Formula for the channel matrix of 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.*

Abstract. Recently, we derived a formula for the channel matrix corresponding to narrow sense group covariant signals with respect to an arbitrary Abelian group. However, some group covariant signals are not "narrow sense" group covariant, so that a generalization of the formula is desired. In a previous study, we defined $(G, \hat{\chi})$-covariant signals, which are generalizations of narrow sense group covariant signals. We derive here a formula for the channel matrix of a $(G, \hat{\chi})$-covariant signal set when $\hat{\chi}$ is a specific map.

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

1 Introduction

In the classical-quantum channel, a coding theorem for a quantum channel has been already proved from which we can calculate a channel capacity, that is, asymptotically attained maximum mutual information in the limit of infinite codeword length [1, 2, 3]. However, the computation of mutual information for finite codeword length is rather difficult. Consequently, to evaluate the performance of a classical-quantum communication system in the real world is hard. As an example, consider the computation of a channel matrix for a classical-quantum communication in which pure-state signals are transmitted and are measured using the 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 using a universal algorithm if there are many signals (typically, more than 1000). We investigated whether an analytical solution of the channel matrix can be derived [4, 5, 6]. Recently, a general formula for narrow sense group covariant quantum signals [7] was introduced [8]. However, some important group covariant signal sets (e.g., the four states used in the BB84 quantum cryptographic protocol [9] and the set of symmetric informationally complete (SIC) states [10]) are not narrow sense group covariant. Because the formula [8] is not applicable to these signals, a further generalization of the formula is necessary. Towards this goal, we defined the $(G, \hat{\chi})$-covariant signal set, which is a generalization of the narrow sense group covariant signal set, and derived its necessary and sufficient condition [11].

In the present paper, we derive a formula for the 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 covered by the original formula.

*im121001@aichi-pu.ac.jp

†keisuke@kumamoto-u.ac.jp

‡usuda@ist.aichi-pu.ac.jp

2 $(G, \hat{\chi})$-covariant quantum signal set and their necessary and sufficient condition

In this section, we shall describe this $(G, \hat{\chi})$-covariant quantum signal set. Its definition is as follows:

Definition 1 [11]
Let $(G; \circ)$ be a finite group with a set of parameters that are used to characterize 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*

$$U_k |\psi_i\rangle = \hat{\chi}(k, i) |\psi_{k \circ i}\rangle, \ \forall i, k \in G, \tag{1}$$

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

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

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

Proposition 2 [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 $i, j \in G$,

$$\langle \psi_{k \circ i} | \psi_{k \circ j} \rangle = \hat{\chi}(k, i) \overline{\hat{\chi}(k, j)} \langle \psi_i | \psi_j \rangle, \tag{2}$$

for all $k \in G$. Here the overline denotes complex conjugation.

Proposition 2 provides the form of the Gram matrix $\Gamma_G = [\langle \psi_i | \psi_j \rangle]$. The following matrix is an example of the Gram matrix of a $(G, \hat{\chi})$-covariant signal set for four pure quantum state signals:

$$\Gamma_G = \begin{bmatrix} 1 & a & b & c \\ a & 1 & -c & -b \\ -b & -c & 1 & a \\ c & b & a & 1 \end{bmatrix}, \tag{3}$$

If $b \neq 0$ or $c \neq 0$, the above is not a Gram matrix of a narrow sense group covariant signal set. An example of

a quantum signal set with the above Gram matrix form is the four-state set of the BB84 protocol [9].

3 Main result

Now we derive the main result: the formula for 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:

$$\hat{\chi}(i^{-1}, j) = \begin{cases} 1 & i = 0 \text{ or } j = 0 \text{ or } j = i, \\ -1 & \text{otherwise.} \end{cases} \quad (4)$$

Combining Eqs.(2) and (4), we have

$$\langle \psi_i | \psi_j \rangle = \begin{cases} \langle \psi_0 | \psi_{i^{-1} \circ j} \rangle & i = 0 \text{ or } j = 0 \text{ or } j = i, \\ -\langle \psi_0 | \psi_{i^{-1} \circ j} \rangle & \text{otherwise,} \end{cases} \quad (5)$$

Therefore, this signal set is not narrow sense group covariant if there exist i and j such that $i \neq 0, j \neq 0, j \neq i$ and $\langle \psi_i | \psi_j \rangle \neq 0$.

