

COMPOUND INVERSIVE CONGRUENTIAL PSEUDORANDOM NUMBERS: AN AVERAGE-CASE ANALYSIS

JÜRGEN EICHENAUER-HERRMANN AND FRANK EMMERICH

ABSTRACT. The present paper deals with the compound (or generalized) inversive congruential method for generating uniform pseudorandom numbers, which has been introduced recently. Equidistribution and statistical independence properties of the generated sequences over parts of the period are studied based on the discrepancy of certain point sets. The main result is an upper bound for the average value of these discrepancies. The method of proof is based on estimates for 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 attractive field of research is described in the survey articles [2, 5, 12, 13, 14] and in Niederreiter's excellent monograph [15]. A particularly promising approach is the inversive congruential method. The generated sequences of pseudorandom numbers have nice equidistribution and statistical independence properties (cf. [3, 10, 11]). Recently, a compound (or generalized) version of this method was introduced and analyzed (cf. [4, 8]), which shows some additional computational advantages. The present paper deals with the average behavior of these compound inversive congruential pseudorandom numbers and includes corresponding new results for the (ordinary) inversive congruential method.

Let $p_1, \dots, p_r \geq 5$ be distinct primes. For $1 \leq i \leq r$ identify $\mathbb{Z}_{p_i} = \{0, 1, \dots, p_i - 1\}$ with the finite field of order p_i . Let $a_i \in \mathbb{Z}_{p_i}^* = \mathbb{Z}_{p_i} \setminus \{0\}$ and let $(z_n^{(i)})_{n \geq 0}$ be a sequence in \mathbb{Z}_{p_i} with

$$z_{n+1}^{(i)} \equiv a_i(z_n^{(i)})^{-1} + 1 \pmod{p_i}, \quad n \geq 0,$$

where z^{-1} denotes the multiplicative inverse of z in $\mathbb{Z}_{p_i}^*$ and $0^{-1} = 0$. Obviously, the sequence $(z_n^{(i)})_{n \geq 0}$ is always purely periodic and p_i is the maximum possible period length. Let \mathbb{M}_{p_i} be the set of all $a_i \in \mathbb{Z}_{p_i}^*$ which belong to sequences with period length p_i . The set \mathbb{M}_{p_i} is always nonvoid and its elements can be characterized by properties of the polynomial $x^2 - x - a_i \in \mathbb{Z}_{p_i}[x]$ (cf. [7]). In the following, let $a_i \in \mathbb{M}_{p_i}$ and $c_i \in \mathbb{Z}_{p_i}^*$. Let $(y_n^{(i)})_{n \geq 0}$ with $y_0^{(i)} \equiv c_i z_0^{(i)} \pmod{p_i}$ and

$$y_{n+1}^{(i)} \equiv a_i c_i^2 (y_n^{(i)})^{-1} + c_i \pmod{p_i}, \quad n \geq 0,$$

Received by the editor September 19, 1994.

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

Key words and phrases. Uniform pseudorandom numbers, compound inversive congruential method, equidistribution, statistical independence, discrepancy, exponential sums.

be the corresponding (ordinary) *inversive congruential sequence* of elements of \mathbb{Z}_{p_i} , and let $(x_n^{(i)})_{n \geq 0}$ with

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

be the corresponding stream of (ordinary) *inversive congruential pseudorandom numbers*. A short calculation shows that

$$y_n^{(i)} \equiv c_i z_n^{(i)} \pmod{p_i}$$

for any $n \geq 0$. Now, a sequence $(x_n)_{n \geq 0}$ of *compound inversive congruential pseudorandom numbers* in the interval $[0, 1)$ is defined by

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

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

Equidistribution and statistical independence properties of the generated sequences, which are very important for their usability in a stochastic simulation, can be analyzed based on the discrepancy of s -tuples of successive pseudorandom numbers with $s = 1$ and $s \geq 2$, respectively. 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 . In the following, nonoverlapping s -tuples

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

of compound inversive congruential pseudorandom numbers are considered, and the abbreviation

$$D_{N; c_1, \dots, c_r}^{(s)} = D_N(\mathbf{x}_0, \mathbf{x}_1, \dots, \mathbf{x}_{N-1})$$

is used for $1 \leq N \leq m$. The main result of the present paper is established in the third section, namely an upper bound for the average value of the discrepancy $D_{N; c_1, \dots, c_r}^{(s)}$ over the parameters c_1, \dots, c_r . A detailed discussion of this result is given in the fourth section. The second section contains necessary auxiliary results.

2. AUXILIARY RESULTS

First, some further notation is necessary. 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 $e(t) = e^{2\pi it}$ is used, and $\mathbf{u} \cdot \mathbf{v}$ stands for the standard inner product of $\mathbf{u}, \mathbf{v} \in \mathbb{R}^k$. Subsequently, three known general results are stated which follow from [15, Theorem 3.10 and Corollary 3.17] and [6, Lemma 3], respectively.

