

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

神戸大学自然科学研究科 安富 健児 (Kenji Yasutomi)
Graduate School of Science and Technology,
Kobe University

1 Introduction

杉田 [3] は Weyl 変換による擬似乱数生成を提案している. 即ち, $d^{(m)}(x)$ を実数 $x \geq 0$ の 2 進展開の少数点以下第 m 桁目の数を表すものとし, $[0, 1)^2$ 上の $\{0, 1\}$ -値関数 $X_n^{(m)}$ を

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

で定めると, $\{X_n^{(m)}(\cdot, \alpha)\}_{n=0}^\infty$ はほとんど全ての α に対し m が十分大きいとき random であるというものである. 杉田 [3] は次の定理を示し, これについての数学的基礎を与えた.

定理 1. Lebesgue 測度に関してほとんどすべての α に対し確率過程 $\{X_n^{(m)}(\cdot, \alpha)\}_{n=0}^\infty$ は $m \rightarrow \infty$ のとき, 硬貨投げの確率過程に有限次元分布の意味で収束する. 即ち, 任意の $n \in \mathbb{N}$, 任意の $s_0, \dots, s_{n-1} \in \{0, 1\}$ に対して $m \rightarrow \infty$ のとき,

$$P(X_0^{(m)}(\cdot, \alpha) = s_0, \dots, X_{n-1}^{(m)}(\cdot, \alpha) = s_{n-1}) \rightarrow \frac{1}{2^n}.$$

ここで P は $[0, 1)$ 上の Lebesgue 測度である.

過程 $\{X_n^{(m)}(\cdot, \alpha)\}_{n=0}^\infty$ は無理数 α による Weyl 変換によって生成されており, 強い従属性を持っているが定理 1 は $m \rightarrow \infty$ のときにその従属性が消滅することを主張している. 証明は非常に技巧的であったため, 杉田 [4] はエルゴード論的手法による証明を試み, やや弱い以下の定理を独立に証明することに成功している.

定理 2. $[0, 1]^2$ 上で定義された確率過程として, $\{X_n^{(m)}\}_{n=0}^\infty$ は $m \rightarrow \infty$ のとき, 硬貨投げの確率過程に有限次元分布の意味で収束する. 即ち, 任意の $n \in \mathbb{N}$, 任意の $s_0, \dots, s_{n-1} \in \{0, 1\}$ に対して $m \rightarrow \infty$ のとき,

$$P(X_0^{(m)}(\cdot, \cdot) = s_0, \dots, X_{n-1}^{(m)}(\cdot, \cdot) = s_{n-1}) \rightarrow \frac{1}{2^n}.$$

ここで P は $[0, 1]^2$ 上の Lebesgue 測度である.

高信 [5] もこの定理について調べている. ここではその考察を押し進め, 定理 1 の拡張にシンプルな証明を与える. 杉田 [3] による証明は従属性の消滅が成立するような α について具体的に十分条件を与えるので, 厳密には我々の定理は完全な拡張ではない.

我々の定理を述べる為に記号等をあらたに定義し直す. b を 2 以上の自然数とする. $d^{(m)}(x)$ は実数 $x \geq 0$ の b 進展開の少数点以下第 m 桁目の数を表すとし, $[0, 1]^2$ からの $\{0, \dots, b-1\}$ -値関数 $X_n^{(m)}$ を先と同様に

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

で定める.

μ, ν は $[0, 1]$ 上の Bernoulli 測度とする, ここでは Bernoulli 測度とは $\{d^{(m)}\}_m$ を $\mu(d^{(1)} = l) \neq 0, l \in \{0, \dots, b-1\}$ なる i.i.d. にする確率測度とする.

定理 3. μ に関してほとんどすべての α に対し $([0, 1], \nu)$ 上の確率過程 $\{X_n^{(m)}(\cdot, \alpha)\}_{n=0}^\infty$ は $m \rightarrow \infty$ のとき, $\{0, \dots, b-1\}$ 値の fair な i.i.d. に有限次元分布の意味で収束する. 即ち, 任意の $n \in \mathbb{N}$, 任意の $s_0, \dots, s_{n-1} \in \{0, \dots, b-1\}$ に対して $m \rightarrow \infty$ のとき,

$$\nu(X_0^{(m)}(\cdot, \alpha) = s_0, \dots, X_{n-1}^{(m)}(\cdot, \alpha) = s_{n-1}) \rightarrow \frac{1}{b^n}.$$

定理 1 は定理 3 で特に μ, ν を Lebesgue 測度, $b = 2$ とおいて得られるものである.

2 Proof of the theorem

この節では定理 3 の証明を与えるが, まず $n \in \mathbb{N}$ を任意に取って固定して議論を始める. さらに以下の議論はすべて $\Omega := [0, 1]^3$ 上で行う. Ω 上の測度 P は直積測度 $\nu \times \nu \times \mu$ とする. $\{0, \dots, b-1\}$ -値関数 $\mathbf{X}_1, \mathbf{X}_2$ を

$$\mathbf{X}_j^{(m)}(x_1, x_2, \alpha) := \sum_{k=1}^m (d^{(k)}(x_j), d^{(k)}(x_j + \alpha), \dots, d^{(k)}(x_j + (n-1)\alpha)) \pmod{b}$$

とくに $\mathbf{X}_1, \mathbf{X}_2$ は共に $(X_0^{(m)}, \dots, X_{n-1}^{(m)})$ と同分布であり, 定理 3 の証明には任意の $\mathbf{s} \in \{0, \dots, b-1\}^n$ に対し

$$\nu(\mathbf{X}_1^{(m)}(\cdot, x_2, \alpha) = \mathbf{s}) \rightarrow \frac{1}{b^n} \quad \mu\text{-a.s.}\alpha \quad (1)$$

を示せばよい.

