Uniform Distribution Theory 2 (2007), no.2, 105–120

uniform distribution theory

PSEUDO-RANDOMNESS OF QUADRATIC GENERATORS

Oľga Blažeková — Oto Strauch

ABSTRACT. Let x_n, $n = 0, 1, \ldots, M-1$, be a sequence produced by quadratic generator $ax^2 + bx + c \pmod M$. In this paper we describe a new method which gives a new bound for discrepancy $D_M(x_n, x_{n+1})$. The analysis is restricted by the case of x_n with maximal period length M.

Communicated by Harald Niederreiter

1. Introduction

There is no formal fully satisfactory definition of random and pseudo-random number sequences, we have only a scale of tests which such a sequence should satisfy, see [DT, pp. 424–430], [SP, p. 2–243, 2.25], and [N, pp. 161–175]. D.E. Knuth [K] proposed the test that for an infinite uniformly random sequence x_n, $n = 0, 1, \ldots$ in $[0, 1)$, all of sequences (x_n, x_{n+1}), $n = 0, 1, \ldots$; (x_n, x_{n+1}, x_{n+2}), $n = 0, 1, \ldots$; etc. must be uniformly distributed. For finite pseudo-random sequence x_n, $n = 0, 1, \ldots, M-1$, (which is generated by a deterministic algorithm) the sequences (x_n, x_{n+1}), $n = 0, 1, \ldots, M-2$, (x_n, x_{n+1}, x_{n+2}), $n = 0, 1, \ldots, M-3$, etc. must have "sufficiently" small discrepancies.

In this paper we study so-called quadratic generator (see [SP, p. 2–248, 2.25.5], [N, pp. 181–182] and [DT, pp. 428–429]) which again was proposed by D.E. Knuth in 1969 (see [K, p. 25]): Let $M \geq 2$ be a large integer, called the modulus and let a, b, c be three integer parameters and y_0 be the initial integer starting point, all from $[0, M)$. The quadratic congruential generator produces

2000 Mathematics Subject Classification: 11K06, 11K36.
Keywords: Pseudo-randomness, quadratic generator, discrepancy.
This research was supported by the VEGA Grant No. 2/7138/27.

the sequence

$$x_n = \frac{y_n}{M}, \text{ where } y_{n+1} \equiv a y_n^2 + b y_n + c \pmod{M} \text{ and } 0 \le y_n \le M-1 \quad (1)$$

of pseudo-random numbers x_n, $n = 0, 1, \ldots, M-1$. By Knuth [K, p. 34] the sequence y_n is purely periodic with the maximum possible period length M (i.e. $\{0, 1, 2, \ldots, M-1\} = \{y_n; n = 0, 1, \ldots, M-1\}$) if and only if:

$(c, M) = 1$;

$p|a$ for every prime $p|M, p > 2$;

$b \equiv 1 \pmod{p}$ for every prime $p|M, p > 2$;

If $9|M$, then either $9|a$ or $b \equiv 1 \pmod{9}$ and $ac \equiv 6 \pmod{9}$;

If $4|M$, then $2|a$ and $a \equiv b - 1 \pmod{4}$;

If $2|M$, then $a \equiv b - 1 \pmod{2}$.

We assume from now (as usual) that these conditions for the maximum possible period length hold.

Some papers (cf. [EHHW]) investigated the performance of quadratic generator (or pseudo-randomness of x_n, $n = 0, 1, \ldots, M-1$) under the extremal discrepancy D_M of the two-dimensional sequence

$$(x_n, x_{n+1}) = \left(\frac{y_n}{M}, \frac{y_{n+1}}{M}\right), \quad n = 0, 1, \ldots, M-1. \quad (2)$$

Here the extremal discrepancy D_M is defined by

$$D_M(x_n, x_{n+1}) = \sup_{I \subset [0,1]^2} \left| \frac{A(I; N; (x_n, x_{n+1}))}{M} - |I| \right|, \quad (3)$$

where the counting function $A(I; M; (x_n, x_{n+1}))$ is defined as the number of terms of (x_n, x_{n+1}), $n = 0, 1, \ldots, M-1$, for which (x_n, x_{n+1}) belong to the interval I and $|I|$ is the area of I. In this paper we use so-called star discrepancy $D_M^*(x_n, x_{n+1})$, where the intervals I in (3) have the form $I = [0, x) \times [0, y)$, $x, y \in [0, 1]$. In any case $D_M^* \le D_M \le 4D_M^*$, consult [KN, DT, SP].

For a quadratic generator with power of two modulus $M = 2^\omega$ assumed that $a \equiv 2 \pmod{4}$, $b \equiv 3 \pmod{4}$, $c \equiv 1 \pmod{2}$, J. Eichenauer-Herrmann and H. Niederreiter (see [EHN1]) proved that

$$D_M < \frac{2\sqrt{2}+8}{7\pi^2} \cdot \frac{(\log M)^2}{\sqrt{M}} - 0.0791 \frac{\log M}{\sqrt{M}} + \frac{0.3173}{\sqrt{M}} + \frac{4}{M} \text{ and} \quad (4)$$

$$D_M \ge \frac{1}{3(\pi+2)\sqrt{M}}.$$

For modulus $M = p^\omega$, $p > 2$ is a prime, $\omega \ge 2$, $p|a$, $b \equiv 1 \pmod{p}$, $p \nmid c$, and if $p = 3$, then $a \not\equiv 3c \pmod{9}$ and $a \not\equiv 0 \pmod{p^2}$, J. Eichenauer-Herrmann

and H. Niederreiter (see [EHN2]) found

$$D_M < \frac{4+5p^{-3/2}}{\sqrt{M}}\left(\frac{\sqrt{p}}{9}+\frac{1}{\pi^2\sqrt{p}}\left(\log M+\frac{2\pi}{3}\log p\right)(\log M+1.395)\right)+\frac{2}{M}. \tag{5}$$

