数理解析研究所講究録 1351 巻 2004 年 25-32

Weyl変換に関する従属性消滅定理とマルコフ連鎖

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

記号

$d^{(m)}(x)$ を $x \geq 0$ の 2 進小数展開の第 m 桁目とする. $\omega, \alpha \in [0,1)$ に対して $\{0,1\}$-値関数 $X_l^{(m)}$ を

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

と置く.

例: $\alpha = 0.10011101000\cdots$, $\omega = 0.11110110010\cdots$ の時の $X_3^{(5)}$.
$\omega+3\alpha = 10.11001101\cdots$ なので $X_3^{(5)}(\omega,\alpha) = 1+1+0+0+1 = 1 \pmod 2$

fact: m と無理数 α を fix する. l についての数列 $\{X_l^{(m)}(\,\cdot\,,\alpha)\}_{l=0}^{\infty}$ は $X_0^{(m)}(\,\cdot\,,\alpha)$ の Weyl 変換 (α-回転) によって生成される;

$$X_l^{(m)}(\omega,\alpha) = \sum_{k=1}^{m} d^{(k)}(\omega + l\alpha) = X_0^{(m)}(\omega + l\alpha, \alpha).$$

Sugita [1] はこの過程 $\{X_l^{(m)}(\cdot,\alpha)\}_{l=0}^{\infty}$ について次の定理と予想を示した:

Theorem 1 (Sugita [1]). 任意の正規数 $\alpha \in [0,1)$ について, $X_l^{(m)} := X_l^{(m)}(\,\cdot\,,\alpha)$ を *Lebesgue* 空間 $(\Omega,\mathcal{F},P) := ([0,1),\mathcal{B}([0,1)),\mu)$ 上の確率過程の列と見なせば, 任意の $n \in \mathbb{N}$ 及び $\epsilon_0,\ldots,\epsilon_{n-1} \in \{0,1\}$ について

$$P\left(\left\{\omega \in [0,1) \,\middle|\, (X_0^{(m)}(\omega),\ldots,X_{n-1}^{(m)}(\omega)) = (\epsilon_0,\ldots,\epsilon_{n-1})\right\}\right) \xrightarrow{m\to\infty} \frac{1}{2^n}.$$

即ち $\{X_l^{(m)}\}_{l=0}^{\infty}$ の従属性が消滅する.

Conjecture (Sugita [1]). 任意の無理数 $\alpha \in [0,1)$ について, $\{X_l^{(m)}\}_{l=0}^{\infty}$ の従属性が消滅する.

2 Theorems

この話題に関するいくつかの結果を示す.

Sugita [1] の証明は難解であった為, より単純な証明が探され, Sugita [2] は skew product を用いて Theorem 1 より弱い次をエルゴード論的に示した:

Theorem 2 (Sugita [2]). $X_l^{(m)} := X_l^{(m)}(\,\cdot\,,\cdot\,)$ を 2 次元 *Lebesgue* 空間 $(\Omega,\mathcal{F},P) := ([0,1)^2,\mathcal{B}([0,1)^2),\mu^2)$ 上の確率過程の列と見なせば $m \to \infty$ のとき $\{X_l^{(m)}\}_{l=0}^{\infty}$ の従属性が消滅する.

Sugita [2] の証明は skew product による保測変換が Markov 変換であることが鍵となっている. そこで skew product を介さずに直接 Markov Chain を構成する方法で次が示せる:

Proposition 1 (Y. [4]). $X_l^{(m)} := X_l^{(m)}(\,\cdot\,,\cdot\,)$ を確率空間 $(\Omega,\mathcal{F},P) := ([0,1)^2,\mathcal{B}([0,1)^2),\mu\times\nu)$ 上の確率過程の列と見なせば $m \to \infty$ のとき $\{X_l^{(m)}\}_{l=0}^{\infty}$ の従属性が消滅する. しかもその収束は指数オーダーである.

