ISSN 2186-6570

Evaluation of Error probability for Quantum Gaussian Channels Using Gallager Functions

Masaki Sohma

Quantum Information Science Research Center,
Quantum ICT Research Institute, Tamagawa University
6-1-1 Tamagawa-gakuen, Machida, Tokyo 194-8610, Japan

Tamagawa University Quantum ICT Research Institute Bulletin, Vol.4, No.1, 11-14, 2014

Tamagawa University Quantum ICT Research Institute Bulletin
Vol.4 No.1 : 11-14 (2014)

Evaluation of Error Probability for Quantum Gaussian Channels Using Gallager Functions

Masaki Sohma
Quantum Information Science Research Center, Quantum ICT Research Institute, Tamagawa University
6-1-1 Tamagawa-gakuen, Machida, Tokyo 194-8610, Japan
E-mail: sohma@eng.tamagawa.ac.jp

***Abstract*—We review studies about Gallager functions and related quantities for quantum Gaussian channels. In addition we compute a Gallager function to evaluate error probability at transmission rates above channel capacity.**

I. Introduction

This paper discusses bounds on error probability of quantum Gaussian channels, where classical information is conveyed by quantum Gaussian states and a positive operator valued measure is used in the decoding procedure. Let R be the information rate defined by $\log M/n$[1] when we transmit M messages with n use of the channel, that is, a block code of length n. Then the reliability function $E(R)$ shows the speed of exponential decay of the error probabilities P_e at rates below the capacity: $P_e \approx \exp[-nE(R)]$. Quantum coding theorems for the reliability function were established by Holevo and Burnashev [7], [3]. On the analogy from the classical case, they defined the random coding bound $E_r(R)$ and the expurgated bound $E_{ex}(R)$ and proved that these give lower bounds for reliability function $E(R)$ truly in the pure state case. Then Holevo proved the expurgated bound also holds in the mixed state case [4]. Moreover he extended these results to continuous channels with constrained inputs [5]. On the other hand Ogawa and Nagaoka derived a lower bound on the error probability at rates above capacity for a general classical-quantum channel [12].

In this paper, we summarize results about Gallager functions of one-mode quantum Gaussian channels. We introduce a quantum Gaussian channel and show formulas of Gallager functions for it. In addition we compute a lower bound on error probability at rates above capacity for one-mode quantum Gaussian channels with energy constraint on the basis of [12].

II. Quantum Gaussian Channel

We consider quantum system, such as cavity field with a finite number of modes, described by operators $q_1, p_1, \ldots, q_r, p_r$ satisfying the Heisenberg CCR

$$[q_j, p_k] = i\delta_{jk}\hbar I, \ \ [q_j, q_k] = 0, \ \ [p_j, p_k] = 0.$$

Let $\mathcal{H}$ be the Hilbert space of irreducible representation of CCR. For a real column $2r$-vector $z = (x_1, y_1, \ldots, x_r, y_r)^T$, we introduce a unitary operators in $\mathcal{H}$ as

$$V(z) = \exp\, i \sum_{j=1}^{r} (x_j q_j + y_j p_j).$$

Then the operators $V(z)$ satisfy the Weyl-Segal relation

$$V(z)V(z') = \mathrm{e}^{i\Delta(z,z')/2} V(z+z'), \tag{1}$$

where the skew symmetric form Δ is given by

$$\Delta(z, z') = \hbar \sum_{j=1}^{r} (x'_j y_j - x_j y'_j) = -z^T \Delta_r z',$$

with the skew symmetric matrix Δ_r. Here $V(z)$ gives the representation of the CCR on the symplectic space $(\mathbb{R}^{2r}, \Delta)$.

The density operator ρ is called *Gaussian*, if its quantum characteristic function has the form

$$\mathrm{Tr}\rho V(z) = \exp\left[i m^T z - \frac{1}{2} z^T A z \right], \tag{2}$$

where m is a $2r$-dimensional column vector and A is a correlation matrix, which is a real symmetric matrix satisfying

$$A - \frac{i}{2}\Delta_r \geq 0. \tag{3}$$

In the following our concern is devoted to a single mode Gaussian state ($r = 1$) with a mean $m = (m^q, m^p)^T$ and a correlation matrix

$$A(\lambda, \gamma) = \lambda \begin{bmatrix} \gamma^2 & 0 \\ 0 & \gamma^{-2} \end{bmatrix}, \lambda \geq \frac{\hbar}{2}, \gamma > 0. \tag{4}$$

