

$$y_{n+1} \equiv cy_n + b \pmod M, \quad n = 0, 1, ..., \tag{1.1}$$

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

$$x_n = y_n/M. \tag{1.2}$$

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

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

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

$$y_{n+1} \equiv a\overline{y}_n + b \pmod M, \quad n = 0, 1, ..., \tag{1.3}$$

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 $M = 2^w$,

$$y_{n+1} \equiv a\overline{y}_n + b + cy_n \pmod M, \quad n = 0, 1, ..., \tag{1.4}$$

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, Kloostermann sum.

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

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

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 $k \geqq 2$ and for N arbitrary points $\mathbf{t}_0, \mathbf{t}_1, ..., \mathbf{t}_{N-1} \in [0, 1)^k$ we define the discrepancy

$$D_N(\mathbf{t}_0, \mathbf{t}_1, ..., \mathbf{t}_{N-1}) = \sup_J |F_N(J) - V(J)|, \tag{1.5}$$

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 $\mathbf{t}_0, \mathbf{t}_1, ..., \mathbf{t}_{N-1}$ 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

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

and write their discrepancy $D_p(\mathbf{x}_0, \mathbf{x}_1, ..., \mathbf{x}_{p-1})$ as $D_p^{(k)}$.

Theorem 1. *Let $M = 2^w$ $(w \geqq 6)$ 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*

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

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

(II) *If c is odd* (*hence a is even*), *then writing $a = 2^t a', a'$ odd, we have*

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

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

Theorem 2. *Let $M = 2^w, w \geqq 6$. Let $0 < r \leqq 2$ 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 $a + c \equiv 1 \bmod 4$, and for any $b \in Z_M$ with $b \equiv 2 \bmod 4$, we have

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

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

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

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 $M = 2^w, w \geqq 6$.

Suppose $m = 2^f$, with a positive integer f, be given. For $k \geqq 1$, let $C_k(m)$ be the set of all nonzero lattice points $(h_1, ..., h_k) \in Z^k$ with $-m/2 < h_j \leqq m/2$, for $1 \leqq j \leqq k$. 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 $\mathbf{h} = (h_1, ..., h_k) \in C_k(m)$ we define

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

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

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

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

$$S(u, v; m) = S(1, uv; m) \text{ if } u \text{ is odd,} \tag{2.1}$$

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

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

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

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

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

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

For $f \geqq 6$, we have

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

The following lemmas are from [9, p.136 and p.140].

Lemma 2.1. *Let $m \geqq 2$ be an integer and let $\mathbf{y}_0, \mathbf{y}_1, ..., \mathbf{y}_{N-1} \in Z^k$ be lattice points all of whose coordinates are in $[0, m)$. Then the discrepancy of the points $\mathbf{t}_n = \mathbf{y}_n/m, 0 \leqq n \leqq N-1$, satisfies*

$$D_N(\mathbf{t}_0, \mathbf{t}_1, ..., \mathbf{t}_{N-1}) \leqq \frac{k}{m} + \frac{1}{N} \sum_{\mathbf{h} \in C_k(m)} \frac{1}{r(\mathbf{h}, m)} |\sum_{n=0}^{N-1} e(\mathbf{h} \cdot \mathbf{t}_n)|.$$

Lemma 2.2. *Let $m = 2^f$. For $f \geqq 6$ and r odd, we have*

$$\sum_{k \in C_1(m), k \equiv r (\mathrm{mod}\ 8)} \csc(\frac{\pi|k|}{m}) < \frac{(f+1)(\log 2)}{4\pi} m + 0.2126m, \tag{2.8}$$

and for $f \geqq 3$ we have

$$\sum_{k \in C_1(m), k \text{ odd}} \csc(\frac{\pi|k|}{m}) < \frac{(f+1)(\log 2)}{\pi} m + 0.3024m. \tag{2.9}$$

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

$$\{(y_n, y_{n+1}); 0 \leqq n \leqq M/2 - 1\} = \{(n, a\overline{n} + b + cn);\ n \in G_M\}.$$

Lemma 2.1 yields

$$D^{(2)}_{M/2} \leqq \frac{2}{M} + \frac{2}{M} \sum_{\mathbf{h} \in C_2(M)} \frac{|S(\mathbf{h})|}{r(\mathbf{h}, M)}, \tag{2.10}$$

where for $\mathbf{h} = (h_1, h_2) \in C_2(M)$ we have

$$|S(\mathbf{h})| = |\sum_{n \in G_M} e(\frac{(h_1 + h_2 c)n + h_2 a\overline{n} + h_2 b}{M})| = |S(h_1 + h_2 c, h_2 a; M)|.$$

