J. Math. Kyoto Univ. (JMKYAZ)
43-3 (2003), 599–607

A direct proof of dependence vanishing theorem for sequences generated by Weyl transformation

By

Kenji Yasutomi

1. Introduction

Sugita [1] proposed a problem relating to a pseudo-random number generation. Let $d^{(m)}(x)$ be the m-th digit of $x \geq 0$ in decimal part of its dyadic expansion, and $X_l^{(m)}$ be the $\{0,1\}$-valued function on $[\,0,1)^2$ such that

$$X_l^{(m)}(x,\alpha) = \sum_{k=1}^{m} d^{(k)}(x+l\alpha) \pmod 2.$$

When α is "good", the process $\{X_n^{(m)}(\,\cdot\,,\alpha)\}_{n=0}^{\infty}$ on $([\,0,1),P)$ converges in law to $\{0,1\}$-valued fair i.i.d. when $m \to \infty$, where P is the Lebesgue measure on $[\,0,1)$. Note that the process $\{X_n^{(m)}(\,\cdot\,,\alpha)\}_{n=0}^{\infty}$ is generated by the Weyl transformation and has strong dependence. The convergence claims that the dependence disappears when $m \to \infty$. The problem is the following.

Problem. *What α is "good"?*

Sugita [1] conjectured that any irrational number α is "good" and showed that any α with dyadic expansion containing some finite sequences infinity many times is "good".

Since the method in Sugita [1] was complicated, we showed a.e. α is "good" in [4] for any Bernoulli measure P and any base of expansion by using a simple method originated with Sugita [2]. But, since we regarded α as a random variable, we could not know whether each given α is "good" or not.

In this paper, we show α which satisfies a condition similar to Sugita [1] is "good" by a more direct method. Moreover, our method assures that the extensions of the class of measures P and that base of expansion in [4] are still valid.

Received July 12, 2002
Revised November 12, 2002

2. Theorem

Let $b \geq 2$ be a natural number, $d^{(m)}(x)$ be the m-th digit of $x \geq 0$ in decimal part of its base-b expansion, and $X_l^{(m)}$ be a $\{0,\dots,b-1\}$-valued function on $[\,0,1)^2$ such that

$$X_l^{(m)}(x,\alpha) = \sum_{k=1}^{m} d^{(k)}(x+l\alpha) \pmod b.$$

We assume that P is a measure on $[\,0,1)$ such that $\{d^{(i)}\}_i$ is independent with respect to it, and that

$$\liminf_i \min_{0\leq\varsigma<b} P(d^{(i)}=\varsigma) > 0.$$

Our main result is the following:

Theorem 2.1. *Any α with base-b expansion containing any finite sequence infinity many times is "good", i.e., the process $\{X_n^{(m)}(\,\cdot\,,\alpha)\}_{n=0}^{\infty}$ on $([\,0,1),P)$ converges in law to $\{0,\dots,b-1\}$-valued fair i.i.d. when $m\to\infty$.*

Sugita [1] actually showed Theorem 2.1 in case $b=2$ and P is the Lebesgue measure. In fact, we show the following stronger statement:

Proposition 2.1. *For each $n\in\mathbb{N}$, let $A_n \subset [\,0,1)$ be the set of all $\alpha\in[\,0,1)$ whose base-b expansion contains a finite sequence*

$$\underbrace{0\cdots0}_{k+\kappa}\underbrace{\underbrace{0\cdots0}_{\kappa+2}1\underbrace{0\cdots0}_{\kappa+2}1\cdots\underbrace{0\cdots0}_{\kappa+2}1}_{M}\underbrace{0\cdots0}_{k+\kappa}$$

infinity many times for every k, where $\kappa := \min\{j\in\mathbb{N} \mid b^j \geq n-1\}$ and $M := n(b-1)(b^{\kappa+2}+(b-1)b^{\kappa})$. Then any $\alpha\in\cap_{n=1}^{\infty}A_n$ is "good", i.e., the process $\{X_n^{(m)}(\,\cdot\,,\alpha)\}_{n=0}^{\infty}$ on $([\,0,1),P)$ converges in law to $\{0,\dots,b-1\}$-valued fair i.i.d. when $m\to\infty$.