For composite modulus $M = p_1^{\omega_1}\dots p_r^{\omega_r}$ with primes $p_i \geq 3$ and exponents $\omega_i \geq 2$, S. Strand [S] found

$$D_M < \frac{1}{\sqrt{M}}\prod_{i=1}^{r}\left(1+\frac{5}{4}p_i^{-3/2}\right)\cdot$$
$$\cdot\left(\frac{4}{\pi^2\sqrt{P}}\Big(\log M+\frac{4\sqrt{3}\pi}{9}\log P\Big)(\log M+0.778)+\frac{16}{27}\sqrt{P}\right)+\frac{2}{M}, \text{ and} \tag{6}$$

$$D_M \geq \frac{\sqrt{P}}{2(\pi+2)}\frac{1}{\sqrt{M}}, \quad \text{where } P = p_1\dots p_r.$$

Every bound in (4), (5) and (6) contains some term multiplied by $\frac{(\log M)^2}{\sqrt{M}}$. In this paper we find an upper bound of star discrepancy D_M^* of (2) which contains some term with $\frac{(\log M)^{3/2}}{\sqrt{M}}$.

Theorem 1. *Let $M \geq 9$[1] and $M \nmid ha$ be for $1 \leq h \leq [\sqrt{M}]$ (it holds if $a < \sqrt{M}$) and assume that the quadratic generator $ax^2+bx+c \pmod M$ has the full period of the length M. Then the star discrepancy $D_M^*(x_n, x_{n+1})$ of the sequence (2) satisfies*

$$D_M^* < 58\frac{1}{M}+40\frac{a}{M}+\sqrt{2}\frac{1}{\sqrt{aM}}\frac{c}{M}\left(1-\frac{c}{M}\right)^{1/2}+\sqrt{\frac{2}{3}}\frac{1}{\sqrt{aM}}\left(1-\frac{c}{M}\right)^{3/2}+$$
$$+24\left(\frac{2}{\sqrt{M}}+(8\sqrt{2}+3)\frac{(\log M)^{3/2}}{\sqrt{M}}+36\frac{\sqrt{(a,M)}}{\sqrt{M}}(\log M)2^{\omega(M)}\right). \tag{7}$$

In our proof, by using a geometric approach, we transform the discrepancy problem of a two-dimensional sequence to one-dimensional sequences. More precisely, to approximate the discrepancy D_M^* of (2) we use $D_k^* = \max_{y\in[0,1]} D_k^*(y)$, where $D_k^*(y)$ is the star discrepancy of one-dimensional sequence

$$\sqrt{\frac{M}{a}}\sqrt{\frac{b^2-4ac}{4aM}+i+y} \bmod 1, \quad i = 1, 2, \dots, k,$$

[1] We require it for $1+\log\sqrt{M} < \log M$.

where $y \in [0,1]$ is arbitrary but fixed. Then, to approximate $D_k^*(y)$ we use $D_K^* = \max_{t\in[0,1]} D_K^*(t)$, where $D_K^*(t)$ is the star discrepancy of one-dimensional sequence

$$(i+t+B)^2 \frac{a}{M} \bmod 1, \quad i = 1, 2, \ldots, K,$$

where $t \in [0,1]$ is arbitrary but fixed and B is an integer depending on y. To approximate $D_K^*(t)$ we use an approximation of an incomplete Gaussian quadratic sum by applying a result of C. Mauduit and A. Sárközy [MS] and then Erdős-Turán formula which gives the term $\frac{(\log M)^{3/2}}{\sqrt{M}}$.

2. Geometric approach

For the quadratic congruent polynomial $ax^2 + bx + c \pmod M$ we define the function $F_M : [0,1] \to [0,\infty)$ such that

$$F_M(x) = Max^2 + bx + \frac{c}{M}.$$

If the generator $ax^2 + bx + c \pmod M$ has a full period, then the sequence (2) contains the same points as

$$\left(\frac{n}{M}, F_M\left(\frac{n}{M}\right) \bmod 1\right), \quad n = 0, 1, \ldots, M-1. \tag{8}$$

We begin to compute the star discrepancy D_M^* of (8) by using that all points of (8) are lying on the graph of $F_M(x) \bmod 1$, see Fig. 1. Define two auxiliary

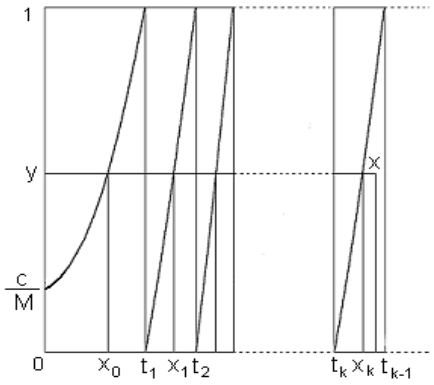

FIGURE 1. Graph of $F_M(x) \bmod 1$

sequences t_i and x_i by equations $F_M(t_i) = i$ and $F_M(x_i) = i + y$. Explicitly

$$t_i = \frac{-b}{2aM} + \frac{1}{\sqrt{aM}}\sqrt{\frac{b^2-4ac}{4aM} + i}, \quad x_i = \frac{-b}{2aM} + \frac{1}{\sqrt{aM}}\sqrt{\frac{b^2-4ac}{4aM} + i + y}. \tag{9}$$

Lemma 1. *The star discrepancy* $D_M^*\left(\frac{n}{M}, F_M\left(\frac{n}{M}\right) \bmod 1\right)$ *satisfies*

$$D_M^* < \frac{2}{M} + \frac{c}{M}t_1 + \max_{c/M \le y \le 1}(x_0 - yx_0) + \max_{1 \le k \le aM+b}\frac{2kD_k^*}{M}, \tag{10}$$

where $D_k^* = \max_{y\in[0,1]} D_k^*(\{Mx_i\})$.

