Mathematica Slovaca

Mordechay B. Levin
Explicit digital inversive pseudorandom numbers

Mathematica Slovaca, Vol. 50 (2000), No. 5, 581--598

Persistent URL: http://dml.cz/dmlcz/136791

Math. Slovaca, **50** (2000), No. 5, 581–598

Mathematica Slovaca

EXPLICIT DIGITAL INVERSIVE PSEUDORANDOM NUMBERS

Mordechay B. Levin

(*Communicated by Stanislav Jakubec*)

ABSTRACT. A new algorithm, the *explicit digital inversive method*, for generating uniform pseudorandom numbers is introduced. This method can be viewed as an analog of the *explicit inversive method* and as a variant of *digital inversive method* for pseudorandom number generation. We study, in particular, the statistical independence properties of pseudorandom sequence generated over part of a period. The method of the proof rests on the classical Weil bound for exponential sums.

1. Introduction

1.1. Several nonlinear methods for generating uniform pseudorandom numbers in the interval $[0,1)$ have been proposed in the literature. Reviews and the bibliography of the development of this area can be found in [DrTi], [Ei], [HeLa], [LEq], [Ni1], [Ni2], [NHLZ], and [Te]. In this paper we propose an explicit variant of the digital inversive method of Eichenauer-Herrmann and Niederreiter [EiNi]. First a detailed description of this method is given.

1.2. Let p be a prime, and put $q = p^k$ for some integer $k \geq 1$. Denote by F_q the finite field with q elements, and by $F_q^* = F_q \setminus \{0\}$ the multiplicative group of nonzero elements of F_q. Identify the set $\mathbb{Z}_p = \{0, 1, \dots, p-1\}$ of integers with a finite field $F_p = \mathbb{Z}/p\mathbb{Z}$ with p elements. For $\gamma \in F_q^*$ let $\bar{\gamma} = \gamma^{-1} \in F_q^*$ be the multiplicative inverse of γ in F_q and define $\bar{0} = 0$. For initial value $\kappa_0 \in F_q$ and parameters $\alpha \in F_q^*$ and $\beta \in F_q$ an inversive sequence $(\kappa_n)_{n \geq 0}$ of elements of F_q is defined by the recursion

$$\kappa_{n+1} = \alpha \bar{\kappa}_n + \beta, \qquad n \geq 0. \tag{1}$$

2000 Mathematics Subject Classification: Primary 65C10; Secondary 11K45.
Key words: random number generation, discrepancy.

Work supported in part by the Israel Science Foundation Grant No. 366-1722.

In the following the finite field F_q is viewed as a k-dimensional vector space over $\mathbb{Z}_p$. Let $(\beta_1, \dots, \beta_k)$ be a basis of F_q over F_p, $(\omega_1, \dots, \omega_k)$ the dual basis of $(\beta_1, \dots, \beta_k)$ (see [LN; Definition 2.30]), and Tr denotes the trace function from F_q to F_p.

For $n = 0, 1, \dots$ let $c_n = (c_{n,1}, \dots, c_{n,k})$ be the coordinate vector of $\gamma_n \in F_q$ relative to $(\beta_1, \dots, \beta_k)$. As in [LN; p. 58]

$$c_{n,i} = \mathrm{Tr}(\omega_i \kappa_n), \qquad n = 0, 1, \dots, \quad i = 1, \dots, k. \tag{2}$$

Now a sequence $(y_n)_{n \geq 0}$ of *digital inversive pseudorandom numbers* in the interval $[0, 1)$ is defined by

$$y_n = \sum_{i=1}^{k} \frac{c_{n,i}}{p^i}, \qquad n = 0, 1, \dots. \tag{3}$$

1.3. Every integer $n \geq 0$ has a unique digit expansion

$$n = \sum_{j \geq 0} a_j(n) p^j \tag{4}$$

in base p, where $a_j(n) \in \{0, 1, \dots, p-1\}$ for all $j \geq 0$ and $a_j(n) = 0$ for all sufficiently large j. For initial value $\gamma_0 \in F_q$ and parameters $\alpha \in F_q^*$ and $\beta \in F_q$, a sequence $(x_n)_{n \geq 0}$ of *explicit digital inversive pseudorandom numbers* in the interval $[0, 1)$ is defined by

$$x_n = \sum_{i=1}^{k} \frac{x_{n,i}}{p^i}, \qquad x_{n,i} = \mathrm{Tr}\big(\omega_i(\alpha \bar{\gamma}_n + \beta)\big) \qquad \text{and} \qquad \gamma_n = \sum_{i=0}^{k-1} \beta_{i+1} a_i(n) + \gamma_0. \tag{5}$$

Obviously, a sequence $(x_n)_{n \geq 0}$ is purely periodic with period length equal to q.

1.4. Equidistribution, as well as statistical independence properties of uniform pseudorandom numbers in the interval $[0, 1)$ can be analyzed by the discrepancy of certain point sets in $[0, 1)^s$ with $s \geq 1$. For N arbitrary points $\mathbf{t}_0, \dots, \mathbf{t}_{N-1} \in [0, 1)^s$ with $s \geq 1$, their *star discrepancy* is defined by

$$D^*\big((\mathbf{t}_n)_{n=0}^{N-1}\big) = \sup_{v = [0, \gamma_1) \times \dots \times [0, \gamma_s) \subset [0,1)^s} \left| \frac{1}{N} \# \{ n \in [0, N) \mid \mathbf{t}_n \in v \} - \gamma_1 \cdots \gamma_s \right|.$$

In accord with [EiNi; Theorem 1]

$$D^*\big((y_n, \dots, y_{n+s-1})_{n=0}^{q-1}\big) = O(p^{-k/2} k^s)$$

for digital inversive method.

For explicit digital inversive pseudorandom numbers we obtain here a slightly worse estimate

$$D^*\big((x_n,\dots,x_{n+s-1})_{n=0}^{q-1}\big) = O\big(p^{-k/2}k^{s+1}\big).$$

But using this method we obtain a discrepancy estimate over part of the period

$$D^*\big((x_n,\dots,x_{n+s-1})_{n=0}^{N-1}\big) = O\big(N^{-1}p^{k/2}k^{s+2}\big), \quad N = 1,2,\dots .$$

Using the approach proposed in [Le] we show that there exists $\alpha \in F_q^*$ with the following discrepancy

$$D^*\big((x_n,\dots,x_{n+s-1})_{n=0}^{N-1}\big) = O\big(N^{-1/2}\log^{s+3} N\big), \qquad N = 1,2,\dots,p^k,$$

for part of the period of the digital inversive method and the explicit digital inversive method.

2. Auxiliary results

First, some further notation is necessary. $C(l) = \mathbb{Z} \cap (-l/2, l/2]$. For real u, the abbreviation $e(u) = \mathrm{e}^{2\pi\sqrt{-1}u}$ is used.

Define

$$r(h,q) = \begin{cases} q\sin\big(\pi|h|/q\big) & \text{for } h \in C(q),\ h \neq 0, \\ 1 & \text{for } h = 0. \end{cases} \tag{6}$$

Subsequently, five known results are stated, which follow from [Ko; Lemma 2], [Ni1; Lemma 2.3], [Ko; p. 13], and [Ni2; p. 35], [Ni2; Theorem 3.12, Lemma 3.13], and [LN; p. 188–190] respectively.

