MATHEMATICS OF COMPUTATION
Volume 66, Number 217, January 1997, Pages 363–372
S 0025-5718(97)00802-8

AVERAGE EQUIDISTRIBUTION PROPERTIES OF COMPOUND NONLINEAR CONGRUENTIAL PSEUDORANDOM NUMBERS

JÜRGEN EICHENAUER–HERRMANN AND GERHARD LARCHER

ABSTRACT. The present paper deals with the compound nonlinear congruential method for generating uniform pseudorandom numbers, which has been introduced recently. Equidistribution properties of the generated sequences over parts of the period are studied, based on the discrepancy of the corresponding point sets. Upper and lower bounds for the average value of these discrepancies are established, which are essentially best possible. These results show that the average equidistribution behavior of compound nonlinear congruential pseudorandom numbers fits well the equidistribution properties of true random numbers. The method of proof relies heavily on estimates of the average value of incomplete exponential sums.

1. INTRODUCTION

Several nonlinear methods of generating uniform pseudorandom numbers in the interval $[0,1)$ have been introduced and studied during the last years. The development of this field of research is described in the survey articles [2, 5, 10, 11, 13] and in Niederreiter's excellent monograph [12]. A particularly attractive approach is the general nonlinear congruential method. The generated sequences of pseudorandom numbers have nice equidistribution and statistical independence properties [3, 8, 9]. Recently, the following compound version of this method, which shows additional computational advantages, has been introduced and analyzed in [4, 6, 7].

Let $p_1, \ldots, p_r \geq 5$ be arbitrary distinct primes. For $1 \leq i \leq r$ identify $\mathbb{Z}_{p_i} = \{0, 1, \ldots, p_i - 1\}$ with the finite field of order p_i. Let $f_i : \mathbb{Z} \to \mathbb{Z}_{p_i}$ be a permutation polynomial of $\mathbb{Z}_{p_i}$ and let $(x_n^{(i)})_{n \geq 0}$, with

$$x_n^{(i)} = f_i(n)/p_i \in [0,1), \qquad n \geq 0,$$

be the corresponding stream of (ordinary) *nonlinear congruential pseudorandom numbers*. A sequence $(x_n)_{n \geq 0}$ of *compound nonlinear congruential pseudorandom numbers* in the interval $[0,1)$ is defined by

$$x_n \equiv x_n^{(1)} + \cdots + x_n^{(r)} \pmod 1, \qquad n \geq 0.$$

Since the primes $p_1, \ldots, p_r$ are distinct and $f_1, \ldots, f_r$ are permutation polynomials, the sequence $(x_n)_{n \geq 0}$ is purely periodic with period length $m = p_1 \cdots p_r$, and

Received by the editor July 13, 1995.
1991 *Mathematics Subject Classification.* Primary 65C10; Secondary 11K45.
Key words and phrases. Uniform pseudorandom numbers, compound nonlinear congruential method, equidistribution of subsequences, average behavior, discrepancy, incomplete exponential sums.

$x_0, x_1, \ldots, x_{m-1}$ run through all rationals in $[0,1)$ with denominator m. It should be observed that in the compound nonlinear congruential method a very large period length m can be obtained, although exact integer computations have to be performed only in $\mathbb{Z}_{p_1}, \ldots, \mathbb{Z}_{p_r}$. Additionally, the compound approach is particularly suitable for parallel computations, since the computation of the underlying sequences $(x_n^{(i)})_{n\geq 0}$ of (ordinary) nonlinear congruential pseudorandom numbers can be allocated to r parallel processors.

Equidistribution properties of the sequence $(x_n)_{n\geq 0}$ can be analyzed based on the discrepancy of its first N terms. The *discrepancy* of N arbitrary points $t_0, t_1, \ldots, t_{N-1} \in [0,1)$ is defined by

$$D_N(t_0, t_1, \ldots, t_{N-1}) = \sup_{0\leq \alpha < \beta \leq 1} |F_N([\alpha,\beta)) - (\beta - \alpha)|,$$

where $F_N([\alpha,\beta))$ is N^{-1} times the number of points among $t_0, t_1, \ldots, t_{N-1}$ falling into the interval $[\alpha,\beta)$. For a sequence $(x_n)_{n\geq 0}$ of compound nonlinear congruential pseudorandom numbers the abbreviation

$$D_{N;f_1,\ldots,f_r} = D_N(x_0, x_1, \ldots, x_{N-1})$$

will be used. The present paper deals with the average equidistribution behavior of compound nonlinear congruential pseudorandom numbers. In the third section, upper and lower bounds for the average value of the discrepancy $D_{N;f_1,\ldots,f_r}$ are established. A detailed discussion of these results is given in the fourth section. The second section contains several auxiliary results.

2. Auxiliary results

First, some further notation is necessary. For an integer $q \geq 2$, let $C(q)$ be the set of all nonzero integers h with $-q/2 < h \leq q/2$ and define $r(h,q) = q \sin(\pi|h|/q)$ for $h \in C(q)$. For real t, the abbreviation $e(t) = e^{2\pi i t}$ is used. The following three results can be deduced from [12, Theorem 3.10 and Corollary 3.17] and [4, Proof of Theorem 1], respectively.

