MATHEMATICS OF COMPUTATION
Volume 71, Number 238, Pages 781–791
S 0025-5718(01)01328-X
Article electronically published on October 25, 2001

AVERAGE EQUIDISTRIBUTION AND STATISTICAL INDEPENDENCE PROPERTIES OF DIGITAL INVERSIVE PSEUDORANDOM NUMBERS OVER PARTS OF THE PERIOD

FRANK EMMERICH

ABSTRACT. This article deals with the digital inversive method for generating uniform pseudorandom numbers. Equidistribution and statistical independence properties of the generated pseudorandom number sequences over parts of the period are studied based on the distribution of tuples of successive terms in the sequence. The main result is an upper bound for the average value of the star discrepancy of the corresponding point sets. Additionally, lower bounds for the star discrepancy are established. The method of proof relies on bounds for exponential sums.

1. INTRODUCTION

Uniform pseudorandom numbers in the interval $[0, 1)$ are basic ingredients of any stochastic simulation. Their quality is of fundamental importance for the success of the simulation, since the outcome of a typical stochastic simulation strongly depends on the structural and statistical properties of the underlying pseudorandom number generator. Reviews of several methods are given in Harald Niederreiter's excellent monograph [10] and in his comprehensive survey [12]. The classical and most frequently used method for the generation of pseudorandom numbers is still the linear congruential method. However, its simple linear nature implies several undesirable regularities [10]. Mainly for this reason, a variety of nonlinear methods for the generation of pseudorandom numbers has been introduced and studied as alternatives to the linear congruential method. Surveys of this important research area are given in [1, 2, 3, 12]. A particularly interesting nonlinear approach for generating uniform pseudorandom numbers is the *digital inversive method*, which was introduced and studied in [4]. These generators have several attractive properties such as a handy criterion for the maximum possible period length and desirable statistical independence properties over the full period. A review of previously shown results on the digital inversive method can be found in [5]. The present paper deals with the (average) equidistribution and statistical independence properties of digital inversive pseudorandom numbers over parts of the period.

Received by the editor November 10, 1999 and, in revised form, July 12, 2000.
2000 *Mathematics Subject Classification.* Primary 65C10; Secondary 11K45.
Key words and phrases. Uniform pseudorandom numbers, digital inversive method, average equidistribution behaviour, average statistical independence properties, star discrepancy, exponential sums.

In order to describe the digital inversive method, let p be a prime, and put $q = p^k$ for some integer $k \geq 1$. Denote by F_q and F_q^* the finite field with q elements and its multiplicative group, respectively. For $\gamma \in F_q^*$, define $\overline{\gamma} \in F_q^*$ by $\overline{\gamma} = \gamma^{-1}$, i.e., $\overline{\gamma}$ is the multiplicative inverse of γ in F_q^*, and put $\overline{0} = 0$. Now, two parameters $\alpha \in F_q^*$ and $\beta \in F_q$ are selected and a sequence $(\gamma_n)_{n\geq 0}$ of elements of F_q is generated by choosing an initial value $\gamma_0 \in F_q$ and using the inversive 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 the finite field F_p [9, Chapter 1.4]. Let B be an ordered basis of F_q over F_p and denote by $\mathbf{c}_n \in F_p^k$ the coordinate vector of $\gamma_n \in F_q$ relative to B for $n \geq 0$. Let $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$ for any integer $m \geq 1$. Since $F_p = \mathbb{Z}/p\mathbb{Z}$ can be identified with the set $\mathbb{Z}_p$, each vector $\mathbf{c}_n = (c_{n,1}, \ldots, c_{n,k})$ can also be viewed as an element of $\mathbb{Z}_p^k$. Then a *digital inversive sequence* $(x_n)_{n\geq 0}$ of uniform pseudorandom numbers can be defined by

$$x_n = \sum_{j=1}^{k} c_{n,j} p^{-j} \in [0, 1)$$

for $n \geq 0$. It is obvious that the sequences $(x_n)_{n\geq 0}$, $(\mathbf{c}_n)_{n\geq 0}$, and $(\gamma_n)_{n\geq 0}$ are always purely periodic and have the same period length. It was shown by Niederreiter [11, Theorem 1] that the sequence $(\gamma_n)_{n\geq 0}$ has the maximum possible period length $q = p^k$ if and only if the order of $\sigma\tau^{-1}$ in the multiplicative group $F_{q^2}^*$ is equal to $q + 1$, where $\sigma, \tau \in F_{q^2}^*$ are the two roots of the polynomial $x^2 - \beta x - \alpha \in F_q[x]$. Note that any quadratic primitive polynomial over F_q has this property. It is always assumed from now on that the sequence $(\gamma_n)_{n\geq 0}$ has the maximum possible period length $q = p^k$.