Let us consider a classical-quantum one-mode Gaussian channel defined by a mapping $\Theta : \mathbb{R}^2 \ni m \to \rho_m$, where ρ_m is a Gaussian state with a mean m and a correlation matrix (4). Note that ρ_0 describes background noise, comprising quantum noise and ρ_m is obtained by applying the displacement operator to ρ_0. We relate codewords $w = (m_1, \ldots., m_n)$ of length n to the density operators $\rho_w = \rho_{m_1} \otimes \cdots \otimes \rho_{m_n}$ and assume the energy constraint as

$$\sum_{i=1}^{n} f(m_j) \leq nE, \quad j = 1, \ldots, M, \tag{5}$$

with a energy function

$$f(m_j) = ((m_j^q)^2 + (m_j^p)^2)/2.$$

[1]We use the natural logarithm throughout the paper.

We call by code of size M a sequence $(w^1, X_1), ..., (w^M, X_M)$. Here w^k are codewords of length n, satisfying the additive constraint (5) and $\{X_k\}$ is a family of positive operators in $\mathcal{H}^{\otimes n}$, satisfying $\sum_{k=1}^M X_k \leq I$. The average error probability for such a code is give by

$$P(\{(w^j, X_j)\}) = 1 - \frac{1}{M}\sum_{k=1}^{M} \mathrm{Tr}\rho_{w^k} X_k. \qquad (6)$$

We denote $p(n, M)$ the infimum of this error probability with respect to all codes of size M.

III. Gallager Functions

A. Bounds for Error Probability

We introduce some bounds for the error probability $p(n, M)$. According to [5], we have the following bounds: for $\epsilon > 0$ and sufficiently large n

$$P(e^{nR}, n) \leq \exp[-n(E_r(R) - \epsilon)], \qquad R < C, \qquad (7)$$
$$P(e^{nR}, n) \leq \exp[-n(E_{ex}(R) - \epsilon)], \qquad R < C. \qquad (8)$$

Here C is the capacity of the channel, and

$$E_r(R) = \max_{0\leq s\leq 1} (\max_{0\leq p} \max_{\pi\in\mathcal{P}_1} \mu(\pi, s, p) - sR), \qquad (9)$$
$$E_{ex}(R) = \max_{1\leq s} (\max_{0\leq p} \max_{\pi\in\mathcal{P}_1} \tilde{\mu}(\pi, s, p) - sR), \qquad (10)$$

where μ and $\tilde{\mu}$ are quantum Gallager functions given by

$$\mu(\pi, s, p) = -\log \mathrm{Tr}\left(\int e^{p[f(m)-E]} \rho_m^{\frac{1}{1+s}} \pi(dm)\right)^{1+s} \qquad (11)$$

$$\tilde{\mu}(\pi, s, p) = -s\log \int\int e^{p[f(m)+f(m')-2E]} \cdot (\mathrm{Tr}\sqrt{\rho_m}\sqrt{\rho_{m'}})^{\frac{1}{s}} \pi(dm)\pi(dm'), \qquad (12)$$

and $\mathcal{P}_1$ is the set of Gaussian probability distributions π satisfying

$$\int f(m)\pi(dm) < E. \qquad (13)$$

In addition, applying the Ogawa-Nagaoka lower bound [12] to the continuous case, we obtain for all n [9]

$$P(e^{nR}, n) \geq 1 - \exp(-nE_{on}(R)), R > C. \qquad (14)$$

where

$$E_{on}(R) = \max_{-1<s\leq 0} (\min_{\pi\in\mathcal{P}_1} \mu(\pi, s, 0) - sR). \qquad (15)$$