更に, α を固定する毎に独立な, 2 つの Chain を同時に走らせることにより, その収束のオーダーから次が示せる:

Theorem 3 (Y. [4]). μ,ν を任意の *Bernoulli* 測度とする. ν-*a.e.*$\alpha \in [0,1)$ について, $X_l^{(m)} := X_l^{(m)}(\cdot,\alpha)$ を確率空間 $(\Omega,\mathcal{F},P) := ([0,1),\mathcal{B}([0,1)),\mu)$ 上の確率過程の列と見なせば $m \to \infty$ のとき $\{X_l^{(m)}\}_{l=0}^{\infty}$ の従属性が消滅する.

上の議論は α をランダム化して扱っていたが, 実は α を fix しても Markov Chain に近いことがわかる:

Theorem 4 (Y. [5]). 任意の正規数 $\alpha \in [0,1)$ について, $X_l^{(m)} := X_l^{(m)}(\cdot,\alpha)$ を確率空間 $(\Omega,\mathcal{F},P) := ([0,1),\mathcal{B}([0,1)),\mu)$ 上の確率過程の列と見なせば $m \to \infty$ のとき $\{X_l^{(m)}\}_{l=0}^{\infty}$ の従属性が消滅する.

時間非一様な Markov Chain を用いれば Conjecture も示せる:

Theorem 5 (Y. [6]). 任意の無理数 $\alpha \in [0,1)$ について, $X_l^{(m)} := X_l^{(m)}(\cdot, \alpha)$ を確率空間 $(\Omega, \mathcal{F}, P) := ([0,1), \mathcal{B}([0,1)), \mu)$ 上の確率過程の列と見なせば $m \to \infty$ のとき $\{X_l^{(m)}\}_{l=0}^{\infty}$ の従属性が消滅する.

3 Markov Chain

3.1 アイデアと困難

Markov Chain を用いるアイデアは次の事実から直観的に連想される:
fact: $\{d^{(m)}(\cdot + l\alpha)\}_m$ は独立過程で $X_l^{(m)} = \sum_{k=1}^{m} d^{(k)}(\cdot + l\alpha)$ はその和であるから $\{X_l^{(m)}\}_m$ は混合的な Markov Chain.

これにより混合的な Markov Chain の極限分布の収束から 1 次元分布について

$$X_l^{(m)}\text{の分布} \xrightarrow{\text{分布収束}} \{0,1\}\text{上の均等分布}$$

が得られる.

しかしながら, 任意の有限次元分布を見るために, ベクトル値 $\mathbf{X}^{(m)} := (X_0^{(m)}, \ldots, X_{n-1}^{(m)})$ の過程 $\{\mathbf{X}^{(m)}\}_m$ を考えると, スカラーの時と同じ論法で Markov Chain であるとは言えない. 何故ならば,

$$\mathbf{d}^{(m)}(\omega, \alpha) := (d^{(m)}(\omega), \ldots, d^{(m)}(\omega + (n-1)\alpha))$$

とすれば $\mathbf{X}^{(m)} = \sum_{k=1}^{m} \mathbf{d}^{(k)}$ であるが $\{\mathbf{d}^{(m)}\}_m$ は独立過程ではない.

例えば

$$\begin{aligned} & d^{(m)}(\omega + \alpha) \\ &= \begin{cases} \omega_m + \alpha_m + 1 & \text{if } 0.\omega_{m+1}\omega_{m+2}\cdots + 0.\alpha_{m+1}\alpha_{m+2}\cdots \geq 1 \\ \omega_m + \alpha_m & \text{if } 0.\omega_{m+1}\omega_{m+2}\cdots + 0.\alpha_{m+1}\alpha_{m+2}\cdots < 1 \end{cases} \\ &= d^{(m)}(\omega) + d^{(m)}(\alpha) \\ &\quad + \text{繰り上がり } (d^{(m+1)}(\alpha), d^{(m+2)}(\alpha), \ldots, d^{(m+1)}(\omega), d^{(m+2)}(\omega), \ldots) \end{aligned}$$

であり, $d^{(m)}(\cdot + \alpha)$ と $d^{(m)}(\cdot)$ は独立ではない.

