数理解析研究所講究録 1396 巻 2004 年 60-66

情報源符号化定理の量子系への拡張について

東京理科大学 理工学研究科 情報科学専攻 宮下 真行(Masayuki Miyashita)
東京理科大学 理工学部 情報科学科 渡邉 昇(Noboru Watanabe)
Department of Information Sciences Faculty of Science and Technology
Tokyo University of Science

1 はじめに

古典系の情報源符号化定理は,測度論的確率論を基にした McMillan の定理を用いて定式化されており,効率の良い符号を作り上げる上で重要な役割を果たしている.これに対して,量子系の情報源符号化定理は,非常に古典系に近い場合の研究として文献[8]が知られている.

本論文では,文献[6],[7]による量子系の McMillan の定理を基にして量子系の情報源符号化定理を定式化することを目的とする.

2 メッセージ空間と情報源

通信で使用するアルファベットを $A=\{x^{(1)},x^{(2)},\cdots,x^{(n)}\}$ とする.可測空間 $(A,2^A)$ 上の確率測度全体を $P(A)$ とする.ここで,$A,2^A,P$ の組 $(A,2^A,P)$ は,確率空間となる.通常,入力源から通信路に送られる記号列の長さは一定ではないと考えられるので,どのような長さも取り扱うことができるように,通信系を定式化する.

始点が i で,終点が $i+k-1$ (ただし, $i\leq i+k-1, \therefore k\geq 1$) である文字の鎖を記号

$$[x_i^0\cdots x_{i+k-1}^0]\equiv\prod_{j=-\infty}^{i-1}A\times\prod_{j=i}^{i+k-1}\{x_j^0\}\times\prod_{j=i+k}^{+\infty}A\subset A^Z$$

$$(\forall x_j^0\in A, j=i,\cdots,i+k-1)$$

で定められる文字の鎖をメッセージと名付ける.また,A^Z の部分集合 $[x_i^0\cdots x_{i+k-1}^0]$ を筒集合(*cylinder set*)と呼ぶこともある.すなわち,$[x_i^0\cdots x_{i+k-1}^0]$ の $x=\prod_{j=i}^{i+k-1}\{x_j^0\}$ 以外の部分は,どんな記号が送られてもかまわないので,全集合 A の直積で与えられる.この筒集合 $[x_i^0\cdots x_{i+k-1}^0]$ は,入力源からチャネルに送られる長さ k のメッセージを表している.メッセージの全体を M で表わすと,M は,集合体をなす.

$$E,F\in M\Rightarrow E\cup F, E\cap F, E^c\in M$$

この M によって生成される σ-集合体を $\mathfrak{F}_A$ で表わすと,$A^Z,\mathfrak{F}_A$ の組 $(A^Z,\mathfrak{F}_A)$ は,可測空間となる.この可測空間 $(A^Z,\mathfrak{F}_A)$ をメッセージ空間と名付ける,可測空間 $(A^Z,\mathfrak{F}_A)$ 上の確率測度全体を $\mu(A^Z)$ とする.$A^Z,\mathfrak{F}_A,\mu$ の組 $(A^Z,\mathfrak{F}_A,\mu)$ は,確率空間となる.

以上ここまで述べてきた場合は,メッセージの出現確率がアルファベット集合

Aに付随した確率分布に従う場合ではあったが,この場合は,特別な場合であって,一般には各メッセージそのものに出現確率が対応している場合を考える必要がある.つまり,各$E\in\mathfrak{F}_A$に確率$0\le\mu(E)\le1$が対応する場合である.このときの確率空間$\left(A^Z,\mathfrak{F}_A,\mu\right)$を情報源と名付ける.ここより以下では,$[A^Z,\mu]$と省略する.

3 古典系におけるMcMillanの定理

ここで,M_kを長さkのメッセージの集合とする.