B. Gallager Functions for Quantum Gaussian Channels

The Gallager functions $\mu(\pi, s, p)$ and $\tilde{\mu}(\pi, s, p)$ with the a priori Gaussian distribution

$$\pi(dm) = \frac{1}{2\pi\sqrt{\det B}} \exp\left[-\frac{1}{2} m^T B^{-1} m\right] dm, \qquad (16)$$

takes the following forms

$$\begin{aligned}\mu(\pi, s, p) =& \\ &- (1+s)\log\left[\sqrt{\det(I_2 - pB)}^{-1} \mathcal{N}_{\frac{1}{1+s}}(A) e^{-pE}\right] \\ &- \log\left[\mathcal{N}_{1+s}\left(\mathcal{G}_{\frac{1}{1+s}}(A)A + (B^{-1} - pI_2)^{-1}\right)\right],\end{aligned} \qquad (17)$$

$$\begin{aligned}\tilde{\mu}(\pi, s, p) =& 2psE \\ &+ \frac{s}{2}\log\det\left[(I_2 - pB)(I_2 - pB + 2(2s\mathcal{G}_{\frac{1}{s}}(A)A)^{-1}B)\right].\end{aligned} \qquad (18)$$

Here I_2 is a $2\times 2-$identity matrix and the functions $\mathcal{N}_s, \mathcal{G}_s$ are given as

$$\mathcal{N}_s(A) = f_s\left(\sqrt{\det A}/\hbar\right)^{-1}, \qquad (19)$$
$$\mathcal{G}_s(A) = g_s\left(\sqrt{\det A}/\hbar\right) I_2, \qquad (20)$$

where

$$f_s(d) = (d + 1/2)^s - (d - 1/2)^s, \qquad (21)$$
$$g_s(d) = \frac{1}{2d} \cdot \frac{(d+1/2)^s + (d-1/2)^s}{(d+1/2)^s - (d-1/2)^s}, \qquad (22)$$

and $\mathrm{abs}(\cdot)$ is defined as follows: for a diagonalizable matrix $M = T\mathrm{diag}(m_j)T^{-1}$, we put $\mathrm{abs}M = T\mathrm{diag}(|m_j|)T^{-1}$.

We compute the Gallager function $\mu(\pi, s, p)$ in the single mode case; the computation of $\tilde{\mu}(\pi, s, p)$ is summarized in [10]. First we consider the case where ρ_0 is a Gaussian state with a correlation matrix

$$A = A(\lambda, 1) = \lambda I_2, \quad \lambda \geq \hbar/2. \qquad (23)$$

Here the optimum *a priori* Gaussian distribution has the correlation matrix $B = \mathrm{diag}[E, E]$. Then the Gallager function is simplified as follows. In the present case, we have

$$\mathcal{N}_{\frac{1}{1+s}}(A) = f_{\frac{1}{1+s}}(\lambda/\hbar)^{-1} \qquad (24)$$

$$\begin{aligned}1/\mathcal{N}_{1+s}&(\mathcal{G}_{\frac{1}{1+s}}(A)A + (B^{-1} - pI_2)^{-1}) \\ =& \left\{(\lambda/\hbar)g_{\frac{1}{1+s}}(\lambda/\hbar) + \frac{E}{\hbar(1-pE)} + \frac{1}{2}\right\}^{1+s} \\ &- \left\{(\lambda/\hbar)g_{\frac{1}{1+s}}(\lambda/\hbar) + \frac{E}{\hbar(1-pE)} - \frac{1}{2}\right\}^{1+s}.\end{aligned} \qquad (25)$$

Substituting these into (17), we obtain

$$\begin{aligned}\mu(\pi, s, p) =& (1+s)\log f_{\frac{1}{1+s}}(\lambda/\hbar) + p(1+s)E \\ &+ \log\left[X^{1+s}(s, p) - Y^{1+s}(s, p)\right],\end{aligned} \qquad (26)$$

where

$$X(s,p) = ((\lambda/\hbar)g_{\frac{1}{1+s}}(\lambda/\hbar) + 1/2)(1-pE) + E/\hbar,$$
$$Y(s,p) = ((\lambda/\hbar)g_{\frac{1}{1+s}}(\lambda/\hbar) - 1/2)(1-pE) + E/\hbar. \quad (27)$$

For a more general correlation matrix (4), the optimum *a priori* Gaussian distribution has the correlation matrix of the form $B = \mathrm{diag}[E_1, E_2]$. Then the function $\mu(\pi, s, p)$ has a complicated form but it is simplified when $p = 0$ as

$$\mu(\pi, s, 0) = (1+s)\log f_{\frac{1}{1+s}}(\lambda/\hbar) + \log f_{1+s}(\sqrt{D}/\hbar), \quad (28)$$

where

$$D = \det(\mathcal{G}_{\frac{1}{1+s}}(A)A + B) = \lambda^2 g_{\frac{1}{1+s}}(\lambda/\hbar)^2 + (\gamma^2 E_2 + \gamma^{-2}E_1)\lambda g_{\frac{1}{1+s}}(\lambda/\hbar) + E_1E_2. \quad (29)$$