Finally, consider the sequence $(\gamma_{\kappa,n})_{n\geq 0}$ of elements of F_q defined by $\gamma_{\kappa,0} = \kappa\gamma_0$ and

$$\gamma_{\kappa,n+1} = \kappa^2\alpha\overline{\gamma}_{\kappa,n} + \kappa\beta$$

for $n \geq 0$ and an arbitrary (fixed) element $\kappa \in F_q^*$. A short calculation shows that $\gamma_{\kappa,n} = \kappa\gamma_n$ for all $n \geq 0$. Let $\mathbf{c}_{\kappa,n} = (c_{\kappa,n,1}, \ldots, c_{\kappa,n,k}) \in \mathbb{Z}_p^k$ be the coordinate vector of $\gamma_{\kappa,n} \in F_q$ relative to the ordered basis B of F_q over F_p. Then a digital inversive sequence $(x_{\kappa,n})_{n\geq 0}$ of uniform pseudorandom numbers is obtained again by

$$x_{\kappa,n} = \sum_{j=1}^{k} c_{\kappa,n,j} p^{-j} \in [0, 1)$$

for $n \geq 0$.

Equidistribution and statistical independence properties of a sequence of pseudorandom numbers over parts of the period can be studied based on the (star) discrepancy of the first N generated (nonoverlapping) s-tuples of successive terms in the sequence. For a long time, the (star) discrepancy of the first N generated s-tuples of an *individual* sequence of recursively defined pseudorandom numbers could not be analysed successfully and, therefore, the *average* behaviour over certain parameters was often studied. This state of affairs also motivated the present article, which deals with the behaviour of digital inversive pseudorandom number sequences $(x_{\kappa,n})_{n\geq 0}$ on the average over the parameter $\kappa \in F_q^*$. Very recently, it

was even possible to analyse the star discrepancy of the first N generated s-tuples of an individual sequence of digital inversive pseudorandom numbers (cf. [14]). Although in [14] overlapping instead of nonoverlapping s-tuples are considered, these complementary results open up the opportunity to compare the individual and the average behaviour of digital inversive pseudorandom numbers, but this comparison is postponed until the discussion in the final section.

First, in order to define the star discrepancy, let $\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1} \in [0,1)^d$ be N arbitrary points. For any subinterval J of $[0,1)^d$, denote by $L(J)$ the number of points among $\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1}$ falling into J, and let $\mathrm{Vol}(J)$ be the d-dimensional volume of J. Then the *star discrepancy* of the points $\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1}$ is defined by

$$D_N^*(\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1}) = \sup_{J \in \mathcal{J}^*} \left| \frac{L(J)}{N} - \mathrm{Vol}(J) \right|,$$

where $\mathcal{J}^*$ stands for the family of all subintervals J of $[0,1)^d$ containing the origin.

In order to analyse the equidistribution and statistical independence properties of digital inversive sequences over parts of the period, the s-dimensional points

$$\mathbf{x}_{\kappa,n} = (x_{\kappa,sn}, x_{\kappa,sn+1}, \ldots, x_{\kappa,sn+s-1}) \in [0,1)^s$$

for $n \geq 0$ are considered, and the abbreviation

$$D_{\kappa;N}^{*(s)} = D_N^*(\mathbf{x}_{\kappa,0}, \mathbf{x}_{\kappa,1}, \ldots, \mathbf{x}_{\kappa,N-1})$$

for $1 \leq N \leq q/\gcd(s,q)$ is used. In the third section, the main results on the star discrepancy $D_{\kappa;N}^{*(s)}$ are established. A detailed discussion of these results is given in the fourth section. The second section contains some useful auxiliary results.

2. Auxiliary results

First, some further notation is necessary. For integers $r \geq 1$ and $b \geq 2$, let $C_r(b)$ be the set of all lattice points $\mathbf{z} = (z_1, \ldots, z_r)$ with integer coordinates satisfying $-b/2 < z_i \leq b/2$ for $1 \leq i \leq r$, and let $C_r^*(b) = C_r(b) \setminus \{\mathbf{0}\}$. For real x, the abbreviation $e(x) = e^{2\pi\sqrt{-1}x}$ is used.

In order to state an estimate for the star discrepancy of a point set for which all coordinates of all points have a finite digit expansion in a fixed base b, consider points

$$\mathbf{w}_n = (w_{n,0}, w_{n,1}, \ldots, w_{n,d-1}) \in [0,1)^d$$

with

$$w_{n,l} = \sum_{j=1}^{t} w_{n,l,j} b^{-j} \in [0,1)$$

and $w_{n,l,j} \in \mathbb{Z}_b$ for $1 \leq j \leq t$, $0 \leq l \leq d-1$, $0 \leq n < N$, and an integer $t \geq 1$. Further, for $\mathbf{h} = (h_1, \ldots, h_t) \in C_t(b)$, define

$$\ell(h_1, \ldots, h_t) = \begin{cases} \max\{1 \leq \ell \leq t : h_\ell \neq 0\} & \text{for } (h_1, \ldots, h_t) \neq \mathbf{0}, \\ 0 & \text{for } (h_1, \ldots, h_t) = \mathbf{0}, \end{cases}$$