Lemma 1. *Let $N \geq 1$ and $q \geq 2$ be integers. Let $t_n = y_n/q \in [0,1)$, with $y_n \in \{0,1,\ldots,q-1\}$ for $0 \leq n < N$. Then the discrepancy of the points $t_0, t_1, \ldots, t_{N-1}$ satisfies*

$$D_N(t_0, t_1, \ldots, t_{N-1}) \leq \frac{1}{q} + \frac{1}{N} \sum_{h\in C(q)} \frac{1}{r(h,q)} \left| \sum_{n=0}^{N-1} e(ht_n) \right|.$$

Lemma 2. *The discrepancy of N arbitrary points $t_0, t_1, \ldots, t_{N-1} \in [0,1)$ satisfies*

$$D_N(t_0, t_1, \ldots, t_{N-1}) \geq \frac{1}{2N|h|} \left| \sum_{n=0}^{N-1} e(ht_n) \right|$$

for any nonzero integer h.

Lemma 3. *Let $q \geq 2$ be an integer. Then*

$$\sum_{\substack{h\in C(q) \\ h\equiv 0 \,(\mathrm{mod}\, d)}} \frac{1}{r(h,q)} < \frac{1}{d}\left(\frac{2}{\pi}\log q + \frac{2}{5}\right)$$

for any divisor d of q with $1 \leq d < q$.

Later on, Hölder's inequality will be used in the following form.

Lemma 4. *Let $a_1, a_2, \dots, a_q$ be q arbitrary real numbers. Then*

$$\frac{1}{q}\sum_{j=1}^{q}|a_j| \ge \left(\frac{1}{q}\sum_{j=1}^{q}a_j^2\right)^{3/2}\left(\frac{1}{q}\sum_{j=1}^{q}a_j^4\right)^{-1/2}.$$

Proof. First, observe that $a_j^2 = |a_j|^{2/3}|a_j|^{4/3}$ for $1 \le j \le q$. Hence, Hölder's inequality (with $u = 3/2$ and $v = 3$) implies that

$$\sum_{j=1}^{q}a_j^2 \le \left(\sum_{j=1}^{q}\left(|a_j|^{2/3}\right)^{3/2}\right)^{2/3}\left(\sum_{j=1}^{q}\left(|a_j|^{4/3}\right)^{3}\right)^{1/3} = \left(\sum_{j=1}^{q}|a_j|\right)^{2/3}\left(\sum_{j=1}^{q}a_j^4\right)^{1/3},$$

which yields the desired result. □

In the following, let $\mathbb{Z}_{p_i}^* = \mathbb{Z}_{p_i}\setminus\{0\}$ for $1 \le i \le r$, and let $m_I = \prod_{i\in I} p_i$ for subsets I of $\{1,\dots,r\}$. For $\gamma_i \in \mathbb{Z}_{p_i}^*$ and any permutation polynomial $g_i : \mathbb{Z} \to \mathbb{Z}_{p_i}$ denote by $\gamma_i g_i$ the permutation polynomial $f_i : \mathbb{Z} \to \mathbb{Z}_{p_i}$ with $f_i(z) \equiv \gamma_i g_i(z) \pmod{p_i}$.

Lemma 5. *Let $1 \le N \le m$, $h \in C(m)$, and $J = \{1 \le i \le r \mid h \equiv 0 \pmod{p_i}\}$. Then*

$$\sum_{(\gamma_1,\dots,\gamma_r)\in\mathbb{Z}_{p_1}^*\times\cdots\times\mathbb{Z}_{p_r}^*}\left|\sum_{n=0}^{N-1}e\left(h\sum_{i=1}^{r}\gamma_i g_i(n)/p_i\right)\right|^2 \le N(m-N)\prod_{i\in J}(p_i-1).$$

Proof. Let $J^c = \{1,\dots,r\}\setminus J$. Then straightforward calculations show that

$$\begin{aligned}
&\sum_{(\gamma_1,\dots,\gamma_r)\in\mathbb{Z}_{p_1}^*\times\cdots\times\mathbb{Z}_{p_r}^*}\left|\sum_{n=0}^{N-1}e\left(h\sum_{i=1}^{r}\gamma_i g_i(n)/p_i\right)\right|^2\\
&\quad=\prod_{i\in J}(p_i-1)\sum_{\gamma_i\in\mathbb{Z}_{p_i}^*,\,i\in J^c}\left|\sum_{n=0}^{N-1}e\left(h\sum_{i\in J^c}\gamma_i g_i(n)/p_i\right)\right|^2\\
&\quad\le\prod_{i\in J}(p_i-1)\left(\sum_{\gamma_i\in\mathbb{Z}_{p_i},\,i\in J^c}\left|\sum_{n=0}^{N-1}e\left(h\sum_{i\in J^c}\gamma_i g_i(n)/p_i\right)\right|^2-N^2\right)\\
&\quad=\prod_{i\in J}(p_i-1)\left(\sum_{k,n=0}^{N-1}\prod_{i\in J^c}\sum_{\gamma\in\mathbb{Z}_{p_i}}e\Big(h\gamma(g_i(n)-g_i(k))/p_i\Big)-N^2\right)\\
&\quad=\prod_{i\in J}(p_i-1)\Big(m_{J^c}\cdot\#\{(k,n)\in\mathbb{Z}_N^2\mid g_i(n)=g_i(k),\ i\in J^c\}-N^2\Big)\\
&\quad=\prod_{i\in J}(p_i-1)\Big(m_{J^c}\cdot\#\{(k,n)\in\mathbb{Z}_N^2\mid n\equiv k\pmod{m_{J^c}}\}-N^2\Big),
\end{aligned}$$