Lemma 2.1. *Let*

$$\delta_p(a) = \begin{cases} 1 & \text{if } a \equiv 0 \mod p, \\ 0 & \text{otherwise}. \end{cases}$$

Then

$$\delta_p(a) = \frac{1}{p}\sum_{n=0}^{p-1} e(an/p).$$

Lemma 2.2. *Let $q \geq 2$ be an integer. Then*

$$\sum_{h \in C(q)} \frac{1}{r(h,q)} < \frac{2}{\pi}\log q + \frac{7}{5}.$$

LEMMA 2.3. *Let $T \geq N \geq 1$ be integers. Then*

$$\left|\sum_{n=0}^{N-1} e(u_n)\right| \leq \sum_{h \in C(T)} \frac{1}{r(h,T)} \left|\sum_{n=0}^{T-1} e\left(u_n + \frac{nh}{T}\right)\right|.$$

P r o o f . According to [Ni2; p. 35], $1/T\left|\sum_{n\in[0,N-1]} e(nh/T)\right| \leq r^{-1}(h,T)$. Now repeating the proof of [Ko; p. 13] we obtain the assertion of Lemma 2.3. □

Let $b \geq 2$ be integer,

$$\mathbf{w}_n = \left(w_n^{(1)}, \dots, w_n^{(s)}\right) \in [0,1)^s \qquad \text{for} \quad n = 0, 1, \dots, N-1,$$

where for an integer $m_1 \geq 1$, we have

$$w_n^{(i)} = \sum_{j=1}^{m_1} w_{n,j}^{(i)} b^{-j} \qquad \text{for} \quad 0 \leq n \leq N-1, \ i = 1, \dots, s, \tag{7}$$

with $w_{n,j}^{(i)} \in \{0, \dots, b-1\}$ for $0 \leq n \leq N-1$, $1 \leq i \leq s$, $1 \leq j \leq m_1$.

Let $C(b)^{s\times m_1}$ be the set of all $s \times m_1$ matrices with entries in $C(b)$, $H = (h_{ij}) \in C(b)^{s\times m_1}$.

LEMMA 2.4. *Let $s, m_1 \geq 1$ and $b \geq 2$ be integers. If $\left((\mathbf{w}_n)_{n=0}^{N-1}\right)$ is the point set* (7)*, then*

$$D^*\left((\mathbf{w}_n)_{n=0}^{N-1}\right) \leq 1 - (1 - b^{-m_1})^s + \sum_{\substack{H \in C(b)^{s\times m_1} \\ H \neq 0}} W_{b,m_1}(H) \left|\frac{1}{N} \sum_{n=0}^{N-1} e\left(\frac{1}{b} \sum_{i=1}^{s} \sum_{j=1}^{m_1} h_{ij} w_{nj}^{(i)}\right)\right|,$$

where the weight $W_{b,m_1}(H) \geq 0$ satisfies the following inequality

$$\sum_{\substack{H \in C(b)^{s\times m} \\ H \neq 0}} W_{b,m_1}(H) < \left(\frac{2}{\pi} m_1 \log b + \frac{7}{5} m_1 - \frac{m_1 - 1}{b}\right)^s.$$

Remark. Let $\mathbf{x}_n = (x_{n,1}, \dots, x_{n,s})$, $\{\mathbf{x}_n\}_k = (\{x_{n,1}\}_k, \dots, \{x_{n,s}\}_k)$, $\{x_{n,i}\}_k = [b^k\{x_{n,i}\}]/b^k$, $i \in [1,s]$, $k \geq 1$, $n \geq 0$; $v = [0,\gamma_1) \times \dots \times [0,\gamma_s)$; $v' = \prod_{i=1}^{s} [0, \{\gamma_i\}_k]$.

It is easy to see, that

$$\begin{aligned}&1/N\#\{0\le n\le N-1 \mid \ \{\mathbf{x}_n\}\in v\}-\gamma_1\cdots\gamma_s\\ &\le 1/N\#\{0\le n\le N-1 \mid \ \{\mathbf{x}_n\}_k\in v\}-\gamma_1\cdots\gamma_s\\ &\le D^*\Big((\{\mathbf{x}_n\}_k)_{n=0}^{N-1}\Big)\end{aligned}$$

and

$$\begin{aligned}&1/N\#\{0\le n\le N-1 \mid \ \{\mathbf{x}_n\}\in v\}-\gamma_1\cdots\gamma_s\\ &\ge 1/N\#\{0\le n\le N-1 \mid \ \{\mathbf{x}_n\}_k\in v'\}-\gamma_1\cdots\gamma_s\\ &\ge -D^*\Big((\{\mathbf{x}_n\}_k)_{n=0}^{N-1}\Big)-\left|\prod_{i=1}^{s}\gamma_i-\prod_{i=1}^{s}\{\gamma_i\}_k\right|.\end{aligned}$$

Hence

$$\begin{aligned}D^*\big((\mathbf{x}_n)_{n=0}^{N-1}\big)-D^*\Big((\{\mathbf{x}_n\}_k)_{n=0}^{N-1}\Big)&\le \sup_{\gamma_1,\dots,\gamma_s\in[0,1)}\left|\prod_{i=1}^{s}\gamma_i-\prod_{i=1}^{s}\{\gamma_i\}_k\right|\\ &\le 1-\Big(1-\frac{1}{b^k}\Big)^s\le\frac{s}{b^k}.\end{aligned}$$

This yields

$$D^*\big((\mathbf{x}_n)_{n=0}^{N-1}\big)\le\frac{s}{b^k}+D^*\Big((\{\mathbf{x}_n\}_k)_{n=0}^{N-1}\Big).$$

Now from Lemma 2.4 we obtain for all $m\in[1,m_1]$ that

$$D^*\big((\mathbf{w}_n)_{n=0}^{N-1}\big)\le 2s/b^m+\sum_{\substack{H\in C(b)^{s\times m}\\ H\neq 0}}W_{b,m}(H)\left|\frac{1}{N}\sum_{n=0}^{N-1}e\Big(\frac{1}{b}\sum_{i=1}^{s}\sum_{j=1}^{m}h_{ij}w_{nj}^{(i)}\Big)\right|.$$

Applying Lemma 2.3 we have:

Corollary 2.1. *Let $1\le N\le T$, $1\le m\le m_1$. Then*

$$D^*\big((\mathbf{w}_n)_{n=0}^{N-1}\big)\le 2s/b^m+\frac{T}{N}\widetilde{D}_{T,m}(\mathbf{w}_n),$$

where

$$\widetilde{D}_{T,m}(\mathbf{w}_n)=\frac{1}{T}\sum_{\substack{H\in C(b)^{s\times m}\\ H\neq 0}}\sum_{h\in C(q)}\frac{W_{b,m}(H)}{r(h,q)}\left|\sum_{n=0}^{T-1}e\Big(\frac{1}{b}\sum_{i=1}^{s}\sum_{j=1}^{m}h_{ij}w_{nj}^{(i)}+\frac{hn}{T}\Big)\right|.$$

Let

$$\chi(\gamma)=e\Big(\frac{1}{p}\operatorname{Tr}(\gamma)\Big)\qquad\text{for}\quad \gamma\in F_q \tag{8}$$

define a nontrivial additive character χ over F_q.