Theorem 3(Proposition 1), Theorem 4, および Theorem 5 はこの困難に各々異なる解決を与えたものと言える.

3.2 解決策I (Proposition 1, α:ランダマイズ)

$\{\mathbf{d}^{(m)}\}_m$ の従属性は「繰り上がり」によって伝えられるのでその情報を含む過程を用いれば良い.

$$\begin{aligned} Z_l^{(m)}(\omega,\alpha) &:= \lfloor 2(S^{m-1}\omega + lS^{m-1}\alpha)\rfloor, \\ \mathbf{Z}^{(m)}(\omega,\alpha) &:= (d^{(m)}(\alpha), Z_0^{(m)}(\omega,\alpha),\ldots,Z_{n-1}^{(m)}(\omega,\alpha)) \end{aligned}$$

と置けば(ただし S はシフトを表す,i.e., $S0.x_1x_2x_3\cdots = 0.x_2x_3x_4\cdots$),

Lemma 1. $Z_l^{(m)}(\omega,\alpha) = d^{(m)}(\omega + l\alpha) \pmod 2$.

Proof. $\rho_m^l := d^{(m)}(\omega + l\alpha)$ 即ち

$$\begin{array}{rrcl} & \omega &=& 0.\omega_1\omega_2\omega_3 \cdots \omega_m\omega_{m+1}\omega_{m+2}\cdots \\ & \alpha &=& 0.\alpha_1\alpha_2\alpha_3 \cdots \alpha_m\alpha_{m+1}\alpha_{m+2}\cdots \\ & \vdots & \vdots & \vdots \\ + & \alpha &=& 0.\alpha_1\alpha_2\alpha_3 \cdots \alpha_m\alpha_{m+1}\alpha_{m+2}\cdots \\ \hline & \omega + l\alpha &=& \lfloor\omega + l\alpha\rfloor + 0.\rho_1^l\rho_2^l\rho_3^l \cdots \rho_m^l\rho_{m+1}^l\rho_{m+2}^l\cdots \end{array}$$

とすれば, $\sigma_m^l := \lfloor S^{m-1}\omega + lS^{m-1}\alpha\rfloor$ として

$$\begin{array}{rrcl} & S^{m-1}\omega &=& 0.\omega_m\omega_{m+1}\omega_{m+2}\cdots \\ & S^{m-1}\alpha &=& 0.\alpha_m\alpha_{m+1}\alpha_{m+2}\cdots \\ & \vdots & \vdots & \vdots \\ + & S^{m-1}\alpha &=& 0.\alpha_m\alpha_{m+1}\alpha_{m+2}\cdots \\ \hline & S^{m-1}\omega + lS^{m-1}\alpha &=& \sigma_m^l + 0.\rho_m^l\rho_{m+1}^l\rho_{m+2}^l\cdots \end{array}$$

よって, $2\sigma_m^l = 0 \pmod 2$ に注意すれば,

$$\begin{aligned} Z_l^{(m)}(\omega,\alpha) &= \lfloor 2(S^{m-1}\omega + lS^{m-1}\alpha)\rfloor = 2\sigma_m^l + \rho_m^l \\ &= d^{(m)}(\omega + l\alpha) \pmod 2. \end{aligned}$$

□

Lemma 2. $\{\mathbf{Z}^{(m)}\}_m$ は *Markov* 過程.

Proof. 定義より

$$Z_l^{(m)}(\omega,\alpha)-(Z_0^{(m)}(\omega,\alpha)+ld^{(m)}(\alpha))=\sigma_{m+1}^l.$$

直感的に言って, これは $\mathbf{Z}^{(m)}$ が $m+1$ 桁目から m 桁目へ繰り上がりを完全に知り, $m'<m$ なる $\mathbf{Z}^{(m')}$ によってそれ以上の $\mathbf{Z}^{(m+1)}$ についての情報を得ることはできないことを意味する.

