



# Article Non-Orthogonality Measure for a Collection of Pure Quantum States

Kentaro Kato 🕩

Quantum ICT Research Institute, Tamagawa University, 6-1-1 Tamagawagakuen, Machida 194-8610, Tokyo, Japan; kkatop@lab.tamagawa.ac.jp

**Abstract:** Modern optical communication technology can realize a large-scale multilevel (or *M*-ary) optical signal. Investigating the quantum mechanical nature of such a large-scale *M*-ary optical signal is essential for a unified understanding of quantum information science and optical communication technology. This article focuses on the quantum-mechanical non-orthogonality for a collection of pure quantum states and proposes a non-orthogonality index based on the least squares error criterion in quantum detection theory. First, we define the index for linearly independent signals, and the proposed index is analyzed through numerical simulations. Next, the index is applied to a highly large-scale *M*-ary phase-shift keying (PSK) coherent state signal. Furthermore, the index is compared with the capacity of the pure state channel with the PSK signal. As a result, it is shown that a highly large-scale *M*-ary PSK coherent state signal exhibits a quantum nature even when the signal transmission power is very high. Thus, the theoretical characterization of a highly large-scale *M*-ary coherent state signal based on the proposed index will be the first step toward a better understanding of cutting-edge optical communication technologies such as the quantum stream cipher Y00.

**Keywords:** quantum communications; quantum cryptography; quantum states; non-orthogonality; least squares error; *M*-ary optical signal



Citation: Kato, K. Non-Orthogonality Measure for a Collection of Pure Quantum States. *Entropy* **2022**, *24*, 581. https://doi.org/ 10.3390/e24050581

Academic Editor: Giuseppe Vallone

Received: 3 March 2022 Accepted: 15 April 2022 Published: 21 April 2022

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



**Copyright:** © 2022 by the author. 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

In 1967–1968, Helstrom achieved a breakthrough in optical communication theory by providing a new framework with a complete quantum mechanical description of optical signals and receivers [1–3]. In addition, he successfully demonstrated the quantum limit of detection error for binary optical signals based on the Bayes and Neyman–Pearson criteria developed in the classical detection theory (e.g., [4,5]). After Helstrom's work, Yuen et al. investigated the conditions for the optimal quantum detection of general quantum states based on a linear programming method [6,7]. Furthermore, Holevo investigated the existence problem for optimal quantum detection and demonstrated the necessary and sufficient conditions for the optimal quantum detection of general quantum states [8]. These pioneering scientists opened up the field of quantum detection theory. Quantum detection theory has since been extensively developed and is a key theory for unifying quantum information science and optical communication technology.

In quantum detection theory, optical signals are mathematically expressed as quantum states of light. For pure states, error-free quantum detection is only allowed when the states are orthogonal to each other. This is a significant result of quantum detection theory. A similar result is observed from the no-cloning theorem [9–11]. The no-cloning theorem claims that perfect cloning is possible within a collection of quantum states if and only if the quantum states are orthogonal.

Recent development in experimental studies on the quantum stream cipher Y00 demonstrates that highly large-scale multilevel (or *M*-ary [12–14]) optical signals can be realized using advanced technologies in optical communications [15,16]. Therefore, the theoretical characterization of a large-scale collection of coherent states is essential for a unified understanding of quantum information science and optical communication technology.

Coherent states are non-orthogonal, and a collection of coherent states forms a linearly independent set. Hence, the case of linearly independent pure states is of particular interest. A collection of pure states can be almost orthogonal, moderately non-orthogonal, or almost identical states. Therefore, a quantitative measure of the degree of non-orthogonality of each collection is needed for a detailed analysis. In the case of binary pure states, the degree of non-orthogonality is usually measured through the modulus of the inner product between the two states. However, no method to quantify the degree of non-orthogonality of a collection of more than three quantum states has been developed. Therefore, this study aims to develop a quantitative measure for the non-orthogonality of a collection of many states.

