MATHEMATICS OF COMPUTATION
Volume 65, Number 214
April 1996, Pages 749–760

PSEUDORANDOM VECTOR GENERATION BY THE COMPOUND INVERSIVE METHOD

FRANK EMMERICH

Abstract. Pseudorandom vectors are of importance for parallelized simulation methods. In this paper a detailed analysis of the compound inversive method for the generation of k-dimensional uniform pseudorandom vectors, a vector analog of the compound inversive method for pseudorandom number generation, is carried out. In particular, periodicity properties and statistical independence properties of the generated sequences are studied based on the discrete discrepancy of s-tuples of successive terms in the sequence. The results show that the generated sequences have attractive statistical independence properties for pseudorandom vectors of dimensions $k \leq 4$.

1. Introduction

The generation of uniform pseudorandom numbers in the interval $[0,1)$ and of uniform pseudorandom vectors in the interval $[0,1)^k$ is a basic and crucial task in any stochastic simulation. A review of several methods is given in Niederreiter's monograph [12]. Since the simple nature of the classical linear congruential method for the generation of pseudorandom numbers and of the matrix method for the generation of pseudorandom vectors implies undesirable regularities (cf. [1]), several nonlinear methods for the generation of pseudorandom numbers and of pseudorandom vectors have been introduced [1, 2, 4, 5, 10, 11, 13]. A particularly attractive nonlinear approach is the inversive congruential method for the generation of pseudorandom numbers (cf. [1, 2, 5]) and the inversive method for the generation of pseudorandom vectors, which was introduced in [9] and is analyzed in detail in [14]. In [3] a compound version of the inversive congruential method for the generation of pseudorandom numbers was introduced in order to achieve a very long period length and an algorithm which allows a simple parallelized implementation. The analog of this approach for the generation of pseudorandom vectors, the compound inversive method, will be introduced and studied in this paper.

First, the generation of pseudorandom vectors by the (ordinary) *inversive method* is described, which is due to Niederreiter [14]. Let $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ for integers $n \geq 1$. Further, let $k \geq 1$ be an integer, the given dimension of the vectors to be generated. Choose a (large) prime p, and put $q = p^k$. Denote by F_q and F_q^* the finite field with q elements and its multiplicative group of nonzero elements, respectively. For $\gamma \in F_q^*$ define $\overline{\gamma} \in F_q^*$ by $\overline{\gamma} = \gamma^{-1}$, i.e., $\overline{\gamma}$ is the multiplicative

Received by the editor August 1, 1994.
1991 *Mathematics Subject Classification.* Primary 65C10; Secondary 11K45.
Key words and phrases. Uniform pseudorandom numbers, uniform pseudorandom vectors, inversive method, compound inversive method, statistical independence, discrete discrepancy, exponential sums.

inverse of γ in F_q^*, and put $\overline{0} = 0$. Now, parameters $\alpha, \beta \in F_q$ with $\alpha \neq 0$ are selected and a sequence $\gamma_0, \gamma_1, \ldots$ of elements of F_q is generated by choosing an initial value γ_0 and using the recursion

$$\gamma_{n+1} = \alpha\overline{\gamma}_n + \beta$$

for $n \geq 0$. Note that F_q can be viewed as a k-dimensional vector space over F_p (cf. [7, Chapter 1.4]). Let B be an ordered basis of F_q over F_p and denote by $\mathbf{c}_n \in F_p^k$ for $n \geq 0$ the coordinate vector of $\gamma_n \in F_q$ relative to B. Since $F_p = \mathbb{Z}/p\mathbb{Z}$ can be identified with the set $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ of integers, each vector $\mathbf{c}_n$ can be viewed as an element of $\mathbb{Z}_p^k$. Then

$$\mathbf{u}_n = \frac{1}{p}\mathbf{c}_n \in [0,1)^k$$

for $n \geq 0$ defines an *inversive sequence* $(\mathbf{u}_n)_{n\geq 0}$ of pseudorandom vectors.

Now, the *compound inversive method* for the generation of pseudorandom vectors is introduced. Let $m = \prod_{i=1}^r p_i$ for an integer $r \geq 1$ and arbitrary distinct primes $p_1, \ldots, p_r$. Let $m_i = m/p_i$ and $q_i = p_i^k$ for $1 \leq i \leq r$. Then for $1 \leq i \leq r$ sequences $(\gamma_n^{(i)})_{n\geq 0}$ of elements of F_{q_i} are generated by choosing an initial value $\gamma_0^{(i)}$ and using the recursion

$$\gamma_{n+1}^{(i)} = \alpha_i\overline{\gamma}_n^{(i)} + \beta_i$$

for $n \geq 0$, where $\alpha_i \in F_{q_i}^*$ and $\beta_i \in F_{q_i}$ are the parameters of the ith generator. Again, let $\mathbf{c}_n^{(i)}$ be the coordinate vector of $\gamma_n^{(i)}$ relative to an ordered basis B_i of F_{q_i} over F_{p_i} and let

$$\mathbf{u}_n^{(i)} = \frac{1}{p_i}\mathbf{c}_n^{(i)} \in [0,1)^k$$

for $n \geq 0$. Then a *compound inversive sequence* $(\mathbf{u}_n)_{n\geq 0}$ of pseudorandom vectors of $[0,1)^k$ is defined by

$$\mathbf{u}_n \equiv \mathbf{u}_n^{(1)} + \cdots + \mathbf{u}_n^{(r)} \pmod 1.$$

For $r = 1$ one has the (ordinary) inversive method, which is due to Niederreiter [14]. If $k = 1$, the compound inversive congruential method of Eichenauer-Herrmann [3] for the generation of pseudorandom numbers is obtained.

