Pseudorandom binary sequences generated by sequences $(n\alpha)$

Štefan Porubský
Institute of Computer Science
Academy of Sciences of the Czech Republic
Pod Vodárenskou věží 2
182 07 Prague 8

email: Stefan.Porubsky@cs.cas.cz

joint work with Oto Strauch

A **binary sequence** x_n, $n = 1, 2, \ldots,$ is a sequence which elements attains only two values, usually $x_n \in \{0, 1\}$ or $x_n \in \{-1, 1\}$.

A **binary sequence** x_n, $n = 1, 2, \ldots$, is a sequence which elements attains only two values, usually $x_n \in \{0, 1\}$ or $x_n \in \{-1, 1\}$.

Given an arbitrary infinite sequence y_n, $n = 1, 2, \ldots$, in $[0, 1]$ and a non-empty interval $I \subset [0, 1]$, we can generate a new binary (often called **coding**) sequence from x_n using one of the following rules:

A **binary sequence** x_n, $n = 1, 2, \ldots$, is a sequence which elements attains only two values, usually $x_n \in \{0, 1\}$ or $x_n \in \{-1, 1\}$.

Given an arbitrary infinite sequence y_n, $n = 1, 2, \ldots$, in $[0, 1]$ and a non-empty interval $I \subset [0, 1]$, we can generate a new binary (often called **coding**) sequence from x_n using one of the following rules:

- to get a $\{-1, 1\}$-sequence by

$$\chi_I(y_n) = \begin{cases} 1, & \text{if } y_n \in I, \text{ and} \\ -1, & \text{if } y_n \notin I, \end{cases}$$

A **binary sequence** x_n, $n = 1, 2, \ldots$, is a sequence which elements attains only two values, usually $x_n \in \{0, 1\}$ or $x_n \in \{-1, 1\}$.

Given an arbitrary infinite sequence y_n, $n = 1, 2, \ldots$, in $[0, 1]$ and a non-empty interval $I \subset [0, 1]$, we can generate a new binary (often called **coding**) sequence from x_n using one of the following rules:

- to get a $\{-1, 1\}$-sequence by
$$\chi_I(y_n) = \begin{cases} 1, & \text{if } y_n \in I, \text{ and} \\ -1, & \text{if } y_n \notin I, \end{cases}$$
- or to get a $\{0, 1\}$-sequence by
$$c_I(y_n) = \begin{cases} 1, & \text{if } y_n \in I, \text{ and} \\ 0, & \text{if } y_n \notin I. \end{cases}$$

A **Sturmian sequence** x_n is as a $\{0,1\}$-sequence such that for every k the number $p(k)$ of different blocks of elements $x_{n+1},\dots,x_{n+k}$, $n=1,2,\dots,$ is equal to $k+1$. The function $p(k)$ is called the **complexity function**.

A **Sturmian sequence** x_n is as a $\{0,1\}$-sequence such that for every k the number $p(k)$ of different blocks of elements $x_{n+1},\dots,x_{n+k}$, $n=1,2,\dots,$ is equal to $k+1$. The function $p(k)$ is called the **complexity function**. From the complexity point of view they can be defined as a non-periodic sequences of minimal complexity $p(n)=n+1$.

The Sturmian binary $0,1$-sequences u_n can be characterized as follows:

Proposition. *A $0,1$-sequence u_n is Sturmian if and only if*

- *it is non-eventually periodic,*
- *the number of 1's in any pair of finite subsegments of the same length occurring in u_n can differ by at most one.*

The Sturmian binary $0,1$-sequences u_n can be characterized as follows:

Proposition. *A $0,1$-sequence u_n is Sturmian if and only if*

- *it is non-eventually periodic,*
- *the number of 1's in any pair of finite subsegments of the same length occurring in u_n can differ by at most one.*

It is known that the sequence $x_n = c_I(\{n\alpha\})$ with a special choice of interval I of length $|I| = \{\alpha\}$ or $|I| = 1 - \{\alpha\}$ is Sturmian.

The Sturmian binary $0,1$-sequences u_n can be characterized as follows:

Proposition. *A $0,1$-sequence u_n is Sturmian if and only if*

- *it is non-eventually periodic,*
- *the number of 1's in any pair of finite subsegments of the same length occurring in u_n can differ by at most one.*

It is known that the sequence $x_n = c_I(\{n\alpha\})$ with a special choice of interval I of length $|I| = \{\alpha\}$ or $|I| = 1 - \{\alpha\}$ is Sturmian.

