PAPER *Special Section on Information Theory and Its Applications*

A Simplification Algorithm for Calculation of the Mutual Information by Quantum Combined Measurement

Shogo USAMI[†], ***Nonmember***, **Tsuyoshi Sasaki USUDA**[†], **Ichi TAKUMI**[†], ***and*** **Masayasu HATA**[††], ***Members***

SUMMARY Recently, the quantum information theory attracts much attention. In quantum information theory, the existence of superadditivity in capacity of a quantum channel was foreseen conventionally [1], [2]. So far, some examples of codes which show the superadditivity in capacity have been clarified [3], [4]. However in present stage, characteristics of superadditivity are not still clear up enough. The reason is as follows. All examples were shown by calculating the mutual information by quantum combined measurement, so that one had to solve the eigenvalue and the eigenvector problems. In this paper, we construct a simplification algorithm to calculate the mutual information by using square-root measurement as decoding process of quantum combined measurement. The eigenvalue and the eigenvector problems are avoided in the algorithm by using group covariancy of binary linear codes [5], [6]. Moreover, we derive the analytical solution of the mutual information for parity check codes with any length as an example of applying the simplification algorithm.

key words: *quantum information theory, channel capacity, square-root measurement, mutual information, superadditivity*

1. Introduction

We consider classical information transmission over a quantum channel. In quantum information theory, signals are described as an ensemble of quantum states, their decoding process is described by quantum measurements. There are some remarkable differences between the result in quantum and conventional (classical) information theories. One example is the existence of the superadditivity in capacity of a quantum channel [1], [2]. So far some examples of codes which show the superadditivity in capacity have been clarified [3], [4]. All examples of superadditivity were shown by calculating the mutual information by quantum combined measurement. However, according to the reason that one had to solve the eigenvalue and the eigenvector problems, the examples is not many enough and the characteristics of superadditivity is not sufficiently clarified.

In this paper, we construct a simplification algorithm to calculate the mutual information in order to overcome the difficulty of calculation and to show various examples of the superadditivity. This paper is organized as follows. First, we refer to the definition of capacity of a quantum channel and superadditivity in capacity in Sect. 2. To calculate the mutual information is meaningful in order to show an example of superadditivity in capacity. In Sect. 3, the ordinary method to calculate the mutual information by using square-root measurement as decoding process is explained. Since the ordinary method has many costs, a cost reduction method is hoped. In Sect. 4, we show a simplification algorithm to calculate the mutual information for any binary linear code even if the code word length is long. The simplification algorithm gives a general formula of the mutual information for any linear code. In Sect. 5, we derive the analytical solution of the mutual information for parity check codes as an example of applying the simplification algorithm. Then, properties of the mutual information for parity check codes are also considered. Conclusion is given in Sect. 6.

2. Superadditivity in Capacity of a Quantum Channel and Mutual Information

In quantum communication systems, a signal is described by quantum state $\hat{\rho}_i$ with its a priori probabilities ξ_i. A decision process of these signal states $\hat{\rho}_i$ is described by detection operators $\{\hat{\Pi}_j\}$ which are non-negative $\hat{\Pi}_j \geq 0$ and satisfy the resolution of the identity $\sum_j \hat{\Pi}_j = \hat{I}$. Here $\hat{I}$ is the identity operator. Then the mutual information is defined with a priori probabilities $\{\xi_i\}$ and conditional probabilities $\{P(j|i) = \mathrm{Tr}\hat{\rho}_i\hat{\Pi}_j\}$ as

$$I_1(X:Y) = \sum_i \xi_i \sum_j P(j|i) \log \left[\frac{P(j|i)}{\sum_k \xi_k P(j|k)} \right], \quad (1)$$

where $P(j|i)$ is the probability that the signal j is chosen when the signal i is true. The maximum value of the mutual information with respect to detection operators and a priori probabilities is called the capacity without coding C_1:

$$C_1 = \max_{\{\xi_i\}} \max_{\{\hat{\Pi}_j\}} I_1(X;Y). \quad (2)$$

In binary pure-state case, C_1 becomes [7], [8]

Manuscript received January 22, 1999.
Manuscript revised April 26, 1999.