where $\mathbb{Z}_N = \{0,1,\dots,N-1\}$. Let $N_{J^c}\in\mathbb{Z}_{m_{J^c}}$, with $N_{J^c}\equiv N \pmod{m_{J^c}}$, and observe that $m_{J^c}\lfloor N/m_{J^c}\rfloor = N - N_{J^c}$, where $\lfloor x\rfloor$ means the greatest integer less than or equal to x. Then

$$\begin{aligned}
&m_{J^c}\cdot\#\{(k,n)\in\mathbb{Z}_N^2\mid n\equiv k\pmod{m_{J^c}}\}\\
&\quad=m_{J^c}\Big(\lfloor N/m_{J^c}\rfloor(N+N_{J^c})+N_{J^c}\Big)\ =\ (N-N_{J^c})(N+N_{J^c})+m_{J^c}N_{J^c}.
\end{aligned}$$

Hence,

$$\begin{aligned}
&\sum_{(\gamma_1,\dots,\gamma_r)\in\mathbb{Z}_{p_1}^*\times\cdots\times\mathbb{Z}_{p_r}^*}\left|\sum_{n=0}^{N-1}e\left(h\sum_{i=1}^{r}\gamma_i g_i(n)/p_i\right)\right|^2\\
&\quad\le\prod_{i\in J}(p_i-1)\Big((N-N_{J^c})(N+N_{J^c})+m_{J^c}N_{J^c}-N^2\Big)\\
&\quad=N_{J^c}(m_{J^c}-N_{J^c})\prod_{i\in J}(p_i-1)\\
&\quad\le N(m-N)\prod_{i\in J}(p_i-1),
\end{aligned}$$

which is the desired result. □

The following result is the special case $s=1$ of [7, Lemma 6].

Lemma 6. *Let* $1\le N\le 2^{-(r+1)}\prod_{i=1}^{r}(p_i-1)$. *Then*

$$\frac{1}{\prod_{i=1}^{r}(p_i-1)}\sum_{(\gamma_1,\dots,\gamma_r)\in\mathbb{Z}_{p_1}^*\times\cdots\times\mathbb{Z}_{p_r}^*}\left|\sum_{n=0}^{N-1}e\left(\sum_{i=1}^{r}\gamma_i g_i(n)/p_i\right)\right|^2>\frac{N}{2}.$$

Lemma 7. *Let* $r=1$ *and* $1\le N\le m$. *Then*

$$\frac{1}{m-1}\sum_{\gamma_1\in\mathbb{Z}_m^*}\left|\sum_{n=0}^{N-1}e(\gamma_1 g_1(n)/m)\right|^2=\frac{N(m-N)}{m-1}.$$

Proof. It follows at once from the proof of Lemma 5 that, for $r=1$ and $h=1$, equality holds in Lemma 5. This yields the desired result. □

For an integer $b\ge 1$, let $\mathbb{Z}_b=\{0,1,\dots,b-1\}$ and define

$$\begin{aligned}
T_b(1)=\{(k,l,h,n)\in\mathbb{Z}_b^4\mid{}&k,l,h,n\text{ distinct or }k=l\text{ and }k,h,n\text{ distinct}\\
&\text{or }h=n\text{ and }k,l,h\text{ distinct}\},
\end{aligned}$$

$$\begin{aligned}
T_b(2)=\{(k,l,h,n)\in\mathbb{Z}_b^4\mid{}&k=h,\ l\ne n\text{ or }k=n,\ l\ne h\text{ or }k\ne h,\ l=n\\
&\text{or }k\ne n,\ l=h\text{ or }k=l\ne h=n\},
\end{aligned}$$

and

$$T_b(3)=\{(k,l,h,n)\in\mathbb{Z}_b^4\mid k=h,\ l=n\text{ or }k=n,\ l=h\}.$$

Lemma 8. *Let* $1\le N\le m$, *and let* $\{J_1,J_2,J_3\}$ *be a partition of* $\{1,\dots,r\}$, *where it is allowed that some of the sets* J_1,J_2,J_3 *are empty. Then*

$$\begin{aligned}
&\#\{(k,l,h,n)\in\mathbb{Z}_N^4\mid(k,l,h,n)\pmod{p_i}\in T_{p_i}(j),\ i\in J_j,\ 1\le j\le 3\}\\
&\quad\le 6^{\#J_2}2^{\#J_3}\left(4N^2+3N^3\prod_{i\in J_3}\frac{1}{p_i}+N^4\prod_{i\in J_2}\frac{1}{p_i}\prod_{i\in J_3}\frac{1}{p_i^2}\right).
\end{aligned}$$

