


Simplification of the Gram Matrix Eigenvalue Problem for Quadrature Amplitude Modulation Signals

Ryusuke Miyazaki ¹, Tiancheng Wang ^{1,2,*}  and Tsuyoshi Sasaki Usuda ^{1,*}

¹ Graduate School of Information Science and Technology, Aichi Prefectural University, Nagakute 480-1198, Aichi, Japan; im201011@cis.aichi-pu.ac.jp

² Faculty of Engineering, Kanagawa University, Yokohama 221-8686, Kanagawa, Japan

* Correspondence: wang@kanagawa-u.ac.jp (T.W.); usuda@ist.aichi-pu.ac.jp (T.S.U.)

Abstract: In quantum information science, it is very important to solve the eigenvalue problem of the Gram matrix for quantum signals. This allows various quantities to be calculated, such as the error probability, mutual information, channel capacity, and the upper and lower bounds of the reliability function. Solving the eigenvalue problem also provides a matrix representation of quantum signals, which is useful for simulating quantum systems. In the case of symmetric signals, analytic solutions to the eigenvalue problem of the Gram matrix have been obtained, and efficient computations are possible. However, for asymmetric signals, there is no analytic solution and universal numerical algorithms that must be used, rendering the computations inefficient. Recently, we have shown that, for asymmetric signals such as amplitude-shift keying coherent-state signals, the Gram matrix eigenvalue problem can be simplified by exploiting its partial symmetry. In this paper, we clarify a method for simplifying the eigenvalue problem of the Gram matrix for quadrature amplitude modulation (QAM) signals, which are extremely important for applications in quantum communication and quantum ciphers. The results presented in this paper are applicable to ordinary QAM signals as well as modified QAM signals, which enhance the security of quantum cryptography.

Keywords: quantum communication; quantum cipher; quadrature amplitude modulation (QAM); coherent state; Gram matrix; square-root measurement (SRM)



Citation: Miyazaki, R.; Wang, T.; Usuda, T.S. Simplification of Gram Matrix Eigenvalue Problem for Quadrature Amplitude Modulation Signals. *Entropy* **2022**, *24*, 544. <https://doi.org/10.3390/e24040544>

Academic Editor: Osamu Hirota

Received: 21 March 2022

Accepted: 11 April 2022

Published: 13 April 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The efficient computations and evaluations of quantities such as the error probability, mutual information, channel capacity, and reliability function are extremely important in quantum communication, quantum radar, and quantum cipher systems [1–5]. The computation of these quantities is essential not only for evaluating the reliability of quantum communication and the sensitivity of quantum radar but also for guaranteeing the security of quantum cryptography. In particular, because the security of a quantum stream cipher relies on the difference between the quantum optimum receiving capabilities of the legitimate receiver and the eavesdropper, it is essential to evaluate the optimum quantum receiver performance of the eavesdropper to guarantee security [6,7]. In quantum stream ciphers, the number of signals usually runs to several hundreds or thousands [8,9]. However, recent experiments have shown that some cases may contain millions or even billions of signals [10,11].

The eigenvalues and eigenvectors of the Gram matrix are very useful for computing various quantities that evaluate system performance. By solving the eigenvalue problem of the Gram matrix and finding its square root, the channel matrix given by the so-called square-root measurement (SRM) [12–16] can be computed. This implies that the error probability and mutual information using SRM can be directly calculated. SRM is asymptotically optimal for any quantum state signals with respect to minimizing the error probability, and

it is used in the proof of the quantum channel coding theorem [14]. Moreover, SRM is strictly optimal for symmetric pure-state signals with uniform *a priori* probabilities [12–15,17–19]. Actually, SRM is also strictly optimal for some asymmetric pure-state signals with not necessarily uniform *a priori* probabilities [20]. As each component of the square root of the Gram matrix corresponds to the inner product of a signal quantum state and a measurement state of the SRM, a matrix representation of the signal quantum state can be obtained when the signal quantum states are linearly independent [21]. This representation is known to be useful for analyzing quantum systems (e.g., [21]). Furthermore, even if the quantum state is a vector in an infinite-dimensional Hilbert space, such as a coherent state or squeezed state, the matrix form allows numerical calculations to be performed because it provides a representation in a finite-dimensional subspace (e.g., [22]). Because the Gram matrix is a matrix representation of the density operator of the quantum information source, the Holevo capacity [14] and the upper and lower bounds of the reliability function [23,24] can be directly calculated by using its eigenvalues.

In general, the Gram matrix is $M \times M$ for M -ary pure-state signals. Therefore, if we use a universal numerical algorithm to compute the eigenvalues and eigenvectors of the Gram matrix, the computation is hard when M is large. However, if the signals are symmetric, the analytic solutions of the Gram matrix eigenvalues and eigenvectors can be obtained by using well-known operations in linear algebra. In addition, by using the character [25] of a group, analytic solutions [26] can be obtained for narrow-sense group covariant signals [27], which are a generalization of symmetric signals. Narrow-sense group covariant signals are important in applications such as phase-shift keying (PSK) coherent-state signals and coded symmetric signals. Unfortunately, however, several important asymmetric signals are not narrow-sense group covariant, such as amplitude-shift keying (ASK) coherent-state signals and quadrature amplitude modulation (QAM) coherent-state signals [27]. QAM coherent-state signals are extremely important for quantum communication [28] and quantum ciphers [29]; moreover, QAM signals almost achieve the quantum channel capacity under energy constraints [30].

Recently, we showed that the eigenvalue problem of the Gram matrix can be simplified by using its partial symmetry for ASK coherent-state signals and amplitude-modulated phase-modulated (AMPM) signals, which belong to a class of asymmetric signals [31–33]. In this paper, we show that the eigenvalue problem of the Gram matrix can also be simplified by using its partial symmetry for QAM signals, which are more important for applications than ASK and AMPM signals. The method in this paper is applicable to ordinary QAM signals as well as modified QAM signals, which enhance the security of quantum stream ciphers [29]. Note that the signals considered in this paper belong to a class of asymmetric signals defined in Ref. [20], where the class is referred to as “the multiple constellations of geometrical uniform symmetry (GUS) state”. The results of this paper are closely related to Ref. [20].

The remainder of this paper is organized as follows. In Section 2, we introduce some preliminaries and basic theory. First, we define quantum signals and measurements, and then we explain various quantities such as the error probability, mutual information, and Holevo capacity. Next, we introduce the Gram matrix, SRM, and symmetric signals, which are the subject of this paper. In Section 3, we present the main results. For the eigenvalue problem of the Gram matrix of $M = 4m$ QAM signals, we show that the size of the problem can be reduced by using the partial symmetry of the signals. In Section 4, we show examples for the simplest case of $m = 2$ and provide specific forms of eigenvalues and eigenvectors for the smaller matrices than the Gram matrix. In Section 5, we provide numerical experiments as examples of applications for the main result. Finally, in Section 6, we summarize the conclusions to this study.

2. Basic Theory

2.1. Quantum Signals and Measurements

Let \mathcal{H} be the Hilbert space of a quantum system. The set of M -ary pure-state signals is represented by the following:

$$\mathcal{S} = \{|\psi_i\rangle \in \mathcal{H} \mid i = 1, 2, \dots, M\}, \tag{1}$$

where $\langle \psi_i | \psi_i \rangle = 1$. Let ξ_i be the *a priori* probability of state $|\psi_i\rangle$. Then, the pair (\mathcal{S}, ξ) is referred to as a quantum information source or a quantum ensemble.

