

エルゴード理論における

エントロピー

京大 数研 十時 東生

§ 1. 序

C. Shannonは通信理論における符号化の問題を, エントロピーという量を導入することによって定式化し, 基本的な解答を得た。その後, 彼の結果の数学的に厳密な証明や, 拡張が多く, 著者によってなされている。

一方, エルゴード理論における保測変換の同型問題は, 1930年代以降ほとんど進歩がみられなかったが, 50年代末の A. N. Kolmogorov - Ya. G. Sinaiの仕事と最近の D. S. Ornsteinの仕事によって大きく進歩したといえる。彼らの仕事においてもエントロピーが本質的な役割を果たしているのので, その事情を説明したい。また保測変換の同型問題は定常的な場合の符号化の問題にも関連があるので, 符号化の問題の一つの考え方という意味もこめて, 符号化と関係づけて話を進めたい。

符号化の問題は、情報源から出る文字の列を通信の符号に変え、受信側で復号して普通の文に代えるという操作が、どのようなときに、どのように可能であるかという問題である。情報源から出る文字の列は *random* に出ると考えるのが自然である。つまり一定の確率法則——それは情報源固有のもので、例えば文法などに ~~よ~~ 関係して定まっている——に従って現れると考えられる。

Ω をアルファベットとし、 $X = \Omega^{\mathbb{Z}}$ を可能な文の全体と考える。個々の文章は両側に無限な文字の列

$$x = (\dots, x_{-1}, x_0, x_1, x_2, \dots) \in X$$

で表わされる。 X 上に確率測度 μ を定め $[X, \mu]$ を情報源と呼ぶ。*randomness* を支配する μ は時間の経過に関して変わらないことを仮定する（定常な情報源と呼ばれる）；すなわち、 X に時間のずらしに相当する変換 T を

$$(1) \quad (Tx)_n = x_{n+1}, \quad n \in \mathbb{Z}, \quad x \in X,$$

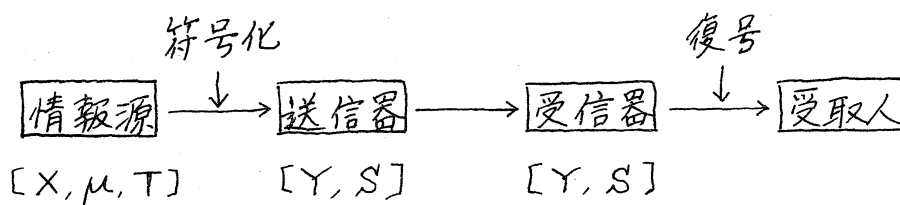
によって定めるとき、

$$(2) \quad \mu(T^{-1}B) = \mu(B), \quad B \in \mathcal{F},$$

であることを仮定する。 $\mathcal{F}$ は μ の定義域であって、それは *cylinder sets* から生成される σ -field である。これは T が保測変換であることを意味する。

送信のアルファベットを Ω とし、 X と同様に可能な送信

文の全体 $Y = \mathcal{L}^{\mathbb{Z}}$ を考える。最も簡単な場合として、送信の間に雑音が入らないとしよう。X から Y への可測写像 (Y に



も cylinder sets から生成される σ -field $\mathcal{G}$ を考えておく) を 符号 と呼ぶ。Y 上にも (1) と同様に時間のずらし S を定める。そして、符号 φ は

$$(3) \quad \varphi \circ T(x) = S \circ \varphi(x), \quad x \in X,$$

をみたすもののみを考えよう。つまり符号化のしかたが、時間の経過によって不変であるもののみを考える。このような符号は 定常的な符号 と呼ばれる。

雑音のない通信路の場合、本質的に 1 対 1 な符号 φ が求まれば問題は解けたことになる。 φ で符号化し、 φ^{-1} で復号すれば、もとの通信文が正確に受け取られるからである。この場合に

$$(4) \quad \gamma(B) = \mu(\varphi^{-1}(B)), \quad B \in \mathcal{G},$$

によって Y 上の確率測度を定めれば、 $[Y, \gamma]$ も 1 つの定常情報源と考えられる。そして、時間のずらしもこめて 2 つの情報源 $[X, \mu, T]$ と $[Y, \gamma, S]$ は、 φ によってたがいに他に移像される。これはまさに、保測変換 T と S が同型であ

