J. Math. Kyoto Univ. (JMKYAZ)
44-2 (2004), 365–380

A dependence vanishing theorem for sequences generated by Weyl transformation

By

Kenji Yasutomi

1. Introduction

Let us develop a real number x into the binary expansion, take the sum of the first m digits under the decimal point, divide the sum by 2, and denote the remainder by $X^{(m)}(x)$. Sugita [2] conjectured that, when α is irrational and m is large, the process $X^{(m)}(\omega)$, $X^{(m)}(\omega+\alpha)$, $X^{(m)}(\omega+2\alpha)$, $\ldots$ is almost i.i.d. on the Lebesgue space $([0,1),\lambda)$, and proved that

$$(*) \qquad \begin{array}{l}\{X^{(m)}(\cdot+n\alpha)\}_{n\in\mathbb{N}} \text{ converges in law to } \{0,1\}\text{-valued fair i.i.d.}\\ \text{as } m\to\infty\end{array}$$

for all normal numbers α. Although the process $\{X^{(m)}(\cdot+n\alpha)\}_{n\in\mathbb{N}}$ is generated by α-rotation and has strong dependence, the mysterious conjecture claims that the dependence vanishes when m is large. In this paper, we give the affirmative answer to the conjecture and prove the convergence $(*)$ for all irrational α.

Various studies [3, 5] were done on this problem. We [6, 7] proved the convergence $(*)$ for a.e. α and for normal α by using a standard technique of Markov chain. In this paper, we apply the technique from a different point of view, and prove the final result.

2. Result and some comments

For real number $x\geq 0$, let $\lfloor x\rfloor$ be the integral part of x, i.e., $\lfloor x\rfloor := \max\{n\in\mathbb{Z}\mid x\geq n\}$.

Let $b\geq 2$ be an integer and $d^{(j)}(x)$ the j-th digit of decimal part of $x\geq 0$ in its base-b expansion, i.e., $d^{(j)}(x):=\lfloor b^j x\rfloor - b\lfloor b^{j-1}x\rfloor$.

For a fixed irrational number α and $m\in\mathbb{N}$, we define $\mathbb{Z}/b\mathbb{Z}$-valued function $X_l^{(m)}$ on $[0,1)$ by

$$X_l^{(m)}(\omega) :\equiv \sum_{1\leq j\leq m} d^{(j)}(\omega+l\alpha)$$

Received May 30, 2003
Revised April 13, 2004

where $z \equiv z'$ means that $z = z'$ modulo b for $z, z' \in \mathbb{Z}$.

Our main theorem is as follows:

Theorem 1. *If b is prime and α is irrational, then the distribution of the process $\{X_l^{(m)}\}_{l=0}^{\infty}$ on the Lebesgue space $([0,1), \lambda)$ converges weakly to the distribution of $\mathbb{Z}/b\mathbb{Z}$-valued fair i.i.d. when m tends to ∞.*

When $b = 2$, Theorem 1 reduces to the conjectured result.

The condition that b is prime, which is equivalent to that $\mathbb{Z}/b\mathbb{Z}$ is a finite field, is used only in Section 4 to show the strong irreducibility on $\mathbb{Z}/b\mathbb{Z}$. Precisely, this condition is necessary for our proof of Lemma 4. But, it may be not so for the statement of that, hence Theorem 1. We believe that this assumption is technical and thus can be removed.

In the first draft, our underlying probability measure was so general μ that $\{d^{(j)}\}_{j>0}$ are independent random variables under μ with

$$\liminf_{j\to\infty} \min_{0\le s<b} \mu(d^{(j)} = s) > 0.$$

It should be noted that, under this setting, we [7] have proved Theorem 1, where λ is replaced by μ and $b \geq 2$ only is an integer (i.e., it need not be prime), but only α is normal. For those μ, everything in Section 3 proceeds with no problem. At the beginning of Section 4, however, we fail in the reduction stated there. If, for instance, we assume that $\{d^{(j)}(\cdot + \beta)\}_{j\geq 1}$ is independent for *all* β, then we can prevent this failure. But, this assumption is too convenient for us and indeed, from it the trivial case occurs, that is, such μ's satisfying it are only the Lebesgue measure λ. So, from this observation, we have restricted underlying probability space to the Lebesgue space. Similarly as the case of b, we are convinced that this restriction for μ can the removed, and hence, under the above setting, Theorem 1 holds for all $b \geq 2$ and all irrational α.

3. Proof of Theorem 1

Let μ be as above, $b \geq 2$ an integer and α irrational. Throughout this section, our underlying probability space is $([0,1), \mathcal{B}([0,1)), \mu)$, unless otherwise stated.

The aim of this section is to find the condition on μ under which Theorem 1 holds with λ replaced by μ, in a word, it holds that

$$\int_{[0,1)} f(X_0^{(m)}, \dots, X_n^{(m)}) d\mu \to \frac{1}{b^{n+1}} \sum_{\mathbf{e}\in(\mathbb{Z}/b\mathbb{Z})^{n+1}} f(\mathbf{e}) \tag{1}$$

for each n and for each complex function f on $(\mathbb{Z}/b\mathbb{Z})^{n+1}$.

We fix n and define $(\mathbb{Z}/b\mathbb{Z})^{n+1}$-valued functions $\mathbf{d}^{(j)}$ and $\mathbf{X}^{(m)}$ by

$$\mathbf{d}^{(j)}(\omega) := (d^{(j)}(\omega), d^{(j)}(\omega+\alpha), \dots, d^{(j)}(\omega+n\alpha)),$$

$$\mathbf{X}^{(m)} := (X_0^{(m)}, X_1^{(m)}, \dots, X_n^{(m)}) \equiv \sum_{j=1}^{m} \mathbf{d}^{(j)} \quad \text{for} \quad m \geq 1,$$

and $\mathbf{X}^{(0)} := \mathbf{0} \in (\mathbb{Z}/b\mathbb{Z})^{n+1}$.

Since $\{d^{(j)}\}_j$ is an independent process, $\{X_0^{(m)}\}_m \equiv \{\sum_{1\le j\le m} d^{(j)}\}_m$ is a Markov chain. But, since $\{\mathbf{d}^{(j)}\}_j$ is not independent, we cannot easily see that $\{\mathbf{X}^{(m)}\}_m \equiv \{\sum_{1\le j\le m} \mathbf{d}^{(j)}\}_m$ is a Markov chain. Thus, we introduce a process $\{\mathbf{Z}^{(m)}\}_m$ to manage the dependence among $\{\mathbf{d}^{(j)}\}_j$. Define $\{0,\dots,2b-1\}^n$-valued function $\mathbf{Z}^{(m)} = (Z_1^{(m)},\dots,Z_n^{(m)})$ by

$$\begin{aligned} Z_l^{(m)}(\omega) &:= \Big\lfloor b^m\omega - b\lfloor b^{m-1}\omega\rfloor + b^m l\alpha - b\lfloor b^{m-1}l\alpha\rfloor\Big\rfloor \\ &= \lfloor b^m(\omega+l\alpha)\rfloor - b(\lfloor b^{m-1}\omega\rfloor + \lfloor b^{m-1}l\alpha\rfloor). \end{aligned}$$

Then, we have that

$$\begin{aligned} Z_l^{(m)}(\omega) &= d^{(m)}(\omega+l\alpha) + b(\lfloor b^{m-1}(\omega+l\alpha)\rfloor - \lfloor b^{m-1}\omega\rfloor - \lfloor b^{m-1}l\alpha\rfloor) \\ &\equiv d^{(m)}(\omega+l\alpha), \end{aligned}$$

and $\mathbf{d}^{(m)} \equiv (d^{(m)}, \mathbf{Z}^{(m)})$. Furthermore, we can say that $\mathbf{Z}^{(1)}$, $\mathbf{Z}^{(2)}$, … is a backward Markov chain, i.e., …, $\mathbf{Z}^{(2)}$, $\mathbf{Z}^{(1)}$ is a Markov chain:

Proposition 1. *The process $\{\mathbf{Z}^{(m)}\}_{m=\infty}^{1}$ is a Markov chain.*