Lemma 1. *Let $N \geq 1$ and $q \geq 2$ be integers. Let $\mathbf{t}_n = \mathbf{y}_n/q \in [0, 1)^k$ with $\mathbf{y}_n \in \{0, 1, \dots, q-1\}^k$ for $0 \leq n < N$. 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. *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 3. *Let $q \geq 2$ be an integer. Then*

$$\sum_{\substack{\mathbf{h} \in C_k(q) \\ \mathbf{h} \equiv \mathbf{0} \pmod{d}}} \frac{1}{r(\mathbf{h}, q)} < \frac{1}{d} \left(\frac{2}{\pi} \log q + \frac{7}{5} \right)^k$$

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

Subsequently, the s -tuples

$$\mathbf{z}_n^{(i)} = (z_{sn}^{(i)}, z_{sn+1}^{(i)}, \dots, z_{sn+s-1}^{(i)}) \in \mathbb{Z}_{p_i}^s$$

for $1 \leq i \leq r$ and $n \geq 0$ play a crucial role for the analysis of the discrepancy $D_{N; c_1, \dots, c_r}^{(s)}$.

Lemma 4. *Let $1 \leq i \leq r$, $1 \leq s < p_i$, $h_0 \in \mathbb{Z}$, and $\mathbf{h} \in \mathbb{Z}^s$ with $\mathbf{h} \not\equiv \mathbf{0} \pmod{p_i}$. Then*

$$\#\{0 \leq n < p_i | \mathbf{h} \cdot \mathbf{z}_n^{(i)} \equiv h_0 \pmod{p_i}\} \leq 2s - 1.$$

Proof. Let $\mathbf{h} = (h_1, \dots, h_s)$. Since the sequence $(z_n^{(i)})_{n \geq 0}$ has period length p_i , one obtains

$$\begin{aligned}
& \#\{0 \leq n < p_i \mid \mathbf{h} \cdot \mathbf{z}_n^{(i)} \equiv h_0 \pmod{p_i}\} \\
&= \#\{0 \leq n < p_i \mid h_1 z_{sn}^{(i)} + \cdots + h_s z_{sn+s-1}^{(i)} \equiv h_0 \pmod{p_i}\} \\
&= \#\{0 \leq n < p_i \mid h_1 z_n^{(i)} + \cdots + h_s z_{n+s-1}^{(i)} \equiv h_0 \pmod{p_i}\} \\
&\leq s-1 + \#\{0 \leq n < p_i \mid z_n^{(i)} \cdots z_{n+s-2}^{(i)} \neq 0, \\
&\quad h_1 z_n^{(i)} + \cdots + h_s z_{n+s-1}^{(i)} \equiv h_0 \pmod{p_i}\} \\
&\leq 2s-1,
\end{aligned}$$

where the last inequality follows from [1, Theorem], [15, Theorem 8.6] which says that the hyperplane

$$H = \{(z_1, \dots, z_s) \in \mathbb{Z}_{p_i}^s \mid h_1 z_1 + \cdots + h_s z_s \equiv h_0 \pmod{p_i}\}$$

contains at most s of the points $(z_n^{(i)}, \dots, z_{n+s-1}^{(i)})$ with $z_n^{(i)} \cdots z_{n+s-2}^{(i)} \neq 0$ and $0 \leq n < p_i$. \square

In the following, let $m_I = \prod_{i \in I} p_i$ for subsets I of $\{1, \dots, r\}$.

Lemma 5. *Let $1 \leq s < \min\{p_1, \dots, p_r\}$, $1 \leq N \leq m$, $\mathbf{h} \in C_s(m)$, and $J = \{1 \leq i \leq r \mid \mathbf{h} \equiv \mathbf{0} \pmod{p_i}\}$. Then*

$$\sum_{(c_1, \dots, c_r) \in \mathbb{Z}_{p_1}^* \times \cdots \times \mathbb{Z}_{p_r}^*} \left| \sum_{n=0}^{N-1} e \left(\sum_{i=1}^r c_i (\mathbf{h} \cdot \mathbf{z}_n^{(i)}) / p_i \right) \right|^2 \leq N m_J^2 \prod_{\substack{i=1 \\ i \notin J}}^r (2s(p_i - 1) + 1).$$