In general, a quantum measurement is mathematically described by a positive operator-valued measure (POVM). The POVM is described as follows:

$$\Pi = \{\hat{\Pi}_j \mid j = 1, 2, \dots, M\}, \tag{2}$$

where $\hat{\Pi}$ is a Hermitian operator on \mathcal{H} satisfying the following.

$$\hat{\Pi} \geq 0, \quad \sum_{j=1}^M \hat{\Pi}_j = \hat{I}.$$

Here, \hat{I} is the identity operator on \mathcal{H} . Although POVM is a mathematical representation of a quantum measurement, it may be called a quantum measurement. The conditional probability that the result j is obtained when performing the measurement Π on quantum state $|\psi_i\rangle$ is as follows.

$$P(j|i) = \text{Tr}(|\psi_i\rangle\langle\psi_i|\hat{\Pi}_j). \tag{3}$$

2.2. Error Probability, Mutual Information, and Holevo Capacity

Suppose we measure the quantum information source (\mathcal{S}, ξ) by a POVM Π . Using Equation (3), the average error probability is defined as follows:

$$P_e = \sum_{i=1}^M \xi_i \sum_{j \neq i} P(j|i) = 1 - \sum_{i=1}^M \xi_i P(i|i), \tag{4}$$

which is also simply called the error probability. Then, the following is the case:

$$P_e^{(\text{opt})} = \min_{\Pi} P_e \tag{5}$$

and it is referred to as the minimum error probability and the set Π that attains $P_e^{(\text{opt})}$ is called the optimum POVM. The mutual information is defined as follows:

$$I(\mathcal{S}, \xi) = \sum_{i=1}^M \xi_i \sum_{j=1}^M P(j|i) \log_2 \left[\frac{P(j|i)}{\sum_{k=1}^M \xi_k P(j|k)} \right], \tag{6}$$

and its maximization with respect to quantum measurements is the following:

$$I_{\text{acc}} = \max_{\Pi} I(\mathcal{S}, \xi), \tag{7}$$

which is called accessible information. For (\mathcal{S}, ξ) , the following is the case:

$$\hat{\rho} = \sum_{i=1}^M \xi_i |\psi_i\rangle\langle\psi_i| \tag{8}$$

and it is called the density operator of the quantum information source. Using the density operator, we define von Neumann entropy as follows.

$$\chi(\xi) = -\text{Tr}(\hat{\rho} \log_2 \hat{\rho}). \quad (9)$$

When the signals are pure states, the maximization of $\chi(\xi)$ with respect to ξ is the so-called Holevo capacity.

$$C = \max_{\xi} \chi(\xi). \quad (10)$$

Let λ_j be the eigenvalues of $\hat{\rho}$ corresponding to the ξ that attains C . Then, the Holevo capacity can be calculated as follows.

$$C = -\sum_j \lambda_j \log_2 \lambda_j. \quad (11)$$

The error probability and mutual information and their optimal values are calculated using the conditional probability (3), while the Holevo capacity uses the density operator (8) of the quantum information source.

2.3. Gram Matrix

For an M -ary pure-state signal set $\mathcal{S} = \{|\psi_i\rangle \mid i = 1, 2, \dots, M\}$, the Gram matrix Γ is defined as follows.

$$\Gamma = \begin{bmatrix} \langle \psi_1 | \psi_1 \rangle & \langle \psi_1 | \psi_2 \rangle & \cdots & \langle \psi_1 | \psi_M \rangle \\ \langle \psi_2 | \psi_1 \rangle & \langle \psi_2 | \psi_2 \rangle & \cdots & \langle \psi_2 | \psi_M \rangle \\ \vdots & \vdots & \ddots & \vdots \\ \langle \psi_M | \psi_1 \rangle & \langle \psi_M | \psi_2 \rangle & \cdots & \langle \psi_M | \psi_M \rangle \end{bmatrix}. \quad (12)$$

The Gram matrix is an $M \times M$ matrix in which the (i, j) -th element is the inner product $\langle \psi_i | \psi_j \rangle$ between quantum state signals (Note that the Gram matrix is sometimes defined by using the inner products between weighted quantum state signals [20,34]). By definition, the Gram matrix is Hermitian; moreover, it is non-negative [35]. Because the norm of the quantum state vector is unity, so are all diagonal components of the Gram matrix, and the sum of the diagonal components is M . The Gram matrix is very useful in the theoretical treatment of M -ary pure-state signal systems. First, for a quantum information source $(\mathcal{S}, \{\frac{1}{M}\})$ for which its *a priori* probabilities are uniform, $\frac{1}{M}\Gamma$ is a matrix representation of its density operator. That is, $\hat{\rho}$ and $\frac{1}{M}\Gamma$ are isomorphic.

$$\hat{\rho} \cong \frac{1}{M}\Gamma. \quad (13)$$

In this case, the eigenvalues of the Gram matrix and those of the density operator are identical, and the von Neumann entropy can be calculated using the eigenvalues of the Gram matrix. For symmetric signals, the Holevo capacity can be calculated directly from the eigenvalues of the Gram matrix, because the Holevo capacity is attained with uniform *a priori* probabilities [36]. A similar statement can be made for the upper and lower bounds of the quantum reliability function [37,38]. Furthermore, the Gram matrix is closely related to the theory of SRM, as described below.

2.4. Square-Root Measurement

The SRM is a quantum measurement defined using the quantum states that are being transmitted. For a set of M -ary pure-state signals $\mathcal{S} = \{|\psi_i\rangle \mid i = 1, 2, \dots, M\}$, the POVM of the SRM $\{\hat{\Pi}_j^{(\text{SRM})} \mid j = 1, 2, \dots, M\}$ is defined as follows:

$$\hat{\Pi}_j^{(\text{SRM})} = |\mu_j\rangle\langle\mu_j|, \tag{14}$$

$$|\mu_j\rangle = \hat{\Psi}^{-\frac{1}{2}}|\psi_j\rangle, \tag{15}$$

$$\hat{\Psi} = \sum_{i=1}^M |\psi_i\rangle\langle\psi_i|, \tag{16}$$

where vector $|\mu_j\rangle$ is the measurement state or measurement quantum state (e.g., [4]). For linearly independent signal systems, the set of measurement quantum states $\{|\mu_j\rangle\}$ is an orthonormal system and is an orthonormal basis of the space spanned by signal quantum states [34]. Although SRM appeared in papers in the 1970s (e.g., Belavkin [12] and earlier papers by Holevo), the name SRM has only been used since 1996, when Hausladen et al. presented the quantum channel coding theorem [14]. They proved that the inner product between quantum states $|\psi_i\rangle$ and $|\mu_j\rangle$ in Equation (15) is equal to the (i, j) -th element of the square root of the Gram matrix, Γ , and called this the “square-root” measurement. Specifically, they showed the following.

$$\langle\psi_i|\mu_j\rangle = \left(\Gamma^{\frac{1}{2}}\right)_{ij}. \tag{17}$$

The existence of $\Gamma^{\frac{1}{2}}$ is always guaranteed because the Gram matrix is non-negative and Hermitian, as mentioned above. Therefore, Equation (17) denotes a component of the matrix representation of the signal quantum state $|\psi_i\rangle$ using the orthonormal basis $\{|\mu_j\rangle\}$. Thus, as the signal quantum state can be represented in matrix form based on the square-root of the Gram matrix, computing $\Gamma^{\frac{1}{2}}$ is very useful for simulating systems such as quantum communication, quantum radar, and quantum ciphers. From Equation (3), we have the following.

$$\begin{aligned} P(j|i) &= \text{Tr}\left(|\psi_i\rangle\langle\psi_i|\hat{\Pi}_j^{(\text{SRM})}\right) = \text{Tr}\left(|\psi_i\rangle\langle\psi_i|\mu_j\rangle\langle\mu_j|\right) \\ &= |\langle\psi_i|\mu_j\rangle|^2 = \left|\left(\Gamma^{\frac{1}{2}}\right)_{ij}\right|^2. \end{aligned} \tag{18}$$

Because the matrix in which the (i, j) -th elements are equal to $P(j|i)$ is the channel matrix and obtaining $P(j|i)$ allows the error probability and mutual information to be calculated using Equations (4) and (6). Therefore, if the square root of the Gram matrix can be computed efficiently, it is easy to compute the error probability and mutual information when SRM is applied. In general, the square root of a matrix can be computed using its eigenvalues and eigenvectors. Thus, being able to efficiently compute the eigenvalues and eigenvectors of a Gram matrix is extremely important.

2.5. Coherent-State Signals

Coherent states are the most fundamental optical quantum states used in macroscopic quantum communication or quantum ciphers. They are the stable states of light that can be realized by an ideal laser. The coherent state $|\alpha\rangle$ with the complex amplitude α is given by the following:

$$|\alpha\rangle = \exp\left(-\frac{|\alpha|^2}{2}\right) \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}}|n\rangle, \tag{19}$$

where $|n\rangle$ is the photon number state, and n is the number of photons. The inner product between two coherent states $|\alpha\rangle$ and $|\beta\rangle$ is as follows:

$$\langle\alpha|\beta\rangle = \exp\left(\alpha^*\beta - \frac{|\alpha|^2}{2} - \frac{|\beta|^2}{2}\right), \quad (20)$$

where $*$ denotes complex conjugation. If α and β are both real numbers, the value of $\langle\alpha|\beta\rangle$ is real. In this paper, we assume that the signal quantum state is a coherent state.