$[\cdot]$ は Gauss 記号または floor function と呼ばれるもので小数部分を切捨てて整数部分を与える. β は b 進小数展開の shift を表す. 即ち, $\beta x := bx - [bx]$.

\mathbb{N}^{2n+1} -値確率変数 $\mathbf{Z}^{(m)}$ を

$$\begin{aligned} \mathbf{Z}^{(m)} &:= (Z_{1,0}^{(m)}, \dots, Z_{1,n-1}^{(m)}, Z_{2,0}^{(m)}, \dots, Z_{2,n-1}^{(m)}, Z_3^{(m)}) \\ Z_{j,i}^{(m)}(x_1, x_2, \alpha) &:= [b(\beta^{m-1}x_j + l\beta^{m-1}\alpha)] \\ Z_3^{(m)}(x_1, x_2, \alpha) &:= [b\beta^{m-1}\alpha] \end{aligned}$$

で定め, $\mathbf{Z}^{(1)}$ の値域を $\text{Im } \mathbf{Z}$ で表す.

定理の証明を述べる. 証明にあたって $\{(\mathbf{Z}^{(m)}, \mathbf{X}_1^{(m)}, \mathbf{X}_2^{(m)})\}_m$ は状態空間が有限な既約非周期的 Markov 過程であり, その $\mathbf{u} \in \text{Im } \mathbf{Z}$, $\mathbf{s}, \mathbf{t} \in \{0, \dots, b-1\}^n$ の極限分布 $\{\pi_{\mathbf{u}, \mathbf{s}, \mathbf{t}}\}$ が

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

で与えられることを仮定する. このことは次節で証明する.

$$\begin{aligned} & \int (\nu(\mathbf{X}_1^{(m)}(\cdot, x_2, \alpha) = \mathbf{s}) - \frac{1}{b^n})^2 \mu(d\alpha) \\ &= \int \{(\nu(\mathbf{X}_1^{(m)}(\cdot, x_2, \alpha) = \mathbf{s}))^2 - \frac{1}{b^{2n}} \\ & \quad - 2\frac{1}{b^n}(\nu(\mathbf{X}_1^{(m)}(\cdot, x_2, \alpha) = \mathbf{s}) - \frac{1}{b^n})\} \mu(d\alpha) \end{aligned}$$

$\mathbf{X}_1^{(m)}, \mathbf{X}_2^{(m)}$ は α を固定したときに独立同分布であるので

$$\begin{aligned} &= \int (\nu \times \nu)(\mathbf{X}_1^{(m)}(\cdot, \cdot, \alpha) = \mathbf{s}, \mathbf{X}_2^{(m)}(\cdot, \cdot, \alpha) = \mathbf{s}) \mu(d\alpha) - \frac{1}{b^{2n}} \\ & \quad - 2\frac{1}{b^n} \left(\int (\nu \times \nu)(\mathbf{X}_1^{(m)}(\cdot, \cdot, \alpha) = \mathbf{s}) \mu(d\alpha) - \frac{1}{b^n} \right) \\ &= P(\mathbf{X}_1^{(m)} = \mathbf{s}, \mathbf{X}_2^{(m)} = \mathbf{s}) - \frac{1}{b^{2n}} - 2\frac{1}{b^n} (P(\mathbf{X}_1^{(m)} = \mathbf{s}) - \frac{1}{b^n}) \end{aligned}$$

であるが, 特に $\{(\mathbf{Z}^{(m)}, \mathbf{X}_1^{(m)}, \mathbf{X}_2^{(m)})\}_m$ は状態空間が有限な既約非周期的 Markov 過程で

$$\sum_{\mathbf{u} \in \text{Im } \mathbf{Z}} \pi_{\mathbf{u}, \mathbf{s}, \mathbf{s}} = \frac{1}{b^{2n}} \quad \sum_{\mathbf{u}, \mathbf{t} \in \text{Im } \mathbf{Z}} \pi_{\mathbf{u}, \mathbf{s}, \mathbf{t}} = \frac{1}{b^n}$$

であることより, 上式右辺の第一項, 第二項は共に指数関数の速さで 0 に収束することがたとえば次の定理より得られる.