Proof. Abbreviating $A\left(I; M; \left(\frac{n}{M}, F_M\left(\frac{n}{M}\right) \bmod 1\right)\right) = A(I)$ we distinguish three following steps:

1^o. Let y be fixed, $y \in [c/M, 1)$, $I = [0, x) \times [0, y)$ and x runs through the interval $[0, 1]$. Then, we can express the discrepancy function $\frac{A(I)}{M} - |I|$ exactly (if x is irrational):

(i) $\frac{A(I)}{M} - |I| = x - \frac{\{Mx\}}{M} + \frac{1}{M} - xy$ for $x \in [0, x_0]$;

(ii) $\frac{A(I)}{M} - |I| = x_0 - \frac{\{Mx_0\}}{M} + \frac{1}{M} - x_0y - y(x - x_0)$ for $x \in [x_0, t_1]$;

(iii) $\frac{A(I)}{M} - |I| = x_0 - \frac{\{Mx_0\}}{M} + \frac{1}{M} + \sum_{i=1}^{k-1}(x_i - t_i) + \frac{1}{M}\sum_{i=1}^{k-1}(\{Mt_i\} - \{Mx_i\}) + x - t_k + \frac{\{Mt_k\}}{M} - \frac{\{Mx\}}{M} - yt_k - y(x - t_k)$ for $x \in [t_k, x_k]$;

(iv) $\frac{A(I)}{M} - |I| = x_0 - \frac{\{Mx_0\}}{M} + \frac{1}{M} + \sum_{i=1}^{k}(x_i - t_i) + \frac{1}{M}\sum_{i=1}^{k}(\{Mt_i\} - \{Mx_i\}) - yx_k - y(x - x_k)$ for $x \in [x_k, t_{k+1}]$;

(v) $\frac{A(I)}{M} - |I| = x_0 - \frac{\{Mx_0\}}{M} + \frac{1}{M} + \sum_{i=1}^{aM+b-1}(x_i - t_i) + \frac{1}{M}\sum_{i=1}^{aM+b-1}(\{Mt_i\} - \{Mx_i\}) - yt_{aM+b} - y(x - t_{aM+b})$ for $x \in [t_{aM+b}, 1]$; In (v) we have used that the interval $[t_{aM+b}, 1]$ does not contain terms from $\frac{0}{M}, \frac{1}{M}, \ldots, \frac{M-1}{M}$ since $t_{k+1} - t_k < \frac{1}{\sqrt{aM}}\frac{1}{\sqrt{k}}$, which implies $1 - t_{aM+b} \le t_{aM+b+1} - t_{aM+b} < \frac{1}{aM}$.

Now, by the theorem of J.F. Koksma [SP, p. 1–42] we have

$$\left|\frac{1}{k}\sum_{i=1}^{k}\{Mt_i\} - \int_0^1 x\mathrm{d}x\right| \le 1.D_k^*(\{Mt_i\}),$$

which gives

$$\left|\frac{1}{M}\sum_{i=1}^{k}(\{Mt_i\} - \{Mx_i\})\right| \le \frac{2k}{M}\max(D_k^*(\{Mt_i\}), D_k^*(\{Mx_i\})). \tag{11}$$

Furthermore, absolute values of $-\frac{\{Mx\}}{M} + \frac{1}{M}$, $-\frac{\{Mx_0\}}{M} + \frac{1}{M}$, $\frac{\{Mt_k\}}{M} - \frac{\{Mx\}}{M}$ are small than $\frac{1}{M}$ and other parts of (i)–(v) depend on x linearly and thus their

extremes appear on boundary points of intervals. Denoting

$$V_k = x_0 + \sum_{i=1}^{k}(x_i - t_i) - yx_k, \quad T_k = x_0 + \sum_{i=1}^{k}(x_i - t_i) - yt_{k+1}, \tag{12}$$

we have
(i) $\left|\frac{A(I)}{M} - |I|\right| \le \frac{1}{M} + x_0 - yx_0$;
(ii) $\left|\frac{A(I)}{M} - |I|\right| \le \frac{1}{M} + \max(x_0 - yx_0, |x_0 - yt_1|)$;
(iii) $\left|\frac{A(I)}{M} - |I|\right| \le \frac{2}{M} + \frac{2k}{M}\max(D_k^*(\{Mt_i\}), D_k^*(\{Mx_i\})) + \max(|T_{k-1}|, |V_k|)$, where $k = 1, 2, \ldots, aM + b - 1$;
(iv) $\left|\frac{A(I)}{M} - |I|\right| \le \frac{1}{M} + \frac{2k}{M}\max(D_k^*(\{Mt_i\}), D_k^*(\{Mx_i\})) + \max(|V_k|, |T_k|)$, where $k = 0, 1, 2, \ldots, aM + b - 1$;
(v) $\left|\frac{A(I)}{M} - |I|\right| \le \frac{1}{M} + \frac{2(aM+b-1)}{M}\max(D_{aM+b-1}^*(\{Mt_i\}), D_{aM+b-1}^*(\{Mx_i\})) + \max(|T_{aM+b-1}|, |x_0 + \sum_{i=1}^{aM+b-1}(x_i - t_i) - y|)$. Here the final part of (v) obtains at $x = 1$ and we shall replace it by $\left|\frac{A(I)}{M} - |I|\right| \le \frac{1}{M}$, since for $I = [0, 1) \times [0, y)$ we have $\frac{A(I)}{M} = y - \frac{\{My\}}{M} + \frac{1}{M}$ (if y is irrational).
Thus, for every fixed $y \in [c/M, 1]$ and any $x \in [0, 1]$ we have

$$\left|\frac{A(I)}{M} - |I|\right| \le \frac{2}{M} + \max_{1\le k\le aM+b-1}\frac{2k}{M}\max(D_k^*(\{Mt_i\}), D_k^*(\{Mx_i\})) + \max(\max_{0\le k\le aM+b-1}|V_k|, \max_{0\le k\le aM+b-1}|T_k|). \tag{13}$$