Note that the coherent state is completely characterized by its complex amplitude α , as shown in Equation (19). A complex number α is graphically described by a point on the complex plane, and so a coherent state signal is also described by a point on the complex plane. In this case, the complex plane is often called the phase plane.

2.6. Symmetric Signals

In the field of quantum information science, Davies defined a group covariant signal [39] with symmetry corresponding to the symmetry of the group, which is sometimes simply called a symmetric signal. Although Davies' definition of group covariant signals applies to a broader class of signals than the pure-state signals treated in this paper, we adopt the following narrow definition of group covariant signals [27], which is applicable only to simpler pure-state signals.

Definition 1 (Narrow-sense group covariant signals [27]). *Let $(G; \circ)$ be a finite group with the operation \circ . A set $\{|\psi_i\rangle | i \in G\}$ of quantum state signals is called (narrow-sense) group covariant with respect to the group $(G; \circ)$ if the following is the case:*

$$\forall i, k \in G, \exists \hat{U}_k, \hat{U}_k |\psi_i\rangle = |\psi_{k \circ i}\rangle, \quad (21)$$

where \hat{U}_k is a unitary operator.

Narrow-sense group covariant signals have the following necessary and sufficient conditions.

Proposition 1 (Necessary and sufficient conditions for narrow-sense group covariant signals [27]). *A set of quantum state signals $\{|\psi_i\rangle | i \in G\}$ is narrow-sense group covariant with respect to $(G; \circ)$ if and only if the following is the case.*

$$\forall i, j, k \in G, \langle\psi_{k \circ i} | \psi_{k \circ j}\rangle = \langle\psi_i | \psi_j\rangle. \quad (22)$$

From this proposition, we can easily show that signals such as arbitrary binary pure-state signals and arbitrary M -ary PSK coherent-state signals are narrow-sense group covariant. In addition, for narrow-sense group covariant signals, analytic solutions for the eigenvalues and eigenvectors of the Gram matrix have been presented, indicating that narrow-sense group covariant signals are very useful for communication and cipher systems. In this study, we apply this knowledge to QAM signals that are not group-covariant.

3. Eigenvalues and Eigenvectors of $M = 4m$ -ary QAM Signals and Their Gram Matrix

In this section, we consider the eigenvalues and eigenvectors of the Gram matrix corresponding to $M = 4m$ -ary QAM signals. First, $M = 4m$ -ary QAM signals are defined and the corresponding Gram matrix is explained. Next, we state that the Gram matrix can be block-partitioned and clarify that it has the structure of the sum of tensor products. Finally, we show that the scale of the computation can be reduced.

3.1. $4m$ -ary QAM Signals

This subsection describes the $4m$ -ary QAM signals treated in this paper. QAM is a major modulation scheme used in digital communication, such as for coherent optical

communication [40], and QAM signals are important for applications in quantum technologies such as quantum communication and quantum ciphers. Ordinary QAM signals are placed in a square lattice on the phase plane. As an example, Figure 1a shows the signal constellation of 256QAM on the phase plane. In quantum ciphers, modified QAM signals in which signals near the origin are removed have been proposed for higher security [29]. As an example, Figure 1b shows the signal constellation of the modified 156QAM on the phase plane. For 256QAM signals, the number of signals is $M = 4m = 256$ and $m = 64 = 8^2$, while for modified 156QAM signals, it is $M = 4m = 156$ and $m = 39$.

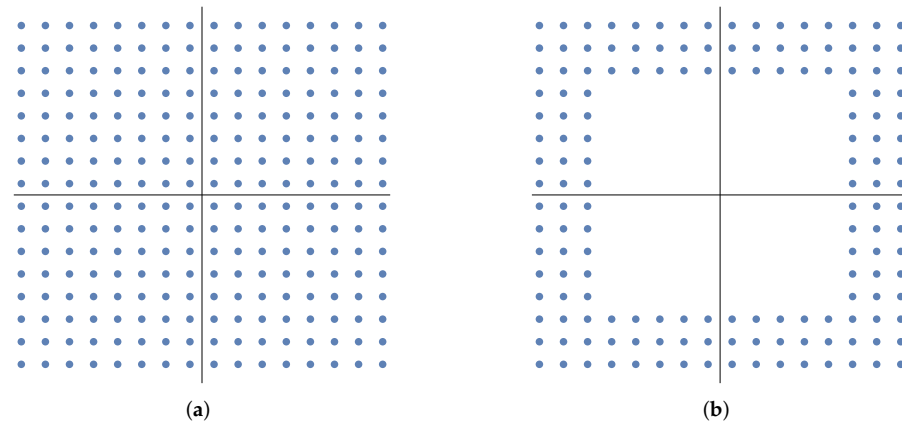


Figure 1. Examples of QAM signals presented in [29]. (a) 256QAM. (b) Modified 156QAM.

In this paper, we consider the signals defined below, which include both the ordinary QAM of Figure 1a and the modified QAM of Figure 1b, and we call them QAM signals.

Definition 2 (*4m-ary QAM Signals*). Let $\{\beta_1, \beta_2, \dots, \beta_m\}$ be any m -ary set of complex amplitudes for which its arguments lie in the range $0 < \varphi < \frac{\pi}{2}$. That is, the complex amplitudes correspond to points in the first quadrant. Here, $\beta_k \neq 0$ ($k = 1, 2, \dots, m$) and $\beta_k \neq \beta_{k'}$ ($k \neq k'$) are assumed. For each β_k , let $\alpha_k^{(1)} = \beta_k$, $\alpha_k^{(2)} = i\beta_k$, $\alpha_k^{(3)} = -\beta_k$, and $\alpha_k^{(4)} = -i\beta_k$, where $i = \sqrt{-1}$. Then, we call the following set of coherent states “4m-ary QAM coherent-state signals” (4m-ary QAM signals for short):

$$S = \bigcup_{k=1}^m S_k, \tag{23}$$

where S_k are sets of coherent states defined as follows.

$$S_k = \{|\alpha_k^{(i)}\rangle \mid i = 1, 2, 3, 4\}. \tag{24}$$

The rotation operator [4] that rotates the phase by an angle θ in the phase plane is represented as follows:

$$\hat{U}(\theta) = \exp[i\theta\hat{a}^\dagger\hat{a}], \tag{25}$$

where \hat{a} and \hat{a}^\dagger are photon annihilation and creation operators, respectively. Rewriting $\hat{U}(\theta = \frac{\pi}{2})$ as simply \hat{U} , S_k becomes the following.

$$S_k = \{|\alpha_k^{(1)}\rangle, \hat{U}|\alpha_k^{(1)}\rangle, \hat{U}^2|\alpha_k^{(1)}\rangle, \hat{U}^3|\alpha_k^{(1)}\rangle\} = \{|\beta_k\rangle, \hat{U}|\beta_k\rangle, \hat{U}^2|\beta_k\rangle, \hat{U}^3|\beta_k\rangle\}. \tag{26}$$

Here, we have the following.

$$\hat{U}^4 = \hat{U}^0 = \hat{I}. \tag{27}$$

The $4m$ -ary QAM signals defined above obviously include both ordinary QAM signals (e.g., Figure 1a) and modified QAM signals (e.g., Figure 1b). Although $4m$ -ary QAM signals are not symmetric signals, each subset S_k is symmetric, group covariant, and geometrical uniform symmetric (GUS). Moreover, we should mention that $4m$ -ary QAM signals in Definition 2 satisfy the definition of the multiple constellations of GUS state [20], which is a particularization of the concept of compound geometrical uniform (CGU) states [41]. Hence, $4m$ -ary QAM signals are practical examples of the multiple constellations of GUS state and CGU states. The following results are also applicable when considering non-coherent states $|\psi_k\rangle$, such as squeezed states, instead of $|\beta_k\rangle$ in Equation (26).

