Uniform Distribution Theory **8** (2013), no.1, 121–133

uniform distribution theory

ON THE STATISTICAL INDEPENDENCE OF SHIFT-REGISTER PSEUDORANDOM MULTISEQUENCE OVER PART OF THE PERIOD

Mordechay B. Levin and Irina L. Volinsky

ABSTRACT. In this paper we construct a pseudorandom multisequence $(x_{(n_1,\dots,n_r)})$ based on kth-order linear recurrences modulo p, such that the discrepancy of the s-dimensional multisequence $(x_{(n_1+i_1,\dots,n_r+i_r)})_{1\le i_j\le s_j,1\le j\le r}$ $1\le n_j\le N_j, 1\le j\le r$ is equal to $O((N_1\cdots N_r)^{-1/2}\ln^{s+3r}(N_1\cdots N_r))$, where $s=s_1\cdots s_r$, for all $N_1,\dots,N_r$ with $1<N_1\cdots N_r\le p^k$.

Communicated by Sergei Konyagin

Dedicated to the memory of Professor N.M. Korobov

1. Introduction

Equidistribution and statistical independence properties of uniform pseudorandom numbers can be analyzed based on the discrepancy of certain point sets in $[0,1)^s$:

Let $\mathbf{x}_n=(x_{n,1},\dots,x_{n,s}),\quad n=0,\dots,N-1$, be a sequence of points in an s-dimensional unit cube $[0,1)^s$; $v=[0,\gamma_1)\times\ldots\times[0,\gamma_s)$ a box in $[0,1)^s$. The quantity:

$$D^*((\mathbf{x}_n)_{n=0}^{N-1})=\sup_{0<\gamma_1,\dots,\gamma_s\le 1}\left|\#\left\{n\in[0,N-1]\;\middle|\;\mathbf{x}_n\in v\right\}/N-\gamma_1\dots\gamma_s\right| \quad (1)$$

is called the *star discrepancy* of $(\mathbf{x}_n)_{n=0}^{N-1}$.

Let us consider pseudorandom numbers (abreviated PRN) obtained by means of the *shift-register* method:

2010 Mathematics Subject Classification: 11k45.
Keywords: pseudorandom sequence.

Let p be a prime, let $k \geq 2$ be an integer, and generate a kth-order linear recurring sequence $y_0, y_1, ... \in \{0, 1, ..., p-1\}$ by

$$y_{n+k} \equiv a_{k-1}y_{n+k-1} + ... + a_0 y_n \mod p, \qquad n = 0, 1, ..., \tag{2}$$

where $y_0, ..., y_{k-1}$ are initial values that are not all zero. The integer coefficients $a_0, ..., a_{k-1}$ in (2) are chosen in such a way that, if they are viewed as elements of the finite field F_p, then the characteristic polynomial

$$f(x) = x^k - a_{k-1}x^{k-1} - ... - a_0 \in F_p[x]$$

of the recursion (2) is a primitive polynomial over F_p. Note that the characteristic polynomial f has a root β in the extension field F_q of F_p, where $q = p^k$. Let $F_q^* = F_q \setminus \{0\}$ be the multiplicative group of nonzero elements of F_q and let $\hat{F}_q = \{\beta \in F_q^* \mid \beta - \text{is a primitive root}\}$. We see that $\#\hat{F}_q = \varphi(q-1)$, where φ is the Euler's function. Let Tr denote the trace function from F_q to F_p. It is known (see, e.g., [Ni, p. 212]) that there exists an $\alpha \in F_q^*$ such that

$$y_n = Tr(\alpha\beta^n) \qquad \text{for} \qquad n = 0, 1, ...$$

In the *digital multistep method*, the sequence $y_0, y_1, ...$ is transformed into a sequence $x_0, x_1, ...$ of uniform PRN in the following way

$$x_n = \sum_{j=1}^{k} y_{kn+j-1}/p^j, \qquad \text{for} \qquad n = 0, 1, \ldots.$$

In a series of papers, Niederreiter (see the review in [Ni]) proved that there exists a characteristic polynomial f such that

$$D^*((x_n, ..., x_{n+s-1})_{n=0}^{N-1}) = O(\frac{\sqrt{\tau}(\ln \tau)^{s+1}}{N}), \quad \text{for} \quad N = 1, ..., \tau,$$

where τ is the period of the sequence of pseudorandom numbers.

This estimate is interesting for $N \gg \sqrt{\tau}(\log \tau)^{s+1}$. In [Le1],[Le2], Levin described a class of uniform PRN sequences $(z_n)_{n\geq 0}$, having a nontrivial discrepancy estimates also for a small part of the period:

$$D^*((z_n, ..., z_{n+s-1})_{n=0}^{N-1}) = O(N^{-1/2}\ln^{s+3} N), \quad \text{for} \quad N = 1, 2, ... \tag{3}$$

Our goal is to obtain a nontrivial discrepancy estimate similar to (3) for a small part of the period for multisequences of PRN based on kth-order linear recurrences modulo p. The method of the proof is based on Korobov's approach [Ko2] (see also [Le1], [Le2], [NiSh]). Similar results can be obtained for the pseudorandom sequences described in [Le2] and [Le3]. In this paper we will prove the following theorem :