and put

$$Q_b(h_1, \ldots, h_t) = \begin{cases} 1/(b^\ell \sin(\pi |h_\ell|/b)) & \text{for } (h_1, \ldots, h_t) \neq \mathbf{0}, \\ 1 & \text{for } (h_1, \ldots, h_t) = \mathbf{0}, \end{cases}$$

where $\ell = \ell(h_1, \ldots, h_t)$. It should be observed that, for base $b = 2$,

$$Q_2(\mathbf{h}) = 2^{-\ell(\mathbf{h})}$$

for any $\mathbf{h} \in C_t(2) = \{0,1\}^t$, i.e., this definition of $Q_2(\mathbf{h})$ is identical with the one given in [10, equation (3.16)]. Finally, for $\mathbf{h} = (\mathbf{h}_0, \ldots, \mathbf{h}_{d-1}) \in C_{td}(b)$ with each $\mathbf{h}_l \in C_t(b)$ for $0 \le l \le d-1$, let

$$W_b(\mathbf{h}) = \prod_{l=0}^{d-1} Q_b(\mathbf{h}_l).$$

Lemma 1 follows at once from [7, Theorem 1(ii) and Lemma 3(iii)] and slightly improves [10, Theorem 3.12].

Lemma 1. *Let $\mathbf{w}_0, \mathbf{w}_1, \ldots, \mathbf{w}_{N-1} \in [0,1)^d$ be N points with a finite digit expansion of the form as described above. Then their star discrepancy $D_N^* = D_N^*(\mathbf{w}_0, \mathbf{w}_1, \ldots, \mathbf{w}_{N-1})$ satisfies*

$$D_N^* \le \frac{1}{N} \sum_{\mathbf{h} \in C_{td}^*(b)} W_b(\mathbf{h}) \left| \sum_{n=0}^{N-1} e\left(\frac{1}{b} \sum_{l=0}^{d-1} \sum_{j=1}^{t} h_{l,j} w_{n,l,j} \right) \right| + \frac{d}{b^t},$$

where the outer summation is extended over all $\mathbf{h} = (\mathbf{h}_0, \ldots, \mathbf{h}_{d-1}) \in C_{td}^*(b)$ with components $\mathbf{h}_l = (h_{l,1}, \ldots, h_{l,t}) \in C_t(b)$ for $0 \le l \le d-1$.

Now, for an integer $b \ge 2$, let $\mathcal{J}_b^*$ be the family of all subintervals J of $[0,1)^d$ of the form

$$J = \prod_{l=0}^{d-1} \left[0, \frac{c_l}{b}\right)$$

with integers $0 < c_l \le b$ for $0 \le l \le d-1$. Subsequently, $\mathbf{x} \cdot \mathbf{y}$ stands for the standard inner product of $\mathbf{x}, \mathbf{y} \in \mathbb{R}^d$. Lemma 2 can be deduced from Lemma 3 in Niederreiter [11].

Lemma 2. *Let $b \ge 2$ be an integer. Let $\mathbf{t}_n = \mathbf{y}_n / b \in [0,1)^d$ be points with $\mathbf{y}_n \in \mathbb{Z}_b^d$ for $0 \le n < N$. Then the corresponding exponential sum satisfies*

$$\left| \sum_{n=0}^{N-1} e(\mathbf{h} \cdot \mathbf{t}_n) \right| \le \frac{2}{\pi} \left(\prod_{l=0}^{d-1} (2\pi |h_l| + 1) - 1 \right) N \max_{J \in \mathcal{J}_b^*} \left| \frac{L(J)}{N} - \mathrm{Vol}(J) \right|$$

for any lattice point $\mathbf{h} = (h_0, \ldots, h_{d-1}) \in \mathbb{Z}^d$ for which not all coordinates are divisible by b.

A crucial role for estimates of the star discrepancy $D_{\kappa;N}^{*(s)}$ in the digital inversive method is played by certain exponential sums. In the following technical lemma, an upper bound for their average absolute value (in the mean-squared sense) over all $\kappa \in F_q^*$ is established.

Lemma 3. *Let $1 \le N \le q/\gcd(s,q)$. Further, let $\mathbf{h} = (\mathbf{h}_0, \ldots, \mathbf{h}_{s-1}) \in C_{ks}^*(p)$ with components $\mathbf{h}_l = (h_{l,1}, \ldots, h_{l,k}) \in C_k(p)$ for $0 \le l \le s-1$. Then*

$$\sum_{\kappa \in F_q^*} \left| \sum_{n=0}^{N-1} e\left(\frac{1}{p} \sum_{l=0}^{s-1} \sum_{j=1}^{k} h_{l,j} c_{\kappa, sn+l, j} \right) \right|^2 \le N(sq - N) + (s-1)(2s-1)q.$$

Proof. (i) First, let $N \le 2s-1$. Then the elementary estimates

$$\begin{aligned}\sum_{\kappa\in F_q^*}\left|\sum_{n=0}^{N-1} e\left(\frac{1}{p}\sum_{l=0}^{s-1}\sum_{j=1}^{k} h_{l,j}c_{\kappa,sn+l,j}\right)\right|^2 &\le N^2(q-1) \le (2s-1)Nq - N^2\\ &= N(sq-N) + (s-1)Nq \le N(sq-N) + (s-1)(2s-1)q\end{aligned}$$

yield already the desired upper bound.

