第21回情報理論とその応用シンポジウム
The 21st Symposium on Information Theory
and Its Applications (SITA98)
Gifu, Japan, December 2-5, 1998

量子通信路容量の解析解と有本–長岡の算法に関する考察
On the analystical solution of quantum channel capacity and the Arimoto–Nagaoka method

加藤 研太郎* 大崎 正雄* 広田 修*
KENTARO KATO MASAO OSAKI OSAMU HIROTA

Abstract— In this paper, we show that the quantum channel capacity can be solved analytically when signals have a certain symmetry. We also show a concrete example applying the quantum version of Arimoto–Blahut method, called Arimoto–Nagaoka method, given by Nagaoka[14].

Keywords— Quantum channel coding theorem, Quantum channel capacity, von Neumann entropy.

1 まえがき

Shannonの情報理論が誕生してから半世紀が過ぎ，情報源符号化定理，通信路符号化定理，そして源符号化定理を基礎として現代の情報通信技術を支える様々な応用が生み出され，また今後も生み出されようとしている[1, 2]．これに対して量子情報理論は1960年代から議論されるようになり，70年代には量子通信路容量に関する議論が盛んに行われた[3, 4, 5]．当時の議論からは量子通信路の特徴である超加法性が明らかにされるなどしたが，量子通信路容量の上界が示されるに止まった[3]．その後90年代に再び議論が活発化し，1994年には量子情報源符号化定理[6, 7]が，1996年には量子通信路符号化定理[8, 9, 10]が証明された．これらにより量子情報理論から次代の情報通信技術が生み出されようとしている．

量子通信路符号化定理からは従来の情報理論のそれと同じように復号誤り確率がゼロになるような符号化が存在し得る最大の伝送速度としての量子通信路容量Cが導き出される．このCはvon Neumannエントロピーを用いて定義される或る量を，信号の先験確率分布に関して最大化をすることによって得られることが明らかになった．従来の情報理論では対称な通信路を除いては通信路容量を解析的に求めることは一般には困難である．しかしながら，有本–Blahutの数値解法アルゴリズム[11, 12]によって数値解析ではあるが効率的に解を得ることが可能である．同様に，量子情報理論でも量子通信路容量Cを解析的に求める問題は困難な問題の一つである．

* 玉川大学 学術研究所 量子通信研究部門，
RESEARCH CENTER FOR QUANTUM COMMUNICATIONS,
TAMAGAWA UNIVERSITY,
Tamagawa-gakuen 6-1-1, Machida, Tokyo 194-8610,
e-mail: kkato@lab.tamagawa.ac.jp

最近，我々は準備された信号系が或る対称性を有する場合には量子通信路容量の解析解を得られることを報告した[13]．本稿ではそれを紹介する．また，長岡によって有本–Blahutの数値解析アルゴリズムを応用した量子通信路容量を求めるための数値解法アルゴリズム（有本–長岡の算法）[14]が明らかにされたので，それの適用例も示す．

2 量子通信路容量

量子情報理論で取り扱う情報伝送モデルと量子通信路容量の定義について述べる．$\mathcal{A} = \{1, 2, \ldots, M\}$を入力アルファベットとし，各レターにはそれを信号として送り出す際に用いる物理現象の量子状態が1対1に対応するものとする．量子状態は密度作用素$\hat{\rho}_i$によって表され，それは次のような性質を持つ：

$$\hat{\rho}_i \geq 0, \quad \mathrm{Tr}\hat{\rho}_i = 1, \quad \forall i. \tag{1}$$

ここで演算記号'Tr'は作用素のトレースを表す．一般には$\mathrm{Tr}\hat{\rho}_i^2 \leq 1$であるが，等号が成立する場合を純粋状態，そうでない場合を混合状態と呼ぶ．特に純粋状態ではブラ'$\langle\cdot|$'とケット'$|\cdot\rangle$'を用いて

$$\hat{\rho}_i = |\psi_i\rangle\langle\psi_i|, \tag{2}$$

と表される．信号$\hat{\rho}_i$は先験確率$\xi_i(\xi_i \geq 0, \sum_{i=1}^{M} \xi_i = 1)$で送信されるものとする．このときの先験確率分布は$M$次元確率ベクトルによって

$$\boldsymbol{\xi} = (\xi_1, \xi_2, \cdots, \xi_M), \tag{3}$$

と表す．従来の情報理論における情報源はアルファベットと各レターの先験確率分布で規定されるが，量子情報理論ではそれらに各レターの量子状態が加わる．この量子情報理論における情報源を次のように定義される密度作用素によって表す．