3.2. Gram Matrix of $4m$ -ary QAM Signals

As shown in Equation (23), $4m$ -ary QAM signals are partitioned into m subsets S_k ($k = 1, 2, \dots, m$). Let $\Gamma_{k,l}^{(4)}$ be the 4×4 matrix for which its entries are the inner product between two signals, where one of the two signals is chosen from the subset S_k , and the other is chosen from the subset S_l . Then, the Gram matrix of the $4m$ -ary QAM signals can be represented in block-partitioned form as follows.

$$\Gamma = \begin{bmatrix} \Gamma_{1,1}^{(4)} & \Gamma_{1,2}^{(4)} & \cdots & \Gamma_{1,m}^{(4)} \\ \Gamma_{2,1}^{(4)} & \Gamma_{2,2}^{(4)} & \cdots & \Gamma_{2,m}^{(4)} \\ \vdots & \vdots & \ddots & \vdots \\ \Gamma_{m,1}^{(4)} & \Gamma_{m,2}^{(4)} & \cdots & \Gamma_{m,m}^{(4)} \end{bmatrix}. \tag{28}$$

From Equation (26), the (i, j) -th element of $\Gamma_{k,l}^{(4)}$ is as follows.

$$(\Gamma_{k,l}^{(4)})_{i,j} = \langle \alpha_k^{(1)} | (\hat{U}^{i-1})^\dagger \hat{U}^{j-1} | \alpha_l^{(1)} \rangle = \langle \alpha_k^{(1)} | \hat{U}^{j-i} | \alpha_l^{(1)} \rangle = \langle \beta_k | \hat{U}^{j-i} | \beta_l \rangle. \tag{29}$$

This implies that $\Gamma_{k,l}^{(4)}$ is cyclic.

Denoting the components of the first row of $\Gamma_{k,l}^{(4)}$ as $a_{k,l}, b_{k,l}, c_{k,l}$ and $d_{k,l}$, the submatrix $\Gamma_{k,l}^{(4)}$ is described as follows:

$$\Gamma_{k,l}^{(4)} = \begin{bmatrix} a_{k,l} & b_{k,l} & c_{k,l} & d_{k,l} \\ d_{k,l} & a_{k,l} & b_{k,l} & c_{k,l} \\ c_{k,l} & d_{k,l} & a_{k,l} & b_{k,l} \\ b_{k,l} & c_{k,l} & d_{k,l} & a_{k,l} \end{bmatrix}, \tag{30}$$

where the following is the case.

$$\begin{aligned} a_{k,l} &= \langle \beta_k | \beta_l \rangle, \\ b_{k,l} &= \langle \beta_k | \hat{U} | \beta_l \rangle = \langle \beta_k | \mathbf{i} \beta_l \rangle, \\ c_{k,l} &= \langle \beta_k | \hat{U}^2 | \beta_l \rangle = \langle \beta_k | -\beta_l \rangle, \\ d_{k,l} &= \langle \beta_k | \hat{U}^3 | \beta_l \rangle = \langle \beta_k | -\mathbf{i} \beta_l \rangle. \end{aligned}$$

3.3. Decomposition of Submatrices

Here, we consider the common properties of each $\Gamma_{k,l}^{(4)}$ by performing a spectral decomposition of each submatrix $\Gamma_{k,l}^{(4)}$ introduced in the previous section. Because $\Gamma_{k,l}^{(4)}$

is cyclic according to Equation (30), the analytic expressions of its eigenvalues $\lambda_i^{(k,l)}$ and eigenvectors λ_i ($i = 1, 2, 3, 4$) are well known. The expressions are as follows.

$$\begin{aligned} \lambda_1^{(k,l)} &= a_{k,l} + b_{k,l} + c_{k,l} + d_{k,l}, \\ \lambda_2^{(k,l)} &= a_{k,l} - b_{k,l} + c_{k,l} - d_{k,l}, \\ \lambda_3^{(k,l)} &= a_{k,l} + \mathbf{i}b_{k,l} - c_{k,l} - \mathbf{i}d_{k,l}, \\ \lambda_4^{(k,l)} &= a_{k,l} - \mathbf{i}b_{k,l} - c_{k,l} + \mathbf{i}d_{k,l}, \end{aligned}$$

$$\lambda_1 = \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}, \lambda_2 = \frac{1}{2} \begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \end{bmatrix}, \lambda_3 = \frac{1}{2} \begin{bmatrix} 1 \\ \mathbf{i} \\ -1 \\ -\mathbf{i} \end{bmatrix}, \lambda_4 = \frac{1}{2} \begin{bmatrix} 1 \\ -\mathbf{i} \\ -1 \\ \mathbf{i} \end{bmatrix}.$$

As eigenvectors $\{\lambda_1, \lambda_2, \lambda_3, \lambda_4\}$ are orthonormal, $\Gamma_{k,l}^{(4)}$ can be spectrally decomposed as follows:

$$\Gamma_{k,l}^{(4)} = \sum_{i=1}^4 \lambda_i^{(k,l)} \lambda_i \lambda_i^H, \tag{31}$$

where λ_i^H denotes the conjugate transpose of λ_i .

3.4. Decomposition of Gram Matrix

In this subsection, we decompose the Gram matrix Γ into a sum of tensor products using the spectral decomposition of submatrices $\Gamma_{k,l}^{(4)}$. All $\Gamma_{k,l}^{(4)}$ have common eigenvectors independent of k and l . Substituting Equation (31) into Equation (28), we obtain the following:

$$\begin{aligned} \Gamma &= \begin{bmatrix} \Gamma_{1,1}^{(4)} & \Gamma_{1,2}^{(4)} & \cdots & \Gamma_{1,m}^{(4)} \\ \Gamma_{2,1}^{(4)} & \Gamma_{2,2}^{(4)} & \cdots & \Gamma_{2,m}^{(4)} \\ \vdots & \vdots & \ddots & \vdots \\ \Gamma_{m,1}^{(4)} & \Gamma_{m,2}^{(4)} & \cdots & \Gamma_{m,m}^{(4)} \end{bmatrix} \\ &= \sum_{i=1}^4 \begin{bmatrix} \lambda_i^{(1,1)} & \lambda_i^{(1,2)} & \cdots & \lambda_i^{(1,m)} \\ \lambda_i^{(2,1)} & \lambda_i^{(2,2)} & \cdots & \lambda_i^{(2,m)} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_i^{(m,1)} & \lambda_i^{(m,2)} & \cdots & \lambda_i^{(m,m)} \end{bmatrix} \otimes \lambda_i \lambda_i^H \\ &= \sum_{i=1}^4 A_i \otimes \lambda_i \lambda_i^H, \end{aligned} \tag{32}$$

where the following is the case.

$$A_i = \begin{bmatrix} \lambda_i^{(1,1)} & \lambda_i^{(1,2)} & \cdots & \lambda_i^{(1,m)} \\ \lambda_i^{(2,1)} & \lambda_i^{(2,2)} & \cdots & \lambda_i^{(2,m)} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_i^{(m,1)} & \lambda_i^{(m,2)} & \cdots & \lambda_i^{(m,m)} \end{bmatrix}. \tag{33}$$

In the following, we show that each matrix A_i consisting of the eigenvalues of $\Gamma_{k,l}^{(4)}$ is Hermitian. As Γ is the Gram matrix (and is therefore Hermitian), its submatrices satisfy the following.

$$\left(\Gamma_{k,l}^{(4)}\right)^H = \Gamma_{l,k}^{(4)}. \tag{34}$$

From Equation (31), we have the following:

$$\left(\Gamma_{k,l}^{(4)}\right)^H = \sum_{i=1}^4 \left(\lambda_i^{(k,l)}\right)^* \lambda_i \lambda_i^H \tag{35}$$

and from Equation (34), it coincides with the following.

$$\Gamma_{l,k}^{(4)} = \sum_{i=1}^4 \lambda_i^{(l,k)} \lambda_i \lambda_i^H. \tag{36}$$

Thus, we have

$$\left(\lambda_i^{(k,l)}\right)^* = \lambda_i^{(l,k)}. \tag{37}$$

Hence, all A_i of Equation (33) are Hermitian.