LEMMA 2.5. *Let $\beta \in F_q$,*

$$\delta(\beta) = \begin{cases} 1 & \text{if } \beta = 0, \\ 0 & \text{otherwise.} \end{cases}$$

Then

$$\delta(\beta) = \frac{1}{q} \sum_{\alpha \in F_q} \chi(\alpha\beta).$$

The following lemma is a convenient form of the Bombieri-Weil bound of exponential sums (see [Mo; Theorem 2]).

We denote by $\bar{F}_q$ the algebraic closure of the field F_q and by $\bar{F}_q(x)$ the field of rational functions over $\bar{F}_q$.

LEMMA 2.6. *Let Q/R be a rational function over F_q which is not of the form $A^p - A$ with $A \in \bar{F}_q(x)$. Let s be the number of the distinct root of the polynomial R in $\bar{F}_q$. Then we have*

$$\Bigg| \sum_{\substack{\gamma \in F_q \\ R(\gamma) \neq 0}} \chi\left(\frac{Q(\gamma)}{R(\gamma)}\right) \Bigg| \leq \Big(\max\big(\deg(Q), \deg(R)\big) + s^* - 2\Big) q^{1/2} + \Delta,$$

where $s^* = s$ and $\Delta = 1$ if $\deg(Q) \leq \deg(R)$, and $s^* = s + 1$ and $\Delta = 0$ otherwise.

LEMMA 2.7. *Let $1 \leq d < q$; $\eta, \theta_1, \dots, \theta_d \in F_q$. Then*

$$|S(\theta)| \leq d(2q^{1/2} + 1) \qquad \text{with} \quad S(\theta) = \sum_{\gamma \in F_q} \chi\left(\sum_{i=1}^{d} \alpha_i \overline{\gamma + \theta_i} + \eta\gamma \right),$$

where $\theta_i \neq \theta_j$ for $i \neq j$, and $\alpha_1, \dots, \alpha_d$ are not all zero.

Proof. The case $\eta \neq 0$ see [Ni3; p. 205]. Let $\eta = 0$. We follow [Ni4; p. 164]. Clearly

$$|S(\theta)| \leq d + \Bigg| \sum_{\substack{\gamma \in F_q \\ R(\gamma) \neq 0}} \chi\left(\frac{Q(\gamma)}{R(\gamma)}\right) \Bigg|,$$

where Q/R is the rational function over F_q given by

$$\frac{Q(x)}{R(x)} = \sum_{i=1}^{d} \frac{\alpha_i}{x + \theta_i} \qquad \text{with} \quad R(x) = \prod_{i=1}^{d} (x + \theta_i).$$

We claim that Q/R is not of the form $A^p - A$ with a rational function $A \in \bar{F}_q(x)$, because if we had $Q/R = (K/L)^p - K/L$ with polynomials K, L over $\bar{F}_p$ and $\gcd(K, L) = 1$, then

$$L^p Q = (K^{p-1} - L^{p-1}) K R. \tag{9}$$

From $\gcd(K,L)=1$ it follows that L^p divides R, but since R has only simple roots, this divisibility relation can only hold if L is a nonzero constant polynomial. Since at least one α_i is nonzero, the uniqueness of the partial fraction decomposition for rational functions implies that $Q \neq 0$. Then a comparison of degrees in (9) yields $\deg(Q) \geq \deg(R)$ and this contradiction proves the claim. Thus we can apply Lemma 2.6. □

For reals u_n, $n = 0,1,\dots$, and $V = \emptyset$ we pose, as usual, $\sum_{n\in V} u_n = 0$.

Let $m, d, r_1 \geq 1$ be integers with $p^{r_1-1} \leq d < p^{r_1} < p^m$, $d_1 = p^{r_1} - d - 1$. Put

$$
\begin{aligned}
&A_{d,m}(r_1-1) = \{0,1,\dots,d_1\},\\
&\quad A_{d,m}(r) = \Big\{ n \in [0,p^{r+1}) \mid n = l + (p-1)\sum_{r_1\leq i<r} p^i + vp^r \\
&\qquad\qquad \text{with } v \in [0,p-2],\ l \in [d_1+1, p^{r_1}-1] \Big\}, \qquad r \in [r_1, m-1],\\
&\quad A_{d,m}(m) = \Big\{ n \in [0,p^m) \mid n = l + (p-1)\sum_{r_1\leq i<m} p^i,\ l \in [d_1+1, p^{r_1}-1] \Big\}.
\end{aligned} \tag{10}
$$

It is easy to see that

$$
n_1 + i < p^{r+1} \qquad \text{for} \quad i \in [1,d],\ n_1 \in A_{d,m}(r) \text{ with } r \in [r_1-1, m-1];
$$

$$
\# A_{d,m}(m) = d, \qquad \# A_{d,m}(m-1) = (p-1)d. \tag{11}
$$

LEMMA 2.8. *Let $m, d, r_1 \geq 1$ be integers, $p^{r_1-1} \leq d < p^{r_1} \leq p^{m-1}$. Then we have a decomposition of the interval $[0,p^m)$ in the following union of disjunct subsets:*

$$
\begin{aligned}
&[0,p^m) \setminus \big(A_{d,m}(m) \cup A_{d,m}(m-1)\big)\\
&= \bigcup_{r=r_1-1}^{m-2} \ \bigcup_{n_1\in A_{d,m}(r)} \{ n \in [0,p^m) \mid n = n_1 + v_{r+1}p^{r+1} + \dots + v_{m-1}p^{m-1},\\
&\qquad\qquad\qquad\qquad\qquad\qquad v_{r+1},\dots,v_{m-1} \in \mathbb{Z}_p \}.
\end{aligned}
$$

P r o o f. It is easy to verify that

$$
[0,p^m) = G_1 \cup G_2 \cup G_3 \cup G_4, \tag{12}
$$

where

$$G_1 = \{n \in [0,p^m) \mid n \equiv l \pmod{p^{r_1}},\ l \in [0,d_1]\},$$

$$G_2 = A_{d,m}(m) = \Big\{n \in [0,p^m) \mid n \equiv l \pmod{p^{r_1}},\ l \in [d_1+1,p^{r_1}-1] \text{ and } n = l + (p-1)\sum_{r_1 \le i < m} p^i\Big\},$$

$$G_3 = A_{d,m}(m-1) = \Big\{n \in [0,p^m) \mid n \equiv l \pmod{p^{r_1}},\ l \in [d_1+1,p^{r_1}-1] \text{ and } n = l + (p-1)\sum_{r_1 \le i < m-1} p^i + vp^{m-1},\ v \in [0,p-2]\Big\},$$

$$G_4 = \Big\{n \in [0,p^m) \mid n \equiv l \pmod{p^{r_1}},\ l \in [d_1+1,p^{r_1}-1] \text{ and } (\exists\, r \in [r_1,m-2])\Big(n \equiv l + (p-1)\sum_{r_1 \le i < r} p^i + vp^r \pmod{p^{r+1}} \ \&\ v \in [0,p-2]\Big)\Big\}$$

for $r_1 \le m-2$, and $G_4 = \emptyset$ for $r_1 = m-1$.