Let $r \geq 2$, $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_r) \in F_q^r$, and $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_r) \in \hat{F}_q^r$, $\mathbf{n} = (n_1, \ldots, n_r)$ and let

$$y(\mathbf{n}, j) \equiv \sum_{l=1}^{r} Tr\left(\alpha_l \beta_l^{k(n_l + s\mu_l(\mathbf{n}))+j-1}\right) \mod p, \quad y(\mathbf{n}, j) \in [0, p-1], \tag{4}$$

where,

$$\mu_l(\mathbf{n}) \equiv \sum_{w \in [1,l)} n_w s^{w-1} + \sum_{w \in (l,r]} n_w s^{w-2} \mod s^{r-1}, \quad \mu_l(\mathbf{n}) \in [0, s^{r-1}),$$

for $l = 1, ..., r$. Let $s_1, ..., s_r, N_1, ..., N_r \geq 1$ be integers, and let $s = s_1 s_2 ... s_r$. We consider the following r-parametric sequence $(\mathbf{x}_{(n_1,\ldots,n_r)})_{0 \leq n_w < N_w,\ 1 \leq w \leq r}$ in the s-dimensional unit cube, where

$$\mathbf{x}_{(n_1,\ldots,n_r)} = \mathbf{x}_{\mathbf{n}} = (z(n_1 + i_1, ..., n_r + i_r))_{0 \leq i_w < s_w,\ 1 \leq w \leq r},$$

and

$$z(n_1, ..., n_r) = \sum_{1 \leq j \leq k} \frac{y(\mathbf{n}, j)}{p^j}. \tag{5}$$

Theorem. *Let $\epsilon \in (0, 1)$. Then there exist more than $(1-\epsilon)q^r(\varphi(q-1))^r$ values $(\boldsymbol{\alpha}, \boldsymbol{\beta}) \in F_q^r \times \hat{F}_q^r$ such that, for any $N_i \in [1, q]$, $1 \leq i \leq r$, $4 \leq N = N_1 \ldots N_r \leq q$, and any $s_1, ..., s_r \geq 1$, the bound*

$$D^*((\mathbf{x}_{\mathbf{n}})_{0 \leq n_w < N_w,\ 1 \leq w \leq r}) \leq spN^{-1} + \epsilon^{-1} c N^{-1/2} \ln^{s+2.5r} N \ln^{2.5r} \ln N$$

holds, where $s = s_1 s_2 \cdots s_r$ and the constant c depends only on $s_1, ..., s_r$.

2. Auxiliary results

For the integer $b \geq 2$, let denote

$$\Delta^*(b, m) = \{\mathbf{H} = (H_1, ..., H_s) \in \mathbb{Z}^s \mid 0 \leq h_i < b^m \ \forall i\} \setminus \{\mathbf{0}\},$$

where $H_i = \sum_{0 \leq j \leq m-1} h_{ij} b^j$, and $\mathbb{Z}$ is the set of integers. Let

$$\varrho^*_{Walsh}(b, \mathbf{H}) = \prod_{i=1}^{s} \varrho^*_{Walsh}(b, H_i),$$

where

$$\varrho^*_{Walsh}(b, H_i) = \begin{cases} 1, & \text{if} \quad H_i = 0, \\ \frac{2}{b^{g+1} \sin(\pi h_{ig}/b)}, & \text{if} \quad b^g \leq H_i < b^{g+1},\ g \geq 0. \end{cases}$$

Consider point sets for which all coordinates of all points have a finite digit expansion in a fixed base $b \geq 2$. Let

$$\mathbf{w}_n = (w_n^{(1)}, \dots, w_n^{(s)}) \in [0,1)^s, \quad n = 0, 1, \dots, N-1, \tag{6}$$

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

$$w_n^{(i)} = \sum_{j=1}^{m} w_{nj}^{(i)} b^{-j}, \quad 0 \leq n \leq N-1, \ \ 1 \leq i \leq s,$$

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

Theorem A. [He, Theorem 1, and Ni, Lemma 4.32, p.68] *If P is the point set (6), and $m \geq [\log_b N]$ then*

$$D^*(P) \leq \frac{sb}{N} + \sum_{\mathbf{H} \in \Delta^*(b,m)} \varrho^*_{Walsh}(b, \mathbf{H}) \left| \frac{1}{N} \sum_{n=0}^{N-1} e\left(\frac{1}{b} \sum_{i=1}^{s} \sum_{j=1}^{m} h_{ij} w_{nj}^{(i)} \right) \right|,$$

where $e(x) = e^{2\pi\sqrt{-1}x}$.

Lemma 1. [He, Corollary 4, and Ni, Lemma 5, p.18] *Let $s \geq 1$ and $m \geq 1$ be integers. Then*

$$\sum_{\mathbf{H} \in \Delta^*(b,m)} \varrho^*_{Walsh}(b, \mathbf{H}) < (1.22 m \ln b + 1)^s.$$

Lemma 2. (see e.g., [KoSh, p.9, p.13, ref. 3.3]) *Let $\beta \in F_q$,*

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

Then

$$\delta(\beta) = \frac{1}{q} \sum_{\alpha \in F_q} e\left(\frac{Tr(\alpha\beta)}{p} \right).$$

For proof of the following well known lemma see, e.g., [Ko, p.13], or [LeVo, Lemma 7, p.156].

Lemma 3. *Let $N \in [0, T-1], \quad T \in [1, q]$ and x_n be a real ($0 \leq n \leq T-1$). Then*

$$\left| \sum_{n=0}^{N-1} e(x_n) \right| \leq \sum_{m=-T/2}^{T/2} \frac{1}{\bar{m}} \left| \sum_{n=1}^{T} e\left(x_n + \frac{nm}{T} \right) \right|,$$

where $\bar{m} = \max(1, |m|)$. It is easy to see that

$$\sum_{m=-T/2}^{T/2} \frac{1}{\bar{m}} \leq 3 + 2 \ln T. \tag{7}$$

Repeating Lemma 3 r times, we obtain

Lemma 4. *Let* $N_i \in [0, T_i - 1], \quad 1 \le i \le r$, *where* $T_i \in [1, q], \quad 1 \le i \le r$, *and* $\bar{\mathbf{n}} = (n_1, \ldots, n_r)$. *Then*

$$\left| \sum_{n_1=0}^{N_1-1} \cdots \sum_{n_r=0}^{N_r-1} e(x_{\mathbf{n}}) \right| \le \sum_{m_1=-T_1/2}^{T_1/2} \cdots \sum_{m_r=-T_r/2}^{T_r/2} \frac{1}{\bar{m}_1 \ldots \bar{m}_r}$$
$$\times \left| \sum_{n_1=0}^{T_1-1} \cdots \sum_{n_r=0}^{T_r-1} e\left(x_{\mathbf{n}} + \frac{n_1 m_1}{T_1} + \ldots + \frac{n_r m_r}{T_r} \right) \right|.$$