Sturmian sequences are usually defined as $\{0,1\}$-sequences rather than $\{-1,1\}$-sequences, but the mutual transformations of these forms are straightforward.

If x_n, $n = 1, 2 \ldots$, is a binary $\{-1, 1\}$-sequence then Mauduit & Sárközy proposed to use the following pseudorandomness measure of x_n, $n = 1, \ldots, N$, $N \in \mathbb{N}$ for such sequences and they called it the **well distribution measure**

$$W_N = W_N(x_n) = \max_{n,K,D} \left| \sum_{k=1}^{D} x_{n+kK} \right|$$

where the maximum is taken over all n, K, D such that $n, K, D \in \mathbb{N}$ and $1 \leq n + K \leq n + DK \leq N$.

If x_n, $n = 1, 2 \ldots$, is a binary $\{-1, 1\}$-sequence then MAUDUIT & SÁRKÖZY proposed to use the following pseudorandomness measure of x_n, $n = 1, \ldots, N$, $N \in \mathbb{N}$ for such sequences and they called it the **well distribution measure**

$$W_N = W_N(x_n) = \max_{n,K,D} \left| \sum_{k=1}^{D} x_{n+kK} \right|$$

where the maximum is taken over all n, K, D such that $n, K, D \in \mathbb{N}$ and $1 \leq n + K \leq n + DK \leq N$.

This well distribution measure was proposed by them as one of three measures for measuring the pseudorandomness of binary $\{-1, 1\}$-sequences.

The third measure was the **correlation measure** of order k of x_n

$$C_{k,N}(x_n) = \max_{M,\mathbf{d}} \left| \sum_{n=1}^{M} x_{n+d_1} x_{n+d_2} \dots x_{n+d_k} \right|$$

where the maximum is taken over all $\mathbf{d} = (d_1, d_2, \dots, d_k)$, $d_1 < d_2 < \dots d_k$, and M such that $M + d_k \leq N$.

Cassaigne, Mauduit & Sárközy showed that for a „truly random“[1] $x_1, \dots, x_N$, both W_N and $C_{k,N}$ for fixed k, are around $\sqrt{N}$ with „near 1“ probability.

$\Rightarrow$ for a „really good“ N term pseudorandom sequence we expect both measures to be not much greater than $\sqrt{N}$

[1] Each $\{x_n\}_{n=1}^{N} \in \{-1, 1\}$ is chosen with probability $1/2^N$.

If

$$m(N) = \min_{x_n \in \{-1,1\}^N} W_N(x_n)$$

then

- Roth proved that $m(N) > c_1 N^{1/4}$,
- Matoušek & Spencer showed that $m(N) < c_2 N^{1/4}$,

so that the order of magnitude of $m(N)$ is known.

Matoušek, J., Spencer, J.: *Discrepancy in arithmetic progressions*, J. Amer. Math. Soc. **9** (1996), 195–204
Roth, K.F.: *Remark concerning integer sequences*, Acta Arith. **9** (1964), 257–260

A prophetical prognosis:

In early 1996, P.Erdős, learning about the first results of MAUDUIT & SÁRKÖZY suggested to study the pseudorandom properties of several sequences. One of the construction given by him was the following: write

$$\chi(x) = \begin{cases} 1, & \text{if } 0 \le \{x\} < 1/2, \text{ and} \\ -1, & \text{if } 1/2 \le \{x\} < 1. \end{cases}$$

and define $x_n = \chi(n\alpha)$ with α irrational. After a short thinking, he said: *This will be a negative example*.

A prophetical prognosis:

In early 1996, P.Erdős, learning about the first results of MAUDUIT & SÁRKÖZY suggested to study the pseudorandom properties of several sequences. One of the construction given by him was the following: write

$$\chi(x) = \begin{cases} 1, & \text{if } 0 \le \{x\} < 1/2, \text{ and} \\ -1, & \text{if } 1/2 \le \{x\} < 1. \end{cases}$$

and define $x_n = \chi(n\alpha)$ with α irrational. After a short thinking, he said: *This will be a negative example*. Then he asked: *What about replacing n by n^2?* After a little more thinking he said briefly: *Perhaps*.

It turned out that Erdős was more or less right: the case $\{n\alpha\}$ is a negative example in the sense that the correlation is large, while well-distribution could be small (e.g. in the case of bounded partial fractions) !!!!

