ACTA ARITHMETICA
LXXXVIII.2 (1999)

On the discrepancy estimate of normal numbers

by

M. B. Levin (Tel-Aviv)

Dedicated to Professor N. M. Korobov
on the occasion of his 80th birthday

1. Introduction

1.1. A number $\alpha \in (0,1)$ is said to be *normal* to base q if in the q-ary expansion of α, $\alpha = .d_1 d_2 \ldots$ ($d_i \in \Delta = \{0,1,\ldots,q-1\}$, $i = 1,2,\ldots$), each fixed finite block of digits of length k appears with an asymptotic frequency of q^{-k} along the sequence $(d_i)_{i\ge 1}$. Normal numbers were introduced by Borel (1909).

1.1.1. Let $(x_n)_{n\ge 1}$ be an arbitrary sequence of real numbers. The quantity

$$(1)\quad D(N) = D(N,(x_n)_{n\ge1}) = \sup_{\gamma\in(0,1]} |\#\{0\le n<N \mid \{x_n\}<\gamma\}/N-\gamma|$$

is called the *discrepancy* of $(x_n)_{n=1}^N$, where $\{x\} = x - [x]$ is the fractional part of x. The sequence $\{x_n\}_{n\ge1}$ is said to be *uniformly distributed* (u.d.) in $[0,1)$ if $D(N)\to 0$.

1.1.2. It is known that a number α is normal to base q if and only if the sequence $\{\alpha q^n\}_{n\ge0}$ is u.d. (Wall, 1949). Borel proved that almost every number (in the sense of Lebesgue measure) is normal to base q. In [G], Gal and Gal proved that

$$D(N,\{\alpha q^n\}_{n\ge0}) = O((N^{-1}\log\log N)^{1/2}) \qquad \text{for a.e. } \alpha.$$

1.2. In [K1] Korobov posed the problem of finding a function ψ with maximum decay, such that

$$\exists\alpha : D(N,\{\alpha q^n\}_{n\ge0}) \le \psi(N), \qquad N = 1,2,\ldots$$

1991 *Mathematics Subject Classification*: 11K16, 11K38.

Work supported in part by the Israel Science Foundation Grant No. 0366-172.

He showed that $\psi(N) = O(N^{-1/2})$ (see [K1]). The lower bound of the discrepancy for the Champernowne and Davenport–Erdős normal numbers was found by Schiffer [S]:

$$D(N, \{\alpha q^n\}_{n\ge 1}) \ge K/\log N \quad \text{with } K>0,\ N=2,3,\ldots$$

For a bibliography on Korobov's problem see [Po, L1].

1.3. In [L2] we proposed using small discrepancy sequences (van der Corput type sequences and $\{n\alpha\}_{n\ge 0}$) to construct normal numbers, and announced that

$$\psi(N) = O(N^{-1}\log^2 N).$$

This result is proved below. The estimate of $\psi(N)$ was previously known to be $O(N^{-2/3}\log^{4/3} N)$ (Korobov [K2] for q prime, and Levin [L1] for arbitrary integer q). We note that the estimate obtained cannot be improved essentially, since according to W. Schmidt, 1972 (see [N, p. 24]), for any sequence of reals,

$$\overline{\lim_{N\to\infty}}\, ND(N)/\log N > 0.$$

1.4. Let $x = [a_0(x); a_1(x), a_2(x), \ldots]$ be the continued fraction expansion of x, with partial quotients $a_i(x)$. For an integer b and $Q>1$ let $\sum a_i(b/Q)$ denote the sum of all partial quotients of b/Q. Following [P] we prove (see Lemma 3) that there exists an integer sequence b_m and a constant $K>0$ with

$$\sum_{r=1}^{m}\sum a_i(\{b_m/q^r\}) \le Km^3, \qquad m=1,2,\ldots \tag{2}$$

Theorem 1. *Let*

$$\alpha = \sum_{m\ge 1}\frac{1}{q^{n_m}}\sum_{0\le k<q^m}\left\{\frac{b_m k}{q^m}\right\}\frac{1}{q^{mk}} \tag{3}$$

where b_m *satisfy* (2),

$$n_1 = 0 \quad \textit{and} \quad n_k = \sum_{1\le r<k} rq^r, \qquad k=2,3,\ldots \tag{4}$$

Then the number α *is normal to base* q, *and*

$$D(N, \{\alpha q^n\}_{n\ge 0}) = O(N^{-1}\log^3 N).$$

1.5. Let $(p'_{i,j})_{i,j\ge 1}$ be Pascal's triangle:

$$p'_{i,1} = p'_{1,i} = 1, \quad i=1,2,\ldots, \quad p'_{i,j} = p'_{i,j-1} + p'_{i-1,j}, \quad i,j=2,3,\ldots,$$

and $(p_{i,j})_{i,j\ge 1}$ be Pascal's triangle mod 2:

$$p_{i,j} \equiv p'_{i,j} \bmod 2, \qquad i,j=1,2,\ldots \tag{5}$$

Every integer $n \geq 0$ has a unique digit expansion in base q,

$$n = \sum_{j\geq 1} e_j(n) q^{j-1} \qquad \text{with } e_j(n) \in \Delta = \{0,\dots,q-1\}, \tag{6}$$

$j = 1, 2, \dots$, and $e_j(n) = 0$ for all sufficiently large j.