$$\hat{\rho}(\boldsymbol{\xi}) = \sum_{i=1}^{M} \xi_i \hat{\rho}_i. \tag{4}$$

量子通信路符号化定理によれば，このような情報源を通信路に接続したとき，その通信路で伝送し得る最大の情

報量，すなわち量子通信路容量は次式で与えられる：

$$C = \max_{\boldsymbol{\xi}} \Delta S(\boldsymbol{\xi}). \tag{5}$$

ただし，

$$\Delta S(\boldsymbol{\xi}) \equiv S(\hat{\rho}(\boldsymbol{\xi})) - \sum_{i=1}^{M} \xi_i S(\hat{\rho}_i), \tag{6}$$

である．このとき $S(\hat{\rho})$ は作用素 $\hat{\rho}$ の von Neumann エントロピーであり，

$$S(\hat{\rho}) \equiv -\mathrm{Tr}\hat{\rho}\log\hat{\rho} = -\sum_i \lambda_i \log \lambda_i, \tag{7}$$

と定義される．λ_i は作用素 $\hat{\rho}$ の固有値である．

式 (5) から，量子通信路容量を求める問題は量 $\Delta S(\boldsymbol{\xi})$ の先験確率分布 $\boldsymbol{\xi}$ に関する最大化問題であることが解る．これを解析的に解くためには $\hat{\rho}(\boldsymbol{\xi})$ ならびに $\hat{\rho}_1, \ldots, \hat{\rho}_M$ の固有値を求め，適当な最適化の手法を用いて最大化を試みるのが正攻法である．しかし，この手順で解を得ることを試みれば次の困難に直面する．ひとつは固有値を得ることの困難さ，もうひとつは式 (7) の中に現れる '$-p\log p$' に起因する非線型性による最適化の困難さである．現在のところ，この手順にしたがって解くことができるのは純粋状態からなる 2 元の場合といくつかの特殊な場合だけである．

これに対して，最近我々は信号が対称である場合には量子通信路容量を与える先験確率分布が一様分布となることを証明した [13]．また，長岡によって数値解析のためのアルゴリズムが明らかにされた [14]．以下でそれらについて述べる．

3 量子通信路容量の解析解

ここでは対称な信号に対する量子通信路容量に関する定理を紹介し，その具体例を示す．対称な信号とは次のように定義される信号である．

定義：M 元信号 $\{\hat{\rho}_i\}$ が次の関係を満足するとき，その信号は対称であるという．

$$\hat{\rho}_i = \hat{V}^{i-1}\hat{\rho}_1\hat{V}^{\dagger\, i-1}, \quad \forall i. \tag{8}$$

ただし，$\hat{V}$ は $\hat{V}^M = \pm\hat{I}, \hat{V}^{-1} = \hat{V}^\dagger$ を満足する作用素であり，$\hat{I}$ は恒等作用素である．

このように定義される M 元対称信号に対しては次の定理が成立する．

定理 [13]：M 元対称信号に対する量子通信路容量は，先験確率分布が一様分布のときに達成される．

証明

まず始めに，M 元対称信号に対する量子通信路容量を見いだす問題は情報源の von Neumann エントロピー $S(\hat{\rho}(\boldsymbol{\xi}))$ の最大化問題に帰着することを示す．M 元対称信号の各信号は作用素 $\hat{V}$ で関係し合っているが，そのような変換の下では von Neumann エントロピーの値は変化しない．つまり，

$$S(\hat{\rho}_i) = S(\hat{\rho}_1), \quad \forall i, \tag{9}$$

である．したがって最大化すべき量 $\Delta S(\boldsymbol{\xi})$ は

$$\Delta S(\boldsymbol{\xi}) = S(\hat{\rho}(\boldsymbol{\xi})) - S(\hat{\rho}_1),$$

となる．このことから量子通信路容量を求める問題は密度作用素 $\hat{\rho}(\boldsymbol{\xi})$ の von Neumann エントロピー $S(\hat{\rho}(\boldsymbol{\xi}))$ の最大化問題に帰着することが解る．

続いて，von Neumann エントロピー $S(\hat{\rho}(\boldsymbol{\xi}))$ を最大にするような先験確率分布は一様分布であることを示す．まず，任意の先験確率分布 $\boldsymbol{\xi}$ を考える．

$$\boldsymbol{\xi} = (\xi_1, \xi_2, \cdots, \xi_M) \equiv \boldsymbol{\xi}^{(1)}. \tag{10}$$