Now, we prove Proposition 2.1.

Proof. To show Proposition 2.1, it is sufficient to see

$$P((X_0^{(m)}(\,\cdot\,,\alpha),\dots,X_{n-1}^{(m)}(\,\cdot\,,\alpha))=\sigma) \to b^{-n} \qquad (m\to\infty) \tag{2.1}$$

for any n and $\sigma\in\{0,\dots,b-1\}^n =: \Sigma$. Therefore we fix n and $\alpha\in A_n$ from now on, and define $\mathbf{X}^{(m)}$ by

$$\mathbf{X}^{(m)} := (X_0^{(m)}(\,\cdot\,,\alpha),\dots,X_{n-1}^{(m)}(\,\cdot\,,\alpha)).$$

Let us consider m as a new time parameter. Then, we can see that for a certain increasing sequence $\{m_i\}_i$, the $\{\mathbf{X}^{(m_i)}\}_i$ is 'almost' a strong irreducible Markov

chain whose unique stationary distribution is the uniform distribution on Σ. From this observation, (2.1) will be derived.

We use two lemmas. Lemma 2.1 claims that $P(\mathbf{X}^{(m)} = \sigma)$ is 'almost' a Markov kernel on Σ. By the assumption of measure P, we can find $p > 0$ and $\bar{m}$ as $\inf_{i \geq \bar{m}} \min_{\varsigma} P(d^{(i)} = \varsigma) \geq p$. Let $\equiv$ mean mod b equality for any component on Σ.

Lemma 2.1. *Let $m \geq \bar{m}$, $m' \geq m + k + \kappa$, and $d^{(i)}(\alpha) = 0$ for $m < i \leq m'$. Then, for any $\sigma' \in \Sigma$,*

$$\left| P(\mathbf{X}^{(m')} = \sigma') - \sum_{\sigma \in \Sigma} P(\mathbf{X}^{(m)} = \sigma) P(\mathbf{X}^{(m')} - \mathbf{X}^{(m)} \equiv \sigma' - \sigma) \right| \leq 2(1-p)^k.$$

Lemma 2.2 claims 'strong irreducibility'. Let $*$ denote any one of $0, 1, \ldots, b-1$.

Lemma 2.2. *There exists $\varepsilon > 0$ such that*

$$\min_{\sigma} P(\mathbf{X}^{(\widehat{m})} - \mathbf{X}^{(m)} \equiv \sigma' - \sigma) \geq \varepsilon$$

for any $\sigma' \in \Sigma$, $k \geq 2$, $m \geq \bar{m}$ such that

$$\alpha = 0.\underbrace{* \cdots *}_{m} \underbrace{0 \cdots 0}_{k+\kappa} \underbrace{\underbrace{0 \cdots 0}_{\kappa+2} 1 \underbrace{0 \cdots 0}_{\kappa+2} 1 \cdots \underbrace{0 \cdots 0}_{\kappa+2} 1}_{M} \underbrace{0 \cdots 0}_{k+\kappa} * \cdots,$$

and $\widehat{m} := m + k + \kappa + M(\kappa + 3)$.

Now, we show (2.1) by using Lemmas 2.1 and 2.2. Let $m_i \geq \bar{m}$ be as

$$\alpha = 0.\underbrace{* \cdots *}_{m_i} \underbrace{0 \cdots 0}_{k_i+\kappa} \underbrace{\underbrace{0 \cdots 0}_{\kappa+2} 1 \underbrace{0 \cdots 0}_{\kappa+2} 1 \cdots \underbrace{0 \cdots 0}_{\kappa+2} 1}_{M} \underbrace{0 \cdots 0}_{k_i+\kappa} * \cdots,$$

$\widehat{m}_i := m_i + k_i + \kappa + M(\kappa + 3)$, and $E^{(j)}(\sigma) := P(\mathbf{X}^{(j)} = \sigma) - b^{-n}$. Then, by Lemma 2.1, for $m' \geq \widehat{m}_i + k_i + \kappa$,

$$\left| E^{(m')}(\sigma') - \sum_{\sigma \in \Sigma} E^{(\widehat{m}_i)}(\sigma) P(\mathbf{X}^{(m')} - \mathbf{X}^{(\widehat{m}_i)} \equiv \sigma' - \sigma) \right| \leq 2(1-p)^{k_i}.$$

