The 25th Symposium on Information Theory
and Its Applications (SITA2002)
Ikaho, Gunma, Japan, Dec. 10–13, 2002

古典-量子通信路における量子信頼性関数の補助関数の性質
Property of the auxiliary function appearing in quantum reliability function in classical-quantum channel

柳　研二郎* 古市　茂† 栗山　憲‡
Kenjiro Yanagi　Shigeru Furuichi　Ken Kuriyama

Abstract— Concavity of the auxiliary function which appears in the random coding exponent as the lower bound of the quantum reliability function for general quantum states is proved for $0 \le s \le 1$ in two dimensional case.

Keywords— Quantum reliability function, random coding exponent, quantum information theory

1　はじめに

量子情報理論において量子信頼性関数に現れる補助関数 $\mu_q(s,\pi)$ の性質を調べることは古典の場合と同様に重要である．古典系における補助関数 $\mu_c(s,p)$ の性質は現在までに次の性質が証明されている．ただし $\mu_c(s,p)$ は信頼性関数の下界を与える random coding exponent $E_r^c(R)$ を次のように定義するものである．

$$E_r^c(R) = \max_{s,\pi}\{\mu_c(s,\pi) - sR\}.$$

補題 1 次の (a),(b),(c),(d),(e) が成立する．

(a) $\mu_c(0,\pi) = 0$.

(b) $\frac{\partial \mu_c(s,\pi)}{\partial s}|_{s=0} = I(X,Y)$, ただし $I(X,Y)$ は相互情報量である．

(c) $\mu_c(s,\pi) > 0\ (0 < s \le 1)$.
$\mu_c(s,\pi) < 0\ (-1 < s \le 0)$.

(d) $\frac{\partial \mu_c(s,\pi)}{\partial s} > 0,\ (-1 < s \le 1)$.

(e) $\frac{\partial^2 \mu_c(s,\pi)}{\partial s^2} \le 0,\ (-1 < s \le 1)$.

量子系においては対応する性質 (a),(b),(c),(d) が成り立つことは [6], [7] で証明されている．また補助関数 $\mu_q(s,\pi)$ の凹性については純粋状態の場合には [1] によって、また expurgation method を採用した場合には [6] によって証明されている．しかし一般の混合状態の場合には未だに未解決のままである．

2　量子信頼性関数

古典-量子通信路における信頼性関数は $0 < R < C$ に対して次のように定義される．

$$E(R) = -\liminf_{n\to\infty}\frac{1}{n}\log P_e(2^{nR},n), \qquad (1)$$

ただし C は classical-quantum capacity であり，R は伝送レート $R = \frac{\log_2 M}{n}$ (n と M はそれぞれ符号語の個数とメッセージの個数を表す) である．C は Holevo によって次のように与えられている．

定理 1 ([5])

$$C = \max_{\pi}\{H(\bar{S}) - \sum_{i=1}^{a}\pi_i H(S_i)\},$$

ただし $\bar{S} = \sum_{i=1}^{a}\pi_i S_i$ であり，$H(S)$ は *von Neumann entropy* である．

誤り確率 $P_e(2^{nR},n)$ は任意に平均誤り確率の最小値

$$\min_{\mathcal{W},X}\bar{P}(\mathcal{W},X)$$

か最大誤り確率の最小値

$$\min_{\mathcal{W},X}P_{\max}(\mathcal{W},X)$$

を取ることができる．これらの誤り確率は

$$\bar{P}(\mathcal{W},X) = \frac{1}{M}\sum_{j=1}^{M}P_j(\mathcal{W},X),$$

$$P_{\max}(\mathcal{W},X) = \max_{1\le j\le M}P_j(\mathcal{W},X),$$

で定義される．ただし

$$P_j(\mathcal{W},X) = 1 - Tr[S_{w^j}X_j]$$

は $\sum_{j=1}^{M}X_j \le I$ を満たす正作用素測度 $X = \{X_j\}$ に関連する通常の誤り率である．ここで S_{w^j} は符号ブロック $\mathcal{W} = \{w^1, w^2, \ldots, w^M\}$ から選ばれた符号語 w^j に対応する密度作用素である．ランダム符号化法が用いられたとき，(1) で定義された量子信頼性関数に対する下界は

$$E(R) \ge E_r^q(R) \equiv \max_{\pi}\sup_{0<s\le 1}\{\mu_q(s,\pi) - sR\},$$

この不等式は pure states のときのみに証明されている．

* 〒755-8611 宇部市常盤台 2-16-1 山口大学工学部共通講座. Dept. of Applied Science, Faculty of Engineering, Yamaguchi University, Tokiwadai 2-16-1, Ube, 755-8611 Japan. E-mail: yanagi@yamaguchi-u.ac.jp