Proof. Let $\mathcal{L} = \{L_1, \dots, L_6\}$ be a partition of J_2 and let $\mathcal{M} = \{M_1, M_2\}$ be a partition of J_3, where again it is allowed that some of the sets $L_1, \dots, L_6$ and M_1, M_2 are empty. Let $Q_i = \prod_{j \in L_i} p_j$, $R_i = \prod_{j \in M_i} p_j$, and $V(\mathcal{L}, \mathcal{M}) = \{(k,l,h,n) \in \mathbb{Z}_N^4 \mid k \equiv l \pmod{Q_1},\ h \equiv n \pmod{Q_2},\ k \equiv h \pmod{Q_3 R_1},\ l \equiv h \pmod{Q_4 R_2},\ k \equiv n \pmod{Q_5 R_2},\ l \equiv n \pmod{Q_6 R_1}\}$. Then $\#\{(k,l,h,n) \in \mathbb{Z}_N^4 \mid (k,l,h,n) \pmod{p_i} \in T_{p_i}(j),\ i \in J_j,\ 1 \le j \le 3\}$ is at most $\sum_{\mathcal{L},\mathcal{M}} \#V(\mathcal{L}, \mathcal{M})$, where the summation is extended over all partitions $\mathcal{L}$ and $\mathcal{M}$ of the form described above. It follows from the Chinese Remainder Theorem that, for given $\mathcal{L}, \mathcal{M}$ and fixed k, l, h, the number of $(k,l,h,n) \in V(\mathcal{L}, \mathcal{M})$ is at most $\lceil N/(Q_2 Q_5 Q_6 R_1 R_2) \rceil$, where $\lceil x \rceil$ means the least integer larger than or equal to x. Further, for given $\mathcal{L}, \mathcal{M}$ and fixed k, l, the number of h for which there exist n with $(k,l,h,n) \in V(\mathcal{L}, \mathcal{M})$ is at most $\lceil N/(Q_3 Q_4 R_1 R_2) \rceil$. Finally, for given $\mathcal{L}, \mathcal{M}$ and fixed k, the number of l for which there exist h and n with $(k,l,h,n) \in V(\mathcal{L}, \mathcal{M})$ is at most $\lceil N/Q_1 \rceil$. Therefore,

$$\begin{aligned} \#V(\mathcal{L}, \mathcal{M}) &\le N\left(\frac{N}{Q_1} + 1\right)\left(\frac{N}{Q_3 Q_4 R_1 R_2} + 1\right)\left(\frac{N}{Q_2 Q_5 Q_6 R_1 R_2} + 1\right) \\ &\le 4N^2 + \frac{3}{R_1 R_2} N^3 + \frac{1}{(\prod_{i=1}^{6} Q_i)(R_1 R_2)^2} N^4 \end{aligned}$$

and the desired result follows. □

Lemma 9. *Let $1 \le N \le m$. Then*

$$\frac{1}{\prod_{i=1}^{r} p_i!} \sum_{f_1, \dots, f_r} \left| \sum_{n=0}^{N-1} e\left(\sum_{i=1}^{r} f_i(n)/p_i \right) \right|^4 < 4.84 \cdot (12.27)^r N^2,$$

where the summation is extended over all permutation polynomials $f_i : \mathbb{Z} \to \mathbb{Z}_{p_i}$ of $\mathbb{Z}_{p_i}$ with $1 \le i \le r$.

Proof. For any $z \in \mathbb{Z}_b$ with $b \ge 5$ and (fixed) integers k, l, h, n, let $A_b(z)$ be the number of permutation polynomials $f : \mathbb{Z} \to \mathbb{Z}_b$ of $\mathbb{Z}_b$ with $f(k) + f(l) - f(h) - f(n) \equiv z \pmod{b}$. Obviously, $A_b(z) = A_b(1)$ for any $z \ne 0$, $A_b(0) + (b-1)A_b(1) = b!$, and

$$A_b(1) = \begin{cases} b(b-3)(b-3)! & \text{for } (k,l,h,n) \pmod{b} \in T_b(1), \\ b(b-2)! & \text{for } (k,l,h,n) \pmod{b} \in T_b(2), \\ 0 & \text{for } (k,l,h,n) \pmod{b} \in T_b(3), \end{cases}$$

which implies that

$$\begin{aligned} \sum_{z \in \mathbb{Z}_b} A_b(z) e(z/b) &= A_b(0) - A_b(1) = b! - bA_b(1) \\ &= \begin{cases} 2b(b-3)! & \text{for } (k,l,h,n) \pmod{b} \in T_b(1), \\ -b(b-2)! & \text{for } (k,l,h,n) \pmod{b} \in T_b(2), \\ b! & \text{for } (k,l,h,n) \pmod{b} \in T_b(3). \end{cases} \end{aligned}$$