Therefore, because $P(\mathbf{X}^{(m')} - \mathbf{X}^{(\widehat{m}_i)} \equiv \sigma' - \sigma) \geq 0$,

$$\left| E^{(m')}(\sigma') \right| \leq \sum_{\sigma \in \Sigma} \left| E^{(\widehat{m}_i)}(\sigma) \right| P(\mathbf{X}^{(m')} - \mathbf{X}^{(\widehat{m}_i)} \equiv \sigma' - \sigma) + 2(1-p)^{k_i}.$$

Note that $\sum_{\sigma \in \Sigma} P(\mathbf{X}^{(m')} - \mathbf{X}^{(\widehat{m}_i)} \equiv \sigma' - \sigma) = 1$. Thus

$$\max_{\sigma \in \Sigma} |E^{(m')}(\sigma)| \leq \max_{\sigma \in \Sigma} |E^{(\widehat{m}_i)}(\sigma)| + 2(1-p)^{k_i}. \tag{2.2}$$

Again, by Lemma 2.1

$$\left| E^{(\widehat{m}_i)}(\sigma') - \sum_{\sigma\in\Sigma} E^{(m_i)}(\sigma) P(\mathbf{X}^{(\widehat{m}_i)} - \mathbf{X}^{(m_i)} \equiv \sigma' - \sigma) \right| \le 2(1-p)^{k_i}.$$

Noting $\varepsilon \sum_{\sigma\in\Sigma} E^{(m_i)}(\sigma) = 0$ and that $P(\mathbf{X}^{(\widehat{m}_i)} - \mathbf{X}^{(m_i)} \equiv \sigma' - \sigma) - \varepsilon \ge 0$ by Lemma 2.2, we have

$$\left| E^{(\widehat{m}_i)}(\sigma') \right| \le \sum_{\sigma\in\Sigma} \left| E^{(m_i)}(\sigma) \right| (P(\mathbf{X}^{(\widehat{m}_i)} - \mathbf{X}^{(m_i)} \equiv \sigma' - \sigma) - \varepsilon) + 2(1-p)^{k_i}.$$

Thus

$$\max_{\sigma\in\Sigma} |E^{(\widehat{m}_i)}(\sigma)| \le (1 - b^n\varepsilon) \max_{\sigma\in\Sigma} |E^{(m_i)}(\sigma)| + 2(1-p)^{k_i}. \tag{2.3}$$

By the assumption of α, we can define $\{m_i, k_i\}$ as $m_{i+1} \ge \widehat{m}_i + k_i + \kappa$ and $k_i \ge i(\log(1 - b^n\varepsilon) - \log 2)/\log(1-p)$. Therefore, by (2.2) and (2.3), we have

(2.4)

$$\begin{aligned}
\max_{\sigma\in\Sigma} |E^{(m_{i+1})}(\sigma)| &\le (1 - b^n\varepsilon) \max_{\sigma\in\Sigma} |E^{(m_i)}(\sigma)| + 4(1-p)^{k_i} \\
&\le (1 - b^n\varepsilon)^i \left(\max_{\sigma\in\Sigma} |E^{(m_1)}(\sigma)| + 4 \sum_{j=1}^{i} (1 - b^n\varepsilon)^{-j} (1-p)^{k_j} \right) \\
&\le (1 - b^n\varepsilon)^i \left(\max_{\sigma\in\Sigma} |E^{(m_1)}(\sigma)| + 4 \sum_{j=1}^{i} \frac{1}{2^j} \right) \\
&= (1 - b^n\varepsilon)^i (\max_{\sigma\in\Sigma} |E^{(m_1)}(\sigma)| + 4).
\end{aligned}$$

Since $k_i \to \infty$ when $i \to \infty$, by (2.2) and (2.4), for $m \ge \widehat{m}_{i+1} + k_{i+1} + \kappa$, we have

$$\max_{\sigma\in\Sigma} |E^{(m)}(\sigma)| \le \max_{\sigma\in\Sigma} |E^{(m_{i+1})}(\sigma)| + 2(1-p)^{k_{i+1}} \to 0 \qquad (i \to \infty).$$