[†]The authors are with the Department of A.I. & Computer Science, Nagoya Institute of Technology, Nagoya-shi, 466–8555 Japan.
[††]The author is with the Department of Applied Information Technology, Aichi Prefectural University, Aichi-ken, 480–1198 Japan.

$$C_1 = 1 + P\log P + (1-P)\log(1-P) \text{ [bits/letter]}, \quad (3)$$

where, P is the error probability in the optimal decision process. For n-th extension of the signals, C_n is defined in a similar way in Eq. (2) and called "channel capacity of code word length n." And it is known that there exists superadditivity in capacity [1], [2]:

$$C_m + C_n \leq C_{m+n} \quad \text{[bits]}. \quad (4)$$

For a classical channel, the capacity is additive and the sign of equality is always attained in Eq. (4). We can define the limit

$$C = \lim_{n\to\infty} \frac{C_n}{n} \quad \text{[bits/letter]}, \quad (5)$$

that is called "the capacity of the quantum channel." Recently Hausladen et al. [9] proved that the capacity is

$$C = \max_{\{\xi_i\}} S(\hat{\rho}) \equiv \max_{\{\xi_i\}} [-\mathrm{Tr}(\hat{\rho}\log\hat{\rho})], \quad (6)$$

$$\hat{\rho} = \sum_i \xi_i \hat{\rho}_i, \quad (7)$$

where $S(\cdot)$ represents the von Neumann entropy. In order to give an example of the strict superadditivity, it is sufficient to calculate C_n for general n and show the inequality $C_m + C_n < C_{m+n}$.

However, it is too difficult to calculate the channel capacity C_n of code word length n, because it includes double optimizatio n of detection operators and a priori probabilities. Here, we will calculate the mutual information $I_n(X;Y)$ which is always smaller than C_n. Then we show an inequality $C_1 < I_n(X;Y)/n$. This ensures the strict superadditivity as

$$C_1 < \frac{I_n(X;Y)}{n} \leq \frac{C_n}{n} \quad \text{[bits/letter]}. \quad (8)$$

3. Mutual Information by Square-Root Measurement

Square-root measurement (srm) is known as a typical quantum combined measurement. Square-root measurement $\{\hat{\Pi}_j^{(\mathrm{srm})}\}$ for pure-state signals $\{|\psi_i\rangle \ |i = 0, 1, \cdots M-1\}$ when $\xi_i = \frac{1}{M}$ is defined as follows:

$$\hat{\Pi}_j^{(\mathrm{srm})} = |\mu_j\rangle\langle\mu_j|, \quad j = 0, 1, \cdots, M-1, \quad (9)$$

$$|\mu_j\rangle = \hat{\Phi}^{-\frac{1}{2}}\sqrt{\xi_j}|\psi_j\rangle, \quad (10)$$

$$\hat{\Phi} = \sum_{i=0}^{M-1} \xi_i |\psi_i\rangle\langle\psi_i|. \quad (11)$$

It is known that the srm is the minimum error decoding process for covariant signals with respect to a group with the operation "Exclusive-OR" when each signal has equal a priori probability [3], [6]. So we employ the srm as the quantum combined measurement.

In general, the calculation of a channel matrix in the srm is difficult because one has to calculate square-root of the Gram operator. However one can easily calculate the channel matrix under a certain condition by applying the following lemma.

Lemma 1 (Hausladen, Jozsa et al. [9]): Let $\{|\psi_i\rangle|i = 0,1,\cdots,M\text{–}1\}$ be M-ary linearly independent pure-state signals, and a priori probability of each signal be equal. Then, the inner product $\langle\mu_j|\psi_i\rangle$ between the measurement quantum state $|\mu_j\rangle$ of the srm and the signal $|\psi_i\rangle$ is related to the square-root of the Gram matrix Γ_M as

$$\langle\mu_j|\psi_i\rangle = (\Gamma_M^{\frac{1}{2}})_{i,j}, \quad (12)$$

where $(\Gamma_M)_{i,j} = \langle\psi_i|\psi_j\rangle$.