Lemma 5. *Let* $r \ge 2$, $s_1, \ldots, s_r \ge 1$ *be integers,* $s = s_1 \cdots s_r$,

$$\mu_l(\mathbf{n} + \mathbf{i}) \equiv \sum_{w \in [1,l)} (n_w + i_w) s^{w-1} + \sum_{w \in (l,r]} (n_w + i_w) s^{w-2} \mod s^{r-1}, \tag{8}$$

and $\mu_l(\mathbf{n} + \mathbf{i}) \in [0, s^{r-1})$. *Then for* $l \in [1, r]$,

$$\# \left\{ k(i_l + s\mu_l(\mathbf{n} + \mathbf{i})) + j \;\middle|\; 0 \le j < k,\ 0 \le i_\nu < s_\nu,\ \nu = 1, \ldots, r \right\} = k s_1 \ldots s_r.$$

Proof. It is enough to prove that there are no two vectors $(i_1, \ldots, i_r, j) \ne (i_1^{'}, \ldots, i_r^{'}, j^{'})$ with

$$k(i_l + s\mu_l(\mathbf{n} + \mathbf{i})) + j = k(i_l^{'} + s\mu_l(\mathbf{n} + \mathbf{i}^{'})) + j^{'}. \tag{9}$$

Suppose that (9) is true. We see $j \equiv j^{'} \mod k$. Hence $j = j^{'}$. By (9), we see

$$i_l + s\mu_l(\mathbf{n} + \mathbf{i})) = i_l^{'} + s\mu_l(\mathbf{n} + \mathbf{i}^{'}) \quad \text{and} \quad i_l \equiv i_l^{'} \mod s. \tag{10}$$

Therefore $i_l = i_l^{'}$. From (10), we have that $\mu_l(\mathbf{n} + \mathbf{i}) = \mu_l(\mathbf{n} + \mathbf{i}^{'})$. By (8), we get

$$\sum_{w \in [1,l)} (n_w + i_w) s^{w-1} + \sum_{w \in (l,r]} (n_w + i_w) s^{w-2}$$
$$\equiv \sum_{w \in [1,l)} (n_w + i_w^{'}) s^{w-1} + \sum_{w \in (l,r]} (n_w + i_w^{'}) s^{w-2} \mod s^{r-1}.$$

Hence

$$\sum_{w \in [1,l)} (i_w - i_w^{'}) s^{w-1} + \sum_{w \in (l,r]} (i_w - i_w^{'}) s^{w-2} \equiv 0 \mod s^{r-1}.$$

Thus

$$\sum_{w \in [2,r]} (i_w - i_w^{'}) s^{w-2} \equiv 0 \mod s^{r-1}, \quad \text{for} \quad l = 1,$$

and

$$(i_1 - i_1^{'}) + \ldots + (i_{l-1} - i_{l-1}^{'}) s^{l-1}$$
$$+ (i_{l+1} - i_{l+1}^{'}) s^{l} + \ldots + (i_{r-1} - i_{r-1}^{'}) s^{r-2} \equiv 0 \mod s^{r-1} \quad \text{for } l \ge 2.$$

Bearing in mind that $i_l = i_l^{'}$, we obtain

$$i_w - i_w^{'} \equiv 0 \mod s, \quad \text{and} \quad i_w = i_w^{'} \quad \text{for} \quad w = 1, ..., r.$$

Hence Lemma 5 is proved. □

Lemma 6. Let $q = p^k$, $T \in [4, 4q]$. Then there exists a constant $c_1 > 0$ such that

$$\frac{kT}{\varphi(q-1)} \le c_1 \ln T \ln\ln T.$$

Proof. By [Sa, p.15, ref. 3a; p.9, ref. 2],

$$\frac{n}{\varphi(n)} < e^{0.58} \ln\ln n + \frac{2.6}{\ln\ln n}, \quad \text{for} \quad \text{n} \ge 30.$$

Therefore

$$\frac{k}{\varphi(q-1)} = O\Big(\frac{\ln q \ln\ln(q-1)}{q-1}\Big). \tag{11}$$

Let $f(x) = x/(\ln x \ln\ln x)$. It is easy to see that $f^{'}(x) > 0$ for $x > 30$. Hence

$$\frac{T}{\ln T \ln\ln T} \le \frac{4q}{\ln 4q \ln\ln 4q} \quad \text{for} \quad T > 30.$$

Using (11), we have

$$\frac{kT}{\varphi(q-1)\ln T \ln\ln T} = O\Big(\frac{4q}{\ln 4q \ln\ln 4q} \cdot \frac{\ln q \ln\ln(q-1)}{q-1}\Big) = O(1).$$