Mauduit, Ch., Sárközy, A.: *On finite pseudorandom binary sequences, V. On* $(n\alpha)$ *and* $(n^2\alpha)$ *sequences*, Monatsh. Math.**129** (2000), 197–216.

Mauduit and Sárközy investigated (among other) binary $\{-1, 1\}$-sequences defined by $x_n = \chi_I(\{\alpha n\})$ with $I = [0, 1/2)$ and α irrational, where

$$\chi_I(y) = \begin{cases} 1, & \text{if } y \in I, \text{ and} \\ -1, & \text{if } y \notin I. \end{cases}$$

They proved that:

(a) If α is an irrational number, $N \in \mathbb{N}$, and $x_n = \chi_{[0,1/2)}(\{n\alpha\})$, $n = 1, \ldots, N$, then

$$W_N(x_n) \geq \sqrt{N/2}.$$

They proved that:

(a) If α is an irrational number, $N \in \mathbb{N}$, and $x_n = \chi_{[0,1/2)}(\{n\alpha\})$, $n = 1, \ldots, N$, then

$$W_N(x_n) \geq \sqrt{N/2}.$$

(b) If moreover α is an irrational number whose partial quotients in the continued fraction expansion of α are bounded by a $K \in \mathbb{N}$, then

$$W_N(x_n) \leq 6 \left(\frac{K}{\log(K+1)} \right)^{1/2} (N \log N)^{1/2} + 1.$$

We shall study the pseudorandomness of sequences $x_n = \chi_I(\{\alpha n\})$ with an arbitrary interval $I \subset [0, 1]$.

We shall study the pseudorandomness of sequences $x_n = \chi_I(\{\alpha n\})$ with an arbitrary interval $I \subset [0,1]$.

Our approach is based on the study of combinatorial properties of set $A = A(\alpha, I)$ defined by

$$A = A(\alpha, I) = \{n \in \mathbb{N} : \{n\alpha\} \in I\},$$

where I is a fixed but arbitrary subinterval of $[0,1]$.

Our motivation to study of the set $A = A(\alpha, I) = \{a_1 < a_2 \dots\}$ has several historical sources:

One of them is **three gaps problem** saying that the differences $a_{i+1} - a_i$ attain at most three distinct values of the form $a, b, a + b$, where a is the first positive integer for which $\{a\alpha\} \in (0, |I|)$ and b is first one such that $\{b\alpha\} \in (1 - |I|, 1))$.

This problem was introduced and proved by N.B.Slater in 1950.

The three gaps problem is directly connected with the so called Steinhaus' **three steps problem** asserting:

If the sequence $\{1\alpha\}, \{2\alpha\}, \ldots, \{N\alpha\}$ with an irrational α is re-ordered with respect to the increasing magnitude of its terms, say $\{n_1\alpha\} < \{n_2\alpha\} < \cdots < \{n_N\alpha\}$, then for every $i = 1, 2, \ldots, N-1$ we have $\{n_{i+1}\alpha\} - \{n_i\alpha\} = d_1$ or d_2 or $d_1 + d_2$ where $d_1 = \{n_1\alpha\}$ and $d_2 = 1 - \{n_N\alpha\}$.

This was proved independently by J.Surányi in 1958, V.T.Sós in 1958 and others.

Theorem (Slater). *Given an interval I of the form $I = (0, t)$, $t \leq 1/2$, define a and b as the least positive integers such that $\{a\alpha\} \in (0, t)$ and $\{b\alpha\} \in (1-t, 1)$. Let $\{n\alpha\} \in (0, t)$ and let k be minimal with $\{(n+k)\alpha\} \in (0, t)$. Then*

$$k = \begin{cases} a, & \text{if } 0 \leq \{n\alpha\} < t - \{a\alpha\}, \\ a + b, & \text{if } t - \{a\alpha\} \leq \{n\alpha\} < 1 - \{b\alpha\}, \\ b, & \text{if } 1 - \{b\alpha\} \leq \{n\alpha\} < t. \end{cases}$$

Moreover a and b are relatively prime.