Proof. Let $m' < m$. By the definition of $d^{(j)}$,

$$\sum_{j=m'}^{m-1} b^{m'-j} d^{(j)}(x) = b^{m'-m+1}\lfloor b^{m-1}x\rfloor - b\lfloor b^{m'-1}x\rfloor,$$

and hence, by letting $m \to \infty$

$$\sum_{j=m'}^{\infty} b^{m'-j} d^{(j)}(x) = b^{m'}x - b\lfloor b^{m'-1}x\rfloor.$$

From the first expression, it follows that

$$\begin{aligned} Z_l^{(m')}(\omega) &= \Big\lfloor b^{m'-m}\lfloor b^m(\omega+l\alpha)\rfloor - b(\lfloor b^{m'-1}\omega\rfloor + \lfloor b^{m'-1}l\alpha\rfloor)\Big\rfloor \\ &= \Big\lfloor b^{m'-m}(Z_l^{(m)}(\omega) + b(\lfloor b^{m-1}\omega\rfloor + \lfloor b^{m-1}l\alpha\rfloor)) \\ &\qquad - b(\lfloor b^{m'-1}\omega\rfloor + \lfloor b^{m'-1}l\alpha\rfloor)\Big\rfloor \\ &= \left\lfloor b^{m'-m}Z_l^{(m)}(\omega) + \sum_{j=m'}^{m-1} b^{m'-j}(d^{(j)}(\omega) + d^{(j)}(l\alpha))\right\rfloor, \end{aligned} \tag{2}$$

and from the second expression

$$Z_l^{(m')}(\omega) = \left\lfloor \sum_{j=m'}^{\infty} b^{m'-j}(d^{(j)}(\omega) + d^{(j)}(l\alpha))\right\rfloor \tag{3}$$

where $1 \le l \le n$.

Let us define a random transformation $\mathbf{\Phi}^{(m,m')}$ on $\{0, \dots, 2b-1\}^n$ by

$$\phi_l^{(m,m')}(\omega; z) = \left\lfloor b^{m'-m} z + \sum_{m' \le j < m} b^{m'-j}(d^{(j)}(\omega) + d^{(j)}(l\alpha)) \right\rfloor$$

and

$$\mathbf{\Phi}^{(m,m')}(\omega; z_1, \dots, z_n) = (\phi_1^{(m,m')}(\omega, z_1), \dots, \phi_n^{(m,m')}(\omega, z_n)),$$

where $z, z_1, \dots, z_n \in \{0, \dots, 2b-1\}$.

Then, we have that $\mathbf{Z}^{(m')}(\omega) = \mathbf{\Phi}^{(m,m')}(\omega; \mathbf{Z}^{(m)}(\omega))$ by (2), that $\omega \mapsto \mathbf{\Phi}^{(m,m')}(\omega; \cdot)$ is $\sigma(d^{(m')}, \dots, d^{(m-1)})$-measurable by definition, and that $\mathbf{Z}^{(m)}$ is $\sigma(d^{(m)}, d^{(m+1)}, \dots)$-measurable by (3). Thus, the independence of $\{d^{(j)}\}_j$ implies that

$$\begin{aligned}
&\mu\Big(\mathbf{Z}^{(m')}(\omega) \in * \,\Big|\, \sigma(d^{(m)}, d^{(m+1)}, \dots)\Big) \\
&= \mu\Big(\mathbf{\Phi}^{(m,m')}(\omega; \mathbf{Z}^{(m)}(\omega)) \in * \,\Big|\, \sigma(d^{(m)}, d^{(m+1)}, \dots)\Big) \\
&= \mu(\mathbf{\Phi}^{(m,m')}(\omega; \mathbf{z}) \in *)\Big|_{\mathbf{z}=\mathbf{Z}^{(m)}(\omega)},
\end{aligned}$$

which shows the Markov property of $\{\mathbf{Z}^{(m)}\}_{m=\infty}^1$. □

From the following proposition, we can say that '$\{(\mathbf{X}^{(\infty)} - \mathbf{X}^{(m-1)}, \mathbf{Z}^{(m)})\}_{m=\infty}^1 \equiv \{(\sum_{m \le j \le \infty} \mathbf{d}^{(j)}, \mathbf{Z}^{(m)})\}_{m=\infty}^1$' is a Markov chain:

Proposition 2. *For each $M \in \mathbb{N}$, the $(\mathbb{Z}/b\mathbb{Z})^{n+1} \times \{0, \dots, 2b-1\}^n$-valued process $\{(\mathbf{X}^{(M)} - \mathbf{X}^{(m-1)}, \mathbf{Z}^{(m)})\}_{m=M,\dots,1}$ is a Markov chain with the transition probability*

$$\widetilde{P}^{(m,m')}_{(\mathbf{e},\mathbf{z}),(\mathbf{e}',\mathbf{z}')} = \mu\left(\sum_{m' \le j < m} (d^{(j)}, \mathbf{\Phi}^{(m,j)}(\mathbf{z})) \equiv \mathbf{e}' - \mathbf{e}, \mathbf{\Phi}^{(m,m')}(\mathbf{z}) = \mathbf{z}' \right),$$

where $1 \le m' < m \le M$, $\mathbf{e}, \mathbf{e}' \in (\mathbb{Z}/b\mathbb{Z})^{n+1}$ and $\mathbf{z}, \mathbf{z}' \in \{0, \dots, 2b-1\}^n$.

Proof. Let $1 \le m' < m \le M$ and let B_m be an arbitrary $\sigma((\mathbf{X}^{(M)} - \mathbf{X}^{(j-1)}, \mathbf{Z}^{(j)}); j = M, \dots, m)$-measurable set. Since $\mathbf{Z}^{(j)}$ is $\sigma(d^{(j)}, d^{(j+1)}, \dots)$-measurable and $\mathbf{X}^{(M)} - \mathbf{X}^{(j-1)} \equiv \sum_{k=j}^M \mathbf{d}^{(k)} \equiv (\sum_{k=j}^M d^{(k)}, \sum_{k=j}^M \mathbf{Z}^{(k)})$, B_m and $\mathbf{X}^{(M)} - \mathbf{X}^{(m-1)}$ are $\sigma(d^{(m)}, d^{(m+1)}, \dots)$-measurable. Noting that $\mathbf{\Phi}^{(m,m')}(\mathbf{z})$ is $\sigma(d^{(m')}, \dots, d^{(m-1)})$-measurable for each $\mathbf{z}$ and that $\mathbf{d}^{(j)} \equiv (d^{(j)}, \mathbf{Z}^{(j)}) =$

$(d^{(j)}, \mathbf{\Phi}^{(m,j)}(\mathbf{Z}^{(m)}))$, we see from the independence of $\{d^{(j)}\}_j$ that

$$\begin{aligned}
&\mu\big(\mathbf{X}^{(M)} - \mathbf{X}^{(m'-1)} \equiv \mathbf{e}', \mathbf{Z}^{(m')} = \mathbf{z}' \\
&\qquad \big| \ \{\mathbf{X}^{(M)} - \mathbf{X}^{(m-1)} \equiv \mathbf{e}, \mathbf{Z}^{(m)} = \mathbf{z}\} \cap B_m\big) \\
&\quad = \mu\left(\sum_{m' \le j < m} \mathbf{d}^{(j)} \equiv \mathbf{e}' - \mathbf{e}, \mathbf{Z}^{(m')} = \mathbf{z}' \right. \\
&\qquad\qquad \left| \ \{\mathbf{X}^{(M)} - \mathbf{X}^{(m-1)} \equiv \mathbf{e}, \mathbf{Z}^{(m)} = \mathbf{z}\} \cap B_m \right) \\
&\quad = \mu\left(\sum_{m' \le j < m} (d^{(j)}, \mathbf{\Phi}^{(m,j)}(\mathbf{z})) \equiv \mathbf{e}' - \mathbf{e}, \mathbf{\Phi}^{(m,m')}(\mathbf{z}) = \mathbf{z}' \right. \\
&\qquad\qquad \left| \ \{\mathbf{X}^{(M)} - \mathbf{X}^{(m-1)} \equiv \mathbf{e}, \mathbf{Z}^{(m)} = \mathbf{z}\} \cap B_m \right) \\
&\quad = \mu\left(\sum_{m' \le j < m} (d^{(j)}, \mathbf{\Phi}^{(m,j)}(\mathbf{z})) \equiv \mathbf{e}' - \mathbf{e}, \mathbf{\Phi}^{(m,m')}(\mathbf{z}) = \mathbf{z}' \right).
\end{aligned}$$

This implies the conclusion of the proposition. □

Note that $\widetilde{P}^{(m,m')}_{(\mathbf{e},\mathbf{z}),(\mathbf{e}',\mathbf{z}')}$ does not depend on M.