For this aim, we propose an index to evaluate the non-orthogonality of a collection of linearly independent pure states based on the least squares error (LSE) criterion in quantum detection theory. We summarize the LSE criterion in Section 2 and define a non-orthogonality index in Section 3. The proposed index is analyzed through numerical simulations with randomly generated vectors in Section 4. Then, the index is applied to the *M*-ary phase-shift keying (PSK) coherent state signal in Section 5. Further, the capacity of a pure state channel with the PSK signal is analyzed to understand the operational meaning of the index in the same section. Finally, we give conclusions in Section 6.

#### 2. LSE Criterion in Quantum Detection Theory

Let  $S = \{ |\psi_m\rangle : 1 \le m \le M \}$  be a collection of M linearly independent pure quantum states, where each state is normalized,  $\|\psi_m\| = 1$ . Then, the squared error  $E(S, \beta)$  for S by adapting an orthonormal basis  $\beta = \{ |v_m\rangle : 1 \le m \le M \}$  in vector space  $\mathcal{V}$  spanned by S as a measurement basis is defined as follows.

$$E(S,\beta) = \frac{1}{M} \sum_{m=1}^{M} \langle e_m | e_m \rangle, \tag{1}$$

where  $|e_m\rangle = |\psi_m\rangle - |v_m\rangle$ . This expression can be arranged into the following form:

$$E(S,\beta) = \frac{1}{M} \sum_{m=1}^{M} \|e_m\|^2 = \frac{1}{M} \sum_{m=1}^{M} \|\psi_m - v_m\|^2.$$
<sup>(2)</sup>

Then, the least squares error (LSE) is defined as

$$E^{\circ}(S) = \min_{\beta} E(S, \beta) = E(S, \beta^{\circ}).$$
(3)

A constructive manner can find the optimal basis  $\beta^{\circ}$  from past studies as follows.

**Theorem 1** ([17,18]). For  $S = \{|\psi_m\rangle : 1 \le m \le M\}$  of linearly independent pure quantum states, the optimal basis  $\beta^\circ = \{|v_m^\circ\rangle : 1 \le m \le M\}$  for the LSE is given by

$$|v_m^{\circ}\rangle = \hat{G}^{-1/2}|\psi_m\rangle, \quad \text{with} \quad \hat{G} = \sum_{m=1}^M |\psi_m\rangle\langle\psi_m|.$$
 (4)

*This basis*  $\beta^{\circ}$  *is known as the square-root measurement* [19–22]. *Then, the LSE can be written as* 

$$E^{\circ}(S) = E(S, \beta^{\circ}) = \frac{1}{M} \sum_{m=1}^{M} \left(1 - \sqrt{\lambda_m}\right)^2,$$
(5)

where  $\lambda_m$  is the eigenvalue of the Gram matrix

$$\mathbf{G} = \begin{bmatrix} \langle \psi_1 | \psi_1 \rangle & \langle \psi_1 | \psi_2 \rangle & \cdots & \langle \psi_1 | \psi_M \rangle \\ \langle \psi_2 | \psi_1 \rangle & \langle \psi_2 | \psi_2 \rangle & \cdots & \langle \psi_2 | \psi_M \rangle \\ \vdots & \vdots & \ddots & \vdots \\ \langle \psi_M | \psi_1 \rangle & \langle \psi_M | \psi_2 \rangle & \cdots & \langle \psi_M | \psi_M \rangle \end{bmatrix}.$$
(6)

# 3. Non-Orthogonality Measure Based on LSE

# 3.1. Maximum and Minimum of LSE

Suppose that *S* consists of orthonormal vectors. Hence, **G** of *S* is the identity matrix of size *M*. Moreover, the optimal basis  $\beta^{\circ}$  is identical to *S*. Therefore,  $E^{\circ}(S) = 0$ . From definition (1),  $E(S,\beta) \ge 0$ . Thus, the minimum value of  $E^{\circ}(S)$  is zero.