□

3. Proof of Lemmas

Let the symbol $\lfloor \cdot \rfloor^m$ be the number which is rounded down to the m-th digit and $\langle \cdot \rangle_m$ be $\cdot - \lfloor \cdot \rfloor^m$, i.e. $\lfloor \cdot \rfloor^m = \cdot - \sum_{j=m+1}^{\infty} b^{-j} d^{(j)}(\cdot)$ and $\langle \cdot \rangle_m = \sum_{j=m+1}^{\infty} b^{-j} d^{(j)}(\cdot)$. For $m < m'$, define $\langle\!\lfloor \cdot \rfloor\!\rangle_m^{m'}$ by $\langle\!\lfloor \cdot \rfloor\!\rangle_m^{m'} := \lfloor \langle \cdot \rangle_m \rfloor^{m'} = \langle \lfloor \cdot \rfloor^{m'} \rangle_m = \sum_{j=m+1}^{m'} b^{-j} d^{(j)}(\cdot)$.

The main idea of Lemma 2.1 is as follows. The dependence of $\mathbf{X}^{(m)}$ and $\mathbf{X}^{(m')} - \mathbf{X}^{(m)}$ is caused by the carry at m-th digit which arises from the addition $x + l\alpha$. Therefore, intuitively, the 'dependence' is 'little' if $\langle \alpha \rangle_m$ is small enough.

Proof of Lemma 2.1. Let

$$A := \left\{ x \in [\,0,1) \mid \langle x \rangle_m < \frac{b^k - 1}{b^{m+k}} \right\}.$$

Since $\langle\!\lfloor \alpha \rfloor\!\rangle_m^{m+k+\kappa} = 0$ by the assumption of α, m and κ, we have

$$l\langle\alpha\rangle_m = l(\langle\!\lfloor \alpha \rfloor\!\rangle_m^{m+k+\kappa} + \langle\alpha\rangle_{m+k+\kappa}) < \frac{l}{b^{m+k+\kappa}} \le \frac{1}{b^{m+k}} \frac{n-1}{b^\kappa} \le \frac{1}{b^{m+k}} \tag{3.1}$$

for $l \le n-1$. Therefore, $\langle x \rangle_m + l\langle\alpha\rangle_m < 1/b^m$ for $x \in A$, and hence no carry arises from the addition $x + l\alpha$ at m-th digit, i.e., $\lfloor \langle x \rangle_m + l\langle\alpha\rangle_m \rfloor^m = 0$. Thus $\lfloor x + l\alpha \rfloor^m = \lfloor x \rfloor^m + l\lfloor \alpha \rfloor^m + \lfloor \langle x \rangle_m + l\langle\alpha\rangle_m \rfloor^m = \lfloor x \rfloor^m + l\lfloor \alpha \rfloor^m = \lfloor x + l\lfloor \alpha \rfloor^m \rfloor^m$, i.e., $\mathbf{X}^{(m)}(\,\cdot\,, \alpha) = \mathbf{X}^{(m)}(\,\cdot\,, \lfloor \alpha \rfloor^m)$ on A. We let $\triangle$ denote the symmetric difference. Then

$$\{\mathbf{X}^{(m)} = \sigma\} \triangle \{\mathbf{X}^{(m)}(\,\cdot\,, \lfloor \alpha \rfloor^m) = \sigma\} \subset A^c.$$

Note that $\mathbf{X}^{(m)}(\cdot, \lfloor \alpha \rfloor^m)$ depend only on $d^{(1)}, \dots, d^{(m)}$ and that $B_{\sigma'} := \{\mathbf{X}^{(m')} - \mathbf{X}^{(m)} \equiv \sigma' - \sigma\}$ depend only on $d^{(m+1)}$, $d^{(m+2)}, \dots$. By the independence of base-b expansion,