THEOREM 2. *Let*

$$\alpha = \sum_{m\geq 1} \frac{1}{q^{n_m}} \sum_{0\leq n<q^{2^m}} \frac{1}{q^{n2^m}} \sum_{i=1}^{2^m} \frac{d_i(n)}{q^i} \tag{7}$$

where

$$d_i(n) \equiv \sum_{j\geq 1} p_{i,j} e_j(n) \bmod q, \quad d_i(n) \in \Delta, \quad i = 1,\dots,2^m,\ n \in [0, q^{2^m}), \tag{8}$$

$$n_1 = 0 \quad \textit{and} \quad n_m = \sum_{1\leq r<m} 2^r q^{2^r}, \quad m = 2, 3, \dots \tag{9}$$

Then the number α is normal to base q and

$$D(N, \{\alpha q^n\}_{n\geq 0}) = O(N^{-1}\log^2 N).$$

REMARK 1. We use here the sequence of $2^m \times 2^m$ matrices of Pascal's triangle mod 2. A similar result is valid for the sequence of $m \times m$ matrices of Pascal's triangle (or $m \times m$ matrices of Pascal's triangle mod p) but with $D(N, \{\alpha q^n\}_{n\geq 0}) = O(N^{-1}\log^3 N)$, where α is denoted by a concatenation of blocks ω_m:

$$\alpha = .\omega_1 \dots \omega_m \dots,$$

where

$$\omega_m = (d_1(1)\dots d_m(1)\dots d_1(q^m)\dots d_m(q^m)), \qquad m = 1, 2, \dots,$$

and

$$d_i(n) \equiv \sum_{j\geq 1} p_{i,j} e_j(n) \bmod q.$$

REMARK 2. Let $(\sigma_i)_{i\geq 1}$ be any sequence of substitutions of the set $\Delta = \{0, 1, \dots, q-1\}$. The proof of Theorem 2 does not change if in (8) we use the functions $\sigma_i(e_i(n))$ instead of the functions $e_i(n)$ (see [B], [N, p. 25]).

2. Proof of the theorems. Let $m \geq 1,\ b,\ i$ be integers, $0 \leq i < m$, $(b, q) = 1$,

$$\alpha_m = \alpha_m(b) = \sum_{0\leq k<q^m} \left\{\frac{bk}{q^m}\right\} \frac{1}{q^{mk}}, \tag{10}$$

$$\alpha_{mni} = [q^{2m-i}\{\alpha_m q^{i+mn}\}]/q^{2m-i}. \tag{11}$$

It is easy to see that $\{\{bn/q^m\}q^i\} = \{bn/q^{m-i}\}$, and

$$\{\alpha_m q^{i+mn}\} = \left\{\left\{\frac{bn}{q^m}\right\}q^i + \left\{\frac{b(n+1)}{q^m}\right\}\frac{1}{q^{m-i}} + \left\{\frac{b(n+2)}{q^m}\right\}\frac{1}{q^{2m-i}} + \dots\right\}$$
$$= \left\{\frac{bn}{q^{m-i}}\right\} + \left\{\frac{b(n+1)}{q^m}\right\}\frac{1}{q^{m-i}} + \left\{\frac{b(n+2)}{q^m}\right\}\frac{1}{q^{2m-i}} + \dots$$

Therefore

$$\alpha_{mni} = \left\{\frac{bn}{q^{m-i}}\right\} + \left\{\frac{b(n+1)}{q^m}\right\}\frac{1}{q^{m-i}}. \tag{12}$$

Let $N \in [1, mq^m]$ be an integer, $\gamma \in (0,1]$,

$$A(\gamma, N, (x_n)) = \begin{cases} \#\{0 \le n < N \mid \{x_n\} < \gamma\} & \text{for } \gamma > 0, \\ 0 & \text{for } \gamma \le 0, \end{cases} \tag{13}$$

and

$$A(\gamma, Q, P, (x_n)) = \#\{Q \le n < Q + P \mid \{x_n\} < \gamma\}. \tag{14}$$

Hence and from (10) we obtain

$$\begin{aligned} A(\gamma, N, \{\alpha_m q^n\}_{n\ge0}) &= A(\gamma, m[N/m], \{\alpha_m q^n\}_{n\ge0}) \\ &\quad + A(\gamma, m[N/m], N - m[N/m], \{\alpha_m q^n\}_{n\ge0}) \\ &= \sum_{i=0}^{m-1} A(\gamma, [N/m], \{\alpha_m q^{i+mn}\}_{n\ge0}) + \theta m \end{aligned} \tag{15}$$

with $\theta \in [0,1]$.