定理 4. (Billingsley [1, Theorem 8.9]) (推移確率 $p_{ij}^{(n)}$ をもつ Markov 過程について) 状態空間が有限で過程が既約かつ非周期的ならば, 定常分布 $\{\pi_i\}$ が存在して, ある $A > 0, 0 < \rho < 1$ に対し,

$$|p_{ij}^{(n)} - \pi_j| \leq A\rho^n.$$

よって

$$\sum_{m=1}^{\infty} \int (\nu(\mathbf{X}_1^{(m)}(\cdot, x_2, \alpha) = \mathbf{s}) - \frac{1}{b^n})^2 \mu(d\alpha) < \infty$$

Beppo-Levi の定理または Fatou's lemma より

$$\sum_{m=1}^{\infty} (\nu(\mathbf{X}_1^{(m)}(\cdot, x_2, \alpha) = \mathbf{s}) - \frac{1}{b^n})^2 < \infty \quad \mu\text{-a.e.}\alpha.$$

よって式 1 が得られる。□

3 Lemmas

この節では $\{(\mathbf{Z}^{(m)}, \mathbf{X}_1^{(m)}, \mathbf{X}_2^{(m)})\}_m$ が既約非周期的 Markov 過程であることを順次示す。

補題 1. $\{\mathbf{Z}^{(m)}\}$ は時間的一様な既約非周期的 Markov 過程。

(証明)

$$\mathbf{u}^{(k)} = (u_{1,0}^{(k)}, \dots, u_{1,n-1}^{(k)}, u_{2,0}^{(k)}, \dots, u_{2,n-1}^{(k)}, u_3^{(k)}) \in \text{Im } \mathbf{Z} \quad (1 \leq k \leq m+1)$$

$$A := \left\{ (x_1, x_2, \alpha) \mid \mathbf{Z}^{(k)}(x_1, x_2, \alpha) = \mathbf{u}^{(k)}, 1 \leq k \leq m \right\},$$

$$B := \left\{ (x_1, x_2, \alpha) \mid \mathbf{Z}^{(k)}(x_1, x_2, \alpha) = \mathbf{u}^{(k)}, 1 \leq k \leq m+1 \right\}$$

とし, B の A による条件付き確率を調べる. $P(A) > 0$ のときを調べれば十分であるので, 以下 $P(A) > 0$ として議論する.

$$A' := \left\{ (x_1, x_2, \alpha) \mid \mathbf{Z}^{(m)}(x_1, x_2, \alpha) = \mathbf{u}^{(m)}, \begin{array}{l} Z_{1,0}^{(k)}(x_1, x_2, \alpha) = u_{1,0}^{(k)} \\ Z_{2,0}^{(k)}(x_1, x_2, \alpha) = u_{2,0}^{(k)} \\ Z_3^{(k)}(x_1, x_2, \alpha) = u_3^{(k)} \end{array}, 1 \leq k < m \right\}$$

とおけば $A = A'$ であることを示す. $A \subset A'$ は明らかであるので $A \supset A'$ を示せば良い.

まず $Z_{j,l}^{(k)}$ の定義より ($\cdot \cdot bx = \beta x + [bx]$)

$$\begin{aligned} Z_{j,l}^{(k)}(x_1, x_2, \alpha) &= [b(\beta^{(k-1)}x_j + l\beta^{(k-1)}\alpha)] \\ &= [\beta^k x_j + [b\beta^{(k-1)}x_j] + l\beta^k \alpha + l[b\beta^{(k-1)}\alpha]] \\ &= [\beta^k x_j + l\beta^k \alpha] + [b\beta^{(k-1)}x_j] + l[b\beta^{(k-1)}\alpha] \\ &= \left[\frac{l}{b} Z_{j,l}^{(k+1)}(x_1, x_2, \alpha) \right] + [Z_{j,0}^{(k)}(x_1, x_2, \alpha)] + l[Z_3^{(k)}(x_1, x_2, \alpha)]. \end{aligned}$$

$u_{j,l}^{(k)}$ について $P(A) > 0$ より $A \neq \phi$ であるので

$$u_{j,l}^{(k)} = \lfloor \frac{1}{b} u_{j,l}^{(k+1)} \rfloor + u_{j,0}^{(k)} + l u_3^{(k)}$$

よって

$$Z_{j,l}^{(k+1)} = u_{j,l}^{(k+1)}, Z_{j,0}^{(k)} = u_{j,0}^{(k)}, Z_3^{(k)} = u_3^{(k)} \implies Z_{j,l}^{(k)} = u_{j,l}^{(k)}.$$

k について帰納的に

$$\begin{aligned} Z_{j,l}^{(m)} &= u_{j,l}^{(m)}, Z_{j,0}^{(k)} = u_{j,0}^{(k)}, Z_3^{(k)} = u_3^{(k)}, 0 \leq k < m \\ &\implies Z_{j,l}^{(k)} = u_{j,l}^{(k)}, 0 \leq k \leq m. \end{aligned}$$

即ち $A \supset A'$.