Let us consider a code generated by m-th extension of letter states $\{|0\rangle, |1\rangle\}$ corresponding to classical letters 0 and 1 and selection of $M = 2^n$ code words from the 2^m possible sequences of length m. Then, the Gram matrix Γ_{2^n} and the conditional probability $P(j|i)$ a element of channel matrix $[P(j|i)]$ for the code are

$$\Gamma_{2^n} = [\langle\psi_i|\psi_j\rangle], \quad (13)$$

$$P(j|i) = \mathrm{Tr}|\psi_i\rangle\langle\psi_i|\hat{\Pi}_j^{(\mathrm{srm})} = |\langle\mu_j|\psi_i\rangle|^2 = |(\Gamma_{2^n}{}^{frac12})_{i,j}|^2, \quad (14)$$

which are obtained by calculating the square-root of the Gram matrix. Moreover, each elements of the Gram matrix is represented by the inner product $\kappa = \langle 0|1\rangle$ and the Hamming distance $d_{\mathrm{H}}(\psi_i, \psi_j)$ between classical code words which correspond to code word states $|\psi_i\rangle$ and $|\psi_j\rangle$;

$$(\Gamma_{2^n})_{i,j} = \langle\psi_i|\psi_j\rangle = \kappa^{d_{\mathrm{H}}(\psi_i,\psi_j)}, \quad (15)$$

where the inner product κ is assumed to be real. Using Eq. (14), the mutual information when the srm is applied becomes

$$I_m(X;Y) = \frac{1}{2^n}\sum_{i=0}^{2^n-1}\sum_{j=0}^{2^n-1} P(j|i)\big\{\log P(j|i) + n\big\}, \quad (16)$$

where it is assumed that a priori probabilities of all code words are $\xi_i = \frac{1}{2^n}$. However if the number of the code words increases, to calculate the above quantity is very tedious job. Because the calculation of the square-root of the Gram matrix still remains the eigenvalue and the eigenvector problems.

4. Simplification Algorithm for Calculating the Mutual Information

We would like to consider a possibility of calculating a mutual information for quantum code words with long length. Here we restrict the case of linear codes in

which the number of code words is $M = 2^n$. In this case the code is group covariant with respect to a group with Exclusive-OR $\oplus$. So that, we have the following relations [5], [6]:

$$\forall i, j, k \in \{0, 1, \cdots, 2^n - 1\},$$
$$(\Gamma_{2^n})_{i,j} = (\Gamma_{2^n})_{k\oplus i, k\oplus j} = (\Gamma_{2^n})_{0, i\oplus j}, \tag{17}$$
$$(\Gamma_{2^n}^{\frac{1}{2}})_{i,j} = (\Gamma_{2^n}^{\frac{1}{2}})_{k\oplus i, k\oplus j} = (\Gamma_{2^n}^{\frac{1}{2}})_{0, i\oplus j}. \tag{18}$$

From Eqs. (14) and (18), an element of the channel matrix by the srm is

$$P(j|i) = P(i \oplus j|0) = P(j'|0), \tag{19}$$

where $j' = i \oplus j$ $(j = 0, 1, \cdots, 2^n - 1)$. Then the mutual information can be described as

$$\begin{aligned} I_m(X;Y) &= n + \frac{1}{2^n} \sum_{i=0}^{2^n-1} \sum_{j'=0}^{2^n-1} P(j'|0) \log P(j'|0) \\ &= n + \sum_{j=0}^{2^n-1} P(j|0) \log P(j|0). \end{aligned} \tag{20}$$

Therefore, the mutual information can be calculated by only calculating the 0-th row of the channel matrix $P(j|0)$, that is, it is sufficient to calculate the 0-th row of the square-root of the Gram matrix $(\Gamma_{2^n}^{\frac{1}{2}})_{0,j}$.