Thus Lemma 6 is proved. □

3. Proof of the Theorem

By (1), we obtain that the Theorem is true for $N_1 \cdots N_r \le p$ with $c = 1$. Now let $N_1 \cdots N_r > p$, $s = s_1 \cdots s_r$, $T_i \in [N_i, q]$ be integer $(1 \le i \le r)$, and $m = \min(k, [\log_p T_1 \dots T_r])$. We see that

$$1.22m \ln p + 1 \le m5 \ln p \le 5 \ln(T_1 \cdots T_r), \tag{12}$$

and $m \ge [\log_p N_1 \dots N_r]$. From (4), (5) and Theorem A, we get :

$$N_1 \cdots N_r D^*((\mathbf{x_n})_{1 \le n_w < N_w,\, 1 \le w \le r}) \le sp + \sum_{\mathbf{H} \in \Delta^*(p,m)} \varrho^*_{Walsh}(p, \mathbf{H}) \, |S(\mathbf{H})| \,,$$

where

$$S(\mathbf{H}) = \sum_{n_1=0}^{N_1-1} \cdots \sum_{n_r=0}^{N_r-1} e\Big(\frac{1}{p} \sum_{l=1}^{r} \sum_{i_1=0}^{s_1-1} \cdots \sum_{i_r=0}^{s_r-1} \sum_{j=1}^{m} h_{i_1,\dots,i_r,j}$$

$$\times Tr\big(\alpha_l\beta_l^{k(n_l+i_l+s\mu_l(\mathbf{n}+\mathbf{i}))+j-1}\big)\Big).$$

Using Lemma 4, we get:

$$|S(\mathbf{H})| \le \sum_{m_1=-T_1/2}^{T_1/2} \dots \sum_{m_r=-T_r/2}^{T_r/2} \frac{\dot{S}(\mathbf{H},T,\boldsymbol{\alpha},\boldsymbol{\beta})}{\bar{m}_1\dots\bar{m}_r},$$

where

$$\dot{S}(\mathbf{H},T,\boldsymbol{\alpha},\boldsymbol{\beta}) = \Big|\sum_{t_1=0}^{T_1-1}\dots\sum_{t_r=0}^{T_r-1} e\left(\xi(\mathbf{t},\boldsymbol{\alpha},\boldsymbol{\beta})\right)\Big|, \tag{13}$$

with

$$\xi(\mathbf{t},\boldsymbol{\alpha},\boldsymbol{\beta})$$
$$= \sum_{l=1}^{r}\Big(\frac{1}{p}\sum_{i_1=0}^{s_1-1}\dots\sum_{i_r=0}^{s_r-1}\sum_{j=1}^{m} h_{i_1,\dots,i_r,j} Tr\big(\alpha_l\beta_l^{k(t_l+i_l+s\mu_l(\mathbf{t}+\mathbf{i}))+j-1}\big) + \frac{m_l t_l}{T_l}\Big).$$

Hence,

$$N_1\dots N_r\cdot D^*\big((\mathbf{x_n})_{0\le n_w<N_w,\,1\le w\le r}\big) \le sp + T_1\dots T_r\widetilde{D}_{T_1,\dots,T_r}(\boldsymbol{\alpha},\boldsymbol{\beta}), \tag{14}$$

where,

$$T_1\dots T_r\widetilde{D}_{T_1,\dots,T_r}(\boldsymbol{\alpha},\boldsymbol{\beta})$$
$$= \sum_{\mathbf{H}\in\Delta^*(p,m)} \varrho^*_{Walsh}(p,\mathbf{H}) \sum_{m_1=-T_1/2}^{T_1/2}\dots\sum_{m_r=-T_r/2}^{T_r/2} \frac{\dot{S}(\mathbf{H},T,\boldsymbol{\alpha},\boldsymbol{\beta})}{\bar{m}_1\dots\bar{m}_r}.$$

It is easy to see that

$$\frac{1}{q^r(\varphi(q-1))^r}\sum_{\boldsymbol{\alpha}\in F_q^r}\sum_{\boldsymbol{\beta}\in\hat{F}_q^r} T_1\dots T_r\tilde{D}_{T_1,\dots,T_r}(\boldsymbol{\alpha},\boldsymbol{\beta}) \tag{15}$$

$$= \sum_{\mathbf{H}\in\Delta^*(p,m)}\sum_{m_1=-T_1/2}^{T_1/2}\dots\sum_{m_r=-T_r/2}^{T_r/2} \varrho^*_{Walsh}(p,\mathbf{H})\chi(\mathbf{T})\big(\bar{m}_1\dots\bar{m}_r\big)^{-1},$$

where

$$\chi(\mathbf{T}) = \frac{1}{q^r(\varphi(q-1))^r}\sum_{\boldsymbol{\beta}\in\hat{F}_q^r}\sum_{\boldsymbol{\alpha}\in F_q^r}\dot{S}(\mathbf{H},T,\boldsymbol{\alpha},\boldsymbol{\beta}). \tag{16}$$

Lemma 7. *Let*

$$\zeta_l = \sum_{i_1=0}^{s_1-1}\dots\sum_{i_r=0}^{s_r-1}\sum_{j=1}^{m} h_{i_1,\dots,i_r,j}\Big(\beta_l^{k(t_l^{(2)}+sv_l+i_l)+j-1} - \beta_l^{k(t_l^{(1)}+i_l+s\mu_l(\mathbf{t}^{(1)}+\mathbf{i}))+j-1}\Big). \tag{17}$$

Then

$$\chi^2(\mathbf{T}) \le \prod_{l=1}^{r} \sum_{t_i^{(1)} \in [0, T_i - 1]} \chi_l(\mathbf{t}^{(1)}), \tag{18}$$

with

$$\chi_l(\mathbf{t}^{(1)}) = \frac{1}{\varphi(q-1)} \sum_{\beta_l \in \hat{F}_q} \sum_{t_l^{(2)} \in [0, T_l - 1]} \sum_{v_l \in [0, s^{r-1})} \delta(\zeta_l). \tag{19}$$