Hence,

$$\begin{aligned}
&\frac{1}{\prod_{i=1}^{r} p_i!} \sum_{f_1,\dots,f_r} \left| \sum_{n=0}^{N-1} e\left(\sum_{i=1}^{r} f_i(n)/p_i \right) \right|^4 \\
&\quad = \frac{1}{\prod_{i=1}^{r} p_i!} \sum_{k,l,h,n=0}^{N-1} \prod_{i=1}^{r} \sum_{z \in \mathbb{Z}_{p_i}} A_{p_i}(z) e(z/p_i) \\
&\quad \le \sum_{k,l,h,n=0}^{N-1} \prod_{i=1}^{r} \left| \frac{1}{p_i!} \sum_{z \in \mathbb{Z}_{p_i}} A_{p_i}(z) e(z/p_i) \right| \\
&\quad = \sum_{J_1,J_2,J_3} \sum_{\substack{k,l,h,n=0 \\ (k,l,h,n) \,(\mathrm{mod}\, p_i) \in T_{p_i}(j), \\ i \in J_j,\, 1 \le j \le 3}}^{N-1} \prod_{i \in J_1} \frac{2}{(p_i-1)(p_i-2)} \prod_{i \in J_2} \frac{1}{p_i - 1},
\end{aligned}$$

where the summation over J_1, J_2, J_3 is extended over all partitions $\{J_1, J_2, J_3\}$ of $\{1, \dots, r\}$. Now, Lemma 8 can be used in order to obtain

$$\begin{aligned}
&\frac{1}{\prod_{i=1}^{r} p_i!} \sum_{f_1,\dots,f_r} \left| \sum_{n=0}^{N-1} e\left(\sum_{i=1}^{r} f_i(n)/p_i \right) \right|^4 \\
&\quad \le 2^r \sum_{J_1,J_2,J_3} \prod_{i \in J_1} \frac{1}{(p_i-1)(p_i-2)} \prod_{i \in J_2} \frac{3}{p_i - 1} \\
&\qquad \cdot \left(4N^2 + 3N^3 \prod_{i \in J_3} \frac{1}{p_i} + N^4 \prod_{i \in J_2} \frac{1}{p_i} \prod_{i \in J_3} \frac{1}{p_i^2} \right) \\
&\quad = 2^r N^2 \left(4 \prod_{i=1}^{r} \left(\frac{1}{(p_i-1)(p_i-2)} + \frac{3}{p_i - 1} + 1 \right) \right. \\
&\qquad\qquad + 3\frac{N}{m} \prod_{i=1}^{r} \left(\frac{p_i}{(p_i-1)(p_i-2)} + \frac{3p_i}{p_i - 1} + 1 \right) \\
&\qquad\qquad \left. + \frac{N^2}{m^2} \prod_{i=1}^{r} \left(\frac{p_i^2}{(p_i-1)(p_i-2)} + \frac{3p_i}{p_i - 1} + 1 \right) \right) \\
&\quad \le 2^r N^2 \left(\frac{22}{3} \left(\frac{23}{92} \right)^{r-1} + \frac{31}{2} \left(\frac{71}{92} \right)^{r-1} + \frac{41}{6} \right) \left(\frac{92}{15} \right)^{r-1} \\
&\quad \le \frac{445}{92} \left(\frac{184}{15} \right)^{r} N^2,
\end{aligned}$$

which yields the desired result. □

Lemma 10. *Let $r = 1$ and $1 \le N \le m$. Then*

$$\frac{1}{m!} \sum_{f_1} \left| \sum_{n=0}^{N-1} e\big(f_1(n)/m\big) \right|^4 \le \frac{2N^2(m-N)^2}{m(m-1)},$$

where the summation is extended over all permutation polynomials $f_1 : \mathbb{Z} \to \mathbb{Z}_m$ of $\mathbb{Z}_m$.

Proof. It follows from the proof of Lemma 9 that

$$\begin{aligned}\frac{1}{m!}\sum_{f_1}\left|\sum_{n=0}^{N-1} e\big(f_1(n)/m\big)\right|^4 &= \frac{1}{m!}\sum_{k,l,h,n=0}^{N-1}\sum_{z\in\mathbb{Z}_m} A_m(z)e(z/m)\\ &= \frac{2}{(m-1)(m-2)}\#T_N(1) - \frac{1}{m-1}\#T_N(2) + \#T_N(3)\\ &= \frac{2N(N-1)^2(N-2)}{(m-1)(m-2)} - \frac{N(N-1)(4N-3)}{m-1} + N(2N-1)\\ &= \frac{2N^2(m-N)^2 - mN(m-N)}{(m-1)(m-2)} \le \frac{2N^2(m-N)^2}{m(m-1)}. \qquad \square\end{aligned}$$

3. Main results

Theorem 1. *Let $1 \le N < m$. Then the average value of the discrepancy $D_{N;\gamma_1 g_1,\dots,\gamma_r g_r}$ in the compound nonlinear congruential method over $(\gamma_1,\dots,\gamma_r) \in \mathbb{Z}_{p_1}^* \times \cdots \times \mathbb{Z}_{p_r}^*$ satisfies*

$$\begin{aligned}&\frac{1}{\prod_{i=1}^r (p_i-1)} \sum_{(\gamma_1,\dots,\gamma_r)\in\mathbb{Z}_{p_1}^*\times\cdots\times\mathbb{Z}_{p_r}^*} D_{N;\gamma_1 g_1,\dots,\gamma_r g_r}\\ &\quad< \left(\frac{7\sqrt{5}}{10}\right)^r N^{-1/2}\left(1-\frac{N}{m}\right)^{1/2}\left(\frac{2}{\pi}\log m + \frac{2}{5}\right) + \frac{1}{m}.\end{aligned}$$