To give a rough sketch of our proof of Theorem 1, let us temporarily assume that the Markov chain $\{(\mathbf{X}^{(\infty)} - \mathbf{X}^{(m-1)}, \mathbf{Z}^{(m)})\}_{m=\infty,\dots,1}$ is strongly irreducible, i.e., for an $\epsilon > 0$ and for each $N \in \mathbb{N}$, there exists a pair (m, m') with $N \le m' < m$ such that

$$\min_{\mathbf{e},\mathbf{z},\mathbf{e}',\mathbf{z}'} \widetilde{P}^{(m,m')}_{(\mathbf{e},\mathbf{z}),(\mathbf{e}',\mathbf{z}')} \ge \epsilon. \tag{4}$$

Then, by a standard method of Markov chain, we have that, for every complex function g on $(\mathbb{Z}/b\mathbb{Z})^{n+1} \times \{0, \dots, 2b-1\}^n$,

$$\begin{aligned}
(\widetilde{P}^{(M,1)} g)(\mathbf{e}, \mathbf{z}) &:= \sum_{\mathbf{e}',\mathbf{z}'} \widetilde{P}^{(M,1)}_{(\mathbf{e},\mathbf{z}),(\mathbf{e}',\mathbf{z}')} g(\mathbf{e}', \mathbf{z}') \\
&\to \frac{1}{b^{n+1}(2b)^n} \sum_{\mathbf{e}',\mathbf{z}'} g(\mathbf{e}', \mathbf{z}') \quad (M \to \infty).
\end{aligned}$$

Let $\varpi : (\mathbb{Z}/b\mathbb{Z})^{n+1} \times \{0, \dots, 2b-1\}^n \to (\mathbb{Z}/b\mathbb{Z})^{n+1}$ be the projection. Then, by Proposition 2,

$$\begin{aligned}
\int_{[0,1)} f(\mathbf{X}^{(M)}) d\mu &= \int_{(\mathbb{Z}/b\mathbb{Z})^{n+1} \times \{0,\dots,2b-1\}^n} (f \circ \varpi) d\mu^{(\mathbf{X}^{(M)}, \mathbf{Z}^{(1)})} \\
&= \int_{(\mathbb{Z}/b\mathbb{Z})^{n+1} \times \{0,\dots,2b-1\}^n} \widetilde{P}^{(M,1)} (f \circ \varpi) d\mu^{(\mathbf{X}^{(M)} - \mathbf{X}^{(M-1)}, \mathbf{Z}^{(M)})}
\end{aligned}$$

$$\to \frac{\sum_{\mathbf{e},\mathbf{z}}(f\circ\varpi)(\mathbf{e},\mathbf{z})}{b^{n+1}(2b)^n} = \frac{1}{b^{n+1}}\sum_{\mathbf{e}} f(\mathbf{e}) \quad (M\to\infty),$$

hence we have the convergence (1).

Unfortunately, the assumption (4) is not true. Since the state space $(\mathbb{Z}/b\mathbb{Z})^{n+1}\times\{0,\ldots,2b-1\}^n$ is too big to be irreducible, we use the following trick to make it reasonable size.

For $\mathbf{e}=(e_0,\ldots,e_n)$, $\widehat{\mathbf{e}}=(\widehat{e}_0,\ldots,\widehat{e}_n)\in(\mathbb{Z}/b\mathbb{Z})^{n+1}$, let $\mathbf{e}\cdot\widehat{\mathbf{e}}$ be the inner product, i.e., $\mathbf{e}\cdot\widehat{\mathbf{e}}=\sum_{l=0}^n e_l\widehat{e}_l$.

Then, for every complex function f on $(\mathbb{Z}/b\mathbb{Z})^{n+1}$,

$$f(\mathbf{e}) = \sum_{\widehat{\mathbf{e}}\in(\mathbb{Z}/b\mathbb{Z})^{n+1}} \widehat{f}(\widehat{\mathbf{e}})\exp\Big(\frac{i2\pi\mathbf{e}\cdot\widehat{\mathbf{e}}}{b}\Big),$$

where

$$\widehat{f}(\widehat{\mathbf{e}}) = \frac{1}{b^{n+1}}\sum_{\mathbf{e}\in(\mathbb{Z}/b\mathbb{Z})^{n+1}} f(\mathbf{e})\exp\Big(\frac{-i2\pi\mathbf{e}\cdot\widehat{\mathbf{e}}}{b}\Big),$$

by the Plancherel theorem (cf. H. Dym-H. P. McKean [1, p. 219]).

Since $\mathbf{X}^{(m)}\cdot\mathbf{0}$ is constant 0,

$$\begin{aligned} f(\mathbf{X}^{(m)}) &= \sum_{\widehat{\mathbf{e}}\in(\mathbb{Z}/b\mathbb{Z})^{n+1}\setminus\{\mathbf{0}\}} \widehat{f}(\widehat{\mathbf{e}})\exp\Big(\frac{i2\pi\mathbf{X}^{(m)}\cdot\widehat{\mathbf{e}}}{b}\Big) + \widehat{f}(\mathbf{0}) \\ &= \sum_{\widehat{\mathbf{e}}\in(\mathbb{Z}/b\mathbb{Z})^{n+1}\setminus\{\mathbf{0}\}} \widehat{f}(\widehat{\mathbf{e}})\exp\Big(\frac{i2\pi\mathbf{X}^{(m)}\cdot\widehat{\mathbf{e}}}{b}\Big) + \frac{1}{b^{n+1}}\sum_{\mathbf{e}\in(\mathbb{Z}/b\mathbb{Z})^{n+1}} f(\mathbf{e}). \end{aligned}$$

Thus, for the convergence (1) it is sufficient to see that

$$\int_{[0,1)} \exp\Big(\frac{i2\pi\mathbf{X}^{(m)}\cdot\widehat{\mathbf{e}}}{b}\Big)d\mu \to 0 \tag{5}$$

for each $\widehat{\mathbf{e}}\in(\mathbb{Z}/b\mathbb{Z})^{n+1}\setminus\{\mathbf{0}\}$.

We fix such an $\widehat{\mathbf{e}}$ from now on, and introduce the following Markov chain:

Lemma 1. *For each $M\in\mathbb{N}$, the $(\mathbb{Z}/b\mathbb{Z})\times\{0,\ldots,2b-1\}^n$-valued process $\{((\mathbf{X}^{(M)}-\mathbf{X}^{(m-1)})\cdot\widehat{\mathbf{e}},\mathbf{Z}^{(m)})\}_{m=M,\ldots,1}$ is a Markov chain with the transition probability*

$$P^{(m,m')}_{(z,\mathbf{z}),(z',\mathbf{z}')} = \mu\left(\sum_{m'\le j<m}(d^{(j)},\mathbf{\Phi}^{(m,j)}(\mathbf{z}))\cdot\widehat{\mathbf{e}} \equiv z'-z, \mathbf{\Phi}^{(m,m')}(\mathbf{z})=\mathbf{z}'\right)$$

for $z,z'\in\mathbb{Z}/b\mathbb{Z}$, $\mathbf{z},\mathbf{z}'\in\{0,\ldots,2b-1\}^n$, and $1\le m'<m\le M$.

Proof is the same as that of Proposition 2.