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

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

with

$$T_d = \sum_{\mathbf{h}} \frac{|S(h_1 + h_2 c, h_2 a; M)|}{r(\mathbf{h}, M)},$$

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

$$T_{w-1} = 1 + \frac{1}{2M}. \tag{2.11}$$

Now consider $0 \leqq d \leqq w-2$. 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 $S(h_1+h_2c, h_2a; M) = 0$. 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

$$S(h_1 + h_2c, h_2a; M) = 2^d S(1, (k_1 + k_2c)k_2a; 2^{w-d}).$$

Thus we obtain

$$T_d = 2^d \sum_{\substack{k_1,k_2 \in C_1(2^{w-d}) \\ k_1,k_2 \text{ odd}}} \frac{|S(1, (k_1 + k_2c)k_2a; 2^{w-d})|}{r(k_1 2^d, M) r(k_2 2^d, M)}. \tag{2.12}$$

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

$$T_d \leqq 2^{(w+d+3)/2} \sum \{r(k_1 2^d, M) r(k_2 2^d, M)\}^{-1}, \tag{2.13}$$

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.,

$$k_1 \equiv k_2(a-c) \pmod 8. \tag{2.14}$$

Thus we have

$$T_d \leqq 2^{(-3w+d+3)/2} \sum_{\substack{k_2 \in C_1(2^{w-d}) \\ k_2 \text{ odd}}} \csc(\frac{\pi |k_2|}{2^{w-d}}) \sum_{\substack{k_1 \in C_1(2^{w-d}) \\ k_1 \equiv k_2(a-c) \pmod 8}} \csc(\frac{\pi |k_1|}{2^{w-d}}). \tag{2.15}$$

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

$$\begin{aligned} T_d &\leqq 2^{(w-3d+3)/2} \{\frac{(w-d+1)\log 2}{4\pi} + 0.2126\}\{\frac{(w-d+1)\log 2}{\pi} + 0.3024\} \\ &< 2^{(w-3d+3)/2} \{\frac{(\log M)^2}{4\pi^2} + 0.127 \log M + 0.1401 + 0.0122 d^2\}. \end{aligned}$$

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

$$\sum_{d=0}^{w-6} T_d < M^{1/2}\{K(\log M)^2 + 0.56 \log M + 0.675\} - \frac{876}{M}, \tag{2.16}$$

with $K = 2/\{(2^{3/2}-1)\pi^2\}$.

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

$$T_{w-5} \leqq 2^{-w-2}\sqrt{2+\sqrt{2}} \sum_{\substack{k_2 \in C_1(32) \\ k_2 \text{ odd}}} \csc(\frac{\pi |k_2|}{32}) \sum_{\substack{k_1 \in C_1(32) \\ k_1 \equiv 5k_2(a-c) \pmod 8}} \csc(\frac{\pi |k_1|}{32}),$$

in which we note that, in the second sum, $k_1 \equiv k_2(5a-c) \equiv 5k_2(a-c) \bmod 8$, since c is even. As in [9, p.142], by distinguishing the cases $a-c \equiv 1$ or $a-c \equiv 5 \bmod 8$, we have

$$T_{w-5} < 240/M. \tag{2.17}$$

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

$$T_{w-4} < 60/M, \quad T_{w-3} < 14/M. \tag{2.18}$$

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

$$T_{w-2} = 4/M. \tag{2.19}$$

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

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

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, $a \in Z_M$*. Put $a = 2^t a', a'$ odd. Consider some $T_d, 0 \leqq d \leqq w-2$.

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 $t \geqq w-d-1$. If $s < w-d-1$, then

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

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

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

If $w - d \geqq 3$, then

$$\begin{aligned} T_d &= \frac{M}{2} \sum_{\substack{k_1+k_2c\equiv 0 \bmod 2^{w-d-1} \\ k_1,k_2 \text{ odd}}} \frac{1}{r(k_1 2^d, M) r(k_2 2^d, M)} \\ &= \frac{1}{2M} \sum_{\substack{k_2 \in C_1(2^{w-d}) \\ k_2 \text{ odd}}} \csc(\frac{\pi|k_2|}{2^{w-d}}) \sum_{\substack{k_1 \in C_1(2^{w-d}) \\ k_1 \equiv -k_2 c \bmod 2^{w-d-1}}} \csc(\frac{\pi|k_1|}{2^{w-d}}) \\ &\leqq \frac{1}{2M}\{\frac{(w-d+1)\log 2}{\pi} + 0.3024\}^2\, 2^{2(w-d)} \end{aligned}$$