In §2 a criterion for the sequence $(\mathbf{u}_n)_{n\geq 0}$ having the maximum possible period length m^k will be established. A very important property that should be asked of pseudorandom numbers and of pseudorandom vectors for stochastic simulations is the statistical independence of successive terms in the generated sequence. A reliable theoretical approach for assessing statistical independence properties is based on the notion of *discrepancy* of s-tuples of successive terms in the sequence. Unfortunately, for $k \geq 3$ the discrepancy of an inversive sequence of pseudorandom vectors is dominated by the discretization error. So the *discrete discrepancy* and the *discrete star discrepancy* are introduced. These discrete versions of the corresponding ordinary discrepancies are natural quantities, since the considered pseudorandom vectors are rational points with fixed denominator m (cf. [14]). The definition of the discrete discrepancy and of the discrete star discrepancy, as well as general discrepancy estimates, are stated in §3. In §§5 and 6 upper and lower bounds for the discrete (star) discrepancy are established. These results rely heavily on bounds for certain rational exponential sums which are stated in §4.

2. Period length

In order to obtain a criterion for the maximum possible period length m^k of a compound inversive sequence of pseudorandom vectors, a corresponding result for the underlying inversive sequences is recalled from [14]. For $1 \leq i \leq r$ a key role is played by the polynomial

$$G_i(x) = x^2 - \beta_i x - \alpha_i \in F_{q_i}[x]$$

associated with the underlying recursion in the inversive method. This polynomial has the factorization

$$G_i(x) = (x - \sigma_i)(x - \tau_i)$$

with nonzero roots $\sigma_i, \tau_i \in F_{q_i^2}$, and the quotient $\sigma_i \tau_i^{-1}$ of these roots is decisive in the criterion below, which is due to Niederreiter [14, Theorem 1].

Lemma 1. *Let $1 \leq i \leq r$. The sequence $\mathbf{u}_0^{(i)}, \mathbf{u}_1^{(i)}, \dots$ of pseudorandom vectors generated by the inversive method has period length $q_i = p_i^k$ if and only if the order of $\sigma_i \tau_i^{-1}$ in the multiplicative group $F_{q_i^2}^*$ is equal to $q_i + 1$.*

In order to establish a criterion for the period length of a sequence of pseudorandom vectors generated by the compound inversive method, a sequence $(\mathbf{c}_n)_{n \geq 0}$ of vectors in $\mathbb{Z}_m^k$ is defined by

$$\mathbf{c}_n \equiv m_1 \mathbf{c}_n^{(1)} + \cdots + m_r \mathbf{c}_n^{(r)} \pmod{m},$$

i.e., $\mathbf{u}_n = \mathbf{c}_n / m$ for $n \geq 0$. Then the sequences $(\mathbf{c}_n)_{n \geq 0}$ and $(\mathbf{u}_n)_{n \geq 0}$ have the same period length. Obviously, the sequence $(\mathbf{c}_n)_{n \geq 0}$ has maximum possible period length m^k if and only if the sequences $(\mathbf{c}_n^{(i)})_{n \geq 0}$ have maximum possible period length q_i for $1 \leq i \leq r$. Since for $1 \leq i \leq r$ the recursion $\gamma_{n+1}^{(i)} = \alpha_i \overline{\gamma}_n^{(i)} + \beta_i$ is bijective in F_{q_i}, the sequence $(\mathbf{u}_n^{(i)})_{n \geq 0}$ and also the sequence $(\mathbf{u}_n)_{n \geq 0}$ are always purely periodic. Theorem 1 summarizes these properties.

Theorem 1. *The sequence $\mathbf{u}_0, \mathbf{u}_1, \dots$ of pseudorandom vectors generated by the compound inversive method is always purely periodic and has period length m^k if and only if the underlying inversive sequences $(\mathbf{u}_n^{(i)})_{n \geq 0}$ of pseudorandom vectors have period length q_i for $1 \leq i \leq r$.*

In this paper it will always be assumed that the compound inversive sequence $(\mathbf{u}_n)_{n \geq 0}$ has the maximum possible period length m^k. This standing hypothesis will not be mentioned explicitly in the results below.

3. General estimates for discrete discrepancies

As mentioned above, a reliable theoretical approach for assessing the statistical independence properties of a sequence of pseudorandom vectors is based on the *discrete* (*star*) *discrepancy* of s-tuples of successive terms in the sequence. Let $\mathbf{x}_n = M^{-1} \mathbf{y}_n \in [0,1)^d$ for $0 \leq n < N$, where $d \geq 1$ and $M \geq 2$ are integers and $\mathbf{y}_0, \mathbf{y}_1, \dots, \mathbf{y}_{N-1} \in \mathbb{Z}_M^d$ are N arbitrary lattice points. For any subinterval J of $[0,1)^d$, denote by $L(J)$ the number of points among $\mathbf{x}_0, \mathbf{x}_1, \dots, \mathbf{x}_{N-1}$ falling into J and let $\operatorname{Vol}(J)$ be the d-dimensional volume of J. Then the *discrete discrepancy* $E_{N,M}$ of the points $\mathbf{x}_0, \mathbf{x}_1, \dots, \mathbf{x}_{N-1}$ is defined by

$$E_{N,M} = E_{N,M}(\mathbf{x}_0, \mathbf{x}_1, \dots, \mathbf{x}_{N-1}) = \sup_{J \in \mathcal{J}_M} \left| \frac{L(J)}{N} - \operatorname{Vol}(J) \right|,$$

where $\mathcal{J}_M$ is the family of all subintervals J of $[0,1)^d$ of the form

$$J = \prod_{j=1}^{d} \Big[\frac{a_j}{M}, \frac{c_j}{M}\Big)$$

with integers $0 \le a_j < c_j \le M$ for $1 \le j \le d$. The *discrete star discrepancy* $E^*_{N,M}$ of the points $\mathbf{x}_0, \mathbf{x}_1, \dots, \mathbf{x}_{N-1}$ is defined by

$$E^*_{N,M} = E^*_{N,M}(\mathbf{x}_0, \mathbf{x}_1, \dots, \mathbf{x}_{N-1}) = \sup_{J \in \mathcal{J}^*_M} \left| \frac{L(J)}{N} - \operatorname{Vol}(J) \right|,$$

where $\mathcal{J}^*_M$ is the family of all subintervals J of $[0,1)^d$ of the form

$$J = \prod_{j=1}^{d} \Big[0, \frac{c_j}{M}\Big)$$

with integers $0 < c_j \le M$ for $1 \le j \le d$. It is obvious that $E^*_{N,M} \le E_{N,M}$.

