

Parallel Streams of Nonlinear Congruential Pseudorandom Numbers

Jürgen Eichenauer-Herrmann

*Fachbereich Mathematik, Technische Hochschule, Schlossgartenstrasse 7,
D-64289 Darmstadt, Germany*

and

Harald Niederreiter

*Institute of Information Processing, Austrian Academy of Sciences, Sonnenfelsgasse 19,
A-1010 Vienna, Austria*

E-mail: niederreiter@oeaw.ac.at

Communicated by Peter Jau-Shyong Shiue

Received June 28, 1996; revised January 23, 1997

This paper deals with the general nonlinear congruential method for generating uniform pseudorandom numbers, in which permutation polynomials over finite prime fields play an important role. It is known that these pseudorandom numbers exhibit an attractive equidistribution and statistical independence behavior. In the context of parallelized simulation methods, a large number of parallel streams of pseudorandom numbers with strong mutual statistical independence properties are required. In the present paper, such properties of parallelized nonlinear congruential generators are studied based on the discrepancy of certain point sets. Upper and lower bounds for the discrepancy both over the full period and over (sufficiently large) parts of the period are established. The method of proof rests on the classical Weil bound for exponential sums. © 1997 Academic Press

1. INTRODUCTION

Nonlinear congruential methods for generating uniform pseudorandom numbers in the interval $[0, 1)$ have been studied intensively during the last years. Reviews of the development of this area can be found in the survey articles [2, 5, 10, 14, 17] and in the monograph [15]. The present paper

concentrates on the general nonlinear congruential method with prime modulus. Pseudorandom numbers within the generated sequences have nice equidistribution and statistical independence properties [3, 4, 6–8, 13]. Nowadays, the growing field of parallel computing has a need for generating many parallel streams of uniform pseudorandom numbers with mutual statistical independence properties. This important task provides the motivation for the following analysis of a parallelized version of the general nonlinear congruential method.

Let $p \geq 5$ be an arbitrary prime, and identify $\mathbb{Z}_p = \{0, 1, \dots, p-1\}$ with the finite field of order p . Let $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$ denote its multiplicative group. For $i \in \{1, \dots, s\}$ with $s \geq 2$, let $g_i: \mathbb{Z} \rightarrow \mathbb{Z}_p$ be a monic permutation polynomial of \mathbb{Z}_p with $g_i(0) = 0$ and degree d_i as a polynomial over \mathbb{Z}_p , where $3 \leq d_i \leq p-2$ is assumed in order to avoid trivial and uninteresting cases. The reader is referred to [11] for an introduction to the theory of permutation polynomials over finite fields. For parameters $a_i \in \mathbb{Z}_p^*$ and $b_i \in \mathbb{Z}_p$, a *nonlinear congruential sequence* $(y_n^{(i)})_{n \geq 0}$ of elements of \mathbb{Z}_p is defined by

$$y_n^{(i)} \equiv a_i g_i(n) + b_i \pmod{p}, \quad n \geq 0,$$

and a sequence $(x_n^{(i)})_{n \geq 0}$ of *nonlinear congruential pseudorandom numbers* in the interval $[0, 1)$ is obtained from $x_n^{(i)} = y_n^{(i)}/p$ for $n \geq 0$. Obviously, these sequences are purely periodic with period length p and $\{y_0^{(i)}, y_1^{(i)}, \dots, y_{p-1}^{(i)}\} = \mathbb{Z}_p$.

In the following, mutual statistical independence properties of the parallel streams $(x_n^{(i)})_{n \geq 0}$ of uniform pseudorandom numbers are studied based on the equidistribution behavior of the s -tuples

$$\mathbf{x}_n = (x_n^{(1)}, \dots, x_n^{(s)}) \in [0, 1)^s, \quad n \geq 0,$$

which can be analyzed by the discrepancy of corresponding point sets in $[0, 1)^s$. For N arbitrary points $\mathbf{t}_0, \mathbf{t}_1, \dots, \mathbf{t}_{N-1} \in [0, 1)^s$, the *discrepancy* is defined by

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

where the supremum is extended over all subintervals J of $[0, 1)^s$, $F_N(J)$ is N^{-1} times the number of points among $\mathbf{t}_0, \mathbf{t}_1, \dots, \mathbf{t}_{N-1}$ falling into J , and $V(J)$ denotes the s -dimensional volume of J . It should be observed that the discrepancy of N true random points from $[0, 1)^s$ is almost always of an order of magnitude $N^{-1/2}(\log \log N)^{1/2}$ according to Kiefer's probabilistic

law of the iterated logarithm for discrepancies [9]. Subsequently, for $1 \leq N \leq p$, the abbreviation

$$D_N^{(s)} = D_N(\mathbf{x}_0, \mathbf{x}_1, \dots, \mathbf{x}_{N-1})$$

will be used. In the third section, upper and lower bounds for the discrepancy $D_p^{(s)}$ over the full period are established and discussed. Additionally, parts of the period are studied, and upper and lower bounds for the discrepancy $D_N^{(s)}$ with $N < p$ are given in the fourth section. In the fifth section, an upper bound for the average value of these discrepancies is presented. The second section contains some basic auxiliary results.