† 〒756-0884 小野田市大学通 1-1-1　山口東京理科大学基礎工学部電子・情報工学科. Dept. of Electronics and Computer Science, Faculty of Fund. Engineering, Tokyo University of Science in Yamaguchi, Daigakudori 1-1-1, Onoda, 756-0884 Japan. E-mail: furuichi@ed.yama.tus.ac.jp

‡ 〒755-8611 宇部市常盤台 2-16-1 山口大学工学部共通講座. Dept. of Applied Science, Faculty of Enginnering, Yamaguchi University, Tokiwadai 2-16-1, Ube, 755-8611 Japan. E-mail: kuriyama@yamaguchi-u.ac.jp

で定義される．ただし $\pi = \{\pi_1, \pi_2, \ldots, \pi_a\}$ は $\sum_{i=1}^{a} \pi_i = 1$ を満たす先験確率分布である．また

$$\begin{aligned} \mu_q(s,\pi) &= -\log G(s), \\ G(s) &= Tr[A(s)^{1+s}], \\ A(s) &= \sum_{i=1}^{a} \pi_i S_i^{\frac{1}{1+s}} \end{aligned}$$

とおく．ただし各 S_i は入力アルファベット集合 $A = \{1, 2, \ldots, a\}$ から Hilbert 空間 $\mathcal{H}$ における出力の量子状態への量子通信路 $i \to S_i$ の出力状態に対応する密度作用素である．Holevo [6], Ogawa and Nagaoka [7] では $\mu_q(s,\pi)$ が $-1 < s \leq 1$ で凹関数であることの予想がされているがまだ証明はされていなかった． $\exists\, S_i$; invertible $\Rightarrow A(s)$; invertible

定理 2 ([3]) 次が成り立てば $\mu_q(s,\pi)$ は $-1 < s \leq 1$ で凹関数である．

$$Tr[A(s)^s \sum_{j=1}^{a} \pi_j S_j^{\frac{1}{1+s}} (\log S_j^{\frac{1}{1+s}})^2$$

$$-A(s)^{-1+s} (\sum_{j=1}^{a} \pi_j S_j^{\frac{1}{1+s}} \log S_j^{\frac{1}{1+s}})^2] \geq 0. \quad (2)$$

証明

$$\frac{\partial \mu_q(s,\pi)}{\partial s} = -G(s)^{-1} G'(s),$$

だから次を得る．

$$\frac{\partial \mu_q(s,\pi)}{\partial s^2} = G(s)^{-2} (G'(s)^2 - G(s) G''(s)).$$

[6] の P35 の公式より

$$\begin{aligned} & G'(s) \\ = \ & Tr[A(s)^s (A(s) \log A(s) + (1+s) A'(s))] \\ = \ & -Tr[A(s)^s \Delta H(s,\pi)], \end{aligned}$$

ただし

$$\Delta H(s,\pi) = H(A(s)) - \sum_{i=1}^{a} \pi_i H(S_i^{\frac{1}{1+s}}).$$

簡単な計算により

$$\begin{aligned} & G''(s) \\ = \ & Tr[A(s)^{-1+s} \{A(s)^2 (\log A(s))^2 \\ & + s(1+s) A'(s)^2\}] \\ = \ & Tr[A(s)^{-1+s} \{A(s)(2(1 + (1+s)\log A(s)) \\ & A'(s) + (1+s) A''(s))\}], \end{aligned} \quad (3)$$

ただし

$$A'(s) = -\frac{1}{(1+s)^2} \sum_{i=1}^{a} \pi_i S_i^{\frac{1}{1+s}} \log S_i, \quad (4)$$

$$\begin{aligned} A''(s) \ = \ & \frac{1}{(1+s)^4} \sum_{i=1}^{a} \pi_i S_i^{\frac{1}{1+s}} \\ & (2 \log S_i^{1+s} + (\log S_i)^2). \end{aligned} \quad (5)$$