古典系におけるMcMillanの定理

定常情報源$[A^Z,\mu]$において,シフト変換Tに関して不変な函数$h\in L^1(A^Z)$が存在して,

$$-\frac{1}{k}\sum_{[x_0\cdots x_{k-1}]\in M_k}1_{[x_0\cdots x_{k-1}]}\log\mu([x_0\cdots x_{k-1}])\to h$$

$$(a.e.\ \text{かつ}\ L^1\text{-収束})$$

が成り立つ.さらに,$[A^Z,\mu]$がエルゴード情報源ならば,

$$h=S(\mu)$$

$$(=\text{情報源のエントロピー})\quad a.e.$$

である.このMcMillanの定理は,次のことを意味している.

エルゴード情報源$[A^Z,\mu]$においては,$\varepsilon>0,\delta>0$がどんなに小さくても,十分に大きなkをとれば,

$$\mu\left(\left\{x\in A^Z;\left|\frac{1}{k}f_k(x)-S(\mu)\right|>\varepsilon\right\}\right)<\delta$$

となる.

定義　古典系における典型系列

任意のメッセージ空間A^Z上の分布μ,長さがk（ただし,$k\in N$）のメッセージ,任意のj（ただし,$k\in N,n\in N,1\le j\le n^k$）,任意の$0<\varepsilon<1$に対して,次の条件,

$$\exp\left\{-k\left(S(\mu)+\varepsilon\right)\right\}\le\mu([x_0^j\cdots x_{k-1}^j])\le\exp\left\{-k\left(S(\mu)-\varepsilon\right)\right\}$$

を満たすメッセージ$[x_0^j\cdots x_{k-1}^j]\in M_k$を典型系列(*typical sequence*)と呼ぶ.また,M_kの典型系列全体の集合を$B(k,\varepsilon)$と表わすことにする.

4 古典系における情報源の可変長符号化

メッセージを0と1のビット列で表現することを情報源符号化という.典型系列を利用すれば,A^Z上の分布μを有するメッセージから出力される長さkのメッセージ1文字当たりを平均$S(\mu)$ビット程度の2値系列（ビット列）に符号化できることを示す定理が存在する.ここで,長さkのメッセージ$[x_0^j\cdots x_{k-1}^j]\in M_k$に対応する符号語の長さを$l([x_0^j\cdots x_{k-1}^j])$とし,符号語の平均長を$E\left[l([x_0^j\cdots x_{k-1}^j])\right]$とする.

古典系における情報源の可変長符号化定理

A^Z上の分布μを有するメッセージ全体の集合Mに含まれる出力系列$[x_0^j\cdots x_{k-1}^j]\in M_k$を可変長2値系列に符号化することを考える.このとき,任意の

$0<\varepsilon<1$に対して,符号化が1対1写像（可逆）であり,かつkを十分に大きく選ぶことで平均符号長$E\left[l([x_0^j\cdots x_{k-1}^j])\right]$が,

$$\frac{E\left[l([x_0^j\cdots x_{k-1}^j])\right]}{k}<S(\mu)+\varepsilon$$

を満たすものが存在する.

5 古典系における情報源の固定長符号化

ここでは,すべての系列が完全に復元できるという条件を緩め,復元に失敗する確率がλ以下であるとしたときに,情報源符号化の符号長の限界について考えてみる.

いま,長さkのメッセージの系列を長さmの2値系列に対応させる固定長符号を以下の2つの写像によって定める.

$$\begin{cases} f: M_k \to \{0,1\}^m \\ \varphi: \{0,1\}^m \to M_k \end{cases}$$

このとき,fを符号化写像,φを複号化写像,mを符号長という.A^Z上の確率測度μを有する長さkのメッセージの集合M_kに対して,符号(f,φ)の誤り確率を,

$$e(f,\varphi)\equiv \sum_{\substack{[x_0^j\cdots x_{k-1}^j]\in M_k \\ \varphi(f([x_0^j\cdots x_{k-1}^j]))\neq[x_0^j\cdots x_{k-1}^j]}} \mu([x_0^j\cdots x_{k-1}^j])$$

と定める.ここで,誤り確率$e(f,\varphi)$が十分小さく,さらに,長さkのメッセージ1文字当たりの符号長$R\equiv m/k$が十分小さければ,符号(f,φ)は,M_kの系列の効率的な圧縮法を与えると考えることができる.そこで,長さkのメッセージにおいて,kを大きくしたとき,誤り確率が,$0<\lambda<1$を満たすためには,長さkのメッセージ1文字当たりの符号長R（以下Rを符号化率,または,符号レート（rate）と呼ぶ）をどの程度大きくすれば良いのか考えてみと次の定理を得ることとなる.