2. AUXILIARY RESULTS

Subsequently, for integers $k \geq 1$ and $q \geq 2$, let $C_k(q)$ be the set of all nonzero lattice points $(h_1, \dots, h_k) \in \mathbb{Z}^k$ with $-q/2 < h_j \leq q/2$ for $1 \leq j \leq k$. Define

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

and

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

for $\mathbf{h} = (h_1, \dots, h_k) \in C_k(q)$. For real t , the abbreviation $e(t) = e^{2\pi it}$ will be used, and $\mathbf{u} \cdot \mathbf{v}$ stands for the standard inner product of $\mathbf{u}, \mathbf{v} \in \mathbb{R}^k$.

The following five results are known. The first one follows from [12, Lemma 2.2]; see also [15, Theorem 3.10]. Lemma 2 can be deduced from [16, Lemma 3]; see also [1, Theorem 1; 15, Corollary 3.11]. Lemma 3 follows from [15, Corollary 3.17], and Lemma 4 is a special version of the classical Weil [18] bound for exponential sums; see also [11, Theorem 5.38]. Finally, Lemma 5 is cited from [8, Lemma 3].

LEMMA 1. *Let $N \geq 1$ and $q \geq 2$ be integers. Let $\mathbf{t}_n = \mathbf{y}_n/q$ with $\mathbf{y}_n \in \{0, 1, \dots, q-1\}^k$ for $0 \leq n < N$ be points in $[0, 1)^k$. Then the discrepancy of the points $\mathbf{t}_0, \mathbf{t}_1, \dots, \mathbf{t}_{N-1}$ satisfies*

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

LEMMA 2. Let $p \geq 5$ be a prime, let $N \geq 1$ be an integer, and let $\mathbf{t}_n = \mathbf{y}_n/p$ with $\mathbf{y}_n \in \mathbb{Z}_p^k$ for $0 \leq n < N$ be points in $[0, 1)^k$. Suppose the real number B is such that

$$\left| \sum_{n=0}^{N-1} e(\mathbf{h} \cdot \mathbf{t}_n) \right| \leq B$$

for all lattice points $\mathbf{h} \in \mathbb{Z}^k$ with $\mathbf{h} \not\equiv \mathbf{0} \pmod{p}$. Then the discrepancy of the points $\mathbf{t}_0, \mathbf{t}_1, \dots, \mathbf{t}_{N-1}$ satisfies

$$D_N(\mathbf{t}_0, \mathbf{t}_1, \dots, \mathbf{t}_{N-1}) \leq \frac{k}{p} + \frac{B}{N} \left(\frac{4}{\pi^2} \log p + 1.38 + \frac{0.64}{p} \right)^k.$$

LEMMA 3. The discrepancy of N arbitrary points $\mathbf{t}_0, \mathbf{t}_1, \dots, \mathbf{t}_{N-1} \in [0, 1)^k$ satisfies

$$D_N(\mathbf{t}_0, \mathbf{t}_1, \dots, \mathbf{t}_{N-1}) \geq \frac{\pi}{2N((\pi + 1)^l - 1) \prod_{j=1}^k \max(1, |h_j|)} \left| \sum_{n=0}^{N-1} e(\mathbf{h} \cdot \mathbf{t}_n) \right|$$

for any nonzero lattice point $\mathbf{h} = (h_1, \dots, h_k) \in \mathbb{Z}^k$, where l denotes the number of nonzero coordinates of \mathbf{h} .

LEMMA 4. Let $p \geq 3$ be a prime. Let $Q : \mathbb{Z} \rightarrow \mathbb{Z}_p$ be a polynomial with $\deg(Q) \geq 1$ as a polynomial over \mathbb{Z}_p . Then

$$\left| \sum_{z \in \mathbb{Z}_p} e(Q(z)/p) \right| \leq (\deg(Q) - 1)p^{1/2}.$$

LEMMA 5. Let $1 \leq N \leq q$ be integers. Let $\mathbf{t}_0, \mathbf{t}_1, \dots, \mathbf{t}_{q-1} \in [0, 1)^k$ be arbitrary points, and put $\tilde{\mathbf{t}}_n = (n/q, \mathbf{t}_n) \in [0, 1)^{k+1}$ for $0 \leq n < q$. Then the discrepancies of the two point sets $\mathbf{t}_0, \mathbf{t}_1, \dots, \mathbf{t}_{N-1}$ and $\tilde{\mathbf{t}}_0, \tilde{\mathbf{t}}_1, \dots, \tilde{\mathbf{t}}_{q-1}$ satisfy

$$D_N(\mathbf{t}_0, \mathbf{t}_1, \dots, \mathbf{t}_{N-1}) \leq \frac{q}{N} D_q(\tilde{\mathbf{t}}_0, \tilde{\mathbf{t}}_1, \dots, \tilde{\mathbf{t}}_{q-1}).$$

3. DISCREPANCY OVER THE FULL PERIOD

In the following, the abbreviations $d = \max\{d_1, \dots, d_s\}$ and $\tilde{d} = \max\{d_1, d_2\}$ will be used, where d_1, \dots, d_s are the degrees of the underlying permutation polynomials g_1, \dots, g_s in the parallelized nonlinear congruential method.

THEOREM 1. *Let g_1, \dots, g_s be linearly independent over \mathbb{Z}_p . Then the discrepancy $D_p^{(s)}$ over the full period in the parallelized nonlinear congruential method satisfies*

$$D_p^{(s)} \leq (d-1)p^{-1/2} \left(\frac{4}{\pi^2} \log p + 1.38 + \frac{0.64}{p} \right)^s + \frac{s}{p}$$

for all parameters $a_1, \dots, a_s \in \mathbb{Z}_p^*$ and $b_1, \dots, b_s \in \mathbb{Z}_p$.