Theorem (Slater). *Given an interval I of the form $I = (0, t)$, $t \leq 1/2$, define a and b as the least positive integers such that $\{a\alpha\} \in (0, t)$ and $\{b\alpha\} \in (1 - t, 1)$. Let $\{n\alpha\} \in (0, t)$ and let k be minimal with $\{(n + k)\alpha\} \in (0, t)$. Then*

$$k = \begin{cases} a, & \text{if } 0 \leq \{n\alpha\} < t - \{a\alpha\}, \\ a + b, & \text{if } t - \{a\alpha\} \leq \{n\alpha\} < 1 - \{b\alpha\}, \\ b, & \text{if } 1 - \{b\alpha\} \leq \{n\alpha\} < t. \end{cases}$$

Moreover a and b are relatively prime.

Slater's theorem says not only that $\Delta = \{a_{n+1} - a_n : n \in \mathbb{N}\}$ is finite, but that in addition it has at most three distinct elements.

Theorem. *Let I be an arbitrary interval of $(0,1)$. Let N be such an integer that the sequence $\{1\alpha\},\{2\alpha\},\ldots,\{N\alpha\}$ meets both intervals $(0,|I|/2)$, and $(1-|I|/2,1)$. Let the function $k(x)$ be defined for $x\in[0,|I|]$ as* [2]

$$k(x)=\min\Big\{\min\{i\le N:\{i\alpha\}\in(0,x)\},\ \min\{i\le N:\{i\alpha\}\in(1-|I|+x,1)\}\Big\}.$$

Then we have:

(i) the set Δ coincides with the set $\{k(x):x\in[0,|I|]\}$,

(ii) the function $k(x)$ and the set Δ depend only on the length $|I|$ of interval I but not on the position of I within $(0,1)$,

[2] Here we use the convention that $\min\emptyset=\infty$.

Let $\alpha = (\sqrt{5}+1)/2$ and $I = (1/2, 1)$. The N in Theorem is $N = 3$, where $\{\alpha\} = 0.61\ldots$, $\{2\alpha\} = 0.23\ldots$ and $\{3\alpha\} = 0.85\ldots$.

Let $\alpha = (\sqrt{5}+1)/2$ and $I = (1/2, 1)$. The N in Theorem is $N = 3$, where $\{\alpha\} = 0.61\ldots$, $\{2\alpha\} = 0.23\ldots$ and $\{3\alpha\} = 0.85\ldots$. Then for $x = 0.15$ the minimum $k(x) = \min\{\min\emptyset, \min\{3\}\} = 3$, for $x = 0.23$ it is $k(x) = \min\{\min\{2\}, \min\{3\}\} = 2$ and for $x = 0.5$ it is $k(x) = \min\{\min\{2\}, \min\{1, 3\}\} = 1$.

Let $\alpha = (\sqrt{5}+1)/2$ and $I = (1/2, 1)$. The N in Theorem is $N = 3$, where $\{\alpha\} = 0.61\ldots$, $\{2\alpha\} = 0.23\ldots$ and $\{3\alpha\} = 0.85\ldots$. Then for $x = 0.15$ the minimum $k(x) = \min\{\min\emptyset, \min\{3\}\} = 3$, for $x = 0.23$ it is $k(x) = \min\{\min\{2\}, \min\{3\}\} = 2$ and for $x = 0.5$ it is $k(x) = \min\{\min\{2\}, \min\{1, 3\}\} = 1$. Thus the shortest distances between $a_i, a_j \in A$ are $1, 2$, or 3 only, and each of them is realized infinitely many times.


1010010110100101101011010010110100101001011010010110101101
0010110100101001011010010110100101001011010010110101101001
0110100101001011010010110101101001011010010110101101001011
0100101001011010010110101101001011010010100101101001011010
0101001011010010110101101001011010010100101101001011010110
1001011010010110101101001011010010100101101001011010110100
1011010010100101101001011010110100101101001011010110100101
1010010100101101001011010110100101101001010010110100101101
0010100101101001011010110100101101001010010110100101101011
0100101101001011010110100101101001010010110100101101011010
0101101001010010110100101101001010010110100101101011010010
1101001010010110100101101011010010110100101001011010010110
1001010010110100101101011010010110100101001011010010110101

101001011010010110101101001011010010100101101001011010110100101101010011010010110101101001011010010110101101001011010010100101101001011010110100101101001011010010110101101001011010010100101101001011010011010010110100

In some cases we are able to give the differences a and b explicitly.