古典系における情報源の固定長符号化定理

任意の$0<\lambda<1$が与えられたとき,仮に符号化率Rが,

$$R>S(\mu)$$

を満たすならば,十分に大きな長さkのメッセージにおける固定長符号(f,φ)が存在して,$e(f,\varphi)<\lambda$を満たす.

6 量子系における McMillan の定理

数体K（実数体Rまたは,複素数体C; これらをスカラー体ともいう）上の線形空間の任意の元$x,y,z\in X$と任意の$\lambda\in K$に対して,

(1) $\langle x,x\rangle\geq 0,=0\Leftrightarrow x=0$

(2) $\langle x,y\rangle=\overline{\langle y,x\rangle}$

(3) $\langle x,\lambda y+z\rangle=\lambda\langle x,y\rangle+\langle x,z\rangle$

の条件を満たす数$\langle x,y\rangle\in K$（スカラー値）が定まるとき,$\langle x,y\rangle$をxとyの内積といい,内積をもつ線形空間を内積空間という.

内積空間 X がノルム $\|x\|=\langle x,x\rangle^{1/2}$ に関して完備であるとき，X を（$K=R$ のとき実，$K=C$ のとき複素）ヒルベルト（Hilbert）空間という．以下，ヒルベルト空間を $\mathcal{H}$ で表わす．また，$\mathcal{H}$ 上の有界作用素の全体を $B(\mathcal{H})$ で表わす．

$\mathcal{N},\mathcal{M}$ をそれぞれ $v.N.$ 代数と $v.N.$ 部分代数とする．ここで，$v.N.$ 代数とは，$B(\mathcal{H})$ の*部分代数 $\mathcal{A}$ が $\mathcal{A}''=\mathcal{A}$ を満たす $\mathcal{A}$ のことをいう．$\mathcal{A}'$

$$\mathcal{A}'\equiv\left\{\begin{array}{l}A\in B(\mathcal{H})\\ [A,B]\equiv AB-BA=0,\forall B\in\mathcal{A}\end{array}\right\}$$

と定義して，$\mathcal{A}''$ についても $\mathcal{A}''\equiv(\mathcal{A}')'$ と定義する．また，$\tilde{P}=\{P_j\}$ が最小有限分割とは，$P_j\in\mathcal{M}(\forall j)$ に対して，$P_i\perp P_j(i\neq j)$ かつ $\sum_j P_j=I$ のときには，$0<E<P_j$ を満たす射影作用素 E が存在しないことである．ただし，射影作用素 E とは，$E=E^*=E^2$ を満たす作用素 $E\in B(\mathcal{H})$ のことである．

まず，τ を忠実で正規なものとして，$x\in\mathcal{H}$ に対して，$\tau(\cdot)=\langle x,\cdot x\rangle$ と定める．ただし，$\tau(A^*A)=0$ ならば $A=0$ となるとき τ は，忠実であると定義して，任意の有界な増大ネット $\{A_\alpha\}\subset\mathcal{N}_+$ に対して，