Now, we consider the calculation of the square-root of the Gram matrix. Let $a_j^{(k)}$ be a $(0, j)$ element of the Gram matrix Γ_{2^k}. Then the Gram matrix is represented as

$$\Gamma_{2^k} = \begin{bmatrix} a_0^{(k)} & a_1^{(k)} & \cdots & a_{2^k-1}^{(k)} \\ a_1^{(k)} & a_0^{(k)} & \cdots & a_{2^k-2}^{(k)} \\ \vdots & \vdots & \ddots & \vdots \\ a_{2^k-1}^{(k)} & a_{2^k-2}^{(k)} & \cdots & a_0^{(k)} \end{bmatrix}. \tag{21}$$

Similarly, let $x_j^{(k)}$ be a $(0, j)$ element of the square-root of the Gram matrix $\Gamma_{2^k}^{\frac{1}{2}}$ and the matrix is represented as

$$\Gamma_{2^k}^{\frac{1}{2}} = \begin{bmatrix} x_0^{(k)} & x_1^{(k)} & \cdots & x_{2^k-1}^{(k)} \\ x_1^{(k)} & x_0^{(k)} & \cdots & x_{2^k-2}^{(k)} \\ \vdots & \vdots & \ddots & \vdots \\ x_{2^k-1}^{(k)} & x_{2^k-2}^{(k)} & \cdots & x_0^{(k)} \end{bmatrix}. \tag{22}$$

Since each element of the square-root of the Gram matrix can be represented by only the elements of the Gram matrix, we have

$$x_j^{(k)} = x_j^{(k)}(a_0^{(k)}, a_1^{(k)}, \cdots, a_{2^k-1}^{(k)}). \tag{23}$$

When $k = 0$, the right hand side in Eq. (23) becomes simply a square-root. So we have

$$x_j^{(0)} = x_j^{(0)}(a_0^{(0)}) = \{a_0^{(0)}\}^{\frac{1}{2}}, \quad j = 0. \tag{24}$$

On the other hand, if $k > 0$, the Gram matrices for codes with 2^k code words can be partitioned into a block matrix as

$$\Gamma_{2^k} = \begin{bmatrix} A & B \\ B & A \end{bmatrix}, \tag{25}$$

where A and B are $2^{k-1} \times 2^{k-1}$ submatrices [5], [6]. It is well known that addition, subtraction, and multiplication of a block matrix can be performed by regarding the matrix blocks as matrix elements. So the square-root of the matrix (25) is

$$\Gamma_{2^k}^{\frac{1}{2}} = \begin{bmatrix} X & Y \\ Y & X \end{bmatrix}, \tag{26}$$

where

$$X = \frac{1}{2}\{(A+B)^{\frac{1}{2}} + (A-B)^{\frac{1}{2}}\}, \tag{27}$$
$$Y = \frac{1}{2}\{(A+B)^{\frac{1}{2}} - (A-B)^{\frac{1}{2}}\}, \tag{28}$$

are $2^{k-1} \times 2^{k-1}$ matrices. Here the condition

$$A \geq B \geq 0 \tag{29}$$

must be satisfied for uniqueness of X and Y. Using the above equations, the 0-th row of the square-root of the Gram matrix is represented as follows:

(1) $0 \leq j \leq 2^{k-1} - 1$,

$$\begin{aligned} x_j^{(k)} = \frac{1}{2}\Big\{ & x_j^{(k-1)}\Big(a_0^{(k)} + a_{2^{k-1}}^{(k)}, a_1^{(k)} \\ & + a_{2^{k-1}+1}^{(k)}, \ldots, a_{2^{k-1}-1}^{(k)} + a_{2^k-1}^{(k)}\Big) \\ & + x_j^{(k-1)}\Big(a_0^{(k)} - a_{2^{k-1}}^{(k)}, a_1^{(k)} \\ & - a_{2^{k-1}+1}^{(k)}, \ldots, a_{2^{k-1}-1}^{(k)} - a_{2^k-1}^{(k)}\Big)\Big\}, \end{aligned} \tag{30}$$