by Lemma 2.2. Since $3 \leqq w-d \leqq t+1$, we have

$$T_d \leqq \frac{2^{2t+1}}{M}\{\frac{(t+2)\log 2}{\pi} + 0.3024\}^2.$$

If $w-d=2$, then

$$T_{w-2} \leqq 4\frac{\csc^2(\pi/4)}{2M} = \frac{4}{M}.$$

Hence,

(2.20)

$$\begin{aligned}\sum_{w-2\geqq d\geqq w-t-1} T_d &= T_{w-2} + \sum_{w-3\geqq d\geqq w-t-1} T_d \\ &\leqq \frac{4}{M} + \frac{(t-1)2^{2t+1}}{M}\{\frac{(t+2)\log 2}{\pi} + 0.3024\}^2,\end{aligned}$$

in which the second term does not appear if $t=1$.

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

We define s and r_1, r_2 as above. Obviously, $s \leqq t$, hence $w-d-1-s \geqq 1$. Thus one of r_1 or r_2 must be odd. If one of r_1 or r_2 is even,

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

Hence both r_1 and r_2 must be odd, which implies $s=t$.

Let $d \leqq w-t-6$. We argue as in the case $d \leqq w-6$ of (I), with $w-t$ instead of w; we obtain

$$\begin{aligned}T_d &\leqq 2^{(-3w+d+t+3)/2} \sum_{\substack{k_2\in C_1(2^{w-d})\\ k_2 \text{ odd}}} \csc(\frac{\pi|k_2|}{2^{w-d}}) \sum_{\substack{k_1\in C_1(2^{w-d}), k_1 \text{ odd}\\ r_1r_2\equiv 1 \pmod 8}} \csc(\frac{\pi|k_1|}{2^{w-d}}) \\ &= 2^{(-3w+d+t+3)/2} \sum_{\substack{k_2\in C_1(2^{w-d})\\ k_2 \text{ odd}}} \csc(\frac{\pi|k_2|}{2^{w-d}}) \sum_{\substack{k_1\in C_1(2^{w-d}), k_1 \text{ odd}\\ r_1\equiv r_2 \pmod 8}} \csc(\frac{\pi|k_1|}{2^{w-d}}) \\ &= 2^{(-3w+d+t+3)/2} \sum_{\substack{k_2\in C_1(2^{w-d})\\ k_2 \text{ odd}}} \csc(\frac{\pi|k_2|}{2^{w-d}}) \sum_{\substack{k_1\in C_1(2^{w-d}), k_1 \text{ odd}\\ k_1\equiv k_2(a-c) \pmod{8\cdot 2^t}}} \csc(\frac{\pi|k_1|}{2^{w-d}}) \\ &\leqq 2^{(-3w+d+t+3)/2} \sum_{\substack{k_2\in C_1(2^{w-d})\\ k_2 \text{ odd}}} \csc(\frac{\pi|k_2|}{2^{w-d}}) \sum_{\substack{k_1\in C_1(2^{w-d}), k_1 \text{ odd}\\ k_1\equiv k_2(a-c) \pmod 8}} \csc(\frac{\pi|k_1|}{2^{w-d}}) \\ &\leqq 2^{(w-3d+t+3)/2}\{\frac{(w-d+1)\log 2}{4\pi} + 0.2126\}\{\frac{(w-d+1)\log 2}{\pi} + 0.3024\} \\ &\leqq 2^{(w-3d+t+3)/2}\{\frac{(\log M)^2}{4\pi^2} + (0.127)\log M + 0.1401 + 0.0122d^2\},\end{aligned}$$

since the set $\{k_1; k_1 \equiv k_2(a-c) \pmod{8\cdot 2^t}\}$ is contained in $\{k_1; k_1 \equiv k_2(a-c) \pmod 8\}$. Hence we obtain, as in [9, p.142],

(2.21)
$$\sum_{d=0}^{w-t-6} T_d < 2^{t/2}M^{1/2}\{K(\log M)^2 + 0.56\log M + 0.675\} - 876/M,$$

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,

$$T_{w-t-5} \leqq 2^{-w-2}\sqrt{2+\sqrt{2}} \sum_{\substack{k_2 \in C_1(2^{t+5}) \\ k_2 \text{ odd}}} \csc(\frac{\pi|k_2|}{2^{t+5}}) \sum_{\substack{k_1 \in C_1(2^{t+5}), k_1 \text{ odd} \\ r_1 r_2 \equiv 5 \pmod 8}} \csc(\frac{\pi|k_1|}{2^{t+5}})$$

$$\leqq 2^{-w-2}\sqrt{2+\sqrt{2}} \sum_{\substack{k_2 \in C_1(2^{t+5}) \\ k_2 \text{ odd}}} \csc(\frac{\pi|k_2|}{2^{t+5}}) \sum_{\substack{k_1 \in C_1(2^{t+5}), k_1 \text{ odd} \\ k_1 \equiv k_2(5a-c) \pmod 8}} \csc(\frac{\pi|k_1|}{2^{t+5}})$$