Using (10), we obtain

$$G_1 = \{n \in [0,p^m) \mid n = l + v_{r_1}p^{r_1} + \cdots + v_{m-1}p^{m-1} \text{ with } l \in [0,d_1], \text{ and } v_i \in \mathbb{Z}_p,\ i = r_1,\dots,m-1\}$$
$$= \bigcup_{n_1 \in A_{d,m}(r_1-1)} \{n \in [0,p^m) \mid n = n_1 + v_{r_1}p^{r_1} + \cdots + v_{m-1}p^{m-1}, \text{ and } v_i \in \mathbb{Z}_p,\ i = r_1,\dots,m-1\},$$

and for $r_1 \le m_2$

$$G_4 = \bigcup_{r \in [r_1,m-2]} G_{4,r}, \tag{13}$$

where

$$G_{4,r} = \Big\{n \in [0,p^m) \mid n = l + (p-1)\sum_{r_1 \le i < r} p^i + vp^r + v_{r+1}p^{r+1} + \cdots + v_{m-1}p^{m-1}, \text{ with } l \in [d_1+1,p^{r_1}-1],\ v \in [0,p-2], \text{ and } v_i \in \mathbb{Z}_p,\ i = r+1,\dots,m-1\Big\}$$
$$= \bigcup_{n_1 \in A_{d,m}(r)} \{n \in [0,p^m) \mid n = n_1 + v_{r+1}p^{r+1} + \cdots + v_{m-1}p^{m-1}, \text{ where } v_i \in \mathbb{Z}_p;\ i = r+1,\dots,m-1\}.$$

Now from (12) and (13) we obtain the assertion of the lemma. □

LEMMA 2.9. *Let* $1 \le s \le q = p^k$, $\alpha_0, \alpha_1, \dots, \alpha_s \in F_q$, $(\alpha_1, \dots, \alpha_s) \ne \mathbf{0}$,

$$S(\alpha) = \sum_{n=0}^{p^k-1} e\Big(\frac{1}{p}\operatorname{Tr}\Big(\sum_{i=1}^{s} \alpha_i \overline{\gamma_{n+i}} + \alpha_0 \gamma_n\Big)\Big).$$

Then

$$|S(\alpha)| \le p s^2 k (2p^{k/2} + 1).$$

Proof. It is easy to see, that the assertion of the lemma is trivial for $k \in [1,2]$, and for $k \ge 3$ with $s \ge p^{k-2} \ge p^{(k-1)/2}$.

Now let $k \ge 3$ and $s \in [1, p^{k-2})$.

This yields that $r_1 = [\log_p s] + 1 \le k - 2$.

Using (5), (11), and Lemma 2.8 we have, for $n_1 \in A_{s,k}(r)$, $r \in [r_1 - 1, k-2]$, and $n = n_1 + \sum_{r+1 \le i < k} v_i p^i$ that

$$\gamma_{n+i} = \gamma_{n_1+i} + \sum_{r+1 \le j < k} v_j \beta_{j+1}, \qquad i = 1, \dots, s. \tag{14}$$

From (11) and Lemma 2.8 we obtain that

$$|S(\alpha)| \le ps + \sum_{r=r_1-1}^{k-2} \sum_{n_1 \in A_{s,k}(r)} |\sigma(r, n_1)| \tag{15}$$

with

$$\sigma(r, n_1) = \sum_{v_{r+1}, \dots, v_{k-1} \in \mathbb{Z}_p} e\Big(\frac{1}{p}\operatorname{Tr}\Big(\sum_{i=1}^{s} \alpha_i \big(\overline{\gamma_{n_1+i} + v_{r+1}\beta_{r+2} + \dots + v_{k-1}\beta_k}\big) + \alpha_0\Big(\gamma_{n_1} + \sum_{r+1 \le j < k} v_j \beta_{j+1}\Big)\Big)\Big). \tag{16}$$

Put

$$\eta = \sum_{j=0}^{k-1} v_j \beta_{j+1}.$$

According to [LN; p. 58],

$$v_{j-1} = \operatorname{Tr}(\eta \omega_j), \qquad j = 1, \dots, k, \tag{17}$$

where $(\omega_1, \dots, \omega_k)$ be the dual basis of $(\beta_1, \dots, \beta_k)$.

From (16) – (17) we deduce that

$$\sigma(r,n_1) = \sum_{\eta\in F_q} e\Big(\frac{1}{p}\operatorname{Tr}\Big(\sum_{i=1}^{s}\alpha_i(\overline{\gamma_{n_1+i}+\eta}) + \alpha_0(\gamma_{n_1}+\eta)\Big)\Big)\prod_{j=1}^{r+1}\delta_p(\operatorname{Tr}(\eta\omega_j))\,.$$

Applying Lemma 2.1, we obtain, that

$$\sigma(r,n_1) = $$

$$= \frac{1}{p^{r+1}}\sum_{h_1,\dots,h_{r+1}\in C_p}\ \sum_{\eta\in F_q} e\Big(\frac{1}{p}\operatorname{Tr}\Big(\sum_{i=1}^{s}\alpha_i(\overline{\gamma_{n_1+i}+\eta}) + \alpha_0(\gamma_{n_1}+\eta) + \sum_{j=1}^{r+1}h_j\eta\omega_j\Big)\Big)\,.$$

This yields

$$|\sigma(r,n_1)| \leq$$

$$\leq \frac{1}{p^{r+1}}\sum_{h_1,\dots,h_{r+1}\in C_p}\Big|\sum_{\eta\in F_q}\chi\Big(\sum_{i=1}^{s}\alpha_i\overline{\gamma_{n_1+i}+\eta} + \alpha_0\gamma_{n_1} + \eta\Big(\alpha_0 + \sum_{j=1}^{r+1}h_j\omega_j\Big)\Big)\Big|\,.$$

Hence

$$|\sigma(r,n_1)| \leq \max_{\alpha_0,\beta_0\in F_q}\Big|\sum_{\eta\in F_q}\chi\Big(\sum_{i=1}^{s}\alpha_i\overline{\gamma_{n_1+i}+\eta} + \alpha_0\eta + \beta_0\Big)\Big|\,.$$

By (5), $\gamma_{n_1+i} \neq \gamma_{n_1+j}$ for $i \neq j$, and $n_1 \in A_{s,k}(r)$ $(r \in [r_1-1, k-2]$, $i,j = 1,\dots,s)$. From Lemma 2.7 we obtain that

$$|\sigma(r,n_1)| \leq s(2q^{1/2}+1)\,. \tag{18}$$

Let $s_1 = p^{r_1} - s - 1$. From (10) and (11), we have for $r \in [r_1, k-2]$

$$s_1 + 1 \leq ps - s\,,\quad \#A_{s,k}(r_1-1) = s_1 + 1 \leq ps - s\,,\quad \text{and}\quad \#A_{s,k}(r) = s(p-1)\,. \tag{19}$$

