Formula of channel matrix for a certain class of $(G, \hat{\chi})$-covariant signals

Yoshihiro ISHIKAWA[1] * Keisuke SHIROMOTO[2] Tsuyoshi Sasaki USUDA[1] †

[1] *School of Information Science and Technology, Aichi Prefectural University, 1522-3 Ibaragabasama, Nagakute, Aichi, 480-1198 Japan.*

[2] *Department of Mathematics and Engineering, Kumamoto University, Kurokami, Kumamoto 860-8555, Japan.*

Keywords: classical-quantum channel, channel matrix, Gram matrix, group covariant

1 Introduction

In the classical-quantum channel, coding theorem for quantum channel has been already proved and we can calculate channel capacity that is asymptotically attained maximum mutual information in the limit of infinite codeword length[1, 2, 3]. However, computation of mutual information in finite codeword length is rather difficult. That is, to evaluate performance of classical-quantum communication system in the real world is hard. As an example, consider computation of a channel matrix of classical-quantum communication in which pure-state signals are transmitted and are measured by square-root measurement[1]. The channel matrix is obtained by computing the square-root of the Gram matrix of the quantum signal set. However, it is very difficult to compute by a universal algorithm if there are many signals (typically, more than 1000). Therefore, we have been studied to derive the analytical solution of the channel matrix[4, 5, 6]. Recently, the general formula for narrow sense group covariant quantum signals[7] was shown[8].

However, some important group covariant signal sets (e.g. four states used in BB84 quantum cryptographic protocol [9] and a SIC set [10]) are not narrow sense covariant. Moreover, it is expected that coded M-ary PSK coherent-state signals by a code over an extension field are not narrow sense group covariant unless the code can be constructed over a prime field or the ring of integers modulo M [6]. Since the formula[8] is not applicable to these signals, further generalization of the formula is necessary. Toward this goal, we defined the $(G, \hat{\chi})$-covariant signal set, which is a generalization of narrow sense group covariant, and showed its necessary and sufficient condition[11]. The relationship of general group covariant signals[12], $(G, \hat{\chi})$-covariant signals[11] and narrow sense group covariant signals[7] is shown in Fig.1.

In the present paper, we derive a formula of channel matrix for a $(G, \hat{\chi})$-covariant signal set when $\hat{\chi}$ is a specific map. Such a signal set is not narrow sense group covariant, so that this result is not included in the conventional formula.

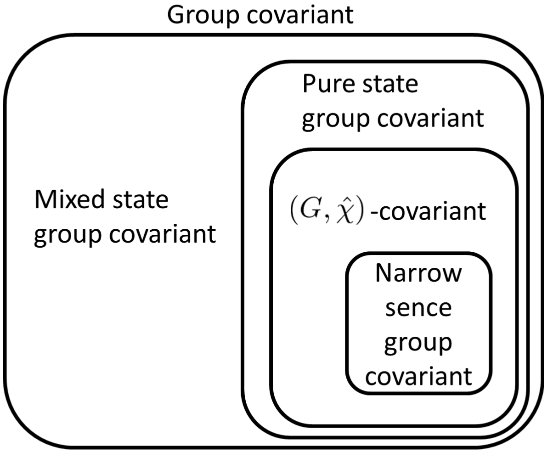
Group covariant
Mixed state group covariant
Pure state group covariant
$(G, \hat{\chi})$ -covariant
Narrow sence group covariant

Figure 1: Relationship of some classes of group covariant signal sets.

2 Narrow sense group covariant signal set and corresponding formula

In [7], a definition of narrow sense group covariant was proposed for a set of pure-state signals and a necessary and sufficient condition was shown. Although the general definition of group covariant signal set was already defined in 1978[12], some useful results such as the formula of a channel matrix were obtained by using the necessary and sufficient condition of a narrow sense group covariant signal set. Here, we briefly survey the definition, the necessary and sufficient condition, and the formula of the channel matrix of a narrow sense group covariant signal set.

2.1 Narrow sense group covariant signals and their necessary and sufficient condition

Definition 1 : Narrow sense group covariant signals[7]
Let $(G; \circ)$ *be a finite group and be a set of parameters characterizing pure quantum state signals* $\{|\psi_i\rangle \, |i \in G\}$. *The set of signals is called* (narrow sense) group covariant *if there exist unitary operators* $U_k (k \in G)$ *such that*

$$U_k|\psi_i\rangle = |\psi_{k \circ i}\rangle \, , \; \forall i, k \in G, \tag{1}$$

*im121001@aichi-pu.ac.jp

†usuda@ist.aichi-pu.ac.jp

For the narrow sense group covariant signals defined in Definition 1, the following necessary and sufficient condition was derived [7].