$$A_i^H = A_i, \quad i \in \{1, 2, 3, 4\}. \tag{38}$$

Therefore, each A_i is spectrally decomposable. Let $a_j^{(i)}$ and $a_j^{(i)}$ be the eigenvalues and corresponding orthonormalized eigenvectors of A_i . Then, the spectral decomposition form of A_i is as follows.

$$A_i = \sum_{j=1}^m a_j^{(i)} a_j^{(i)} a_j^{(i)H}. \tag{39}$$

Substituting this into Equation (32), we obtain the following.

$$\Gamma = \sum_{i=1}^4 \sum_{j=1}^m a_j^{(i)} a_j^{(i)} a_j^{(i)H} \otimes \lambda_i \lambda_i^H. \tag{40}$$

3.5. Eigenvalues and Eigenvectors of Gram Matrix

In this subsection, we derive the eigenvalues and eigenvectors from the decomposition form (40) of the Gram matrix Γ . Because both $\{a_j^{(i)}\}$ and $\{\lambda_i\}$ are orthonormal, we have the following:

$$\Gamma \left(a_j^{(i)} \otimes \lambda_i\right) = a_j^{(i)} \left(a_j^{(i)} \otimes \lambda_i\right) \quad (j = 1, \dots, m, i = 1, 2, 3, 4),$$

and the eigenvalues and eigenvectors of the Gram matrix Γ of $M = 4m$ -ary QAM signals are listed in Table 1.

Therefore, to compute the eigenvalues and eigenvectors of the $4m \times 4m$ matrix Γ , it is sufficient to consider the eigenvalue problem of the smaller matrices A_i ($i = 1, 2, 3, 4$).

3.6. Relation of the Results in the Relevant Literature

In this subsection, we consider the relation between the results in this paper and those in Ref. [20]. As examples of the multiple constellations of GUS state, the new signals were introduced [20]. They are called a double quantum binary phase shift keying (BPSK) and a double quantum pulse position modulation (PPM). As mentioned in Section 3.1, $4m$ -ary

QAM signals also belong to the class of the multiple constellations of GUS state. The signals are not new, but they are rather traditional, and they are well known to be useful. Therefore, it is worth noticing that the results in Ref. [20] are also applicable to $4m$ -ary QAM signals. The most significant result is the optimality of SRM. That is, SRM can be an optimal measurement for $4m$ -ary QAM signals with certain *a priori* probabilities. Furthermore, various results had been obtained in Ref. [20] while they had shown the optimality of SRM. They provided the block-partitioned form of the Gram matrix and showed that each submatrix is diagonalizable by the Fourier matrix. These results correspond to the results in Sections 3.2 and 3.3. Then, they considered a transformation of the matrix block-partitioned by diagonal submatrices into a block diagonal matrix. This result is closely related to the result in Section 3.4. Although they had not mentioned the eigenvalues and eigenvectors, one may connect their discussion for the square-root of the Gram matrix to the results in this section. We would like to emphasize here a reduction in computational costs, whereas they did not explicitly state a reduction.

Table 1. Eigenvalues and eigenvectors of Γ ($j = 1, \dots, m$).

| Eigenvalues | Eigenvectors |
|-------------|-------------------------------|
| $a_j^{(1)}$ | $a_j^{(1)} \otimes \lambda_1$ |
| $a_j^{(2)}$ | $a_j^{(2)} \otimes \lambda_2$ |
| $a_j^{(3)}$ | $a_j^{(3)} \otimes \lambda_3$ |
| $a_j^{(4)}$ | $a_j^{(4)} \otimes \lambda_4$ |

4. Examples for the Case of $m = 2$

Here, we consider the simplest case of $m = 2$ as examples.

4.1. Submatrices A_i

From Equation (33), each A_i consists of the eigenvalues $\lambda_i^{(k,l)}$ of $\Gamma_{(k,l)}^{(4)}$. Since $\lambda_i^{(k,l)}$ is a weighted sum of the inner products $\langle \beta_k | \beta_l \rangle, \langle \beta_k | \mathbf{i}\beta_l \rangle, \langle \beta_k | -\beta_l \rangle$, and $\langle \beta_k | -\mathbf{i}\beta_l \rangle$, it is convenient to describe the forms of the inner product for coherent states by using Equation (20):

$$\langle \alpha | \pm \beta \rangle = e^{\pm \alpha^* \beta} e^{-\frac{|\alpha|^2}{2} - \frac{|\beta|^2}{2}}, \quad \langle \alpha | \pm \mathbf{i}\beta \rangle = e^{\pm \mathbf{i}\alpha^* \beta} e^{-\frac{|\alpha|^2}{2} - \frac{|\beta|^2}{2}},$$

where we set $\alpha = \beta_k$ and $\beta = \beta_l$. Using the above forms, we have the following:

$$\begin{aligned} \lambda_1^{(k,l)} &= \langle \alpha | \beta \rangle + \langle \alpha | \mathbf{i}\beta \rangle + \langle \alpha | -\beta \rangle + \langle \alpha | -\mathbf{i}\beta \rangle \\ &= \left(e^{\alpha^* \beta} + e^{\mathbf{i}\alpha^* \beta} + e^{-\alpha^* \beta} + e^{-\mathbf{i}\alpha^* \beta} \right) e^{-\frac{|\alpha|^2}{2} - \frac{|\beta|^2}{2}} \end{aligned} \tag{41}$$

$$\begin{aligned} \lambda_2^{(k,l)} &= \langle \alpha | \beta \rangle - \langle \alpha | \mathbf{i}\beta \rangle + \langle \alpha | -\beta \rangle - \langle \alpha | -\mathbf{i}\beta \rangle \\ &= 2\{\cosh(\alpha^* \beta) + \cos(\alpha^* \beta)\} e^{-\frac{|\alpha|^2}{2} - \frac{|\beta|^2}{2}}, \end{aligned} \tag{42}$$

$$\begin{aligned} \lambda_3^{(k,l)} &= \langle \alpha | \beta \rangle + \mathbf{i}\langle \alpha | \mathbf{i}\beta \rangle - \langle \alpha | -\beta \rangle - \mathbf{i}\langle \alpha | -\mathbf{i}\beta \rangle \\ &= 2\{\sinh(\alpha^* \beta) - \sin(\alpha^* \beta)\} e^{-\frac{|\alpha|^2}{2} - \frac{|\beta|^2}{2}}, \end{aligned} \tag{43}$$

$$\begin{aligned} \lambda_4^{(k,l)} &= \langle \alpha | \beta \rangle - \mathbf{i}\langle \alpha | \mathbf{i}\beta \rangle - \langle \alpha | -\beta \rangle + \mathbf{i}\langle \alpha | -\mathbf{i}\beta \rangle \\ &= 2\{\sinh(\alpha^* \beta) + \sin(\alpha^* \beta)\} e^{-\frac{|\alpha|^2}{2} - \frac{|\beta|^2}{2}}, \end{aligned} \tag{44}$$

where we write the following.

$$\frac{e^x + e^{-x}}{2} = \cosh(x), \quad \frac{e^{ix} + e^{-ix}}{2} = \cos(x),$$

$$\frac{e^x - e^{-x}}{2} = \sinh(x), \quad \frac{e^{ix} - e^{-ix}}{2i} = \sin(x).$$

From Equations (41)–(44), we obtain for the case of $m = 2$:

$$A_1 = \begin{bmatrix} \cosh(|\beta_1|^2) + \cos(|\beta_1|^2) & \cosh(\beta_1^*\beta_2) + \cos(\beta_1^*\beta_2) \\ \cosh(\beta_2^*\beta_1) + \cos(\beta_2^*\beta_1) & \cosh(|\beta_2|^2) + \cos(|\beta_2|^2) \end{bmatrix} \circ (2X), \quad (45)$$

$$A_2 = \begin{bmatrix} \cosh(|\beta_1|^2) - \cos(|\beta_1|^2) & \cosh(\beta_1^*\beta_2) - \cos(\beta_1^*\beta_2) \\ \cosh(\beta_2^*\beta_1) - \cos(\beta_2^*\beta_1) & \cosh(|\beta_2|^2) - \cos(|\beta_2|^2) \end{bmatrix} \circ (2X), \quad (46)$$

$$A_3 = \begin{bmatrix} \sinh(|\beta_1|^2) - \sin(|\beta_1|^2) & \sinh(\beta_1^*\beta_2) - \sin(\beta_1^*\beta_2) \\ \sinh(\beta_2^*\beta_1) - \sin(\beta_2^*\beta_1) & \sinh(|\beta_2|^2) - \sin(|\beta_2|^2) \end{bmatrix} \circ (2X), \quad (47)$$

$$A_4 = \begin{bmatrix} \sinh(|\beta_1|^2) + \sin(|\beta_1|^2) & \sinh(\beta_1^*\beta_2) + \sin(\beta_1^*\beta_2) \\ \sinh(\beta_2^*\beta_1) + \sin(\beta_2^*\beta_1) & \sinh(|\beta_2|^2) + \sin(|\beta_2|^2) \end{bmatrix} \circ (2X), \quad (48)$$

where \circ denotes the Hadamard product, and the following is the case.