For $0 < m' < m$ and complex function g on $(\mathbb{Z}/b\mathbb{Z}) \times \{0, \dots, 2b-1\}^n$, define a function $P^{(m,m')}g$ on $(\mathbb{Z}/b\mathbb{Z}) \times \{0, \dots, 2b-1\}^n$ by

$$(P^{(m,m')}g)(z, \mathbf{z}) := \sum_{z', \mathbf{z}'} P^{(m,m')}_{(z,\mathbf{z}),(z',\mathbf{z}')} g(z', \mathbf{z}'),$$

and let $\|\cdot\|_\infty$ be the supremum norm, i.e., $\|g\|_\infty := \max_{z,\mathbf{z}} |g(z, \mathbf{z})|$.

Then, by Lemma 1,

$$\begin{aligned}
&\left| \int_{[0,1)} \exp\left(\frac{i2\pi \mathbf{X}^{(m)} \cdot \widehat{\mathbf{e}}}{b} \right) d\mu \right| \\
&= \left| \int_{(\mathbb{Z}/b\mathbb{Z}) \times \{0,\dots,2b-1\}^n} h \, d\mu^{(\mathbf{X}^{(m)} \cdot \widehat{\mathbf{e}}, \mathbf{Z}^{(1)})} \right| \\
&= \left| \int_{(\mathbb{Z}/b\mathbb{Z}) \times \{0,\dots,2b-1\}^n} P^{(m,1)} h \, d\mu^{((\mathbf{X}^{(m)} - \mathbf{X}^{(m-1)}) \cdot \widehat{\mathbf{e}}, \mathbf{Z}^{(m)})} \right| \\
&\le \|P^{(m,1)} h\|_\infty,
\end{aligned}$$

where $h(z, \mathbf{z}) := \exp(i2\pi z/b)$ for $(z, \mathbf{z}) \in (\mathbb{Z}/b\mathbb{Z}) \times \{0, \dots, 2b-1\}^n$. Let

$$\mathcal{G}_0 := \left\{ g : (\mathbb{Z}/b\mathbb{Z}) \times \{0, \dots, 2b-1\}^n \to \mathbb{C} \;\middle|\; \sum_{z,\mathbf{z}} g(z, \mathbf{z}) = 0 \right\},$$

$$\|P^{(m,m')}\|_{\mathcal{G}_0} := \max_{g \in \mathcal{G}_0, \|g\|_\infty \neq 0} \frac{\|P^{(m,m')}g\|_\infty}{\|g\|_\infty}.$$

Then $h \in \mathcal{G}_0$. Similarly as (4), let us temporarily assume that the Markov chain $\{((\mathbf{X}^{(\infty)} - \mathbf{X}^{(m-1)}) \cdot \widehat{\mathbf{e}}, \mathbf{Z}^{(m)})\}_{m=\infty,\dots,1}$ is strong irreducible, i.e., for an $\epsilon > 0$ and for each $N \in \mathbb{N}$, there exists a pair (m, m') with $N \le m' < m$ such that

$$\min_{z,\mathbf{z},z',\mathbf{z}'} P^{(m,m')}_{(z,\mathbf{z}),(z',\mathbf{z}')} \ge \epsilon. \tag{6}$$

Then, we have that $\|P^{(m,m')}\|_{\mathcal{G}_0} \le 1 - b(2b)^n \epsilon$, and hence

$$\begin{aligned}
\left| \int_{[0,1)} \exp\left(\frac{i2\pi \mathbf{X}^{(M)} \cdot \widehat{\mathbf{e}}}{b} \right) d\mu \right| &\le \|P^{(M,1)} h\|_\infty \\
&\le \|P^{(M,1)}\|_{\mathcal{G}_0} \|h\|_\infty \to 0 \quad (M \to \infty).
\end{aligned}$$

Unfortunately, (6) is again not true. But, since h does not depend on the second variable, the strong irreducibility on $\mathbb{Z}/b\mathbb{Z}$ to be stated below is enough for our purpose. To this end, let

$$\mathcal{G} := \left\{ g \in \mathcal{G}_0 \;\middle|\; \sum_{z} g(z, \mathbf{z}) = 0 \ \text{ for each } \mathbf{z} \in \{0, \dots, 2b-1\}^n \right\},$$

$$\|P^{(m,m')}\|_{\mathcal{G}} := \max_{g \in \mathcal{G}, \|g\|_\infty \neq 0} \frac{\|P^{(m,m')}g\|_\infty}{\|g\|_\infty}.$$

Clearly $h \in \mathcal{G}$ and $\|P^{(m,m')}h\|_\infty \leq \|P^{(m,m')}\|_{\mathcal{G}}\|h\|_\infty$. The following lemma enables us to iterate the estimate of $\|P^{(m,m')}\|_{\mathcal{G}}$.

Lemma 2. *$\mathcal{G}$ is $P^{(m,m')}$-invariant, i.e., $P^{(m,m')}\mathcal{G} \subset \mathcal{G}$.*

Proof. For each $g \in \mathcal{G}$,

$$\begin{aligned}
&\sum_z (P^{(m,m')}g)(z,\mathbf{z})\\
&= \sum_{z,z',\mathbf{z}'} \mu\left(\sum_{m' \leq j < m} (d^{(j)}, \mathbf{\Phi}^{(m,j)}(\mathbf{z})) \cdot \widehat{\mathbf{e}} \equiv z' - z, \mathbf{\Phi}^{(m,m')}(\mathbf{z}) = \mathbf{z}'\right) g(z',\mathbf{z}')\\
&= \sum_{z',\mathbf{z}'} \mu\big(\mathbf{\Phi}^{(m,m')}(\mathbf{z}) = \mathbf{z}'\big) g(z',\mathbf{z}')\\
&= \sum_{\mathbf{z}'} \mu\big(\mathbf{\Phi}^{(m,m')}(\mathbf{z}) = \mathbf{z}'\big) \sum_{z'} g(z',\mathbf{z}') = 0.
\end{aligned}$$

□

We present the following condition instead of (6).

Lemma 3. *Let $m' < m$ and $\epsilon > 0$. Suppose that, for each $(z,\mathbf{z}) \in \mathbb{Z}/b\mathbb{Z} \times \{0,\ldots,2b-1\}^n$, there exists $\mathbf{z}'(z,\mathbf{z}) \in \{0,\ldots,2b-1\}^n$ such that*

$$\min_{z' \in \mathbb{Z}/b\mathbb{Z}} P^{(m,m')}_{(z,\mathbf{z}),(z',\mathbf{z}'(z,\mathbf{z}))} \geq \epsilon. \tag{7}$$

Then

$$\|P^{(m,m')}\|_{\mathcal{G}} \leq 1 - b\epsilon.$$

Proof. By assumption, $P^{(m,m')}_{(z,\mathbf{z}),(z',\mathbf{z}')} - \epsilon 1_{\{\mathbf{z}'=\mathbf{z}'(z,\mathbf{z})\}} \geq 0$. Hence, for $g \in \mathcal{G}$,

$$\begin{aligned}
&\left|(P^{(m,m')}g)(z,\mathbf{z})\right|\\
&= \left|\sum_{z',\mathbf{z}'} P^{(m,m')}_{(z,\mathbf{z}),(z',\mathbf{z}')} g(z',\mathbf{z}')\right|\\
&= \left|\sum_{z',\mathbf{z}'} (P^{(m,m')}_{(z,\mathbf{z}),(z',\mathbf{z}')} - \epsilon 1_{\{\mathbf{z}'=\mathbf{z}'(z,\mathbf{z})\}}) g(z',\mathbf{z}') + \epsilon \sum_{z'} g(z',\mathbf{z}'(z,\mathbf{z}))\right|\\
&= \left|\sum_{z',\mathbf{z}'} (P^{(m,m')}_{(z,\mathbf{z}),(z',\mathbf{z}')} - \epsilon 1_{\{\mathbf{z}'=\mathbf{z}'(z,\mathbf{z})\}}) g(z',\mathbf{z}')\right|\\
&\leq \sum_{z',\mathbf{z}'} (P^{(m,m')}_{(z,\mathbf{z}),(z',\mathbf{z}')} - \epsilon 1_{\{\mathbf{z}'=\mathbf{z}'(z,\mathbf{z})\}}) \|g\|_\infty = (1 - b\epsilon)\|g\|_\infty.
\end{aligned}$$

Thus, we have $\|P^{(m,m')}g\|_\infty \le (1-b\epsilon)\|g\|_\infty$. □

We finally arrive at the desired 'strong irreducibility'. We show in Section 4 that this is valid when μ is the Lebesgue measure λ and b is prime.