Before general upper and lower estimates for the discrete (star) discrepancy can be stated, some further notation is necessary. Let $C_d(M)$ be the set of points $\mathbf{h} = (h_1, \dots, h_d)$ with integer coordinates satisfying $-M/2 < h_j \le M/2$ for $1 \le j \le d$, and let $C^*_d(M) = C_d(M) \backslash \{\mathbf{0}\}$. Further, let

$$r(h, M) = \begin{cases} M \sin(\pi |h| / M) & \text{for } h \in C^*_1(M), \\ 1 & \text{for } h = 0, \end{cases}$$

and

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

for $\mathbf{h} = (h_1, \dots, h_d) \in C_d(M)$. For real t the abbreviation $e(t) = e^{2\pi i t}$ is used, and $\mathbf{x} \cdot \mathbf{y}$ stands for the standard inner product of $\mathbf{x}, \mathbf{y} \in \mathbb{R}^d$.

In the following, three general results for estimating discrete (star) discrepancies are stated. Lemmas 2 and 3 follow from [14, Lemmas 1 and 3], and Lemma 4 is due to Niederreiter [8, Lemma 2.3].

Lemma 2. *Let $M \ge 2$ be an integer and $\mathbf{y}_0, \mathbf{y}_1, \dots, \mathbf{y}_{N-1} \in \mathbb{Z}^d_M$. Then the discrete discrepancy $E_{N,M}$ of the points $\mathbf{x}_n = M^{-1}\mathbf{y}_n \in [0,1)^d$, $0 \le n < N$, satisfies*

$$E_{N,M} \le \sum_{\mathbf{h} \in C^*_d(M)} \frac{1}{r(\mathbf{h}, M)} \left| \frac{1}{N} \sum_{n=0}^{N-1} e(\mathbf{h} \cdot \mathbf{x}_n) \right|.$$

Lemma 3. *Let $M \ge 2$ be an integer and $\mathbf{y}_0, \mathbf{y}_1, \dots, \mathbf{y}_{N-1} \in \mathbb{Z}^d_M$. Then the discrete star discrepancy $E^*_{N,M}$ of the points $\mathbf{x}_n = M^{-1}\mathbf{y}_n \in [0,1)^d$, $0 \le n < N$, satisfies*

$$\left| \sum_{n=0}^{N-1} e(\mathbf{h} \cdot \mathbf{x}_n) \right| \le \frac{2}{\pi} \left(\prod_{j=1}^{d} (2\pi |h_j| + 1) - 1 \right) N E^*_{N,M}$$

for any $\mathbf{h} = (h_1, \dots, h_d) \in \mathbb{Z}^d$ for which not all coordinates are divisible by M.

Lemma 4. *Let $M \ge 2$ be an integer. Then*

$$\sum_{h \in C^*_1(M)} \frac{1}{r(h, M)} < \frac{2}{\pi} \log M + \frac{2}{5}.$$

4. Exponential sums

Lemmas 2 and 3 show that a crucial role for estimating the discrete (star) discrepancy of s-tuples of successive terms in a compound inversive sequence $(\mathbf{u}_n)_{n\geq 0}$ is played by certain exponential sums which are defined below. Subsequently, the ks-dimensional points

$$\mathbf{v}_n = (\mathbf{u}_n, \ldots, \mathbf{u}_{n+s-1}) \in [0,1)^{ks}$$

for $n \geq 0$ and

$$\mathbf{v}_n^{(i)} = (\mathbf{u}_n^{(i)}, \ldots, \mathbf{u}_{n+s-1}^{(i)}) \in [0,1)^{ks}$$

for $n \geq 0$ and $1 \leq i \leq r$ are considered, and the abbreviations

$$S(\mathbf{h}) = \sum_{n=0}^{m^k-1} e(\mathbf{h}\cdot\mathbf{v}_n)$$

and

$$S_i(\mathbf{h}) = \sum_{n=0}^{p_i^k-1} e(\mathbf{h}\cdot\mathbf{v}_n^{(i)})$$

for $1 \leq i \leq r$ and $\mathbf{h} \in \mathbb{Z}^{ks}$ will be used. Some properties of these exponential sums are collected in the following two results. Lemma 6 follows from [14, Proof of Theorem 2].

Lemma 5. *Let* $\mathbf{h} \in \mathbb{Z}^{ks}$. *Then*

$$S(\mathbf{h}) = \prod_{i=1}^{r} S_i(\mathbf{h}).$$

Proof. First, it follows from $\mathbf{v}_n \equiv \sum_{i=1}^{r} \mathbf{v}_n^{(i)} \pmod 1$ for $n \geq 0$ that

$$S(\mathbf{h}) = \sum_{n=0}^{m^k-1} e\left(\sum_{i=1}^{r} \mathbf{h}\cdot\mathbf{v}_n^{(i)}\right) = \sum_{n=0}^{m^k-1} \prod_{i=1}^{r} e(\mathbf{h}\cdot\mathbf{v}_n^{(i)}).$$