(ii) Subsequently, $N > 2s-1$ is always assumed. Let $\{\delta_1,\ldots,\delta_k\}$ be the dual basis of the ordered basis B of F_q over F_p [9, Definition 2.30], and put $\eta_{l+1} = \sum_{j=1}^{k} h_{l,j}\delta_j \in F_q$ for $0 \le l \le s-1$. Note that $\mathbf{h} \ne \mathbf{0}$ implies that there exists at least one index $0 \le \ell \le s-1$ with $\eta_{\ell+1} \ne 0$. Now, it follows directly from the first half of the proof of Lemma 5 in [6] that

$$\begin{aligned}&\sum_{\kappa\in F_q^*}\left|\sum_{n=0}^{N-1} e\left(\frac{1}{p}\sum_{l=0}^{s-1}\sum_{j=1}^{k} h_{l,j}c_{\kappa,sn+l,j}\right)\right|^2\\ &\quad= q\#\left\{(n,t)\in\mathbb{Z}_N^2 : \sum_{l=0}^{s-1}\eta_{l+1}(\gamma_{sn+l}-\gamma_{st+l}) = 0\right\} - N^2\\ &\quad= q\#\left\{(n,t)\in\mathbb{Z}_N^2 : \sum_{l=0}^{s-1}\eta_{l+1}\gamma_{sn+l} = \sum_{l=0}^{s-1}\eta_{l+1}\gamma_{st+l}\right\} - N^2\\ &\quad= q\sum_{\eta_0\in F_q}(A_N(\eta_0))^2 - N^2,\end{aligned}$$

where

$$A_N(\eta_0) = \#\left\{n\in\mathbb{Z}_N : \sum_{l=0}^{s-1}\eta_{l+1}\gamma_{sn+l} = \eta_0\right\}$$

for $\eta_0 \in F_q$. For $s=1$, it is obvious that $A_N(\eta_0) = 1$ for exactly N values of $\eta_0 \in F_q$ and $A_N(\eta_0) = 0$ for all other values of $\eta_0 \in F_q$, which immediately yields the desired upper bound $N(q-N)$. Therefore, $s \ge 2$ will be assumed from now on.

(iii) For any $\eta_0 \in F_q$, let

$$A_N^0(\eta_0) = \#\left\{n\in\mathbb{Z}_N : \gamma_{sn}\cdots\gamma_{sn+s-2} = 0, \sum_{l=0}^{s-1}\eta_{l+1}\gamma_{sn+l} = \eta_0\right\}$$

and

$$A_N^*(\eta_0) = \#\left\{n\in\mathbb{Z}_N : \gamma_{sn}\cdots\gamma_{sn+s-2} \ne 0, \sum_{l=0}^{s-1}\eta_{l+1}\gamma_{sn+l} = \eta_0\right\}.$$

Now, the condition $N \le q/\gcd(s,q)$ and some short calculations show that

$$\begin{aligned}\sum_{\eta_0\in F_q} A_N^0(\eta_0) &= \#\{n\in\mathbb{Z}_N : \gamma_{sn}\cdots\gamma_{sn+s-2} = 0\}\\ &\le \#\{n\in\mathbb{Z}_{q/\gcd(s,q)} : \gamma_{sn}\cdots\gamma_{sn+s+2} = 0\}\\ &= \#\{n\in\mathbb{Z}_{q/\gcd(s,q)} : \gamma_{\gcd(s,q)n}\cdots\gamma_{\gcd(s,q)n+s-2} = 0\}\\ &\le \#\{n\in\mathbb{Z}_q : \gamma_n\cdots\gamma_{n+s-2} = 0\} = s-1\end{aligned}$$

and

$$\begin{aligned} A_N^*(\eta_0) &\le \#\left\{ n \in \mathbb{Z}_{q/\gcd(s,q)} : \gamma_{sn} \cdots \gamma_{sn+s-2} \neq 0, \sum_{l=0}^{s-1} \eta_{l+1}\gamma_{sn+l} = \eta_0 \right\} \\ &= \#\left\{ n \in \mathbb{Z}_{q/\gcd(s,q)} : \gamma_{\gcd(s,q)n} \cdots \gamma_{\gcd(s,q)n+s-2} \neq 0, \right. \\ &\qquad\qquad \left. \sum_{l=0}^{s-1} \eta_{l+1}\gamma_{\gcd(s,q)n+l} = \eta_0 \right\} \\ &\le \#\left\{ n \in \mathbb{Z}_q : \gamma_n \cdots \gamma_{n+s-2} \neq 0, \sum_{l=0}^{s-1} \eta_{l+1}\gamma_{n+l} = \eta_0 \right\} \le s \end{aligned}$$