ることを意味しているが、同型の厳密な定義は次節で与える。

§2. 保測変換の同型問題

一般の確率空間 $(X, \mathcal{F}, \mu)$ を考える。

定義1. X から X への可測な写像 T ($T^{-1}\mathcal{F} \subset \mathcal{F}$) が

$$(i) \mu(T^{-1}B) = \mu(B), \quad B \in \mathcal{F},$$

$$(ii) T: X \rightarrow X \text{ one to one, onto, } T^{-1}: \text{可測},$$

を満たせば、 T は 保測変換 と呼ばれる。もし T が (i) のみを満たせば、 T は 逆を持たない保測変換 と呼ばれる。

例1. $\Omega = \{a_1, \dots, a_N\}$, $X = \Omega^{\mathbb{Z}}$ とし, cylinder sets ($\{x; x_n = a_{i_n}, \dots, x_{n+m} = a_{i_{n+m}}\}$ の形の集合) から生成される σ -field を $\mathcal{F}$ とおく。 Ω 上に確率測度 μ_0 が与えられているとする。 μ_0 は値 $p_i = \mu_0(a_i)$, $1 \leq i \leq N$, の組 $(p_1, \dots, p_N)$ によって定まる。 $\mathcal{F}$ 上の確率測度 μ を μ_0 の直積として定める, すなわち μ は関係式

$$\mu(\{x; x_n = a_{i_n}, \dots, x_{n+m} = a_{i_{n+m}}\}) = p_{i_n} \cdots p_{i_{n+m}}$$

によって定まる。このとき (1) で定まる変換 T は、明らかに保測変換になる。そして確率変数列 $\{x_n\}$ が Bernoulli 列 (同分布に従う独立確率変数列) をなすことから、 T は Bernoulli 変換 $B(p_1, \dots, p_N)$ と呼ばれる。

例2. $X, \mathcal{F}, T$ は例1と同じとし、測度 μ がつぎのよ

うに定まっているとする。

$$g_{ij} \geq 0, \quad \sum_{j=1}^N g_{ij} = 1,$$

なる $\{g_{ij}; 1 \leq i, j \leq N\}$ と,

$$p_i \geq 0, \quad \sum_{i=1}^N p_i = 1, \quad \sum_{i=1}^N p_i g_{ij} = p_j,$$

をみたす $\{p_i; 1 \leq i \leq N\}$ が与えられ, μ は関係式

$$\mu(\{x; x_n = a_{i_0}, \dots, x_{n+m} = a_{i_m}\}) = p_{i_0} g_{i_0 i_1} \cdots g_{i_{m-1} i_m}$$

で定まる。このときも T が保測変換であることは明らかである。この場合は $\{x_n\}$ が Markov 連鎖をなすので, T は Markov 変換 と呼ばれる。

例 3. $X = [0, 1)$, $\mathcal{B}$ = Borel sets の全体, μ = Lebesgue 測度とし, $\alpha \in X$ を固定して変換 T を

$$Tx = x + \alpha, \quad \text{mod } 1,$$

によって定めれば, T は保測変換である。

さて一般に, 確率空間 $(X, \mathcal{B}, \mu)$ 上の保測変換 T と $(Y, \mathcal{C}, \gamma)$ 上の保測変換 S が与えられたとしよう。もし X から Y への本質的に 1 対 1 かつ onto な写像 φ で (3) と (4) をみたすものがあれば, これら 2 つの変換 T と S は測度論的に同じ構造を持つと考えられ, 同型と呼ばれる。厳密には,