Proof. First, for $\mathbf{h} = (h_1, \dots, h_s) \in \mathbb{Z}^s$, put

$$S(\mathbf{h}) = \sum_{n=0}^{p-1} e(\mathbf{h} \cdot \mathbf{x}_n).$$

Then a short calculation shows that

$$\begin{aligned} |S(\mathbf{h})| &= \left| \sum_{n=0}^{p-1} e \left(\sum_{i=1}^s h_i y_n^{(i)} / p \right) \right| \\ &= \left| \sum_{n=0}^{p-1} e \left(\sum_{i=1}^s h_i a_i g_i(n) / p \right) \right| \\ &= \left| \sum_{z \in \mathbb{Z}_p} e(Q(\mathbf{h}; z) / p) \right|, \end{aligned}$$

where the polynomial $Q(\mathbf{h}; \cdot) : \mathbb{Z} \rightarrow \mathbb{Z}_p$ is defined by

$$Q(\mathbf{h}; z) \equiv h_1 a_1 g_1(z) + \dots + h_s a_s g_s(z) \pmod{p}.$$

Since $Q(\mathbf{h}; 0) = 0$ and g_1, \dots, g_s are linearly independent over \mathbb{Z}_p , the polynomial $Q(\mathbf{h}; \cdot)$ is nonconstant over \mathbb{Z}_p for all lattice points $\mathbf{h} \in \mathbb{Z}^s$ with $\mathbf{h} \not\equiv \mathbf{0} \pmod{p}$. Therefore, Weil's bound for exponential sums in Lemma 4 (with $Q = Q(\mathbf{h}; \cdot)$) implies that

$$|S(\mathbf{h})| \leq (\deg(Q(\mathbf{h}; \cdot)) - 1)p^{1/2} \leq (d-1)p^{1/2}$$

for all lattice points $\mathbf{h} \in \mathbb{Z}^s$ with $\mathbf{h} \not\equiv \mathbf{0} \pmod{p}$. Hence, Lemma 2 can be applied with $N = p$, $k = s$, $t_n = \mathbf{x}_n$ for $0 \leq n < p$, and $B = (d-1)p^{1/2}$. This yields the desired result. ■

THEOREM 2. *Let g_1, g_2 be linearly independent over \mathbb{Z}_p . Let $0 < t \leq \sqrt{p/(p-1)}$ and $a_2 \in \mathbb{Z}_p^*$ be fixed. Then there exist more than $(p - (p-1)t^2)/((\tilde{d}-1)^2 - t^2)$ values of $a_1 \in \mathbb{Z}_p^*$ such that the discrepancy $D_p^{(s)}$ over the full period in the parallelized nonlinear congruential method satisfies*

$$D_p^{(s)} \geq \frac{t}{2(\pi+2)} p^{-1/2}$$

for all permutation polynomials g_3, \dots, g_s and all parameters $a_3, \dots, a_s \in \mathbb{Z}_p^*$ and $b_1, \dots, b_s \in \mathbb{Z}_p$.

Proof. First, for $a_1 \in \mathbb{Z}_p$, put

$$T(a_1) = \sum_{n=0}^{p-1} e((a_1 g_1(n) + a_2 g_2(n))/p).$$

Since g_2 is a permutation polynomial over \mathbb{Z}_p , one obtains $T(0) = 0$. Hence, a short calculation shows that

$$\begin{aligned} \sum_{a_1 \in \mathbb{Z}_p^*} |T(a_1)|^2 &= \sum_{a_1 \in \mathbb{Z}_p} |T(a_1)|^2 \\ &= \sum_{a_1 \in \mathbb{Z}_p} \sum_{k,n=0}^{p-1} e((a_1(g_1(k) - g_1(n)) + a_2(g_2(k) \\ &\quad - g_2(n)))/p) \\ &= \sum_{k,n=0}^{p-1} e(a_2(g_2(k) - g_2(n))/p) \sum_{a_1 \in \mathbb{Z}_p} e(a_1(g_1(k) \\ &\quad - g_1(n))/p) = p^2, \end{aligned}$$

where the last equality follows from the fact that the inner sum over a_1 is p for $k = n$ and 0 for $k \neq n$. Now, let $A(t)$ denote the number of values of $a_1 \in \mathbb{Z}_p^*$ with $|T(a_1)| \geq tp^{1/2}$. Since g_1, g_2 are linearly independent over \mathbb{Z}_p , it follows as in the proof of Theorem 1 that $|T(a_1)| \leq (\tilde{d}-1)p^{1/2}$ for all $a_1 \in \mathbb{Z}_p^*$. Therefore,

$$\begin{aligned} \sum_{a_1 \in \mathbb{Z}_p^*} |T(a_1)|^2 &= \sum_{\substack{a_1 \in \mathbb{Z}_p^* \\ |T(a_1)| \geq tp^{1/2}}} |T(a_1)|^2 + \sum_{\substack{a_1 \in \mathbb{Z}_p^* \\ |T(a_1)| < tp^{1/2}}} |T(a_1)|^2 < A(t)(\tilde{d}-1)^2 p \\ &\quad + (p-1-t^2)p \\ &= A(t)((\tilde{d}-1)^2 - t^2)p + (p-1)t^2 p, \end{aligned}$$

which implies that $A(t) > (p - (p - 1)t^2)/((\tilde{d} - 1)^2 - t^2)$. Finally, Lemma 3 is applied with $N = p$, $k = s$, $\mathbf{t}_n = \mathbf{x}_n$ for $0 \leq n < p$, and $\mathbf{h} = (1, 1, 0, \dots, 0) \in \mathbb{Z}^s$. This yields

$$\begin{aligned} D_p^{(s)} &\geq \frac{1}{2(\pi + 2)p} \left| \sum_{n=0}^{p-1} e(\mathbf{h} \cdot \mathbf{x}_n) \right| \\ &= \frac{1}{2(\pi + 2)p} \left| \sum_{n=0}^{p-1} e((y_n^{(1)} + y_n^{(2)})/p) \right| = \frac{1}{2(\pi + 2)p} |T(a_1)|. \end{aligned}$$