(2) $2^{k-1} \leq j \leq 2^k - 1$,

$$\begin{aligned} x_j^{(k)} = \frac{1}{2}\Big\{ & x_{j-2^{k-1}}^{(k-1)}\Big(a_0^{(k)} + a_{2^{k-1}}^{(k)}, a_1^{(k)} \\ & + a_{2^{k-1}+1}^{(k)}, \ldots, a_{2^{k-1}-1}^{(k)} + a_{2^k-1}^{(k)}\Big) \\ & - x_{j-2^{k-1}}^{(k-1)}\Big(a_0^{(k)} - a_{2^{k-1}}^{(k)}, a_1^{(k)} \\ & - a_{2^{k-1}+1}^{(k)}, \ldots, a_{2^{k-1}-1}^{(k)} - a_{2^k-1}^{(k)}\Big)\Big\}. \end{aligned} \tag{31}$$

Applying Eqs. (30) and (31) n times repeatedly, every elements $x_j^{(n)}$ of square-root matrix $\Gamma_{2^n}^{\frac{1}{2}}$ can be described by only $x_0^{(0)}(\cdot)$.

As a result, we obtain the following formula.

$$x_j^{(n)} = \frac{1}{2^n} \sum_{k=0}^{2^n-1} (-1)^{w_{\mathrm{H}}(j \cdot k)}$$

$$\times \sqrt{\sum_{l=0}^{2^n-1} (-1)^{w_{\rm H}(k\cdot l)} a_l^{(n)}}, \tag{32}$$

here $w_{\rm H}(i)$ denotes Hamming weight of i in binary notation. And $j \cdot k$ means "AND" operation for each bits when j and k are represented as binary numbers of n-digits. The answer is unique if Eqs. (27) and (28) satisfy the condition (29). On the other hand, when Eqs. (27) and (28) do not satisfy the condition, the answer does not have uniqueness. However, we confirmed that parity check codes with any length always satisfy the condition (29) at least.

5. Analytical Solution of the Mutual Information for Parity Check Codes

Here we apply the simplification algorithm to derive the analytical solution of the mutual information for parity check codes.

In binary linear code with $M = 2^n$ code words, a $(0, j)$ element of the Gram matrix $(\Gamma_{2^n})_{0,j}$ is represented as

$$(\Gamma_{2^n})_{0,j} = a_j^{(n)} = \kappa^{d_{\rm H}(\psi_0,\psi_j)}, \tag{33}$$

where κ is the inner product between the letter states and $|\psi_0\rangle = |0\rangle \cdots |0\rangle$. $d_{\rm H}(\psi_0, \psi_j)$ is Hamming weight of the classical code word corresponding to $|\psi_j\rangle$. So there are $n + 1$ kinds of $a_j^{(n)}$.

Single parity check codes have 2^{m-1} code words when code word length is m. Assume that the j-th code word is defined by adding a parity bit at the end of the binary notation of the number j. Then the Hamming weight of each code word $d_{\rm H}(\psi_0, \psi_j)$ becomes $2p$ when $w_{\rm H}(j) = 2p$(even) or $2p - 1$(odd). So Eq. (33) is represented by $\lfloor \frac{m}{2} \rfloor + 1$ kinds. Therefore, the detail of the square-root in Eq. (32) consists of $\lfloor \frac{m}{2} \rfloor + 1$ terms. Here, coefficient of κ^{2p} is the subtraction of the number of code words with $(-1)^{w_{\rm H}(k\cdot l)} = -1$ from that with $(-1)^{w_{\rm H}(k\cdot l)} = 1$ in code words of Hamming weight $w_{\rm H}(j) = 2p$.

Since execution of AND operations between k and l are performed at the range: $l = 0, 1, \cdots, 2^{m-1} - 1$, the square-roots in Eq. (32) are classified by Hamming weight $w_{\rm H}(k)$ of k in binary notation. Besides, that is the same between Hamming weight $w_{\rm H}(k) = i$ and $w_{\rm H}(k) = m - i, i = 0, 1, \cdots, \lfloor \frac{m}{2} \rfloor + 1$. As a result, the number of classes of square-root in Eq. (32) is $\lfloor \frac{m}{2} \rfloor + 1$.