$$\begin{aligned}
&\left| P(\mathbf{X}^{(m)} = \sigma) - \sum_{\sigma' \in \Sigma} P(\mathbf{X}^{(m)} = \sigma) P(\mathbf{X}^{(m')} - \mathbf{X}^{(m)} \equiv \sigma' - \sigma) \right| \\
&\quad \le \sum_{\sigma' \in \Sigma} \left| P(\{\mathbf{X}^{(m)} = \sigma\} \cap B_{\sigma'}) - P(\mathbf{X}^{(m)} = \sigma) P(B_{\sigma'}) \right| \\
&\quad \le \sum_{\sigma' \in \Sigma} \left| P(\{\mathbf{X}^{(m)} = \sigma\} \cap B_{\sigma'}) - P(\{\mathbf{X}^{(m)}(\,\cdot\,, \lfloor \alpha \rfloor^m) = \sigma\} \cap B_{\sigma'}) \right| \\
&\qquad + \sum_{\sigma' \in \Sigma} \left| P(\{\mathbf{X}^{(m)}(\,\cdot\,, \lfloor \alpha \rfloor^m) = \sigma\} \cap B_{\sigma'}) - P(\mathbf{X}^{(m)} = \sigma) P(B_{\sigma'}) \right| \\
&\quad \le \sum_{\sigma' \in \Sigma} \left| P(\{\mathbf{X}^{(m)} = \sigma\} \cap B_{\sigma'}) - P(\{\mathbf{X}^{(m)}(\,\cdot\,, \lfloor \alpha \rfloor^m) = \sigma\} \cap B_{\sigma'}) \right| \\
&\qquad + \sum_{\sigma' \in \Sigma} P(B_{\sigma'}) \left| P(\mathbf{X}^{(m)}(\,\cdot\,, \lfloor \alpha \rfloor^m) = \sigma) - P(\mathbf{X}^{(m)} = \sigma) \right| \\
&\quad \le \sum_{\sigma' \in \Sigma} P(A^c \cap B_{\sigma'}) + \sum_{\sigma' \in \Sigma} P(B_{\sigma'}) P(A^c) = 2P(A^c).
\end{aligned}$$

By the definition of A,

$$\begin{aligned}
P(A^c) &= P(0 < \forall i \le k,\ d^{(m+i)}(x) = b - 1) \\
&= \prod_{i=1}^{k} P(d^{(m+i)}(x) = b - 1) \le (1 - p)^k.
\end{aligned}$$

□

To prove Lemma 2.2 we use following lemma. For $u \in \mathbb{N}$, let

$$Y(u) := \sum_{i=1}^{\kappa+3} d^{(i)}\left(\frac{u}{b^{\kappa+3}}\right) \pmod b,$$
$$\mathbf{Y}(u) := (Y(u), Y(u+1), \dots, Y(u+n-1)).$$

Lemma 3.1. *For any $\sigma \in \Sigma$, there exist $0 \le \varsigma < b$ and $0 \le u_i < b^{\kappa+3} - b^{\kappa+1}$ such that*

$$\sigma \equiv \varsigma \mathbf{1} + \sum_{i=1}^{M} \mathbf{Y}(u_i).$$

Now we can see the proof of Lemma 2.2.

Proof of Lemma 2.2. Let $\widetilde{m}_{-1} := m$, $\widetilde{m}_i := m + k + \kappa + i(\kappa+3)$ for $0 \le i \le M$ and

$$A_{\varsigma,u_1,\dots,u_M} := \left\{ x \;\middle|\; \sum_{i=\widetilde{m}_{-1}+1}^{\widetilde{m}_0} d^{(i)}(x) = \varsigma,\ \langle\!\lfloor x \rfloor\!\rangle_{\widetilde{m}_0}^{\widetilde{m}_M+1} = \sum_{i=1}^{M} \frac{u_i}{b^{\widetilde{m}_i}} \right\}.$$

First, by the independence of $\{d^{(i)}\}_i$, we have

$$\begin{aligned}
&P(A_{\varsigma,u_1,\dots,u_M}) \\
&\quad = P\left(\sum_{i=\widetilde{m}_{-1}+1}^{\widetilde{m}_0} d^{(i)}(x) = \varsigma\right) \prod_{j=\widetilde{m}_0+1}^{\widetilde{m}_M+1} P\left(d^{(j)}(x) = d^{(j)}\left(\sum_{i=1}^{M} \frac{u_i}{b^{\widetilde{m}_i}}\right)\right) \\
&\quad \ge p^{M(\kappa+3)+1} \sum_{\varsigma'} P\left(\sum_{i=\widetilde{m}_{-1}+1}^{\widetilde{m}_0-1} d^{(i)}(x) = \varsigma'\right) P\left(d^{(\widetilde{m}_0)} = \varsigma - \varsigma'\right) \\
&\quad \ge p^{M(\kappa+3)+2} \sum_{\varsigma'} P\left(\sum_{i=\widetilde{m}_{-1}+1}^{\widetilde{m}_0-1} d^{(i)}(x) = \varsigma'\right) = p^{M(\kappa+3)+2} =: \varepsilon.
\end{aligned}$$