Let $c = [q^m\gamma]$, $N_1 \in [1, q^m]$ and $0 \le i < m$. From (11) and (13) we deduce

$$\begin{aligned} A\left(\frac{c-1}{q^m}, N_1, (\alpha_{mni})_{n\ge0}\right) &\le A(\gamma, N_1, \{\alpha_m q^{mn+i}\}_{n\ge0}) \\ &\le A\left(\frac{c+1}{q^m}, N_1, (\alpha_{mni})_{n\ge0}\right). \end{aligned} \tag{16}$$

Lemma 1. *Let* $N \in [1, mq^m]$ *be an integer*, $\gamma \in (0,1]$, $(b,q) = 1$. *Then*

$$\begin{aligned} &A(\gamma, N, \{\alpha_m q^n\}_{n\ge0}) \\ &\qquad = \gamma N + \varepsilon_1\Big(4m + 3\sum_{i=1}^{m} \max_{1\le N\le q^i} ND(N, \{bn/q^i\}_{n\ge0})\Big), \end{aligned} \tag{17}$$

$$A(\gamma, mq^m, \{\alpha_m q^n\}_{n\ge0}) = \gamma mq^m + 3\varepsilon_2 m \tag{18}$$

with $|\varepsilon_j| < 1$, $j = 1, 2$.

Proof. Let $0 \le i < m$, d, d_1, and d_2 be integers, $d = d_1 q^i + d_2$, $d_1 \in [0, q^{m-i})$, $d_2 \in [0, q^i)$. By (12) and (13) we get

$$A\left(\frac{d}{q^m}, N_1, (\alpha_{mni})_{n\ge 0}\right) = \#\left\{0 \le n < N_1 \;\middle|\; \left\{\frac{bn}{q^{m-i}}\right\} + \left\{\frac{b(n+1)}{q^m}\right\}\frac{1}{q^{m-i}} < \frac{d_1}{q^{m-i}} + \frac{1}{q^{m-i}} \cdot \frac{d_2}{q^i}\right\}.$$

Consequently,

$$A(d/q^m, N_1, (\alpha_{mni})_{n\ge 0}) = T_1(N_1) + T_2(N_1), \tag{19}$$

where

$$T_1(N) = \#\left\{0 \le n < N \;\middle|\; \left\{\frac{bn}{q^{m-i}}\right\} < \frac{d_1}{q^{m-i}}\right\}, \tag{20}$$

$$T_2(N) = \#\left\{0 \le n < N \;\middle|\; \left\{\frac{bn}{q^{m-i}}\right\} = \frac{d_1}{q^{m-i}} \text{ and } \left\{\frac{b(n+1)}{q^m}\right\} < \frac{d_2}{q^i}\right\}. \tag{21}$$

Let $N_1 = N_2 q^{m-i} + N_3$ with $N_3 \in [0, q^{m-i})$ and $N_2 \in [0, q^i)$. It is easy to see that

$$T_1(N_1) = T_1(q^{m-i} N_2) + T_1(N_3).$$

We see from (20) and (1) that

$$T_1(N_2 q^{m-i}) = N_2 d_1, \tag{22}$$

and

$$T_1(N_3) = \frac{d_1}{q^{m-i}} N_3 + \varepsilon N_3 D\left(N_3, \left\{\frac{bn}{q^{m-i}}\right\}_{n\ge 0}\right) \quad \text{with } |\varepsilon| \le 1.$$

This yields

$$T_1(N_1) = \frac{d_1}{q^{m-i}} N_1 + \varepsilon \max_{1 \le N < q^{m-i}} N D\left(N, \left\{\frac{bn}{q^{m-i}}\right\}_{n\ge 0}\right) \text{ with } |\varepsilon| \le 1. \tag{23}$$

Now we compute $T_2(N)$. Let d_0 be an integer, $d_0 \equiv d_1 b^{-1} \bmod q^{m-i}$ with $d_0 \in [0, q^{m-i})$, and

$$Y = \{0 \le n < N_1 \mid \{bn/q^{m-i}\} = d_1/q^{m-i}\}.$$

Clearly if $\{bn/q^{m-i}\} = d_1/q^{m-i}$, then $bn \equiv d_1 \bmod q^{m-i}$, $n \equiv d_0 \bmod q^{m-i}$, and

$$Y = \{d_0 + r q^{m-i} \mid 0 \le r < N_4\} \quad \text{with } N_4 = \left[\frac{N_1 - d_0 - 1}{q^{m-i}}\right] + 1. \tag{24}$$

Combining (21) and (1) we obtain

$$T_2(N_1) = \#\left\{n \in Y \,\middle|\, \left\{\frac{b(n+1)}{q^m}\right\} < \frac{d_2}{q^i}\right\} \tag{25}$$
$$= \#\left\{0 \le r < N_4 \,\middle|\, \left\{\frac{b(d_0+1)}{q^m} + \frac{br}{q^i}\right\} < \frac{d_2}{q^i}\right\}$$
$$= N_4 \frac{d_2}{q^i} + \varepsilon_2 N_4 D\biggl(N_4, \left\{\frac{bn}{q^i} + \theta\right\}_{n\ge 0}\biggr)$$

with $\theta = b(d_0+1)/q^m,\ |\varepsilon_2| \le 1$.