for any $\eta_0 \in F_q$, where the last inequality follows at once from Lemma 4 in [6] with $d = s$. Further, observe that

$$A_N(\eta_0) = A_N^0(\eta_0) + A_N^*(\eta_0)$$

for $\eta_0 \in F_q$ and

$$\sum_{\eta_0 \in F_q} A_N(\eta_0) = N.$$

Note that the sum of squares

$$\sum_{\eta_0 \in F_q} (A_N(\eta_0))^2 = \sum_{\eta_0 \in F_q} (A_N^0(\eta_0) + A_N^*(\eta_0))^2$$

achieves its maximum possible value under the restrictions $A_N^0(\eta_0) \ge 0$ for any $\eta_0 \in F_q$, $\sum_{\eta_0 \in F_q} A_N^0(\eta_0) \le s-1$, $0 \le A_N^*(\eta_0) \le s$ for any $\eta_0 \in F_q$, and $\sum_{\eta_0 \in F_q} A_N(\eta_0) = N$, if all entries $A_N(\eta_0)$ take extreme values, which means more precisely that

- $A_N^0(\eta_0) = s-1$ and $A_N^*(\eta_0) = s$ for exactly one value of $\eta_0 \in F_q$,
- $A_N^0(\eta_0) = 0$ and $A_N^*(\eta_0) = s$ for exactly ν other values of $\eta_0 \in F_q$,
- $A_N^0(\eta_0) = 0$ and $A_N^*(\eta_0) = \mu$ for exactly one further value of $\eta_0 \in F_q$, and finally
- $A_N^0(\eta_0) = A_N^*(\eta_0) = 0$ for all other values of $\eta_0 \in F_q$,

where $\nu \ge 0$ and $0 \le \mu < s$ are suitable integers such that $N = 2s - 1 + \nu s + \mu$. Therefore, one obtains the estimate

$$\begin{aligned} \sum_{\eta_0 \in F_q} (A_N(\eta_0))^2 &\le (2s-1)^2 + \nu s^2 + \mu^2 \\ &= sN + (s-1)(2s-1) - \mu(s-\mu) \\ &\le sN + (s-1)(2s-1). \end{aligned}$$

Together with the formula of step (ii), this estimate yields the desired result. □

3. Main results

Theorem 1. *Let $1 \le N \le q/\gcd(s,q)$. Then the average value of the star discrepancy $D_{\kappa;N}^{*(s)}$ in the digital inversive method over $\kappa \in F_q^*$ satisfies*

$$\frac{1}{q-1}\sum_{\kappa\in F_q^*} D_{\kappa;N}^{*(1)} \le \begin{cases} \dfrac{2k}{\sqrt{N}}\sqrt{\dfrac{q-N}{q-1}}\left(\dfrac{1}{\pi}\log p+\dfrac{1}{5}\right)+\dfrac{1}{q} & \text{for } p\ge 3,\\ \dfrac{k}{2\sqrt{N}}\sqrt{\dfrac{q-N}{q-1}}+\dfrac{1}{q} & \text{for } p=2,\end{cases}$$

and, for $s \ge 2$,

$$\frac{1}{q-1}\sum_{\kappa\in F_q^*} D_{\kappa;N}^{*(s)} < \begin{cases} \dfrac{1}{\sqrt{N}}\sqrt{s+(s-1)(2s-1)/N}\left(\dfrac{2}{\pi}\log q+\dfrac{2}{5}k+1\right)^s & \text{for } p\ge 3,\\ \dfrac{1}{\sqrt{N}}\sqrt{s+(s-1)(2s-1)/N}\left(\dfrac{k}{2}+1\right)^s & \text{for } p=2.\end{cases}$$

Proof. First, observe that the result is trivial for $s > q$, since the corresponding upper bounds are greater than 1; hence, assume $s \le q$ from now on. Since all coordinates of the points $\mathbf{x}_{\kappa,n}$ have a finite digit expansion in base p, Lemma 1 is applied with $b = p, d = s, t = k$, and $\mathbf{w}_n = \mathbf{x}_{\kappa,n}$ for $0 \le n < N$. Thus, with $\mathbf{h} = (\mathbf{h}_0, \dots, \mathbf{h}_{s-1}) \in C_{ks}^*(p)$ and $\mathbf{h}_l = (h_{l,1}, \dots, h_{l,k}) \in C_k(p)$ for $0 \le l \le s-1$, it follows that

$$D_{\kappa;N}^{*(s)} \le \frac{1}{N}\sum_{\mathbf{h}\in C_{ks}^*(p)} W_p(\mathbf{h})\left|\sum_{n=0}^{N-1} e\left(\frac{1}{p}\sum_{l=0}^{s-1}\sum_{j=1}^{k} h_{l,j}c_{\kappa,sn+l,j}\right)\right| + \frac{s}{p^k}.$$