今 $Z_{j,0}^{(k)}(x_1, x_2, \alpha) = \lfloor b\beta^{(k-1)}x_j \rfloor = d^{(k)}(x_j)$ であり, $\mathbf{Z}^{(m)}$ は x_1, x_2, α の b 進展開の m 桁目以後にのみ依るので $d^{(m)}(\cdot), d^{(m+1)}(\cdot), \dots$ の関数で表現できるので, $\{d^{(k)}(x_1), d^{(k)}(x_2), d^{(k)}(\alpha)\}$ の独立性より,

$$P(A) = P(A') = P(\mathbf{Z}^{(m)} = \mathbf{u}^{(m)}) \prod_{k=1}^{m-1} P \left(\begin{array}{l} d_k(x_j) = u_{j,0}^{(k)} \\ d_k(\alpha) = u_3^{(k)} \end{array} \right)$$

同様にして

$$P(B) = P(\mathbf{Z}^{(m+1)} = \mathbf{u}^{(m+1)}, \mathbf{Z}^{(m)} = \mathbf{u}^{(m)}) \prod_{k=1}^{m-1} P \left(\begin{array}{l} d_k(x_j) = u_{j,0}^{(k)} \\ d_k(\alpha) = u_3^{(k)} \end{array} \right)$$

よって

$$P(B|A) = P(\mathbf{Z}^{(m+1)} = \mathbf{u}^{(m+1)} | \mathbf{Z}^{(m)} = \mathbf{u}^{(m)}).$$

即ち $\{\mathbf{Z}^{(m)}\}_m$ は Markov 過程. さらに b 進変換の保測性より時間的一様で, 弱混合性より既約非周期的である \square

ここで記号を整理する. 特に $\text{Im } \mathbf{Z}$ 上にある $\{0, \dots, b-1\}^n$ -値関数 $\hat{\mathbf{d}}_1, \hat{\mathbf{d}}_2$ が存在して

$$(\hat{\mathbf{d}}_j \circ \mathbf{Z}^{(m)})(x_1, x_2, \alpha) = (d^{(m)}(x_j), d^{(m)}(x_j + \alpha), \dots, d^{(m)}(x_j + (n-1)\alpha))$$

とできる. ($\hat{\mathbf{d}}_j = (\hat{d}_{j,0}, \dots, \hat{d}_{j,n-1})$, $\hat{d}_{j,l}(\cdot) := \cdot - b \lfloor \frac{\cdot}{b} \rfloor$, ($j = 1, 2, 0 \leq l \leq n-1$) とすれば良い.)

これにより

$$\mathbf{X}_j^{(m)} = \sum_{k=1}^m \hat{\mathbf{d}}_j \circ \mathbf{Z}^{(k)} \pmod{b}$$

$$G := \{0, \dots, b-1\}^n \times \{0, \dots, b-1\}^n$$

$$\varphi : \rho \ni \mathbf{u} \mapsto (\hat{\mathbf{d}}_1(\mathbf{u}), \hat{\mathbf{d}}_2(\mathbf{u})) \in G$$

$$W^{(m)} := (\mathbf{X}_1^{(m)}, \mathbf{X}_2^{(m)})$$

とおく. 特に G は各成分を $\text{mod } b$ で和をとる演算に対し有限群を成す. $\mathbf{X}_1^{(m)}$, $\mathbf{X}_2^{(m)}$, $\hat{\mathbf{d}}_1$, $\hat{\mathbf{d}}_2$ の定義より $W^{(m)} = \sum_{k=1}^m \varphi(\mathbf{Z}^{(k)})$ がいえる.

補題 2. $\{(\mathbf{Z}^{(m)}, W^{(m)})\}_m$ は時間的一様 Markov 過程

(証明)

$$\mathbf{u}^{(k)} = (u_{1,0}^{(k)}, \dots, u_{1,n-1}^{(k)}, u_{2,0}^{(k)}, \dots, u_{2,n-1}^{(k)}, u_3^{(k)}) \in \text{Im } \mathbf{Z} \quad g_k \in G$$

$$\tilde{A} := \{(\mathbf{Z}^{(k)}, W^{(k)}) = (\mathbf{u}^{(k)}, g_k), 1 \leq k \leq m\}$$

$$\tilde{B} := \{(\mathbf{Z}^{(k)}, W^{(k)}) = (\mathbf{u}^{(k)}, g_k), 1 \leq k \leq m+1\}$$

とおいて, \tilde{B} の \tilde{A} による条件付き確率を調べる.

$W^{(k)} = \varphi(\mathbf{Z}^{(k)}) + W^{(k-1)}$ より $g_0 := 0$ として

$$P(\tilde{A}) = P(\mathbf{Z}^{(k)} = \mathbf{u}^{(k)}, g_k = \varphi(\mathbf{u}^{(k)}) + g_{k-1}, 1 \leq k \leq m)$$

$$= P(\mathbf{Z}^{(k)} = \mathbf{u}^{(k)}, 1 \leq k \leq m) \prod_{k=1}^m \delta_{g_k}^{\varphi(\mathbf{u}^{(k)}) + g_{k-1}}.$$

同様にして

$$P(\tilde{B}) = P(\mathbf{Z}^{(k)} = \mathbf{u}^{(k)}, 1 \leq k \leq m+1) \prod_{k=1}^{m+1} \delta_{g_k}^{\varphi(\mathbf{u}^{(k)}) + g_{k-1}}.$$

