数理解析研究所講究録 1340 巻 2003 年 163-169

量子信頼性函数の補助函数の性質

柳 研二郎 (Kenjiro Yanagi)
山口大・工
(Department of Applied Science, Yamaguchi University)
古市 茂 (Shigeru Furuichi)
山口東京理科大・基礎工
(Department of Electronics and Computer Science,
Tokyo University of Science in Yamaguchi)
栗山 憲 (Ken Kuriyama)
山口大・工
(Department of Applied Science, Yamaguchi University)

1 量子信頼性函数

量子通信路に対する信頼性函数は

$$E(R) \equiv -\liminf_{n\to\infty} \frac{1}{n} \log P_e(2^{nR}, n), \quad 0 < R < C \tag{1}$$

で定義される. ただし C は量子通信路容量であり, R は伝送レートであり $R = \frac{\log_2 M}{n}$ (n と M はそれぞれ入力と出力の符号語数を表わす), 誤り確率 $P_e(M, n)$ 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 $\sum_{j=1}^{M} X_j \le I$ を満たす正作用素値測度 $X = \{X_j\}$ 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 $\mathcal{W} = \{w^1, w^2, \dots, w^M\}$ から選ばれた符合語 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函数に対する下界は

$$E(R) \geq E_q(R) \equiv \max_{\pi} \sup_{0<s\leq 1} \{\mu_q(\pi, s) - sR\},$$

で与えられることが予想されている．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．すべての S_i が純粋状態のときやすべての S_i が可換のときには上で与えられる下界が得られている．したがって少なくとも 1 つの S_i が混合状態のときには conjecture として提起されている．また

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

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．ここでは $\dim[H] < \infty$ とする．Holevo [6], Ogawa and Nagaoka [7] では $\mu_q(\pi, s)$ が $-1 < s \leq 1$ で凹函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．この論文では $a = 2$ で 2 次元密度作用素の場合に $0 \leq s \leq 1$ の範囲で $\mu_q(\pi, s)$ は凹函数であることを証明する．

2 補助函数の凹性(その1)

Proposition 1 ([2], [3]) $A(s)$ を *invertible* と仮定する．このとき次が成り立てば $\mu_q(\pi, s)$ は凹函数である．

$$Tr[(\sum_{i=1}^{a} \pi_i S_i^{\frac{1}{1+s}})^s (\sum_{j=1}^{a} \pi_j S_j^{\frac{1}{1+s}} (\log S_j^{\frac{1}{1+s}})^2) - (\sum_{i=1}^{a} \pi_i S_i^{\frac{1}{1+s}})^{-1+s} (\sum_{j=1}^{a} \pi_j S_j^{\frac{1}{1+s}} \log S_j^{\frac{1}{1+s}})^2] \geq 0.$$

Remark 1 $A(s)$ が *invertible* であるという仮定はそれほど特別ではない．すべての π_i が 0 でないときすべての S_i が *invertible* でなくても $A(s)$ が *invertible* になる場合もある．またどれか 1 個だけ　S_i が *invertible* であれば $A(s)$ は *invertible* となる．

$a = 2$ のときを考える．このとき $S_1^{\frac{1}{1+s}} = A, S_2^{\frac{1}{1+s}} = B$ とおき簡単のため $\pi_1 = \pi_2 = \frac{1}{2}$ とする．したがって補助函数の凹性を示すには

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

を証明すればよい．ここで (2) を次のように変形する．

$$\begin{aligned}
& Tr[(A+B)^s(A(\log A)^2+B(\log B)^2)] - Tr[(A+B)^{-1+s}(A\log A+B\log B)^2] \\
= \; & Tr[(A+B)^{-1+s}(A+B)(A(\log A)^2+B(\log B)^2)] \\
& -Tr[(A+B)^{-1+s}(A\log A+B\log B)^2] \\
= \; & Tr[(A+B)^{-1+s}\{A^2(\log A)^2+AB(\log B)^2+BA(\log A)^2+B^2(\log B)^2\}] \\
& -Tr[(A+B)^{-1+s}\{A^2(\log A)^2+A\log AB\log B+B\log BA\log A+B^2(\log B)^2\}] \\
= \; & Tr[(A+B)^{-1+s}\{AB(\log B)^2+BA(\log A)^2\}] \\
& -Tr[(A+B)^{-1+s}A\log AB\log B] - Tr[(A+B)^{-1+s}B\log BA\log A] \\
= \; & Tr[(A+B)^{-1+s}AB(\log B)^2] + Tr[(A+B)^{-1+s}BA(\log A)^2] \\
& -2\mathrm{Re}\, Tr[A\log A(A+B)^{-1+s}B\log B]. \qquad (3)
\end{aligned}$$

Theorem 1 $s=1$ のとき成り立つ．すなわち

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

Proof. (3) は次のように変形できる．

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

□

Remark 2 Theorem *1* は一般の a に対して成り立つ．また一般の π についても成り立つ．

Theorem 2 $s=0$ のとき成り立つ．すなわち

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

Proof. A,B ともに invertible のとき次のように変形できる．

$$(A+B)^{-1}=A^{-1}(A^{-1}+B^{-1})^{-1}B^{-1}=B^{-1}(A^{-1}+B^{-1})^{-1}A^{-1}.$$

このとき (3) は次のように変形できる.

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

次に A または B が invertible でないときは $A_\varepsilon=A+\varepsilon I$ または $B_\varepsilon=B+\varepsilon I$ とおくと上の計算から次を得る.

$$\begin{aligned}
& Tr[B_\varepsilon(A_\varepsilon+B_\varepsilon)^{-1}A_\varepsilon(\log B_\varepsilon)^2]+Tr[A_\varepsilon(A_\varepsilon+B_\varepsilon)^{-1}B_\varepsilon(\log A_\varepsilon)^2] \\
& -2\mathrm{Re}\, Tr[\log A_\varepsilon A_\varepsilon(A_\varepsilon+B_\varepsilon)^{-1}B_\varepsilon\log B_\varepsilon]\geq 0.
\end{aligned}$$

ここで $\varepsilon\to 0$ とすれば目的の不等式を得る. □

Remark 3 Theorem *2* は一般の π についても成り立つが, 一般の a のとき成り立つかどうかわからない.

3 補助函数の凹性(その2)

$A+B$ を次のように Schatten 分解する.

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

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

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

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

ここで次のような Lemma を必要とする.

Lemma 1 $t_1, t_2, a_1, a_2, b_1, b_2 > 0$ 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.

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

Proof. $t_1 = t_2$ 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. □

Remark 4 個数が増えると Lemma *1* 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

$$t_1a_1+t_2a_2+t_3a_3=b_1+b_2+b_3=\frac{11}{2}.$$

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

となり 2 条件は成り立つが

$$t_1^sa_1+t_2^sa_2+t_3^sa_3=\frac{2\sqrt{3}}{3}+\sqrt{2}+\frac{3}{2}=4.068914.$$

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

したがってこの場合は結論が成り立たない.

Theorem 3 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

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

Proof. Theorem 1, 2 から Lemma 1 の 2 条件が得られるので結論が成り立つ.

□

Remark 5 Theorem *3* は一般の π_1,π_2 のときも成り立つ.

References

[1] M.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 reliability function, INFORMATION, vol.6, no.1, pp.71-76, 2003.

[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.