In the following, we extend maxima also for $k = aM + b$. We can see that $V_0 > V_1 > \cdots > V_{aM+b}$, $T_0 < T_1 < \cdots < T_{aM+b}$, $V_k > T_k$ for $k = 0, 1, \ldots, aM + b$ and $V_0 > 0$. Thus we have

$$T_0 < T_1 < T_2 < \cdots < T_{aM+b} < V_{aM+b} < \cdots < V_1 < V_0 \tag{14}$$

and from this

$$\max(\max_{0\le k\le aM+b}|V_k|, \max_{0\le k\le aM+b}|T_k|) = \max(|T_0|, V_0).$$

2^o. Now, let y vary in the interval $[c/M, 1]$. Putting $x_0 = x$ and $y = aMx^2 + bx + \frac{c}{M}$, we rewrite functions $T_0(y) = x_0 - yt_1$ and $V_0(y) = x_0 - yx_0$ to forms

$$T_0(x) = x - \left(aMx^2 + bx + \frac{c}{M}\right)t_1, \text{ and } V_0(x) = x - \left(aMx^2 + bx + \frac{c}{M}\right)x$$

and we shall find their maxima for $x \in [0, t_1]$. By definition, for $x = 0$ we have $T_0(x) = -\frac{c}{M}t_1$ and for $x = t_1$ we have $T_0(x) = 0$. Since by (14) for $T_0(x) \ge 0$

we have $T_0(x) \le V_0(x)$, then

$$\max_{x\in[0,t_1]} |T_0(x)| \le \max\left(\frac{c}{M}t_1, \max_{x\in[0,t_1]} V_0(x)\right). \tag{15}$$

3^o. Let $y \in [0, c/M]$. Omitting all parts of (ii)-(v) which include x_0 and replacing V_k and T_k by $\tilde{V}_k$ and $\tilde{T}_k$ defined as

$$\tilde{V}_k = \sum_{i=1}^{k}(x_i - t_i) - yx_k, \quad \tilde{T}_k = \sum_{i=1}^{k}(x_i - t_i) - yt_{k+1}, \tag{16}$$

we find (13) in the form

$$\begin{aligned}\left|\frac{A(I)}{M} - |I|\right| \le \frac{2}{M} + \max_{1\le k\le aM+b}\frac{2k}{M}\max(D_k^*(\{Mt_i\}), D_k^*(\{Mx_i\})) \\ + \max(\max_{0\le k\le aM+b}|\tilde{V}_k|, \max_{0\le k\le aM+b}|\tilde{T}_k|).\end{aligned} \tag{17}$$

Again,

$$\tilde{T}_0 < \tilde{T}_1 < \tilde{T}_2 < \cdots < \tilde{T}_{aM+b} < \tilde{V}_{aM+b} < \cdots < \tilde{V}_1 < \tilde{V}_0 = 0 \tag{18}$$

and from this

$$\max(\max_{0\le k\le aM+b}|\tilde{V}_k|, \max_{0\le k\le aM+b}|\tilde{T}_k|) = \max_{y\in[0,c/M]}(|\tilde{T}_0(y)|) = \frac{c}{M}t_1.$$

Summing up $1^0, 2^0, 3^0$ we find (10). □

Note that for any $I = [0, x) \times [0, y)$ we have

$$\left|\frac{A(I)}{M} - |I|\right| \le y + \frac{1}{M} \tag{19}$$

since $\left|\frac{A(I)}{M} - |I|\right| \le \max\left(\frac{A(I)}{M}, |I|\right)$, $|I| \le y$, $\frac{A(I)}{M} \le \frac{A([0,1)\times[0,y))}{M} = y + \theta$, $|\theta| \le \frac{1}{M}$, where we apply the full period

$$\left\{\frac{n}{M}; n = 0, 1, \ldots, M-1\right\} = \left\{F_M\left(\frac{n}{M}\right) \bmod 1, n = 0, 1, \ldots, M-1\right\}.$$

For $y \in [0, c/M]$ this gives worse estimation $\left|\frac{A(I)}{M} - |I|\right| \le \frac{c}{M} + \frac{1}{M}$.

3. Discrepancy of $f(n) \pmod 1$ for special increasing $f(x)$

Looking for bound of D_M by (10) we must find a bound of

$$D_k^* = \max_{y\in[0,1]} D_k^*(\{Mx_i(y)\}),$$

where $D_k^*(\{Mx_i(y)\})$ is the star discrepancy of the sequence

$$\{Mx_i(y)\} = -\frac{b}{2a} + \sqrt{\frac{M}{a}}\sqrt{\frac{b^2-4ac}{4aM} + i + y} \bmod 1, \quad i = 1, 2, \ldots, k, \tag{20}$$

and $y \in [0,1]$ is fixed but arbitrary, see definition (9). Now, we exclude the term $-\frac{b}{2a}$. We employ that for an arbitrary real sequence $w_1, \ldots, w_N$ and any constant c the extremal discrepancy $D_N(w_n \bmod 1) = D_N(w_n + c \bmod 1)$ and for the star discrepancy $D_N^* \le D_N \le 2D_N^*$, then we have $D_N^*(w_n \bmod 1) \le 2D_N^*(w_n + c \bmod 1)$. Thus

$$D_k^*(\{Mx_i(y)\}) \le 2D_k^*(f(i) \bmod 1)$$

for the star discrepancy of the sequence $f(i) \bmod 1$, $i = 1, 2, \ldots, k$, where

$$f(x) = \sqrt{\frac{M}{a}}\sqrt{\frac{b^2-4ac}{4aM} + x + y} - B, \text{ where} \tag{21}$$

$$B = \left[\sqrt{\frac{M}{a}}\sqrt{\frac{b^2-4ac}{4aM} + 1 + y}\right]$$

and y is fixed but arbitrary in $[0,1]$.