Hence, there exist more than $(p - (p - 1)t^2)/((\tilde{d} - 1)^2 - t^2)$ values of $a_1 \in \mathbb{Z}_p^*$ with

$$D_p^{(s)} \geq \frac{t}{2(\pi + 2)} p^{-1/2},$$

which is the desired result. ■

The upper bound in Theorem 1 for the discrepancy $D_p^{(s)}$ over the full period is independent of both the parameters $a_1, \dots, a_s, b_1, \dots, b_s$ and the specific choice of the permutation polynomials g_1, \dots, g_s in the parallelized nonlinear congruential method, as long as g_1, \dots, g_s are linearly independent over \mathbb{Z}_p with maximal degree d . This upper bound is of the order of magnitude $dp^{-1/2}(\log p)^s$, which fits well the asymptotic behavior of the discrepancy of p true random points from $[0, 1)^s$ according to the law of the iterated logarithm, provided the maximal degree d is bounded. In general, the upper bound for $D_p^{(s)}$ is the best possible up to the logarithmic factor, since Theorem 2 implies that, for any underlying permutation polynomials with bounded degree \tilde{d} , there exists a positive fraction of the parameters in the parallelized nonlinear congruential method such that $D_p^{(s)}$ is of an order of magnitude at least $p^{-1/2}$. The upper bound for $D_p^{(s)}$ could suggest that a small value of the maximal degree d is most favorable. However, it should be observed that the number of parallel streams is bounded by d , since the underlying permutation polynomials g_1, \dots, g_s are assumed to be linearly independent over \mathbb{Z}_p . Additionally, it is not known whether the dependence of the upper bound on d is the best possible.

4. DISCREPANCY OVER PARTS OF THE PERIOD

Subsequently, let a polynomial $g_0 : \mathbb{Z} \rightarrow \mathbb{Z}_p$ be defined by $g_0(z) \equiv z \pmod{p}$.

THEOREM 3. *Let g_0, g_1, \dots, g_s be linearly independent over \mathbb{Z}_p . Then the discrepancy $D_N^{(s)}$ over parts of the period in the parallelized nonlinear congruential method satisfies*

$$D_N^{(s)} \leq \frac{(d-1)p^{1/2}}{N} \left(\frac{4}{\pi^2} \log p + 1.38 + \frac{0.64}{p} \right)^{s+1} + \frac{s+1}{N}$$

for $1 \leq N < p$ and all parameters $a_1, \dots, a_s \in \mathbb{Z}_p^*$ and $b_1, \dots, b_s \in \mathbb{Z}_p$.

Proof. First, for $\tilde{\mathbf{h}} = (h_0, \mathbf{h}) = (h_0, h_1, \dots, h_s) \in \mathbb{Z}^{s+1}$, put

$$\tilde{S}(\tilde{\mathbf{h}}) = \sum_{n=0}^{p-1} e(\mathbf{h} \cdot \mathbf{x}_n + h_0 n/p).$$

Then a short calculation shows that

$$\begin{aligned} |\tilde{S}(\tilde{\mathbf{h}})| &= \left| \sum_{n=0}^{p-1} e \left(\left(h_0 n + \sum_{i=1}^s h_i y_n^{(i)} \right) / p \right) \right| \\ &= \left| \sum_{n=0}^{p-1} e \left(\left(h_0 n + \sum_{i=1}^s h_i a_i g_i(n) \right) / p \right) \right| \\ &= \left| \sum_{z \in \mathbb{Z}_p} e(\tilde{Q}(\tilde{\mathbf{h}}; z)/p) \right|, \end{aligned}$$

where the polynomial $\tilde{Q}(\tilde{\mathbf{h}}; \cdot) : \mathbb{Z} \rightarrow \mathbb{Z}_p$ is defined by

$$\tilde{Q}(\tilde{\mathbf{h}}; z) \equiv h_0 g_0(z) + h_1 a_1 g_1(z) + \dots + h_s a_s g_s(z) \pmod{p}.$$