(4), (5) を (3) に代入すると

$$\begin{aligned} & G''(s) \\ = \ & Tr[A(s)^{-1+s} \{H(A(s))^2 + \frac{s}{1+s} \\ & (\sum_{i=1}^{a} \pi_i H(S_i^{\frac{1}{1+s}}))^2 \\ & -2H(A(s)) \sum_{i=1}^{a} \pi_i H(S_i^{\frac{1}{1+s}}) \\ & + \frac{1}{1+s} \sum_{i=1}^{a} \pi_i S_i^{\frac{1}{1+s}} \sum_{j=1}^{a} \pi_j S_j^{\frac{1}{1+s}} (\log S_j^{\frac{1}{1+s}})^2\}] \\ = \ & Tr[A(s)^{-1+s} \{H(A(s))^2 \\ & -2H(A(s)) \sum_{i=1}^{a} \pi_i H(S_i^{\frac{1}{1+s}}) \\ & + (\sum_{i=1}^{a} \pi_i H(S_i^{\frac{1}{1+s}}))^2 \\ & + \frac{1}{1+s} \sum_{i=1}^{a} \pi_i S_i^{\frac{1}{1+s}} \sum_{j=1}^{a} \pi_j S_j^{\frac{1}{1+s}} (\log S_j^{\frac{1}{1+s}})^2 \\ & - \frac{1}{1+s} (\sum_{i=1}^{a} \pi_i H(S_i^{\frac{1}{1+s}}))^2\}]. \end{aligned} \quad (6)$$

ここで

$$\tilde{G}''(s) = Tr[A(s)^{-1+s} \Delta H(s,\pi)^2]. \quad (7)$$

とおくと Cauchy-Schwarz の不等式より

$$G'(s)^2 - G(s) \tilde{G}''(s) \leq 0.$$

したがってもし

$$\tilde{G}''(s) \leq G''(s), \quad (8)$$

が成り立てば $H(A(s))$ は $A(s)^{-1+s}$ と可換だから (6), (7) から (8) は定理の結論を導く．q.e.d.

3 部分的解決

定理 3 次の場合には (2) が成り立つ．

(i) $a = 2$, $\pi_1 = \pi_2 = \frac{1}{2}$, $s = 1$.

(ii) $a = 2$, $\pi_1 = \pi_2 = \frac{1}{2}$, $s = 0$.

証明 $S_1^{\frac{1}{1+s}} = A$, $S_2^{\frac{1}{1+s}} = B$ とおく．このとき次を証明すればよい．

$$Tr[(\frac{A+B}{2})^{-1+s}\{(\frac{A+B}{2})$$
$$(\frac{1}{2}A(\log A)^2 + \frac{1}{2}B(\log B)^2)$$
$$-(\frac{1}{2}A\log A + \frac{1}{2}B\log B)^2\}] \geq 0.$$

簡単な計算により次を得る．

$$\begin{aligned}
& Tr[(A+B)^{-1+s}(A+B) \\
& (A(\log A)^2 + B(\log B)^2)] \\
& -Tr[(A+B)^{-1+s}(A\log A + B\log B)^2] \\
= \; & Tr[(A+B)^{-1+s}AB(\log B)^2] \\
& +Tr[(A+B)^{-1+s}BA(\log A)^2] \\
& -2\mathrm{Re}\, Tr[A\log A(A+B)^{-1+s}B\log B].
\end{aligned}$$

(i) の場合 $(s = 1)$ は次のように変形される．

$$\begin{aligned}
& Tr[AB(\log B)^2] + Tr[BA(\log A)^2] \\
& -2\mathrm{Re}\, Tr[A\log AB\log B] \\
= \; & Tr[AB(\log B)^2] + Tr[BA(\log A)^2] \\
& -2\mathrm{Re}\, Tr[B^{1/2}A^{1/2}\log AA^{1/2}B^{1/2}\log B] \\
\geq \; & Tr[AB(\log B)^2] + Tr[BA(\log A)^2] \\
& -2(Tr[A^{1/2}\log ABA^{1/2}\log A])^{1/2} \\
& (Tr[B^{1/2}\log BAB^{1/2}\log B])^{1/2} \\
= \; & \{(Tr[BA(\log A)^2])^{1/2} \\
& -(Tr[AB(\log B)^2])^{1/2}\}^2 \geq 0.
\end{aligned}$$

(ii) の場合 $(s = 0)$ は次の等式を使う．

有 A^{-1}, B^{-1} のとき.

$$\begin{aligned}
& (A+B)^{-1} \\
= \; & B^{-1}(A^{-1}+B^{-1})^{-1}A^{-1} \\
= \; & A^{-1}(A^{-1}+B^{-1})^{-1}B^{-1}. \qquad (9)
\end{aligned}$$