 $E^{\circ}(S)$  is the solution to the minimization problem of  $E(S,\beta)$  with respect to  $\beta$  for given S. However, the maximum of  $E^{\circ}(S)$  for S has not been discussed. As mentioned above, the minimum value is attained when S consists of orthogonal vectors. Hence, we suppose that the other extreme case, where S consists of almost identical vectors, will provide the maximum value. Therefore, we assume that each vector in S is close to the barycenter |barycenter⟩ for  $\beta^{\circ}$ . That is,

$$|\psi_m
angle \sim | ext{barycenter}
angle = rac{1}{\sqrt{M}}\sum_{\ell=1}^M |v_\ell^\circ
angle,$$

and, hence,  $|e_m\rangle \sim |\text{barycenter}\rangle - |v_m^{\circ}\rangle$ . This implies

$$E^{\circ}(S) \sim 2\left(1 - \frac{1}{\sqrt{M}}\right).$$

To give a clear description, we use Equation (5). Applying a simple inequality on the square root  $(\sum \sqrt{\cdot} \ge \sqrt{\sum \cdot})$ , we have

$$E^{\circ}(S) = 2\left\{1 - \frac{1}{M}\sum_{m=1}^{M}\sqrt{\lambda_m}\right\} \le 2\left\{1 - \frac{1}{M}\sqrt{\sum_{m=1}^{M}\lambda_m}\right\} = 2\left(1 - \frac{1}{\sqrt{M}}\right). \tag{7}$$

Thus,  $2(1 - 1/\sqrt{M})$  is an upper bound of  $E^{\circ}(S)$  for linearly independent *S*.

According to Eldar and Forney [18], the LSE for linearly dependent *S* is given by  $E^{\circ}(S) = 2[1 - (1/M)\sum_{i=1}^{r}\sqrt{\lambda_i}]$ , where *r* is the rank of **G** and  $\lambda_i$  is the nonzero eigenvalue of **G**. From the convexity of the square root and the inequality used in Equation (7), we have  $2(1 - \sqrt{r/M}) \leq E^{\circ}(S) \leq 2(1 - 1/\sqrt{M})$  for linearly dependent *S*. If all the vectors in *S* are identical, then r = 1 and  $\lambda_1 = M$ . Therefore, the upper bound  $2(1 - 1/\sqrt{M})$  can be attained by the case that all the vectors in *S* are identical. Thus, the quantity  $2(1 - 1/\sqrt{M})$  can be regarded as the maximum of  $E^{\circ}(S)$  if the identical vector case is allowed. Furthermore, a simple calculation derives the inequality  $X_r(\lambda_1, \lambda_2, \lambda_3, \dots, \lambda_r) \geq X_{r-1}(\lambda_1 + \lambda_2, \lambda_3, \dots, \lambda_r)$ , where  $X_r(\lambda_1, \lambda_2, \lambda_3, \dots, \lambda_r) = \sum_{i=1}^r \sqrt{\lambda_i}$  for  $2 \leq r \leq M$ . Therefore, we have

$$2\left(1-\frac{1}{M}X_r(\lambda_1,\lambda_2,\lambda_3,\ldots,\lambda_r)\right) \le 2\left(1-\frac{1}{M}X_{r-1}(\lambda_1+\lambda_2,\lambda_3,\ldots,\lambda_r)\right).$$
(8)

The orthonormal states and the identical state case attain the minimum and maximum values of LSE, respectively. That is, the smallest rank r = 1 case gives the maximum, and the full rank r = M case provides the minimum. The inequality above supports this fact. A lower rank has a higher non-orthogonality and vice versa.

3.2. A Non-Orthogonality Index of a Collection of Pure State Signals

The range of  $E^{\circ}(S)$  is given by

$$0 \le E^{\circ}(S) \le 2\left(1 - \frac{1}{\sqrt{M}}\right) \le 2.$$
(9)

Hence, we define the non-orthogonality index (NOI), which is a new measure of the non-orthogonality of a collection of linearly independent pure states, as follows:

$$NOI(S) \equiv \frac{1}{2\left(1 - 1/\sqrt{M}\right)} E^{\circ}(S), \tag{10}$$

where  $0 \le NOI(S) \le 1$ . The vectors in *S* are almost orthogonal to each other when NOI(S) is approximately equal to 0. Conversely, all vectors in *S* are almost identical when NOI(S) is approximately equal to 1.