Note that $\varepsilon > 0$ does not depend on $0 \le \varsigma < b$ or $0 \le u_i < b^{\kappa+3} - b^{\kappa+1}$. Thus, by Lemma 3.1, it is sufficient to prove Lemma 2.2 to see that

$$\left\{ x \;\middle|\; \mathbf{X}^{(\widehat{m})}(x) - \mathbf{X}^{(m)}(x) \equiv \varsigma \mathbf{1} + \sum_{i=1}^{M} \mathbf{Y}(u_i) \right\} \supset A_{\varsigma,u_1,\dots,u_M} \tag{3.2}$$

for any $0 \le \varsigma < b$ and $0 \le u_i < b^{\kappa+3} - b^{\kappa+1}$.

We will see that $\mathbf{X}^{(\widetilde{m}_{i-1})} - \mathbf{X}^{(\widetilde{m}_i)}$ is determined only by $\langle\!\lfloor x \rfloor\!\rangle_{\widetilde{m}_{i-1}}^{\widetilde{m}_i}$ on $A_{\varsigma,u_1,\dots,u_M}$. Note the assumption of k, α, and m, i.e., $k \ge 2$ and

$$\alpha = 0.\underbrace{*\cdots*}_{m}\underbrace{0\cdots0}_{k+\kappa}\underbrace{\underbrace{0\cdots0}_{\kappa+2}1\underbrace{0\cdots0}_{\kappa+2}1\cdots\underbrace{0\cdots0}_{\kappa+2}1}_{M}\underbrace{0\cdots0}_{k+\kappa}*\cdots.$$

Since $\langle\!\lfloor\alpha\rfloor\!\rangle_{\widetilde{m}_i}^{\widetilde{m}_i+\kappa+2}=0$, we have

$$l\langle\alpha\rangle_{\widetilde{m}_i}<\frac{1}{b^{\widetilde{m}_i+2}}\qquad\text{for}\quad 0\le i\le M$$

in the same way as (3.1).

Let $x\in A_{\varsigma,u_1,\dots,u_M}$. Since $\langle\!\lfloor x\rfloor\!\rangle_{\widetilde{m}_i}^{\widetilde{m}_{i+1}}=u_{i+1}/b^{\widetilde{m}_{i+1}}$ for $0\le i<M$ and $\langle\!\lfloor x\rfloor\!\rangle_{\widetilde{m}_M}^{\widetilde{m}_M+1}=0$, we have

$$\begin{aligned}\langle x\rangle_{\widetilde{m}_i}&=\langle\!\lfloor x\rfloor\!\rangle_{\widetilde{m}_i}^{\widetilde{m}_{i+1}}+\langle x\rangle_{\widetilde{m}_{i+1}}\\&<\frac{u_{i+1}+1}{b^{\widetilde{m}_{i+1}}}\le\frac{b^{\kappa+3}-b^{\kappa+1}}{b^{\widetilde{m}_{i+1}}}=\frac{1}{b^{\widetilde{m}_i}}-\frac{1}{b^{\widetilde{m}_i+2}}\qquad\text{for}\quad 0\le i<M,\\\langle x\rangle_{\widetilde{m}_M}&=\langle\!\lfloor x\rfloor\!\rangle_{\widetilde{m}_M}^{\widetilde{m}_M+1}+\langle x\rangle_{\widetilde{m}_M+1}\le\frac{1}{b^{\widetilde{m}_M+1}}<\frac{1}{b^{\widetilde{m}_M}}-\frac{1}{b^{\widetilde{m}_M+2}}.\end{aligned}$$