Proposition 3. *Suppose that the Markov chain* $\{((\mathbf{X}^{(\infty)} - \mathbf{X}^{(m-1)}) \cdot \widehat{\mathbf{e}}, \mathbf{Z}^{(m)})\}_{m=\infty,\dots,1}$ *is strong irreducible on* $\mathbb{Z}/b\mathbb{Z}$*, i.e., for an* $\epsilon > 0$ *and for each* $N \in \mathbb{N}$*, there exists a pair* (m, m') *with* $N \le m' < m$ *satisfying the condition of Lemma* 3*. Then* $\|P^{(M,1)}\|_{\mathcal{G}} \to 0$ $(M \to \infty)$*.*

Proof. By assumption, we can take a sequence $1 < m_1' < m_1 < m_2' < m_2 < \cdots < m_{j-1} < m_j' < m_j < \cdots$ such that every (m_j, m_j') satisfies the condition of Lemma 3.

By Lemma 2, we have $\|P^{(m,m'')}\|_{\mathcal{G}} \le \|P^{(m,m')}\|_{\mathcal{G}} \|P^{(m',m'')}\|_{\mathcal{G}}$ for $m > m' > m''$. Thus, thanks to that $\|P^{(m,m')}\|_{\mathcal{G}} \le 1$ for $m > m'$, Lemma 3 implies that

$$\begin{aligned}\|P^{(M,1)}\|_{\mathcal{G}} &\le \|P^{(M,m_{J(M)})}\|_{\mathcal{G}} \prod_{j=1}^{J(M)} \|P^{(m_j,m_j')}\|_{\mathcal{G}} \|P^{(m_j',m_{j-1})}\|_{\mathcal{G}} \\ &\le \prod_{j=1}^{J(M)} \|P^{(m_j,m_j')}\|_{\mathcal{G}} \le (1-b\epsilon)^{J(M)} \to 0 \quad (M \to \infty),\end{aligned}$$

where $J(M) := \max\{j \ge 1 \mid M > m_j\}$ and $m_0 := 1$. □

Collecting all the above, we have immediately Theorem 1 by the following implications:

$\{((\mathbf{X}^{(\infty)} - \mathbf{X}^{(m-1)}) \cdot \widehat{\mathbf{e}}, \mathbf{Z}^{(m)})\}_{m=\infty,\dots,1}$ is strong irreducible on $\mathbb{Z}/b\mathbb{Z}$ for each $\widehat{\mathbf{e}} \in (\mathbb{Z}/b\mathbb{Z})^{n+1} \setminus \{\mathbf{0}\}$ and $n \in \mathbb{N}$

$\Rightarrow$ $\|P^{(M,1)}\|_{\mathcal{G}} \to 0$ $(M \to \infty)$ for each $\widehat{\mathbf{e}} \in (\mathbb{Z}/b\mathbb{Z})^{n+1} \setminus \{\mathbf{0}\}$ and $n \in \mathbb{N}$

$\Rightarrow$ The convergence (5) holds for each $\widehat{\mathbf{e}} \in (\mathbb{Z}/b\mathbb{Z})^{n+1} \setminus \{\mathbf{0}\}$ and $n \in \mathbb{N}$

$\Rightarrow$ The convergence (1) holds for each complex function f on $(\mathbb{Z}/b\mathbb{Z})^{n+1}$ and $n \in \mathbb{N}$

$\Rightarrow$ Theorem 1 holds.

4. Strong irreducibility

In this section, we suppose that μ is the Lebesgue measure λ and b is prime, and show the strong irreducibility on $\mathbb{Z}/b\mathbb{Z}$ of the Markov chain $\{((\mathbf{X}^{(\infty)} - \mathbf{X}^{(m-1)}) \cdot \widehat{\mathbf{e}}, \mathbf{Z}^{(m)})\}_{m=\infty,\dots,1}$, where $\widehat{\mathbf{e}} = (\widehat{e}_0, \dots, \widehat{e}_n) \in (\mathbb{Z}/b\mathbb{Z})^{n+1} \setminus \{\mathbf{0}\}$.

First of all, we can suppose $\widehat{e}_0 \not\equiv 0$ without loss of generality. This reduction is easily seen in the following way: Let $l_0 := \min\{0 \le l \le n \mid \widehat{e}_l \not\equiv 0\}$ and $\widehat{\mathbf{e}}' := (\widehat{e}_0', \dots, \widehat{e}_n')$ be such that

$$\widehat{e}_l' := \begin{cases} \widehat{e}_{l+l_0} & \text{if } l \le n - l_0, \\ 0 & \text{otherwise.} \end{cases}$$

Then, $\widehat{e}'_0 \not\equiv 0$ and

$$\begin{aligned}\int_{[0,1)} \exp\left(\frac{i2\pi\mathbf{X}^{(m)}\cdot\widehat{\mathbf{e}}}{b}\right) d\lambda &= \int_{[0,1)} \exp\left(\frac{i2\pi}{b}\sum_{l=0}^{n} X_0^{(m)}(\omega + l_0\alpha + l\alpha)\widehat{e}'_l\right)\lambda(d\omega)\\ &= \int_{[0,1)} \exp\left(\frac{i2\pi\mathbf{X}^{(m)}\cdot\widehat{\mathbf{e}}'}{b}\right) d\lambda.\end{aligned}$$

Here we have used the shift invariance: $\lambda(\,\cdot\, - l_0\alpha) = \lambda(\,\cdot\,)$.

Thus, we now check the strong irreducibility on $\mathbb{Z}/b\mathbb{Z}$ for $\widehat{\mathbf{e}} = (\widehat{e}_0, \dots, \widehat{e}_n)$ with $\widehat{e}_0 \not\equiv 0$. The key for doing so is the following proposition, which claims that every irrational number α has infinite number of 'irregular' digits. This is shown in Section 5.

Proposition 4. *Let α be an irrational number. Then, for each $n \in \mathbb{N}$ there exist infinitely many m's satisfying the following condition*:

$$(8)\quad \begin{cases} \textit{For each } 1 \le l \le n, \textit{ there exist } j_l \textit{ and } j'_l \textit{ with } m - 3n - 1 \le j_l, j'_l < m \\ \textit{such that } 0 < d^{(j_l)}(l\alpha) \quad \textit{and} \quad d^{(j'_l)}(l\alpha) < b - 1. \end{cases}$$

This condition is slightly weak compared with that at the beginning of Section 5, that is, we here admit that $j_l = j'_l$ when $b \ge 3$.

We begin with showing that the chain can visit a neighborhood.