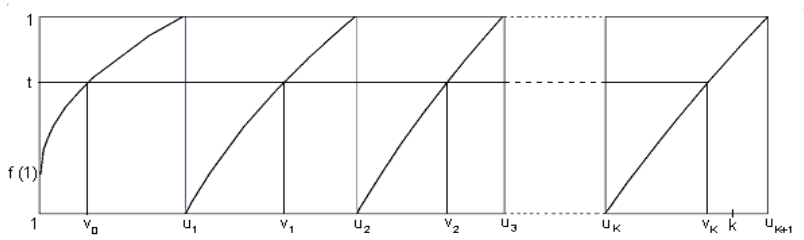

FIGURE 2. Graph of $f(x) \bmod 1$

LEMMA 2. *Let u_i, v_i be two sequences defined by $f(u_i) = i$ and $f(v_i) = t + i$. For given k find K such that $k \in (u_K, u_{K+1}]$. Then the star discrepancy $D_k^*(f(i) \bmod 1)$ satisfies*

$$D_k^* \le \frac{2}{k} + \frac{a}{M}\frac{(K-1)}{k} + 2\frac{u_1}{k} + 2\frac{u_{K+1} - u_K}{k} + 2\frac{(K-1)D_{K-1}^*}{k}, \tag{22}$$

where $D_K^* = \max_{t\in[0,1]} D_K^*(\{v_i\})$.

P r o o f. Abbreviating $A(t) = A([0,t); k; f(i) \bmod 1)$ and by definition

$$D_k^* = \max_{t\in[0,1]} \left| \frac{A(t)}{k} - t \right|.$$

Using Fig. 2, for $t \in [f(1), 1]$, we have

$$\frac{A(t)}{k} - t = \frac{v_0 - \{v_0\}}{k} + \left(\frac{\sum_{i=1}^{K-1}(v_i - u_i)}{k} - t \right) + \frac{\sum_{i=1}^{K-1}(\{u_i\} - \{v_i\})}{k} + \frac{\min(k - u_K + \{u_K\}, v_K - u_K + \{u_K\} - \{v_K\})}{k}, \tag{23}$$

and for $t \in [0, f(1)]$ the first term in (23) must be omitted. From definition of u_i and v_i we have

$$u_i = (i+B)^2 \frac{a}{M} - \frac{b^2 - 4ac}{4aM} - y, \quad v_i = (i+t+B)^2 \frac{a}{M} - \frac{b^2 - 4ac}{4aM} - y, \tag{24}$$

and

$$\frac{v_i - u_i}{u_{i+1} - u_i} = t - \frac{t - t^2}{2i + 2B + 1},$$

which gives

$$\left(\frac{\sum_{i=1}^{K-1}(v_i - u_i)}{k} - t \right) = -t \left((1-t)\frac{a}{M}\frac{K-1}{k} + \frac{u_1}{k} + \frac{k - u_K}{k} \right).$$

Adding

$$\left| \frac{v_0 - \{v_0\}}{k} \right| \le \frac{u_1}{k} + \frac{1}{k},$$

$$\left| \frac{\sum_{i=1}^{K-1}(\{u_i\} - \{v_i\})}{k} \right| \le 2\frac{(K-1)D_{K-1}^*}{k},$$

where $D_K^* = \max(D_K^*(\{u_i\}), D_K^*(\{v_i\}))$ and

$$\frac{\min(k - u_K + \{u_K\}, v_K - u_K + \{u_K\} - \{v_K\})}{k} \le \frac{u_{K+1} - u_K}{k} + \frac{1}{k},$$

we find (22). □

4. Discrepancy of $\left\{(i+t+B)^2\frac{a}{M}\right\}, i=1,2,\dots,K$

For application of (22) we must approximate $D_K^* = \max_{t\in[0,1]} D_K^*(\{v_i(t)\})$ where $D_K^*(\{v_i(t)\})$ is the star discrepancy of the sequence in (24)

$$v_i(t) = (i+t+B)^2\frac{a}{M} - \frac{b^2-4ac}{4aM} - y \bmod 1, \quad i=1,2,\dots,K,$$

and $t\in[0,1]$ is arbitrary but fixed. We see that $D_K^*(\{v_i(t)\}) \le D_K$, where D_K is the extremal discrepancy of the sequence

$$\left\{(i+t+B)^2\frac{a}{M}\right\}, i=1,2,\dots,K,$$

for $t\in[0,1]$.

Lemma 3. *For every $t,y\in[0,1]$ the extremal discrepancy D_K of the sequence $\left\{(i+t+B)^2\frac{a}{M}\right\}, i=1,2,\dots,K$ satisfies*

$$D_K \le 3\left(\frac{1}{\sqrt{M}} + \left(\frac{8}{\sqrt{K}} + 3\frac{\sqrt{M}}{K}\right)(\log M)^{3/2} + \frac{6}{\sqrt{M}}\sum_{h=1}^{[\sqrt{M}]}\frac{1}{h}\sqrt{(ha,M)}\right) \quad (25)$$

assuming that $M \nmid ha$ for $1\le h\le[\sqrt{M}]$.