C. Optimizations

Firstly we review results about the random coding bound in the case where ρ_0 is a Gaussian state with correlation matrix (23) [5]. Trying to maximize $\mu(\pi, s, p)$ with respect to p we obtain the equation

$$2(1/\hbar - (p\lambda/\hbar)g_{\frac{1}{1+s}}(\lambda/\hbar))(X(s,p)^s - Y(s,p)^s) = p(X(s,p)^s + Y(s,p)^s). \quad (30)$$

Explicit solutions for this equation are only known for $s = 0, 1$. Thus, contrary to the classical case [11], the maximum in (9) in general has not been found only numerically.

Next we compute $E_{on}(R)$ in the case where ρ_0 is a Gaussian state with a correlation matrix (4). Let us find the optimum a priori distribution π. Putting $E_1 = x$ and $E_2 = 2E - x$ $(0 \le x \le 2E)$, we rewrite D in Eq. (28) as

$$D = -\left[x - \left(\frac{\gamma^{-2}-\gamma^2}{2}\lambda g_{\frac{1}{1+s}}(\lambda/\hbar) + E\right)\right]^2 + \left[\frac{\gamma^{-2}+\gamma^2}{2}\lambda g_{\frac{1}{1+s}}(\lambda/\hbar) + E\right]^2. \quad (31)$$

Since $f_{1+s}(d)$ $(-1 < s < 0)$ is a monotonously decreasing function, the optimum a priori distribution π_{opt} is given by putting $x = (\gamma^{-2} - \gamma^2)\lambda g_{1/1+s}(\lambda/\hbar) + E$. Then we have

$$\mu(\pi_{opt}, s, 0) = \log\left[\left(\frac{\lambda}{\hbar}+\frac{1}{2}\right)^{\frac{1}{1+s}} - \left(\frac{\lambda}{\hbar}-\frac{1}{2}\right)^{\frac{1}{1+s}}\right]^{1+s} + \log\left[\left(\frac{E}{\hbar} + \frac{\gamma^2+\gamma^{-2}}{2}\frac{\lambda g_{\frac{1}{1+s}}(\lambda/\hbar)}{\hbar} + \frac{1}{2}\right)^{1+s} - \left(\frac{E}{\hbar} + \frac{\gamma^2+\gamma^{-2}}{2}\frac{\lambda g_{\frac{1}{1+s}}(\lambda/\hbar)}{\hbar} - \frac{1}{2}\right)^{1+s}\right]. \quad (32)$$

Restricting ourselves to the pure state case ($\lambda = \hbar/2$), we can simplify this equation as

$$\mu(\pi_{opt}, s, 0) = \log(\mu_1^{1+s} - \mu_2^{1+s}) \quad (33)$$

with

$$\mu_1 = \frac{E}{\hbar} + \frac{\gamma^2+\gamma^{-2}}{4} + \frac{1}{2}, \quad \mu_2 = \frac{E}{\hbar} + \frac{\gamma^2+\gamma^{-2}}{4} - \frac{1}{2}, \quad (34)$$

and hence we have

$$\mu(\pi_{opt}, s, 0) - sR = R + \log(\mathcal{L}(s)), \quad (35)$$

with

$$\mathcal{L}(s) = \left(\frac{\mu_1}{e^R}\right)^{1+s} - \left(\frac{\mu_2}{e^R}\right)^{1+s}. \quad (36)$$

Differentiating $\mathcal{L}(s)$ with respect to s,

$$\mathcal{L}'(s) = \left(\frac{\mu_1}{e^R}\right)^{1+s}\log\left(\frac{\mu_1}{e^R}\right) - \left(\frac{\mu_2}{e^R}\right)^{1+s}\log\left(\frac{\mu_2}{e^R}\right). \quad (37)$$

Putting $\mathcal{L}'(s) = 0$, we get the optimum value of s as

$$s = \frac{1}{\log\mu_1 - \log\mu_2}\log\frac{\log\mu_2 - R}{\log\mu_1 - R} - 1 =: s_{opt}(R). \quad (38)$$

Thus we obtain

$$E_{on}(R) = \mu(\pi_{opt}, s_{opt}(R), 0) - s_{opt}(R)R,$$

for a one-mode quantum Gaussian channel with correlation matrix (4). Fig. 1 shows graphs of $s_{opt}(R)$ with respect to R for squeezing parameters $\gamma = 1, 3, 5, 10$. Fig. 2 gives graphs of $E_{on}(R)$ with respect to R for $\gamma = 1, 3, 5, 10$.