Lemma 4. *Let m satisfy the condition* (8). *Then, for each $\mathbf{z} \in \{0, \dots, 2b-1\}^n$, there exist $m' \in \mathbb{N}$ with $m - 3n - b - 1 \le m' < m$, $\mathbf{z}' \in \{0, \dots, 2b-1\}^n$ and $y \in \mathbb{Z}/b\mathbb{Z}$ such that*

$$\min_{z\in\mathbb{Z}/b\mathbb{Z}, z'\equiv z+y, z+y+1} P^{(m,m')}_{(z,\mathbf{z}),(z',\mathbf{z}')} \ge \left(\frac{1}{b}\right)^{3n+b+1}.$$

Proof. Let $m' < m - 3n - 1$ and

$$\overline{A} := \{d^{(m')} = 0, d^{(j)} = b-1 \quad \text{for } m' < j < m\},$$
$$\underline{A} := \{d^{(m')} = 1, d^{(j)} = 0 \quad \text{for } m' < j < m\}.$$

Then $d^{(k)}$ and $\mathbf{\Phi}^{(m,k)}$ are non random either on $\overline{A}$ or on $\underline{A}$ where $m' \le k < m$. Let

$$\overline{y} :\equiv \sum_{m'\le j<m} (d^{(j)}(\overline{\omega}), \mathbf{\Phi}^{(m,j)}(\overline{\omega};\mathbf{z}))\cdot\widehat{\mathbf{e}}, \quad \overline{\mathbf{z}}' := \mathbf{\Phi}^{(m,m')}(\overline{\omega};\mathbf{z}),$$
$$\underline{y} :\equiv \sum_{m'\le j<m} (d^{(j)}(\underline{\omega}), \mathbf{\Phi}^{(m,j)}(\underline{\omega};\mathbf{z}))\cdot\widehat{\mathbf{e}}, \quad \underline{\mathbf{z}}' := \mathbf{\Phi}^{(m,m')}(\underline{\omega};\mathbf{z}),$$

where $\overline{\omega} \in \overline{A}$ and $\underline{\omega} \in \underline{A}$. Then,

$$\overline{A} \subset \left\{\sum_{m'\le j<m} (d^{(j)}, \mathbf{\Phi}^{(m,j)}(\mathbf{z}))\cdot\widehat{\mathbf{e}} \equiv \overline{y}, \mathbf{\Phi}^{(m,m')}(\mathbf{z}) = \overline{\mathbf{z}}'\right\},$$

$$\underline{A} \subset \left\{\sum_{m'\le j<m} (d^{(j)}, \mathbf{\Phi}^{(m,j)}(\mathbf{z}))\cdot\widehat{\mathbf{e}} \equiv \underline{y}, \mathbf{\Phi}^{(m,m')}(\mathbf{z}) = \underline{\mathbf{z}}'\right\}.$$

Since

$$\lambda\left(\sum_{m'\le j<m}(d^{(j)},\mathbf{\Phi}^{(m,j)}(\mathbf{z}))\cdot\widehat{\mathbf{e}}\equiv\overline{y},\mathbf{\Phi}^{(m,m')}(\mathbf{z})=\overline{\mathbf{z}}'\right)=P^{(m,m')}_{(z,\mathbf{z}),(z+\overline{y},\overline{\mathbf{z}}')},$$

$$\lambda\left(\sum_{m'\le j<m}(d^{(j)},\mathbf{\Phi}^{(m,j)}(\mathbf{z}))\cdot\widehat{\mathbf{e}}\equiv\underline{y},\mathbf{\Phi}^{(m,m')}(\mathbf{z})=\underline{\mathbf{z}}'\right)=P^{(m,m')}_{(z,\mathbf{z}),(z+\underline{y},\underline{\mathbf{z}}')}$$

and $\lambda(\overline{A})=\lambda(\underline{A})=(\frac{1}{b})^{m-m'}$, it is sufficient to show that there exists m' with $m-3n-b-1\le m'<m$ such that $\overline{\mathbf{z}}'=\underline{\mathbf{z}}'$ and $\overline{y}\equiv\underline{y}+1$.

Firstly, we show that $\overline{\mathbf{z}}'=\underline{\mathbf{z}}'$ for all m' with $m'<m-3n-1$. By the definition of $\phi_l^{(m,m')}$,

$$\begin{aligned}
\phi_l^{(m,m')}(\overline{\omega};z)&=\left\lfloor b^{m'-m}z+\sum_{m'\le j<m}b^{m'-j}(d^{(j)}(\overline{\omega})+d^{(j)}(l\alpha))\right\rfloor\\
&=\left\lfloor b^{m'-m}z+1-b^{m'-m+1}+\sum_{m'\le j<m}b^{m'-j}d^{(j)}(l\alpha)\right\rfloor\\
&=d^{(m')}(l\alpha)+\left\lfloor b^{m'-m}z+1-b^{m'-m+1}+\sum_{m'<j<m}b^{m'-j}d^{(j)}(l\alpha)\right\rfloor,\\
\phi_l^{(m,m')}(\underline{\omega};z)&=\left\lfloor b^{m'-m}z+\sum_{m'\le j<m}b^{m'-j}(d^{(j)}(\underline{\omega})+d^{(j)}(l\alpha))\right\rfloor\\
&=\left\lfloor b^{m'-m}z+1+\sum_{m'\le j<m}b^{m'-j}d^{(j)}(l\alpha)\right\rfloor\\
&=d^{(m')}(l\alpha)+1+\left\lfloor b^{m'-m}z+\sum_{m'<j<m}b^{m'-j}d^{(j)}(l\alpha)\right\rfloor.
\end{aligned}$$

By Proposition 4, we can verify, for $k<m-3n-1$,

$$b^{k-m+1}\le\sum_{k<j<m}b^{k-j}d^{(j)}(l\alpha)\le1-2b^{k-m+1}.$$

Therefore,

$$\left\lfloor b^{k-m}z+1-b^{k-m+1}+\sum_{k<j<m}b^{k-j}d^{(j)}(l\alpha)\right\rfloor=1,\tag{9}$$

$$\left\lfloor b^{k-m}z+\sum_{k<j<m}b^{k-j}d^{(j)}(l\alpha)\right\rfloor=0.\tag{10}$$

Thus, we have that

$$\phi_l^{(m,m')}(\overline{\omega}; z) = d^{(m')}(l\alpha) + 1 = \phi_l^{(m,m')}(\underline{\omega}; z),$$

and hence $\overline{\mathbf{z}}' = \underline{\mathbf{z}}'$.

Secondly, we show that $\overline{y} \equiv \underline{y} + 1$ for suitably chosen m'. For all m' and k with $m' < k < m - 3n - 1$, we have

$$\begin{aligned}\phi_l^{(m,k)}(\overline{\omega}; z) &= \left\lfloor b^{k-m} z + b - b^{k-m+1} + \sum_{k \le j < m} b^{k-j} d^{(j)}(l\alpha) \right\rfloor \\ &= d^{(k)}(l\alpha) + b - 1 + \left\lfloor b^{k-m} z + 1 - b^{k-m+1} + \sum_{k < j < m} b^{k-j} d^{(j)}(l\alpha) \right\rfloor, \\ \phi_l^{(m,k)}(\underline{\omega}; z) &= \left\lfloor b^{k-m} z + \sum_{k \le j < m} b^{k-j} d^{(j)}(l\alpha) \right\rfloor \\ &= d^{(k)}(l\alpha) + \left\lfloor b^{k-m} z + \sum_{k < j < m} b^{k-j} d^{(j)}(l\alpha) \right\rfloor.\end{aligned}$$

Again, by (9) and (10), we have that

$$\phi_l^{(m,k)}(\overline{\omega}; z) = d^{(k)}(l\alpha) + b \equiv d^{(k)}(l\alpha) = \phi_l^{(m,k)}(\underline{\omega}; z)$$

and hence

$$\begin{aligned}\overline{y} - \underline{y} \equiv &\sum_{m-3n-1 \le j < m} \big((d^{(j)}(\overline{\omega}), \mathbf{\Phi}^{(m,j)}(\overline{\omega}; \mathbf{z})) - (d^{(j)}(\underline{\omega}), \mathbf{\Phi}^{(m,j)}(\underline{\omega}; \mathbf{z}))\big) \cdot \widehat{\mathbf{e}} \\ &+ \sum_{m' \le j < m-3n-1} (d^{(j)}(\overline{\omega}) - d^{(j)}(\underline{\omega}))\widehat{e}_0 \\ = &\sum_{m-3n-1 \le j < m} \big((d^{(j)}(\overline{\omega}), \mathbf{\Phi}^{(m,j)}(\overline{\omega}; \mathbf{z})) - (d^{(j)}(\underline{\omega}), \mathbf{\Phi}^{(m,j)}(\underline{\omega}; \mathbf{z}))\big) \cdot \widehat{\mathbf{e}} \\ &- \widehat{e}_0 + (m - 3n - 2 - m')(b-1)\widehat{e}_0 \\ \equiv &\sum_{m-3n-1 \le j < m} \big((d^{(j)}(\overline{\omega}), \mathbf{\Phi}^{(m,j)}(\overline{\omega}; \mathbf{z})) - (d^{(j)}(\underline{\omega}), \mathbf{\Phi}^{(m,j)}(\underline{\omega}; \mathbf{z}))\big) \cdot \widehat{\mathbf{e}} \\ &- (m - 3n - 1 - m')\widehat{e}_0.\end{aligned}$$

Since $\mathbb{Z}/b\mathbb{Z}$ is a finite field and $\widehat{e}_0 \ne 0$, linear congruence equation $\widehat{e}_0 X \equiv Y \pmod{b}$ is solvable for a given Y, and therefore we can take m' with $m - 3n - b - 1 \le m' < m - 3n - 1$ and $\overline{y} \equiv \underline{y} + 1$. □

At last, we can show that the chain can visit everywhere.