Theorem. *Suppose that* $|I| \leq 1/2$ *and denote* $B = \{k \in \mathbb{N} : \{k\alpha\} \in (|I|, 1 - |I|)\}$. *Then*

(a) If $k \in B$ *then the equation* $a_j - a_i = k$ *is not solvable in* $a_i, a_j \in A$;

(b) If $k \notin B$ *then the equation* $a_j - a_i = k$ *has infinitely many solutions in* $a_i, a_j \in A$ *with the exception, when* $\{k\alpha\} = |I|$ *or if* $1 - \{k\alpha\} = |I|$ *and* I *is closed, in which case it possesses at most one solution.*

Take $I = (0, 1/3)$ and $\alpha = (1 + \sqrt{5})/2$. Then the initial segment of set A is $\{2,\ 5,\ 7,\ 10,\ 13,\ 15,\ 18,\ 23,\ 26,\ 28,\ 31,\ 34,\ 36,\ 39,\ 44,\ 47,\ 49,\ 52,\ 57,\ 60,\ 62,\ 65,\ 68,\ 70,\ 73,\ 78,\ 81,\ 83,\ 86,\ 89,\ 91,\ 94,\ 96,\ 99,\ \ldots\}$ and the initial segment of the set B for which elements k_s the equation $a_j - a_i = k_s$ has no solution in A is $\{1,\ 4,\ 9,\ 12,\ 14,\ 17,\ 20,\ 22,\ 25,\ 30,\ 33,\ 35,\ 38,\ 41,\ 43,\ 46,\ 48,\ 51,\ 54,\ 56,\ 59,\ 64,\ 67,\ 69,\ 72,\ 75,\ 77,\ 80,\ 85,\ 88,\ 90,\ 93,\ 98,\ \ldots\}$.

Lemma. *The set A contains an arbitrarily long arithmetic progression. More precisely, let $D \in \mathbb{N}$ be given, and $K_1, K_2 \in \mathbb{N}$ be such that*

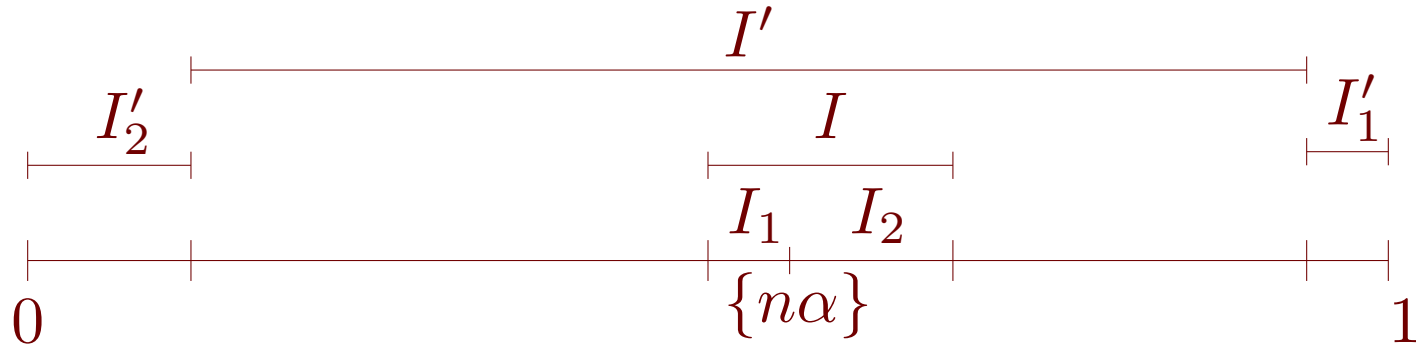
$$|1 - \{K_1\alpha\}| < \frac{|I|}{2D},$$
$$|0 - \{K_2\alpha\}| < \frac{|I|}{2D}.$$