IV. Conclusion

We have reviewed results about random coding bound for quantum Gaussian channels and computed a lower bound on error probability at transmission rates above capacity on the basis of [12].

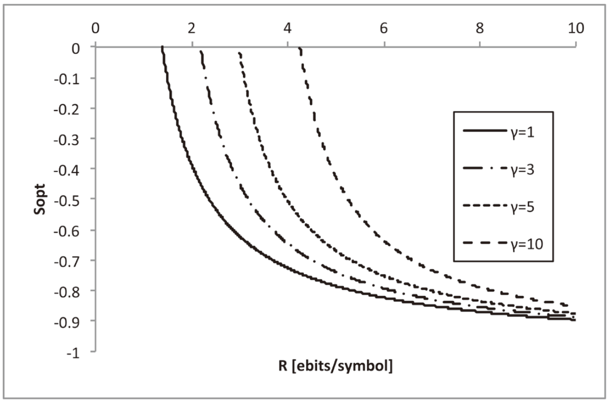

Fig. 1. Dependence of optimum values of s on the transmission rates R [ebits/symbol] for squeezing parameters $\gamma = 1, 3, 5, 10$.

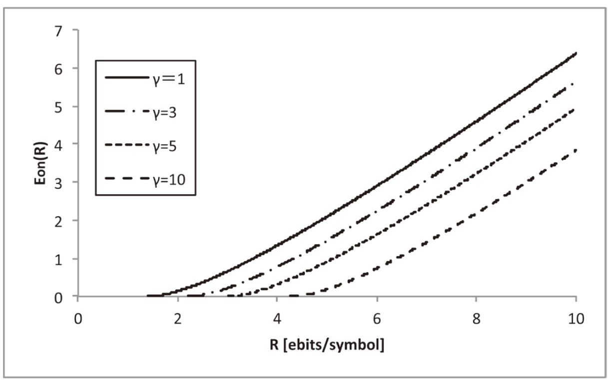

Fig. 2. Error exponents $E_{on}(R)$, which gives a lower bound of error probability as $P(e^{nR}, n) \geq 1 - \exp(-nE_{on}(R))$, for squeezing parameters $\gamma = 1, 3, 5, 10$.

References

[1] A.S. Holevo, Probabilistic and Statistical Aspects of Quantum Theory, North Holland, 1982
[2] A.S. Holevo, M. Sohma, O. Hirota, Capacity of quantum Gaussian channels, vol.59, No. 3, 1999
[3] A. S. Holevo, Coding theorems for quantum channels, Tamagawa University Research Review, 4, 1, 1998
[4] A. S. Holevo, Reliability function of general classical-quantum channel, IEEE Trans. on Information Theory, 46(6), 2256-2260, 2000
[5] A. S. Holevo and M. Sohma and O. Hirota, Error exponents for quantum channels with constrained inputs,Reports on Mathematical Physics, 46, 3, 343-358, 2000
[6] A. S. Holevo and M. Sohma and O. Hirota,Capacity of quantum Gaussian channels,Phys. Rev. A, 59, 1820-1828, 1999
[7] M. V. Burnashev and A. S. Holevo, On reliability function of quantum communication channel, Probl. Peredachi Inform., 34, 1-13, 1998
[8] M. Sohma and O. Hirota, Squeezing is good at low information rates.,Physical Review A, 65, 022319, 2002
[9] M. Sohma and O. Hirota, The Gallager functions and related quantities for quantum Gaussian channel, Proc. of IEEE Int. Symp. on Information Theory, 254, 2001
[10] M. Sohma, Transmission of classical information with squeezed states,Tamagawa University Quantum ICT Research Institute Bulletin Vol.3 No.1, 2013
[11] R. G. Gallager, Information theory and reliable communication,J. Wiley, New York, 1968
[12] T. Ogawa and H. Nagaoka, Strong Converse to the Quantum Channel Coding Theorem, IEEE Trans. on Information Theory, vol. 45, no. 7, 2486-2489, 1999