Proof. Straightforward calculations show that

$$\begin{aligned}
& \sum_{(c_1, \dots, c_r) \in \mathbb{Z}_{p_1}^* \times \cdots \times \mathbb{Z}_{p_r}^*} \left| \sum_{n=0}^{N-1} e \left(\sum_{i=1}^r c_i (\mathbf{h} \cdot \mathbf{z}_n^{(i)}) / p_i \right) \right|^2 \\
&= \sum_{(c_1, \dots, c_r) \in \mathbb{Z}_{p_1}^* \times \cdots \times \mathbb{Z}_{p_r}^*} \sum_{k, n=0}^{N-1} e \left(\sum_{i=1}^r c_i (\mathbf{h} \cdot \mathbf{z}_n^{(i)} - \mathbf{h} \cdot \mathbf{z}_k^{(i)}) / p_i \right) \\
&= \sum_{k, n=0}^{N-1} \sum_{(c_1, \dots, c_r) \in \mathbb{Z}_{p_1}^* \times \cdots \times \mathbb{Z}_{p_r}^*} \prod_{i=1}^r e(c_i (\mathbf{h} \cdot \mathbf{z}_n^{(i)} - \mathbf{h} \cdot \mathbf{z}_k^{(i)}) / p_i) \\
&= \sum_{k, n=0}^{N-1} \prod_{i=1}^r \sum_{c \in \mathbb{Z}_{p_i}^*} e(c (\mathbf{h} \cdot \mathbf{z}_n^{(i)} - \mathbf{h} \cdot \mathbf{z}_k^{(i)}) / p_i).
\end{aligned}$$

Since

$$\sum_{c \in \mathbb{Z}_{p_i}^*} e(c(\mathbf{h} \cdot \mathbf{z}_n^{(i)} - \mathbf{h} \cdot \mathbf{z}_k^{(i)})/p_i) = \begin{cases} p_i - 1 & \text{for } \mathbf{h} \cdot \mathbf{z}_n^{(i)} \equiv \mathbf{h} \cdot \mathbf{z}_k^{(i)} \pmod{p_i}, \\ -1 & \text{for } \mathbf{h} \cdot \mathbf{z}_n^{(i)} \not\equiv \mathbf{h} \cdot \mathbf{z}_k^{(i)} \pmod{p_i} \end{cases}$$

for $1 \leq i \leq r$ and $0 \leq k, n < N$, it follows that

$$\begin{aligned} & \sum_{(c_1, \dots, c_r) \in \mathbb{Z}_{p_1}^* \times \dots \times \mathbb{Z}_{p_r}^*} \left| \sum_{n=0}^{N-1} e \left(\sum_{i=1}^r c_i (\mathbf{h} \cdot \mathbf{z}_n^{(i)})/p_i \right) \right|^2 \\ &= \sum_{k, n=0}^{N-1} (-1)^r \prod_{\substack{i=1 \\ \mathbf{h} \cdot \mathbf{z}_n^{(i)} \equiv \mathbf{h} \cdot \mathbf{z}_k^{(i)} \pmod{p_i}}}^r (1 - p_i) \\ &\leq \sum_{k, n=0}^{N-1} \prod_{\substack{i=1 \\ \mathbf{h} \cdot \mathbf{z}_n^{(i)} \equiv \mathbf{h} \cdot \mathbf{z}_k^{(i)} \pmod{p_i}}}^r (p_i - 1) \\ &= \sum_{I \subset \{1, \dots, r\}} \sum_{\substack{k, n=0 \\ \mathbf{h} \cdot \mathbf{z}_n^{(i)} \equiv \mathbf{h} \cdot \mathbf{z}_k^{(i)} \pmod{p_i}, i \in I \\ \mathbf{h} \cdot \mathbf{z}_n^{(i)} \not\equiv \mathbf{h} \cdot \mathbf{z}_k^{(i)} \pmod{p_i}, i \notin I}}^{N-1} \prod_{i \in I} (p_i - 1) \\ &\leq \sum_{I \subset \{1, \dots, r\}} \sum_{\substack{k, n=0 \\ \mathbf{h} \cdot \mathbf{z}_n^{(i)} \equiv \mathbf{h} \cdot \mathbf{z}_k^{(i)} \pmod{p_i}, i \in I}}^{N-1} \prod_{i \in I} (p_i - 1) \\ &= \sum_{I \subset \{1, \dots, r\}} \sum_{k=0}^{N-1} \#\{0 \leq n < N \mid \mathbf{h} \cdot \mathbf{z}_n^{(i)} \equiv \mathbf{h} \cdot \mathbf{z}_k^{(i)} \pmod{p_i}, i \in I\} \\ &\quad \cdot \prod_{i \in I} (p_i - 1). \end{aligned}$$

Now, the definition of the set J implies that

$$\begin{aligned} & \#\{0 \leq n < N \mid \mathbf{h} \cdot \mathbf{z}_n^{(i)} \equiv \mathbf{h} \cdot \mathbf{z}_k^{(i)} \pmod{p_i}, i \in I\} \\ &= \#\{0 \leq n < N \mid \mathbf{h} \cdot \mathbf{z}_n^{(i)} \equiv \mathbf{h} \cdot \mathbf{z}_k^{(i)} \pmod{p_i}, i \in I \setminus J\} \\ &\leq \#\{0 \leq n < m \mid \mathbf{h} \cdot \mathbf{z}_n^{(i)} \equiv \mathbf{h} \cdot \mathbf{z}_k^{(i)} \pmod{p_i}, i \in I \setminus J\} \\ &= \frac{m}{m_{I \setminus J}} \#\{0 \leq n < m_{I \setminus J} \mid \mathbf{h} \cdot \mathbf{z}_n^{(i)} \equiv \mathbf{h} \cdot \mathbf{z}_k^{(i)} \pmod{p_i}, i \in I \setminus J\} \\ &= \frac{m}{m_{I \setminus J}} \prod_{i \in I \setminus J} \#\{0 \leq n < p_i \mid \mathbf{h} \cdot \mathbf{z}_n^{(i)} \equiv \mathbf{h} \cdot \mathbf{z}_k^{(i)} \pmod{p_i}\} \end{aligned}$$