$$\tau\left(\sup_\alpha A_\alpha\right)=\sup_\alpha\tau(A_\alpha)$$

となるとき τ は，正規であると定義する．また，$\langle\cdot,\cdot\rangle$ は，内積である．さらに，$\mathcal{K}$ は，$x\in\mathcal{H}$ に対して，$\mathcal{K}=\overset{+\infty}{\underset{-\infty}{\otimes}}\{\mathcal{H},x\}$ で定められている．ここで，非可換なメッセージ空間 $\mathcal{A}$ とは，$\mathcal{A}=\overset{+\infty}{\underset{-\infty}{\otimes}}\{\mathcal{N},\tau\}$ であり，これは，$v.N.$ 代数 $\mathcal{N}$ の無限テンソル積である．シフト演算子 α は，$\alpha(\otimes A_k)\equiv\otimes A_{k+1}$ と定義され，$\mathcal{B}_n$ は，$\mathcal{B}_n=\bigvee_{k=0}^{n-1}\alpha^{-k}\mathcal{B}_1$ で与えられている．

情報源とは，$(\mathcal{K},\mathcal{A},\alpha)$ とメッセージ空間 $\mathcal{A}$ 上の状態 φ からなる．ただし，$\|\varphi\|=1$ である $\varphi\in\mathcal{A}_+^*$ を $\mathcal{A}$ 上の状態という．また，エントロピー型作用素 $H_\tau(\mathcal{M})$

$$H_\tau(\mathcal{M})\equiv-\sum_k P_k\log\tau(P_k)$$

と定義する．ここで $\{P_k\}$ は，$\mathcal{M}$ の最小有限分割である．さらに，φ を $\mathcal{N}_n$ に制限したものを φ_n で表わすことにすると，φ_n もトレース（状態）となる．したがって，エントロピー型作用素 $H_\varphi(\mathcal{B}_n)$ を φ と $\mathcal{B}_n$ に対して，

$$H_\varphi(\mathcal{B}_n)=-\sum_k Q_k^{(n)}\log\varphi_n\left(Q_k^{(n)}\right)$$

と定義する．ここで，$\{Q_k^{(n)}\}$ は，$\mathcal{N}_n$ の最小有限分割である．さらに，$v.N.$ 代数 $\mathcal{N}$ 上のトレース φ とは，次の性質を持つ写像 $\varphi:\mathcal{N}_+\to[0,\infty]$ である．ただし，$0\times\infty=0$ と

約束する.

(1) $\varphi(A+B)=\varphi(A)\varphi(B),\forall A,B\in\mathfrak{N}_+$

(2) $\varphi(\lambda A)=\lambda\varphi(A),\forall A\in\mathfrak{N}_+,\forall\lambda\in[0,\infty)$

(3) $\varphi(A^*A)=\varphi(AA^*),\forall A\in\mathfrak{N}$

また,$\mathfrak{M}_n$ が有限次元な $v.N.$ 代数であれば,

$$H_\varphi(\mathcal{B}_n)=-\sum_{i_1,\cdots,i_n=1}^{N}P_{i_1}\otimes\cdots\otimes P_{i_n}\log\varphi_n\left(P_{i_1}\otimes\cdots\otimes P_{i_n}\right)$$

となる.

量子系における McMillan の定理

可換な $v.N.$ 部分代数 $\mathfrak{M}_n$ 上では,$\varphi-a.u.=\tilde{\mu}-a.e.$ なので,$L^1(\tilde{\Omega},\tilde{\mu}),\varphi-a.u.$ である.したがって,

$$\frac{H_\varphi(\mathcal{B}_n)}{n}\to h\quad a.e.$$

に $\alpha-$一様収束する.また,α がエルゴード的 $\left(i.e.\{A\in\mathcal{A};\alpha(A)=A\}=CI\right)$ なら,$h=\varphi(h)I$ である.