It follows from (1) that for every real θ,

$$D(N, \{x_n + \theta\}_{n\ge 0}) \le 2D(N, \{x_n\}_{n\ge 0}). \tag{26}$$

By (24) and (25), this yields

$$T_2(N_1) = \left[\frac{N_1 + q^{m-i} - d_0 - 1}{q^{m-i}}\right]\frac{d_2}{q^i} + 2\varepsilon_2 \max_{1\le N\le q^i} ND(N, \{bn/q^i\}_{n\ge 0}) \tag{27}$$
$$= N_1 \frac{d_2}{q^m} + \varepsilon_3 + 2\varepsilon_2 \max_{1\le N\le q^i} ND(N, \{bn/q^i\}_{n\ge 0})$$

with $|\varepsilon_j| \le 1,\ j = 2, 3$.

If $N_1 = q^m$, then $N_4 = q^i$, and $N_4 D(N_4, \{bn/q^i\}_{n\ge 0}) = 1$. Hence and from (25) and (26) we obtain

$$T_2(q^m) = d_2 + 2\varepsilon_4 \quad \text{with } |\varepsilon_4| \le 1. \tag{28}$$

Substituting (23) and (27) into (19), we obtain

$$A(d/q^m, N_1, (\alpha_{mni})_{n\ge 0})$$
$$= N_1 d/q^m + \varepsilon_5 (1 + \max_{1\le N<q^{m-i}} ND(N, \{bn/q^{m-i}\}_{n\ge 0})$$
$$+ 2 \max_{1\le N\le q^i} ND(N, \{bn/q^i\}_{n\ge 0})) \quad \text{with } |\varepsilon_5| \le 1.$$

Using (16) and (15) we get

$$A(\gamma, N_1, \{\alpha_m q^{mn+i}\}_{n\ge 0})$$
$$= \gamma N_1 + \varepsilon_6 (2 + \max_{1\le N<q^{m-i}} ND(N, \{bn/q^{m-i}\}_{n\ge 0})$$
$$+ 2 \max_{1\le N\le q^i} ND(N, \{bn/q^i\}_{n\ge 0})) \quad \text{with } |\varepsilon_6| \le 1,$$

and

$$A(\gamma, N, \{\alpha_m q^n\}_{n\ge 0}) = \theta m + \sum_{i=1}^m \gamma [N/m]$$
$$+ \varepsilon_7 \Bigl(2m + 3 \sum_{i=1}^m \max_{1\le N\le q^i} ND(N, \{bn/q^i\}_{n\ge 0})\Bigr)$$
$$= \gamma N + \varepsilon_8 \Bigl(4m + 3 \sum_{i=1}^m \max_{1\le N\le q^i} ND(N, \{bn/q^i\}_{n\ge 0})\Bigr),$$

where $|\varepsilon_j| \le 1$, $j = 7, 8$. Assertion (17) is proved. Assertion (18) follows analogously from (22) and (28). ∎

LEMMA 2. *Let* $j \ge 1$, $1 \le N \le q^j$, $(b, q) = 1$, *and* $a_i(x)$ *be partial quotients of* $\{x\}$. *Then*

$$ND(N, \{bn/q^j\}_{n\ge 0}) \le \sum a_i(b/q^j).$$

For the proof of this well-known theorem, see for example [N, p. 26].

LEMMA 3. *There exists a constant* $K > 0$ *and integers* $c_m \in [0, q^m)$ *such that*

$$\sum_{r=1}^{m} \sum a_i(\{c_m/q^r\}) \le Km^3, \qquad m = 1, 2, \ldots$$

Proof. According to [P, p. 2144] there exist constants K_q such that

$$\sum_{1\le c\le q^r,\,(c,q)=1} \sum a_i(c/q^r) \le K_q q^r r^2, \qquad r = 1, 2, \ldots$$

Therefore

$$\sum_{1\le c\le q^m,\,(c,q)=1} \sum_{r=1}^{m} \sum a_i(\{c/q^r\}) = \sum_{r=1}^{m} q^{m-r} \sum_{1\le c\le q^r,\,(c,q)=1} \sum a_i(c/q^r) \le \sum_{r=1}^{m} q^m K_q r^2 \le K_q q^m m^3. \tag{29}$$

Let $\phi(q^m) = \#\{1 \le c \le q^m \mid (c, q) = 1\}$ and $K = K_q q/\phi(q)$. It is known that $\phi(q^m) = q^{m-1}\phi(q)$. Now the assertion of Lemma 3 follows from (29). ∎

COROLLARY. *Let* $1 \le N \le mq^m$. *Then*

$$A(\gamma, N, \{\alpha_m(b_m)q^n\}_{n\ge 0}) = \gamma N + O(m^3). \tag{30}$$

The statement follows from (1), (2), (10), and Lemmas 1–3. ∎

Applying (3) and (10) we get

$$\{\alpha q^{n_m+n}\} = \{\alpha_m(b_m)q^n\} + \theta q^{n-mq^m} \qquad \text{with } 0 < \theta < 1 \text{ and } 0 \le n < mq^m.$$