Proposition 2 : necessary and sufficient condition of narrow sense group covariant signals[7]
A set of pure quantum state signals $\{|\psi_i\rangle\,|i \in G\}$ is (narrow sense) group covariant if and only if, for any $i, j \in G$,

$$\langle\psi_{k\circ i}|\psi_{k\circ j}\rangle = \langle\psi_i|\psi_j\rangle, \tag{2}$$

for all $k \in G$.

Proposition 2 shows the condition for the inner products of the signals. Since the Gram matrix is a matrix of the inner products of the signals, the proposition provides the form of the Gram matrix. As an example, from the proposition, the Gram matrix of any narrow sense group covariant signal set with four elements has the following form.

$$\Gamma = \begin{bmatrix} 1 & a & b & c \\ a & 1 & c & b \\ b & c & 1 & a \\ c & b & a & 1 \end{bmatrix} \text{ or } \begin{bmatrix} 1 & a & b & c \\ c & 1 & a & b \\ b & c & 1 & a \\ a & b & c & 1 \end{bmatrix} \quad (a, b, c \in \mathbb{C}), \tag{3}$$

Note that a, b and c are complex numbers but are not arbitrary since the Gram matrix is hermitian and absolute values of its elements are not exceed unity.

2.2 Formula of channel matrix for narrow sense group covariant signal set

Let $(G; \circ)$ be an abelian group of order M with operation $\circ$ such that

$$G = \{0, 1, \cdots, M-1\}, \tag{4}$$

where, 0 is the identity element of G (i.e. $\forall i \in G, 0 \circ i = i \circ 0 = i$). And let

$$\hat{G} = \{\chi_0, \chi_1, \cdots, \chi_{M-1}\}, \tag{5}$$

be the multiplicative group of the set of all characters [13] of G. We consider a narrow sense group covariant signal set $\{|\psi_i\rangle|i \in G\}$ and its Gram matrix $\Gamma_G = [\langle\psi_i|\psi_j\rangle]$. Then we have the following proposition[11].

Proposition 3 : Formula of channel matrix for narrow sense group covariant set[11]
For any $0 \le i, j \le M-1$,

$$(\Gamma_G)^{1/2}_{ij} = \frac{1}{M}\sum_{l\in G}\chi_l(i\circ j^{-1})\sqrt{\sum_{k\in G}\chi_l(k)\langle\psi_0|\psi_k\rangle} \tag{6}$$

3 $(G, \hat{\chi})$-covariant quantum signal set and their necessary and sufficient condition

In this section, we describe $(G, \hat{\chi})$-covariant quantum signal set which is a generalization of a narrow sense group covariant signal set. The definition of $(G, \hat{\chi})$-covariant quantum signal set is as follows:

Definition 4 : $(G, \hat{\chi})$-covariant quantum signal set[11]
*Let $(G; \circ)$ be a finite group and be a set of parameters characterizing pure quantum state signals $\{|\psi_i\rangle\,|i \in G\}$. The set of signals is called $(G, \hat{\chi})$-*covariant *if there exist unitary operators $U_k (k \in G)$ such that*

$$U_k|\psi_i\rangle = \hat{\chi}(k, i)|\psi_{k\circ i}\rangle, \ \forall i, k \in G, \tag{7}$$

where $\hat{\chi}$ is a map from $G \times G$ into $\mathbb{U} = \{x \in \mathbb{C} \mid |x| = 1\}$.

Note that the original definition includes not only unitary operators but also anti-unitary operators. Here, for simplicity, we asuume the operators which determine $(G, \hat{\chi})$-covariant signal set are unitary.

In Definition 4, if $\hat{\chi}(i, j) = 1, (\forall i, j \in G)$, the set of the signals is narrow sense group covariant. Therefore, $(G, \hat{\chi})$-covariant is a generalization of narrow sense group covariant. For $(G, \hat{\chi})$-covariant signal set, we have the following necessary and sufficient condition.

Proposition 5 : Necessary and sufficient condition of $(G, \hat{\chi})$-covariant signals[11]
A set of pure quantum state signals $\{|\psi_i\rangle\,|i \in G\}$ is $(G, \hat{\chi})$-covariant if and only if, for any $i, j \in G$,

$$\langle\psi_{k\circ i}|\psi_{k\circ j}\rangle = \hat{\chi}(k, i)\overline{\hat{\chi}(k, j)}\langle\psi_i|\psi_j\rangle, \tag{8}$$

for all $k \in G$.

Proposition 5 provides provides the form of the Gram matrix. The following matrix is an example of the Gram matrix of a $(G, \hat{\chi})$-covariant signal set.

$$\Gamma = \begin{bmatrix} 1 & a & b & c \\ a & 1 & -c & -b \\ b & -c & 1 & -a \\ c & -b & -a & 1 \end{bmatrix} \quad (a, b, c \in \mathbb{C}) \tag{9}$$

Apparently, the above example is not a Gram matrix of narrow sense group covariant signal set.