On the other hand, $x_j^{(n)}$ is also classified by the Hamming weight of code words by performing AND operation between j and $k (= 0, 1, \cdots, 2^{m-1} - 1)$. So the square-root of the Gram matrix consists of only $\lfloor \frac{m}{2} \rfloor + 1$ elements.

As a result, the mutual information $I_m(X;Y)$ by the srm for parity check code with code word length m is

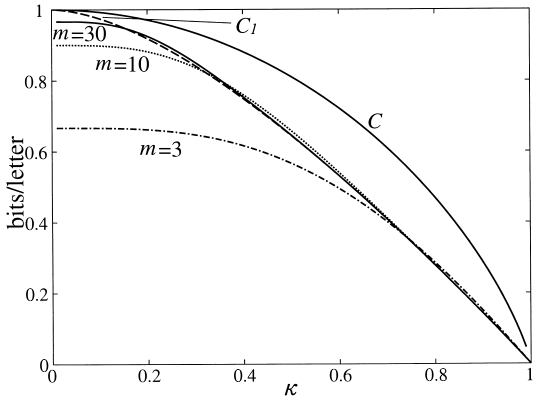


Fig. 1 The mutual information per letter $I_m(X;Y)/m$ for parity check codes (for code word length m = 3,10, and 30) and C_1 and C as functions of κ.

$$\begin{aligned} I_m(X;Y) &= m - 1 + \sum_{i=0}^{\lfloor \frac{m}{2} \rfloor} ({}_{m-1}C_{2i-1} + {}_{m-1}C_{2i}) \\ &\quad \times f_{m,i}(\kappa) \log f_{m,i}(\kappa) \\ &= m - 1 + \sum_{i=0}^{\lfloor \frac{m}{2} \rfloor} {}_mC_{2i} \\ &\quad \times f_{m,i}(\kappa) \log f_{m,i}(\kappa), \end{aligned} \tag{34}$$

where

$$\begin{aligned} f_{m,i}(\kappa) = \Bigg\{ \frac{1}{2^{m-1}} \Bigg(& \sum_{j=0}^{m-1} \Big({}_{m-1}C_j \\ & - 2 \sum_{k=0}^{i-1} \big({}_{2i-1}C_{2k+1} \times {}_{m-2i}C_{j-2k-1} \big) \Big) \\ & \times r_{m,\min(j,m-j)}(\kappa) \Bigg) \Bigg\}^2, \end{aligned} \tag{35}$$

$$\begin{aligned} r_{m,j}(\kappa) = \Bigg\{ \sum_{p=0}^{\lfloor \frac{m}{2} \rfloor} \Bigg(& {}_mC_{2p} - 2 \sum_{q=0}^{j \geq 2q+1} {}_jC_{2q+1} \\ & \times {}_{m-j}C_{2p-2q-1} \Bigg) \kappa^{2p} \Bigg\}^{\frac{1}{2}}, \end{aligned} \tag{36}$$

$${}_iC_{-j} \ , \ {}_iC_{i+j} = 0, \quad j > 0. \tag{37}$$

Here, the channel matrix relates to $f_{m,i}$ as

$$P(j|0) = f_{m,\lceil \frac{w_{\rm H}(j)}{2} \rceil}(\kappa). \tag{38}$$

Equation (34) is the analytical solution of the mutual information for parity check codes.

Figure 1 shows the mutual information per letter for parity check codes $I_m(X;Y)/m$ in comparison with the capacity C_1 without coding and the quantum capacity C. It can be seen that $I_m(X;Y)/m > C_1$ if κ is larger than a certain value which depends on the code

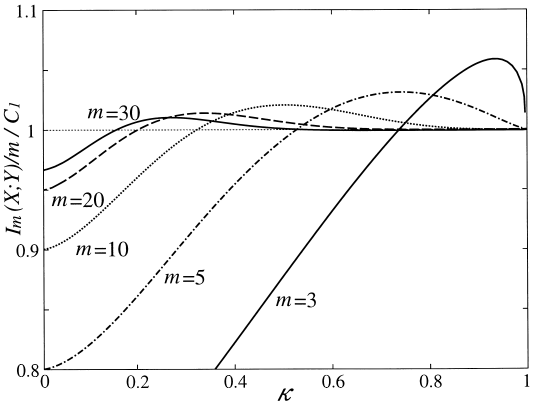


Fig. 2 The ratios of the mutual information per letter for parity check codes to the channel capacity without coding C_1 (for code word length m=3,5,10,20, and 30) as functions of κ.