Hence and from (13) we have, for $N \in [1, mq^m]$,

$$A(\gamma - 1/q^m, N - m, \{\alpha_m(b_m)q^n\}_{n\ge 0}) \le A(\gamma, N, \{\alpha q^{n_m+n}\}_{n\ge 0}) \le A(\gamma, N, \{\alpha_m(b_m)q^n\}_{n\ge 0}).$$

By using (30) and (14), we obtain

$$A(\gamma, n_m, N, \{\alpha q^n\}_{n\ge 0}) = \gamma N + O(m^3) \qquad \text{with } 1 \le N \le mq^m. \tag{31}$$

Similarly, from (18) we deduce that

$$A(\gamma, n_m, mq^m, \{\alpha q^n\}_{n\ge 0}) = \gamma mq^m + O(m). \tag{32}$$

End of the proof of Theorem 1. For every $N \geq 1$ there exists an integer k such that $N \in [n_k, n_{k+1})$. By (4) this yields

$$N = n_k + R \quad \text{with } 0 \leq R < kq^k,\ N > (k-1)q^{k-1},\ k \leq 2\log_q N. \tag{33}$$

Applying (4), (14) and (31)–(33) we obtain

$$\begin{aligned} A(\gamma, N, \{\alpha q^n\}_{n\geq 0}) &= \sum_{r=1}^{k-1} A(\gamma, n_r, rq^r, \{\alpha q^n\}_{n\geq 0}) + A(\gamma, n_k, R, \{\alpha q^n\}_{n\geq 0}) \\ &= \sum_{r=1}^{k-1} (\gamma r q^r + O(r)) + \gamma R + O(k^3) \\ &= \gamma N + O(k^3) = \gamma N + O(\log^3 N). \end{aligned}$$

Thus, by (1), the theorem is proved. ■

Proof of Theorem 2. In [So] Sobol' proposed the use of Pascal's triangle mod 2 to construct small discrepancy sequences (see also [F], [N]). Here we use Pascal's triangle mod 2 to construct normal numbers.

Let P_n be a sequence of a $2^n \times 2^n$ matrices such that

$$P_1 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \quad \ldots, \quad P_{n+1} = \begin{pmatrix} P_n & P_n \\ P_n & 0 \end{pmatrix}, \quad \ldots$$

It is easy to prove by induction that P_n is the $2^n \times 2^n$ upper left-hand corner of Pascal's triangle (5), and P_n is a triangular-type matrix. The following lemma is proved in [BH] for Pascal's triangle, and it is clearly valid also for Pascal's triangle mod 2.

Lemma 4. *The determinant of any $n \times n$ array taken with its first row along a row of ones, or with its first column along a column of ones in Pascal's triangle, written in rectangular form, is one.*

From (7) we have

$$\{\alpha q^{n_m + 2^m n + k}\} = .d_{k+1}(n) d_{k+2}(n) \ldots d_{2^m}(n) d_1(n+1) \ldots \tag{34}$$

Let $1 \leq k, i \leq 2^m$ and

$$\alpha_{ki}(n) = [\{\alpha q^{n_m + 2^m n + k}\} q^i]/q^i. \tag{35}$$

It is easy to see that

$$\alpha_{ki}(n) = \begin{cases} .d_{k+1}(n) \ldots d_{k+i}(n) & \text{if } k + i \leq 2^m, \\ .d_{k+1}(n) \ldots d_{2^m}(n) d_1(n+1) \ldots d_{k+i-2^m}(n+1) & \text{otherwise.} \end{cases} \tag{36}$$

Lemma 5. *Let m, k, i, B, f be integers, $1 \leq i, k \leq 2^m$, $B \in [0, q^{2^m - i})$, $f \in [0, q^i)$. Then*

$$A(f/q^i, Bq^i, q^i, (\alpha_{ki}(n))_{n\geq 0}) = f + 2\varepsilon \quad \textit{with } |\varepsilon| < 1.$$

Proof. Case 1. Let $k+i \le 2^m$, $c_j \in \Delta = \{0,1,\dots,q-1\}$ $(j=1,\dots,i)$. We examine the system of equations

$$d_{k+j}(n) = c_j, \qquad j = 1,\dots,i,\ n \in [Bq^i,(B+1)q^i). \tag{37}$$

According to (8) this system is equivalent to the system of i congruences

$$\sum_{1\le\nu\le 2^m} p_{k+j,\nu} e_\nu(n+Bq^i) \equiv c_j \bmod q, \qquad j=1,\dots,i,\ n\in[0,q^i).$$

Applying (6) we see that $e_\nu(n+Bq^i) = e_\nu(n) + e_\nu(Bq^i)$, $\nu = 1,2,\dots$, and

$$\sum_{1\le\nu\le i} p_{k+j,\nu} e_\nu(n) \equiv c_j - \sum_{i<\nu\le 2^m} p_{k+j,\nu} e_\nu(Bq^i) \bmod q, \qquad j=1,\dots,i, \tag{38}$$

with $n\in[0,q^i)$. It follows from Lemma 4 that

$$|\det(p_{k+j,\nu})_{1\le j,\nu\le i}| = 1. \tag{39}$$

For any $c_1,\dots,c_i$ the system (38) has a unique solution $(e_1(n),\dots,e_i(n))$, and consequently there exists a unique $n_0\in[Bq^i,(B+1)q^i)$ satisfying (37).

