On Finite Pseudorandom Binary Sequences, VI,  
(On \(n^k\alpha\) Sequences)  

By  
Christian Mauduit\(^1\) and András Sárközy\(^2\,*\)  
\(^1\) CNRS-UPR, Marseille, France  
\(^2\) Eötvös Lóránd University, Budapest, Hungary  

(Received 5 November 1997; in revised form 7 March 2000)  

Abstract. Let \(k\) be a positive integer and \(\alpha\) be a real number, and for \(n = 1, 2, \ldots\) let \(e_n = +1\) if the fractional part of \(n^k\alpha\) is \(< 1/2\), and \(e_n = -1\) if it is \(\geq 1/2\). The pseudorandom properties of the sequence \(e_1, e_2, \ldots\), are studied. As measures of pseudorandomness, the regularity of the distribution relative to arithmetic progressions and the correlation are used. In a previous paper the authors studied the special cases \(k = 1\) and \(k = 2\), while here the case \(k > 2\) is considered.  

1991 Mathematics Subject Classification: 11K45  
Key words: Pseudorandom, binary sequence, uniform distribution  

1. Introduction  

We write \(e(\alpha) = e^{2\pi i\alpha}\). The fractional part of \(\alpha\) is denoted by \(\{\alpha\}\). We define \(\chi(x)\) by  

\[
\chi(x) = \begin{cases}  
+1 & \text{for } 0 \leq \{x\} < 1/2 \\
-1 & \text{for } 1/2 \leq \{x\} < 1. 
\end{cases}  
\]  

(1.1)  

The discrepancy (see [4]) of the finite or infinite sequence \(x_1, \ldots, x_N, \ldots\) of points in \(\mathbb{R}^d\) is denoted by \(D_N(x_1, \ldots, x_N)\).  

Let \(\alpha\) be an irrational number, and for \(k \in \mathbb{N}\), \(N \in \mathbb{N}\) define the sequence \(E_N = E_N(n^k\alpha) = \{e_1, \ldots, e_N\}\) by  

\[
e_n = \chi(n^k\alpha).  
\]  

(1.2)  

In Part I of this paper [8], starting out from a problem of Erdős, we studied the pseudorandom (briefly, PR) properties of the binary sequences \(E_N(n\alpha), E_N(n^2\alpha)\). In this paper, we will study the PR properties of the sequence \(E_N(n^k\alpha)\) for general \(k\). As in Part I, we will use the following measures of pseudorandomness (introduced in [7]):  

---  

\* Research partially supported by Hungarian National Foundation for Scientific Research, Grant No. T 029759, MKM fund FKFP-0139/1997 and French-Hungarian APAPE-OMFB exchange program F-5/97. This paper was written while the second author was visiting the Institut de Mathématiques de Luminy.
For a binary sequence $E_N = \{e_1, e_2, \ldots, e_N\} \in \{-1, +1\}^N$, write

$$U(E_N, t, a, b) = \sum_{j=1}^{t} e_{a+jb}$$

and, for $d = (d_1, d_2, \ldots, d_\ell)$ with non-negative integers $d_1 < d_2 < \cdots < d_\ell$,

$$V(E_N, M, d) = \sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} \cdots e_{n+d_\ell}.$$ 

Then the well-distribution measure of $E_N$ is defined as

$$W(E_N) = \max_{a,b,t} |U(E_N, t, a, b)| = \max_{a,b,t} \left| \sum_{j=1}^{t} e_{a+jb} \right|,$$

where the maximum is taken over all $a, b, t$ such that $a \in \mathbb{Z}$, $b, t \in \mathbb{N}$ and $1 \leq a + b \leq a + tb \leq N$, while the correlation measure of order $\ell$ of $E_N$ is defined as

$$C_\ell(E_N) = \max_{M,d} |V(E_N, M, d)| = \max_{M,d} \left| \sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} \cdots e_{n+d_\ell} \right|,$$

where the maximum is taken over all $d = (d_1, d_2, \ldots, d_\ell)$ and $M$ such that $M + d_\ell \leq N$. If both $W(E_N)$ and $C_\ell(E_N)$ (for “small” $\ell$) are “small”, then $E_N$ is considered as a “good” PR sequence.

In Part I we showed that $E(n\alpha)$ and $E(n^2\alpha)$ possess certain PR properties (but some other PR properties fail) under the condition that the partial quotients in the continued fraction expansion of $\alpha$ are bounded:

$$\alpha = [a_0; a_1, a_2, \ldots], \quad a_i \leq K \quad \text{for} \quad i \geq 1. \quad (1.3)$$

Here we will show that under the same condition, $E_N(n^k\alpha)$ provides a positive example in the sense that both the well-distribution measure and correlation measure of order $\leq \frac{k-1}{2}$ are small:

**Theorem 1.** (i) Assume that $k \in \mathbb{N}$, $k \geq 3$, and $\alpha$ is an irrational number whose partial quotients satisfy (1.3) with some $K \in \mathbb{N}$. Define $\sigma_k$ by the following table:

<table>
<thead>
<tr>
<th>$k$</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\sigma_k$</td>
<td>9</td>
<td>20</td>
<td>51</td>
<td>116</td>
<td>247</td>
<td>422</td>
<td>681</td>
<td>1090</td>
<td>1781</td>
</tr>
</tbody>
</table>

Then for all $\varepsilon > 0$, there is a number $N_0 = N_0(k, k, \varepsilon)$ such that if $N > N_0$, then defining $E_N = E_N(n^k\alpha) = \{e_1, \ldots, e_N\}$ by (1.2) we have

$$W(E_N) < N^{1-1/\sigma_k + \varepsilon}. \quad (1.4)$$

(ii) If $k \to +\infty$, then under the same assumption as in (i), (1.4) also holds with

$$\sigma_k = \frac{3}{2} k^2 (\log k + O(\log \log k)). \quad (1.5)$$

**Theorem 2.** (i) Assume that $k \in \mathbb{N}$, $k \geq 2$, $\ell \in \mathbb{N}$,

$$k \geq 2\ell + 1, \quad (1.6)$$