Hence

$$\sum_{r_1-1\leq r\leq k-2}\#A_{s,k}(r) \leq (k-r_1)s(p-1) \leq (k-1)s(p-1)\,. \tag{20}$$

Substituting (18) and (20) into (15), we obtain that

$$|S(\alpha)| \leq sp + s(k-1)(p-1)s(2q^{1/2}+1) \leq ps^2k(2q^{1/2}+1)\,.$$

□

Let $\eta_0, \eta_1, \dots, \eta_d$ be elements in F_q with $(\eta_1,\dots,\eta_d) \neq \mathbf{0}$, and define a hyperplane E in F_q^d by

$$E = \{(\xi_1,\dots,\xi_d) \in F_q^d \mid \eta_1\xi_1 + \dots + \eta_d\xi_d = \eta_0\}\,.$$

Put

$$B(m,\eta,\eta_0) = \#\{n \in [0,p^m) \mid \eta_1\overline{\gamma_{n+1}} + \dots + \eta_d\overline{\gamma_{n+d}} = \eta_0\}\,. \tag{21}$$

Lemma 2.10. *For $1 \le m \le k$, $d \ge 2$ and every sequence $(\mathbf{x}_n)_{n\ge 0}$ defined by the explicit digital inversive method, any hyperplane E in F_q^d contains at most $2d^2pm$ points $(x_n, \dots, x_{n+d-1})$ with $0 \le n \le p^m - 1 < q$:*

$$B(m,\eta,\eta_0) < 2d^2pm\,.$$

P r o o f. Let $r_1 = [\log_p d] + 1$ and $d_1 = p^{r_1} - d - 1$. If $r_1 \ge m$, then

$$B(m,\eta,\eta_0) \le p^m \le p^{2m-1} \le p^{2r_1-1} \le d^2p < 2d^2pm\,.$$

This is the assertion of the lemma.

Now let $r_1 \le m-1$.

Using (11), (14), Lemma 2.8 and (21), we get, that

$$\begin{aligned} &B(m,\eta,\eta_0) \le \\ &\le \#A_{d,m}(m) + \#A_{d,m}(m-1) \times \\ &\times \sum_{r=r_1-1}^{m-2} \sum_{n_1\in A_{d,m}(r)} \#\Big\{n = n_1 + v_{r+1}p^{r+1} + \dots + v_{m-1}p^{m-1} \mid \\ &\qquad v_{r+1},\dots,v_{m-1} \in \mathbb{Z}_p,\ \eta_1\overline{\gamma_{n+1}} + \dots + \eta_d\overline{\gamma_{n+d}} = \eta_0\Big\}\,. \end{aligned}$$

From (4), (5) and (11) we deduce, that

$$\begin{aligned} &B(m,\eta,\eta_0) \le \\ &\le dp + \sum_{r_1-1\le r\le m-2} \sum_{n_1\in A_{d,m}(r)} \#\Big\{(v_{r+1},\dots,v_{m-1}) \in \mathbb{Z}_p^{m-r-1} \mid \\ &\qquad \sum_{1\le i\le d} \eta_i\overline{\gamma_{n_1+i} + v_{r+1}\beta_{r+2} + \dots + v_{m-1}\beta_m} = \eta_0\Big\}\,. \end{aligned}$$

Hence

$$\begin{aligned} &B(m,\eta,\eta_0) \le \\ &\le dp + \sum_{r_1-1\le r\le m-2} \sum_{n_1\in A_{d,m}(r)} \Big(\#\Big\{\gamma \in F_q \mid \sum_{1\le i\le d} \eta_i\overline{\gamma_{n_1+i} + \gamma} = \eta_0\Big\}\Big) \\ &\le dp + \sum_{r_1-1\le r\le m-2} \sum_{n_1\in A_{d,m}(r)} \Big(d + \#\Big\{\gamma \in F_q \mid \gamma_{n_1+i} + \gamma \ne 0,\ i = 1,\dots,d, \\ &\qquad \sum_{1\le i\le d} \eta_i(\gamma_{n_1+i} + \gamma)^{-1} = \eta_0\Big\}\Big)\,. \end{aligned}$$

Applying (20), we obtain that

$$B(m,\eta,\eta_0) \le dp + (m-1)d(p-1) \max_{\substack{r\in[r_1-1,m-2]\\ n_1\in A_{d,m}(r)}} \Big(d + \#\{\gamma \in F_q \mid P(\gamma) = 0\}\Big)\,, \tag{22}$$

where the polynomial P over F_q is given by

$$P(\gamma) = \eta_0 \prod_{i=1}^{d} (\gamma_{n_1+i} + \gamma) - \sum_{i=1}^{d} \eta_i \prod_{\substack{1\leq j\leq d \\ j\neq i}} (\gamma_{n_1+j} + \gamma).$$

If P were the zero polynomial, then, by looking at the coefficient of γ^d, one would obtain $\eta_0 = 0$. Furthermore, for $1 \leq i \leq d$, it follows that

$$0 = P(-\gamma_{n_1+i}) = -\eta_i \prod_{\substack{1\leq i\leq d \\ j\neq i}} (\gamma_{n_1+j} - \gamma_{n_1+i}).$$

Hence $\eta_i = 0$, a contradiction to $(\eta_1, \dots, \eta_d) \neq 0$. Thus $\deg P \in [1, d]$.

Now from (22) we have

$$B(m, \eta, \eta_0) \leq dp + 2d(m-1)d(p-1) < 2md^2 p.$$

□

LEMMA 2.11. *Let $N, m \geq 1$, $b \geq 2$ be integers, $N \in [1, b^m]$, $(f_n)_{n\geq 0}$ be sequence of reals. Then*

$$\Big|\sum_{n=0}^{N-1} e(f_n)\Big| \leq \min\big(b, \tfrac{2}{\pi}\log b + \tfrac{7}{5}\big) \sum_{r=1}^{m} \max_{h_1,\dots,h_r \in C(b)} \Big|\sum_{n=0}^{b^m-1} e\Big(f_n + \frac{1}{b}\sum_{j=1}^{r} h_j a_{m-j}(n)\Big)\Big|. \tag{23}$$

Proof. Let $u = u(N) = N/b^m = \sum_{1\leq j\leq m} u_j b^{-j}$ with $u_j \in \{0, \dots, b-1\}$ $(1 \leq j \leq m-1)$, $u_m \in \{0, \dots, b\}$; $w_n = \sum_{1\leq j\leq m} w_{n,j} b^{-j} = n/b^m = \sum_{1\leq j\leq m} a_{m-j}(n) b^{-j}$ (see (4)); $c(u, x)$ is the characteristic function of the interval $[0, u)$. In accord with [Ni2; p. 38]

$$c(u(N), w_n) = \sum_{r=1}^{m} \frac{1}{b^r} \sum_{h_1,\dots,h_r \in C(b)} e\Big(\frac{1}{b}\sum_{j=1}^{r} h_j w_{n,j} - \frac{1}{b}\sum_{j=1}^{r-1} h_j u_j\Big) \sum_{v=0}^{u_r-1} e\Big(\frac{-h_r v}{b}\Big).$$