From (36) and (37) we see that the set $\{\alpha_{ki}(n) \mid n\in[Bq^i,(B+1)q^i)\}$ coincides with $\{j/q^i \mid j\in[0,q^i)\}$. Hence and from (14) we have

$$A(f/q^i, Bq^i, q^i, (\alpha_{ki}(n))_{n\ge 0}) = f. \tag{40}$$

Case 2. Let $k+i > 2^m$, $l_1 = 2^m - k$. As in (37) and (38), the system of equations

$$d_{k+j}(n) = c_j, \qquad j = 1,\dots,l_1, \tag{41}$$

$$d_j(n+1) = c_{j+l_1}, \qquad j = 1,\dots,i-l_1, \tag{42}$$

with $n\in[Bq^i,(B+1)q^i)$, is equivalent to the systems of congruences

$$\sum_{1\le\nu\le i} p_{k+j,\nu} e_\nu(n) \equiv c_j - \sum_{i<\nu\le 2^m} p_{k+j,\nu} e_\nu(Bq^i) \bmod q, \qquad j=1,\dots,l_1, \tag{43}$$

$$\sum_{1\le\nu\le i} p_{j,\nu} e_\nu(n+1) \equiv c_{j+l_1} - \sum_{i<\nu\le 2^m+1} p_{j,\nu} e_\nu((B+[(n+1)/q^i])q^i) \bmod q, \tag{44}$$

where $j=1,\dots,i-l_1$ and $n\in[0,q^i)$.

Let $n = n_1 + n_2 q^{l_1}$ with $n_1\in[0,q^{l_1})$ and $n_2\in[0,q^{i-l_1})$. It is evident that $e_\nu(n) = e_\nu(n_1)$ for $\nu = 1,\dots,l_1$.

The matrix P_m is triangular. Hence

$$p_{k+j,\nu} = 0 \qquad \text{with } \nu > 2^m - k - j = l_1 - j.$$

The system (43) is equivalent to the following system of congruences:

$$(45)\qquad \sum_{1\le\nu\le l_1} p_{k+j,\nu}e_\nu(n_1) \equiv c_j - \sum_{i<\nu\le 2^m} p_{k+j,\nu}e_\nu(Bq^i) \bmod q, \qquad j=1,\ldots,l_1,$$

where $n_1 \in [0,q^{l_1})$ and $n_2 \in [0,q^{i-l_1})$.

Applying (39) with $i=l_1$ shows that this system has a unique solution with $(e_1(n_1),\ldots,e_{l_1}(n_1))$. Consequently, there exists a unique solution $n_1 = n_1' \in [0,q^{l_1})$ satisfying (45).

By (41) and (43) we obtain

$$(46)\qquad \{(d_{k+1}(n_1+n_2q^{l_1}+Bq^i),\ldots,d_{k+l_1}(n_1+n_2q^{l_1}+Bq^i)) \mid 0\le n_1<q^{l_1}\} = \{(c_1,\ldots,c_{l_1}) \mid c_j\in\Delta,\ j=1,\ldots,l_1\}.$$

Now we examine the system (44) with $n_1=n_1'$ the solution of (45).

Case 2.1. Let $n_1' \le q^{l_1}-2$. Bearing in mind that

$$e_\nu(n+1) = e_\nu(n_1'+1+q^{l_1}n_2) = e_\nu(n_1'+1)+e_\nu(q^{l_1}n_2),$$

we deduce from (44) that

$$\sum_{l_1<\nu\le i} p_{j,\nu}e_\nu(q^{l_1}n_2) \equiv c_{j+l_1} - \sum_{1\le\nu\le l_1} p_{j,\nu}e_\nu(n_1'+1) - \sum_{i<\nu\le 2^m} p_{j,\nu}e_\nu(Bq^i) \bmod q$$

with $j=1,\ldots,i-l_1$ and $0\le n_2<q^{i-l_1}$.

Applying Lemma 4 we obtain a unique solution for this system with $(e_{l_1+1}(q^{l_1}n_2),\ldots,e_i(q^{l_1}n_2))$.

By (42) and (44) we get

$$(47)\qquad \{(d_1(n_1'+n_2q^{l_1}+Bq^i+1),\ldots,d_{i-l_1}(n_1'+n_2q^{l_1}+Bq^i+1)) \mid 0\le n_2<q^{i-l_1}\} = \{(c_{l_1+1},\ldots,c_i) \mid c_{l_1+j}\in\Delta,\ j=1,\ldots,i-l_1\}.$$