よって, $P(\tilde{A}) \neq 0$ のとき,

$$P(\tilde{B} | \tilde{A}) = P(\mathbf{Z}^{(m+1)} = \mathbf{u}^{(m+1)} | \mathbf{Z}^{(k)} = \mathbf{u}^{(k)}, 1 \leq k \leq m) \delta_{g_{m+1}}^{\varphi(\mathbf{u}^{(m+1)}) + g_m}$$

$$= P(\mathbf{Z}^{(2)} = \mathbf{u}^{(m+1)} | \mathbf{Z}^{(1)} = \mathbf{u}^{(m)}) \delta_{g_{m+1}}^{\varphi(\mathbf{u}^{(m+1)}) + g_m} \quad \square$$

既約非周期的を示す為更に幾つかの記号を定義する. 時間的一様 Markov 過程 $\{(\mathbf{Z}^{(m)}, W^{(m)})\}_m$ の (\mathbf{u}, g) から (\mathbf{u}', g') への推移確率を $p^{(k)}((\mathbf{u}, g), (\mathbf{u}', g'))$ で表す. 特に $\{\mathbf{Z}^{(m)}\}_m$ の \mathbf{u} から \mathbf{u}' への推移確率を $p_{\mathbf{Z}}^{(k)}(\mathbf{u}, \mathbf{u}')$ で表せば, Lemma 2 の proof 中の議論から

$$p^{(1)}((\mathbf{u}, g), (\mathbf{u}', g')) = p_{\mathbf{Z}}^{(1)}(\mathbf{u}, \mathbf{u}') \delta_{\varphi(\mathbf{u}') + g}^{g'}$$

特に G の零元を 0_G と書いて

$$p^{(1)}((\mathbf{u}, 0_G), (\mathbf{u}', g)) = p^{(1)}((\mathbf{u}, \cdot), (\mathbf{u}', \cdot + g))$$

であるが、これから容易に

$$p^{(k)}((\mathbf{u}, 0_G), (\mathbf{u}', g)) = p^{(k)}((\mathbf{u}, \cdot), (\mathbf{u}', \cdot + g))$$

が得られる.

$\mathbf{u} \in \text{Im } \mathbf{Z}$ に対し

$$H_{\mathbf{u}} := \{h \mid \exists k p^{(k)}((\mathbf{u}, 0_G), (\mathbf{u}, h)) \neq 0\}$$

とおく. ($\{\mathbf{Z}^{(m)}\}_m$ の既約性より $H_{\mathbf{u}} \neq \emptyset$.)

補題 3. $H_{\mathbf{u}}$ は G の部分群を成す.

(証明)

$h \in H_{\mathbf{u}}$, 任意の $m \in \mathbf{N}$ に対し

$$\begin{aligned} p^{(mk)}((\mathbf{u}, 0_G), (\mathbf{u}, nh)) &\geq \prod_{j=1}^{m-1} p^{(k)}((\mathbf{u}, jh), (\mathbf{u}, (j+1)h)) \\ &= \{p^{(k)}((\mathbf{u}, 0_G), (\mathbf{u}, h))\}^m \end{aligned}$$

であるから $\exists k p^{(mk)}((\mathbf{u}, 0_G), (\mathbf{u}, mh)) \neq 0$, 即ち $mh \in H_{\mathbf{u}}$. G の有限性より $H_{\mathbf{u}}$ は部分群になる \square

補題 4. $H_{\mathbf{u}}$ は \mathbf{u} によらない. ($H := H_{\mathbf{u}}$ が well def)

(証明)

\mathbf{u}, \mathbf{u}' を fix して $H_{\mathbf{u}} = H_{\mathbf{u}'}$ を示す.

$\{\mathbf{Z}^{(m)}\}_m$ の既約性よりある $k_1, k_2 \in \mathbf{N}$, $g_1, g_2 \in G$ が存在して

$$\begin{aligned} p^{(k_1)}((\mathbf{u}, 0_G), (\mathbf{u}', g_1)) &\neq 0 \\ p^{(k_2)}((\mathbf{u}', 0_G), (\mathbf{u}, g_2)) &\neq 0. \end{aligned}$$

$h \in H_{\mathbf{u}}$ についてある k が存在して

$$\begin{aligned} &p^{(k_1+k_2+k)}((\mathbf{u}', 0_G), (\mathbf{u}', g_1 + g_2 + h)) \\ &\geq p^{(k_2)}((\mathbf{u}', 0_G), (\mathbf{u}, g_2)) p^{(k)}((\mathbf{u}, g_2), (\mathbf{u}, g_2 + h)) p^{(k_1)}((\mathbf{u}, g_2 + h), (\mathbf{u}', g_2 + h + g_1)) \\ &\neq 0 \end{aligned}$$

よって $g_1 + g_2 + h \in H_{\mathbf{u}'}$. $0_G \in H_{\mathbf{u}}$ より $g_1 + g_2 \in H_{\mathbf{u}'}$ であるから

$$H_{\mathbf{u}} \subset H_{\mathbf{u}'} - (g_1 + g_2) = H_{\mathbf{u}'}$$

同様にして逆も良い \square

補題 5.

$$D := \{\mathbf{u} \in \text{Im } \mathbf{Z} \mid p_{\mathbf{Z}}^{(1)}(\mathbf{u}, \mathbf{u}) \neq 0\}$$

とおく. $\varphi(D)$ が G を生成することは $\{\{\mathbf{Z}^{(m)}, W^{(m)}\}_m$ が既約になるための十分条件である.