It is easy to see that

$$\sum_{n=0}^{N-1} e(f_n) = \sum_{n=0}^{b^m-1} e(f_n) c\Big(\frac{N}{b^m}, \frac{n}{b^m}\Big)$$

$$= \sum_{r=1}^{m} \frac{1}{b^r} \sum_{\substack{h_1,\dots,h_r \\ \in C(b)}} \sum_{n=0}^{b^m-1} e\Big(f_n + \frac{1}{b}\sum_{j=1}^{r} h_j a_{m-j}(n)\Big) e\Big(-\frac{1}{b}\sum_{j=1}^{r-1} h_j u_j\Big) \sum_{v\in[0,u_r)} e\Big(\frac{-h_r v}{b}\Big).$$

Put

$$T_r(h,N) = e\Big(-\frac{1}{b}\sum_{j=1}^{r-1} h_j u_j\Big) \sum_{v\in[0,u_r)} e\Big(\frac{-h_r v}{b}\Big).$$

Then

$$\Big|\sum_{n=0}^{N-1} e(f_n)\Big| \le \sum_{r=1}^{m} \frac{1}{b^r} \sum_{h_1,\dots,h_r\in C(b)} \Big|\sum_{n=0}^{b^m-1} e\Big(f_n + \frac{1}{b}\sum_{j=1}^{r} h_j a_{m-j}(n)\Big) T_r(h,N)\Big|. \tag{24}$$

Clearly

$$|T_r(h,N)| \le \min\big(u_r,\ 1/\sin(\pi|h_r|/b)\big) \le b.$$

Applying (6) and Lemma 2.2 we get, that

$$\frac{1}{b}\sum_{h_r\in C(b)} |T_r(h,N)| \le \min\big(b,\ \tfrac{2}{\pi}\log b + \tfrac{7}{5}\big).$$

Now from (24) we obtain the assertion of the lemma. □

Lemma 2.12. *Let $k, N \ge 1$ be integers, $N \le p^k = q$, $1 \le s < q$, $\alpha \in F_q^*$, $\big((h_{ij})_{1\le i\le s,\,1\le j\le k}\big) = H \ne \mathbf{0}$. Then*

$$\Big|\sum_{n=0}^{N-1} e\Big(\frac{1}{p}\operatorname{Tr}\Big(\alpha\sum_{i=1}^{s}\sum_{j=1}^{k} h_{ij}\overline{\gamma_{n+i}}\omega_j\Big)\Big)\Big| \le \min\big(p,\ \tfrac{2}{\pi}\log p + \tfrac{7}{5}\big) p s^2 k^2 \big(2p^{k/2}+1\big). \tag{25}$$

Proof. Put $\alpha\sum_{j=1}^{k} h_{ij}\omega_j = \alpha_i$, $i = 1,\dots,s$. Since $(\omega_1,\dots,\omega_k)$ is the basis of F_q over F_p, $\alpha \ne 0$ and $H \ne \mathbf{0}$, it follows that $(\alpha_1,\dots,\alpha_s) \ne (0,\dots,0)$. From (4), (5), and (17) we have, that

$$a_{k-j}(n) = \operatorname{Tr}\big((\gamma_n - \gamma_0)\omega_{k-j+1}\big), \qquad j = 1,\dots,k,\ \ n = 0,1,\dots,p^k-1.$$

Applying Lemma 2.11, we obtain that the left side of (25) is less than

$$\min\big(p,\ \tfrac{2}{\pi}\log p + \tfrac{7}{5}\big)\sum_{r=1}^{k} \max_{\substack{h_1,\dots,h_r\\ \in C(p)}} \Big|\sum_{n=0}^{p^k-1} e\Big(\frac{1}{p}\operatorname{Tr}\Big(\sum_{i=1}^{s}\alpha_i\overline{\gamma_{n+i}} + (\gamma_n-\gamma_0)\sum_{j=1}^{r} h_j\omega_{k-j+1}\Big)\Big)\Big|.$$

Now from Lemma 2.9 we obtain the assertion of the lemma. □

3. Discrepancy bounds

3.1. Upper bounds.

THEOREM 1. *Let $(x_n)_{n\geq 0}$ be a sequence of the explicit digital inversive pseudorandom numbers* (5). *Then*

$$D^*\big((x_n,\dots,x_{n+s-1})_{n=0}^{p^k-1}\big) \leq \frac{s}{p^k} + ps^2\big(2p^{-k/2}+p^{-k}\big)k\Big(\frac{2}{\pi}k\log p + \frac{7}{5}k - \frac{k-1}{p}\Big)^s, \qquad s=1,2,\dots, \tag{26}$$

$$D^*\big((x_n,\dots,x_{n+s-1})_{n=0}^{N-1}\big) \leq \frac{s}{p^k} + p^2s^2N^{-1}\big(2p^{k/2}+1\big)k^2\Big(\frac{2}{\pi}k\log p + \frac{7}{5}k - \frac{k-1}{p}\Big)^s, \qquad N=1,\dots,p^k. \tag{27}$$

Proof. Substituting $b=p$, $m_1=k$, and $w_{n,j}^{(i)} = \mathrm{Tr}\big((\alpha\overline{\gamma_{n+i}}+\beta)\omega_j\big)$ in Lemma 2.4, we obtain the assertion (27) from Lemma 2.12. Similarly, applying Lemma 2.9 instead Lemma 2.12 we get (26). □

3.2. Lower bounds.

LEMMA 3.1. *Let $(\mathbf{w}_n)_{n\geq 0}$ be a sequence defined in* (7). *Then*

$$\Big|\sum_{0\leq n<N} e\Big(\frac{1}{p}\big(w_{n,1}^{(1)}\big)\Big)\Big| \leq 4ND^*\big((\mathbf{w}_n)_{0\leq n<N}\big)\,. \tag{28}$$

Proof. We apply [Ni3; Lemma 3] with $M=p$, $d=s$, $\mathbf{y}_n = \big(w_{n,1}^{(1)},\dots$ $\dots,w_{n,1}^{(s)}\big)$, and $\mathbf{h}=(1,0,\dots,0)$. This yields that the left side of (28) is less than $4NE_{N,p}^*$ where is a discrete star discrepancy of the points $p^{-1}\mathbf{y}_n \in [0,1)^s$, $0\leq n\leq N-1$. Now, repeating the final proof of [EiNi; Lemma 2.3], we obtain the desired result. □

THEOREM 2. *Let $(x_n)_{n\geq 0}$ be a sequence of the explicit digital inversive pseudorandom numbers* (5), $1\leq N\leq q$. *Then there exist values of $\alpha\in F_q^*$ such that*

$$D^*\big((x_n,\dots,x_{n+s-1})_{n=0}^{N-1}\big) \geq \frac{1}{4\sqrt{N}}\sqrt{\frac{q-N}{q-1}}\,.$$