for $0 \leq k < N$ and $I \subset \{1, \dots, r\}$, where in the last step the Chinese Remainder Theorem has been used. Since $\mathbf{h} \not\equiv \mathbf{0} \pmod{p_i}$ for $i \in \{1, \dots, r\} \setminus J$, it follows from Lemma 4 that

$$\#\{0 \leq n < p_i \mid \mathbf{h} \cdot \mathbf{z}_n^{(i)} \equiv \mathbf{h} \cdot \mathbf{z}_k^{(i)} \pmod{p_i}\} \leq 2s - 1$$

for $0 \leq k < N$ and $i \in \{1, \dots, r\} \setminus J$. Therefore,

$$\begin{aligned}
& \sum_{(c_1, \dots, c_r) \in \mathbb{Z}_{p_1}^* \times \dots \times \mathbb{Z}_{p_r}^*} \left| \sum_{n=0}^{N-1} e \left(\sum_{i=1}^r c_i (\mathbf{h} \cdot \mathbf{z}_n^{(i)}) / p_i \right) \right|^2 \\
& \leq Nm \sum_{I \subset \{1, \dots, r\}} \prod_{i \in I \setminus J} \frac{2s-1}{p_i} \prod_{i \in I} (p_i - 1) \\
& = Nm \sum_{I \subset \{1, \dots, r\}} \prod_{i \in I \setminus J} \frac{(2s-1)(p_i - 1)}{p_i} \prod_{i \in I \cap J} (p_i - 1) \\
& = Nm \prod_{\substack{i=1 \\ i \notin J}}^r \left(\frac{(2s-1)(p_i - 1)}{p_i} + 1 \right) \prod_{i \in J} p_i \\
& = Nm_J^2 \prod_{\substack{i=1 \\ i \notin J}}^r (2s(p_i - 1) + 1),
\end{aligned}$$

which is the desired result. \square

Lemma 6. *Let $1 \leq s < \min\{p_1, \dots, p_r\}$ and $1 \leq N \leq 2^{-(r+1)} \prod_{i=1}^r (p_i - 1)$. Then*

$$\sum_{(c_1, \dots, c_r) \in \mathbb{Z}_{p_1}^* \times \dots \times \mathbb{Z}_{p_r}^*} \left| \sum_{n=0}^{N-1} e \left(\sum_{i=1}^r c_i z_{sn}^{(i)} / p_i \right) \right|^2 > \frac{N}{2} \prod_{i=1}^r (p_i - 1).$$

Proof. Straightforward calculations show that

$$\begin{aligned}
& \sum_{(c_1, \dots, c_r) \in \mathbb{Z}_{p_1}^* \times \dots \times \mathbb{Z}_{p_r}^*} \left| \sum_{n=0}^{N-1} e \left(\sum_{i=1}^r c_i z_{sn}^{(i)} / p_i \right) \right|^2 \\
& = \sum_{I \subset \{1, \dots, r\}} (-1)^{r-\#I} \sum_{c_i \in \mathbb{Z}_{p_i}, i \in I} \left| \sum_{n=0}^{N-1} e \left(\sum_{i \in I} c_i z_{sn}^{(i)} / p_i \right) \right|^2 \\
& = \sum_{I \subset \{1, \dots, r\}} (-1)^{r-\#I} \sum_{c_i \in \mathbb{Z}_{p_i}, i \in I} \sum_{k, n=0}^{N-1} \prod_{i \in I} e(c_i (z_{sn}^{(i)} - z_{sk}^{(i)}) / p_i) \\
& = \sum_{I \subset \{1, \dots, r\}} (-1)^{r-\#I} \sum_{k, n=0}^{N-1} \prod_{i \in I} \sum_{c \in \mathbb{Z}_{p_i}} e(c (z_{sn}^{(i)} - z_{sk}^{(i)}) / p_i) \\
& = \sum_{I \subset \{1, \dots, r\}} (-1)^{r-\#I} \sum_{\substack{k, n=0 \\ z_{sn}^{(i)} = z_{sk}^{(i)}, i \in I}}^{N-1} m_I \\
& = \sum_{I \subset \{1, \dots, r\}} (-1)^{r-\#I} m_I \cdot \#\{(k, n) \in \mathbb{Z}_N^2 \mid n \equiv k \pmod{m_I}\},
\end{aligned}$$

