# Simplification of the Calculation of the Channel Matrix for $4m^2$-ary QAM Coherent-state Signals

Ryusuke Miyazaki[1] * Mana Yoshida[1] † Tiancheng Wang[1] ‡ Souichi Takahira[1 2] §
Tsuyoshi Sasaki Usuda[1] ¶

[1] *Graduate School of Information Science and Technology, Aichi Prefectural University, Aichi, Japan*
[2] *Graduate School of Engineering Science, Osaka University, Osaka, Japan*

**Abstract.** The square-root measurement (SRM) is regarded as the optimum quantum measurement for symmetric signals and the quasi-optimum measurements for any quantum signals. In this paper, we demonstrate that the calculation of the channel matrix with the SRM for $4m^2$-ary QAM coherent-state signals can be simplified by using their partial symmetry.

**Keywords:** Gram matrix, Channel matrix, Non-symmetric signals

## 1 Introduction

Well-known modulation scheme such as phase-shift keying (PSK), amplitude-shift keying (ASK), and quadrature amplitude modulation (QAM) are used in quantum cryptography [1]∼[4]. Among these signals using these modulation schemes, the channel matrix formulae have been obtained for symmetric signals using the square-root measurement (SRM) [5, 6]. However, for non-symmetric signals (e.g., ASK signals, QAM signals), the channel matrix formula has not been obtained. We recently showed for the ASK and AMPM signals that the calculation of the channel matrix can be simplified by using partial symmetry of the signals [7, 8].

In this paper, we deal with practically more important signals, i.e., QAM signals. Applying an analytical approach to $4m^2$-ary QAM signals (where, $m = 1, 2, \ldots$), we show that the size of the problem is reduced by a quarter of the original problem.

## 2 Main result

We consider QAM coherent-state signals with $4m^2$ signal points as depicted in Fig. 1. Using SRM, the channel matrix for the signals can be computed using the eigenvalues and eigenvectors of their Gram matrix $\Gamma^{(4m^2)}$, which is a square matrix of order $4m^2$. Looking closely at Fig. 1, the $4m^2$-ary QAM signals are a collection of $m^2$ 4-ary PSK signals. To take advantage of this fact, consider block partitioning of the Gram matrix into $m^2$ submatrices $\Gamma^{(4)}_{k,l}$ of order four. Here, $k, l \in \{1, 2, \ldots, m^2\}$. Considering the signal location, we notice all $\Gamma^{(4)}_{k,l}$ have common eigenvectors independent of $k$ and $l$. Let $|\lambda_i\rangle$ $(i = 1, 2, 3, 4)$ be the common eigenvectors and let $\lambda_i^{(k,l)}$ be the corresponding eigenvalues. Then, we have $\Gamma^{(4)}_{k,l} = \sum_{i=1}^{4} \lambda_i^{(k,l)} |\lambda_i\rangle\langle\lambda_i|$ and

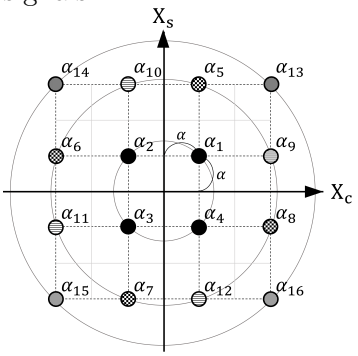


Fig. 1: $4m^2$-ary QAM coherent-state signals ($m = 2$)

$$\Gamma^{(4m^2)} = \sum_{i=1}^{4} A_i \otimes |\lambda_i\rangle\langle\lambda_i|, \tag{1}$$

where $A_i$ is $m^2 \times m^2$ matrix which consists of $\lambda_i^{(k,l)}$. We can see that $A_i$ is hermitian and has a spectral decomposition $A_i = \sum_{j=1}^{m^2} a_j^{(i)} |a_j^{(i)}\rangle\langle a_j^{(i)}|$. Therefore,

$$\Gamma^{(4m^2)} = \sum_{i=1}^{4} \sum_{j=1}^{m^2} a_j^{(i)} \, |a_j^{(i)}\rangle \, \langle a_j^{(i)}| \otimes |\lambda_i\rangle\langle\lambda_i|, \tag{2}$$

from which we can calculate the channel matrix.

## 3 Conclusion

We have clarified for $4m^2$-ary QAM coherent-state signals that the size of the problem of calculating the channel matrix reduces to $m^2$, which is a quarter of the number of elements.

**Acknowledgments:** This work has been supported in part by JSPS KAKENHI Grant Number JP20H00581, JP20K20397, and Marubun Research Promotion Foundation. T. Wang has been supported by The NEC C&C Foundation.

* im201011@cis.aichi-pu.ac.jp
† im191013@cis.aichi-pu.ac.jp
‡ id191002@cis.aichi-pu.ac.jp
§ takahira@qc.ee.es.osaka-u.ac.jp
¶ usuda@ist.aichi-pu.ac.jp

## References


[1] H. P. Yuen. KCQ: A new approach to quantum cryptography I. General principles and key generation. quant-ph/0311061v6, 2004.

[2] E. Corndorf, C. Liang, G. S. Kanter, P. Kumar, and H. P. Yuen. Quantum-noise randomized data encryption for wavelength-division-multiplexed fiber-optic networks. *Phys. Rev.* **A71**, 062326, 2005.

[3] O. Hirota, M. Sohma, M. Fuse, and K. Kato. Quantum stream cipher by Yuen 2000 protocol: Design and experiment by intensity modulation scheme. *Phys. Rev.* **A72**, 022335, 2005.

[4] K. Kato and O. Hirota. Quantum quadrature amplitude modulation system and its applicability to coherent-state quantum cryptography. In *Proc. SPIE 5893, Quantum Communications and Quantum Imaging III*, 2005.

[5] M. Ban, K. Kurokawa, R. Momose, and O. Hirota. Optimum measurements for discrimination among symmetric quantum states and parameter estimation. *Int. J. Theor. Phys.* **36***, no.6,* pages 1269–1288, 1997.

[6] 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, pages 97–100, 2011.

[7] R. Miyazaki, M. Yoshida, and T. S. Usuda. Simplification of calculation of channel matrix for $2m$-ary ASK coherent-state signals. 2019 Tokai-Section Joint Conference on Electrical, Electronics, Information, and Related Engineering, F5-4, 2019.

[8] R. Miyazaki, M. Yoshida, T. Wang, and T. S. Usuda. Simplification of the calculation of the channel matrix for AMPM coherent-state signals. In *Proc. of ISITA2020*, pages 121–125, 2020.