Proof. Using the Cauchy - Shwartz inequality, (16) and (13) we get:

$$\chi^2(\mathbf{T}) \le \frac{1}{q^r \cdot (\varphi(q-1))^r} \sum_{\boldsymbol{\beta} \in \hat{F}_q^r} \sum_{\boldsymbol{\alpha} \in F_q^r} \Big| \sum_{t_1=0}^{T_1-1} \dots \sum_{t_r=0}^{T_r-1} e\left(\xi(\mathbf{t}, \boldsymbol{\alpha}, \boldsymbol{\beta})\right) \Big|^2.$$

By (13), we have

$$\chi^2(\mathbf{T}) = \frac{1}{q^r \cdot (\varphi(q-1))^r} \sum_{\boldsymbol{\beta} \in \hat{F}_q^r} \sum_{\boldsymbol{\alpha} \in F_q^r} \sum_{t_1^{(1)}, t_1^{(2)} = 0}^{T_1 - 1} \dots \sum_{t_r^{(1)}, t_r^{(2)} = 0}^{T_r - 1} 1$$

$$\times e\Big(\frac{1}{p} \sum_{i_1=0}^{s_1-1} \dots \sum_{i_r=0}^{s_r-1} \sum_{j=1}^{m} \sum_{l=1}^{r} h_{i_1,\dots,i_r,j} \Big(Tr\big(\alpha_l \beta_l^{k(t_l^{(2)} + i_l + s\mu_l(\mathbf{t}^{(2)} + \mathbf{i})) + j - 1}\big)$$

$$- Tr\big(\alpha_l \beta_l^{k(t_l^{(1)} + i_l + s\mu_l(\mathbf{t}^{(1)} + \mathbf{i})) + j - 1}\big)\Big) + \frac{m_1(t_1^{(2)} - t_1^{(1)})}{T_1} + \dots + \frac{m_r(t_r^{(2)} - t_r^{(1)})}{T_r}\Big).$$

Using Lemma 2, we get

$$\chi^2(\mathbf{T}) \le \frac{1}{(\varphi(q-1))^r} \sum_{\boldsymbol{\beta} \in \hat{F}_q^r} \sum_{t_1^{(1)}, t_1^{(2)} = 0}^{T_1 - 1} \dots \sum_{t_r^{(1)}, t_r^{(2)} = 0}^{T_r - 1} \prod_{l=1}^{r} \delta\Big(\sum_{i_1=0}^{s_1-1} \dots \sum_{i_r=0}^{s_r-1} 1$$

$$\times \sum_{j=1}^{m} h_{i_1,\dots,i_r,j} \big(\beta_l^{k(t_l^{(2)} + i_l + s\mu_l(\mathbf{t}^{(2)} + \mathbf{i})) + j - 1} - \beta_l^{k(t_l^{(1)} + i_l + s\mu_l(\mathbf{t}^{(1)} + \mathbf{i})) + j - 1}\big)\Big)$$

$$\times e\Big(\frac{m_1(t_1^{(2)} - t_1^{(1)})}{T_1} + \dots + \frac{m_r(t_r^{(2)} - t_r^{(1)})}{T_r}\Big).$$

It is easy to see that

$$\chi^2(\mathbf{T}) \le \frac{1}{(\varphi(q-1))^r} \sum_{\substack{\beta_i \in \hat{F}_q \\ i=1,\dots,r}} \sum_{\substack{t_i^{(1)} \in [0, T_i - 1] \\ i=1,\dots,r}} \sum_{\substack{t_i^{(2)} \in [0, T_i - 1] \\ i=1,\dots,r}} \prod_{l=1}^{r} \delta\Big(\sum_{i_1=0}^{s_1-1} \dots \sum_{i_r=0}^{s_r-1} 1$$

$$\times \sum_{j=1}^{m} h_{i_1,\dots,i_r,j} \big(\beta_l^{k(t_l^{(2)} + s\mu_l(\mathbf{t}^{(2)} + \mathbf{i})) + j - 1} - \beta_l^{k(t_l^{(1)} + i_l + s\mu_l(\mathbf{t}^{(1)} + \mathbf{i})) + j - 1}\big)\Big).$$

We take a new variable v_l instead of $\mu_l(\mathbf{t}^{(2)}+\mathbf{i})$, $l=1,\dots,r$. Enlarging the domain of the summation, we obtain from (17) that:

$$\chi^2(\mathbf{T}) \le \frac{1}{(\varphi(q-1))^r} \sum_{\substack{\beta_i\in\hat{F}_q\\ i=1,\dots,r}} \sum_{\substack{t_i^{(1)}\in[0,T_i-1]\\ i=1,\dots,r}} \sum_{\substack{t_i^{(2)}\in[0,T_i-1]\\ i=1,\dots,r}} \prod_{l=1}^{r} \sum_{v_l\in[0,s^{r-1})} \delta(\zeta_l).$$

By (19), we get (18). Hence Lemma 7 is proved. □

Lemma 8. *With notations as above*

$$\chi(\mathbf{T}) \le \prod_{l=1}^{r} \left(T_l 3 s^r c_1 \ln T_l \ln\ln T_l\right)^{1/2}.$$

Proof. Consider the equation $\zeta_l = 0$. By (17), we have:

$$\zeta_l = \beta_l^{kt_l^{(2)}}\gamma_2 - \beta_l^{kt_l^{(1)}}\gamma_1, \quad \text{where} \quad \gamma_2 = \sum_{i_1=0}^{s_1-1}\dots\sum_{i_r=0}^{s_r-1}\sum_{j=1}^{m} h_{i_1,\dots,i_r,j}\beta_l^{k(sv_l+i_l)+j-1}, \tag{20}$$

and

$$\gamma_1 = \gamma_1(\beta_l) = \sum_{i_1=0}^{s_1-1}\dots\sum_{i_r=0}^{s_r-1}\sum_{j=1}^{m} h_{i_1,\dots,i_r,j}\beta_l^{k(i_l+s\mu_l(\mathbf{t}^{(1)}+\mathbf{i}))+j-1}. \tag{21}$$