Proof. Using (5) and Lemma 2.5, we have that

$$\sum_{\alpha\in F_q^*}\left|\sum_{n=0}^{N-1} e(x_{n,1})\right|^2 = \sum_{n,m=0}^{N-1}\sum_{\alpha\in F_q} e\left(\tfrac{1}{p}\operatorname{Tr}(\alpha(\overline{\gamma_n}-\overline{\gamma_m})\omega_1)\right) - N^2$$
$$= \sum_{n,m=0}^{N-1} q\delta(\overline{\gamma_n}-\overline{\gamma_m}) - N^2$$
$$= \sum_{n=m=0}^{N-1} q\delta(\overline{\gamma_n}-\overline{\gamma_m}) - N^2 = qN - N^2 .$$

This shows that there exist values $\alpha \in F_q^*$ with

$$\left|\sum_{n=0}^{N-1} e(x_{n,1})\right| \geq \sqrt{\frac{N(q-N)}{q-1}} .$$

Finally, an application of Lemma 3.1 yields the desired result. □

3.3. The choice of parameters.

For $\eta = (\eta_1,\dots,\eta_d) \neq \mathbf{0}$, $\xi_n = (\xi_{n,1},\dots,\xi_{n,d}) \in F_q^d$ $(i = 1,\dots,d,\ n = 0,1,\dots)$ define

$$B(m) = \max_{\substack{\eta\in F_q^d,\ \eta\neq \mathbf{0}\\ \eta'\in F_q}} \widetilde{B}(m,\eta,\eta') , \tag{29}$$

where

$$\widetilde{B}(m,\eta,\eta') = \#\{0 \leq n < p^m \mid \eta\cdot\xi_n = \eta'\} .$$

Lemma 3.2. *Let $1 \leq T \leq p^m \leq q$, $\eta \in F_q^d$, $\eta \neq \mathbf{0}$. Then*

$$\sum_{\alpha\in F_q^*}\left|\sum_{n=0}^{T-1}\chi(\alpha(\eta\cdot\xi_n))e\left(\frac{nh}{T}\right)\right|^2 \leq TqB(m) . \tag{30}$$

Proof. Changing the order of the summation and bearing in mind Lemma 2.5, we obtain that the left side of (30) is less than

$$\sum_{n_1,n_2=0}^{T-1}\left|\sum_{\alpha\in F_q}\chi(\alpha(\eta\cdot\xi_{n_1}-\eta\cdot\xi_{n_2}))e\left(\frac{h(n_1-n_2)}{T}\right)\right| = \sum_{n_1,n_2=0}^{T-1} q\delta(\eta\cdot\xi_{n_1}-\eta\cdot\xi_{n_2})$$
$$\leq q\sum_{n_2=0}^{T-1}\widetilde{B}(m,\eta,\eta\cdot\xi_{n_2}) .$$

□

In the following we use the abbreviation (see (7) and Corollary 2.1):

$$\widetilde{D}^{(s)}_{\alpha,m}(T) = \widetilde{D}_{T,m}(\mathbf{w}_n(\alpha)) \qquad \text{with} \quad \mathbf{w}_n(\alpha) = \left(w_n^{(1)}(\alpha), \dots, w_n^{(s)}(\alpha)\right),$$

$$w_n^{(i)}(\alpha) = \sum_{j=1}^{k} w_{n,j}^{(i)} p^{-j} \qquad \text{and} \qquad w_{n,j}^{(i)} = \mathrm{Tr}(\alpha \xi_{n,i} \omega_j), \tag{31}$$

$$1 \le i \le s, \quad 1 \le j \le k, \quad n = 0, 1, \dots .$$

LEMMA 3.3. *Let $1 \le T \le p^m \le q$. Then*

$$\frac{1}{q-1} \sum_{\alpha \in F_q^*} \widetilde{D}^{(s)}_{\alpha,m}(T) < \left(\frac{qB(m)}{(q-1)T}\right)^{1/2} \left(\frac{2}{\pi} m \log p + \frac{7}{5} m - \frac{m-1}{p}\right)^s \left(\frac{2}{\pi} \log T + \frac{7}{5}\right).$$

P r o o f . Applying the Cauchy-Schwarz inequality we find from Corollary 2.1, (8) and (31) that

$$\frac{1}{q-1} \sum_{\alpha \in F_q^*} \widetilde{D}^{(s)}_{\alpha,m}(T)$$

$$\le \frac{1}{T} \sum_{\substack{H \in C(p)^{s \times m} \\ H \ne \mathbf{0}}} \sum_{h \in C(T)} \frac{W_{p,m}(H)}{r(h,T)} \left(\frac{1}{q-1} \sum_{\alpha \in F_q^*} \left| \sum_{n=0}^{T-1} \chi\left(\alpha \sum_{i=1}^{s} \sum_{j=1}^{k} h_{ij} \xi_{n,i} \omega_j\right) e\left(\frac{hn}{T}\right) \right|^2 \right)^{1/2}.$$

Put $\sum_{j=1}^{k} h_{ij} \omega_j = \eta_i$, $i = 1, \dots, s$. Since $(\omega_1, \dots, \omega_k)$ is the basis of F_q over F_p, and $H \ne \mathbf{0}$, it follows that $(\eta_1, \dots, \eta_s) \ne \mathbf{0}$. From Lemma 3.2 and (29) we have

$$\frac{1}{(q-1)} \sum_{\alpha \in F_q^*} \widetilde{D}^{(s)}_{\alpha,m}(T) < \frac{1}{T} \sum_{\substack{H \in C(p)^{s \times m} \\ H \ne \mathbf{0}}} \sum_{h \in C(T)} \frac{W_{p,m}(H)}{r(h,T)} \left(\frac{TqB(m)}{q-1}\right)^{1/2}.$$

Now from Lemma 2.2 and Lemma 2.4 we deduce the desired result. □

LEMMA 3.4. *With the notation defined above we have:*

$$\frac{1}{(q-1)} \sum_{\alpha \in F_q^*} \sum_{1 \le m \le k} \widetilde{D}^{(s)}_{\alpha,m}(p^m) \frac{\sqrt{p^m / 2B(m)}}{(m+3) \log^{3/2}(m+3)} \times$$

$$\times \left(\frac{2}{\pi} m \log p + \frac{7}{5} m - \frac{m-1}{p}\right)^{-s} \left(\frac{2}{\pi} m \log p + \frac{7}{5}\right)^{-1} < 2.$$

P r o o f . Bearing in mind that

$$\sum_{j=1}^{\infty} \frac{1}{(j+3) \log^{3/2}(j+3)} < \int_3^{\infty} \frac{\mathrm{d}x}{x \log^{3/2} x} = -2 \log^{-1/2} x \Big|_3^{\infty} < 2,$$

we get the desired result from Lemma 3.3. □

Now we obtain the following discrepancy estimate for the distribution of the sequence $\mathbf{w}_n(\alpha) \in [0,1)^s$, $n = 0, 1, \dots$ (31):

THEOREM 3. *Let $0 < \varepsilon \le 1$. Then there exist more than $(1-\varepsilon)(q-1)$ values of $\alpha \in F_q^*$ such that*

$$D^*\big((\mathbf{w}_n(\alpha))_{n=0}^{N-1}\big) \le \frac{2sp}{N} + \frac{1}{\varepsilon}\sqrt{\frac{8pB(m)}{N}}\Big(\frac{2}{\pi}m\log p + \frac{7}{5}m - \frac{m-1}{p}\Big)^s \times \\ \times \Big(\frac{2}{\pi}m\log p + \frac{7}{5}\Big)(m+3)\log^{3/2}(m+3), \quad (32) \\ N = 1, 2, \dots, p^k,$$

with $m = \lceil \log_p N \rceil$, where $\lceil x \rceil = [x]$ for integer x; otherwise $\lceil x \rceil = [x+1]$.