Now, the Chinese Remainder Theorem implies that

$$S(\mathbf{h}) = \sum_{\substack{(n_1,\ldots,n_r)\in\mathbb{Z}_{p_1^k}\times\cdots\times\mathbb{Z}_{p_r^k} \\ n\equiv n_i \pmod{p_i^k},\, 1\leq i\leq r}} \prod_{i=1}^{r} e(\mathbf{h}\cdot\mathbf{v}_n^{(i)}).$$

Since the sequence $(\mathbf{v}_n^{(i)})_{n\geq 0}$ has period length $q_i = p_i^k$ for $1 \leq i \leq r$, one finally obtains

$$S(\mathbf{h}) = \sum_{(n_1,\ldots,n_r)\in\mathbb{Z}_{p_1^k}\times\cdots\times\mathbb{Z}_{p_r^k}} \prod_{i=1}^{r} e(\mathbf{h}\cdot\mathbf{v}_{n_i}^{(i)}) = \prod_{i=1}^{r} \sum_{n\in\mathbb{Z}_{p_i^k}} e(\mathbf{h}\cdot\mathbf{v}_n^{(i)}) = \prod_{i=1}^{r} S_i(\mathbf{h}). \quad \square$$

Lemma 6. *Let* $\mathbf{h} \in \mathbb{Z}^{ks}$ *and* $1 \leq i \leq r$. *Then* $|S_i(\mathbf{h})| = p_i^k$ *for* $\mathbf{h} \equiv \mathbf{0} \pmod{p_i}$ *and*

$$|S_i(\mathbf{h})| \leq (s-1)(2p_i^{k/2}+1)$$

for $\mathbf{h} \not\equiv \mathbf{0} \pmod{p_i}$.

5. Upper bounds for the discrete discrepancy

Theorem 2. *The discrete discrepancy* $E^{(ks)}_{m^k,m} = E_{m^k,m}(\mathbf{v}_0,\mathbf{v}_1,\dots,\mathbf{v}_{m^k-1})$ *satisfies*

$$E^{(ks)}_{m^k,m} < m^{-k/2}\left(\frac{2}{\pi}\log m+\frac{7}{5}\right)^{ks}\left(\prod_{i=1}^{r}((s-1)(2+p_i^{-k/2})+p_i^{(k-4)/2})-m^{(k-4)/2}\right)$$

for any sequence of k*-dimensional pseudorandom vectors generated by the compound inversive method and all* $s \geq 2$*.*

Proof. First, Lemma 2 is applied with $M = m$, $N = m^k$, $d = ks$, and $\mathbf{x}_n = \mathbf{v}_n$ for $0 \leq n < m^k$. This yields

$$\begin{aligned}
E^{(ks)}_{m^k,m} &\leq \frac{1}{m^k}\sum_{\mathbf{h}\in C^*_{ks}(m)}\frac{1}{r(\mathbf{h},m)}|S(\mathbf{h})| \\
&= \frac{1}{m^k}\sum_{\mathbf{h}\in C^*_{ks}(m)}\frac{1}{r(\mathbf{h},m)}\prod_{i=1}^{r}|S_i(\mathbf{h})| \\
&= \frac{1}{m^k}\sum_{\substack{I\subset\{1,\dots,r\}\\|I|<r}}\;\sum_{\substack{\mathbf{h}\in C^*_{ks}(m)\\ \mathbf{h}\equiv\mathbf{0}(\bmod p_i),i\in I\\ \mathbf{h}\not\equiv\mathbf{0}(\bmod p_i),i\notin I}}\frac{1}{r(\mathbf{h},m)}\prod_{i=1}^{r}|S_i(\mathbf{h})|,
\end{aligned}$$

where in the second step Lemma 5 has been used. Now, denote by $A(\mathbf{h})$ the number of nonzero coordinates of $\mathbf{h} \in \mathbb{Z}^{ks}$. Observe that always $A(\mathbf{h}) \geq 1$ for $\mathbf{h} \in C^*_{ks}(m)$ and that $S(\mathbf{h}) = 0$ for $A(\mathbf{h}) = 1$. Hence, it follows that

$$E^{(ks)}_{m^k,m} \leq \frac{1}{m^k}\sum_{\substack{I\subset\{1,\dots,r\}\\|I|<r}}\;\sum_{\substack{\mathbf{h}\in C^*_{ks}(m)\\ \mathbf{h}\equiv\mathbf{0}(\bmod p_i),i\in I\\ \mathbf{h}\not\equiv\mathbf{0}(\bmod p_i),i\notin I\\ A(\mathbf{h})\geq 2}}\frac{1}{r(\mathbf{h},m)}\prod_{i=1}^{r}|S_i(\mathbf{h})|.$$

Now, Lemma 6 can be applied in order to obtain

$$\begin{aligned}
E^{(ks)}_{m^k,m} &\leq \frac{1}{m^k}\sum_{\substack{I\subset\{1,\dots,r\}\\|I|<r}} m_I^k \prod_{\substack{i\in\{1,\dots,r\}\\ i\notin I}}(s-1)(2p_i^{k/2}+1)\sum_{\substack{\mathbf{h}\in C^*_{ks}(m)\\ \mathbf{h}\equiv\mathbf{0}(\bmod p_i),i\in I\\ \mathbf{h}\not\equiv\mathbf{0}(\bmod p_i),i\notin I\\ A(\mathbf{h})\geq 2}}\frac{1}{r(\mathbf{h},m)} \\
&\leq \frac{1}{m^k}\sum_{\substack{I\subset\{1,\dots,r\}\\|I|<r}} m_I^k \prod_{\substack{i\in\{1,\dots,r\}\\ i\notin I}}(s-1)(2p_i^{k/2}+1)\sum_{\substack{\mathbf{h}\in C^*_{ks}(m)\\ \mathbf{h}\equiv\mathbf{0}(\bmod m_I)\\ A(\mathbf{h})\geq 2}}\frac{1}{r(\mathbf{h},m)},
\end{aligned}$$