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

$$T_{w-t-5} < (t+6)^2\, 2^{2t+3}/M. \tag{2.22}$$

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

$$T_{w-t-4} < (t+5)^2\, 2^{2t}/M, \quad T_{w-t-3} < (t+4)^2\, 2^{2t}/M. \tag{2.23}$$

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

$$T_{w-t-2} \leqq (t+3)^2\, 2^{2t+2}/M. \tag{2.24}$$

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

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

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 $\mathbf{h} = (1, 1, 0, ..., 0)$, we have

$$(\pi+2)MD_{M/2}^{(k)} \geqq |\sum e(\frac{y_n + y_{n+1}}{M})| = |S(1+c, a; M)| = |S(1, (1+c)a; M)|.$$

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 $|S(1, (1+c)a; M)| \geqq rM^{1/2}$. 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 $\mathbf{h} = (3, 1, 0, ..., 0)$ and get

$$3(\pi+2)MD_{M/2}^{(k)} \geqq |\sum e(\frac{3y_n + y_{n+1}}{M})| = |S(3+c, a; M)|$$

$$= 4|S(1+2k, a/4; M/4)| \geqq 4r(M/4)^{1/2} = 2rM^{1/2},$$

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 $\mathbf{h} = (-1,1,0,...,0)$ and get

$$(\pi+2)MD_{M/2}^{(k)} \geqq |\sum e(\frac{-y_n+y_{n+1}}{M})| = |S(c-1,a;M)|$$

$$= 2|S(1+2k,a/2;M/2)| \geqq 2r(M/2)^{1/2} = \sqrt{2}rM^{1/2}$$

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 $\mathbf{h} = (-1,1,0,...,0)$ and get

$$(\pi+2)MD_{M/2}^{(k)} \geqq |S(c-1,a;M)| = 4|S(1+2k,a/4;M/4)| \geqq 2rM^{1/2}$$

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 $a \equiv 4+8k = c-1$, 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
2. J. Eichenauer-Herrmann, *Statistical independence of a new class of inversive congruential pseudorandom numbers*, Math. Comp. **60** (1993), 375–384. MR **93d:**65011
3. J. Eichenauer-Herrmann, *On generalized inversive congruential pseudorandom numbers,* Math. Comp. **63** (1994), 293–299. MR **94k:**11088
4. J. Eichenauer-Herrmann, H. Grothe, H. Niederreiter, and A. Topuzoglu, *On the lattice structure of a nonlinear generator with modulus* 2^α, J. Comp. Appl. Math. **31** (1990), 81–85. MR **91j:**65012
5. J. Eichenauer, J. Lehn, and A. Topuzoglu, *A nonlinear congruential pseudorandom number generator with power of two modulus*, Math. Comp. **51** (1988), 757–759. MR **89i:**65007
6. J. Eichenauer-Herrmann and H. Niederreiter, *Lower bounds for the discrepancy of inversive congruential pseudorandom numbers with power of two modulus*, Math. Comp. **58** (1992), 775–779. MR **92i:**65018
7. T. Kato, L.-M. Wu, and N. Yanagihara, *On a nonlinear congruential pseudorandom number generator*, Math. Comp. **65** (1996) (to appear).
8. D. E. Knuth, *The Art of Computer Programming* Vol.2: Seminumerical Algorithms, 2nd Ed., Addison-Wesley, Reading, Mass., 1981. MR **83i:**68003
9. H. Niederreiter, *The serial test for congruential pseudorandom numbers generated by inversions*, Math. Comp. **52** (1989), 135–144. MR **90e:**65008
10. H. Niederreiter, *Recent trends in random number and random vector generation*, Ann. Oper. Res. **31** (1991), 323–345. MR **92h:**65010
11. H. Niederreiter, *Random number generation and quasi-Monte Carlo methods*, SIAM, Philadelphia, PA, 1992. MR **93h:**65008
12. H. Salié, *Über die Kloostermanschen Summen S(u,v;q)*, Math. Z. **34** (1932), 91–109.

Department of Mathematics, Faculty of Education, Chiba University. 1-33 Yayoi-cho, Chiba City, 263 Japan

Department of Mathematics, Faculty of Science, Chiba University, 1-33 Yayoi-cho, Chiba City, 263 Japan

Department of Mathematics, Faculty of Science, Chiba University, 1-33 Yayoi-cho, Chiba City, 263 Japan

E-mail address: yanagi@math.s.chiba-u.ac.jp