定義 2. 集合 $X_0 \subset X$, $Y_0 \subset Y$ と X_0 から Y_0 への写像 φ で

$$(i) \quad TX_0 = X_0, \quad SY_0 = Y_0, \quad \mu(X_0) = \gamma(Y_0) = 1,$$

(ii) $\varphi: X_0 \rightarrow Y_0$, one to one, onto,

(iii) $A \subset X_0, A \in \mathcal{F} \Rightarrow \varphi(A) \in \mathcal{G}$,

$B \subset Y_0, B \in \mathcal{G} \Rightarrow \varphi^{-1}(B) \in \mathcal{F}, \mu(\varphi^{-1}(B)) = \nu(B),$

(iv) $x \in X_0 \Rightarrow \varphi \circ T(x) = S \circ \varphi(x),$

をみたすものがあれば, $(X, \mathcal{F}, \mu, T)$ と $(Y, \mathcal{G}, \nu, S)$ は 同型 であるといわれる。

たがいに同型である変換はどのように特徴づけられるであろうか。保測変換 $(X, \mathcal{F}, \mu, T)$ に対して, $L^2(X)$ 上のユニタリ作用素 U_T が

$$U_T f(x) = f(Tx), \quad f \in L^2(X),$$

によって定まる。 T と S が同型であれば, 明らかに U_T と U_S はユニタリ同値 ($L^2(X)$ から $L^2(Y)$ の上への等距離写像 V があって, $V \circ U_T = U_S \circ V$) である。ユニタリ作用素 U_T は変換 T の構造を相当に反映することが期待される。変換 T がエルゴード的であるというのは,

$$TA = A, A \in \mathcal{F}, \Rightarrow \mu(A)\mu(A^c) = 0$$

となることである。これは, エルゴード定理によって

$$\lim_{n \rightarrow \infty} \frac{1}{n} \sum_{i=0}^{n-1} f(T^i x) = \int_X f d\mu, \quad \text{a.e. } f \in L^1(X)$$

と同値である。ユニタリ作用素 U_T の固有関数が $L^2(X)$ を張るとき, T は純点スペクトルを持つという。

定理 1. (J. von Neumann) 2つの保測変換 T と S はともにエルゴード的であつ純点スペクトルを持つとする。もし U_T と U_S がユニタリ同値であれば, T と S は同型である。

1932年にこの定理が示されて以来, それでは純点スペクトルでない変換に対しても, U_T が T の構造を完全に決定するのかということが問題となった。特に, Bernoulli 変換に対しては, それから導かれるユニタリ作用素はすべてユニタリ同値であり, 連続スペクトルを持つことが知られていたもので, それらが同型であるかどうかに興味ある問題として残されていた。H. Amzai は 1951年に, ユニタリ同値ではあるが同型ではない例を作った。そして 1958-59年に, A.N. Kolmogorov - Ya. G. Sinai は, エントロピーを導入して, たがいに同型でない Bernoulli 変換が無限に多くあることを示した。これについて次節で述べる。

§3. エントロピー

保測変換 $(X, \mathcal{F}, \mu, T)$ のエントロピーを Ya. G. Sinai にしたがって定義する。まず $\alpha = \{A_1, \dots, A_N\}$ を X の有限分割, すなわち

$$A_i \in \mathcal{F}, A_i \cap A_j = \emptyset \ (i \neq j), \bigcup_{i=1}^N A_i = X$$

として, α のエントロピーを

$$H(\alpha) = - \sum_{i=1}^N \mu(A_i) \log \mu(A_i)$$

によって定める。 $T^{-1}\alpha = \{T^{-1}A_1, \dots, T^{-1}A_N\}$ も有限分割であり、 $A_i \cap T^{-1}A_j$ の形の集合への有限分割を $\alpha \vee T^{-1}\alpha$ で表わす。 $\alpha \vee T^{-1}\alpha \vee \dots \vee T^{-m}\alpha$ などにも同様に定められる。このとき

極限

$$h(\alpha, T) = \lim_{m \rightarrow \infty} \frac{1}{m} H(\alpha \vee T^{-1}\alpha \vee \dots \vee T^{-m+1}\alpha)$$