(証明)

任意の $(\mathbf{u}, g), (\mathbf{u}', g')$ に対し $\{\mathbf{Z}^{(m)}\}_m$ の既約性より適当な k' が存在して

$$\begin{aligned} p^{(k'+k)}((\mathbf{u}, g), (\mathbf{u}', g')) &\geq p^{(k')}((\mathbf{u}, g), (\mathbf{u}', g'')) p^{(k)}((\mathbf{u}', g''), (\mathbf{u}', g')) \\ &= (\text{positive}) p^{(k)}((\mathbf{u}', g''), (\mathbf{u}', g')) \end{aligned}$$

よって既約性を得る為には $H = G$ を示せば良い。

$\mathbf{u} \in D$ ならば $\varphi(\mathbf{u})$ について

$$P^{(1)}((\mathbf{u}, 0_G), (\mathbf{u}, \varphi(\mathbf{u}))) = P_{\mathbf{Z}}^{(1)}(\mathbf{u}, \mathbf{u}) \delta_{\varphi(\mathbf{u})}^{\varphi(\mathbf{u})+0_G} = P_{\mathbf{Z}}^{(1)}(\mathbf{u}, \mathbf{u}) \neq 0,$$

即ち $\varphi(\mathbf{u}) \in H_{\mathbf{u}} = H$. よって $\varphi(D)$ が G を生成すれば $H = G$ □

補題 6. $\{\{\mathbf{Z}^{(m)}, W^{(m)}\}\}_m$ は既約な Markov 過程.

(証明)

補題 5 より $\varphi(D)$ が G を生成することを示せば良い. 特に $\mathbf{e}_{n_1, n_2} \in \mathbf{N}^{2n+1}$, $1 \leq n_1, n_2 \leq n$ を

$$\mathbf{e}_{n_1, n_2} := \underbrace{(b-1, \dots, b-1, b, \dots, b)}_{n_1} \underbrace{(b-1, \dots, b-1, b, \dots, b)}_{n_2}, 0$$

とおけば $\varphi = (\hat{\mathbf{d}}_1, \hat{\mathbf{d}}_2)$ の定義より

$$\varphi(\mathbf{e}_{n_1, n_2}) = \left(\underbrace{(b-1, \dots, b-1, 0, \dots, 0)}_{n_1}, \underbrace{(b-1, \dots, b-1, 0, \dots, 0)}_{n_2} \right)$$

であり, $\{\varphi(\mathbf{e}_{n_1, n_2})\}_{n_1, n_2}$ は G を生成するので, 後は $\mathbf{e}_{n_1, n_2} \in \text{Im } \mathbf{Z}^{(1)}$ と $\mathbf{e}_{n_1, n_2} \in D$, 即ち $p_{\mathbf{Z}}^{(1)}(\mathbf{e}_{n_1, n_2}, \mathbf{e}_{n_1, n_2}) \neq 0$ を示せば証明が完結する.

具体的には $P(\mathbf{Z}^{(1)} = \mathbf{Z}^{(2)} = \mathbf{e}_{n_1, n_2}) \neq 0$ を調べれば十分である.

$$\begin{aligned} \mathbf{Z}^{(1)}(x_1, x_2, \alpha) = \mathbf{e}_{n_1, n_2} &\Leftrightarrow \begin{cases} 1 - \frac{1}{b} \leq x_j + l\alpha < 1 & 0 \leq l < n_j \\ 1 \leq x_j + l\alpha < 1 + \frac{1}{b} & n_j \leq l < n \\ 0 \leq \alpha < \frac{1}{b} \end{cases} \\ &\Leftrightarrow \begin{cases} 1 - l\alpha - \frac{1}{b} \leq x_j < 1 - l\alpha & 0 \leq l < n_j \\ 1 - l\alpha \leq x_j < 1 - l\alpha + \frac{1}{b} & n_j \leq l < n \\ 0 \leq \alpha < \frac{1}{b} \end{cases} \\ &\Leftrightarrow \begin{cases} 1 - \frac{1}{b} \leq x_j < 1 - (n_j - 1)\alpha \\ 1 - n_1\alpha \leq x_j < 1 - (n - 1)\alpha + \frac{1}{b} & \text{if } n_j \neq n \\ 0 \leq \alpha < \frac{1}{b} \end{cases} \end{aligned}$$

である. 簡単の為に α により強い条件 $\alpha < \frac{1}{b(n-1)}$ を課した範囲を考えれば,

$$(\mathbf{Z}^{(1)})^{-1}(\mathbf{e}_{n_1, n_2}) \supset \left\{ (x_1, x_2, \alpha) \mid \begin{array}{l} 1 - n_j\alpha \leq x_2 < 1 - (n_j - 1)\alpha \\ 0 \leq \alpha < \frac{1}{b(n-1)} \end{array} \right\}$$

と書いて $(\mathbf{Z}^{(1)})^{-1}(\mathbf{e}_{n_1, n_2})$ は空でない内部を持つのでその Bernoulli 測度は 0 でない. 特に $\mathbf{e}_{n_1, n_2} \in \text{Im } \mathbf{Z}^{(1)}$. さらに

$$\begin{aligned} & (\mathbf{Z}^{(1)})^{-1}(\mathbf{e}_{n_1, n_2}) \cap (\mathbf{Z}^{(2)})^{-1}(\mathbf{e}_{n_1, n_2}) \\ & \supset \left\{ (x_1, x_2, \alpha) \left| \begin{array}{l} 1 - n_j \alpha \leq x_2 < 1 - (n_j - 1)\alpha \\ 0 \leq \alpha < \frac{1}{b^2(n-1)} \end{array} \right. \right\} \end{aligned}$$

でこれもまた正の測度を持つ \square

補題 7. Markov 過程 $\{(\mathbf{Z}^{(m)}, W^{(m)})\}_m$ は非周期的.