Further, the average value of $D_{\kappa;N}^{*(s)}$ satisfies

$$\begin{aligned}\frac{1}{q-1}\sum_{\kappa\in F_q^*} D_{\kappa;N}^{*(s)} &\le \frac{1}{N}\sum_{\mathbf{h}\in C_{ks}^*(p)} W_p(\mathbf{h})\left(\frac{1}{q-1}\sum_{\kappa\in F_q^*}\left|\sum_{n=0}^{N-1} e\left(\frac{1}{p}\sum_{l=0}^{s-1}\sum_{j=1}^{k} h_{l,j}c_{\kappa,sn+l,j}\right)\right|\right)+\frac{s}{q}\\ &\le \frac{1}{N}\sum_{\mathbf{h}\in C_{ks}^*(p)} W_p(\mathbf{h})\sqrt{\frac{1}{q-1}\sum_{\kappa\in F_q^*}\left|\sum_{n=0}^{N-1} e\left(\frac{1}{p}\sum_{l=0}^{s-1}\sum_{j=1}^{k} h_{l,j}c_{\kappa,sn+l,j}\right)\right|^2}+\frac{s}{q},\end{aligned}$$

where in the last step the Cauchy–Schwarz inequality was applied. By Lemma 3 one obtains that

$$\begin{aligned}
&\frac{1}{q-1}\sum_{\kappa\in F_q^*} D_{\kappa;N}^{*(s)} \\
&\quad\le \frac{1}{N}\sum_{\mathbf{h}\in C_{ks}^*(p)} W_p(\mathbf{h})\sqrt{\frac{1}{q-1}(N(sq-N)+(s-1)(2s-1)q)}+\frac{s}{q} \\
&\quad= \frac{1}{\sqrt{N}}\sqrt{\frac{(s+(s-1)(2s-1)/N)q-N}{q-1}}\sum_{\mathbf{h}\in C_{ks}^*(p)} W_p(\mathbf{h})+\frac{s}{q}.
\end{aligned}$$

(i) For $p\ge 3$, it follows from [13, Proof of Theorem 2, equation (14)] that

$$\sum_{\mathbf{h}\in C_{ks}^*(p)} W_p(\mathbf{h}) < \left(\frac{2}{\pi}\log q+\frac{2}{5}k+1\right)^s-1,$$

which implies that

$$\begin{aligned}
\frac{1}{q-1}\sum_{\kappa\in F_q^*} D_{\kappa;N}^{*(s)} &\le \frac{1}{\sqrt{N}}\sqrt{\frac{(s+(s-1)(2s-1)/N)q-N}{q-1}} \\
&\quad\times\left(\left(\frac{2}{\pi}\log q+\frac{2}{5}k+1\right)^s-1\right)+\frac{s}{q}.
\end{aligned}$$

For $s=1$, this is already the desired result. For $s\ge 2$, a short calculation and the assumption $N\ge s+(s-1)(2s-1)/N$ (or equivalently, $N\ge 2s-1$) yield the estimates

$$\begin{aligned}
&\frac{1}{q-1}\sum_{\kappa\in F_q^*} D_{\kappa;N}^{*(s)} \\
&\quad\le \frac{1}{\sqrt{N}}\sqrt{s+(s-1)(2s-1)/N}\left(\left(\frac{2}{\pi}\log q+\frac{2}{5}k+1\right)^s-1\right)+\frac{s}{q} \\
&\quad< \frac{1}{\sqrt{N}}\sqrt{s+(s-1)(2s-1)/N}\left(\frac{2}{\pi}\log q+\frac{2}{5}k+1\right)^s.
\end{aligned}$$

For $N<s+(s-1)(2s-1)/N$, the result is trivial, since the upper bound is greater than 1.

(ii) For $p=2$, it follows from the second part of [10, Lemma 3.13] that

$$\sum_{\mathbf{h}\in C_{ks}^*(2)} W_2(\mathbf{h}) = \left(\frac{k}{2}+1\right)^s-1,$$

and the same arguments as in (i) yield the desired result. □

Corollary 1. *Let $1\le N\le q/\gcd(s,q)$ and $0<x\le 1$ be fixed. Then there exist more than $(1-x)(q-1)$ values of $\kappa\in F_q^*$ such that the star discrepancy $D_{\kappa;N}^{*(s)}$ in the digital inversive method satisfies*