Let

$$(48)\qquad F = \{d_{k+1}(n)\ldots d_{2^m}(n)d_1(n+1)\ldots d_{k+i-2^m}(n+1) \mid 0\le n_1<q^{l_1}-1,\ 0\le n_2<q^{i-l_1},\ n=n_1+n_2q^{l_1}+Bq^i\},$$

and

$$(49)\qquad g_\nu = d_{k+\nu}(q^{l_1}-1+Bq^i), \qquad \nu=1,\ldots,l_1.$$

From (46) and (47) we have

$$(50)\quad F = \{(c_1,\ldots,c_i) \mid c_j\in\Delta,\ j=1,\ldots,i,\ (c_1,\ldots,c_{l_1})\ne(g_1,\ldots,g_{l_1})\}$$

and

$$(51)\qquad \#F = q^i - q^{i-l_1}.$$

Case 2.2. Let $n_1' = q^{l_1}-1$, $n_2\in[0,q^{i-l_1}-2]$ and $n=n_1'+n_2q^{l_1}$. Then $e_\nu(n_1'+1)=0$ for $1\le\nu\le l_1$ and $e_\nu(n+1)=e_\nu((n_2+1)q^{l_1})$ for $l_1<\nu\le i$.

The system (44) is equivalent to the following system of congruences:

$$(52)\qquad \sum_{l_1<\nu\le i} p_{j,\nu}e_\nu((n_2+1)q^{l_1}) \equiv c_{j+l_1} - \sum_{i<\nu\le 2^m} p_{j,\nu}e_\nu(Bq^i) \bmod q, \qquad j=1,\dots,i-l_1,$$

with $0\le n_2\le q^{i-l_1}-2$.

For $n_2\in[0,q^{i-l_1}-2]$ we have the $q^{i-l_1}-1$ distinct vectors of

$$(e_{l_1+1}((n_2+1)q^{l_1}),\dots,e_i((n_2+1)q^{l_1})).$$

Using Lemma 4 and by (52) we obtain for $n_2\in[0,q^{i-l_1}-2]$ the $q^{i-l_1}-1$ distinct vectors of $(c_{l_1+1},\dots,c_i)$.

Let

$$G=\{(g_1,\dots,g_{l_1},d_1((n_2+1)q^{l_1}+Bq^i),\dots,d_{i-l_1}((n_2+1)q^{l_1}+Bq^i))\mid 0\le n_2\le q^{i-l_1}-2\}.$$

From (42), (44) and (52) we find that $\#G=q^{i-l_1}-1$, and from (46) and (48)–(51) that $\#(F\cup G)=q^i-1$. Hence and from (36) the set $\{\alpha_{ki}(n)\mid n\in[Bq^i,(B+1)q^i-2]\}$ coincides with q^i-1 distinct values of j/q^i with $j\in[0,q^i)$. By (14) we get

$$A(f/q^i,Bq^i,q^i,(\alpha_{ki}(n))_{n\ge0})=f+2\varepsilon \quad \text{with } |\varepsilon|<1.$$

Hence and from (40) we have the assertion of Lemma 5. ∎

Corollary 1.

$$(53)\qquad A(\gamma,Bq^i,q^i,\{\alpha q^{n_m+2^m n+k}\}_{n\ge0})=\gamma q^i+4\varepsilon \quad \textit{with } |\varepsilon|<1.$$

Proof. Analogously to (16), from (14) and (35) we have

$$A\left(\frac{f-1}{q^i},Bq^i,q^i,(\alpha_{ki}(n))_{n\ge0}\right)\le A(\gamma,Bq^i,q^i,\{\alpha q^{n_m+2^m n+k}\}_{n\ge0}) \le A((f+1)/q^i,Bq^i,q^i,(\alpha_{ki}(n))_{n\ge0})$$

with $f=[\gamma q^i]$. By using Lemma 5 we obtain (53).

Corollary 2. *Let* $1\le N<2^m q^{2^m}$. *Then*

$$(54)\qquad A(\gamma,n_m,N,\{\alpha q^n\}_{n\ge0})=\gamma N+5q\varepsilon 2^{2m} \quad \textit{with } |\varepsilon|<1,$$

$$(55)\qquad A(\gamma,n_m,2^m q^{2^m},\{\alpha q^n\}_{n\ge0})=\gamma 2^m q^{2^m}+5\varepsilon 2^m \quad \textit{with } |\varepsilon|<1.$$

Proof. Let $N'=[N/2^m]$, $N''=N-2^m N'$, $N'=\sum_{i=0}^{2^m-1} b_i q^i$ with $b_i\in\Delta$,

$$(56)\qquad N_0=0,\quad N_j=\sum_{i=0}^{j-1} b_{2^m-i}q^{2^m-i},\quad j=1,2,\dots,\quad B_i=N_{2^m-i-1}/q^i.$$

It is evident that B_i $(i = 1, 2, \ldots)$ are integers, and $N'' \in [0, 2^m)$. As in (15) we see from (14) that

$$A(\gamma, n_m, N, \{\alpha q^n\}_{n\geq 0}) = \varepsilon N_2 + \sum_{k=1}^{2^m} A(\gamma, N', \{\alpha q^{n_m+2^m n+k}\}_{n\geq 0}),$$

and

$$\begin{aligned} A(\gamma, N', &\{\alpha q^{n_m+2^m n+k}\}_{n\geq 0}) \\ &= \sum_{i=1}^{2^m} A(\gamma, N_{i-1}, b_{2^m-i} q^{2^m-i}, \{\alpha q^{n_m+2^m n+k}\}_{n\geq 0}) \\ &= \sum_{i=0}^{2^m-1} A(\gamma, N_{2^m-i-1}, b_i q^i, \{\alpha q^{n_m+2^m n+k}\}_{n\geq 0}) \\ &= \sum_{i=0}^{2^m-1} \sum_{B=0}^{b_i-1} A(\gamma, N_{2^m-i-1} + Bq^i, q^i, \{\alpha q^{n_m+2^m n+k}\}_{n\geq 0}). \end{aligned}$$