P r o o f. We start with the result of C. Mauduit and A. Sárközy [MS, p. 207, Lemma 8]:

Lemma 4. *Let α_1,α_2 be any real numbers, p,q be integers such that $q>1$, $\left|\alpha_2-\frac{p}{q}\right| < \frac{1}{q^2}$ and $(p,q)=1$. Then*

$$\left|\sum_{n=1}^{N} e^{2\pi i(\alpha_2 n^2+\alpha_1 n)}\right| \le \left(8\sqrt{N}+3\sqrt{q}\right)\sqrt{\log q} + 6\frac{N}{\sqrt{q}}.$$

Putting $\alpha_1=0$, $\alpha_2=\frac{ha}{M}$ and $\frac{p}{q}=\frac{ha}{M}$, then $\left|\alpha_2-\frac{p}{q}\right| = 0 < \frac{1}{q^2}$, where for coprimality of p and q we give $q=\frac{M}{(ha,M)}$. By Lemma 4, assuming $\frac{M}{(ha,M)}>1$, we have

$$\begin{aligned}\left|\sum_{n=1}^{N} e^{2\pi i h n^2\frac{a}{M}}\right| &\le \left(8\sqrt{N}+3\sqrt{\frac{M}{(ha,M)}}\right)\sqrt{\log\frac{M}{(ha,M)}} + 6\frac{N}{\sqrt{\frac{M}{(ha,M)}}}\\ &\le \left(8\sqrt{N}+3\sqrt{M}\right)\sqrt{\log M} + 6\frac{N}{\sqrt{M}}\sqrt{(ha,M)}. \quad (26)\end{aligned}$$

The same bound holds for $\left|\sum_{n=1}^{N} e^{2\pi i h(n+t+B(y))^2 \frac{a}{M}}\right|$ for every $t, y \in [0,1]$. Applying Erdős-Turán formula, for any positive integer $m \geq 3$ we have

$$D_K \leq 3\left(\frac{1}{m} + \left(\frac{8}{\sqrt{K}} + 3\frac{\sqrt{M}}{K}\right)\sqrt{\log M}.2\log m + \frac{6}{\sqrt{M}}\sum_{h=1}^{m}\frac{1}{h}\sqrt{(ha, M)}\right).$$

Putting $m = [\sqrt{M}]$ we find (25). □

5. Proof of Theorem 1

We use the following four steps:

1^0. Denote by $\tilde{D}_K$ the right-hand side of (25). Because $\tilde{D}_K$ is independent on $t \in [0,1]$, then also $D_K^* = \max_{t\in[0,1]} D_K^*(\{v_i(t)\}) \leq \tilde{D}_K$. Replacing D_{K-1}^* by $\tilde{D}_{K-1}$ in (22) and using $D_k^*(\{Mx_i(y)\}) \leq 2D_k^*(f(i) \bmod 1)$ and that $K\tilde{D}_K$ increases, we find

$$\frac{kD_k^*(\{Mx_i(y)\})}{M} \leq \frac{4}{M} + 2\frac{a}{M}\frac{K}{M} + 4\frac{u_1}{M} + 4\frac{u_{K+1}-u_K}{M} + 4\frac{K\tilde{D}_K}{M}. \tag{27}$$

Then, using $K = f(u_K) \leq f(k)$, $k \leq aM + b$ and by (24) we find

$$K \leq \sqrt{\frac{M}{a}(k-1)} + 1 \leq 2M,$$

$$\frac{u_1}{M} = \frac{1}{M} + \frac{a}{M^2}\left((1+B)^2 - (f(1)+B)^2\right) \leq \frac{6}{M},$$

$$\frac{u_{K+1}-u_K}{M} = \frac{a}{M^2}(2K + 2B + 1) \leq 4\frac{a}{M}.$$

Substituting preceding in (27) we have

$$\frac{kD_k^*(\{Mx_i(y)\})}{M} \leq \frac{28}{M} + 20\frac{a}{M} + 4\frac{K\tilde{D}_K}{M}. \tag{28}$$

The right-hand side of (28) does not depend on $y \in [0,1]$, thus for

$$D_k^* = \max_{y\in[0,1]} D_k^*(\{Mx_i(y)\})$$

we have

$$\max_{1\leq k\leq aM+b}\frac{kD_k^*}{M} \leq \frac{28}{M} + 20\frac{a}{M} + 4\max_{1\leq K\leq 2M}\frac{K\tilde{D}_K}{M}. \tag{29}$$

Here

$$\max_{1\leq K\leq 2M}\frac{K\tilde{D}_K}{M} = 2\tilde{D}_{2M}.$$

Substituting (29) in (10) we have

$$D_M^* < \frac{58}{M} + 40\frac{a}{M} + \frac{c}{M}t_1 + \max_{c/M\le y\le 1}(x_0 - yx_0) + 16\tilde{D}_{2M}, \tag{30}$$

where $D_M^* = D_M^*\left(\frac{n}{M}, F_M\left(\frac{n}{M}\right) \bmod 1\right)$ and

$$\tilde{D}_{2M} = 3\left(\frac{1}{\sqrt{M}} + \left(\frac{8}{\sqrt{2M}} + \frac{3}{2\sqrt{M}}\right)(\log M)^{3/2} + \frac{6}{\sqrt{M}}\sum_{h=1}^{[\sqrt{M}]}\frac{1}{h}\sqrt{(ha, M)}\right). \tag{31}$$

2^0. We simplify (31). We have

$$\sum_{h=1}^{[\sqrt{M}]}\frac{\sqrt{(h,M)}}{h} = \sum_{d|M}\frac{1}{\sqrt{d}}\sum_{h=1,(h,M)=d}^{[\sqrt{M}]}\frac{1}{h/d} \le 3.2^{\omega(M)}\log M$$

because

$$\sum_{d|M}\frac{1}{\sqrt{d}} \le \prod_{p|M}\left(1 - \frac{1}{\sqrt{p}}\right)^{-1} \le 3.2^{\omega(M)},$$

where $\omega(M)$ is the number of distinct prime divisors of M. From this we have

$$\frac{6}{\sqrt{M}}\sum_{h=1}^{[\sqrt{M}]}\frac{1}{h}\sqrt{(ha,M)} \le \frac{6.3\sqrt{(a,M)}}{\sqrt{M}}(\log M)2^{\omega(M)}$$

and we substitute it in (31).