Since $\tilde{Q}(\tilde{\mathbf{h}}; 0) = 0$ and g_0, g_1, \dots, g_s are linearly independent over \mathbb{Z}_p , the polynomial $\tilde{Q}(\tilde{\mathbf{h}}; \cdot)$ is nonconstant over \mathbb{Z}_p for all lattice points $\tilde{\mathbf{h}} \in \mathbb{Z}^{s+1}$ with $\tilde{\mathbf{h}} \not\equiv \mathbf{0} \pmod{p}$. Therefore, Weil's bound for exponential sums in Lemma 4 (with $Q = \tilde{Q}(\tilde{\mathbf{h}}; \cdot)$) implies that

$$|\tilde{S}(\tilde{\mathbf{h}})| \leq (\deg(\tilde{Q}(\tilde{\mathbf{h}}; \cdot)) - 1)p^{1/2} \leq (d-1)p^{1/2}$$

for all lattice points $\mathbf{h} \in \mathbb{Z}^{s+1}$ with $\mathbf{h} \not\equiv \mathbf{0} \pmod{p}$. Hence, Lemma 2 can be applied with $N = p$, $k = s + 1$, $\mathbf{t}_n = \mathbf{x}_n = (n/p, \mathbf{x}_n)$ for $0 \leq n < p$, and $B = (d - 1)p^{1/2}$. This yields

$$D_p(\mathbf{x}_0, \mathbf{x}_1, \dots, \mathbf{x}_{p-1}) \leq \frac{s+1}{p} + (d-1)p^{-1/2} \left(\frac{4}{\pi^2} \log p + 1.38 + \frac{0.64}{p} \right)^{s+1}.$$

Finally, Lemma 5 is used with $q = p$, $k = s$, and $\mathbf{t}_n = \mathbf{x}_n$ for $0 \leq n < p$, which completes the proof. ■

THEOREM 4. *Let g_0, g_1, g_2 be linearly independent over \mathbb{Z}_p . Let $1 \leq N < p$ and $0 < t \leq \sqrt{(p^2 - 2p + N)/(p - 1)^2}$ be fixed. Then there exist more than*

$$C_N(t) = \frac{p^2 - 2p + N - (p - 1)^2 t^2}{(\tilde{d} - 1)^2 (p/N) ((4/\pi^2) \log p + 1.38)^2 - t^2}$$

ordered pairs $(a_1, a_2) \in \mathbb{Z}_p^ \times \mathbb{Z}_p^*$ such that the discrepancy $D_N^{(s)}$ over parts of the period in the parallelized nonlinear congruential method satisfies*

$$D_N^{(s)} \geq \frac{t}{2(\pi + 2)} N^{-1/2}$$

for all permutation polynomials g_3, \dots, g_s and all parameters $a_3, \dots, a_s \in \mathbb{Z}_p^$ and $b_1, \dots, b_s \in \mathbb{Z}_p$.*

Proof. First, for $a_1, a_2 \in \mathbb{Z}_p$ and $1 \leq N < p$, put

$$T_N(a_1, a_2) = \sum_{n=0}^{N-1} e((a_1 g_1(n) + a_2 g_2(n))/p).$$

(i) Subsequently, an upper bound for $|T_N(a_1, a_2)|$ with $a_1, a_2 \in \mathbb{Z}_p^*$ is established. Straightforward calculations show that

$$\begin{aligned} T_N(a_1, a_2) &= \sum_{n=0}^{p-1} e((a_1 g_1(n) + a_2 g_2(n))/p) \sum_{k=0}^{N-1} \frac{1}{p} \sum_{u=0}^{p-1} e(u(n-k)/p) \\ &= \frac{1}{p} \sum_{u=0}^{p-1} \left(\sum_{k=0}^{N-1} e(-ku/p) \right) \left(\sum_{n=0}^{p-1} e((un + a_1 g_1(n) + a_2 g_2(n))/p) \right), \end{aligned}$$

where the first equality follows from the fact that on the right-hand side the sum over k is 1 for $0 \leq n < N$ and 0 for $N \leq n < p$. Hence, one obtains

$$|T_N(a_1, a_2)| \leq \frac{1}{p} \sum_{u=0}^{p-1} \left| \sum_{k=0}^{N-1} e(ku/p) \right| \left| \sum_{z \in \mathbb{Z}_p} e(Q(u; z)/p) \right|,$$

where the polynomial $Q(u; \cdot) : \mathbb{Z} \rightarrow \mathbb{Z}_p$ is defined by

$$Q(u; z) \equiv ug_0(z) + a_1g_1(z) + a_2g_2(z) \pmod{p}.$$

Since $Q(u; 0) = 0$ and g_0, g_1, g_2 are linearly independent over \mathbb{Z}_p , the polynomial $Q(u; \cdot)$ is nonconstant over \mathbb{Z}_p for all $u \in \mathbb{Z}$. Therefore, Weil's bound in Lemma 4 (with $Q = Q(u; \cdot)$) implies that

$$\left| \sum_{z \in \mathbb{Z}_p} e(Q(u; z)/p) \right| \leq (\deg(Q(u; \cdot)) - 1)p^{1/2} \leq (\tilde{d} - 1)p^{1/2}$$

for all $u \in \mathbb{Z}$. This yields

$$\begin{aligned} |T_N(a_1, a_2)| &\leq (\tilde{d} - 1)p^{1/2} \left(\frac{N}{p} + \frac{1}{p} \sum_{u=1}^{p-1} \left| \sum_{k=0}^{N-1} e(ku/p) \right| \right) \\ &= (\tilde{d} - 1)p^{1/2} \left(\frac{N}{p} + \frac{1}{p} \sum_{u=1}^{p-1} \left| \frac{\sin(\pi u N/p)}{\sin(\pi u/p)} \right| \right) \\ &< (\tilde{d} - 1)p^{1/2} \left(\frac{N}{p} + \frac{4}{\pi^2} \log p + 0.38 + \frac{0.64}{p} \right) \\ &< (\tilde{d} - 1)p^{1/2} \left(\frac{4}{\pi^2} \log p + 1.38 \right), \end{aligned}$$

where [1, Theorem 1] was used in the penultimate step.