# 4. Numerical Simulations

4.1. Binary Case

For  $S = \{ |\psi_1\rangle, |\psi_2\rangle \},\$ 

$$NOI(S) = \frac{2 - \sqrt{1 - |\kappa|} - \sqrt{1 + |\kappa|}}{2 - \sqrt{2}},$$
(11)

where the inner product  $\kappa = \langle \psi_1 | \psi_2 \rangle$ . NOI(S) = 0 when  $|\psi_1\rangle$  and  $|\psi_2\rangle$  are orthogonal ( $\kappa = 0$ ), and NOI(S) = 1 when  $|\psi_1\rangle = |\psi_2\rangle$  ( $\kappa = 1$ ). From Equation (11), we have

$$|\kappa| = \frac{1}{2}(2-t)\sqrt{t(4-t)}, \quad t = (2-\sqrt{2})NOI(S).$$
 (12)

The minimum average probability of the quantum detection error is given by  $P_e = (1 - \sqrt{1 - |\kappa|^2})/2$  [23], where we assume that the states are equiprobable. Moreover, the capacity for a binary pure state channel,  $b \rightarrow |\psi_b\rangle$  (b = 1, 2), is given by  $C = -\mu_+ \log_2 \mu_+ - \mu_- \log_2 \mu_-$ , where  $\mu_{\pm} = (1 \pm |\kappa|)/2$  [24]. Figure 1 illustrates the plot of these quantities versus *NOI*(*S*) instead of the modulus of the inner product  $|\kappa|$ . The error probability  $P_e$  is nearly proportional to *NOI*(*S*), and the capacity *C* monotonically decreases with respect to *NOI*(*S*).



**Figure 1.** Binary case. (left) Minimum error probability  $P_e$  vs. NOI(S). (right) Capacity C vs. NOI(S).

#### 4.2. Numerical Simulation I: (Condition-Free)

A simple computer simulation was performed to verify the property  $0 \le NOI(0) \le 1$ . In this simulation, *M* normalized complex vectors,  $|\psi_m\rangle = |r_m\rangle \in \mathbb{C}^M$ , are randomly generated, and NOI(S) is computed if  $S = \{|\psi_m\rangle : 1 \le m \le M\}$  is linearly independent. This procedure was repeated 1000 times for each *M*, where M = 4, 8, 16, 32, 64, 128, 256. No exceptional values of NOI(S) were observed in this simulation.

#### 4.3. Numerical Simulation II: (Almost Orthogonal Case)

A simulation for the case of almost orthogonal quantum states was performed to see how NOI(S) approaches zero.

Let  $\beta^{\bullet} = \{ |v_1^{\bullet}\rangle, \dots, |v_M^{\bullet}\rangle \}$  be the standard basis for  $\mathbb{C}^M$ . For each *m*, a normalized vector  $|r_m\rangle \in \mathbb{C}^M$  is randomly generated and the state vector is set to  $|\psi'_m\rangle = \mathcal{N}(|v_m^{\bullet}\rangle + \tilde{\delta}|r_m\rangle)$ , where  $\mathcal{N}$  is a normalization factor and  $\tilde{\delta}$  is a small positive number. When  $S' = \{|\psi'_1\rangle, \dots, |\psi'_M\rangle\}$  is linearly independent, NOI(S') and  $\delta = \max\{\delta_1, \dots, \delta_M\}$  are evaluated, where  $\delta_m = \|\psi'_m - v_m^{\bullet}\|$ . This procedure was repeated 200 times for each  $\tilde{\delta}$ , where  $\tilde{\delta}$  was chosen from 0.001 to 0.3 with step 0.001. Hence, the total number of trials was 60000 for each *M*, where M = 8, 16, 32, 64, 128, 256.

Figure 2 illustrates the graph of NOI(S') versus  $\delta$  for each M. The overall trend of the figures is that NOI(S') almost depends on  $\delta^2$ , which reflects the definition of  $\delta_m$ . We observed that the variance of NOI(S'), which means the dispersion of values at each  $\delta$ , decreases and the typical value of NOI(S') approaches zero when  $\delta$  approaches zero. Conversely, the smallest value in each  $\delta$  leaves from the floor line of NOI(S) = 0 and the variance of NOI(S') increases when  $\delta$  increases.

