A limit theorem for sequences generated by Weyl transformation : Disappearance of dependence

Kenji Yasutomi
Graduate School of Science and Technology Kobe University
Rokko, Kobe 657-8501, Japan
yasutomi@math.sci.kobe-u.ac.jp

1 Introduction

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

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

Let us identify $\{0,1\}$ with the group $\mathbb{Z}/2\mathbb{Z}$ and define an addition.

Theorem A. *For* a.e. α *with respect to the Lebesgue measure, the process* $\{X_n^{(m)}(\,\cdot\,,\alpha)\}_{n=0}^{\infty}$ *converges in law to* $\{0,1\}$*-valued fair i.i.d. when* $m \to \infty$*, i.e., for all* $n \in \mathbb{N}$ *and* $s_0, \ldots, s_{n-1} \in \{0,1\}$*,*

$$P\big(X_0^{(m)}(\,\cdot\,,\alpha) = s_0, \ldots, X_{n-1}^{(m)}(\,\cdot\,,\alpha) = s_{n-1}\big) \longrightarrow \frac{1}{2^n} \qquad (m \to \infty)$$

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. Theorem **??** claims that the dependence disappears when $m \to \infty$. Since the proof of this mysterious theorem is very complicated, Sugita [**?**] tried to give a simple proof based on ergodic theory. He showed the following theorem, which is weaker than Theorem **??** but can be proved simply.

Theorem B. *The process* $\{X_n^{(m)}(\,\cdot\,,\,\cdot\,)\}_{n=0}^{\infty}$ *on* $[0,1)^2$ *converges in law to* $\{0,1\}$*-valued fair i.i.d. when* $m \to \infty$ *where the measure of* $[0,1)^2$ *is the Lebesgue measure.*

Takanobu [**?**] studied on this theorem in detail. In this paper, we extend Theorem **??** and give a simple proof by modifying the idea of Sugita [**?**].

To state our result, we introduce notation. Let b be a natural number greater than 1, $d^{(m)}(x)$ be the m-th digit of $x \geq 0$ in its base-b expansion, and $X_n^{(m)}$ be a $\{0, \ldots, b-1\}$-valued function on $[0,1)^2$ such that

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

Let us identify $\{0, \ldots, b-1\}$ with the group $\mathbb{Z}/b\mathbb{Z}$. We define μ and ν to be two Bernoulli measures on $[0,1)$, i.e., each μ and ν makes $\{d^{(m)}\}_m$ an i.i.d., and assume that $\nu\big(d^{(m)} = l\big) \neq 0$ and $\mu\big(d^{(m)} = l\big) \neq 0$ for $l \in \{0, \ldots, b-1\}$.

Theorem 1. *For μ-a.e. α, the process $\{X_n^{(m)}(\,\cdot\,, \alpha)\}_{n=0}^{\infty}$ on $([0,1), \nu)$ converges in law to the $\{0, \ldots, b-1\}$-valued fair i.i.d. when $m \to \infty$, i.e., for all $n \in \mathbb{N}$ and $s_0, \ldots, s_{n-1} \in \{0, \ldots, b-1\}$,*

$$\nu\big(X_0^{(m)}(\,\cdot\,, \alpha) = s_0, \ldots, X_{n-1}^{(m)}(\,\cdot\,, \alpha) = s_{n-1}\big) \longrightarrow \frac{1}{b^n} \qquad (m \to \infty). \tag{1}$$

Theorem **??** implies Theorem **??** when μ and ν are the Lebesgue measures and $b = 2$. We can show that Theorem **??** is valid when ν is replaced with a measure ν' which is absolutely continuous with respect to a Bernoulli measure ν and that the order of convergence of the Theorem **??** is exponential for μ-a.e. α.

2 Proof of the Theorem

To prove Theorem **??**, it is sufficient to show the formula (**??**) for all $n \in \mathbb{N}$ and $s_0, \ldots, s_{n-1} \in \{0, \ldots, b-1\}$. Let $\Omega := [0,1)^3$, and $P := \nu \times \nu \times \mu$. Two processes $\{\mathbf{X}^{(m)}\}_m$ and $\{\mathbf{Y}^{(m)}\}_m$ are defined on (Ω, P) as

$$\mathbf{X}^{(m)}(x, y, \alpha) := \sum_{k=1}^{m} (d^{(k)}(x), d^{(k)}(x+\alpha), \ldots, d^{(k)}(x+(n-1)\alpha)) \pmod b,$$

$$\mathbf{Y}^{(m)}(x, y, \alpha) := \sum_{k=1}^{m} (d^{(k)}(y), d^{(k)}(y+\alpha), \ldots, d^{(k)}(y+(n-1)\alpha)) \pmod b.$$

Let us identify $\{0, \ldots, b-1\}^n$ with the group $(\mathbb{Z}/b\mathbb{Z})^n$. Note that $\mathbf{X}^{(m)}$, $\mathbf{Y}^{(m)}$, and $(X_0^{(m)}, \ldots, X_{n-1}^{(m)})$ have the same distribution. Therefore, the formula (**??**) can be written as

$$\nu\big(\mathbf{X}^{(m)}(\,\cdot\,, y, \alpha,) = \mathbf{s}\big) \longrightarrow \frac{1}{b^n} \quad \mu\text{-a.e. } \alpha \qquad (m \to \infty). \tag{2}$$

Thus, it is sufficient to show that

$$\sum_{m=1}^{\infty} \int \left\{ \nu\big(\mathbf{X}^{(m)}(\,\cdot\,, y, \alpha) = \mathbf{s}\big) - \frac{1}{b^n} \right\}^2 \mu(d\alpha) < \infty. \tag{3}$$

Let $\lfloor \cdot \rfloor$ be the floor function, and β be the base-b transformation, i.e., $\beta x := bx - \lfloor bx \rfloor$.