同時に，この各確率を次のように置換した分布を考える．

$$\begin{aligned}
\boldsymbol{\xi}^{(2)} &= (\xi_2, \xi_3, \cdots, \xi_1), \\
\boldsymbol{\xi}^{(3)} &= (\xi_3, \xi_4, \cdots, \xi_2), \\
&\vdots \\
\boldsymbol{\xi}^{(M)} &= (\xi_M, \xi_1, \cdots, \xi_{M-1}).
\end{aligned}$$

この M 個の分布に対する各密度作用素 $\hat{\rho}(\boldsymbol{\xi}^{(i)})$ の間には次の関係がある．

$$\hat{\rho}(\boldsymbol{\xi}^{(i)}) = \hat{V}^{-(i-1)}\hat{\rho}(\boldsymbol{\xi})\hat{V}^{\dagger-(i-1)}. \tag{11}$$

つまり，各密度作用素 $\hat{\rho}(\boldsymbol{\xi}^{(i)})$ は作用素 $\hat{V}$ によって $\hat{\rho}(\boldsymbol{\xi})$ と関係付けられる．von Neumann エントロピーの $\hat{V}$ による変換の下での不変性と先験確率分布に関しての凸性 [15] から，次の不等式が得られる．

$$S(\hat{\rho}(\boldsymbol{\xi})) = \frac{1}{M}\sum_{i=1}^{M} S(\hat{\rho}(\boldsymbol{\xi}^{(i)})) \le S(\hat{\rho}(\frac{1}{M}\sum_{i=1}^{M}\boldsymbol{\xi}^{(i)})). \tag{12}$$

この不等式の右辺に現れる分布は

$$\frac{1}{M}\sum_{i=1}^{M}\boldsymbol{\xi}^{(i)} = \left(\frac{1}{M}, \frac{1}{M}, \cdots, \frac{1}{M}\right) \equiv \boldsymbol{\xi}', \tag{13}$$

である．つまり式 (12) が意味することは，任意の先験確率分布 $\boldsymbol{\xi}$ に対しての von Neumann エントロピーは一様分布 $\boldsymbol{\xi}'$ の場合のそれを越えないということである．したがって式 (8) で表される信号系に対しての量子通信路容量は先験確率分布が一様分布のときに達成されることが明らかになった．

3.1 例：混合状態からなる M 元対称信号

例として熱浴中のスピン 1/2 の系を取り上げる．スピン 1/2 の粒子が磁場 $\mathbf{B}$ の中にあるものとし，

$$\mathbf{B} = (B\sin\theta, 0, B\cos\theta), \tag{14}$$

とする．θ は z 軸となす角度である．このときのハミルトニアンは

$$H = -\mu\boldsymbol{\sigma}\cdot\mathbf{B}, \tag{15}$$

である．ただし，μ は磁気モーメント，$\boldsymbol{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ であり，$\mathrm{i} = \sqrt{-1}$ として，

$$\sigma_x = \begin{bmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & 0 \end{bmatrix}, \sigma_y = \begin{bmatrix} 0 & -\frac{\mathrm{i}}{2} \\ \frac{\mathrm{i}}{2} & 0 \end{bmatrix}, \sigma_z = \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & -\frac{1}{2} \end{bmatrix},$$

である．これが内部エネルギーが或る値に定まっているという条件の下で，熱浴との相互作用の結果，熱平衡に達したときの状態は次のように表される [16].

$$\begin{aligned} \rho_{th} &= \frac{\exp[-\beta H]}{\mathrm{Tr}(\exp[-\beta H])} \\ &= \begin{bmatrix} \frac{1}{2} + (\frac{1}{2} - f)\cos\theta & (\frac{1}{2} - f)\sin\theta \\ (\frac{1}{2} - f)\sin\theta & \frac{1}{2} - (\frac{1}{2} - f)\cos\theta \end{bmatrix}. \end{aligned} \tag{16}$$

ただし，

$$f \equiv 1/(\exp[\beta\mu B)] + 1), \quad \beta \equiv 1/T, \tag{17}$$

であり，T は温度である．ここで，

$$V(\theta) \equiv \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}, \tag{18}$$

と定義すると，式 (16) は次のように表すことができる．

$$\rho_{th} = V(\theta) \begin{bmatrix} 1-f & 0 \\ 0 & f \end{bmatrix} V^\dagger(\theta). \tag{19}$$

これを用いて，次のような M 元信号 $\{\rho_i\}$ を考える．

$$\rho_i = V^{i-1}(2\pi/M) \begin{bmatrix} 1-f & 0 \\ 0 & f \end{bmatrix} V^{\dagger i-1}(2\pi/M). \tag{20}$$