$$D_{\kappa;N}^{*(1)} \le \begin{cases} \dfrac{1}{x}\left(\dfrac{2k}{\sqrt{N}}\sqrt{\dfrac{q-N}{q-1}}\left(\dfrac{1}{\pi}\log p+\dfrac{1}{5}\right)+\dfrac{1}{q}\right) & \text{for } p\ge 3, \\ \dfrac{1}{x}\left(\dfrac{k}{2\sqrt{N}}\sqrt{\dfrac{q-N}{q-1}}+\dfrac{1}{q}\right) & \text{for } p=2, \end{cases}$$

and, for $s \ge 2$,

$$D_{\kappa;N}^{*(s)} < \begin{cases} \dfrac{1}{x\sqrt{N}} \sqrt{s + (s-1)(2s-1)/N} \left(\dfrac{2}{\pi} \log q + \dfrac{2}{5} k + 1 \right)^s & \text{for } p \ge 3, \\ \dfrac{1}{x\sqrt{N}} \sqrt{s + (s-1)(2s-1)/N} \left(\dfrac{k}{2} + 1 \right)^s & \text{for } p = 2. \end{cases}$$

Theorem 2. *Let* $1 \le N \le q$. *Then there exist values* $\kappa \in F_q^*$ *such that the star discrepancy* $D_{\kappa;N}^{*(s)}$ *in the digital inversive method satisfies*

$$D_{\kappa;N}^{*(s)} \ge \begin{cases} \dfrac{1}{4\sqrt{N}} \sqrt{\dfrac{q-N}{q-1}} & \text{for } p \ge 3, \\ \dfrac{1}{2\sqrt{N}} \sqrt{\dfrac{q-N}{q-1}} & \text{for } p = 2, \end{cases}$$

and any dimension $s \ge 1$.

Proof. First, consider the s-dimensional points

$$\mathbf{y}_{\kappa,n} = (c_{\kappa,sn,1}, \ldots, c_{\kappa,sn+s-1,1}) \in \mathbb{Z}_p^s$$

for $n \ge 0$, where $c_{\kappa,sn+l,1} \in \mathbb{Z}_p$ is the first coordinate of the vector $\mathbf{c}_{\kappa,sn+l}$ for $0 \le l \le s-1$. Let

$$\mathbf{t}_{\kappa,n} = \mathbf{y}_{\kappa,n}/p \in [0,1)^s$$

for $n \ge 0$. For any subinterval $J \in \mathcal{J}_p^*$, let $L(J)$ be the number of points among $\mathbf{t}_{\kappa,0}, \mathbf{t}_{\kappa,1}, \ldots, \mathbf{t}_{\kappa,N-1}$ falling into J.

(i) Now, observe that $\mathbf{x}_{\kappa,n} \in J$ if and only if $\mathbf{t}_{\kappa,n} \in J$ for any $n \ge 0$ and $J \in \mathcal{J}_p^*$, which implies that

$$D_{\kappa;N}^*(\mathbf{x}_{\kappa,0}, \mathbf{x}_{\kappa,1}, \ldots, \mathbf{x}_{\kappa,N-1}) \ge \max_{J \in \mathcal{J}_p^*} \left| \frac{L(J)}{N} - \mathrm{Vol}(J) \right|.$$

(ii) An application of Lemma 2 with $b = p, d = s, \mathbf{t}_n = \mathbf{t}_{\kappa,n}$ for $0 \le n < N$, and $\mathbf{h} = (1, 0, \ldots, 0) \in \mathbb{Z}^s$ yields

$$\begin{aligned} \left| \sum_{n=0}^{N-1} e(c_{\kappa,sn,1}/p) \right| &= \left| \sum_{n=0}^{N-1} e(\mathbf{h} \cdot \mathbf{t}_{\kappa,n}) \right| \\ &\le \frac{2}{\pi} \left(\prod_{l=0}^{s-1} (2\pi |h_l| + 1) - 1 \right) N \max_{J \in \mathcal{J}_p^*} \left| \frac{L(J)}{N} - \mathrm{Vol}(J) \right| \\ &= 4N \max_{J \in \mathcal{J}_p^*} \left| \frac{L(J)}{N} - \mathrm{Vol}(J) \right| \end{aligned}$$

for any arbitrary prime $p \ge 2$.

(iii) For $p = 2$, the estimate in (ii) can be improved by the following short calculation, namely

$$\begin{aligned}
&\left|\sum_{n=0}^{N-1} e(c_{\kappa,sn,1}/2)\right| \\
&\quad = |\#\{0 \le n < N : c_{\kappa,sn,1} = 0\} - \#\{0 \le n < N : c_{\kappa,sn,1} = 1\}| \\
&\quad = |2\#\{0 \le n < N : c_{\kappa,sn,1} = 0\} - N| \\
&\quad = |2L([0,1/2) \times [0,1)^{s-1}) - N| \\
&\quad = 2N \left| \frac{L([0,1/2) \times [0,1)^{s-1})}{N} - \mathrm{Vol}([0,1/2) \times [0,1)^{s-1}) \right| \\
&\quad \le 2N \max_{J \in \mathcal{J}_2^*} \left| \frac{L(J)}{N} - \mathrm{Vol}(J) \right|.
\end{aligned}$$