Comparing the figures, the variance of NOI(S') shrinks as M increases. The transition from NOI(S) = 0 to NOI(S) = 1 in a figure is related to the change in the rank of **G**. Each graph shows only the case of linearly independent S, namely the case of r = M. Taken together with Equation (8), one may infer that the boundary of the plotted points means a borderline of whether the randomly generated vector set is linearly independent or not. Based on this thought, the variance in each  $\delta$  shows the existing range of linearly independent S. Hence, we conjecture that the range of possible values of the NOI for linearly independent sets becomes relatively smaller when M increases.



**Figure 2.** NOI(S') vs.  $\delta$  for almost orthogonal cases.

# 4.4. Numerical Simulation III: (Almost Identical Case)

A simulation for the case that the quantum states are almost identical was performed to see how NOI(S) approaches one.

Let  $|c\rangle = (1/\sqrt{M}, ..., 1/\sqrt{M}) \in \mathbb{C}^{M}$ . For each *m*, a normalized vector  $|r_{m}\rangle \in \mathbb{C}^{M}$  is randomly generated and the state vector is set to  $|\psi'_{m}\rangle = \mathcal{N}(|c\rangle + \tilde{\epsilon}|r_{m}\rangle)$ , where  $\mathcal{N}$  is

a normalization factor and  $\tilde{\epsilon}$  is a small positive number. When  $S' = \{|\psi'_1\rangle, \dots, |\psi'_M\rangle\}$  is linearly independent, NOI(S') and  $\epsilon = \max\{\epsilon_1, \dots, \epsilon_M\}$  are evaluated, where  $\epsilon_m = \|\psi'_m - c\|$ . This procedure was repeated 200 times for each  $\tilde{\epsilon}$ , where  $\tilde{\epsilon}$  was chosen from 0.001 to 0.3 with step 0.001. Hence, the total number of trials was 60,000 for each M, where M = 8, 16, 32, 64, 128, 256.

Figure 3 illustrates the graph of NOI(S') versus  $\epsilon$ . The overall trend of the figures is that NOI(S') is linear for  $\epsilon$ . In each figure, the variance of NOI(S') decreases, and the typical value of NOI(S') approaches one as  $\epsilon$  approaches zero. Conversely, the largest value leaves from the ceiling line of NOI(S) = 1 and the variance of NOI(S') increases when  $\epsilon$  increases. Comparing the figures, the variance of NOI(S') shrinks as M increases, as in the almost orthogonal case.



**Figure 3.** NOI(S) vs.  $\epsilon$  for almost identical cases.

# 5. An Application of the Proposed Technique

Let us consider the case of an *M*-ary PSK coherent state signal as a practical application of the index. As for the *M*-ary PSK coherent state signal, many researchers have studied it in various ways. The performance of the optimal quantum receiver for the PSK signals has been well studied (e.g., [25–28]). The closed-form expression of the capacity of the pure state channel with the PSK signal was derived in Ref. [29]. The reliability function of the pure state channel with the PSK signal at a high information rate was analyzed in Ref. [30]. Furthermore, an experiment utilizing the 2<sup>17</sup>-ary (131072-ary) optical PSK signal was reported in Ref. [15].

An optical signal emitted from a laser can be expressed as a coherent state of light. The coherent state with complex amplitude  $\alpha$  [31] is expressed as

$$|\alpha\rangle = \exp\left[-\frac{|\alpha|^2}{2}\right] \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle, \tag{13}$$

where  $|n\rangle$  is the number state. The average number of signal photons in the state  $|\alpha\rangle$  is given by  $\langle n \rangle = |\alpha|^2$ . In a communication scenario, the complex amplitude of a coherent

state signal is determined based on the signal modulation format. For an *M*-ary PSK coherent state signal, *S* is given by

$$S = \left\{ \left| \alpha_0 \exp[\frac{2m\pi j}{M}] \right\rangle : 0 \le m \le M - 1 \right\},\tag{14}$$

where  $j = \sqrt{-1}$ , and the fundamental amplitude  $\alpha_0$  is assumed to be a positive real number. The *M*-ary PSK coherent state signal is designed to be symmetric on the constellation diagram. Hence, the average number of signal photons does not depend on the probability distribution  $\mathbf{p} = (p_0, \dots, p_{M-1})$  of the signal. That is,

$$N_{S} = \sum_{m=0}^{M-1} p_{m} \left| \alpha_{0} \exp[\frac{2m\pi \eta}{M}] \right|^{2} = \alpha_{0}^{2}.$$
 (15)