Proof. First, Lemma 1 is applied with $q = m$ and $t_n = x_n$ for $0 \le n < N$. This yields

$$\begin{aligned}&\frac{1}{\prod_{i=1}^r (p_i-1)} \sum_{(\gamma_1,\dots,\gamma_r)\in\mathbb{Z}_{p_1}^*\times\cdots\times\mathbb{Z}_{p_r}^*} D_{N;\gamma_1 g_1,\dots,\gamma_r g_r}\\ &\quad\le \frac{1}{m} + \frac{1}{N}\sum_{h\in C(m)}\frac{1}{r(h,m)}\\ &\qquad\cdot\left(\frac{1}{\prod_{i=1}^r (p_i-1)}\sum_{(\gamma_1,\dots,\gamma_r)\in\mathbb{Z}_{p_1}^*\times\cdots\times\mathbb{Z}_{p_r}^*}\left|\sum_{n=0}^{N-1} e\left(h\sum_{i=1}^r \gamma_i g_i(n)/p_i\right)\right|\right)\\ &\quad\le \frac{1}{m} + \frac{1}{N}\sum_{h\in C(m)}\frac{1}{r(h,m)}\\ &\qquad\cdot\sqrt{\frac{1}{\prod_{i=1}^r (p_i-1)}\sum_{(\gamma_1,\dots,\gamma_r)\in\mathbb{Z}_{p_1}^*\times\cdots\times\mathbb{Z}_{p_r}^*}\left|\sum_{n=0}^{N-1} e\left(h\sum_{i=1}^r \gamma_i g_i(n)/p_i\right)\right|^2}\\ &\quad= \frac{1}{m} + \frac{1}{N}\sum_{J\subset\{1,\dots,r\}\atop \#J<r}\ \sum_{\substack{h\in C(m)\\ h\equiv 0 \,(\mathrm{mod}\, p_i),\, i\in J\\ h\not\equiv 0 \,(\mathrm{mod}\, p_i),\, i\notin J}}\frac{1}{r(h,m)}\\ &\qquad\cdot\sqrt{\frac{1}{\prod_{i=1}^r (p_i-1)}\sum_{(\gamma_1,\dots,\gamma_r)\in\mathbb{Z}_{p_1}^*\times\cdots\times\mathbb{Z}_{p_r}^*}\left|\sum_{n=0}^{N-1} e\left(h\sum_{i=1}^r \gamma_i g_i(n)/p_i\right)\right|^2},\end{aligned}$$

where the penultimate step follows from Schwarz's inequality. Now, Lemma 5 can be used in order to obtain

$$\frac{1}{\prod_{i=1}^{r}(p_i-1)} \sum_{(\gamma_1,\dots,\gamma_r)\in\mathbb{Z}_{p_1}^*\times\cdots\times\mathbb{Z}_{p_r}^*} D_{N;\gamma_1 g_1,\dots,\gamma_r g_r}$$
$$\le \frac{1}{m} + \sqrt{\frac{1}{N}\left(1-\frac{N}{m}\right)} \sum_{\substack{J\subset\{1,\dots,r\}\\ \#J<r}} \sum_{\substack{h\in C(m)\\ h\equiv 0 \,(\mathrm{mod}\, p_i),\, i\in J\\ h\not\equiv 0 \,(\mathrm{mod}\, p_i),\, i\notin J}} \frac{1}{r(h,m)} \prod_{i\in J}\sqrt{p_i} \prod_{\substack{i=1\\ i\notin J}}^{r} \sqrt{\frac{p_i}{p_i-1}}\,.$$

Hence, it follows from Lemma 3 that

$$\begin{aligned}
&\frac{1}{\prod_{i=1}^{r}(p_i-1)} \sum_{(\gamma_1,\dots,\gamma_r)\in\mathbb{Z}_{p_1}^*\times\cdots\times\mathbb{Z}_{p_r}^*} D_{N;\gamma_1 g_1,\dots,\gamma_r g_r} \\
&\quad< \frac{1}{m} + \sqrt{\frac{1}{N}\left(1-\frac{N}{m}\right)}\left(\frac{2}{\pi}\log m+\frac{2}{5}\right) \sum_{\substack{J\subset\{1,\dots,r\}\\ \#J<r}} \prod_{i\in J}\frac{1}{\sqrt{p_i}} \prod_{\substack{i=1\\ i\notin J}}^{r}\sqrt{\frac{p_i}{p_i-1}} \\
&\quad< \frac{1}{m} + \sqrt{\frac{1}{N}\left(1-\frac{N}{m}\right)}\left(\frac{2}{\pi}\log m+\frac{2}{5}\right) \prod_{i=1}^{r}\left(\frac{1}{\sqrt{p_i}}+\sqrt{\frac{p_i}{p_i-1}}\right) \\
&\quad\le \frac{1}{m} + \sqrt{\frac{1}{N}\left(1-\frac{N}{m}\right)}\left(\frac{2}{\pi}\log m+\frac{2}{5}\right)\left(\frac{1}{\sqrt{5}}+\frac{1}{2}\sqrt{5}\right)^r,
\end{aligned}$$