実際は $(\Omega,\mathcal{F},P):=([0,1)^2,\mathcal{B}([0,1)^2),\mu\times\nu)$ 上で

$$\begin{aligned}P(\mathbf{Z}^{(m+1)}=\mathbf{z}_{m+1}\mid\mathbf{Z}^{(m)}=\mathbf{z}_m,\dots,\mathbf{Z}^{(1)}=\mathbf{z}_1)\\=P(\mathbf{Z}^{(m+1)}=\mathbf{z}_{m+1}\mid\mathbf{Z}^{(m)}=\mathbf{z}_m)\end{aligned}$$

をチェックする. □

$\mathbf{X}^{(m)}=\sum_{k=1}^m\mathbf{Z}^{(k)}$ は Markov Chain$\{\mathbf{Z}^{(m)}\}_m$ の和であるから $\{(\mathbf{Z}^{(m)},\mathbf{X}^{(m)})\}_m$ は Markov Chain となる.

fact: $\mathbf{Z}^{(m)}(\omega,\alpha)=\mathbf{Z}^{(1)}(S^{m-1}\omega,S^{m-1}\alpha)$ なることに注意すれば 2 進変換の混合性より Markov 過程 $\{\mathbf{Z}^{(m)}\}_m$ も混合的.

+少々の議論により Markov Chain$\{(\mathbf{Z}^{(m)},\mathbf{X}^{(m)})\}_m$ は混合的である事が示せ,$\{X_l^{(m)}\}_{l=0}^\infty$ の従属性が消滅する ⇒Proposition 1.

3.3 解決策 II (Theorem 4, α:正規数)

α の 2 進小数展開で長い 0 の連なりが現れる部分ではほとんど繰り上がりが起きない事に注意する.

例えば $\alpha=0.\underset{123456789}{011000001}\cdots$ の時, $\omega+\alpha$ に 4 桁目から 3 桁目への繰り上がりが在るのは ω の 4 桁目から 8 桁目までが全て 1 である時に限られる. その確率は 2^{-5} しかない. これにより

$$|P(\mathbf{X}^{(1,3)}=\mathbf{e},\mathbf{X}^{(4,m)}=\mathbf{e}')-P(\mathbf{X}^{(1,3)}=\mathbf{e})P(\mathbf{X}^{(4,m)}=\mathbf{e}')|\le 2^{-5}.$$

左辺が 0 に等しいことが独立性を表すので, $\mathbf{X}^{(1,3)}:=\sum_{j=1}^3(d^{(j)}(\cdot),d^{(j)}(\cdot+\alpha))$ と $\mathbf{X}^{(4,m)}:=\sum_{j=4}^m(d^{(j)}(\cdot),d^{(j)}(\cdot+\alpha))$ は "ほぼ" 独立であると言える.

α は正規数と仮定すれば, 無限列 $m_1 < m_2 < \cdots$ を, α の小数展開が各 m_i 桁目で0の連なりを持つ様に採れる. 上の議論により,

$$\mathbf{X}^{(m_i)} = \sum_{j=0}^{i-1} \mathbf{X}^{(m_j+1, m_{j+1})}$$

は"ほぼ"独立な過程 $\{\mathbf{X}^{(m_j+1,m_{j+1})}\}_j$ の和であるから $\{\mathbf{X}^{(m_i)}\}_i$ は"ほぼ"Markov過程である.

実際に0の連の長さを適当にとって次が示せる:

Lemma 3. 任意の $\epsilon > 0$ について無限列 $m_1 < m_2 < \cdots$ と独立過程 $\widetilde{\mathbf{X}}^{(m_i+1,m_{i+1})}$ が存在して任意の i,$\mathbf{e} \in \{0,1\}^n$ ついて

$$|P(\sum_{j=0}^{i-1} \widetilde{\mathbf{X}}^{(m_j+1,m_{j+1})} = \mathbf{e}) - P(\mathbf{X}^{(m_i)} = \mathbf{e})| < \varepsilon$$

更に m_i を適当に選ぶことにより Markov Chain $\sum_{j=0}^{i-1} \widetilde{\mathbf{X}}^{(m_j+1,m_{j+1})}$ を混合的にとることができ, $\{X_l^{(m)}\}_{l=0}^{\infty}$ の従属性消滅が示せる ⇒Theorem 4