It is easy to see, that

$$\delta(\zeta_l) \le \delta(\zeta_l)(1-\delta(\gamma_1)) + \delta(\gamma_1).$$

We derive from (19) and (20) that

$$\chi_l(\mathbf{t}^{(1)}) = \frac{1}{\varphi(q-1)} \sum_{\beta_l\in\hat{F}_q} \sum_{t_l^{(2)}\in[0,T_l-1]} \sum_{v_l\in[0,s^{r-1})} 1$$

$$\times\big(\delta(\beta_l^{k(t_l^{(2)}-t_l^{(1)})}\gamma_2-\gamma_1)(1-\delta(\gamma_1))+\delta(\gamma_1)\big).$$

Hence

$$\chi_l(\mathbf{t}^{(1)}) \le \dot{\chi}_l(\mathbf{t}^{(1)}) + \ddot{\chi}_l(\mathbf{t}^{(1)}), \tag{22}$$

where

$$\dot{\chi}_l(\mathbf{t}^{(1)}) = \frac{1}{\varphi(q-1)} \sum_{\beta_l\in\hat{F}_q} \sum_{t_l^{(2)}\in[0,T_l-1]} \sum_{v_l\in[0,s^{r-1})} \delta\Big(\beta_l^{k(t_l^{(2)}-t_l^{(1)})}\gamma_2-\gamma_1\Big)$$

$$\times\,(1-\delta(\gamma_1))\,, \quad \text{and} \quad \ddot{\chi}_l(\mathbf{t}^{(1)}) = \mathrm{T_l}\frac{1}{\varphi(\mathrm{q}-1)} \sum_{\beta_1\in\hat{\mathrm{F}}_\mathrm{q}} \sum_{\mathrm{v_1}\in[0,\mathrm{s}^{\mathrm{r}-1})} \delta(\gamma_1). \tag{23}$$

Consider $\dot{\chi}_l(\mathbf{t}^{(1)})$. We see that if $\gamma_1=0$, then $\dot{\chi}_l(\mathbf{t}^{(1)})=0$. By (23) if $\gamma_1\neq 0$ and $\gamma_2=0$, then also $\dot{\chi}_l(\mathbf{t}^{(1)})=0$. Now let $\gamma_2\neq 0$ and $\gamma_1\neq 0$. We fix β_l, v_l and $\mathbf{t}^{(1)}$.

There exists an integer a, such that $\beta_l^a = \gamma_1/\gamma_2$. Let $\zeta_l = 0$. Bearing in mind that β_l is primitive root, we get $k(t_l^{(2)} - t_l^{(1)}) \equiv a \mod \varphi(q-1)$. We see that

$$\# \left\{ 0 \le t_l^{(2)} < T_l \;\middle|\; k(t_l^{(2)} - t_l^{(1)}) \equiv a \mod \varphi(q-1) \right\} \le 1 + [T_l/(\varphi(q-1)/k_1)] \le 1 + kT_l/\varphi(q-1),$$

where $k_1 = \gcd(\mathrm{k}, \varphi(\mathrm{q}-1))$. By (23) and Lemma 6, we get

$$\dot{\chi}_l(\mathbf{t}^{(1)}) \le s^{r-1}(1 + kT_l/\varphi(q-1)) \le s^{r-1}(1 + c_1 \ln T_l \ln\ln T_l). \tag{24}$$

Now consider $\ddot{\chi}_l(\mathbf{t}^{(1)})$. Let $\rho = \sum_{\beta_l \in \hat{F}_q} \delta(\gamma_1(\beta_l))$. By (21), ρ is equal to the number of solution of the following polynomial equation:

$$\sum_{i_1=0}^{s_1-1} \cdots \sum_{i_r=0}^{s_r-1} \sum_{j=1}^{m} h_{i_1,\ldots,i_r,j} \beta_l^{k(i_l + s\mu_l(\mathbf{t}^{(1)}+\mathbf{i}))+j-1} = 0.$$

Bearing in mind Lemma 5 and that $\max_{i_1,\ldots,i_r,j} |h_{i_1,\ldots,i_r,j}| > 0$, $m \le k$, we get: $\rho \le ks$. Using (23), we have

$$\ddot{\chi}_l(\mathbf{t}^{(1)}) \le ks^r T_l/\varphi(q-1).$$

By (22), (24) and Lemma 6 we obtain

$$\chi_l(\mathbf{t}^{(1)}) \le s^{r-1}(1 + c_1 \ln T_l \ln\ln T_l) + s^r c_1 \ln T_l \ln\ln T_l \le 3s^r c_1 \ln T_l \ln\ln T_l.$$

From (18), we have

$$\chi^2(\mathbf{T}) \le \prod_{l=1}^{r} T_l 3s^r c_1 \ln T_l \ln\ln T_l.$$

Hence Lemma 8 is proved. □

End of the proof of Theorem. Using (7), we obtain

$$\sum_{m_1=-T_1/2}^{T_1/2} \cdots \sum_{m_r=-T_r/2}^{T_r/2} \left(\bar{m}_1 \ldots \bar{m}_r\right)^{-1} \le \prod_{l=1}^{r} \left(3 + 2\ln T_l\right).$$

Applying Lemma 1 and (12), we have

$$\sum_{\mathbf{H} \in \Delta^*(p,m)} \varrho^*_{Walsh}(p, \mathbf{H}) \le \left(5 \ln(T_1 \ldots T_r)\right)^s.$$