where $m_I = \prod_{i\in I} p_i$ for subsets I of $\{1,\dots,r\}$. Straightforward calculations show that

$$\begin{aligned}
\sum_{\substack{\mathbf{h}\in C_{ks}^*(m)\\ \mathbf{h}\equiv 0\,(\mathrm{mod}\,m_I)\\ A(\mathbf{h})\geq 2}} \frac{1}{r(\mathbf{h},m)} &= \left(\sum_{\substack{h\in C_1^*(m)\\ h\equiv \mathbf{0}\,(\mathrm{mod}\,m_I)}} \frac{1}{r(h,m)} + 1\right)^{ks} - ks \sum_{\substack{h\in C_1^*(m)\\ h\equiv 0\,(\mathrm{mod}\,m_I)}} \frac{1}{r(h,m)} - 1\\
&= \left(\frac{1}{m_I}\sum_{g\in C_1^*(m/m_I)} \frac{1}{r(g,m/m_I)} + 1\right)^{ks} - \frac{ks}{m_I}\sum_{g\in C_1^*(m/m_I)} \frac{1}{r(g,m/m_I)} - 1\\
&= \sum_{n=2}^{ks} \frac{1}{m_I^n}\binom{ks}{n}\left(\sum_{g\in C_1^*(m/m_I)} \frac{1}{r(g,m/m_I)}\right)^n\\
&\leq \frac{1}{m_I^2}\sum_{n=2}^{ks}\binom{ks}{n}\left(\sum_{g\in C_1^*(m/m_I)} \frac{1}{r(g,m/m_I)}\right)^n\\
&< \frac{1}{m_I^2}\left(1+\sum_{g\in C_1^*(m/m_I)} \frac{1}{r(g,m/m_I)}\right)^{ks}.
\end{aligned}$$

Hence, Lemma 4 implies that

$$\sum_{\substack{\mathbf{h}\in C_{ks}^*(m)\\ \mathbf{h}\equiv \mathbf{0}\,(\mathrm{mod}\,m_I)\\ A(\mathbf{h})\geq 2}} \frac{1}{r(\mathbf{h},m)} < \frac{1}{m_I^2}\left(\frac{2}{\pi}\log(m/m_I)+\frac{7}{5}\right)^{ks} \leq \frac{1}{m_I^2}\left(\frac{2}{\pi}\log m+\frac{7}{5}\right)^{ks}.$$

Altogether, one obtains

$$\begin{aligned}
E_{m^k,m}^{(ks)} &< \frac{1}{m^k}\left(\frac{2}{\pi}\log m+\frac{7}{5}\right)^{ks} \sum_{\substack{I\subset\{1,\dots,r\}\\ |I|<r}} m_I^{k-2} \prod_{\substack{i\in\{1,\dots,r\}\\ i\notin I}} (s-1)(2p_i^{k/2}+1)\\
&= \frac{1}{m^k}\left(\frac{2}{\pi}\log m+\frac{7}{5}\right)^{ks}\left(\sum_{I\subset\{1,\dots,r\}} m_I^{k-2} \prod_{\substack{i\in\{1,\dots,r\}\\ i\notin I}} (s-1)(2p_i^{k/2}+1) - m^{k-2}\right)\\
&= \frac{1}{m^k}\left(\frac{2}{\pi}\log m+\frac{7}{5}\right)^{ks}\left(\prod_{i=1}^{r}((s-1)(2p_i^{k/2}+1)+p_i^{k-2}) - m^{k-2}\right)\\
&= m^{-k/2}\left(\frac{2}{\pi}\log m+\frac{7}{5}\right)^{ks}\left(\prod_{i=1}^{r}((s-1)(2+p_i^{-k/2})+p_i^{(k-4)/2}) - m^{(k-4)/2}\right),
\end{aligned}$$

which is the desired result. □

For a fixed number r of prime factors of m, Theorem 2 shows that $E_{m^k,m}^{(ks)} = O(m^{-k/2}(\log m)^{ks})$ for $k \leq 4$ or $r = 1$. For $k \geq 5$ and $r \geq 2$ the order of magnitude increases, since $\prod_{i=1}^{r}((s-1)(2+p_i^{-k/2})+p_i^{(k-4)/2}) - m^{(k-4)/2}$ has an order of magnitude $m_1^{(k-4)/2}$ in this case, where $m_1 = m/p_1$ and $p_1 = \min_{1\le i\le r} p_i$ is assumed. Then it follows that $E^{(ks)}_{m^k,m} = O(m_1^{(k-4)/2} m^{-k/2}(\log m)^{ks})$. Lower bounds for $E^{(ks)}_{m^k,m}$, which will be established in the next section, show that the result of Theorem 2 is best possible up to the logarithmic factor. Further, it should be observed that this bound is independent of the specific choice of the parameters α_i and β_i in the underlying recursions provided the parameters are chosen in such a way that the quotient $\sigma_i\tau_i^{-1}$ has order $q_i + 1$ in the multiplicative group $F^*_{q_i^2}$. It should also be observed that the bound is independent of the ordered basis B_i of F_{q_i} over F_{p_i}, which is used for the representation of the sequence $(\mathbf{c}_n^{(i)})_{n\ge 0}$.