(証明)

既約性を示したので非周期的な state が一つ存在すれば良く, (x_1, x_2, α) が十分小さいところを考えれば $\mathbf{0} = (0, \dots, 0) \in D$. 即ち,

$$\begin{aligned} p^{(1)}((\mathbf{0}, g), (\mathbf{0}, g)) &= p_{\mathbf{Z}}^{(1)}(\mathbf{0}, \mathbf{0}) \delta_g^{\varphi(\mathbf{0})+g} \\ &= P(\mathbf{Z}^{(1)} = \mathbf{Z}^{(2)} = \mathbf{0}) \neq 0 \end{aligned}$$

より明らか ($\because \varphi(\mathbf{0}) = 0_G$) \square

補題 8. 既約非周期的 Markov 過程 $\{(\mathbf{Z}^{(m)}, W^{(m)})\}_m$ の $\mathbf{u} \in \text{Im } \mathbf{Z}$, $g \in G$ の極限分布 $\{\pi_{\mathbf{u}, g}\}$ は

$$\pi_{\mathbf{u}, g} := P(\mathbf{Z}^{(1)} = \mathbf{u}) \frac{1}{b^{2n}}$$

で与えられる.

(証明)

既約非周期的より極限分布が一意であるので, $\{\pi_{\mathbf{u}, g}\}$ が定常分布であることを示せば良い.

$$\begin{aligned} & \sum_{\mathbf{u}, g} \pi_{\mathbf{u}, g} P^{(1)}((\mathbf{u}, g), (\mathbf{u}', g')) \\ &= \sum_{\mathbf{u}, g} P(\mathbf{Z}^{(1)} = \mathbf{u}) \frac{1}{b^{2n}} P(\mathbf{Z}^{(2)} = \mathbf{u}' \mid \mathbf{Z}^{(1)} = \mathbf{u}) \delta_{g'}^{\varphi(\mathbf{u}')+g} \\ &= \sum_{\mathbf{u}} P(\mathbf{Z}^{(1)} = \mathbf{u}) \frac{1}{b^{2n}} P(\mathbf{Z}^{(2)} = \mathbf{u}' \mid \mathbf{Z}^{(1)} = \mathbf{u}) \\ &= P(\mathbf{Z}^{(2)} = \mathbf{u}') \frac{1}{b^{2n}} = \pi_{\mathbf{u}', g'} \quad \square \end{aligned}$$

4 The order of the convergence

収束の order について以下の議論ができる. 証明の過程より $\exists \rho < 1$

$$\int \left\{ \nu \left(\mathbf{X}^{(m)}(\cdot, \alpha) = \mathbf{s} \right) - \frac{1}{2^n} \right\}^2 \mu(d\alpha) \leq \text{const.} \rho^m$$

であるので, $\rho < \forall \rho' < 1$

$$\int \left\{ \nu(\mathbf{X}^{(m)}(\cdot, \alpha) = \mathbf{s}) - \frac{1}{2^n} \right\}^2 \mu(d\alpha) \left(\frac{\rho'}{\rho} \right)^m \leq \text{const.} \rho'^m$$

であることより

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

よって定理の証明と同様に

$$C^2(\alpha) := \sum_{m=1}^{\infty} \left\{ \nu(\mathbf{X}^{(m)}(\cdot, \alpha) = \mathbf{s}) - \frac{1}{2^n} \right\}^2 \left(\frac{\rho'}{\rho} \right)^m < \infty \quad \mu\text{-a.e.} \alpha.$$

特に各項を和で評価すれば,

$$\left| \nu(\mathbf{X}^{(m)}(\cdot, \alpha) = \mathbf{s}) - \frac{1}{2^n} \right| \leq C(\alpha) \left(\frac{\rho}{\rho'} \right)^{m/2}.$$

即ち $\rho'' := (\rho/\rho')^{1/2}$ と書いて $\rho'' < 1$ で

$$\left| \nu(\mathbf{X}^{(m)}(\cdot, \alpha) = \mathbf{s}) - \frac{1}{2^n} \right| \leq C(\alpha) \rho''^m.$$

または

$$\log \left| \nu(\mathbf{X}^{(m)}(\cdot, \alpha) = \mathbf{s}) - \frac{1}{2^n} \right| \leq \log C(\alpha) + m \log \rho''.$$

5 Absolutely continuous measures

定理 3 において測度 ν は Bernoulli 測度であったが, 実はそれに絶対連続な確率測度 ν' について良い. ν に対する ν' の密度関数を h とする.