Then for every $n \in A$ either

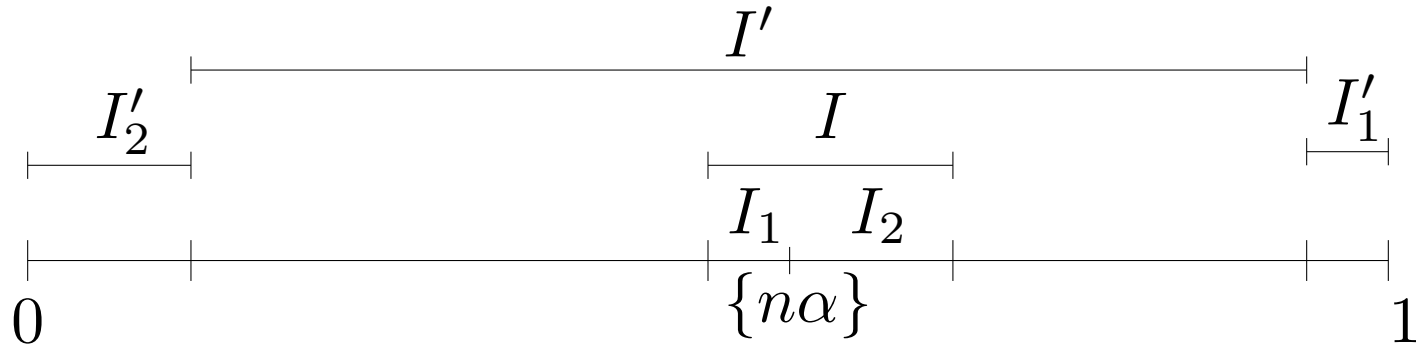
$$\{n, n + K_1, n + 2K_1, \ldots, n + DK_1\} \subset A$$

or

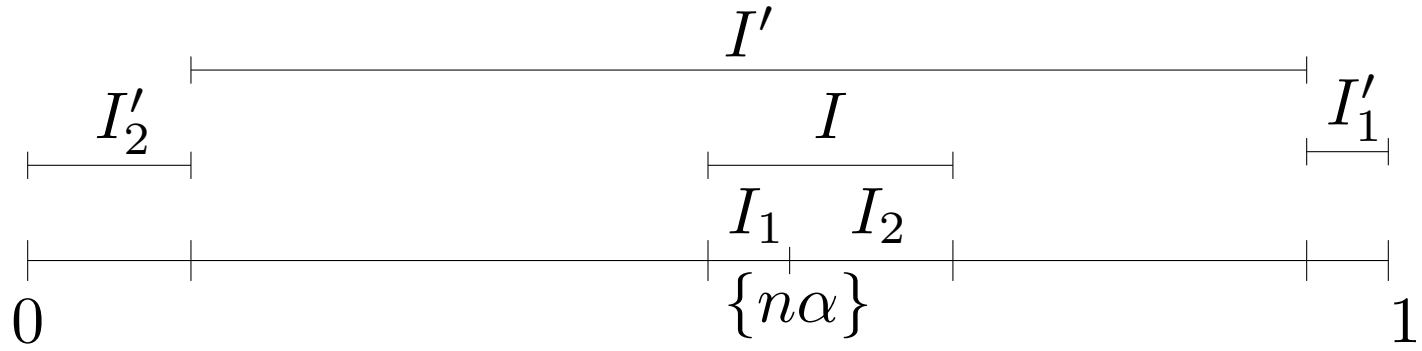
$$\{n, n + K_2, n + 2K_2, \ldots, n + DK_2\} \subset A.$$



Let $n \in A$, i.e. $\{n\alpha\} \in I$. The point $\{n\alpha\}$ splits interval I into two subintervals, say I_1, the left one, and I_2, the right one, respectively.



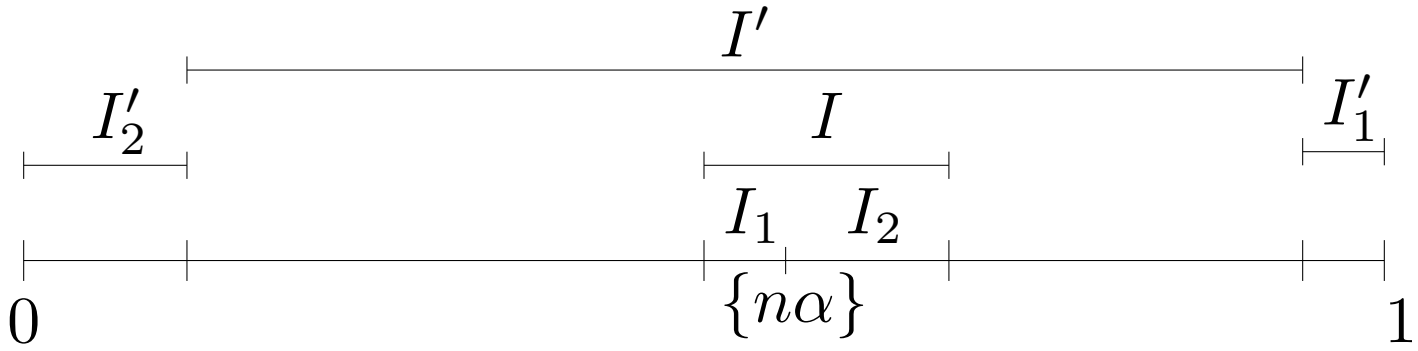
Let $n \in A$, i.e. $\{n\alpha\} \in I$. The point $\{n\alpha\}$ splits interval I into two subintervals, say I_1, the left one, and I_2, the right one, respectively. Translate these intervals towards the endpoints of $[0, 1]$ as follows: $I'_1 = I_1 + 1 - \{n\alpha\}$ and $I'_2 = I_2 - \{n\alpha\}$.