Using (56) we have

$$\begin{aligned} A(\gamma, &n_m, N, \{\alpha q^n\}_{n\geq 0}) \\ &= \varepsilon 2^m + \sum_{k=1}^{2^m} \sum_{i=0}^{2^m-1} \sum_{B=0}^{b_i-1} A(\gamma, (B_i + B) q^i, q^i, \{\alpha q^{n_m+2^m n+k}\}_{n\geq 0}). \end{aligned}$$

Applying (53) we obtain

$$A(\gamma, n_m, N, \{\alpha q^n\}_{n\geq 0}) = \varepsilon 2^m + \sum_{k=1}^{2^m} \sum_{i=0}^{2^m-1} \sum_{B=0}^{b_i-1} (\gamma q^i + 4\varepsilon_i) = \gamma N + 5q\varepsilon_1 2^{2m}$$

with $|\varepsilon_1| \leq 1$.

Assertion (54) is proved. We prove (55) analogously.

End of the proof of Theorem 2. For every $N \geq q$ there exists an integer k such that $N \in [n_k, n_{k+1})$. By (9), this yields $N = n_k + R$ with $0 \leq R < 2^k q^{2^k}$, $N \geq 2^{(k-1)} q^{2^{k-1}}$, $2^k \leq 2 \log_q N$. Applying (9), (13), (14), (54) and (55) we obtain

$$\begin{aligned} A(\gamma, N, \{\alpha q^n\}_{n\geq 0}) &= \sum_{m=1}^{k-1} A(\gamma, n_m, 2^m q^{2^m}, \{\alpha q^n\}_{n\geq 0}) \\ &\quad + A(\gamma, n_k, R, \{\alpha q^n\}_{n\geq 0}) \\ &= \sum_{m=1}^{k-1} (\gamma 2^m q^{2^m} + O(2^m)) + \gamma R + O(2^{2k}) \\ &= \gamma N + O(2^{2k}) = \gamma N + O(\log^2 N). \end{aligned}$$

Thus, by (1), the theorem is proved. ■

Acknowledgments. I am very grateful to Professor Meir Smorodinsky for his hospitality, and to the referee for his valuable suggestions.

References

[B] R. Bejian, *Sur certaines suites présentant une faible discrépance à l'origine*, C. R. Acad. Sci. Paris Sér. A 286 (1978), 135–138.

[BH] M. Bicknell and V. E. Hoggart, Jr., *Unit determinants in generalized Pascal triangles*, Fibonacci Quart. 11 (1978), 131–144.

[F] H. Faure, *Discrépance de suites associées à un système de numération* (*en dimension s*), Acta Arith. 41 (1982), 337–351.

[G] I. S. Gal and L. Gal, *The discrepancy of the sequence* $(2^n x)$, Indag. Math. 26 (1964), 129–143.

[K1] N. M. Korobov, *Numbers with bounded quotient and their applications to questions of Diophantine approximation*, Izv. Akad. Nauk SSSR Ser. Mat. 19 (1955), 361–380.

[K2] —, *Distribution of fractional parts of exponential function*, Vestnik Moskov. Univ. Ser. I Mat. Mekh. 21 (1966), no. 4, 42–46.

[L1] M. B. Levin, *The distribution of fractional parts of the exponential function*, Soviet Math. (Izv. VUZ) 21 (1977), no. 11, 41–47.

[L2] —, *On the upper bounds of discrepancy of completely uniform distributed and normal sequences*, AMS-IMU joint meeting, Jerusalem, Israel, May 24–26, 1995, Abstracts Amer. Math. Soc. 16 (1995), 556–557.

[N] H. Niederreiter, *Random Number Generation and Quasi-Monte Carlo Methods*, CBMS-NSF Regional Conf. Ser. in Appl. Math. 63, Philadelphia, 1992.

[P] V. N. Popov, *Asymptotic formula for the sum of sums of the elements of the continued fractions for numbers of the form* a/p, J. Soviet Math. 17 (1981), 2137–2147.

[Po] A. G. Postnikov, *Arithmetic modeling of random processes*, Proc. Steklov Inst. Math. 57 (1960).

[S] J. Schiffer, *Discrepancy of normal numbers*, Acta Arith. 47 (1986), 175–186.

[So] I. M. Sobol', *Multidimensional Quadrature Formulas and Haar Functions*, Nauka, Moscow, 1969 (in Russian).

School of Mathematical Sciences
Tel-Aviv University
69978 Tel-Aviv, Israel
E-mail: mlevin@math.tau.ac.il

Received on 30.12.1996
and in revised form on 29.5.1998 (3105)