where $\mathbb{Z}_N = \{0, 1, \dots, N-1\}$. Let $N_I \in \mathbb{Z}_{m_I}$ with $N_I \equiv N \pmod{m_I}$ for subsets I of $\{1, \dots, r\}$ and observe that $m_I[N/m_I] = N - N_I$. Then

$$\begin{aligned}
& m_I \cdot \#\{(k, n) \in \mathbb{Z}_N^2 \mid n \equiv k \pmod{m_I}\} \\
& = m_I([N/m_I](N + N_I) + N_I) = (N - N_I)(N + N_I) + m_I N_I
\end{aligned}$$

for $I \subset \{1, \dots, r\}$. Hence,

$$\begin{aligned}
 & \sum_{(c_1, \dots, c_r) \in \mathbb{Z}_{p_1}^* \times \dots \times \mathbb{Z}_{p_r}^*} \left| \sum_{n=0}^{N-1} e \left(\sum_{i=1}^r c_i z_{sn}^{(i)} / p_i \right) \right|^2 \\
 &= \sum_{I \subset \{1, \dots, r\}} (-1)^{r-\#I} (N^2 - N_I^2 + m_I N_I) \\
 &= N^2 \sum_{I \subset \{1, \dots, r\}} (-1)^{r-\#I} + \sum_{I \subset \{1, \dots, r\}} (-1)^{r-\#I} N_I (m_I - N_I) \\
 &= \sum_{I \subset \{1, \dots, r\}} (-1)^{r-\#I} N_I (m_I - N_I) \\
 &= \sum_{\substack{I \subset \{1, \dots, r\} \\ m_I > N}} (-1)^{r-\#I} N (m_I - N) + \sum_{\substack{I \subset \{1, \dots, r\} \\ m_I \leq N}} (-1)^{r-\#I} N_I (m_I - N_I) \\
 &= \sum_{I \subset \{1, \dots, r\}} (-1)^{r-\#I} N (m_I - N) \\
 &\quad + \sum_{\substack{I \subset \{1, \dots, r\} \\ m_I \leq N}} (-1)^{r-\#I} (N_I (m_I - N_I) + N (N - m_I)) \\
 &= N \prod_{i=1}^r (p_i - 1) + \sum_{\substack{I \subset \{1, \dots, r\} \\ m_I \leq N}} (-1)^{r-\#I} (N_I (m_I - N_I) + N (N - m_I)) \\
 &\geq N \prod_{i=1}^r (p_i - 1) - \sum_{\substack{I \subset \{1, \dots, r\} \\ m_I \leq N}} (N_I (m_I - N_I) + N (N - m_I)) \\
 &\geq N \prod_{i=1}^r (p_i - 1) - \sum_{\substack{I \subset \{1, \dots, r\} \\ m_I \leq N}} \left(N - \frac{1}{2} m_I \right)^2 \\
 &> N \prod_{i=1}^r (p_i - 1) - 2^r N^2 \geq \frac{N}{2} \prod_{i=1}^r (p_i - 1)
 \end{aligned}$$

for $N \leq 2^{-(r+1)} \prod_{i=1}^r (p_i - 1)$. \square

3. PRINCIPAL RESULTS

The main result of the present paper is Theorem 1, which provides an upper bound for the average value of the discrepancy of s -tuples in the compound inversive congruential method over the parameters $(c_1, \dots, c_r) \in \mathbb{Z}_{p_1}^* \times \dots \times \mathbb{Z}_{p_r}^*$. Theorem 2 is an immediate consequence of this result. A proof is added for the sake of completeness. In Theorem 3 a corresponding lower bound for the discrepancy of s -tuples is established.

Theorem 1. *Let $1 \leq s < \min\{p_1, \dots, p_r\}$, $1 \leq N \leq m$, and $a_i \in \mathbb{M}_{p_i}$ for $1 \leq i \leq r$. Then the average value of the discrepancy $D_{N; c_1, \dots, c_r}^{(s)}$ of s -tuples in the compound*

inversive congruential method over $(c_1, \dots, c_r) \in \mathbb{Z}_{p_1}^* \times \dots \times \mathbb{Z}_{p_r}^*$ satisfies

$$\frac{1}{\prod_{i=1}^r (p_i - 1)} \sum_{(c_1, \dots, c_r) \in \mathbb{Z}_{p_1}^* \times \dots \times \mathbb{Z}_{p_r}^*} D_{N; c_1, \dots, c_r}^{(s)} < (\sqrt{2s + 0.25} + 0.5)^r N^{-1/2} \left(\frac{2}{\pi} \log m + \frac{7}{5} \right)^s.$$