このとき次のように変形される．

$$\begin{aligned}
& Tr[B(A+B)^{-1}A(\log B)^2] \\
& +Tr[A(A+B)^{-1}B(\log A)^2] \\
& -2\mathrm{Re}\, Tr[\log AA(A+B)^{-1}B\log B] \\
= \; & Tr[(A^{-1}+B^{-1})^{-1}(\log B)^2] \\
& +Tr[(A^{-1}+B^{-1})^{-1}(\log A)^2] \\
& -2\mathrm{Re}\, Tr[\log A(A^{-1}+B^{-1})^{-1}\log B] \\
= \; & Tr[(A^{-1}+B^{-1})^{-1}(\log B)^2] \\
& +Tr[(A^{-1}+B^{-1})^{-1}(\log A)^2] \\
& -2\mathrm{Re}\, Tr[\log A(A^{-1}+B^{-1})^{-1/2} \\
& (A^{-1}+B^{-1})^{-1/2}\log B] \\
\geq \; & Tr[(A^{-1}+B^{-1})^{-1}(\log B)^2] \\
& +Tr[(A^{-1}+B^{-1})^{-1}(\log A)^2] \\
& -2(Tr[(A^{-1}+B^{-1})^{-1}(\log A)^2])^{1/2} \\
& (Tr[(A^{-1}+B^{-1})^{-1}(\log B)^2])^{1/2} \\
= \; & \{(Tr[(A^{-1}+B^{-1})^{-1}(\log B)^2])^{1/2} \\
& -(Tr[(A^{-1}+B^{-1})^{-1}(\log A)^2])^{1/2}\}^2 \\
\geq \; & 0. \quad \text{q.e.d.}
\end{aligned}$$

注意 1 (i) は任意の a と任意の π でも成り立つ．ところが (ii) は任意の π では成り立つが任意の a で成り立つとは限らない．なぜなら $a \geq 3$ では (9) に対応する表現ができないからである．

次に $0 \leq s \leq 1$ に対して (2) を証明するために $A+B$ の Schatten 分解を用意する．つまり

$$A + B = \sum_n t_n|\phi_n>< \phi_n|,$$

ただし $\{|\phi_n>\}$ は $A+B$ の固有値 $\{t_n\}$ に対応する固有ベクトルである．このとき

$$X = A(\log A)^2 + B(\log B)^2$$

とおくと

$$\begin{aligned}
& Tr[(A+B)^s X] \\
= \; & \sum_n < \phi_n|(A+B)^s X|\phi_n > \\
= \; & \sum_n < (A+B)^{s/2}\phi_n|X(A+B)^{s/2}|\phi_n > \\
= \; & \sum_n t_n^s < \phi_n|X|\phi_n > \\
= \; & \sum_n t_n^s a_n.
\end{aligned}$$

同様に

$$Y = (A\log A + B\log B)^2$$

とおくと

$$\begin{aligned}
& Tr[(A+B)^{-1+s}\mathrm{Y}] \\
= \; & \sum_n < \phi_n|(A+B)^{-1+s}Y|\phi_n > \\
= \; & \sum_n < (A+B)^{\frac{-1+s}{2}}\phi_n|Y(A+B)^{\frac{-1+s}{2}}|\phi_n > \\
= \; & \sum_n t_n^{-1+s} < \phi_n|Y|\phi_n > \\
= \; & \sum_n t_n^{-1+s} b_n.
\end{aligned}$$

補題 2 $t_1, t_2, a_1, a_2, b_1, b_2 > 0$ が次の2条件を満たすとする．

(1) $t_1 a_1 + t_2 a_2 \geq b_1 + b_2$

(2) $a_1 + a_2 \geq t_1^{-1} b_1 + t_2^{-1} b_2$

このとき任意の $0 \leq s \leq 1$ に対して次式が成り立つ．

$$t_1^s a_1 + t_2^s a_2 \geq t_1^{-1+s} b_1 + t_2^{-1+s} b_2.$$

証明. $t_1 = t_2$ のときは明らか．$t_1 > t_2$ として一般性を失わない．

このとき次を得る．

$$\begin{aligned}
& t_1^s a_1 + t_2^s a_2 - t_1^{-1+s} b_1 - t_2^{-1+s} b_2 \\
= \ & t_1^s a_1 - t_1^{-1+s} b_1 + t_2^s a_2 - t_2^{-1+s} b_2 \\
= \ & t_1^{-1+s}(t_1 a_1 - b_1) + t_2^{-1+s}(t_2 a_2 - b_2) \\
\geq \ & t_1^{-1+s}(b_2 - t_2 a_2) + t_2^{-1+s}(t_2 a_2 - b_2) \\
= \ & (t_2^{-1+s} - t_1^{-1+s})(t_2 a_2 - b_2).
\end{aligned}$$