which yields the desired result. □

Theorem 2. *Let $1 \le N < m$ and fix the permutation polynomials $g_1,\dots,g_r$. Let $0<\alpha\le 1$. Then there exist more than $(1-\alpha)\prod_{i=1}^{r}(p_i-1)$ values of $(\gamma_1,\dots,\gamma_r)\in\mathbb{Z}_{p_1}^*\times\cdots\times\mathbb{Z}_{p_r}^*$ such that the discrepancy $D_{N;\gamma_1 g_1,\dots,\gamma_r g_r}$ in the compound nonlinear congruential method satisfies*

$$D_{N;\gamma_1 g_1,\dots,\gamma_r g_r} < \frac{1}{\alpha}\left(\left(\frac{7\sqrt{5}}{10}\right)^r N^{-1/2}\left(1-\frac{N}{m}\right)^{1/2}\left(\frac{2}{\pi}\log m+\frac{2}{5}\right)+\frac{1}{m}\right).$$

Proof. Let

$$M = \left(\frac{7\sqrt{5}}{10}\right)^r N^{-1/2}\left(1-\frac{N}{m}\right)^{1/2}\left(\frac{2}{\pi}\log m+\frac{2}{5}\right)+\frac{1}{m},$$

and suppose that there exist at most $(1-\alpha)\prod_{i=1}^{r}(p_i-1)$ values of $(\gamma_1,\dots,\gamma_r)\in\mathbb{Z}_{p_1}^*\times\cdots\times\mathbb{Z}_{p_r}^*$ with $D_{N;\gamma_1 g_1,\dots,\gamma_r g_r} < \alpha^{-1}M$, i.e., there exist at least $\alpha\prod_{i=1}^{r}(p_i-1)$ values of $(\gamma_1,\dots,\gamma_r)\in\mathbb{Z}_{p_1}^*\times\cdots\times\mathbb{Z}_{p_r}^*$ with $D_{N;\gamma_1 g_1,\dots,\gamma_r g_r}\ge\alpha^{-1}M$. Hence, one obtains

$$\sum_{(\gamma_1,\dots,\gamma_r)\in\mathbb{Z}_{p_1}^*\times\cdots\times\mathbb{Z}_{p_r}^*} D_{N;\gamma_1 g_1,\dots,\gamma_r g_r} \ge M\prod_{i=1}^{r}(p_i-1),$$

which contradicts Theorem 1. □

Theorem 3. *Let $1\le N\le 2^{-(r+1)}\prod_{i=1}^{r}(p_i-1)$. Then the average value of the discrepancy $D_{N;f_1,\dots,f_r}$ in the compound nonlinear congruential method over all*

permutation polynomials $f_i : \mathbb{Z} \to \mathbb{Z}_{p_i}$ *of* $\mathbb{Z}_{p_i}$ *with* $1 \le i \le r$ *satisfies*

$$\frac{1}{\prod_{i=1}^{r} p_i!} \sum_{f_1,\dots,f_r} D_{N;f_1,\dots,f_r} > \frac{1}{12.45 \cdot (3.51)^r} N^{-1/2}.$$

Proof. First, Lemma 2 is applied with $t_n = x_n$ for $0 \le n < N$ and $h = 1$. This yields

$$\begin{aligned}\frac{1}{\prod_{i=1}^{r} p_i!} \sum_{f_1,\dots,f_r} D_{N;f_1,\dots,f_r} &\ge \frac{1}{2N \prod_{i=1}^{r} p_i!} \sum_{f_1,\dots,f_r} \left| \sum_{n=0}^{N-1} e\left(\sum_{i=1}^{r} f_i(n)/p_i \right) \right| \\ &\ge \frac{1}{2N} \left(\frac{1}{\prod_{i=1}^{r} p_i!} \sum_{f_1,\dots,f_r} \left| \sum_{n=0}^{N-1} e\left(\sum_{i=1}^{r} f_i(n)/p_i \right) \right|^2 \right)^{3/2} \\ &\quad \cdot \left(\frac{1}{\prod_{i=1}^{r} p_i!} \sum_{f_1,\dots,f_r} \left| \sum_{n=0}^{N-1} e\left(\sum_{i=1}^{r} f_i(n)/p_i \right) \right|^4 \right)^{-1/2},\end{aligned}$$

where the last inequality follows from Lemma 4. Finally, Lemmas 6 and 9 can be used in order to obtain

$$\begin{aligned}\frac{1}{\prod_{i=1}^{r} p_i!} \sum_{f_1,\dots,f_r} D_{N;f_1,\dots,f_r} &> \frac{1}{2N} \left(\frac{N}{2} \right)^{3/2} \left(4.84 \cdot (12.27)^r N^2 \right)^{-1/2} \\ &> \frac{1}{12.45 \cdot (3.51)^r} N^{-1/2},\end{aligned}$$

which completes the proof. □

Theorem 4. *Let* $r = 1$ *and* $1 \le N \le m$. *Then the average value of the discrepancy* $D_{N;f_1}$ *in the (ordinary) nonlinear congruential method over all permutation polynomials* $f_1 : \mathbb{Z} \to \mathbb{Z}_m$ *of* $\mathbb{Z}_m$ *satisfies*

$$\frac{1}{m!} \sum_{f_1} D_{N;f_1} > \frac{1}{2\sqrt{2}} N^{-1/2} \left(1 - \frac{N}{m} \right)^{1/2}.$$