Proof. First, Lemma 1 is applied with $k = s, q = m$, and $\mathbf{t}_n = \mathbf{x}_n$ for $0 \leq n < N$. This yields

$$\begin{aligned} D_{N; c_1, \dots, c_r}^{(s)} &\leq \frac{s}{m} + \frac{1}{N} \sum_{\mathbf{h} \in C_s(m)} \frac{1}{r(\mathbf{h}, m)} \left| \sum_{n=0}^{N-1} e(\mathbf{h} \cdot \mathbf{x}_n) \right| \\ &= \frac{s}{m} + \frac{1}{N} \sum_{\mathbf{h} \in C_s(m)} \frac{1}{r(\mathbf{h}, m)} \left| \sum_{n=0}^{N-1} e \left(\sum_{i=1}^r c_i(\mathbf{h} \cdot \mathbf{z}_n^{(i)})/p_i \right) \right| \end{aligned}$$

for any $(c_1, \dots, c_r) \in \mathbb{Z}_{p_1}^* \times \dots \times \mathbb{Z}_{p_r}^*$, where the s -tuple $\mathbf{z}_n^{(i)}$ is defined as in the second section. Therefore, the average value of the discrepancy $D_{N; c_1, \dots, c_r}^{(s)}$ over $(c_1, \dots, c_r) \in \mathbb{Z}_{p_1}^* \times \dots \times \mathbb{Z}_{p_r}^*$ satisfies

$$\begin{aligned} \frac{1}{\prod_{i=1}^r (p_i - 1)} \sum_{(c_1, \dots, c_r) \in \mathbb{Z}_{p_1}^* \times \dots \times \mathbb{Z}_{p_r}^*} D_{N; c_1, \dots, c_r}^{(s)} &\leq \frac{s}{m} + \frac{1}{N} \sum_{\mathbf{h} \in C_s(m)} \frac{1}{r(\mathbf{h}, m)} \\ &\cdot \left(\frac{1}{\prod_{i=1}^r (p_i - 1)} \sum_{(c_1, \dots, c_r) \in \mathbb{Z}_{p_1}^* \times \dots \times \mathbb{Z}_{p_r}^*} \left| \sum_{n=0}^{N-1} e \left(\sum_{i=1}^r c_i(\mathbf{h} \cdot \mathbf{z}_n^{(i)})/p_i \right) \right| \right) \\ &\leq \frac{s}{m} + \frac{1}{N} \sum_{\mathbf{h} \in C_s(m)} \frac{1}{r(\mathbf{h}, m)} \\ &\cdot \sqrt{\frac{1}{\prod_{i=1}^r (p_i - 1)} \sum_{(c_1, \dots, c_r) \in \mathbb{Z}_{p_1}^* \times \dots \times \mathbb{Z}_{p_r}^*} \left| \sum_{n=0}^{N-1} e \left(\sum_{i=1}^r c_i(\mathbf{h} \cdot \mathbf{z}_n^{(i)})/p_i \right) \right|^2} \\ &= \frac{s}{m} + \frac{1}{N} \sum_{\substack{J \subset \{1, \dots, r\} \\ \#J < r}} \sum_{\substack{\mathbf{h} \in C_s(m) \\ \mathbf{h} \equiv \mathbf{0} \pmod{p_i}, i \in J \\ \mathbf{h} \not\equiv \mathbf{0} \pmod{p_i}, i \notin J}} \frac{1}{r(\mathbf{h}, m)} \\ &\cdot \sqrt{\frac{1}{\prod_{i=1}^r (p_i - 1)} \sum_{(c_1, \dots, c_r) \in \mathbb{Z}_{p_1}^* \times \dots \times \mathbb{Z}_{p_r}^*} \left| \sum_{n=0}^{N-1} e \left(\sum_{i=1}^r c_i(\mathbf{h} \cdot \mathbf{z}_n^{(i)})/p_i \right) \right|^2}, \end{aligned}$$

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

$$\begin{aligned}
 & \frac{1}{\prod_{i=1}^r (p_i - 1)} \sum_{(c_1, \dots, c_r) \in \mathbb{Z}_{p_1}^* \times \dots \times \mathbb{Z}_{p_r}^*} D_{N; c_1, \dots, c_r}^{(s)} \\
 & \leq \frac{s}{m} + \frac{1}{N} \sum_{\substack{J \subset \{1, \dots, r\} \\ \#J < r}} \sum_{\substack{\mathbf{h} \in C_s(m) \\ \mathbf{h} \equiv \mathbf{0} \pmod{p_i}, i \in J \\ \mathbf{h} \not\equiv \mathbf{0} \pmod{p_i}, i \notin J}} \frac{1}{r(\mathbf{h}, m)} \\
 & \quad \cdot \sqrt{Nm_J^2 \prod_{\substack{i=1 \\ i \notin J}}^r (2s + (p_i - 1)^{-1}) \prod_{i \in J} (p_i - 1)^{-1}} \\
 & \leq \frac{s}{m} + \frac{1}{N^{1/2}} \sum_{\substack{J \subset \{1, \dots, r\} \\ \#J < r}} \prod_{\substack{i=1 \\ i \notin J}}^r (2s + (p_i - 1)^{-1})^{1/2} \\
 & \quad \cdot \prod_{i \in J} (p_i - 1)^{-1/2} m_J \sum_{\substack{\mathbf{h} \in C_s(m) \\ \mathbf{h} \equiv \mathbf{0} \pmod{m_J}}} \frac{1}{r(\mathbf{h}, m)},
 \end{aligned}$$