3^0. For $\max_{c/M\le y\le 1}(x_0 - yx_0) = \max_{x\in[0,t_1]} V_0(x)$ we have

$$\max_{x\in[0,t_1]} V_0(x) = \frac{2}{3}\frac{1}{\sqrt{3aM}}\left(\left(\left(1 - \frac{c}{M}\right) + \frac{b^2}{3aM}\right)^{3/2} - \left(\frac{b^2}{3aM}\right)^{3/2}\right) - \left(1 - \frac{c}{M}\right)\frac{b}{3aM} \tag{32}$$

directly and this maximum is required at

$$x = \frac{1}{\sqrt{3aM}}\left(\sqrt{\left(1 - \frac{c}{M}\right) + \frac{b^2}{3aM}} - \sqrt{\frac{b^2}{3aM}}\right).$$

Let us simplify (32) by using Lagrange difference theorem.

If $b < \sqrt{\left(1-\frac{c}{M}\right)3aM}$ then we use

$$\begin{aligned}\max_{x\in[0,t_1]} V_0(x) &\le \frac{2}{3}\frac{1}{\sqrt{3aM}}\left(\left(\left(1-\frac{c}{M}\right)+\frac{b^2}{3aM}\right)^{3/2}-\left(\frac{b^2}{3aM}\right)^{3/2}\right)\\ &= \frac{1}{\sqrt{3aM}}\left(1-\frac{c}{M}\right)\sqrt{\frac{b^2}{3aM}+u}\quad (u\in(0,1-c/M))\\ &< \frac{1}{\sqrt{3aM}}\left(1-\frac{c}{M}\right)^{3/2}\sqrt{2}.\end{aligned}$$

If $b \ge \sqrt{\left(1-\frac{c}{M}\right)3aM}$ and repeating application of Lagrange difference theorem on (32) we find

$$\begin{aligned}\max_{x\in[0,t_1]} V_0(x) &= \left(1-\frac{c}{M}\right)\frac{1}{\sqrt{3aM}}u\frac{1}{2\sqrt{\frac{b^2}{3aM}+v}}\quad (u\in(0,1-c/M), v\in(0,u))\\ &\le \left(1-\frac{c}{M}\right)^2\frac{1}{2b} \le \frac{1}{\sqrt{3aM}}\left(1-\frac{c}{M}\right)^{3/2}\frac{1}{2}.\end{aligned}$$

Altogether

$$\max_{x\in[0,t_1]} V_0(x) \le \sqrt{2}\frac{1}{\sqrt{3aM}}\left(1-\frac{c}{M}\right)^{3/2}. \tag{33}$$

4^0. Now, we simplify $\frac{c}{M}t_1$, where t_1 defined in (9) can also be rewritten as

$$t_1 = \frac{1}{\sqrt{aM}}\left(\sqrt{\left(1-\frac{c}{M}\right)+\frac{b^2}{4aM}}-\sqrt{\frac{b^2}{4aM}}\right).$$

If $b < \sqrt{\left(1-\frac{c}{M}\right)4aM}$ we see

$$t_1 < \frac{1}{\sqrt{aM}}\sqrt{\left(1-\frac{c}{M}\right)+\frac{b^2}{4aM}} \le \frac{1}{\sqrt{aM}}\left(1-\frac{c}{M}\right)^{1/2}\sqrt{2}.$$

If $b \ge \sqrt{\left(1-\frac{c}{M}\right)4aM}$ we see

$$\begin{aligned}t_1 &= \frac{1}{\sqrt{aM}}\left(1-\frac{c}{M}\right)\frac{1}{2}\frac{1}{\sqrt{\frac{b^2}{4aM}+u}}\quad (u\in(0,1-c/M))\\ &\le \left(1-\frac{c}{M}\right)\frac{1}{b} \le \frac{1}{\sqrt{aM}}\left(1-\frac{c}{M}\right)^{1/2}\frac{1}{2}.\end{aligned}$$

Summarizing

$$\frac{c}{M}t_1 \le \sqrt{2}\frac{1}{\sqrt{aM}}\frac{c}{M}\left(1-\frac{c}{M}\right)^{1/2}. \tag{34}$$

Finally, all above results give (7).

6. Concluding remarks

1^0. For lower bound of $D_M(x_n, x_{n+1})$ in Fig. 1 we see that the intervals $I_1 = [0, x) \times (y, 1]$ and $|I_2| = [x, t_1) \times [0, y)$ do not contain any point of (8) and thus the extremal discrepancy D_M of (8) satisfies

$$D_M \geq \max(\max_{x\in[0,t_1]} |I_1|, \max_{x\in[0,t_1]} |I_2|)$$

Furthermore, directly from definitions we have $V_0(x) = |I_1|$ and $T_0(x) = |I_1| - |I_2|$. Thus, we can use

$$D_M \geq \max(\max_{x\in[0,t_1]} V_0(x), |T_0(0)|),$$

where $|T_0(0)| = \frac{c}{M} t_1$, but it is worse than in [EHN1] and [S].