が存在することが知られ、これを分割 α の変換 T に関するエントロピーと呼ぶ。最後に、変換 T のエントロピー を

$$h(T) = \sup \{ h(\alpha, T); \alpha \text{ は有限分割} \}$$

によって定める。一般に $0 \leq h(T) \leq \infty$ である。

定理 2. T と S が同型であれば、 $h(T) = h(S)$ である。

変換のエントロピーを計算するのに有効な公式が下記の定理によって与えられる。

定理 3. (Ya. G. Sinai) 有限分割 α に対して、 $\bigvee_{n=0}^{\infty} T^n \alpha$ が一点一点への分割であれば、 $h(T) = h(\alpha, T)$ である。

例えば、 $X = \Omega^{\mathbb{Z}}$ と T を例 1 と同じとし、確率測度 μ は (2) をみたす任意のものとしよう。 $A_i = \{\omega; \omega_0 = a_i\}$, $1 \leq i \leq N$ とおけば、 $\alpha = \{A_1, \dots, A_N\}$ は有限分割であって定理 3 の条件をみたすことが容易にわかる。したがって $h(T) = h(\alpha, T)$ である。特に μ が例 1 のものであれば、有限分割の列 $\{T^{-i}\alpha\}$

は独立であって, $H(\alpha \vee T^{-1}\alpha \vee \cdots \vee T^{-n+1}\alpha) = nH(\alpha)$ が得られる。この場合, 明らかに

$$H(\alpha) = H(p_1, \dots, p_N) \equiv -\sum_{i=1}^N p_i \log p_i$$

だから, つぎのことがわかる。

系 1. T を Bernoulli 変換 $B(p_1, \dots, p_N)$ とすれば

$$h(T) = H(p_1, \dots, p_N)$$

である。

容易にわかるように, $0 < H(p_1, \dots, p_N) \leq \log N$ であって $H(p_1, \dots, p_N)$ は $\{p_i\}$ について連続だから,

系 2. 任意の $0 < h < \infty$ に対して, $h(T) = h$ なる Bernoulli 変換 T が存在する。したがって, たがいに同型でない Bernoulli 変換が無数個 (連続濃度) 存在する。

例 2 の Markov 変換に対しても $h(\alpha, T)$ が計算できて,

$$h(T) = -\sum_{i,j} p_i z_{ij} \log z_{ij}$$

であることがわかる。

つぎには, エントロピーの等しい Bernoulli 変換は同型であるか, あるいはエントロピーが等しければ同型となるような変換のクラスは何か, ということが問題となる。この問題は最近 D. S. Ornstein 達によって, ほとんど解決された。

定理 4. (D. S. Ornstein) エントロピーの等しい Bernoulli 変換は同型である。

この定理はもう少し広いクラスに拡張される。 $X = \Omega^{\mathbb{Z}}$,
 T を例 1 と同じとし, α を上に述べた α_0 によって定まる有限
 分割とする。確率測度 μ は (2) をみたし, さらに

$$\lim_{k \rightarrow \infty} \sup_{n \geq 0} \sum_{\substack{A \in \bigvee_{k=0}^{k+n} T^i \alpha, \\ B \in \bigvee_{-n}^0 T^i \alpha}} |\mu(A \cap B) - \mu(A)\mu(B)| = 0$$

をみたすと仮定する。このとき T を 弱 Bernoulli 変換 と
 呼ぶ。混合的な Markov 変換は弱 Bernoulli 変換であること
 が知られている。

定理 5. (N. A. Friedman - D. S. Ornstein) エントロピーの
 等しい弱 Bernoulli 変換は同型である。

D. S. Ornstein はさらに, エントロピーの等しいことから
 同型が導かれる変換のクラスは本質的に弱 Bernoulli に限
 ることも示している。

同型問題で未解決の問題は, Kolmogorov 変換と呼ばれる
 弱 Bernoulli よりも本当に広いクラスに対する分類と, 逆を
 持たない変換 (特に逆を持たない Bernoulli 変換や Markov
 変換 — それらは $X = \Omega^{\mathbb{N}}$ として定義される) の同型問題で
 ある。