この可換な $v.N.$ 部分代数 $\mathfrak{M}_n$ 上の McMillan の定理は,次の,

$$\varphi\left(\sum_{i_1,\cdots,i_n=1}^{N}P_{i_1}\otimes\cdots\otimes P_{i_n}\left|\left\|\frac{H_\varphi(\mathcal{B}_n)}{n}-h\right\|>\varepsilon\right.\right)<\delta$$

を意味している.また,φ が可換独立であれば,$h=S(\rho)\cdot I$ になる.ここで,代数的確率空間 $(\mathcal{A},\varphi)$ の $*-$部分代数の族 $\{\mathcal{A}_\lambda\}$ が,可換独立であるとは,任意の相異なる λ,μ に対して,$[\mathcal{A}_\lambda,\mathcal{A}_\mu]=0$ が成り立ち,さらに相異なる有限個の $\lambda_1,\cdots,\lambda_n$ に対して,

$$\varphi(A_{\lambda_1}\otimes A_{\lambda_2}\otimes\cdots\otimes A_{\lambda_n})=\varphi(A_{\lambda_1})\varphi(A_{\lambda_2})\cdots\varphi(A_{\lambda_n})\quad(A_{\lambda_i}\in\mathcal{A}_{\lambda_i})$$

が成り立つことをいう.

定義　量子系における典型系列

$$\frac{H_\varphi(\mathcal{B}_n)}{n}=-\frac{1}{n}\sum_{i_1,\cdots,i_n=1}^{N}P_{i_1}\otimes\cdots\otimes P_{i_n}\log\varphi\left(P_{i_1}\otimes\cdots\otimes P_{i_n}\right)$$

が成り立ち,φ が可換独立であるとき,

$$\left\|\frac{H_\varphi(\mathcal{B}_n)}{n}-S(\rho)\cdot I\right\|<\varepsilon$$

を満たす $P_{i_1}\otimes\cdots\otimes P_{i_n}\in\mathfrak{M}_n$ を量子系における典型系列 (*typical sequence*) と呼ぶ.また,$\mathfrak{M}_n$ の典型系列全体の集合を $\mathcal{B}(n,\varepsilon)$ と表わすことにする.

ここで,M_n を長さ n のメッセージの集合を,

$$M_n=\left\{P_{i_1}\otimes\cdots\otimes P_{i_n}\in\mathfrak{M}_n\middle|\,i_1,\cdots,i_n=1,\cdots,N\right\}$$

と定める.

7 量子系における情報源の可変長符号化

古典系では,メッセージを0と1のビット列で表現することを情報源符号化といったが,量子系では 2 状態$|x_0\rangle\langle x_0|,|x_1\rangle\langle x_1|(x_0,x_1\in\mathcal{H})$の列で表現することを情報源符号化という.量子系における典型系列を利用すれば,$\mathcal{A}$上の状態φを有する長さnのメッセージ1文字当たりを平均$S(\rho)$程度の2状態系列に符号化できることを示す定理が存在する.ここで,$P_{i_1}\otimes\cdots\otimes P_{i_n}$に対応する符号語の長さを$l(P_{i_1}\otimes\cdots\otimes P_{i_n})$とし,符号語の平均長を$E\left[l(P_{i_1}\otimes\cdots\otimes P_{i_n})\right]$とする.

量子系における情報源の可変長符号化定理

$(\mathcal{A},\varphi)$を代数的確率空間とし,$*-$部分代数の族$\{\mathcal{A}_\lambda\}$が可換独立とすると,$P_{i_j}\in\mathcal{A}_\lambda(1\le j\le n)$において,$\mathcal{A}$上の状態$\varphi$を有する長さ$n$のメッセージに含まれる任意の量子系の出力系列$P_{i_1}\otimes\cdots\otimes P_{i_n}$を可変長2状態系列に符号化することを考える.このとき,任意の$0<\varepsilon<1$に対して,符号化が1対1写像(可逆)であり,かつnを十分大きく選ぶことで,平均符号長$E\left[l(P_{i_1}\otimes\cdots\otimes P_{i_n})\right]$が,

$$\frac{E\left[l(P_{i_1}\otimes\cdots\otimes P_{i_n})\right]}{n}<S(\rho)+\varepsilon$$

を満たすものが存在する.

8 量子系における情報源の固定長符号化

ここでは,すべての系列が完全に復元できるという条件を緩め,復元に失敗する確率がλ以下であるとしたときに,情報源符号化の符号長の限界について考えてみる.