2^0. H. Niederreiter [N2] proved the following quantitative form of well-known Fejer's theorem: If a function $f(x)$, $x \geq 1$, satisfies

(i) $f(x) \to \infty$ monotonically,

(ii) $xf'(x) \to \infty$,

(iii) $f'(x) \to 0$ monotonically as $x \to \infty$,

then the star discrepancy D_k^* of the sequence $f(i) \bmod 1$, $i = 1, 2, \ldots, k$ satisfies

$$D_k^* = O\left(\frac{f(k)}{k} + \frac{1}{kf'(k)}\right). \tag{35}$$

This can be employed for $f(x) = \sqrt{x}$. Our function in (21) also satisfies (i)–(iii), but for the left-hand side of (29) the (35) gives

$$\begin{aligned}\max_{1\leq k\leq aM+b} \frac{kD_k^*}{M} &= O\left(\frac{f(aM+b)}{M} + \frac{1}{Mf'(aM+b)}\right)\\ &= O\left(\frac{1}{M}\sqrt{\frac{b^2}{4aM} + \left(1 - \frac{c}{M}\right) + aM + b}\left(\sqrt{\frac{M}{a}} + 2\sqrt{\frac{a}{M}}\right)\right),\end{aligned}$$

where $\frac{1}{M}\sqrt{aM+b}\sqrt{\frac{M}{a}} > 1$.

3^0. Finally, we compare order of magnitudes of upper bounds in (4), (5), (6) and (7):

In (4) we have $\frac{(\log M)^2}{\sqrt{M}}$ for $M = 2^\alpha$,

in (5) we have $\frac{(\log M)^2}{\sqrt{pM}} + \sqrt{\frac{p}{M}}$ for $M = p^\alpha$,

in (6) we have $\frac{(\log M)^2}{\sqrt{PM}} + \sqrt{\frac{P}{M}}$ for $M = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ and $P = p_1 \dots p_r$, and

in (7) we have $\frac{(\log M)^{3/2}}{\sqrt{M}} + \frac{\sqrt{(a,M)}}{\sqrt{M}}(\log M)2^{\omega(M)} + \frac{a}{M}$.

Replacing the modulus M by M^α, for sufficiently large integer exponent α, we see that the order in (7) is better than in (4), (5) and (6), in this case.

REFERENCES

[DT] DRMOTA, M.–TICHY, R. F.: *Sequences, Discrepancies and Applications*, Lecture Notes in Mathematics **1651**, Springer-Verlag, Berlin, Heidelberg, 1997.

[EHHW] EICHENAUER-HERRMANN, J. – HERRMANN, E. – WEGENKITTL, S.: *A survey of quadratic and inverse congruential pseudorandom numbers*, in:*Monte Carlo and Quasi–Monte Carlo Methods 1996* (Proceedings of a conference at the University of Salzburg, Austria, July 9–12, 1996), eds. H. Niederreiter, P. Hellekalek, G. Larcher and P. Zinterhof. Lecture Notes in Statistics **127**, Springer Verlag, New York, Berlin, 1998, pp. 66–97 (MR 99d:11085).

[EHN1] EICHENAUER-HERRMANN, J. – NIEDERREITER, H.: *On the discrepancy of quadratic congruential pseudorandom numbers*, J. Comput. Appl. Math. **34** (1991), no. 2, 243–249 (MR 92c:65010).

[EHN2] EICHENAUER-HERRMANN, J. – NIEDERREITER, H.: *An improved upper bound for the discrepancy of quadratic congruential pseudorandom numbers*, Acta Arith. **69** (1995), no. 2, 193–198 (MR 95k:11099).

[K] KNUTH, D.E.: *Seminumerical Algorithms. The Art of Computer Programming, Vol 2, 2nd*, Addison Wesley,Reading, MA, 1981. (First ed.: Reading, MA, 1969 (MR **44**#3531)) Russian translation Izd. Mir, Moscow, 1977.

[KN] KUIPERS, L.– NIEDERREITER, H.: *Uniform Distribution of Sequences*, John Wiley & Sons, New York, 1974. Reprint edition Dover Publications, Inc. Mineola, New York, 2006.

[MS] MAUDUIT, C. – SÁRKÖZY, A.: *On finite pseudorandom binary sequences, V. On* $(n\alpha)$ *and* $(n^2\alpha)$ *sequences*, Monatsh. Math. **129** (2000), 197–216.

[N] NIEDERREITER, H.: *Random Number Generation and Quasi–Monte Carlo Methods*, CBMS–NSF Regional Conference Series in Applied Mathematics **63**, Society for Industrial and Applied Mathematics, Philadelphia, PA, 1992.

[N2] NIEDERREITER, H.: *Almost-arithmetic progressions and uniform distribution*, Trans. Amer. Math. Soc. **161** (1971), 283–291.

[S] STRANDT, S.: *Quadratic congruential generators with odd composite modulus*, in:*Monte Carlo and Quasi–Monte Carlo Methods 1996* (Proceedings of a conference at the University of Salzburg, Austria, July 9–12, 1996), eds. H. Niederreiter, P. Hellekalek, G. Larcher and P. Zinterhof. Lecture Notes in Statistics **127**, Springer Verlag, New York, Berlin, 1998, pp. 415–426 (MR MR 99d:65024).

[SP] STRAUCH, O.– PORUBSKÝ, Š.: *Distribution of Sequences: A Sampler*, Peter Lang, Frankfurt am Main, 2005.

Received October 9, 2007
Accepted December 21, 2007

Oľga Blažeková
Mathematical Institute
Slovak Academy of Sciences
Štefánikova 49
SK-814 73 Bratislava
SLOVAKIA
E-mail: olgablazekova@gmail.com

Oto Strauch
Mathematical Institute
Slovak Academy of Sciences
Štefánikova 49
SK-814 73 Bratislava
SLOVAKIA
E-mail: strauch@mat.savba.sk