ここで不等号は条件 (1) から得られる．
$t_2 a_2 - b_2 \geq 0$ ならば $t_2^{-1+s} - t_1^{-1+s} \geq 0$ だから上式は非負となり結論が言える．一方 $t_2 a_2 - b_2 < 0$ ならば次を得る．

$$\begin{aligned}
& t_1^s a_1 + t_2^s a_2 - t_1^{-1+s} b_1 - t_2^{-1+s} b_2 \\
= \ & t_1^s a_1 - t_1^{-1+s} b_1 + t_2^s a_2 - t_2^{-1+s} b_2 \\
= \ & t_1^s (a_1 - t_1^{-1} b_1) + t_2^s (a_2 - t_2^{-1} b_2) \\
\geq \ & t_1^s (t_2^{-1} b_2 - a_2) + t_2^s (a_2 - t_2^{-1} b_2) \\
= \ & (t_1^s - t_2^s)(t_2^{-1} b_2 - a_2) \geq 0.
\end{aligned}$$

ここで不等号は条件 (2) から得られる．また最後の非負性は $t_1^s - t_2^s \geq 0$ と仮定から得られる．　q.e.d.

注意 2 個数が増えると 補題 *2* は必ずしも成り立たない．反例として

$$t_1 = 3, t_2 = 2, t_3 = 1,$$

$$a_1 = \frac{2}{3}, a_2 = 1, a_3 = \frac{3}{2},$$

$$b_1 = \frac{1}{2}, b_2 = 4, b_3 = 1, s = \frac{1}{2}$$

とすると

$$t_1 a_1 + t_2 a_2 + t_3 a_3 = b_1 + b_2 + b_3 = \frac{11}{2}.$$

$$a_1 + a_3 + a_3 = t_1^{-1} b_1 + t_2^{-1} b_2 + t_3^{-1} b_3 = \frac{19}{6}.$$

となり2条件は成り立つが

$$t_1^s a_1 + t_2^s a_2 + t_3^s a_3 = \frac{2\sqrt{3}}{3} + \sqrt{2} + \frac{3}{2} = 4.068914.$$

$$t_1^{-s} b_1 + t_2^{-s} b_2 + t_3^{-s} b_3 = \frac{\sqrt{3}}{6} + 2\sqrt{2} + 1 = 4.1171021.$$

したがってこの場合は結論が成り立たない．

注意 3 $-1 < s < 0$ の場合は補題 *2* が成り立つかどうかは不明である．

定理 4 A, B を2次元正作用素とする．このとき任意の $0 \leq s \leq 1$ に対して成り立つ．すなわち

$$Tr[(A+B)^s (A(\log A)^2 + B(\log B)^2)$$
$$-(A+B)^{-1+s}(A \log A + B \log B)^2] \geq 0.$$

証明 定理3から補題2の2条件が得られるので結論が成り立つ．q.e.d.

注意 4 定理 *4* は一般の π_1, π_2 のときも成り立つ．

参考文献

[1] M.V.Burnashev and A.S.Holevo, On reliability function of quantum communication channel, Problems of Information Transmission, vol.34, no.2, pp.97-107, 1998.

[2] S.Furuichi, K.Yanagi and K.Kuriyama, A remark on concavity of the function appearing in quantum reliability function, ERATO-2002.

[3] S.Furuichi, K.Yanagi and K.Kuriyama, A sufficient condition on concavity of the auxiliary function appearing in quantum reliablity function, submitted.

[4] R.G.Gallager, Information theory and reliable communication, John Wiley and Sons, 1968.

[5] A.S.Holevo, The capacity of quantum channel with general signal states, IEEE Trans. IT., vol.44, no.1, pp.269-273, 1998.

[6] A.S.Holevo, Reliability function of general classical-quantum channel, IEEE Trans. IT., vol.46, no.6, pp.2256-2261, 2000.

[7] T.Ogawa and H.Nagaoka, Strong converse to the quantum channel coding theorem, IEEE Trans. IT., vol.45, no.7, pp.2486-2489, 1999.