6. Lower bounds for the discrete discrepancy

Theorem 1 shows that a sequence of pseudorandom vectors generated by the compound inversive method has the maximum possible period length m^k if and only if all underlying (ordinary) inversive sequences of pseudorandom vectors have maximum possible period length q_i, which depends on the quotient of the roots σ_i, $\tau_i \in F_{q_i^2}$ of the polynomial

$$G_i(x) = x^2 - \beta_i x - \alpha_i = (x - \sigma_i)(x - \tau_i)$$

according to Lemma 1. Since $\sigma_i + \tau_i = \beta_i$ and $\sigma_i\tau_i = -\alpha_i$, an easy calculation shows that

$$\left(x - \frac{\sigma_i}{\tau_i}\right)\left(x - \frac{\tau_i}{\sigma_i}\right) = x^2 + \left(\frac{\beta_i^2}{\alpha_i} + 2\right)x + 1.$$

Therefore, the desired property that $\sigma_i\tau_i^{-1}$ has order $q_i + 1$ in $F^*_{q_i^2}$ just depends on the value of $\beta_i^2\alpha_i^{-1} \in F_{q_i}$. Now, put $\beta_i^{-2}\alpha_i = \zeta_i$ and let P_{q_i} be the set of ζ_i's for which the desired property is satisfied, i.e., for which $x^2 + (\zeta_i^{-1} + 2)x + 1$ has roots of order $q_i + 1$ in $F^*_{q_i^2}$. Further, for a fixed nontrivial additive character η_i of F_{q_i} and any β_i, $\zeta_i \in F^*_{q_i}$ put

$$K_i(\beta_i, \zeta_i) = \sum_{\gamma\in F_{q_i}} \eta_i(\beta_i\gamma + \beta_i\zeta_i\overline{\gamma}).$$

The following result, which is due to Niederreiter [14, Lemma 6], will be used in the proof of a lower bound for the discrete star discrepancy in Theorem 3 below. To avoid trivial cases, it will be assumed that $q_i = p_i^k \ge 4$ for $1 \le i \le r$.

Lemma 7. *Let $1 \le i \le r$ and η_i be a nontrivial additive character of F_{q_i}. Then for any $\zeta_i \in F^*_{q_i}$ and $0 < t \le \sqrt{\frac{q_i-3}{q_i-1}}$, there exist more than $H_{q_i}(t)(q_i - 1)$ values of $\beta_i \in F^*_{q_i}$ such that*

$$|K_i(\beta_i, \zeta_i)| \ge t q_i^{1/2},$$

where

$$H_{q_i}(t) = \frac{1 - t^2 - 2(q_i - 1)^{-1}}{4 - t^2 + 4q_i^{-1/2} + q_i^{-1}}.$$

Theorem 3. (i) *Let $k \le 4$. For $1 \le i \le r$ let $\zeta_i \in P_{q_i}$ and $0 < t_i \le \sqrt{\frac{q_i-3}{q_i-1}}$, and let $H_{q_i}(t_i)$ be defined as in Lemma 7. Then for fixed underlying ordered bases of F_{q_i} over F_{p_i} there exist more than $\prod_{i=1}^r H_{q_i}(t_i)(q_i - 1)$ values of $(\beta_1, \dots, \beta_r) \in F^*_{q_1} \times \cdots \times F^*_{q_r}$ such that the discrete star discrepancy $E^{*(ks)}_{m^k,m} = E^*_{m^k,m}(\mathbf{v}_0, \mathbf{v}_1, \dots, \mathbf{v}_{m^k-1})$*

for any compound inversive sequence of k-dimensional pseudorandom vectors with $\alpha_i = \beta_i^2\zeta_i$ satisfies

$$E^{*(ks)}_{m^k,m} \geq \frac{1}{8(\pi+1)}\left(\prod_{i=1}^{r} t_i\right) m^{-k/2}$$

for all $s \geq 2$.

(ii) *Let $k \geq 5$ and suppose that $p_1 = \min_{1\leq i\leq r} p_i$. Let $\zeta_1 \in P_{q_1}$ and $0 < t \leq \sqrt{\frac{q_1-3}{q_1-1}}$, and let $H_{q_1}(t)$ be defined as in Lemma 7. Then for a fixed underlying ordered basis of F_{q_1} over F_{p_1} there exist more than $H_{q_1}(t)(q_1-1)$ values of $\beta_1 \in F^*_{q_1}$ such that the discrete star discrepancy $E^{*(ks)}_{m^k,m} = E^*_{m^k,m}(\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_{m^k-1})$ for any compound inversive sequence of k-dimensional pseudorandom vectors with $\alpha_1 = \beta_1^2\zeta_1$ satisfies*

$$E^{*(ks)}_{m^k,m} \geq \frac{t}{8(\pi+1)} m_1^{(k-4)/2} m^{-k/2}$$

for all $s \geq 2$.

Proof. First, Lemma 3 is applied with $M = m$, $N = m^k$, $d = ks$, $\mathbf{x}_n = \mathbf{v}_n$ for $0 \leq n < m^k$, and

$$\mathbf{h} = (\mathbf{h}_0, \ldots, \mathbf{h}_{s-1}) \in \mathbb{Z}^{ks},$$

where $\mathbf{h}_l = (h_{l,1}, \ldots, h_{l,k}) \in \mathbb{Z}^k$ for $0 \leq l \leq s-1$ with $h_{0,1} = h_{1,1} = m_I = \prod_{i\in I} p_i$ for an arbitrary subset I of $\{1, \ldots, r\}$ with $|I| < r$ and all other $h_{l,j} = 0$. This yields

$$|S(\mathbf{h})| \leq \frac{2}{\pi}\left(\prod_{l=0}^{s-1}\prod_{j=1}^{k}(2\pi|h_{l,j}|+1) - 1\right) m^k E^{*(ks)}_{m^k,m} = 8(\pi + m_I^{-1}) m_I^2 m^k E^{*(ks)}_{m^k,m}.$$

Thus, it follows from Lemma 5 that

$$E^{*(ks)}_{m^k,m} \geq \frac{1}{8(\pi + m_I^{-1}) m_I^2 m^k}\prod_{i=1}^{r}|S_i(\mathbf{h})| \geq \frac{1}{8(\pi+1) m_I^2 m^k}\prod_{i=1}^{r}|S_i(\mathbf{h})|.$$