We define an $\mathbb{Z}^{2n+1}$-valued process $\mathbf{Z}^{(m)}$ by

$$\begin{aligned} Z_{1,l}^{(m)}(x, y, \alpha) &:= \lfloor b(\beta^{m-1}x + l\beta^{m-1}\alpha) \rfloor, \\ Z_{2,l}^{(m)}(x, y, \alpha) &:= \lfloor b(\beta^{m-1}y + l\beta^{m-1}\alpha) \rfloor, \\ Z_{3}^{(m)}(x, y, \alpha) &:= \lfloor b\beta^{m-1}\alpha \rfloor, \\ \mathbf{Z}^{(m)} &:= (Z_{1,0}^{(m)}, \dots, Z_{1,n-1}^{(m)}, Z_{2,0}^{(m)}, \dots, Z_{2,n-1}^{(m)}, Z_{3}^{(m)}). \end{aligned}$$

Proposition 2. *$\{(\mathbf{Z}^{(m)}, \mathbf{X}^{(m)}, \mathbf{Y}^{(m)})\}_m$ is an irreducible and aperiodic markov process, and its stationary initial distribution $\{\pi_{\mathbf{u},\mathbf{s},\mathbf{t}}\}$ satisfies*

$$\pi_{\mathbf{u},\mathbf{s},\mathbf{t}} = P(\mathbf{Z}^{(1)} = \mathbf{u}) \frac{1}{b^{2n}}.$$

Now, let us show the formula (**??**). By noting that $\mathbf{X}^{(m)}$ and $\mathbf{Y}^{(m)}$ are identically distributed, that $\mathbf{X}^{(m)}$ does not depend on y and $\mathbf{Y}^{(m)}$ does not depend on x, and that $\mathbf{X}^{(m)}$ and $\mathbf{Y}^{(m)}$ are independent when α is fixed, we have

$$\begin{aligned} &\int \big\{ \nu\big(\mathbf{X}^{(m)}(\,\cdot\,, y, \alpha) = \mathbf{s}\big) - \frac{1}{b^n} \big\}^2 \mu(d\alpha) \\ &= \int \nu\big(\mathbf{X}^{(m)}(\,\cdot\,, y, \alpha) = \mathbf{s}\big) \nu\big(\mathbf{Y}^{(m)}(x, \,\cdot\,, \alpha) = \mathbf{s}\big) \mu(d\alpha) - \frac{1}{b^{2n}} \\ &\qquad - 2\frac{1}{b^n} \Big\{ \int \nu\big(\mathbf{X}^{(m)}(\,\cdot\,, y, \alpha) = \mathbf{s}\big) \mu(d\alpha) - \frac{1}{b^n} \Big\} \\ &= P\big(\mathbf{X}^{(m)} = \mathbf{s}, \mathbf{Y}^{(m)} = \mathbf{s}\big) - \frac{1}{b^{2n}} - 2\frac{1}{b^n} \big\{ P\big(\mathbf{X}^{(m)} = \mathbf{s}\big) - \frac{1}{b^n} \big\}. \end{aligned}$$

By Proposition **??**, we have

$$\sum_{\mathbf{u}} \pi_{\mathbf{u},\mathbf{s},\mathbf{s}} = \frac{1}{b^{2n}}, \qquad \sum_{\mathbf{u},\mathbf{t}} \pi_{\mathbf{u},\mathbf{s},\mathbf{t}} = \frac{1}{b^n}.$$

Therefore, by noting the following theorem, we see that the summand in the formula (**??**) converges to 0 in exponential order and is summable in m. □

Theorem C. (Billingsley [**?**, theorem 8.9]) *For an irreducible and aperiodic markov process which have a finite state space and transition probability $p_{ij}^{(n)}$, there exists a stationary distribution $\{\pi_i\}$ such that $|p_{ij}^{(n)} - \pi_j| \le A\rho^n$ for some $A > 0$ and $0 \le \rho < 1$.*

References

[1] Billingsley, Patrick, Probability and measure. Third edition. Wiley Series in Probability and Mathematical Statistics. A Wiley-Interscience Publication, John Wiley & Sons Inc. (1995)

[2] Billingsley, Patrick, Convergence of probability measures. Second edition. Wiley Series in Probability and Statistics: Probability and Statistics. A Wiley-Interscience Publication. John Wiley & Sons, Inc. (1999)

[3] Sugita, Hiroshi, Pseudo-random number generator by means of irrational rotation. Monte Carlo Methods Appl. 1 (1995), no. 1, 35–57.

[4] Sugita, Hiroshi, Lectures at Kobe university (2000)

[5] Takanobu, Satoshi, On the strong-mixing property of skew product of binary transformation on 2-dimensional torus by irrational rotation. (preprint) (2000)

RESUME

Dans le article [**?**] Sugita étudie un générateur de nombres pseudo-aléatoires et montre un théoréme sur la disparition de dépendance de quelques suites. Parce que la preuve du théoréme est trés compliquée, nous faisons une extension du théoréme et donnons une preuve simple.