このとき，

$$V^M(2\pi/M) = -\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \tag{21}$$

となるので，この信号は対称である．したがって上述の定理から最適な先験確率分布は一様分布であることが解る．そしてこのときの量子通信路容量は

$$C = 1 + (1-f)\log_2(1-f) + f\log_2 f, \tag{22}$$

となる．

一般には信号が混合状態である場合にはその次元は無限次元になる．その場合，最適な先験確率分布が一様分布であることが解っても，固有値の計算が困難なので，量子通信路容量を式で表現することも困難である．

3.2 例：純粋状態からなる M 元対称信号

信号が $\hat{\rho}_1 = |\psi\rangle\langle\psi|$ のように与えられる純粋状態の場合は量子通信路容量は次式のようになる．

$$C = -\sum_{i=1}^{M} \lambda_i^* \log \lambda_i^*. \tag{23}$$

ただし，

$$\lambda_i^* = \frac{1}{M}\sum_{k=1}^{M} \langle\psi|\hat{V}^{k-1}|\psi\rangle \exp\left[-\frac{2i(k-1)\pi\mathrm{i}}{M}\right], \tag{24}$$

である．

より具体的には，レーザー光を用いた M 元位相シフトキーイング信号がこれに相当する [17].

4 有本–長岡の算法

従来の情報理論において，数値解析的に通信路容量を求めるアルゴリズムに有本–Blahut の算法がある．これにより任意の通信路の通信路容量を計算することができる．

量子情報理論においても，最近，任意の通信路の量子通信路容量を求めるための数値解析アルゴリズムが長岡によって明らかにされた [14]．これは次のようなアルゴリズムである：

1. 初期先験確率分布 $\boldsymbol{\xi}^{(1)} = (\xi_1^{(1)}, \xi_2^{(1)}, \cdots, \xi_M^{(1)})$ を適当に選ぶ．
2. $\Delta S(\boldsymbol{\xi}^{(n)})$ の値が収束するまで次の一連の計算を $n = 1, 2, \ldots$ と繰り返す．
   - $\alpha_i^{(n)} = \mathrm{Tr}\{\hat{\rho}_i(\log\hat{\rho}_i - \log[\sum_{i=1}^{M}\xi_i^{(n)}\hat{\rho}_i])\}$
   - $\Delta S(\boldsymbol{\xi}^n) = \sum_{i=1}^{M}\xi_i^{(n)}\alpha_i^{(n)}$
   - $\xi_i^{(n+1)} = \xi_i^{(n)}\exp[\alpha_i^{(n)}]/\sum_{i=1}^{M}\xi_i^{(n)}\exp[\alpha_i^{(n)}]$

従来の情報理論おいて有本–Blahut の算法によって効率的に数値解析が行えるようになったのと同じように，この有本–長岡の算法によって量子通信路容量の数値解析が効率的に行えるようになった．以下に具体例を示す．

4.1 有本–長岡の算法の適用例

対称でなく，数値解析によらなければ解を得ることができない例として振幅シフトキーイング (ASK) 変調されたレーザー光を用いた 3 元信号を取り上げる．レーザー光は次式によって定義されるコヒーレント状態 $|\alpha\rangle$ によって表される：

$$\hat{a}|\alpha\rangle = \alpha|\alpha\rangle. \tag{25}$$

ただし，$\hat{a}$ は光子消滅作用素であり，α はレーザー光の複素振幅である．これを用いて次式で与えられるような 3ASK 信号を考える．

$$\hat{\rho}_1 = |0\rangle\langle 0|, \quad \hat{\rho}_2 = |\alpha\rangle\langle\alpha|, \quad \hat{\rho}_3 = |-\alpha\rangle\langle-\alpha|. \tag{26}$$

この信号に対する量子通信路容量とそれを与える先験確率分布を有本–長岡の算法で計算した結果を図1に示す．シミュレーションの際には N ステップ目の計算終了時に $\Delta S(\boldsymbol{\xi}^{(N)}) - \Delta S(\boldsymbol{\xi}^{(N-1)}) < 10^{-8}$ となる場合をもって収束したと判定した．この結果から，量子通信路容量を与える先験確率分布では信号 2 と 3 の先験確率が等しくなることが判る．また，先験確率分布の初期値 $\boldsymbol{\xi}^{(1)}$ を乱数によって発生させ，収束までに要した計算回数の平均値を図2に示す．このとき，各点毎に異なる 50 個の初期値でシミュレーションを行った．この結果から振幅 α が大きくなるにしたがって速く収束する傾向があることが判る．