By (15) and Lemma 8, we get

$$\sigma := \frac{1}{q^r(\varphi(q-1))^r} \sum_{\boldsymbol{\alpha} \in F_q^r} \sum_{\boldsymbol{\beta} \in \hat{F}_q^r} T_1 \ldots T_r \tilde{D}_{T_1,\ldots,T_r}(\boldsymbol{\alpha}, \boldsymbol{\beta})$$

$$\le \prod_{l=1}^{r} \Big(T_l 3 s^r c_1 \ln T_l \ln\ln T_l \Big)^{1/2}$$

$$\times \sum_{\mathbf{H}\in\Delta^*(p,m)} \sum_{m_1=-T_1/2}^{T_1/2} \dots \sum_{m_r=-T_r/2}^{T_r/2} \varrho^*_{Walsh}(p,\mathbf{H}) \big(\bar m_1 \dots \bar m_r\big)^{-1}. \tag{25}$$

Hence

$$\sigma \le (5\ln(T_1\dots T_r))^s \prod_{l=1}^{r} (2+3\ln T_l) \Big(T_l 3 s^r c_1 \ln T_l \ln\ln T_l \Big)^{1/2}. \tag{26}$$

Let $T_{j_i} = 4^{j_i},\ j_i = 1,2,...,\ i = 1,...,r$, and let

$$R(\boldsymbol{\alpha},\boldsymbol{\beta}) = \sum_{s_1,\dots,s_r\ge 1} \sum_{\substack{1\le j_1,\dots,j_r\le \log_4 q \\ \log_4 p\le j_1+\dots+j_r\le \log_4 4q}} R_1(j,T,\boldsymbol{\alpha},\boldsymbol{\beta}) \tag{27}$$

$$\times \prod_{i=1}^{r} \frac{\big(\ln(4^3 T_{j_i}) \ln^2 \ln(4^3 T_{j_i})\big)^{-1}}{(s_i+3)\ln^2(s_i+3)}$$

where

$$R_1(j,T,\boldsymbol{\alpha},\boldsymbol{\beta}) = T_{j_1}\cdots T_{j_r} \tilde D_{T_{j_1},\dots,T_{j_r}}(\boldsymbol{\alpha},\boldsymbol{\beta})$$

$$\times (5\ln\dots T_{j_r})^{-s} \prod_{l=1}^{r} (2+3\ln T_{j_l})^{-1} \Big(T_{j_l}, 3 s^r c_1 \ln T_{j_l} \ln\ln T_{j_l} \Big)^{-1/2}. \tag{28}$$

We derive from (27) and (28), that

$$T_{j_1}\dots T_{j_r} \tilde D_{T_1,\dots,T_r}(\boldsymbol{\alpha},\boldsymbol{\beta}) \tag{29}$$

$$= R_1(j,T,\boldsymbol{\alpha},\boldsymbol{\beta})(5\ln T_{j_1}\dots T_{j_r})^s \prod_{l=1}^{r} (2+3\ln T_{j_l}) \Big(T_{j_l} 3 s^r c_1 \ln T_{j_l} \ln\ln T_{j_l} \Big)^{1/2}$$

$$\le R(\boldsymbol{\alpha},\boldsymbol{\beta})(5\ln T_{j_1}\dots T_{j_r})^s$$

$$\times \prod_{l=1}^{r} \frac{\ln(4^3 T_{j_l}) \ln^2 \ln(4^3 T_{j_l})}{\big((s_i+3)\ln^2(s_i+3)\big)^{-1}} (2+3\ln T_{j_l}) \Big(T_{j_l} 3 s^r c_1 \ln T_{j_l} \ln\ln T_{j_l} \Big)^{1/2}.$$

Using (25), (26) and (28), we obtain

$$\frac{1}{q^r\,(\varphi(q-1))^r} \sum_{\boldsymbol{\alpha}\in F_q^r} \sum_{\boldsymbol{\beta}\in \hat F_q^r} R_1(j,T,\boldsymbol{\alpha},\boldsymbol{\beta}) \le 1.$$

By (27), we have

$$\frac{1}{q^r\,(\varphi(q-1))^r} \sum_{\boldsymbol{\alpha}\in F_q^r} \sum_{\boldsymbol{\beta}\in \hat F_q^r} R(\boldsymbol{\alpha},\boldsymbol{\beta})$$

$$\le \sum_{s_1,\dots,s_r\ge 1} \sum_{\substack{1\le j_1,\dots,j_r\le \log_4 q \\ \log_4 p\le j_1+\dots+j_r\le \log_4 4q}} \prod_{i=1}^{r} \frac{1}{(s_i+3)\ln^2(s_i+3)\ln(4^3T_{j_i})\ln^2\ln(4^3T_{j_i})}.$$

Bearing in mind that

$$\sum_{k\ge 1}\frac{1}{(k+3)\ln^2(k+3)} \le \int_3^\infty \frac{dx}{x\ln^2 x} = \frac{1}{\ln 3} < 1,$$

we get

$$\frac{1}{q^r\left(\varphi(q-1)\right)^r}\sum_{\boldsymbol{\alpha}\in F_q^r}\sum_{\boldsymbol{\beta}\in \hat{F}_q^r} R(\boldsymbol{\alpha},\boldsymbol{\beta})$$

$$\le \prod_{i=1}^{r}\sum_{s_i,j_i=1}^{\infty}\frac{1}{(s_i+3)\ln^2(s_i+3)(j_i+3)\ln^2(j_i+3)} \le 1. \tag{30}$$

Let

$$\Omega_\epsilon = \left\{\boldsymbol{\alpha}\in F_q^r, \boldsymbol{\beta}\in \hat{F}_q^r \;\middle|\; R(\boldsymbol{\alpha},\boldsymbol{\beta}) < \frac{1}{\epsilon}\right\}, \qquad \#\Omega_\epsilon = \gamma q^r\left(\varphi(q-1)\right)^r. \tag{31}$$