$$X = \begin{bmatrix} e^{-|\beta_1|^2} & e^{-\frac{|\beta_1|^2}{2} - \frac{|\beta_2|^2}{2}} \\ e^{-\frac{|\beta_1|^2}{2} - \frac{|\beta_2|^2}{2}} & e^{-|\beta_2|^2} \end{bmatrix}. \quad (49)$$

The remaining task is to calculate the eigenvalues and eigenvectors of the 2×2 matrices $A_1 \sim A_4$. Although it is possible to calculate eigenvalues and eigenvectors of a 2×2 matrix, the general form may be slightly complicated. In the following, we consider simple two cases.

4.2. Case of $|\beta_1| = |\beta_2| = \gamma$

This case corresponds to phase-mismatching PSK signals. The signals are similar to the double quantum BPSK with a misalignment or a systematic bias error in the angle defining one of the two constellations [20]. Note that the number of signals is different. In this case, from the following:

$$X = \begin{bmatrix} e^{-\gamma^2} & e^{-\gamma^2} \\ e^{-\gamma^2} & e^{-\gamma^2} \end{bmatrix},$$

“ $\circ(2X)$ ” in Equations (45)–(48) becomes simply a scalar product “ $\times(2e^{-\gamma^2})$ ”. Therefore, each A_i has the following form:

$$\begin{bmatrix} a & b \\ b^* & a \end{bmatrix},$$

where a is a real number and b is a complex number. The eigenvalues and the corresponding orthonormal eigenvectors of the above form are the following:

$$a \pm |b|, \quad \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ \pm e^{-i\mu} \end{bmatrix}, \quad (50)$$

where $\mu = \arg(b)$. Therefore, the eigenvalues of A_i are as follows:

$$a_1^{(1)} = 2e^{-\gamma^2} \left\{ \cosh(\gamma^2) + \cos(\gamma^2) + |\cosh(\delta) + \cos(\delta)| \right\}, \tag{51}$$

$$a_2^{(1)} = 2e^{-\gamma^2} \left\{ \cosh(\gamma^2) + \cos(\gamma^2) - |\cosh(\delta) + \cos(\delta)| \right\}, \tag{52}$$

$$a_1^{(2)} = 2e^{-\gamma^2} \left\{ \cosh(\gamma^2) - \cos(\gamma^2) + |\cosh(\delta) - \cos(\delta)| \right\}, \tag{53}$$

$$a_2^{(2)} = 2e^{-\gamma^2} \left\{ \cosh(\gamma^2) - \cos(\gamma^2) - |\cosh(\delta) - \cos(\delta)| \right\}, \tag{54}$$

$$a_1^{(3)} = 2e^{-\gamma^2} \left\{ \sinh(\gamma^2) - \sin(\gamma^2) + |\sinh(\delta) - \sin(\delta)| \right\}, \tag{55}$$

$$a_2^{(3)} = 2e^{-\gamma^2} \left\{ \sinh(\gamma^2) - \sin(\gamma^2) - |\sinh(\delta) - \sin(\delta)| \right\}, \tag{56}$$

$$a_1^{(4)} = 2e^{-\gamma^2} \left\{ \sinh(\gamma^2) + \sin(\gamma^2) + |\sinh(\delta) + \sin(\delta)| \right\}, \tag{57}$$

$$a_2^{(4)} = 2e^{-\gamma^2} \left\{ \sinh(\gamma^2) + \sin(\gamma^2) - |\sinh(\delta) + \sin(\delta)| \right\}, \tag{58}$$

where we set $\beta_1 = \gamma e^{v_1}, \beta_2 = \gamma e^{v_2}, \beta_1^* \beta_2 = \gamma^2 e^{i(v_2 - v_1)} = \delta$.

The eigenvectors of A_i are as follows:

$$\mathbf{a}_1^{(i)} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ e^{-i\mu_i} \end{bmatrix}, \quad \mathbf{a}_2^{(i)} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -e^{-i\mu_i} \end{bmatrix}, \quad (i = 1, 2, 3, 4) \tag{59}$$

where the following is the case.

$$\begin{aligned} \mu_1 &= \arg(\cosh(\delta) + \cos(\delta)), & \mu_2 &= \arg(\cosh(\delta) - \cos(\delta)), \\ \mu_3 &= \arg(\sinh(\delta) - \sin(\delta)), & \mu_4 &= \arg(\sinh(\delta) + \sin(\delta)). \end{aligned}$$

4.3. Case of $\arg(\beta_1) = \arg(\beta_2) = v$

The signals in this case are similar to the four-pulse amplitude modulation (PAM) [20]. Note that the number of signals is eight in this case, but four for the 4-PAM. In this case, the form of A_i is as follows:

$$\begin{bmatrix} a & b \\ b & c \end{bmatrix}, \tag{60}$$

where a, b , and c are real numbers. The eigenvalues of the matrix with this form are as follows:

$$\frac{1}{2} \left(a + c \pm \sqrt{(a - c)^2 + 4b^2} \right), \tag{61}$$

and the corresponding orthogonal eigenvectors are the following.

$$\begin{bmatrix} a - c \pm \sqrt{(a - c)^2 + 4b^2} \\ 2b \end{bmatrix}. \tag{62}$$

We obtain the orthonormal eigenvectors by normalizing them. Using the above equations, we can obtain the explicit forms of $\mathbf{a}_1^{(1)} \sim \mathbf{a}_2^{(4)}$ and $\mathbf{a}_1^{(1)} \sim \mathbf{a}_2^{(4)}$ as the same manner in Section 4.2.

5. Numerical Experiments

Here, we provide numerical experiments as examples of application for the results in Section 3. We consider 16QAM signals (the case of $m = 4$) in this section. Set $\beta_1 = (1 + i)\alpha$,

$\beta_2 = (3 + \mathbf{i})\alpha, \beta_3 = (3 + 3\mathbf{i})\alpha, \beta_4 = (1 + 3\mathbf{i})\alpha$. The average number of photons of 16QAM coherent-state signals is as follows:

$$\frac{1}{4} \left(|(1 + \mathbf{i})\alpha|^2 + |(3 + \mathbf{i})\alpha|^2 + |(3 + 3\mathbf{i})\alpha|^2 + |(1 + 3\mathbf{i})\alpha|^2 \right) = 10|\alpha|^2,$$

and it is proportional to $|\alpha|^2$. Hence, in the following, we show numerical results of some quantities with respect to $|\alpha|^2$.

5.1. Von Neumann Entropy

First, we consider the von Neumann entropy, which is calculated by using eigenvalues of the Gram matrix. Since the Holevo capacity is the maximization of the von Neumann entropy with respect to *a priori* probabilities, the von Neumann entropy is a lower bound on the capacity. Let $\hat{\rho}$ be the density operator of 16QAM signals. Then, the von Neumann entropy (9) is calculated by the eigenvalues of $\hat{\rho}$ as follows.

$$\chi = - \sum_{j=1}^{16} \lambda_j \log_2 \lambda_j.$$

Each λ_j is equal to an eigenvalue of $\frac{1}{16}\Gamma$ from Equation (13). According to the results in Section 3, the following is the case:

$$\begin{aligned} \chi &= - \sum_{i=1}^4 \sum_{j=1}^4 \left(\frac{1}{16} a_j^{(i)} \right) \log_2 \left(\frac{1}{16} a_j^{(i)} \right) = - \frac{1}{16} \sum_{i=1}^4 \sum_{j=1}^4 a_j^{(i)} \left(\log_2 a_j^{(i)} - \log_2 16 \right) \\ &= 4 - \frac{1}{16} \sum_{i=1}^4 \sum_{j=1}^4 a_j^{(i)} \log_2 a_j^{(i)}, \end{aligned}$$

where $a_j^{(i)}$ are eigenvalues of the matrices A_i described in Section 3, and we numerically calculate $a_j^{(i)}$. Note that we only need numerical calculation of eigenvalues for smaller matrices A_i than the original Gram matrix Γ .