Proof. The desired estimate follows as in the proof of Theorem 3, where Lemmas 7 and 10 are used instead of Lemmas 6 and 9, respectively. □

4. Discussion

First, note that the results of the present paper apply for the ordinary nonlinear congruential method ($r = 1$) as well as for the compound method ($r \ge 2$). In the following, let the number r of prime factors of m be fixed. Then Theorem 1 shows that for any permutation polynomials $g_1, \dots, g_r$ the discrepancy $D_{N;\gamma_1 g_1,\dots,\gamma_r g_r}$, on the average over $\gamma_1, \dots, \gamma_r$, has an order of magnitude at most $N^{-1/2}(1 - N/m)^{1/2} \log m$. If N is not too large, this result is basically in accordance with the law of the iterated logarithm for the discrepancy of N true random numbers from $[0, 1)$, which is almost always of the order of magnitude $N^{-1/2}(\log \log N)^{1/2}$ (cf. [1]). Of course, the upper bound in Theorem 1 remains valid for the average value of the discrepancy $D_{N;f_1,\dots,f_r}$ over all permutation polynomials $f_1, \dots, f_r$. Theorem 2 provides even more information, since it implies that for any permutation polynomials $g_1, \dots, g_r$ only an arbitrarily small percentage of the parameters $\gamma_1, \dots, \gamma_r$ may lead to a discrepancy $D_{N;\gamma_1 g_1,\dots,\gamma_r g_r}$ of an order of

magnitude greater than $N^{-1/2}(1-N/m)^{1/2}\log m$. On the other hand, Theorem 3 shows that the average value of the discrepancy $D_{N;f_1,\dots,f_r}$ over all permutation polynomials $f_1,\dots,f_r$ is of an order of magnitude at least $N^{-1/2}$, provided N is not too large, which implies that the upper bound in Theorem 1 is in general best possible up to the logarithmic factor. Finally, Theorem 4 yields a slightly improved version of the lower bound in case of the ordinary nonlinear congruential method.

Acknowledgment

The authors would like to thank the referee for valuable comments.

References

1. K.L. Chung, *An estimate concerning the Kolmogoroff limit distribution*, Trans. Amer. Math. Soc. **67** (1949), 36–50. MR **11:**606c
2. J. Eichenauer–Herrmann, *Inversive congruential pseudorandom numbers: a tutorial*, Int. Statist. Rev. **60** (1992), 167–176.
3. ———, *Equidistribution properties of nonlinear congruential pseudorandom numbers*, Metrika **40** (1993), 333–338. MR **95a:**65018
4. ———, *Compound nonlinear congruential pseudorandom numbers*, Monatsh. Math. **117** (1994), 213–222. MR **96f:**11099
5. ———, *Pseudorandom number generation by nonlinear methods*, Int. Statist. Rev. **63** (1995), 247–255.
6. ———, *A unified approach to the analysis of compound pseudorandom numbers*, Finite Fields and Their Appl. **1** (1995), 102–114. MR **96h:**11075
7. J. Eichenauer–Herrmann and G. Larcher, *Average behaviour of compound nonlinear congruential pseudorandom numbers*, Finite Fields and Their Appl. **2** (1996), 111–123. CMP 96:07
8. J. Eichenauer–Herrmann and H. Niederreiter, *On the statistical independence of nonlinear congruential pseudorandom numbers*, ACM Trans. Modeling and Computer Simulation **4** (1994), 89–95.
9. H. Niederreiter, *Statistical independence of nonlinear congruential pseudorandom numbers*, Monatsh. Math. **106** (1988), 149–159. MR **89j:**11079
10. ———, *Recent trends in random number and random vector generation*, Ann. Operations Res. **31** (1991), 323–345. MR **92h:**65010
11. ———, *Nonlinear methods for pseudorandom number and vector generation*, Simulation and Optimization (G. Pflug and U. Dieter, eds.), Lecture Notes in Econom. and Math. Systems, vol. 374, Springer, Berlin, 1992, pp. 145–153.
12. ———, *Random Number Generation and Quasi–Monte Carlo Methods*, SIAM, Philadelphia, PA, 1992. MR **93h:**65008
13. ———, *Finite fields, pseudorandom numbers, and quasirandom points*, Finite Fields, Coding Theory, and Advances in Communications and Computing (G.L. Mullen and P.J.-S. Shiue, eds.), Dekker, New York, 1993, pp. 375–394. MR **94a:**11121

Fachbereich Mathematik, Technische Hochschule Darmstadt, Schlossgartenstrasse 7, D–64289 Darmstadt, F.R. Germany

Institut für Mathematik, Universität Salzburg, Hellbrunner Strasse 34, A–5020 Salzburg, Austria

E-mail address: Gerhard.Larcher@sbg.ac.at