In order to compute NOI(S) of the *M*-ary PSK coherent state signal, we use the eigenvalues of **G** constructed from *S* of Equation (14). In this case, the eigenvalues are given as follows.

$$\lambda_m = \sum_{\ell=1}^M A_{(1,\ell)} \cos \Big[ \Theta_{(1,\ell)} - \frac{2\pi}{M} m(\ell-1) \Big],$$
(16)

where

$$A_{(1,\ell)} = \exp\left[-2|\alpha_0|^2 \sin^2\left[\frac{\pi}{M}(\ell-1)\right]\right],$$
(17)

$$\Theta_{(1,\ell)} = |\alpha|^2 \sin\left[\frac{2\pi}{M}(\ell-1)\right].$$
(18)

Figure 4 illustrates the graph of NOI(S) of the *M*-ary PSK coherent state signal versus  $\log_2 M$  (the size of *M* in bits). Typical values of *M* are  $2^4 = 16$ ,  $2^6 = 64$ ,  $2^8 = 256$ ,  $2^{10} = 1024$ ,  $2^{12} = 4096$ ,  $2^{14} = 16,384$ ,  $2^{16} = 65,536$ , and  $2^{17} = 131,072$ . In this computation, the average number  $N_s$  of signal photons was between 10 and 1,000,000 photons. From Figure 4, we observe that NOI(S) increases monotonically for *M*. This mutual relationship was observed for all values of  $N_S$ . The non-orthogonality of the states is one of the fundamental properties of a quantum system. Therefore, Figure 4 shows that the *M*-ary PSK coherent state signal exhibits a quantum nature for a significantly large number of signal photons when the total number *M* of the signals is large enough.



**Figure 4.** *NOI*(*S*) vs. log<sub>2</sub> *M* for *M*-ary PSK coherent state signal.

The capacity of the pure state channel  $m \rightarrow |\psi_m\rangle$  for the *M*-ary PSK coherent state signal is analyzed to understand the operational meaning of *NOI*(*S*). From Ref. [29], the capacity of this channel is given by

$$C = -\sum_{m=1}^{M} \mu_m \log_2 \mu_m, \quad \mu_m = \frac{\lambda_m}{M}, \tag{19}$$

where  $\lambda_m$  is given by Equation (16), because the optimal signal distribution to achieve the capacity is a uniform distribution  $\mathbf{p} = (1/M, ..., 1/M)$ . Normalized quantity C', which represents the number of Shannon bits per one binary digit of a signal, is obtained by dividing the capacity C by  $\log_2 M$ . Figure 5 illustrates the graph of the normalized capacity versus  $\log_2 M$ . From Figures 4 and 5, we observe that the normalized capacity is maximum (or 1) in the region where NOI(S) is almost zero, and the capacity decreases when NOI(S) increases. Thus, NOI(S) effectively detects the trend of the capacity.



**Figure 5.** Normalized capacity C' vs. log<sub>2</sub> M for M-ary PSK coherent state signal.

#### 6. Conclusions

We have proposed a novel index to measure the non-orthogonality of a collection of linearly independent pure states based on the least squares error criterion in quantum detection theory. We call this index the non-orthogonality index (NOI). First, the nonorthogonality index was analyzed using numerical simulations for binary, condition-free, almost orthogonal, and almost identical cases. The index effectively measured the nonorthogonality of a collection of linearly independent signals from the computer simulations. Next, the non-orthogonality index was applied to the *M*-ary phase-shift keying (PSK) coherent state signal. It was shown that a highly large-scale *M*-ary PSK coherent state signal exhibits high non-orthogonality when the total number of signals is sufficiently large. Furthermore, the index was compared with the capacity of the pure state channel with the PSK signal. Then, we observed that the proposed index effectively detects the trend of the capacity.