Proof. It follows from Lemma 3.4 that there exist more $(1-\varepsilon)(q-1)$ values of $\alpha \in F_q^*$ with

$$\sum_{1 \le m \le k} \widetilde{D}^{(s)}_{\alpha,m}(p^m)\frac{\sqrt{p^m/2B(m)}}{(m+3)\log^{3/2}(m+3)}\Big(\frac{2}{\pi}m\log p + \frac{7}{5}m - \frac{m-1}{p}\Big)^{-s} \times \\ \times \Big(\frac{2}{\pi}m\log p + \frac{7}{5}\Big)^{-1} < \frac{2}{\varepsilon}.$$

Hence there exist more than $(1-\varepsilon)(q-1)$ values of $\alpha \in F_q^*$ such that

$$\widetilde{D}^{(s)}_{\alpha,m}(p^m) \le \frac{1}{\varepsilon}\sqrt{\frac{8B(m)}{p^m}}\Big(\frac{2}{\pi}m\log p + \frac{7}{5}m - \frac{m-1}{p}\Big)^s\Big(\frac{2}{\pi}m\log p + \frac{7}{5}\Big) \times \\ \times (m+3)\log^{3/2}(m+3), \qquad m = 1, \dots, k.$$

For $N = 1$ the inequality (32) is trivial. Now let $N \in (p^{m-1}, p^m]$ for any $m \in [1, k]$. Applying Corollary 2.1 with $T = p^m$ and $b = p$ we obtain the assertion of Theorem 3. □

Let $\mathbf{w}_n(\alpha) = \mathbf{x}_n(\alpha) = (x_n, \dots, x_{n+s-1}) \in [0,1)^s$, where $(x_n)_{n\ge 0}$ is the sequence of *explicit digital inversive pseudorandom numbers* (see (5) and (31)). Using (21), (29) and Lemma 2.10 we have that $B(m) \le 2s^2pm$, $m = 1, 2, \dots$. This yields:

COROLLARY 3.1. *For any parameters $\beta, \gamma_0 \in F_q$ and any dimension $s \ge 1$ there exist parameters $\alpha \in F_q^*$ such that*

$$D^*\big((\mathbf{x}_n(\alpha))_{n=0}^{N-1}\big) = O\big(N^{-1/2}\log^{s+2.5} N \log^{3/2}\log N\big), \qquad N = 1, 2, \dots, p^k.$$

Let $\mathbf{w}_n(\alpha) = \mathbf{y}_n(\alpha) = (y_n, \dots, y_{n+s-1}) \in [0,1)^s$, where $(y_n)_{n\ge 0}$ (1)–(3) is the sequence of *digital inversive pseudorandom numbers* with period length equal to q ([EiNi]). According to [Em; Lemma 4], $B(m) \le 2s$. This yields:

COROLLARY 3.2. *For any parameters $\beta, \kappa_0 \in F_q$ and any dimension $s \ge 1$ there exist parameters $\alpha \in F_q^*$ such that*

$$D^*\big((\mathbf{y}_n(\alpha))_{n=0}^{N-1}\big) = O\big(N^{-1/2}\log^{s+2} N \log^{3/2}\log N\big), \qquad N = 1, 2, \dots, p^k.$$

Acknowledgment

I am very grateful to the referee for many corrections and suggestions which improved this paper.

REFERENCES

[DrTi] DRMOTA, M.—TICHY, R. F.: *Sequences, Discrepancies and Applications.* Lecture Notes in Math. 1651, Springer-Verlag, New York, 1997.

[Ei] EICHENAUER-HERRMANN, J.: *Pseudorandom number generation by nonlinear methods*, Internat. Statist. Rev. **63** (1995), 247–255.

[EiNi] EICHENAUER-HERRMANN, J.—NIEDERREITER, H.: *Digital inversive pseudo-random numbers*, ACM Trans. Model. Comput. Simul. **4** (1994), 339–349.

[Em] EMMERICH, F.: *Statistical independence properties of inversive pseudorandom vectors over parts of the period*, ACM Trans. Model. Comput. Simul. **8** (1998), 140–152.

[HeLa] HELLEKALEK, P.—LARCHER, G.: *Random and Quasi-Random Point Sets.* Lectures Notes in Statist. 138, Springer-Verlag, New York, 1998.

[Ko] KOROBOV, N. M.: *Exponential Sums and Their Applications*, Kluwer Academic Publishers, Dordrecht, 1992.

[LEq] L'ECUYER, P.: *Uniform number generation*, Ann. Oper. Res. **53** (1994), 77–120.

[Le] LEVIN, M. B.: *On the choice of parameters in generators of pseudorandom numbers*, Sov. Math. Dokl **40** (1989), 101–105.

[LiNi] LIDL, R.—NIEDERREITER, H.: *Finite Fields*, Addison-Wesley, Reading, Mass., 1983.

[Mo] MORENO, C. J.—MORENO, O.: *Exponential sums and Goppa codes. I*, Proc. Amer. Math. Soc. **111** (1991), 523–531.

[Ni1] NIEDERREITER, H.: *Pseudo-random numbers and optimal coefficients*, Adv. Math. **26** (1977), 99–181.

[Ni2] NIEDERREITER, H.: *Random Number Generation and Quasi-Monte Carlo Methods.* CBMS-NSF Regional Conf. Ser. in Appl. Math. 63, SIAM, Philadelphia, PA, 1992.

[Ni3] NIEDERREITER, H.: *Pseudorandom vector generation by the inversive method*, ACM Trans. Model Comput. Simul. **4** (1994), 191–212.

[Ni4] NIEDERREITER, H.: *On a new class of pseudorandom numbers for simulation methods*, J. Comput. Appl. Math. **56** (1994), 159–167.

[NHLZ] NIEDERREITER, H.—HELLEKALEK, P.—LARCHER, G.—ZINTERHOF, P.: *Monte Carlo and Quasi-Monte Carlo Methods 1996.* Lectures Notes in Statist. 127, Springer-Verlag, New York, 1997.

[Te] TEZUKA, S.: *Uniform Random Numbers. Theory and Practice*, Kluwer Academic Publishers, Dordrecht, 1995.

Received April 19, 1999

Department of Mathematics
and Computer Science
Bar-Ilan University
Ramat-Gan, 52900
ISRAEL
E-mail: mlevin@macs.biu.ac.il