Since p_i divides $h_{0,1} = h_{1,1} = m_I$ for $i \in I$ and all other $h_{l,j} = 0$, it follows that $|S_i(\mathbf{h})| = q_i$ for $i \in I$ according to Lemma 6. This yields

$$E^{*(ks)}_{m^k,m} \geq \frac{1}{8(\pi+1)m^k} m_I^{k-2} \prod_{\substack{i\in\{1,\ldots,r\}\\ i\notin I}} |S_i(\mathbf{h})|.$$

Now, let $i \in \{1, \ldots, r\}$ with $i \notin I$ be fixed. Let $\zeta_i \in P_{q_i}$ and let $\alpha_i = \beta_i^2\zeta_i$. Subsequently, a lower bound for $|S_i(\mathbf{h})|$ with $h_{0,1} = h_{1,1} = m_I$ and all other $h_{l,j} = 0$ will be established. Let $(\delta_1^{(i)}, \ldots, \delta_k^{(i)})$ be the dual basis B_i' of the fixed underlying ordered basis B_i of F_{q_i} over F_{p_i}. Further, let α_i, $\beta_i \in F^*_{q_i}$ be the parameters of the ith recursion. Define a nontrivial additive character χ_i of F_{q_i} by $\chi_i(\gamma) = e(\frac{1}{p_i}\mathrm{Tr}(\gamma))$ for $\gamma \in F_{q_i}$, where Tr denotes the trace function from F_{q_i} in F_{p_i}. Then

$$S_i(\mathbf{h}) = \sum_{n=0}^{q_i-1}\chi_i\left(\sum_{l=0}^{s-1}\mu_l^{(i)}\gamma_{n+l}^{(i)}\right),$$

where $\mu_l^{(i)} = \sum_{j=1}^{k} h_{l,j}\delta_j^{(i)} \in F_{q_i}$ for $0 \leq l \leq s-1$ (cf. [14, Proof of Theorem 2]). Since $h_{0,1} = h_{1,1} = m_I$ and all other $h_{l,j} = 0$, it follows that $\mu_0^{(i)} = \mu_1^{(i)} = m_I\delta_1^{(i)}$ and $\mu_l^{(i)} = 0$ for $2 \leq l \leq s-1$. Hence, one obtains

$$\begin{aligned} S_i(\mathbf{h}) &= \sum_{n=0}^{q_i-1} \chi_i(m_I\delta_1^{(i)}\gamma_n^{(i)} + m_I\delta_1^{(i)}\gamma_{n+1}^{(i)}) \\ &= \sum_{n=0}^{q_i-1} \chi_i(m_I\delta_1^{(i)}\gamma_n^{(i)} + m_I\delta_1^{(i)}(\alpha_i\overline{\gamma}_n^{(i)} + \beta_i)) \\ &= \sum_{\gamma\in F_{q_i}} \chi_i(m_I\delta_1^{(i)}\gamma + m_I\delta_1^{(i)}(\alpha_i\overline{\gamma} + \beta_i)). \end{aligned}$$

With $\eta_i(\gamma) = \chi_i(m_I\delta_1^{(i)}\gamma)$ for $\gamma \in F_{q_i}$ it follows that

$$|S_i(\mathbf{h})| = \left|\sum_{\gamma\in F_{q_i}} \eta_i(\gamma + \alpha_i\overline{\gamma} + \beta_i)\right| = \left|\sum_{\gamma\in F_{q_i}} \eta_i(\gamma + \alpha_i\overline{\gamma})\right|.$$

Since $\alpha_i = \beta_i^2\zeta_i$, one obtains

$$|S_i(\mathbf{h})| = \left|\sum_{\gamma\in F_{q_i}} \eta_i(\gamma + \beta_i^2\zeta_i\overline{\gamma})\right|.$$

Now, by changing $\beta_i^{-1}\gamma$ into γ' in the summation, one sees that

$$|S_i(\mathbf{h})| = \left|\sum_{\gamma'\in F_{q_i}} \eta_i(\beta_i\gamma' + \beta_i\zeta_i\overline{\gamma}')\right| = |K_i(\beta_i,\zeta_i)|.$$

Now, let $0 < t_i \leq \sqrt{\frac{q_i-3}{q_i-1}}$, and let $H_{q_i}(t_i)$ be defined as in Lemma 7. Then there exist more than $H_{q_i}(t_i)(q_i-1)$ values of $\beta_i \in F_{q_i}^*$ with

$$|S_i(\mathbf{h})| = |K_i(\beta_i,\zeta_i)| \geq t_i q_i^{1/2}$$

according to Lemma 7. Therefore, one obtains more than $\prod_{i\in\{1,\ldots,r\}\setminus I} H_{q_i}(t_i)(q_i-1)$ values of $(\beta_i)_{i\in\{1,\ldots,r\}\setminus I} \in \prod_{i\in\{1,\ldots,r\}\setminus I} F_{q_i}^*$ with

$$\begin{aligned} E_{m^k,m}^{*(ks)} &\geq \frac{1}{8(\pi+1)m^k} m_I^{k-2} \prod_{\substack{i\in\{1,\ldots,r\}\\ i\notin I}} t_i q_i^{1/2} \\ &= \frac{1}{8(\pi+1)} m_I^{(k-4)/2} \left(\prod_{\substack{i\in\{1,\ldots,r\}\\ i\notin I}} t_i\right) m^{-k/2}. \end{aligned}$$

(i) For $k \leq 4$ the choice $I = \varnothing$, i.e., $m_I = 1$, implies that there exist more than $\prod_{i=1}^{r} H_{q_i}(t_i)(q_i-1)$ values of $(\beta_1,\ldots,\beta_r) \in F_{q_1}^* \times \cdots \times F_{q_r}^*$ with

$$E_{m^k,m}^{*(ks)} \geq \frac{1}{8(\pi+1)} \left(\prod_{i=1}^{r} t_i\right) m^{-k/2}.$$