Lemma 5. *Let* $\epsilon := \left(\dfrac{\varepsilon^{3n+b+1}}{b(2b)^n}\right)^{b-1}$ *for* $\varepsilon := \dfrac{1}{b}$. *Then, the strong irreducibility on* $\mathbb{Z}/b\mathbb{Z}$ *is valid with this* ϵ, *i.e., for each* $N \in \mathbb{N}$, *there exists a pair* (m, m') *with* $N \le m' < m$ *satisfying the condition of Lemma* 3.

Proof. Let $N \in \mathbb{N}$ be given arbitrarily. By Proposition 4, we can take a monotone decreasing sequence $m^{(1)} > m^{(2)} > \cdots > m^{(b)} \geq N$ such that $m^{(j+1)} < m^{(j)} - 3n - b - 1$ and $m^{(j)}$ satisfies the condition (8).

Let $\mathbf{z} \in \{0, \ldots, 2b-1\}^n$.

Then, by Lemma 4, there exist $m'^{(1)}$, $\mathbf{z}'^{(1)}$ and $y'^{(1)}$ with $m^{(2)} < m'^{(1)} < m^{(1)}$ such that

$$\min_{z \in \mathbb{Z}/b\mathbb{Z}} \min_{z' \equiv z + y'^{(1)}, z + y'^{(1)} + 1} P^{(m^{(1)}, m'^{(1)})}_{(z,\mathbf{z}),(z',\mathbf{z}'^{(1)})} \geq \varepsilon^{3n+b+1}.$$

Since the cardinal number of the state space is $b(2b)^n$, there exist $y^{(1)}$ and $\mathbf{z}^{(2)}$ such that

$$P^{(m'^{(1)}, m^{(2)})}_{(y'^{(1)},\mathbf{z}'^{(1)}),(y^{(1)},\mathbf{z}^{(2)})} \geq \frac{1}{b(2b)^n}.$$

Noting that, by the definition, $P^{(k,k')}_{(w,\mathbf{w}),(w',\mathbf{w}')}$ is shift invariant on $\mathbb{Z}/b\mathbb{Z}$, i.e., $P^{(k,k')}_{(w,\mathbf{w}),(w',\mathbf{w}')} = P^{(k,k')}_{(w+v,\mathbf{w}),(w'+v,\mathbf{w}')}$ where $k > k'$, $w, w', v \in \mathbb{Z}/b\mathbb{Z}$ and $\mathbf{w}, \mathbf{w}' \in \{0, \ldots, 2b-1\}^n$, we see that, for any $z \in \mathbb{Z}/b\mathbb{Z}$,

$$\begin{aligned} P^{(m^{(1)}, m^{(2)})}_{(z,\mathbf{z}),(z+y^{(1)},\mathbf{z}^{(2)})} &\geq P^{(m^{(1)}, m'^{(1)})}_{(z,\mathbf{z}),(z+y'^{(1)},\mathbf{z}'^{(1)})} P^{(m'^{(1)}, m^{(2)})}_{(z+y'^{(1)},\mathbf{z}'^{(1)}),(z+y^{(1)},\mathbf{z}^{(2)})} \\ &= P^{(m^{(1)}, m'^{(1)})}_{(z,\mathbf{z}),(z+y'^{(1)},\mathbf{z}'^{(1)})} P^{(m'^{(1)}, m^{(2)})}_{(y'^{(1)},\mathbf{z}'^{(1)}),(y^{(1)},\mathbf{z}^{(2)})} \geq \frac{\varepsilon^{3n+b+1}}{b(2b)^n}. \end{aligned}$$

Since we can verify $P^{(m^{(1)}, m^{(2)})}_{(z,\mathbf{z}),(z+y^{(1)}+1,\mathbf{z}^{(2)})} \geq \frac{\varepsilon^{3n+b+1}}{b(2b)^n}$ in the same way,

$$\min_{z \in \mathbb{Z}/b\mathbb{Z}} \min_{z' \equiv z + y^{(1)}, z + y^{(1)} + 1} P^{(m^{(1)}, m^{(2)})}_{(z,\mathbf{z}),(z',\mathbf{z}^{(2)})} \geq \frac{\varepsilon^{3n+b+1}}{b(2b)^n}.$$

Hence, inductively, we have that there exist $\mathbf{z}^{(3)}, \ldots, \mathbf{z}^{(b)}$ and $y^{(2)}, \ldots, y^{(b-1)}$ such that

$$\min_{z \in \mathbb{Z}/b\mathbb{Z}} \min_{z' \equiv z + y^{(j)}, z + y^{(j)} + 1} P^{(m^{(j)}, m^{(j+1)})}_{(z,\mathbf{z}^{(j)}),(z',\mathbf{z}^{(j+1)})} \geq \frac{\varepsilon^{3n+b+1}}{b(2b)^n},$$

where $j = 1, \ldots, b-1$ and $\mathbf{z}^{(1)} = \mathbf{z}$. Again, using the shift invariance of $P^{(k,k')}_{(w,\mathbf{w}),(w',\mathbf{w}')}$, we have that

$$\min_{z' = z + y^{(1)} + y^{(2)}, z + y^{(1)} + y^{(2)} + 1, z + y^{(1)} + y^{(2)} + 2} P^{(m^{(1)}, m^{(3)})}_{(z,\mathbf{z}),(z',\mathbf{z}^{(3)})} \geq \left(\frac{\varepsilon^{3n+b+1}}{b(2b)^n} \right)^2.$$

Repeat that to $m^{(b)}$ and let $m := m^{(1)}$, $m' := m^{(b)}$, $z^{(b)} := z + y^{(1)} + \cdots + y^{(b-1)}$ and $\mathbf{z}'(z, \mathbf{z}) := \mathbf{z}^{(b)}$. Then, we have

$$\min_{z'} P^{(m,m')}_{(z,\mathbf{z}),(z',\mathbf{z}'(z,\mathbf{z}))} = \min_{z' \equiv z^{(b)}, \cdots, z^{(b)} + b - 1} P^{(m^{(1)}, m^{(b)})}_{(z,\mathbf{z}),(z',\mathbf{z}^{(b)})} \geq \left(\frac{\varepsilon^{3n+b+1}}{b(2b)^n} \right)^{b-1} = \epsilon.$$

□

5. Proof of Proposition 4

In this section, integer $b \geq 2$ need not be prime.

We here show the contraposition of Proposition 4, i.e., we check that α is a rational number when only a finite number of m satisfies the condition (8).

For a fixed $n \in \mathbb{N}$, let

$$N = N_n := \max\left\{ m \;\middle|\; \begin{array}{l} \text{for each } 1 \leq l \leq n, \text{ there exist } m-3n-1 \leq j_l < \\ j_l' < m \text{ such that } d^{(j_l)}(l\alpha) \neq d^{(j_l')}(l\alpha) \end{array} \right\}.$$

Then, the following lemma clearly implies Proposition 4:

Lemma 6. *If N is finite, α is a rational number.*

We prepare two lemmas to see Lemma 6.