$$\nu'(\mathbf{X}^{(m)}(\cdot, \alpha) = \mathbf{s}) = \int 1_{\{\mathbf{X}^{(m)}(x, \alpha) = \mathbf{s}\}} h(x) \nu(dx) \rightarrow \frac{1}{b^n} \quad \mu\text{-a.e.} \alpha$$

を示せば良い. $\mathcal{F}(d_1, \dots, d_i)$ -可測単関数 h_i を適当に定めて

$$\int |h_i - h| d\nu \rightarrow 0$$

にできる.

$$A \in \mathcal{F}_{\infty} := \bigcup_{i=1}^{\infty} \mathcal{F}(d_1, \dots, d_i)$$

を考える. ($\#\mathcal{F}_{\infty}$: 可算に注意する)

以下定理 3 の証明と同様に

$$\begin{aligned}
& \int (\nu(\mathbf{X}_1^{(m)}(\cdot, x_2, \alpha) = \mathbf{s}, A) - \frac{\nu(A)}{b^n})^2 \mu(d\alpha) \\
&= \int \left\{ (\nu(\mathbf{X}_1^{(m)}(\cdot, x_2, \alpha) = \mathbf{s}, A))^2 - \frac{\nu(A)^2}{b^{2n}} \right. \\
&\quad \left. - 2 \frac{\nu(A)}{b^n} (\nu(\mathbf{X}_1^{(m)}(\cdot, x_2, \alpha) = \mathbf{s}, A) - \frac{\nu(A)}{b^n}) \right\} \mu(d\alpha) \\
&= \int (\nu \times \nu)(\mathbf{X}_1^{(m)}(\cdot, \cdot, \alpha) = \mathbf{s}, A \times [0, 1]) \\
&\quad (\nu \times \nu)(\mathbf{X}_2^{(m)}(\cdot, \cdot, \alpha) = \mathbf{s}, [0, 1] \times A) \mu(d\alpha) - \frac{\nu(A)^2}{b^{2n}} \\
&\quad - 2 \frac{\nu(A)}{b^n} \left(\int (\nu \times \nu)(\mathbf{X}_1^{(m)}(\cdot, \cdot, \alpha) = \mathbf{s}, A \times [0, 1]) \mu(d\alpha) - \frac{\nu(A)}{b^n} \right) \\
&= P(\mathbf{X}_1^{(m)} = \mathbf{s}, \mathbf{X}_2^{(m)} = \mathbf{s}, A \times A \times [0, 1]) - \frac{\nu(A)^2}{b^{2n}} \\
&\quad - 2 \frac{\nu(A)}{b^n} (P(\mathbf{X}_1^{(m)} = \mathbf{s}, A \times [0, 1] \times [0, 1]) - \frac{\nu(A)}{b^n})
\end{aligned}$$

ある n があって $A \in \mathcal{F}_n$ であるので上式の例えば第一項目は

$$\sum_{\mathbf{u}} \pi_{\mathbf{u}, \mathbf{s}, \mathbf{s}} P(A \times A \times [0, 1]) = \frac{1}{b^{2n}} \nu(A)^2$$

に収束し、第一項と第二項の和は 0 に収束する。第三項も同様に 0 に収束するが、とくに定理 3 のときと同様に指数関数の速度での収束であることが例えば Billingsley [2, p.201] によって与えられているので、同様の議論ができて $\mu(D_A) = 1$ なる $D_A \in \mathcal{B}([0, 1])$ が存在して

$$\nu(\mathbf{X}_1^{(m)}(\cdot, x_2, \alpha) = \mathbf{s}, A) - \frac{\nu(A)}{b^n} \rightarrow 0, \quad \alpha \in D_A$$

$D := \bigcap_{A \in \mathcal{F}_\infty} D_A$ とおけば $\mu(D) = 1$ であって、 $\alpha \in D$ について、

$$\int 1_{\{\mathbf{X}^{(m)}(x, \alpha) = \mathbf{s}\}} h_i(x) \nu(dx) - \frac{\int h_i d\nu}{b^n} \rightarrow 0$$

任意の $\varepsilon > 0$ に対し、ある N_ε が存在して $i > N_\varepsilon$ ならば $\int |h_i - h| d\nu < \varepsilon$

$$\begin{aligned}
& \left| \int 1_{\{\mathbf{X}^{(m)}(x, \alpha) = \mathbf{s}\}} h(x) \nu(dx) - \frac{1}{b^n} \right| \\
&= \left| \int 1_{\{\mathbf{X}^{(m)}(x, \alpha) = \mathbf{s}\}} h_i(x) \nu(dx) - \frac{\int h_i d\nu}{b^n} \right| \\
&\quad + \left| \int 1_{\{\mathbf{X}^{(m)}(x, \alpha) = \mathbf{s}\}} (h_i(x) - h(x)) \nu(dx) \right| + \frac{1}{b^n} \left| 1 - \int h_i d\nu \right| \\
&\leq \left| \int 1_{\{\mathbf{X}^{(m)}(x, \alpha) = \mathbf{s}\}} h_i(x) \nu(dx) - \frac{\int h_i d\nu}{b^n} \right| + 2\varepsilon
\end{aligned}$$

参考文献

- [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)