Figure 2 shows the von Neumann entropy of 16QAM signals with respect to $|\alpha|^2$. The blue line is drawn by using the results in Section 3, while the red dots are plotted by using direct calculation of eigenvalues for the Gram matrix. From Figure 2, we can confirm that both results are identical.

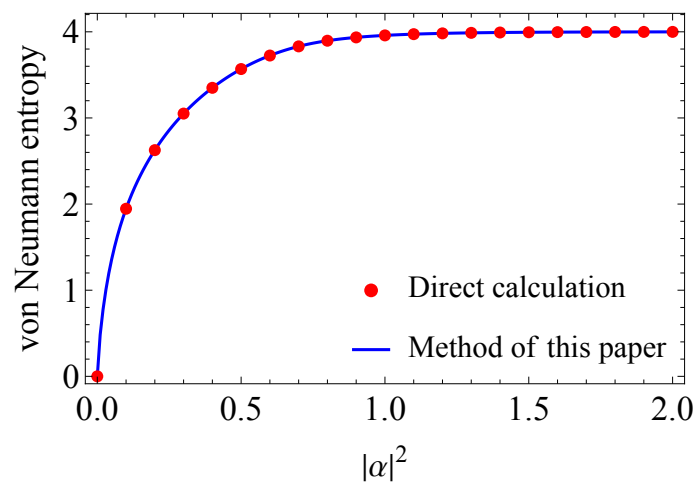


Figure 2. von Neumann entropy of 16QAM signals with respect to $|\alpha|^2$. The blue line is drawn by using the results in Section 3, while the red dots are plotted by using direct calculation of eigenvalues for the Gram matrix.

5.2. Error Probability

Now, we consider the error probability by using the SRM. To compute the error probability, both eigenvalues and eigenvectors of the Gram matrix are needed. As explained in Section 2, the error probability is as follows.

$$P_e = 1 - \frac{1}{16} \sum_{i=1}^{16} P(i|i) = 1 - \frac{1}{16} \sum_{i=1}^{16} \left| \left(\Gamma^{\frac{1}{2}} \right)_{i,i} \right|^2.$$

From Equation (40), we have the following.

$$\Gamma^{\frac{1}{2}} = \sum_{i=1}^4 \sum_{j=1}^4 \sqrt{a_j^{(i)} a_j^{(i)}} a_j^{(i)H} \otimes \lambda_i \lambda_i^H.$$

Then, numerically calculating the eigenvalues $a_j^{(i)}$ and the eigenvectors $a_j^{(i)}$ for matrices A_i , and substituting them into the above equation, we obtain the error probability.

Figure 3 shows the error probability of 16QAM signals with respect to $|\alpha|^2$. The blue line and the red dots have the same meaning as in Figure 2. From Figure 3, we can confirm that both results are identical.

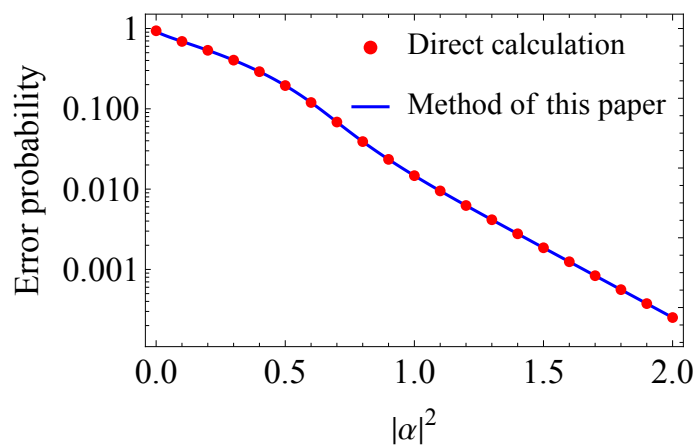


Figure 3. Error probability of 16QAM signals with respect to $|\alpha|^2$. The blue line is drawn by using the results in Section 3, while the red dots are plotted by using direct calculation of the matrix square-root for the Gram matrix.

6. Conclusions

In this paper, we have described the simplification of the Gram matrix eigenvalue problem for QAM coherent-state signals and shown that the scale of the computation can be reduced. As explained in Section 2, by solving the eigenvalue problem of the Gram matrix, it is possible to calculate quantities such as the error probability, mutual information, Holevo capacity, and the upper and lower bounds of the reliability function, which are important for evaluating the performance of quantum communication, quantum radar, and the security of quantum cryptography. The QAM signals treated in this study are very versatile, being applicable not only to ordinary QAM signals but also to any signals generated by rotation in the first quadrant of the phase plane. The quantum state used is typically but not necessarily the coherent state. In fact, the QAM signals defined in this paper belong to the class of the multiple constellations of GUS [20] and CGU states [41]. Therefore, the results in the literature are also applicable to QAM signals. Moreover, some results in Ref. [20] are closely related to the results in this paper, as explained in Section 3.6.

The most significant challenge for the future is the further simplification of the eigenvalue problem of the Gram matrix. For this purpose, the regularity of the signal constellation in the first quadrant of the phase plane should be taken into account. Therefore, carefully determining the order of signals in the first quadrant is important, even if they are

the same signals. Another challenge is to apply the methods of this study to actual problems, whereas we have shown simple examples for 16QAM. For this purpose, the combined use of numerical algorithms (e.g., [42]) for the matrix calculations should be considered.

Author Contributions: Conceptualization, T.S.U.; methodology, R.M.; validation, T.W.; formal analysis, R.M.; investigation, R.M.; writing—original draft preparation, R.M.; writing—review and editing, T.W. and T.S.U.; supervision, T.S.U.; project administration, T.S.U.; funding acquisition T.W. and T.S.U. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by JSPS KAKENHI (grant number JP20K20397, JP20H00581, and JP21K04064) and research grants from the Marubun Research Promotion Foundation and the Nitto Foundation.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors would like to thank S. Takahira and M. Yoshida for valuable discussions during this and previous research studies. We thank Stuart Jenkinson, PhD, from Edanz (<https://jp.edanz.com/ac>, accessed on 12 April 2022) for editing a draft of this manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

| | |
|------|--------------------------------------|
| SRM | Square-root measurement; |
| PSK | Phase shift keying; |
| ASK | Amplitude shift keying; |
| QAM | Quadrature amplitude modulation; |
| AMPM | Amplitude-modulated phase-modulated; |
| POVM | Positive operator-valued measure. |