(ii) Since g_1, g_2 are permutation polynomials over \mathbb{Z}_p , a short calculation shows that

$$\sum_{a_1, a_2 \in \mathbb{Z}_p^*} |T_N(a_1, a_2)|^2 = \sum_{\substack{a_1 \in \mathbb{Z}_p^* \\ a_2 \in \mathbb{Z}_p^*}} |T_N(a_1, a_2)|^2 - \sum_{a_2 \in \mathbb{Z}_p} |T_N(0, a_2)|^2 + |T_N(0, 0)|^2$$

$$\begin{aligned}
&= \sum_{k,n=0}^{N-1} \left(\sum_{a_1 \in \mathbb{Z}_p} e(a_1(g_1(k) - g_1(n))/p) \right) \left(\sum_{a_2 \in \mathbb{Z}_p^*} e(a_2(g_2(k) - g_2(n))/p) \right) \\
&\quad - \sum_{k,n=0}^{N-1} \sum_{a_2 \in \mathbb{Z}_p} e(a_2(g_2(k) - g_2(n))/p) + N^2 \\
&= p(p-1)N - pN + N^2 = (p^2 - 2p + N)N.
\end{aligned}$$

(iii) Now, let $A_N(t)$ denote the number of ordered pairs $(a_1, a_2) \in \mathbb{Z}_p^* \times \mathbb{Z}_p^*$ with $|T_N(a_1, a_2)| \geq tN^{1/2}$. Then it follows from the results in (i) and (ii) that

$$\begin{aligned}
\sum_{a_1, a_2 \in \mathbb{Z}_p^*} |T_N(a_1, a_2)|^2 &= \sum_{\substack{a_1, a_2 \in \mathbb{Z}_p^* \\ |T_N(a_1, a_2)| \geq tN^{1/2}}} |T_N(a_1, a_2)|^2 + \sum_{\substack{a_1, a_2 \in \mathbb{Z}_p^* \\ |T_N(a_1, a_2)| < tN^{1/2}}} |T_N(a_1, a_2)|^2 \\
&< A_N(t)(\tilde{d}-1)^2 p \left(\frac{4}{\pi^2} \log p + 1.38 \right)^2 + ((p-1)^2 - A_N(t))t^2 N \\
&= A_N(t) \left((\tilde{d}-1)^2 p \left(\frac{4}{\pi^2} \log p + 1.38 \right)^2 - t^2 N \right) + (p-1)^2 t^2 N,
\end{aligned}$$

which implies that $A_N(t) > C_N(t)$.

(iv) Finally, Lemma 3 is applied with $k = s$, $\mathbf{t}_n = \mathbf{x}_n$ for $0 \leq n < N$, and $\mathbf{h} = (1, 1, 0, \dots, 0) \in \mathbb{Z}^s$. This yields

$$\begin{aligned}
D_N^{(s)} &\geq \frac{1}{2(\pi+2)N} \left| \sum_{n=0}^{N-1} e(\mathbf{h} \cdot \mathbf{x}_n) \right| \\
&= \frac{1}{2(\pi+2)N} \left| \sum_{n=0}^{N-1} e((y_n^{(1)} + y_n^{(2)})/p) \right| \\
&= \frac{1}{2(\pi+2)N} |T_N(a_1, a_2)|.
\end{aligned}$$

Hence, it follows from part (iii) that there exist more than $C_N(t)$ ordered pairs $(a_1, a_2) \in \mathbb{Z}_p^* \times \mathbb{Z}_p^*$ with

$$D_N^{(s)} \geq \frac{t}{2(\pi+2)} N^{-1/2},$$

which is the desired result. ■

The upper bound in Theorem 3 for the discrepancy $D_N^{(s)}$ over parts of the period is independent of both the parameters $a_1, \dots, a_s, b_1, \dots, b_s$ and the specific choice of the permutation polynomials g_1, \dots, g_s in the parallelized nonlinear congruential method, provided g_0, g_1, \dots, g_s are linearly independent over \mathbb{Z}_p with maximal degree d . This upper bound is of the order of magnitude $dN^{-1}p^{1/2}(\log p)^{s+1}$. On the other hand, Theorem 4 implies that, for any underlying permutation polynomials, there exist parameters in the parallelized nonlinear congruential method such that $D_N^{(s)}$ is of an order of magnitude at least $N^{-1/2}$. Concerning the role of d in the upper bound, the reader is referred to the discussion at the end of the previous section.

5. AVERAGE DISCREPANCY

In the following, it will be assumed that $a_i \equiv ac_i \pmod{p}$ for $i \in \{1, \dots, s\}$ with parameters $c_1, \dots, c_s \in \mathbb{Z}_p^*$ and an additional parameter $a \in \mathbb{Z}_p^*$. For $1 \leq N \leq p$, the abbreviation $D_{N;a}^{(s)} = D_N(\mathbf{x}_0, \mathbf{x}_1, \dots, \mathbf{x}_{N-1})$ will be used.

THEOREM 5. *Let g_1, \dots, g_s be linearly independent over \mathbb{Z}_p . Then the average value of the discrepancy $D_{N;a}^{(s)}$ over the parameter $a \in \mathbb{Z}_p^*$ in the parallelized nonlinear congruential method satisfies*

$$\frac{1}{p-1} \sum_{a \in \mathbb{Z}_p^*} D_{N;a}^{(s)} < d^{1/2} N^{-1/2} \left(\frac{2}{\pi} \log p + \frac{7}{5} \right)^s$$

for $1 \leq N \leq p$ and all parameters $c_1, \dots, c_s \in \mathbb{Z}_p^*$ and $b_1, \dots, b_s \in \mathbb{Z}_p$.