Let $n \in A$, i.e. $\{n\alpha\} \in I$. The point $\{n\alpha\}$ splits interval I into two subintervals, say I_1, the left one, and I_2, the right one, respectively. Translate these intervals towards the endpoints of $[0, 1]$ as follows: $I'_1 = I_1 + 1 - \{n\alpha\}$ and $I'_2 = I_2 - \{n\alpha\}$.

Then

$$\{(n+k)\alpha\} \in I_1 \Leftrightarrow \{k\alpha\} \in I'_1$$
$$\{(n+k)\alpha\} \in I_2 \Leftrightarrow \{k\alpha\} \in I'_2.$$

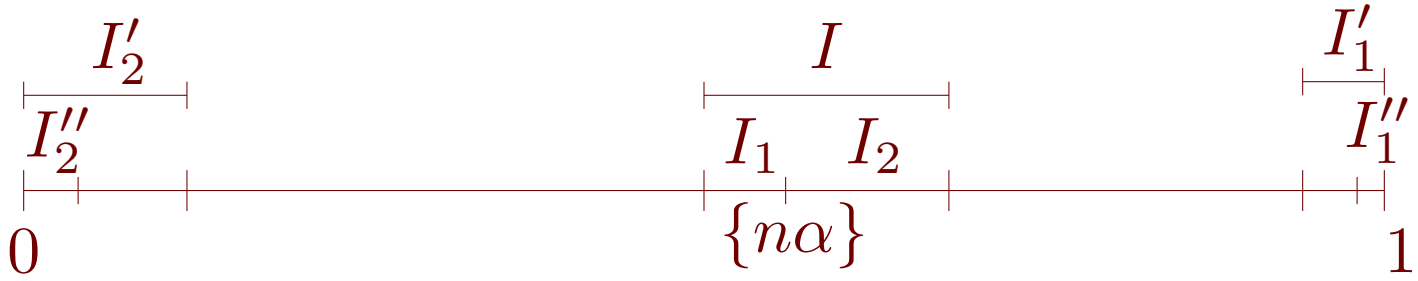


Let $n \in A$, i.e. $\{n\alpha\} \in I$. The point $\{n\alpha\}$ splits interval I into two subintervals, say I_1, the left one, and I_2, the right one, respectively. Translate these intervals towards the endpoints of $[0, 1]$ as follows: $I'_1 = I_1 + 1 - \{n\alpha\}$ and $I'_2 = I_2 - \{n\alpha\}$.

Then

$$\{(n+k)\alpha\} \in I_1 \Leftrightarrow \{k\alpha\} \in I'_1$$
$$\{(n+k)\alpha\} \in I_2 \Leftrightarrow \{k\alpha\} \in I'_2.$$

In other words, $\{(k+n)\alpha \in I\} \Leftrightarrow \{k\alpha\} \notin I'$.



Given D, let the intervals I_1'' and I_2'' of lengths $|I_1''| = |I_1'|/D$ and $|I_2''| = |I_2'|/D$, respectively, be located as depicted in the figure. Then

$$\{K_1\alpha\} \in I_1'' \Rightarrow \{kK_1\alpha\} \in I_1' \quad \text{for every } k = 1, 2\ldots, D,$$

$$\{K_2\alpha\} \in I_2'' \Rightarrow \{kK_2\alpha\} \in I_2' \quad \text{for every } k = 1, 2\ldots, D.$$

Since the sequence $\{(n+kK)\alpha\}$, $k = 1, 2, \ldots$, is uniformly distributed in $[0, 1]$ for irrational α, the set A does not contain an infinite arithmetic sequence.