We next present the formula for the associated channel matrix. Let

$$\hat{G} = \{\chi_0, \chi_1, \cdots, \chi_{M-1}\}, \quad (6)$$

be the multiplicative group of the set of all characters [12] of G and let Γ_G be a Gram matrix. Then we have the following propositions.

Proposition 3

$$\begin{aligned} \lambda_i &= \chi_i(0) - \sum_{j=1}^{M-1} \chi_i(j) \langle \psi_0 | \psi_j \rangle, \\ &= 1 - \sum_{j=1}^{M-1} \chi_i(j) \langle \psi_0 | \psi_j \rangle, \end{aligned} \quad (7)$$

and

$$\boldsymbol{\lambda}_i = \frac{1}{\sqrt{M}} \begin{bmatrix} \chi_i(0) \\ -\chi_i(1) \\ \vdots \\ -\chi_i(M-1) \end{bmatrix}, \quad (8)$$

are eigenvalues and corresponding eigenvectors of the Gram matrix Γ_G, respectively, where $i \in G$.

Proof

Proposition 3 directly follows by confirming $\Gamma_G \boldsymbol{\lambda}_i = \lambda_i \boldsymbol{\lambda}_i$ for all i. □

Proposition 4

The eigenvectors $\boldsymbol{\lambda}_0, \boldsymbol{\lambda}_1, \cdots, \boldsymbol{\lambda}_{M-1}$ of Proposition 3 are orthonormal.

Proof

From the first orthogonality relation for characters [12], we have $\boldsymbol{\lambda}_i \cdot \boldsymbol{\lambda}_j = \delta_{ij}$. Here, δ_{ij} is the Krönecker delta. □

Finally, we have the following theorem from Propositions 3 and 4.

Theorem 5

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

$$(\Gamma_G)_{ij}^{1/2} = \frac{1}{M} \sum_{l \in G} \chi_l(i \circ j^{-1}) \sqrt{1 - \sum_{k=1}^{M-1} \chi_l(k) \langle \psi_0 | \psi_k \rangle}, \quad (9)$$

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

$$(\Gamma_G)_{ij}^{1/2} = -\frac{1}{M} \sum_{l \in G} \chi_l(i \circ j^{-1}) \sqrt{1 - \sum_{k=1}^{M-1} \chi_l(k) \langle \psi_0 | \psi_k \rangle}. \quad (10)$$

4 Conclusion

In the present paper, we derived the formula for the channel matrix of a $(G, \hat{\chi})$-covariant quantum signal set given a specific map $\hat{\chi}$. 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, Phys. Rev. **A54**, pp.1869-1876, (1996).

[2] A.S. Holevo, IEEE Trans. Inform. Theory **44**, pp.269-272, (1998).

[3] B. Schumacher and M. Westmoreland, Phys. Rev. **A56**, pp.131-138, (1997).

[4] S. Usami, T.S. Usuda, I. Takumi, and M. Hata, IEICE Trans. Fundamentals. **E82-A**, no.10, pp.2185-2190, (1999).

[5] T.S. Usuda, S. Usami, I. Takumi, and M. Hata, Phys. Lett. **A305**, pp.125-134, (2002).

[6] M. Ota, H. Kumazawa, K. Shiromoto, and T.S. Usuda, Proc. of ISITA2010, pp.1035-1040, (2010).

[7] T.S. Usuda and I. Takumi, Quantum Communication, Computing, and Measurement 2, Plenum Press, New York, pp.37-42, (2000).

[8] T.S. Usuda and K. Shiromoto, Quantum Communication, Measurement and Computing (QCMC), AIP Conf. Proc. **1363**, American Institute of Physics, New York, pp.97-100, (2011).

[9] C.H. Bennett and G. Brassard, Proc. IEEE International Conference on Computers Systems and Signal Processing, pp.175-179, (1984).

[10] C.A. Fuchs, QCMC2010, Prize Talk, (2010).

[11] T.S. Usuda, Y. Ishikawa, and K. Shiromoto, Abstracts of Papers of QCMC2012, p.361, (2012).

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