4 Main result: formula of channel matrix for a $(G, \hat{\chi})$-covariant quantum signal set

Now we show the main result: the formula of the channel matrix of a $(G, \hat{\chi})$-covariant quantum signal set with a specific map $\hat{\chi}$. We define the map $\hat{\chi}$ as follows.

$$\hat{\chi}(i^{-1}, j) = \begin{cases} 1 & i = 0 \text{ or } j = 0 \text{ or } j = i, \\ -1 & \text{otherwise,} \end{cases} \tag{10}$$

Note that when the order of the group G is four, the Gram matrix of this $(G, \hat{\chi})$-covariant quantum signal set has the form of Eq.(9).

Then, we finally obtain the following theorem.

Theorem 6 : Formula of channel matrix for a $(G, \hat{\chi})$-covariant quantum signal set

For $i=j=0$ *or* $1 \le i,j \le M-1$,

$$(\Gamma_G)^{1/2}_{ij} = \frac{1}{M}\sum_{l\in G}\chi_l(i\circ j^{-1})\sqrt{1-\sum_{k=1}^{M-1}\chi_l(k)\langle\psi_0|\psi_k\rangle}, \quad (11)$$

For $i=0, 1 \le j \le M-1$ *or* $j=0, 1 \le i \le M-1$,

$$(\Gamma_G)^{1/2}_{ij} = -\frac{1}{M}\sum_{l\in G}\chi_l(i\circ j^{-1})\sqrt{1-\sum_{k=1}^{M-1}\chi_l(k)\langle\psi_0|\psi_k\rangle}, \quad (12)$$

The proof of Theorem 6 is shown in the technical version of the paper and will be presented at the conference.

5 Conclusion

In the present paper, we have shown the formula of the channel matrix of a $(G,\hat{\chi})$-covariant quantum signal set when $\hat{\chi}$ is a specific map. The derived formula is not included in the conventional result. Therefore, combining the conventional and the new formulae, we obtain a generalized formula. We will further generalize the formula by considering the other maps.

Acknowledgment

This work has been supported in part by JSPS KAKENHI Grant Number 24360151.

References

[1] P. Hausladen, R. Jozsa, B. Schumacher, M. Westmoreland, and W.K. Wootters, “Classical information capacity of a quantum channel,” Phys. Rev. **A54**, pp.1869-1876, (1996).

[2] A.S. Holevo, “The capacity of quantum communication channel with general signal states,” IEEE Trans. Inform. Theory **44**, pp.269-272, (1998).

[3] B. Schumacher and M. Westmoreland, “Sending classical information via noisy quantum channel,” Phys. Rev. **A56**, pp.131-138, (1997).

[4] S. Usami, T.S. Usuda, I. Takumi, and M. Hata, “A simplification algorithm for calculation of the mutual information by quantum combined measurement,” IEICE Trans. Fundamentals. **E82-A**, no.10, pp.2185-2190, (1999).

[5] T.S. Usuda, S. Usami, I. Takumi, and M. Hata, “Superadditivity in capacity of quantum channel for q-ary linearly dependent real symmetric-state signals,” Phys. Lett. **A305**, pp.125-134, (2002).

[6] M. Ota, H. Kumazawa, K. Shiromoto, and T.S. Usuda, “Formula of channel matrix for coded quantum signals by classical linear codes over $\mathbb{Z}_m$,” Proc. of ISITA2010, pp.1035-1040, (2010).

[7] T.S. Usuda and I. Takumi, “Group covariant signals in quantum information theory,” Quantum Communication, Computing, and Measurement 2, P. Kumar, G. M. D’Ariano, and O. Hirota (Eds.), Plenum Press, New York, pp.37-42, (2000).

[8] T.S. Usuda and K. Shiromoto, “Analytical expression of s-th power of Gram matrix for group covariant signals and its application,” Quantum Communication, Measurement and Computing (QCMC), AIP Conference Proceedings Vol.1363, T. Ralph and P.K. Lam (Eds.), American Institute of Physics, New York, pp.97-100, (2011).

[9] C.H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” Proc. IEEE International Conference on Computers Systems and Signal Processing, Bangalore India, pp.175-179, (1984).

[10] C.A. Fuchs, “Charting the shape of Hilbert space,” The Tenth International Conference on Quantum Communication, Measurement and Computation (QCMC2010), Prize Talk, (2010).

[11] T.S. Usuda, Y. Ishikawa, and K. Shiromoto, “A class of group covariant signal sets and its necessary and sufficient condition,” Abstracts of Papers of QCMC2012 (11th International Conference on Quantum Communication, Measurement and Computing), p.361, (2012).

[12] E.B. Davies, “Information and quantum measurement,” IEEE Trans. Inform. Theory **IT-24**, pp.596-599, (1978).

[13] I.M. Isaacs, *Character theory of finite groups*, Academic Press, New York-London, (1976).