(ii) For $k \geq 5$ the choice $I = \{2, \ldots, r\}$, i.e., $m_I = m_1$, implies that there exist more than $H_{q_1}(t)(q_1 - 1)$ values of $\beta_1 \in F_{q_1}^*$ with

$$E_{m^k,m}^{*(ks)} \geq \frac{t}{8(\pi+1)} m_1^{(k-4)/2} m^{-k/2}. \qquad \square$$

Corollary 1. (i) *Let $k \leq 4$. Then for fixed underlying ordered bases of F_{q_i} over F_{p_i} for $1 \leq i \leq r$ and any $(\zeta_1, \ldots, \zeta_r) \in P_{q_1} \times \cdots \times P_{q_r}$ there exists a value of $(\beta_1, \ldots, \beta_r) \in F_{q_1}^* \times \cdots \times F_{q_r}^*$ such that the discrete star discrepancy $E_{m^k,m}^{*(ks)} = E_{m^k,m}^*(\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_{m^k-1})$ for the sequence of k-dimensional pseudorandom vectors generated by the compound inversive method with $\alpha_i = \beta_i^2 \zeta_i$ satisfies*

$$E_{m^k,m}^{*(ks)} \geq \frac{1}{8(\pi+1)} \left(\prod_{i=1}^{r} \sqrt{\frac{q_i - 3}{q_i - 1}} \right) m^{-k/2}$$

for all $s \geq 2$.

(ii) *Let $k \geq 5$ and suppose that $p_1 = \min_{1 \leq i \leq r} p_i$. Then for a fixed underlying ordered basis of F_{q_1} over F_{p_1} and any $\zeta_1 \in P_{q_1}$ there exists a value $\beta_1 \in F_{q_1}^*$ such that the discrete star discrepancy $E_{m^k,m}^{*(ks)} = E_{m^k,m}^*(\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_{m^k-1})$ for the sequence of k-dimensional pseudorandom vectors generated by the compound inversive method with $\alpha_1 = \beta_1^2 \zeta_1$ satisfies*

$$E_{m^k,m}^{*(ks)} \geq \frac{1}{8(\pi+1)} \sqrt{\frac{q_1 - 3}{q_1 - 1}} m_1^{(k-4)/2} m^{-k/2}$$

for all $s \geq 2$.

For a fixed number r of prime factors of m, Theorem 3 and Corollary 1 imply that for any underlying ordered basis of F_{q_i} over F_{p_i} and any $\zeta_i \in P_{q_i}$ there exist compound inversive generators with discrete star discrepancy $E_{m^k,m}^{*(ks)}$ of the order of magnitude at least $m^{-k/2}$ for $k \leq 4$ and of the order of magnitude at least $m_1^{(k-4)/2} m^{-k/2}$ for $k \geq 5$, where $m_1 = m/p_1$ and $p_1 = \min_{1 \leq i \leq r} p_i$. This shows that the order of magnitude of the upper bounds for the discrete discrepancy $E_{m^k,m}^{(ks)}$ in Theorem 2 is best possible up to the logarithmic factor. The law of the iterated logarithm for discrepancies [6] implies that the discrepancy of M independent and uniformly distributed points from $[0, 1)^d$ is almost always of an order of magnitude $M^{-1/2}(\log \log M)^{1/2}$. A law of the iterated logarithm for discrete discrepancies is not yet known, but it is tempting to conjecture that such a result holds for the discrete discrepancy, too. In that case the lower and upper bounds for the discrete discrepancy in the compound inversive method for pseudorandom vector generation with $k \leq 4$ are in good accordance with such a result. On the other hand, for $k \geq 5$ (and $r \geq 2$) the lower bound for the discrete discrepancy is already too large compared with such a result.

Note, that in the cases $k = 1$ and $k = 2$ similar results for the (star) discrepancy instead of the discrete (star) discrepancy can be established, since the order of the discretization error is small enough.

Acknowledgment

The author would like to thank a referee for valuable comments.

References

1. J. Eichenauer and J. Lehn, *A non-linear congruential pseudorandom number generator*, Statist. Hefte **27** (1986), 315–326. MR **88i:**65014
2. J. Eichenauer-Herrmann, *Inversive congruential pseudorandom numbers: a tutorial*, Internat. Statist. Rev. **60** (1992), 167–176.
3. ______, *On generalized inversive congruential pseudorandom numbers*, Math. Comp. **63** (1994), 293–299. MR **94k:**11088
4. ______, *Pseudorandom number generation by nonlinear methods*, Internat. Statist. Rev. **63** (1995), 247–255.
5. 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
6. 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
7. R. Lidl and H. Niederreiter, *Finite fields*, Addison-Wesley, Reading, MA, 1983. MR **86c:**11106
8. H. Niederreiter, *Pseudo-random numbers and optimal coefficients*, Adv. in Math. **26** (1977), 99–181. MR **57:**16238
9. ______, *Finite fields and their applications*, Contributions to General Algebra 7 (D. Dorninger, G. Eigenthaler, H. K. Kaiser, and W. B. Müller, eds.), Teubner, Stuttgart, 1991, pp. 251–264. MR **92j:**11146
10. ______, *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.
11. ______, *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
12. ______, *Random number generation and quasi-Monte Carlo methods*, SIAM, Philadelphia, PA, 1992. MR **93h:**65008
13. ______, *Pseudorandom numbers and quasirandom points*, Z. Angew. Math. Mech. **73** (1993), T648-T652. CMP 94:01
14. ______, *Pseudorandom vector generation by the inversive method*, ACM Trans. Modeling and Computer Simulation **4** (1994), 191–212.

Fachbereich Mathematik, AG9, Technische Hochschule Darmstadt, Schlossgartenstrasse 7, D-64289 Darmstadt, Germany