Proof. First, for $\mathbf{h} = (h_1, \dots, h_s) \in \mathbb{Z}^s$, $a \in \mathbb{Z}_p^*$, and $1 \leq N \leq p$, put

$$S_N(\mathbf{h}; a) = \sum_{n=0}^{N-1} e(\mathbf{h} \cdot \mathbf{x}_n).$$

(i) A short calculation shows that

$$\begin{aligned} \sum_{a \in \mathbb{Z}_p^*} |S_N(\mathbf{h}; a)|^2 &= \sum_{a \in \mathbb{Z}_p} \left| \sum_{n=0}^{N-1} e \left(a \sum_{i=1}^s h_i c_i g_i(n)/p \right) \right|^2 - N^2 \\ &= \sum_{k,n=0}^{N-1} \sum_{a \in \mathbb{Z}_p} e(a(Q(\mathbf{h}; k) - Q(\mathbf{h}; n))/p) - N^2, \end{aligned}$$

where the polynomial $Q(\mathbf{h}; \cdot) : \mathbb{Z} \rightarrow \mathbb{Z}_p$ is defined by

$$Q(\mathbf{h}; z) \equiv h_1 c_1 g_1(z) + \cdots + h_s c_s g_s(z) \pmod{p}.$$

Since $Q(\mathbf{h}; 0) = 0$ and g_1, \dots, g_s are linearly independent over \mathbb{Z}_p , the polynomial $Q(\mathbf{h}; \cdot)$ is nonconstant over \mathbb{Z}_p for all lattice points $\mathbf{h} \in \mathbb{Z}^s$ with $\mathbf{h} \not\equiv \mathbf{0} \pmod{p}$. Therefore,

$$\begin{aligned} \sum_{a \in \mathbb{Z}_p^*} |S_N(\mathbf{h}; a)|^2 &= p \sum_{k=0}^{N-1} \#\{0 \leq n < N \mid Q(\mathbf{h}; n) = Q(\mathbf{h}; k)\} - N^2 \\ &\leq \deg(Q(\mathbf{h}; \cdot))pN - N^2 \leq (dp - N)N \end{aligned}$$

for all lattice points $\mathbf{h} \in \mathbb{Z}^s$ with $\mathbf{h} \not\equiv \mathbf{0} \pmod{p}$.

(ii) Now, Lemma 1 is applied with $k = s$, $q = p$, and $\mathbf{t}_n = \mathbf{x}_n$ for $0 \leq n < N$. This yields

$$D_{N;a}^{(s)} \leq \frac{s}{p} + \frac{1}{N} \sum_{\mathbf{h} \in C_s(p)} \frac{1}{r(\mathbf{h}, p)} |S_N(\mathbf{h}; a)|$$

for any $a \in \mathbb{Z}_p^*$. Hence, the average value of the discrepancy $D_{N;a}^{(s)}$ over $a \in \mathbb{Z}_p^*$ satisfies

$$\begin{aligned} \frac{1}{p-1} \sum_{a \in \mathbb{Z}_p^*} D_{N;a}^{(s)} &\leq \frac{s}{p} + \frac{1}{N} \sum_{\mathbf{h} \in C_s(p)} \frac{1}{r(\mathbf{h}, p)} \left(\frac{1}{p-1} \sum_{a \in \mathbb{Z}_p^*} |S_N(\mathbf{h}; a)| \right) \\ &\leq \frac{s}{p} + \frac{1}{N} \sum_{\mathbf{h} \in C_s(p)} \frac{1}{r(\mathbf{h}, p)} \sqrt{\frac{1}{p-1} \sum_{a \in \mathbb{Z}_p^*} |S_N(\mathbf{h}; a)|^2}, \end{aligned}$$

where the last step follows from the Cauchy-Schwarz inequality. Now, note that $s \leq d$, since the underlying permutation polynomials g_1, \dots, g_s with maximal degree d are assumed to be linearly independent over \mathbb{Z}_p . Finally, part (i) can be used to obtain

$$\begin{aligned} \frac{1}{p-1} \sum_{a \in \mathbb{Z}_p^*} D_{N;a}^{(s)} &\leq \frac{s}{p} + \sqrt{\frac{dp - N}{N(p-1)}} \sum_{\mathbf{h} \in C_s(p)} \frac{1}{r(\mathbf{h}, p)} \leq \frac{d}{N} + \sqrt{\frac{d}{N}} \sum_{\mathbf{h} \in C_s(p)} \frac{1}{r(\mathbf{h}, p)} \\ &\leq \sqrt{\frac{d}{N}} \left(1 + \sum_{\mathbf{h} \in C_s(p)} \frac{1}{r(\mathbf{h}, p)} \right) < \sqrt{\frac{d}{N}} \left(\frac{2}{\pi} \log p + \frac{7}{5} \right)^s \end{aligned}$$

for $d \leq N \leq p$, where in the last step [12, Lemma 2.3] was applied. If $1 \leq N < d$, then the result is trivial, since the upper bound is greater than 1. ■