いま,長さnのメッセージの系列を長さmの2状態系列に対応させる固定長符号を以下の2つの写像によって定める.

$$\begin{cases} f: M_n\to\{|x_0\rangle\langle x_0|,|x_1\rangle\langle x_1|\}^m \\ \phi: \{|x_0\rangle\langle x_0|,|x_1\rangle\langle x_1|\}^m\to M_n \end{cases}$$

このとき,fを符号化写像,ϕを複号化写像,mを符号長という.$\mathcal{A}$上の状態φを有する長さnのメッセージの集合M_nに対して,符号(f,ϕ)の誤り確率を,

$$e(f,\phi)\equiv\sum_{\substack{P_{i_1}\otimes\cdots\otimes P_{i_n}\in M_n\\ \phi(f(P_{i_1}\otimes\cdots\otimes P_{i_n}))\neq P_{i_1}\otimes\cdots\otimes P_{i_n}}}\varphi(P_{i_1}\otimes\cdots\otimes P_{i_n})$$

と定める.ここで,誤り確率$e(f,\phi)$が十分小さく,さらに,長さnのメッセージ1文字当たりの符号長$R\equiv m/n$が十分小さければ,符号(f,ϕ)は,M_nの系列の効率的な圧縮法を与えると考えることができる.そこで,長さnのメッセージにおいて,nを大きくしたとき,誤り確率が,$0<\lambda<1$を満たすためには,長さnのメッセージ1文字当たりの符号長R(以下Rを符号化率,または,符号レート(rate)と呼ぶ)をどの程度大きくすれば良いのか考えてみと次の定理を得ることとなる.

量子系における情報源の固定長符号化定理

任意の$0<\lambda<1$が与えられたとき,仮に符号化率Rが,

$$R>S(\rho)$$

を満たすならば,十分に大きな長さnのメッセージにおける固定長符号(f,ϕ)が存在して,$e(f,\phi)<\lambda$を満たす.

9 考察と今後の課題

この論文では,量子系における McMillan の定理において,φを可換独立という条件のもとでは,量子系ではあるが,古典系の形に近くなる.この理由として,量子系は,一般的に非可換である.しかしながら,この論文では,φを可換独立という条件にしたことである.その結果,量子系においては,量子系ではあるが,古典系の形に近くなる.

今後の課題としては,φに対して可換独立という厳しい条件を徐々に緩め,一般的な量子系の形に近づける.

参考文献

[1] アカルディ・ルイジ, 尾畑信明, “代数的確率論入門”.
[2] 宮沢政清, “確率と確率過程”, 近代科学社, 1993.
[3] 日合文雄, 柳研二朗, “ヒルベルト空間と線型作用素”, 牧野書店, 1995.
[4] 大矢雅則, 渡邉昇, “量子通信理論の基礎”, 牧野書店, 1998.
[5] M. Ohya and D. Petz, “Quantum Entropy and its Use”, Springer-Verlag, 1993.
[6] M. Ohya, “Entropy operators and McMillan type convergence theorems in a noncommutative dynamical system”, Lecture Notes in Mathematics, 1299, Springer-Verlag, 384-390, 1986.
[7] M. Ohya, M. Tsukada and H. Umegaki, “A formulation of noncommutative McMillan theorem”, Proc. Japan Acad. Ser. A Math. Sci. 63, 50-53 (1987).
[8] B. Schumacher, Physical Review A, Vol. 51, (1995), p. 2738.
[9] 植松友彦, “現代シャノン理論”, 培風館, 1998.
[10] 梅垣壽春, 大矢雅則, “確率論的エントロピー”, 共立出版, 1983.
[11] 梅垣壽春, 大矢雅則, “量子論的エントロピー”, 共立出版, 1984.
[12] 梅垣壽春, 大矢雅則, 塚田真, “測度・積分・確率”, 共立出版, 1987.
[13] 梅垣壽春, 大矢雅則, 日合文雄, “作用素代数入門”, 共立出版, 1985.