where $m_J = \prod_{i \in J} p_i$ for subsets J of $\{1, \dots, r\}$. Hence, it follows from Lemma 3 that

$$\begin{aligned}
 & \frac{1}{\prod_{i=1}^r (p_i - 1)} \sum_{(c_1, \dots, c_r) \in \mathbb{Z}_{p_1}^* \times \dots \times \mathbb{Z}_{p_r}^*} D_{N; c_1, \dots, c_r}^{(s)} \\
 & < \frac{s}{m} + \frac{1}{N^{1/2}} \sum_{\substack{J \subset \{1, \dots, r\} \\ \#J < r}} \prod_{\substack{i=1 \\ i \notin J}}^r (2s + (p_i - 1)^{-1})^{1/2} \\
 & \quad \cdot \prod_{i \in J} (p_i - 1)^{-1/2} \left(\frac{2}{\pi} \log m + \frac{7}{5} \right)^s \\
 & < \frac{1}{N^{1/2}} \sum_{\substack{J \subset \{1, \dots, r\} \\ \#J < r}} \prod_{\substack{i=1 \\ i \notin J}}^r (2s + (p_i - 1)^{-1})^{1/2} \\
 & \quad \cdot \prod_{i \in J} (p_i - 1)^{-1/2} \left(\frac{2}{\pi} \log m + \frac{7}{5} \right)^s \\
 & = \frac{1}{N^{1/2}} \prod_{i=1}^r ((2s + (p_i - 1)^{-1})^{1/2} + (p_i - 1)^{-1/2}) \left(\frac{2}{\pi} \log m + \frac{7}{5} \right)^s \\
 & \leq \frac{1}{N^{1/2}} ((2s + 0.25)^{1/2} + 0.5)^r \left(\frac{2}{\pi} \log m + \frac{7}{5} \right)^s,
 \end{aligned}$$

which is the desired result. □

Theorem 2. *Let $1 \leq s < \min\{p_1, \dots, p_r\}$, $1 \leq N \leq m$, and $a_i \in \mathbb{M}_{p_i}$ for $1 \leq i \leq r$ be fixed. Let $0 < \alpha \leq 1$. Then there exist more than $(1 - \alpha) \prod_{i=1}^r (p_i - 1)$ values of $(c_1, \dots, c_r) \in \mathbb{Z}_{p_1}^* \times \dots \times \mathbb{Z}_{p_r}^*$ such that the discrepancy $D_{N; c_1, \dots, c_r}^{(s)}$ of s -tuples in the*

compound inversive congruential method satisfies

$$D_{N;c_1,\dots,c_r}^{(s)} < \frac{1}{\alpha} (\sqrt{2s + 0.25} + 0.5)^r N^{-1/2} \left(\frac{2}{\pi} \log m + \frac{7}{5} \right)^s.$$

Proof. Subsequently, the abbreviation

$$M = (\sqrt{2s + 0.25} + 0.5)^r N^{-1/2} \left(\frac{2}{\pi} \log m + \frac{7}{5} \right)^s$$

is used. Suppose that there exist at most $(1 - \alpha) \prod_{i=1}^r (p_i - 1)$ values of $(c_1, \dots, c_r) \in \mathbb{Z}_{p_1}^* \times \dots \times \mathbb{Z}_{p_r}^*$ with $D_{N;c_1,\dots,c_r}^{(s)} < \alpha^{-1}M$, i.e., there exist at least $\alpha \prod_{i=1}^r (p_i - 1)$ values of $(c_1, \dots, c_r) \in \mathbb{Z}_{p_1}^* \times \dots \times \mathbb{Z}_{p_r}^*$ with $D_{N;c_1,\dots,c_r}^{(s)} \geq \alpha^{-1}M$. Hence, one obtains

$$\sum_{(c_1,\dots,c_r) \in \mathbb{Z}_{p_1}^* \times \dots \times \mathbb{Z}_{p_r}^*} D_{N;c_1,\dots,c_r}^{(s)} \geq M \prod_{i=1}^r (p_i - 1),$$