Lemma 7. *The finite sequence $d^{(m-2n-1)}(\alpha), \ldots, d^{(m-1)}(\alpha)$ is periodic and its period is at most n when there exists $1 \leq l \leq n$ such that $d^{(m-3n-1)}(l\alpha) = \cdots = d^{(m-1)}(l\alpha)$.*

Proof. There are two ways of finding a division $l\alpha/l$. One is a trivial computation: $l\alpha/l = \alpha = \sum_{j=1}^{\infty} \frac{d^{(j)}(\alpha)}{b^j} = 0.d^{(1)}(\alpha)d^{(2)}(\alpha)\cdots$. Another is a manual computation given by the following:

$$\begin{array}{ll}
 & \quad 0.\ a_1\ \ a_2\ \cdots\cdots\ a_{j-1}\ \ a_j\ \ \cdots\ \cdots \\ \cline{2-2}
l\,\big) & \lfloor l\alpha \rfloor.d_l^{(1)} d_l^{(2)} \cdots\cdots d_l^{(j-1)} d_l^{(j)} d_l^{(j+1)} \cdots \\
 & \quad\ \ la_1 \\ \cline{2-2}
 & \quad\ \ r_1\ d_l^{(2)} \\
 & \qquad\quad\ la_2 \\ \cline{2-2}
 & \qquad\quad\ r_2\ d_l^{(3)} \\
 & \qquad\qquad\quad \ddots \\
 & \qquad\qquad\qquad \ddots \\
 & \qquad\qquad\qquad\quad r_{j-1}\ d_l^{(j)} \\
 & \qquad\qquad\qquad\qquad\quad la_j \\ \cline{2-2}
 & \qquad\qquad\qquad\qquad\quad r_j\ d_l^{(j+1)} \\
 & \qquad\qquad\qquad\qquad\qquad\qquad \ddots
\end{array}$$

where $\lfloor l\alpha \rfloor.d_l^{(1)} d_l^{(2)} \cdots$ $(d_l^{(k)} := d^{(k)}(l\alpha), k \geq 1)$ is the b-adic representation of $l\alpha$ and $r_{j-1}d_l^{(j)}$ is that of $br_{j-1} + d_l^{(j)}$, and $l\alpha_j = l \times \alpha_j$. Hence

$$\begin{aligned}
a_1 &= \max\{0 \leq a < b \mid la \leq b\lfloor l\alpha \rfloor + d^{(1)}(l\alpha)\} \\
&= \max\{0 \leq a < b \mid la \leq \lfloor bl\alpha \rfloor\}, \\
r_1 &= b\lfloor l\alpha \rfloor + d^{(1)}(l\alpha) - la_1 = \lfloor bl\alpha \rfloor - la_1,
\end{aligned}$$

and for $j > 1$

$$a_j = \max\{0 \le a < b \mid la \le br_{j-1} + d^{(j)}(l\alpha)\},$$
$$r_j = br_{j-1} + d^{(j)}(l\alpha) - la_j.$$

Since the representations above are equal, we have the identity

$$d^{(j)}(\alpha) = a_j, \quad j \ge 1.$$

Next, noting that $r_j \in \{0, \dots, l-1\}$ $(j \ge 1)$, we set

$$p = \min\{i \ge 1 \mid r_{m-2n-2+i} = r_{m-2n-2}\}.$$

Clearly $1 \le p \le l$ and $r_{m-2n-2} = r_{m-2n-2+p}$. By the assumption $d^{(m-3n-1)}(l\alpha) = \cdots = d^{(m-1)}(l\alpha)$, and by the recursion formulas of a_j and r_j, we can easily verify that

$$r_k = r_{k+p}, \ a_{k+1} = a_{k+1+p} \quad \text{for} \ \ m-2n-2 \le k < m-p-1.$$

Thus, combining this with the identity above, we complete the proof. □

Next lemma is concerned with the least periods of a sequence and its consecutive subsequence.

Lemma 8. *Let $\{a_j\}_{j=0}^{p-1}$ be a sequence with the least period k $(2k \le p)$. Then, that of any subsequence $\{a_j\}_{j=q}^{q+p'-1}$ $(0 \le q < q+p' \le p)$ is also k whenever $p' \ge 2k$.*

Proof. Let k' be the least period of $\{a_j\}_{j=q}^{q+p'-1}$. Then $k' \le k$. For any $0 \le l < p - k'$, there exist $j \in \mathbb{Z}$ and $0 \le r < k$ such that $l - q = kj + r$. Since $r + k' < 2k \le p'$,

$$a_l = a_{q+kj+r} = a_{q+r} = a_{q+r+k'} = a_{q+kj+r+k'} = a_{l+k'}.$$

Hence k' is a period of $\{a_j\}_{j=0}^{p-1}$ and $k' = k$. □

Now, we prove Lemma 6.

Proof of Lemma 6. For any $m > N$, there exists $1 \le l_m \le n$ such that

$$d^{(m-3n-1)}(l_m\alpha) = \cdots = d^{(m-1)}(l_m\alpha).$$

Let $m := N+1$. Then, by Lemma 7, $\{d^{(j)}(\alpha)\}_{j=N-2n}^{N}$ is periodic. Let the least period be k_1. Similarly, $\{d^{(j)}(\alpha)\}_{j=N-2n+1}^{N+1}$ is periodic. Let the least period be k_2. Since $k_1, k_2 \le n$, Lemma 8 implies that both k_1 and k_2 are same as the least period of $\{d^{(j)}(\alpha)\}_{j=N-2n+1}^{N}$, hence $k_1 = k_2$. Thus, by the induction, $\{d^{(j)}(\alpha)\}_{j=N-2n}^{\infty}$ is periodic and α is a rational number. □

We conclude this paper with some remarks.

The converse of Lemma 6 is trivial. For, if $\alpha = \frac{m}{l}$, where $l \in \mathbb{N}$ and $m \in \mathbb{Z}$, then clearly $d^{(j)}(l\alpha) = 0$ for all j. Thus, a criterion to be irrational is obtained:

A real number α is irrational if and only if N_n is infinite for every $n \in \mathbb{N}$.

When $b = 2$, $N_n = \infty$ is in words that the condition (8) holds for infinitely many m's. This condition, in fact, has already appeared in Sugita-Takanobu [4]. In this unpublished note [4], they have tried a refinement of the argument in Sugita [2], where only the case of $b = 2$ is treated, and improved his result, so that it has been obtained that Theorem 1 is valid for any irrational number α having $N_n = \infty$ for every $n \in \mathbb{N}$. Here their method is what is called a method of cancellation established in [2], and different from ours. Therefore, we may say by the criterion above that as a historical matter, Sugita's conjecture was affirmatively solved earlier than we here do. But, this comment does not match with a fact that they had not this criterion at that time. In fact, viewing their note carefully, we find the following: They have thought that the condition imposed for α, i.e., $N_n = \infty$ for all n only clarifies a part of the irrationality of α, and so this condition is insignificant compared with the irrationality, still less they have not expected at all that the irrationality implies this condition. From this observation, the credit of the proof of Sugita's conjecture belongs to us. Anyway, thanks to our criterion, this conjecture has been now advanced to a theorem by our or his method.

Ritsumeikan University
1-1-1 Nojihigashi, Kusatsu
Shiga 525-8577, Japan
e-mail: yasutomi@se.ritsumei.ac.jp

References

[1] H. Dym and H. P. McKean, *Fourier series and integrals*, Academic Press, 1972.

[2] H. Sugita, *Pseudo-random number generator by means of irrational rotation*, Monte Carlo Methods and Appl. **1** (1995), 35–57.

[3] ———, Lectures at Kobe University (2000).

[4] H. Sugita and S. Takanobu, *Weyl transformation and binary transformation* (in Japanese), preprint (Jul. 1998).

[5] S. Takanobu, *On the strong-mixing property of skew product of binary transformation on* 2*-dimensional torus by irrational rotation*, Tokyo J. Math. **25** (2002), 1–15.

[6] K. Yasutomi, *A limit theorem of sequences generated by Weyl transformation*, Probab. Theory Related Fields **124** (2002), 178–188.

[7] ———, *A direct proof of dependence vanishing theorem for sequences generated by Weyl transformation*, to appear in J. Math. Kyoto Univ. **43**-3 (2003), 599–607.