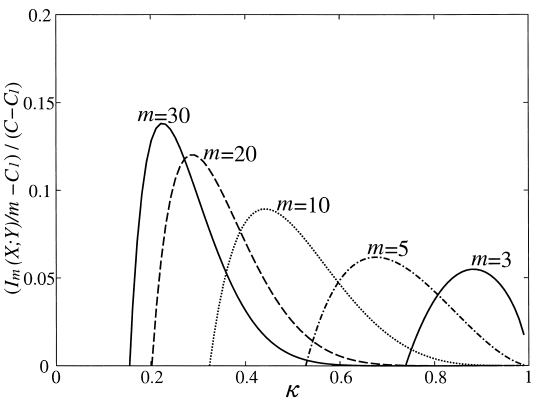


Fig. 3 Achievement factors $(I_m(X;Y)/m - C_1)/(C - C_1)$ of superadditivity as functions of κ.

word length m. We call it a threshold point. This ensures the strict superadditivity. The longer code word length is, the smaller threshold point becomes. Concerned with κ, superadditivity is achieved in wide range when the code word length is long.

Figure 2 shows the ratios $I_m(X;Y)/m/C_1$ of the mutual information per letter to channel capacity without coding C_1 for various length of parity check codes as functions of the inner product κ. According to Fig. 2, once the ratio exceeds 1, the ratio never fall below 1 to what kind of large κ in any length. Moreover, the longer code word length becomes, the more the peak of the ratio approaches 1 asymptotically.

Figure 3 shows achievement factors $(I_m(X;Y)/m - C_1)/(C - C_1)$ for parity check codes with code word lengths m=3,5,10,20, and 30 as functions of κ. Differences the mutual information per letter from C_1 represents an amount of the superadditivity. Since the capacity C is the upper bound for any $I_m(X;Y)/m$, $I_m(X;Y)/m - C_1$ never exceed $C - C_1$ and it is equal to $C - C_1$ in the limit of infinite length of the code. So $C - C_1$ can be regarded as the target value of the amount of the superadditivity. Therefore, Fig. 3 describes how much is the superadditivity achieved to the "full quantum gain." According to Fig. 3, the longer code word length is, the larger achievement factor is. But the longer code word length is, the faster the mutual information approaches to C_1. So the achievement factor approaches to 0 rapidly when the code word length is long.

As a result, we must decide the code word length depending upon the inner product κ of the letter states when parity check code is employed in order to show the superadditivity. A parity check code is a single error-detecting code in classical coding theory. We should employ a code which has higher error-detecti on and correction capabilities in order to show higher superadditivit y.

6. Conclusion

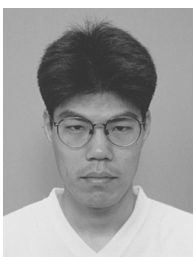
In this paper, we have shown the simplification algorithm to calculate mutual information by quantum combined measurement such as square-root measurement of a binary linear code. The simplification is based on group covariancy of linear codes. As a result, we can calculate the square-root of the Gram matrix without calculating eigenvalues and eigenvectors. This gives a useful tool to derive an analytical solution of the mutual information. Then, we applied the algorithm to derive the analytical solution of the mutual information for parity check codes with any length and show properties of it.

We will derive the analytical solution of the mutual information for any other code, such as BCH code, by applying our formula and study a relation between superadditivity in capacity and error-correction capability in classical channel of the codes.