References

- Helstrom, C.W. Detection theory and quantum mechanics. *Inform. Control* **1967**, *10*, 254–291. [[CrossRef](#)]
- Holevo, A.S. Statistical decision theory for quantum systems. *J. Multivar. Anal.* **1973**, *3*, 337–394. [[CrossRef](#)]
- Yuen, H.P.; Kennedy, R.S.; Lax, M. Optimum testing of multiple hypotheses in quantum detection theory. *IEEE Trans. Inform. Theory* **1975**, *21*, 125–134. [[CrossRef](#)]
- Helstrom, C.W. *Quantum Detection and Estimation Theory*; Academic Press: New York, NY, USA, 1976.
- Hirota, O.; Ikehara, S. Minimax strategy in the quantum detection theory and its application to optical communication. *Trans. IECE* **1982**, *65*, 627–633.
- Yuen, H.P. KCQ: A new approach to quantum cryptography I. General principles and key generation. *arXiv* **2004**, arXiv:quant-ph/0311061.
- Yuen, H.P. Key generation: Foundations and a new quantum approach. *IEEE J. Sel. Top. Quantum Electron.* **2009**, *15*, 1630–1645. [[CrossRef](#)]
- Corndorf, E.; Liang, C.; Kanter, G.S.; Kumar, P.; Yuen, H.P. Quantum-noise randomized data encryption for wavelength-division-multiplexed fiber-optic networks. *Phys. Rev. A* **2005**, *71*, 062326. [[CrossRef](#)]
- Hirota, O.; Sohma, M.; Fuse, M.; Kato, K. Quantum stream cipher by Yuen 2000 protocol: Design and experiment by intensity modulation scheme. *Phys. Rev. A* **2005**, *72*, 022335. [[CrossRef](#)]
- Tanizawa, K.; Futami, F. Digital coherent PSK Y-00 quantum stream cipher with 2^{17} randomized phase levels. *Opt. Express* **2019**, *27*, 1071–1079. [[CrossRef](#)]
- Chen, X.; Tanizawa, K.; Winzer, P.; Dong, P.; Cho, J.; Futami, F.; Kato, K.; Melikyan, A.; Kim, K.W. Experimental demonstration of 4,294,967,296-QAM based Y-00 quantum stream cipher template carrying 160-Gb/s 16-QAM signals. *Opt. Express* **2021**, *29*, 5658–5664. [[CrossRef](#)]
- Belavkin, V.P. Optimal multiple quantum statistical hypothesis testing. *Stochastics* **1975**, *1*, 315–345. [[CrossRef](#)]
- Belavkin, V.P. Optimal distinction of non-orthogonal quantum signals. *Radio Eng. Electron. Phys.* **1975**, *20*, 39–47.
- Hausladen, P.; Jozsa, R.; Schumacher, B.; Westmoreland, M.; Wootters, W.K. Classical information capacity of a quantum channel. *Phys. Rev. A* **1996**, *54*, 1869–1876. [[CrossRef](#)] [[PubMed](#)]

15. Eldar, Y.C.; Forney, G.D., Jr. On quantum detection and the square-root measurement. *IEEE Trans. Inform. Theory* **2001**, *47*, 858–872. [[CrossRef](#)]
16. Kato, K.; Hirota, O. Square-root measurement for quantum symmetric mixed state signals. *IEEE Trans. Inform. Theory* **2003**, *49*, 3312–3317. [[CrossRef](#)]
17. Ban, M.; Kurokawa, K.; Momose, R.; Hirota, O. Optimum measurements for discrimination among symmetric quantum states and parameter estimation. *Int. J. Theor. Phys.* **1997**, *36*, 1269–1288. [[CrossRef](#)]
18. Usuda, T.S.; Takumi, I.; Hata, M.; Hirota, O. Minimum error detection of classical linear code sending through a quantum channel. *Phys. Lett. A* **1999**, *256*, 104–108. [[CrossRef](#)]
19. Usuda, T.S.; Usami, S.; Takumi, I.; Hata, M. Superadditivity in capacity of quantum channel for q -ary linearly dependent real symmetric-state signals. *Phys. Lett. A* **2002**, *305*, 125–134. [[CrossRef](#)]
20. Dalla Pozza, N.; Pierobon, G. Optimality of square-root measurements in quantum state discrimination. *Phys. Rev. A* **2015**, *91*, 042334. [[CrossRef](#)]
21. Osaki, M.; Usuda, T.S.; Hirota, O. Group covariant detection for a three-phase shift keyed signal. *Phys. Lett. A* **1998**, *245*, 189–196. [[CrossRef](#)]
22. Takeuchi, H.; Yamaguchi, S.; Usuda, T.S. Entanglement-assisted classical communication using quasi Bell states. In Proceedings of the 1st International Workshop on Entangled Coherent State and Its Application to Quantum Information Science—Towards Macroscopic Quantum Communications, Tokyo, Japan, 26–28 November 2012; pp. 115–119.
23. Burnashev, M.V.; Holevo, A.S. On reliability function of quantum communication channel. *Probl. Peredachi Inform.* **1998**, *34*, 1–13.
24. Dalai, M. Lower bounds on the probability of error for classical and classical-quantum channels. *IEEE Trans. Inform. Theory* **2013**, *59*, 8027–8056. [[CrossRef](#)]
25. Isaacs, I.M. *Character Theory of Finite Groups*; Academic Press: New York, NY, USA; London, UK, 1976.
26. Usuda, T.S.; Shiromoto, K. Analytical expression of s -th power of Gram matrix for group covariant signals and its application. In *Quantum Communication, Measurement and Computing (QCMC), AIP Conference Proceedings*; American Institute of Physics: New York, NY, USA, 2011; Volume 1363, pp. 97–100.
27. Usuda, T.S.; Takumi, I. Group covariant signals in quantum information theory. In *Quantum Communication, Computing, and Measurement 2*; Plenum Press: New York, NY, USA, 2000; pp. 37–42.
28. Kato, K.; Osaki, M.; Sasaki, M.; Hirota, O. Quantum detection and mutual information for QAM and PSK signals. *IEEE Trans. Commun.* **1999**, *47*, 248–254. [[CrossRef](#)]
29. Kato, K.; Hirota, O. Quantum quadrature amplitude modulation system and its applicability to coherent-state quantum cryptography. In Proceedings of the SPIE, Quantum Communications and Quantum Imaging III, San Diego, CA, USA, 31 July 2005; Volume 5893.
30. Ishida, Y.; Kato, K.; Usuda, T.S. Capacity of attenuated channel with discrete-valued input. In Proceedings of the 8th International Conference on Quantum Communication, Measurement and Computing, Tsukuba, Japan, 28 November–3 December 2006; NICT Press: Tokyo, Japan, 2007; pp. 323–326.
31. Miyazaki, R.; Yoshida, M.; Usuda, T.S. Simplification of calculation of channel matrix for $2m$ -ary ASK coherent-state signals. In Proceedings of the 2019 Tokai-Section Joint Conference on Electrical, Electronics, Information, and Related Engineering, Nagoya, Japan, 9–10 September 2019; No. F5-4. (In Japanese)
32. Miyazaki, R.; Yoshida, M.; Wang, T.; Usuda, T.S. Simplification of the calculation of the channel matrix for AMPM coherent-state signals. In Proceedings of the 2020 International Symposium on Information Theory and Its Applications (ISITA2020), Hawai'i, HI, USA, 24–27 October 2020; pp. 121–125.
33. Miyazaki, R.; Yoshida, M.; Wang, T.; Takahira, S.; Usuda, T.S. Simplification of calculation of channel matrix for non-symmetric signals. *IEICE Trans. Commun.* **2022**, *J105-B*, 74–87. (In Japanese)
34. Sasaki, M.; Kato, K.; Izutsu, M.; Hirota, O. Quantum channels showing superadditivity in classical capacity. *Phys. Rev. A* **1998**, *58*, 146–158. [[CrossRef](#)]
35. Horn, R.A.; Jonson, C.R. *Matrix Analysis*; Cambridge University Press: Cambridge, UK, 1985.
36. Kato, K.; Osaki, M.; Hirota, O. Derivation of classical capacity of quantum channel for discrete information source. *Phys. Lett. A* **1999**, *251*, 157–163. [[CrossRef](#)]
37. Kato, K. Error exponents of quantum communication system with M -ary PSK coherent state signal. *Tamagawa Univ. Quantum ICT Res. Inst. Bull.* **2011**, *1*, 33–40.
38. Kato, K. A note on the reliability function for M -ary PSK coherent state signal. *Tamagawa Univ. Quantum ICT Res. Inst. Bull.* **2018**, *8*, 21–25.
39. Davies, E.B. Information and quantum measurement. *IEEE Trans. Inform. Theory* **1978**, *IT-24*, 596–599. [[CrossRef](#)]
40. Kikuchi, K. Digital coherent optical communication systems: Digital coherent optical communication systems. *IEICE Electron. Express* **2011**, *8*, 1642–1662. [[CrossRef](#)]
41. Eldar, Y.C.; Megretski, A.; Verghese, G. Optimal detection of symmetric mixed quantum states. *IEEE Trans. Inform. Theory* **2004**, *50*, 1198–1207. [[CrossRef](#)]
42. Mizuno, S.; Moriiizumi, Y.; Usuda, T.S.; Sogabe, T. An initial guess of Newton's method for the matrix square root based on a sphere constrained optimization problem. *SIAM Lett.* **2016**, *8*, 17–20. [[CrossRef](#)]