THEOREM 6. *Let g_1, \dots, g_s be linearly independent over \mathbb{Z}_p . Let $1 \leq N \leq p$, $c_1, \dots, c_s \in \mathbb{Z}_p^*$, $b_1, \dots, b_s \in \mathbb{Z}_p$, and $0 < \alpha \leq 1$ be fixed. Then there exist more than $(1 - \alpha)(p - 1)$ values of $a \in \mathbb{Z}_p^*$ such that the discrepancy $D_{N;a}^{(s)}$ in the parallelized nonlinear congruential method satisfies*

$$D_{N;a}^{(s)} < \alpha^{-1} d^{1/2} N^{-1/2} \left(\frac{2}{\pi} \log p + \frac{7}{5} \right)^s.$$

Proof. Subsequently, the abbreviation

$$M = d^{1/2} N^{-1/2} \left(\frac{2}{\pi} \log p + \frac{7}{5} \right)^s$$

will be used. Suppose that there exist at most $(1 - \alpha)(p - 1)$ values of $a \in \mathbb{Z}_p^*$ with $D_{N;a}^{(s)} < \alpha^{-1} M$. Then there exist at least $\alpha(p - 1)$ values of $a \in \mathbb{Z}_p^*$ with $D_{N;a}^{(s)} \geq \alpha^{-1} M$, which implies that $\sum_{a \in \mathbb{Z}_p^*} D_{N;a}^{(s)} \geq (p - 1)M$. This contradiction to Theorem 5 proves the desired result. ■

The upper bound in Theorem 5 for the average value of the discrepancy $D_{N;a}^{(s)}$ (over the parameter a) is independent of both the parameters $c_1, \dots, c_s, b_1, \dots, b_s$ and the specific choice of the permutation polynomials g_1, \dots, g_s in the parallelized nonlinear congruential method, as long as g_1, \dots, g_s are linearly independent over \mathbb{Z}_p with maximal degree d . This upper bound is of the order of magnitude $d^{1/2} N^{-1/2} (\log p)^s$, which fits well the asymptotic behavior of the discrepancy of N true random points from $[0, 1]^s$ according to the law of the iterated logarithm, provided the maximal degree d is bounded and N is not too small. Theorem 6 provides even more information, since it implies that, for any underlying linearly independent permutation polynomials with bounded degree d and parameters $c_1, \dots, c_s, b_1, \dots, b_s$, only an arbitrarily small percentage of the values of the parameter a may lead to a discrepancy $D_{N;a}^{(s)}$ with an order of magnitude that is greater than $d^{1/2} N^{-1/2} (\log p)^s$. A remark similar to that at the end of the third section could be made regarding the choice of the value of d .

ACKNOWLEDGMENT

The authors thank a referee for valuable comments.

REFERENCES

1. T. Cochrane, On a trigonometric inequality of Vinogradov, *J. Number Theory* **27** (1987), 9–16.
2. J. Eichenauer-Herrmann, Inversive congruential pseudorandom numbers: A tutorial, *Internat. Statist. Rev.* **60** (1992), 167–176.
3. J. Eichenauer-Herrmann, Equidistribution properties of nonlinear congruential pseudorandom numbers, *Metrika* **40** (1993), 333–338.
4. J. Eichenauer-Herrmann, Compound nonlinear congruential pseudorandom numbers, *Monatsh. Math.* **117** (1994), 213–222.
5. J. Eichenauer-Herrmann, Pseudorandom number generation by nonlinear methods, *Internat. Statist. Rev.* **63** (1995), 247–255.
6. J. Eichenauer-Herrmann and G. Larcher, Average behaviour of compound nonlinear congruential pseudorandom numbers, *Finite Fields Appl.* **2** (1996), 111–123.
7. J. Eichenauer-Herrmann and G. Larcher, Average equidistribution properties of compound nonlinear congruential pseudorandom numbers, *Math. Comp.* **66** (1997), 363–372.
8. J. Eichenauer-Herrmann and H. Niederreiter, On the statistical independence of nonlinear congruential pseudorandom numbers, *ACM Trans. Modeling Comput. Simul.* **4** (1994), 89–95.
9. J. Kiefer, On large deviations of the empiric d.f. of vector chance variables and a law of the iterated logarithm, *Pacific J. Math.* **11** (1961), 649–660.
10. P. L'Ecuyer, Uniform random number generation, *Ann. Oper. Res.* **53** (1994), 77–120.
11. R. Lidl and H. Niederreiter, “Finite Fields,” Addison-Wesley, Reading, MA, 1983.
12. H. Niederreiter, Pseudo-random numbers and optimal coefficients, *Adv. in Math.* **26** (1977), 99–181.
13. H. Niederreiter, Statistical independence of nonlinear congruential pseudorandom numbers, *Monatsh. Math.* **106** (1988), 149–159.
14. H. Niederreiter, Recent trends in random number and random vector generation, *Ann. Oper. Res.* **31** (1991), 323–345.
15. H. Niederreiter, “Random Number Generation and Quasi-Monte Carlo Methods,” SIAM, Philadelphia, 1992.
16. H. Niederreiter, On a new class of pseudorandom numbers for simulation methods, *J. Comput. Appl. Math.* **56** (1994), 159–167.
17. H. Niederreiter, New developments in uniform pseudorandom number and vector generation, in “Monte Carlo and Quasi-Monte Carlo Methods in Scientific Computing” (H. Niederreiter and P.J.-S. Shiue, Eds.), pp. 87–120, Lecture Notes in Statistics, Vol. 106, Springer-Verlag, New York, 1995.
18. A. Weil, On some exponential sums, *Proc. Nat. Acad. Sci. U.S.A.* **34** (1948), 204–207.