Thus, no carry arises from the addition $x+l\alpha$ at $\widetilde{m}_i$-th digit, i.e. $\lfloor\langle x\rangle_{\widetilde{m}_i}+l\langle\alpha\rangle_{\widetilde{m}_i}\rfloor^{\widetilde{m}_i}=0$ for $0\le i\le M$. Therefore

$$\langle\!\lfloor x+l\alpha\rfloor\!\rangle_{\widetilde{m}_{i-1}}^{\widetilde{m}_i}=\langle\lfloor x\rfloor^{\widetilde{m}_i}+l\lfloor\alpha\rfloor^{\widetilde{m}_i}\rangle_{\widetilde{m}_{i-1}}=\langle\langle\!\lfloor x\rfloor\!\rangle_{\widetilde{m}_{i-1}}^{\widetilde{m}_i}+l\langle\!\lfloor\alpha\rfloor\!\rangle_{\widetilde{m}_{i-1}}^{\widetilde{m}_i}\rangle_{\widetilde{m}_{i-1}}.$$

Thus

$$\begin{aligned}X_l^{(\widetilde{m}_i)}(x)-X_l^{(\widetilde{m}_{i-1})}(x)&=\sum_{j=\widetilde{m}_{i-1}+1}^{\widetilde{m}_i}d^{(j)}(\langle\!\lfloor x+l\alpha\rfloor\!\rangle_{\widetilde{m}_{i-1}}^{\widetilde{m}_i})\\&=\sum_{j=\widetilde{m}_{i-1}+1}^{\widetilde{m}_i}d^{(j)}(\langle\!\lfloor x\rfloor\!\rangle_{\widetilde{m}_{i-1}}^{\widetilde{m}_i}+l\langle\!\lfloor\alpha\rfloor\!\rangle_{\widetilde{m}_{i-1}}^{\widetilde{m}_i}).\end{aligned}$$

Since $\langle\!\lfloor\alpha\rfloor\!\rangle_{\widetilde{m}_{i-1}}^{\widetilde{m}_i}=1/b^{\widetilde{m}_i}$ for $1\le i\le M$ and $\langle\!\lfloor\alpha\rfloor\!\rangle_{\widetilde{m}_{-1}}^{\widetilde{m}_0}=0$,

$$\begin{aligned}X_l^{(\widetilde{m}_i)}(x)-X_l^{(\widetilde{m}_{i-1})}(x)&=\sum_{j=\widetilde{m}_{i-1}+1}^{\widetilde{m}_i}d^{(j)}\left(\frac{u_i+l}{b^{\widetilde{m}_i}}\right)\\&=Y(u_i+l)\qquad\text{for}\quad 1\le i\le M,\\X_l^{(\widetilde{m}_0)}(x)-X_l^{(\widetilde{m}_{-1})}(x)&=\sum_{j=\widetilde{m}_{-1}+1}^{\widetilde{m}_0}d^{(j)}(\langle\!\lfloor x\rfloor\!\rangle_{\widetilde{m}_{-1}}^{\widetilde{m}_0})=\varsigma.\end{aligned}$$

Therefore

$$\mathbf{X}^{(\widehat{m})}(x)-\mathbf{X}^{(m)}(x)\equiv\varsigma\mathbf{1}+\sum_{i=1}^{M}\mathbf{Y}(u_i).$$

Now we have the inclusion relation (3.2) and complete the proof of Lemma 2.2. □

Finally, we see Lemma 3.1.

Proof of Lemma 3.1. We begin with some properties of the function Y. Let $J := (b-1)b^\kappa + b^{\kappa+2}$ and

$$s_j := \sum_{i=1}^{J} Y(j+i).$$

Then, we have that for $0 \le j < b^\kappa$,

$$\begin{aligned} s_j - s_{j-1} &= \sum_{i=1}^{J} Y(j+i) - \sum_{i=1}^{J} Y(j-1+i) \\ &= Y(j+J) - Y(j) \\ &= \sum_{h=1}^{\kappa+3} \left(d^{(h)} \left(\frac{j}{b^{\kappa+3}} + \frac{b-1}{b^3} + \frac{1}{b^1} \right) - d^{(h)} \left(\frac{j}{b^{\kappa+3}} \right) \right) \\ &= \sum_{h=4}^{\kappa+3} \left(d^{(h)} \left(\frac{j}{b^{\kappa+3}} \right) - d^{(h)} \left(\frac{j}{b^{\kappa+3}} \right) \right) + b - 1 + 1 = 0 \pmod b \end{aligned}$$