(iv) Finally, it follows as in [6, Theorem 3] that there exist values of $\kappa \in F_q^*$ with

$$\left|\sum_{n=0}^{N-1} e(c_{\kappa,sn,1}/p)\right| \ge \sqrt{\frac{N(q-N)}{q-1}},$$

which yields altogether the desired lower bounds for the star discrepancy $D_{\kappa;N}^{*(s)}$. □

4. Conclusions

Theorem 1 shows that in the digital inversive method the star discrepancy $D_{\kappa;N}^{*(s)}$, on the average over the parameter κ, has an order of magnitude at most $N^{-1/2}(\log q)^s$ for any parameters α and β, provided that the condition for the maximum possible period length is met. Corollary 1 is an immediate consequence of Theorem 1, which says that, for any fixed parameters α and β, only an arbitrarily small percentage of the values of the parameter κ may lead to a star discrepancy $D_{\kappa;N}^{*(s)}$ with an order of magnitude greater than $N^{-1/2}(\log q)^s$. On the other hand, Theorem 2 shows that, for any parameters α and β, there exist values of the parameter κ such that the star discrepancy $D_{\kappa;N}^{*(s)}$ is of an order of magnitude at least $N^{-1/2}$, if N is not too close to q. These results are in good accordance with Jack Kiefer's probabilistic law of the iterated logarithm for the star discrepancy of N independent and uniformly distributed random points from $[0,1)^s$, which is almost always of an order of magnitude $N^{-1/2}(\log\log N)^{1/2}$ [8].

The average-case results of the present paper complement recently obtained upper bounds for the star discrepancy of (overlapping s-tuples of) individual sequences over parts of the period with an order of magnitude $N^{-1/2}q^{1/4}(\log q)^s$ (cf. [14, Theorem 2]), which may be viewed as corresponding worst-case results. It should be observed (and has also been pointed out by the referee) that both types of results provide useful information on the distribution properties of digital inversive pseudorandom numbers and none implies the other.

Acknowledgment

The author would like to thank the referee for useful hints and comments, which certainly improved the original version of this article.

References

1. J. Eichenauer-Herrmann, *Inversive congruential pseudorandom numbers: a tutorial*, Internat. Statist. Rev. **60** (1992), 167–176.
2. ———, *Pseudorandom number generation by nonlinear methods*, Internat. Statist. Rev. **63** (1995), 247–255.
3. J. Eichenauer-Herrmann, E. Herrmann, and S. Wegenkittl, *A survey of quadratic and inversive congruential pseudorandom numbers*, Monte Carlo and Quasi–Monte Carlo Methods 1996 (H. Niederreiter, P. Hellekalek, G. Larcher, and P. Zinterhof, eds.), Lecture Notes in Statistics, vol. 127, Springer, New York, 1998, pp. 66–97. MR **99d:**11085
4. J. Eichenauer-Herrmann and H. Niederreiter, *Digital inversive pseudorandom numbers*, ACM Trans. Modeling and Computer Simulation **4** (1994), 339–349.
5. F. Emmerich, *Pseudorandom number and vector generation by compound inversive methods*, Thesis, Darmstadt, 1996.
6. ———, *Statistical independence properties of inversive pseudorandom vectors over parts of the period*, ACM Trans. Modeling and Computer Simulation **8** (1998), 140–152.
7. P. Hellekalek, *General discrepancy estimates: the Walsh function system*, Acta Arith. **67** (1994), 209–218. MR **95h:**65003
8. 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
9. R. Lidl and H. Niederreiter, *Finite fields*, Addison-Wesley, Reading, MA, 1983. MR **86c:**11106
10. H. Niederreiter, *Random number generation and quasi–Monte Carlo methods*, SIAM, Philadelphia, PA, 1992. MR **93h:**65008
11. ———, *Pseudorandom vector generation by the inversive method*, ACM Trans. Modeling and Computer Simulation **4** (1994), 191–212.
12. ———, *New developments in uniform pseudorandom number and vector generation*, Monte Carlo and Quasi–Monte Carlo Methods in Scientific Computing (H. Niederreiter and P. J.-S. Shiue, eds.), Lecture Notes in Statistics, vol. 106, Springer, New York, 1995, pp. 87–120. MR **97k:**65019
13. ———, *Improved bounds in the multiple–recursive matrix method for pseudorandom number and vector generation*, Finite Fields Appl. **2** (1996), 225–240. MR **97d:**11120
14. H. Niederreiter and I. E. Shparlinski, *On the distribution of pseudorandom numbers and vectors generated by inversive methods*, Appl. Algebra Engrg. Comm. Comput. **10** (2000), 189–202.

T-Nova Deutsche Telekom Innovationsgesellschaft, Technologiezentrum, Am Kavalleriesand 3, D-64295 Darmstadt, F. R. Germany