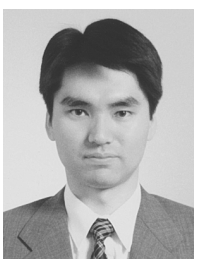
References

[1] A.S. Kholevo, "Information-theoretical aspects of quantum measurement," Problemy Peredachi Informatsii, vol.9, no.2, pp.31–42, 1973.
[2] A.S. Kholevo, "Capacity of a quantum communication channel," Problemy Peredachi Informatsii, vol.15, no.4, pp.3–11, 1979.
[3] M. Sasaki, K. Kato, M. Izutsu, and O. Hirota, "Quantum channels showing superadditivity in classical capacity," Phys. Rev., vol.A58, no.1, pp.146–158, 1998.
[4] K. Kato, M. Osaki, and O. Hirota, "Calculation of mutual information for quantum code words with very long length," Abst. of Forth International Conference on Quantum Communication, Measurement, and Computing (QCM'98), p.30, Aug. 1998.
[5] T.S. Usuda and I. Takumi, "Group covariant signals in quantum information theory," Abst. of Fourth International Conference on Quantum Communication, Measurement, and Computing (QCM'98), p.51, Aug. 1998.
[6] T.S. Usuda, I. Takumi, M. Hata, and O. Hirota, "Minimum error detection of classical linear code sending through a quantum channel," Phys. Lett., vol A256, pp.104–108, 1999.

[7] M. Osaki, M. Ban, and O. Hirota, "The maximum mutual information without coding for binary quantum-state signals," J. Mod. Opt., vol.45, no.2, pp.269–282, 1998.
[8] M. Ban, K. Kurokawa, and O. Hirota, "Cut-off rate performance of quantum communication channels with symmetric states," Quantum and Semiclass. Opt., no.1, pp.206–218, 1999.
[9] P. Hausladen, R. Jozsa, B. Schumacher, M. Westmoreland, and W.K. Wootters, "Classical information capacity of a quantum channel," Phys. Rev., vol.A54, no.3, pp.1869–1876, 1996.
[10] M. Ohya, "On capacity of quantum channel," IEICE Trans., vol.J81-A, no.12, pp.1638–1643, Dec. 1998.
[11] M. Ohya, D. Petz, and N. Watanabe, "On capacities of channels," Probability and Mathematical Statics, vol.17, pp.179–196, 1997.



Shogo Usami received the B.E. and M.S. degrees from Nagoya Institute of Technology, Nagoya, Japan in 1997 and 1999 respectively, both in Department of A.I. and Computer Science, he has been attending Department of A.I. and Computer Science, Nagoya Institute of Technology as a doctoral course student. His current research is quantum information theory. He is a student member of Information Processing Society of Japan.



Tsuyoshi Sasaki Usuda received the B.E., M.E., and Ph.D. degrees in information and communication engineering from Tamagawa University, Tokyo Japan, in 1990, 1992, and 1995, respectively. Since 1995 he has been with Department of A.I. and Computer Science, Nagoya Institute of Technology, Nagoya Japan, where he is presently an Assistant. His current research interests are in quantum information and communication theories and their applications.

Ichi Takumi received the B.E. and M.S. degrees from Nagoya Institute of Technology, Nagoya, Japan in 1982 and 1984 respectively, both in electronic engineering. After graduation he joined Oki Electric Co. He has a Doctor of Eng. degree from Nagoya Institute of Technology. Since December 1985 he has been with Nagoya Institute of Technology, where he is now an Associate Professor of Department of A.I. and Computer Science. His current research interests include digital signal processing and its applications. He is a member of the Society of Instrument and Control Engineerings of Japan.

Masayasu Hata graduated in 1958 from Department of Electronic Engineering, Faculty of Engineering, Nagoya Institute of Technology, and affiliated with Oki Electric Co. He has a Doctor of Eng. degree from Tokyo Institute of Technology. He was engaged in R&D of digital communication system, application of electronic circuits and millimeter wave communication equipment. Retired from Oki Electric Co. in 1985 and became a Professor in the Department of A.I. and Computer Science, Nagoya Institute of Technology. Since 1998 he has been with Aichi Prefectural University as a Professor in the Department of Applied Information Technology. He is engaged in research on digital signal processing and information communication.