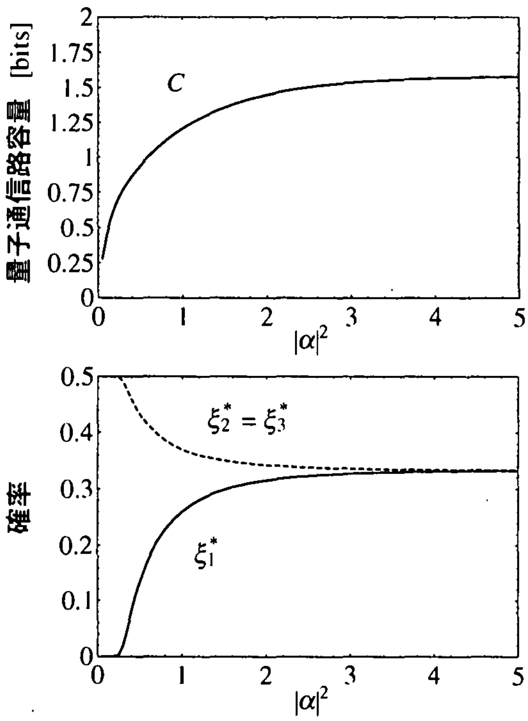

図 1: 3ASK 信号の量子通信路容量とそれを与える先験確率分布

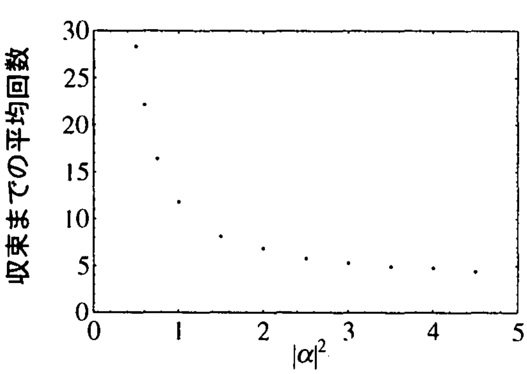

図 2: 収束までの平均計算回数

5 まとめ

M 元対称信号の量子通信路容量は先験確率分布が一様分布であるときに達成されることを解析的に示し，その具体例を示した．また，有本–長岡の算法に基づく数値解析の具体例を示した．

参考文献

[1] R.G. Gallager, *Information Theory and Reliable Communication*, John Wiley & Sons, 1968.

[2] T.M. Cover and J.A. Thomas, *Elements of Information Theory*", John Wiley & Sons, 1991.

[3] A.S. Holevo, *J. Multivar. Anal.*, vol.3, pp.337-394, 1973.

[4] R.L. Stratonovich and A.G. Vantsjan, *Probl. Control Inform. Theory*, vol.7, no.3, pp.161-174, 1978.

[5] A.S. Holevo, *Probl. Inform. Transm.*, vol.15, no.4, pp.3-11, Oct.-Dec. 1979.

[6] B. Schumacher, *Phys. Rev. A*, vol.51, no.4, pp.2738-2747, Apr. 1995.

[7] R. Jozsa and B. Schumacher, *J. Mod. Opt.*, vol.41, pp.2343-2349, 1994.

[8] P. Hausladen, R. Jozsa, B. Schumacher, M. Westmoreland and W.K. Wootters, *Phys. Rev. A*, vol.54, no.3, pp.1869-1876, Sep. 1996.

[9] B. Schumacher and M.D. Westmoreland, *Phys. Rev. A*, vol.56, no.1, pp.131-138, Jul. 1997.

[10] A. S. Holevo, *IEEE Trans. Inform. Theory*, vol.44, no.1, pp.269-273, Jan. 1998.

[11] S. Arimoto, *IEEE Trans. Inform. Theory*, vol.IT-18, no.1, pp.14-20, Jan. 1972.

[12] R. Blahut, *IEEE Trans. Inform. Theory*, vol.IT-18, no.4, pp.460-473, Jul. 1972.

[13] K. Kato, M. Osaki and O. Hirota, submitted to *Phys. Lett. A*, (Jun. 1998).

[14] H. Nagaoka, *Proc. ISIT 1998*, Cambridge, MA, USA, pp.354, Aug. 1998.

[15] A. Peres, *Quantum Theory: Concepts and Methods*, Kluwer Academic Publishers, 1993.

[16] J.J. Sakurai, *Modern Quantum Mechanics*, The Benjamin/Cummings Publishing Company, 1985.

[17] K. Kato, M. Osaki, M. Sasaki and O. Hirota, to be appeared in *IEEE Trans. Commun.*