§ 4. 符号化の問題への応用

1 節で定式化したように, 雑音のない通信路に対する逆

をもつ符号 φ は保測変換 (X, μ, T) と $(Y, \nu = \mu \circ \varphi^{-1}, S)$ の間の同型を与える写像であった。したがって、3節で述べた諸定理からつぎの結論が直ちに導かれる。

送信のアルファベット $\mathfrak{A}$ の元の個数を $\#\mathfrak{A}$ で表わそう。

3節で述べたように、 $\mathfrak{A}$ から定まる Y の有限分割を β とすれば、 $h(S) = h(\beta, S)$ である。さらに容易にわかるように、 $h(\beta, S) \leq H(\beta) \leq \log(\#\mathfrak{A})$ が成り立つ。もし ~~逆~~^逆 符号 φ があれば $h(T) = h(S)$ だから、つぎのことがわかる。

定理6. もし $h(T) > \log(\#\mathfrak{A})$ ならば、逆をもつ符号は存在しない。

さらにつぎのことが示される。

定理7. もし情報源 (X, μ, T) が弱Bernoulli変換であり、さらに $h(T) \leq \log(\#\mathfrak{A})$ であれば、逆をもつ符号が存在する。

なぜなら、 $\mathfrak{A} = \#\mathfrak{A}$ とおき、 $H(p_1, \dots, p_n) = h(T)$ をみたす確率ベクトル $\{p_1, \dots, p_n\}$ を1つとり、 S をBernoulli変換 $B(p_1, \dots, p_n)$ にする Y 上の確率測度を ν とする。そうすれば、 $h(S) = H(p_1, \dots, p_n) = h(T)$ だから定理5によって S と T は同型である。この同型を定める X から Y への写像 φ が求まる符号である。

符号の中に予測をしない符号がある。それは、各 $n \in \mathbb{Z}$

と $b \in \mathfrak{b}$ に対し, 集合 $\varphi^{-1}\{y; y_n = b\}$ が $(x_n, x_{n-1}, \dots)$ に対する条件のみで定まるような符号 φ として定義される。逆をもち予測をしない符号の存在の問題は, 逆をもたない保測変換の同型問題と深く関係している。

雑音のある通信路の場合の符号化の問題は, 雑音のない場合のように保測変換の同型問題に直接関係してはいないが, 一定のかかわりがあることが, 例えば P. Billingsley によって指てきされている。

文 献

[1] シャノン: コミュニケーションの数学的理論, 明治図書。

(長谷川淳・井上光洋訳)

[2] J. von Neumann: Zur operatoren Methode in der klassischen Mechanik, Ann. Math. 33 (1932), 587-642.

[3] H. Amzai: Ergodic skew product transformations on the torus, Osaka Math. J. 3 (1951), 83-99.

[4] A.N. Kolmogorov: A new metrical invariant for transitive dynamical systems and automorphisms in Lebesgue spaces, Доклады Акад. Наук 119 (1958), 861-864; Entropy per unit time as a metrical invariant of automorphisms, ibid. 124 (1959), 754-755.

- [5] Ya. G. Sinai : On the concept of entropy a dynamical system, Доклады Акад. Наук 124(1959), 768-771.
- [6] D. S. Ornstein : Bernoulli shifts with the same entropy are isomorphic, Advances in Math. 4(1970), 337-352 ; Two Bernoulli shifts with infinite entropy are isomorphic, ibid. 5(1971), 339-348.
- [7] N. A. Friedman and D. S. Ornstein : An isomorphism of weak Bernoulli transformations, Advances in Math. 5(1971), 365-394.
- [8] D. S. Ornstein : A simpler example of a Kolmogorov automorphism that is not a Bernoulli shift, preprint.
- [9] ビリングスレイ : 確率論とエントロピー, 吉岡書店.
(渡辺毅・+時東生訳)