Since the sequence $\{(n+kK)\alpha\}$, $k = 1, 2, \ldots$, is uniformly distributed in $[0, 1]$ for irrational α, the set A does not contain an infinite arithmetic sequence.

But Lemma implies that A contains infinite double-arithmetic sequences of the following type

Theorem. *Let $D \in \mathbb{N}$, and K_1, K_2 satisfy conditions of the Lemma. Then for every given $n \in A$ the set A contains an infinite double arithmetic sequence of the form $n, n + K_{i_1}, n + 2K_{i_1}, \ldots, n + DK_{i_1}, n + DK_{i_1} + K_{i_2}, n + DK_{i_1} + 2K_{i_2}, \ldots, n + DK_{i_1} + DK_{i_2}, n + DK_{i_1} + DK_{i_2} + K_{i_3}, \ldots$, where $i_1, i_2, i_3, \cdots \in \{1, 2\}$, and K_{i_s}, $K_{i_{s+1}}$ need not be different.*

Consider an arbitrary subsequence x_{n+kK}, $k = 0, 1, 2 \ldots$, of $x_j = \chi_I(\{j\alpha\})$, $j = 1, 2, \ldots$, satisfying conditions $x_n = x_{n+K} = 1$. Split this subsequence x_{n+kK} into blocks of 1's of lengths $D_0, D_2, \ldots$, and blocks of -1's of lengths $D_1, D_3, \ldots$, that is

$$x_n = x_{n+K} = x_{n+2K} = \cdots = x_{n+D_0K} = 1,$$

$$x_{n+(D_0+1)K} = x_{n+(D_0+2)K} = \cdots = x_{n+(D_0+D_1)K} = -1,$$

$$x_{n+(D_0+D_1+1)K} = x_{n+(D_0+D_1+2)K} = \cdots = x_{n+(D_0+D_1+D_2)K} = 1,$$

$$\ldots.$$

Theorem. *Let the number $D_0, D_1, D_2, D_3, \ldots$ be defined as above.*

(i) If $|I| \leq 1/2$, then there exist integers $D^{(1)}$ and $D^{(2)}$ such that

$$|D_{2i-1} - D^{(1)}| \leq 1, \quad \text{and} \quad |D_{2i} - D^{(2)}| \leq 1 \qquad (*)$$

for every $i = 1, 2, \ldots$.

(ii) If $|I| = 1/2$ then $D^{(1)} = D^{(2)}$.

(iii) If $|I| > 1/2$ and $\{K\alpha\} < 1 - |I|$ then there exist integers $D^{(1)}$ and $D^{(2)}$ such that $(*)$ again holds.

Theorem. *Let $\alpha = [a_0; a_1, a_2, \dots]$ be the continued fraction expansion of a given irrational α. Assume that $\{\alpha\} \in I$ and that it divides the interval I into two subintervals I_1 and I_2. Put*

$$M_i = q_n \left\lfloor |I_i|\, q_n \left(r_{n+1} + \frac{q_{n-1}}{q_n} \right) \right\rfloor \qquad \text{for} \quad i = 1, 2,$$

where $r_{n+1} = [a_{n+1}; a_{n+2}, a_{n+3} \dots]$ and $\frac{p_n}{q_n} = [a_0; a_1, a_2, \dots, a_n]$. Then

$$W_{M_i} \geq \sqrt{M_i} \sqrt{|I_i| a_{n+1}}$$

for odd n if $i = 1$ and for even n if $i = 2$, provided $q_{n-1} > \max(1/|I_1|, 1/|I_2|)$.

Theorem. *Given an irrational* α *and an arbitrary interval* $I \subset [0,1]$*, the inequality*

$$W_M \geq \frac{\max(|I|, 1-|I|)}{2D_{\lfloor\sqrt{M}\rfloor}},$$

holds for all sufficiently large M*, where* $D_{\lfloor\sqrt{M}\rfloor}$ *is the extremal discrepancy of the sequence* $\{1\alpha\}, \{2\alpha\}, \ldots, \{\lfloor\sqrt{M}\rfloor\alpha\}$*.*

Theorem. *If α is an algebraic irrational and $I \subset [0,1]$ is an arbitrary interval, then*

$$W_M = M|1 - 2|I|\,| + O(M^{\frac{1}{2}+\varepsilon}).$$

for every $\varepsilon > 0$.

Thank you!