which contradicts Theorem 1. □

Theorem 3. *Let $1 \leq s < \min\{p_1, \dots, p_r\}$, $1 \leq N \leq 2^{-(r+1)} \prod_{i=1}^r (p_i - 1)$, and $a_i \in \mathbb{M}_{p_i}$ for $1 \leq i \leq r$ be fixed. Then there exist parameters $(c_1, \dots, c_r) \in \mathbb{Z}_{p_1}^* \times \dots \times \mathbb{Z}_{p_r}^*$ such that the discrepancy $D_{N;c_1,\dots,c_r}^{(s)}$ of s -tuples in the compound inversive congruential method satisfies*

$$D_{N;c_1,\dots,c_r}^{(s)} > \frac{1}{2\sqrt{2}} N^{-1/2}.$$

Proof. First, Lemma 2 is applied with $k = s$, $\mathbf{t}_n = \mathbf{x}_n$ for $0 \leq n < N$, and $\mathbf{h} = (1, 0, \dots, 0) \in \mathbb{Z}^s$. This yields

$$D_{N;c_1,\dots,c_r}^{(s)} \geq \frac{1}{2N} \left| \sum_{n=0}^{N-1} e \left(\sum_{i=1}^r c_i z_{sn}^{(i)} / p_i \right) \right|.$$

Now, the desired result follows at once from Lemma 6. □

4. DISCUSSION

First, it should be observed that the main results apply for the full period ($N = m$) as well as for parts of the period ($N < m$), for equidistribution properties ($s = 1$) as well as for statistical independence properties ($s \geq 2$), and for the ordinary inversive congruential method ($r = 1$) as well as for the compound method ($r \geq 2$). In the following, let the number r of prime factors of m be fixed. Then Theorem 1 shows that for any parameters $a_1 \in \mathbb{M}_{p_1}, \dots, a_r \in \mathbb{M}_{p_r}$ in the compound inversive congruential method and any dimension s the discrepancy $D_{N;c_1,\dots,c_r}^{(s)}$, on the average over the parameters c_1, \dots, c_r , has an order of magnitude at most $N^{-1/2}(\log m)^s$. It should be observed that this upper bound is independent of the specific choice of the parameters a_1, \dots, a_r . This result is basically in accordance with the law of the iterated logarithm for the discrepancy of N true random points from $[0, 1]^s$, which is almost always of an order of magnitude $N^{-1/2}(\log \log N)^{1/2}$ (cf. [9]). Theorem 2 provides even more information, since it implies that for any parameters a_1, \dots, a_r and any dimension s only an arbitrarily small percentage of the parameters c_1, \dots, c_r may lead to a discrepancy $D_{N;c_1,\dots,c_r}^{(s)}$ with an order of magnitude greater than $N^{-1/2}(\log m)^s$. On the other hand, Theorem 3 shows that for any parameters a_1, \dots, a_r and any dimension s there exist parameters c_1, \dots, c_r

such that the discrepancy $D_{N;c_1,\dots,c_r}^{(s)}$ is of an order of magnitude at least $N^{-1/2}$, provided N is not too large.

REFERENCES

1. J. Eichenauer-Herrmann, *Inversive congruential pseudorandom numbers avoid the planes*, Math. Comp. **56** (1991), 297–301. MR **91k**:65021
2. ———, *Inversive congruential pseudorandom numbers: a tutorial*, Internat. Statist. Rev. **60** (1992), 167–176.
3. ———, *Improved lower bounds for the discrepancy of inversive congruential pseudorandom numbers*, Math. Comp. **62** (1994), 783–786. MR **94g**:11058
4. ———, *On generalized inversive congruential pseudorandom numbers*, Math. Comp. **63** (1994), 293–299. MR **94k**:11088
5. ———, *Pseudorandom number generation by nonlinear methods*, Internat. 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.
7. M. Flahive and H. Niederreiter, *On inversive congruential generators for pseudorandom numbers*, Finite Fields, Coding Theory, and Advances in Communications and Computing (G. L. Mullen and P. J.-S. Shiue, eds.), Dekker, New York, 1993, pp. 75–80. MR **94a**:11117
8. K. Huber, *On the period length of generalized inversive pseudorandom number generators*, Appl. Algebra Engrg. Comm. Comput. **5** (1994), 255–260. CMP: 94 14
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. MR **24**:A1732
10. H. Niederreiter, *The serial test for congruential pseudorandom numbers generated by inversions*, Math. Comp. **52** (1989), 135–144. MR **90e**:65008
11. ———, *Lower bounds for the discrepancy of inversive congruential pseudorandom numbers*, Math. Comp. **55** (1990), 277–287. MR **91e**:65016
12. ———, *Recent trends in random number and random vector generation*, Ann. Oper. Res. **31** (1991), 323–345. MR **92h**:65010
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
14. ———, *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.
15. ———, *Random number generation and quasi-Monte Carlo methods*, SIAM, Philadelphia, PA, 1992. MR **93h**:65008

FACHBEREICH MATHEMATIK, TECHNISCHE HOCHSCHULE DARMSTADT, SCHLOSSGARTEN-STRASSE 7, D-64289 DARMSTADT, GERMANY