and that

$$\begin{aligned} s_{b^\kappa} - s_{b^\kappa - 1} &= \sum_{i=1}^{J} Y(b^\kappa + i) - \sum_{i=1}^{J} Y(b^\kappa - 1 + i) \\ &= Y(b^\kappa + J) - Y(b^\kappa) \\ &= \sum_{h=1}^{\kappa+3} (d^{(h)}(b^{-2} + b^{-1}) - d^{(h)}(b^{-3})) = 1 \pmod b. \end{aligned}$$

Thus, we have $s := s_{-1} = \cdots = s_{b^\kappa - 1} \pmod b$ and $s_{b^\kappa} = s + 1 \pmod b$.

Then, for $1 \le l \le n$,

$$\begin{aligned} \sum_{i=1}^{J} \mathbf{Y}(b^\kappa - l + i) &\equiv \sum_{i=1}^{J} (Y(b^\kappa - l + i), \ldots, Y(b^\kappa - l + n - 1 + i)) \\ &\equiv (s_{b^\kappa - l}, \ldots, s_{b^\kappa - l + n - 1}) \\ &\equiv (\underbrace{s, \ldots, s}_{l}, s+1, s_{b^\kappa + 1}, \ldots, s_{b^\kappa - l + n - 1}). \end{aligned}$$

Therefore,

$$-s\mathbf{1} + \sum_{i=1}^{J} \mathbf{Y}(b^\kappa - l + i) \equiv (\underbrace{0, \ldots, 0}_{l}, 1, s_{b^\kappa + 1} - s, \ldots, s_{b^\kappa - l + n - 1} - s) \equiv: \sigma_l.$$

Let $\sigma_0 := \mathbf{1}$. Then, for any $\sigma \in \Sigma$, there exist $M_l \ge 0$ such that $\sigma \equiv M_0\sigma_0 + \cdots + M_{n-1}\sigma_{n-1}$ and $M_0 + \cdots + M_{n-1} \le n(b-1)$. Therefore, since $\sigma_n \equiv \mathbf{0}$, $\sigma \equiv M_0\sigma_0 + \cdots + M_{n-1}\sigma_{n-1} + M_n\sigma_n$ and $M_1 + \cdots + M_n = n(b-1)$

where $M_n := n(b-1) - (M_1 + \cdots + M_{n-1})$. Thus, we have

$$\begin{aligned}\sigma &\equiv M_0\mathbf{1} + \sum_{l=1}^{n} M_l \left(-s\mathbf{1} + \sum_{i=1}^{J} \mathbf{Y}(b^\kappa - l + i) \right) \\ &\equiv \left(M_0 - s\sum_{l=1}^{n} M_l \right) \mathbf{1} + \sum_{l=1}^{n} M_l \sum_{i=1}^{J} \mathbf{Y}(b^\kappa - l + i).\end{aligned}$$

Let

$$\begin{aligned}\varsigma &:= M_0 - s\sum_{l=1}^{n} M_l \pmod b \\ u_i &:= b^\kappa - l' + ((i-1) \bmod J) + 1\end{aligned}$$

for $1 \le l' \le n$ and $J\sum_{1\le l<l'} M_l < i \le J\sum_{1\le l\le l'} M_l$. Then, since $M = (b^{\kappa+2} + (b-1)b^\kappa)n(b-1) = J\sum_{l=1}^{n} M_l$, we have

$$\sigma \equiv \varsigma\mathbf{1} + \sum_{i=1}^{M} \mathbf{Y}(u_i)$$

and $0 \le u_i \le b^\kappa + J - 1 = b^{\kappa+1} + b^{\kappa+2} - 1 < b^{\kappa+3} - b^{\kappa+1}$. □

Kobe University
Rokko Kobe 657-8501, Japan
e-mail: yasutomi@math.kobe-u.ac.jp

References

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

[2] ———, Lectures at Kobe university, 2000.

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

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