3.4 解決策 III(I+) (Theorem 5, α:無理数)

3.2 の解決策:"「繰り上がり」の情報を含む過程を用いる" は α をランダム化しなくても時間非一様の Markov Chain を扱うことにより有効である.

$$\begin{aligned} C_l^{(m)}(\omega) &:= \lfloor S^{m-1}\omega + S^{m-1}\alpha^l \rfloor \\ \mathbf{C}^{(m)} &:= (C_1^{(m)}, \ldots, C_{n-1}^{(m)}) \end{aligned}$$

とおく (ただし $\alpha^l := l\alpha - \lfloor l\alpha \rfloor$).

Lemma 4. $\{(\mathbf{C}^{(m)}, \mathbf{X}^{(m,M)})\}_{m=M}^{1}$ は時間非一様 *Markov Chain.*

Proof. $C_l^{(m)}(\omega) = c_m^l$ とおけば,

$$\begin{array}{rrcl} & S^{m-1}\omega & = & 0.\omega_m\omega_{m+1}\omega_{m+2}\cdots \\ + & S^{m-1}\alpha^l & = & 0.\alpha_m^l\alpha_{m+1}^l\alpha_{m+2}^l\cdots \\ \hline & S^{m-1}\omega + S^{m-1}\alpha^l & = & c_m^l + 0.\rho_m^l\rho_{m+1}^l\rho_{m+2}^l\cdots \end{array}$$

であるから

$$2c_m^l + \rho_m^l = c_{m+1}^l + \omega_m + \alpha_m^l.$$

辺々2で割って $\lfloor \cdot \rfloor$ をとると $c_m^l = \lfloor 2^{-1}(c_{m+1}^l + \omega_m + \alpha_m^l) \rfloor$. また, mod 2 でみると $\rho_m^l = c_{m+1}^l + \omega_m + \alpha_m^l \pmod 2$ であるから

$$\begin{aligned} C_l^{(m)}(\omega) &= \lfloor 2^{-1}(C_l^{(m+1)}(\omega) + d^{(m)}(\omega) + \alpha_m^l) \rfloor \\ X^{(m,M)}(\omega) &= d^{(m)}(\omega + \alpha) + X^{(m+1,M)}(\omega) \\ &= \rho_m^l + X^{(m+1,M)}(\omega) \\ &= C_l^{(m+1)}(\omega) + d^{(m)}(\omega) + \alpha_m^l + X^{(m+1,M)}(\omega) \pmod 2 \end{aligned}$$

よって $G : \{0,1\} \times \Sigma \to \Sigma$($\Sigma$ は state space) を適当に定めれば,

$$(\mathbf{C}^{(m)}, \mathbf{X}^{(m,M)}) = G(d^{(m)}, (\mathbf{C}^{(m+1)}, \mathbf{X}^{(m+1,M)}))$$

とできる. 更に $d^{(1)}, \ldots, d^{(M-1)}, \mathbf{C}^{(M)}$ の独立性に注意すれば $\{(\mathbf{C}^{(m)}, \mathbf{X}^{(m,M)})\}_{m=M}^1$ は Markov Chain である.(Norris,p8,Exercises1.1.3)

□

混合性については更に詳しい議論によって $\{X_l^{(m)}\}_{l=0}^\infty$ の従属性が消滅する事を示すのに十分なだけの事実が示せる. ⇒Theorem 5

参考文献

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

[2] Sugita, Hiroshi.: Lectures at Kobe university (2000)

[3] Takanobu, Satoshi.: On the strong-mixing property of skew product of binary transformation on 2-dimensional torus by irrational rotation. Tokyo J. Math. **25** (2002), no. 1, 1–15

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

[5] Yasutomi, Kenji.: A direct proof of dependence vanishing theorem for sequences generated by Weyl transformation. J. Math. Kyoto Univ. (in press)

[6] Yasutomi, Kenji.: A dependence vanishing theorem for sequences generated by Weyl transformation. (preprint)