Let us prove, that

$$\gamma \ge 1-\epsilon. \tag{32}$$

We see that $q\cdot\varphi(q-1)(1-\gamma)$ is the number of $\boldsymbol{\alpha}\in F_q, \boldsymbol{\beta}\in\hat{F}_q$, such that $R(\boldsymbol{\alpha},\boldsymbol{\beta})\ge 1/\epsilon$. From (30) and (31), we obtain

$$1 \ge \frac{1}{q^r(\varphi(q-1))^r}\sum_{\boldsymbol{\alpha}\in F_q}\sum_{\boldsymbol{\beta}\in\hat{F}_q} R(\boldsymbol{\alpha},\boldsymbol{\beta}) \ge \frac{1}{q^r(\varphi(q-1))^r}\sum_{(\alpha,\beta)\in\Omega_\epsilon^c} R(\boldsymbol{\alpha},\boldsymbol{\beta})$$

$$\ge \frac{1}{q^r(\varphi(q-1))^r}\sum_{(\boldsymbol{\alpha},\boldsymbol{\beta})\in\Omega_\epsilon^c}\frac{1}{\epsilon} = \frac{1}{q^r(\varphi(q-1))^r}\frac{1}{\epsilon}\#\Omega_\epsilon^c$$

$$= \frac{1}{q^r(\varphi(q-1))^r}\frac{1}{\epsilon}(1-\gamma)q^r(\varphi(q-1))^r = \frac{1-\gamma}{\epsilon}.$$

The inequality (32) is proved.

Now, let $N_i\in[T_{j_i-1},T_{j_i})$ for some $j_i\in[1,\log_4 q]$, $i=1,...,r$, with $T_{j_i}=4^{j_i}$. From (14), (29) and (31), we have for all $(\boldsymbol{\alpha},\boldsymbol{\beta})\in\Omega_\epsilon$ that

$$N_1\dots N_r D^*\left((\mathbf{x_n})_{0\le n_w<N_w,\,1\le w\le r}\right) - sp$$

$$\le T_{j_1}\dots T_{j_r}\tilde{D}_{T_1,\dots,T_r}(\boldsymbol{\alpha},\boldsymbol{\beta}) \le \epsilon^{-1}(5\ln T_{j_1}\dots T_{j_r})^s$$

$$\times\prod_{l=1}^{r}\frac{\ln(4^3T_{j_l})\ln^2\ln(4^3T_{j_l})}{\left((s_i+3)\ln^2(s_i+3)\right)^{-1}}(2+3\ln T_{j_l})\Big(T_{j_l}3s^r c_1\ln T_{j_l}\ln\ln T_{j_l}\Big)^{1/2}.$$

Hence

$$N_1\dots N_r D^*\left((\mathbf{x_n})_{0\le n_w<N_w,\,1\le w\le r}\right) - sp$$

$$\leq \epsilon^{-1} c_2 \left(T_{j_1} \dots T_{j_r}\right)^{1/2} \ln^{s+2.5r}(T_{j_1} \cdots T_{j_r}) \ln^{2.5r} \ln(T_{j_1} \cdots T_{j_r})$$
$$\leq \epsilon^{-1} c \left(N_1 \dots N_r\right)^{1/2} \ln^{s+2.5r}(N_1 \cdots N_r) \ln^{2.5r} \ln(N_1 \cdots N_r)$$

with some $c, c_2 > 0$. By (32), the Theorem is proved. □

Acknowledgment. We are very grateful to the referee for many corrections and suggestions which improved this paper.

REFERENCES

[He] Hellekalek, P., General discrepancy estimates: the Walsh function system, Acta Arith., 67 (1994), no. 3, 209-218.

[KoSh] Konyagin, S., Shparlinski, I., Character sums with exponential functions and their applications, Cambridge, 1999.

[Ko1] Korobov, N.M., Estimates of trigonometric sums and sums of characters. (Russian) Diophantine approximations, Part 1, 42-47, Moskov. Gos. Univ., Mekh.-Mat. Fak., Moscow, 1985.

[Ko2] Korobov, N.M., Exponential Sums and their Applications, Kluwer Academic Publishers, Dordrecht, 1992.

[Le1] Levin, M.B., The choice of parameters in generators of pseudorandom numbers. Dokl. Akad. Nauk SSSR, 307 (1989), no. 3, 529-534. English translation in Soviet Math. Dokl. 40 (1990), no. 1, 101-103.

[Le2] Levin, M.B., Explicit digital inversive pseudorandom numbers, Math. Slovaca, 2000, v. 50, no. 5, p. 581-598.

[Le3] Levin, M.B., On the statistical independence of compound pseudorandom numbers over part of the period, ACM Trans. Model Comput. Simulation, 11 (2001), no. 3, p. 294-311.

[LeVo] Levin M. B., Volinsky I. L., Discrepancy estimate of normal vectors (the case of hyperbolic matrices), Uniform Distribution Theory, 5 (2010), no.2, 141-167.

[Ni] Niederreiter, H., Random Number Generation and Quasi-Monte Carlo Methods, SIAM, Philadelphia, 1992.

[NiSh] Niederreiter, H., Shparlinski, I.E., On the average distribution of inversive pseudorandom numbers, Finite Fields Appl., 8 (2002), no. 4, 491-503.

[Sa] Sándor, J., Mitrinovic, D., Crstici, B., Handbook of number theory. I. Springer, Dordrecht, 2006.

Received January 4, 2011
Accepted September 9, 2012

Department of Mathematics,
Bar-Ilan University,
Ramat-Gan, 52900 Israel
E-mail: mlevin@math.biu.ac.il
volinskaya_i@yahoo.com