In general, a quantum cryptographic system must use a quantum signal set that is unable to distinguish the signals with small detection error or extract much information for an eavesdropper. A simple method is to use single-photon or very weak coherent states. However, this approach has inherent limitations in transmission speed and distance. On the other hand, the coherent state signal having very high power can behave as an almost non-orthogonal signal if the number of signals is sufficiently large. Thus, using a highly large-scale multilevel coherent state signal can create an advantage for legitimate users against the eavesdropper from quantum signal detection. Quantum stream cipher Y00 is a protocol that uses a sufficient number of high-power coherent state signals. Therefore, we conclude that the characterization of a highly large-scale *M*-ary coherent state signal based on the non-orthogonality index provides a basis for understanding cutting-edge optical communication technologies such as quantum stream cipher Y00.

This article discussed the non-orthogonality index in the case of linearly independent pure state signals. Therefore, the generalization of the index remains for future work, which will involve a more precise analysis of linearly dependent cases and the cases of mixed states. In addition, the application to other multilevel coherent state signals such as quadrature amplitude modulation signals will be considered in future work.

Funding: This research was funded under Grant No. JPJ004596 from ATLA, Japan.

Institutional Review Board Statement: Not applicable

**Data Availability Statement:** All relevant simulation parameters and equations are within the paper. No experimental data was used in this study.

Acknowledgments: The author would like to thank Fumio Futami and Ken Tanizawa of Tamagawa University for their helpful discussions. The author is grateful to Shigeo Tsujii of Chuo University for his encouragement.

Conflicts of Interest: The author declares no conflict of interest associated with this manuscript.

#### Abbreviations

The following abbreviations are used in this manuscript:

- LSE Least squares error
- NOI Non-orthogonality index
- PSK Phase-shift keying

#### References

- 1. Helstrom, C.W. Detection theory and quantum mechanics. *Inf. Control* **1967**, *10*, 254–291. [CrossRef]
- 2. Helstrom, C.W. Detection theory and quantum mechanics (II). Inf. Control 1968, 13, 156–171. [CrossRef]
- 3. Helstrom, C.W. Fundamental limitations on the detectability of electromagnetic signals. *Int. J. Theor. Phys.* **1968**, *1*, 37–50. [CrossRef]
- 4. Middleton, D. An Introduction to Statistical Communication Theory; McGraw-Hill: New York, NY, USA, 1960; pp. 771–1070.
- 5. Van Trees, H.L. Detection, Estimation, and Modulation Theory; Part I; John Wiley and Sons: New York, NY, USA, 1968; pp. 19–165.
- Yuen, H.P.; Kennedy, R.S.; Lax, M. On optimal quantum receivers for digital signal detection. *Proc. IEEE* 1970, 58, 1770–1773. [CrossRef]
- Yuen, H.P.; Kennedy, R.S.; Lax, M. Optimum testing of multiple hypotheses in quantum detection theory. *IEEE Trans. Inf. Theor.* 1975, 21, 125–134. [CrossRef]
- 8. Holevo, A.S. Statistical decision theory for quantum systems. J. Multivar. Anal. 1973, 3, 337–394. [CrossRef]
- 9. Wootters, W.K.; Zurek, W.H. A single quantum cannot be cloned. *Nature* **1982**, *299*, 802–803. [CrossRef]
- 10. Dieks, D. Communication by EPR devices. Phys. Lett. 1982, 92, 271–272. [CrossRef]
- 11. Yuen, H.P. Amplification of quantum states and noiseless photon amplifiers. Phys. Lett. 1986, 113, 405–407. [CrossRef]
- 12. Middleton, D.; Van Meter, D. On optimum multiple-alternative detection of signals in noise. *IRE Trans. Inf. Theor.* **1955**, *1*, 1–9. [CrossRef]
- 13. Gallager, R.G. Principles of Digital Communication; Cambridge University Press: New York, NY, USA, 2008; Section 8.4.
- 14. Papen, G.C.; Blahut, R. E. Lightwave Communications; Cambridge University Press: New York, NY, USA, 2019; Chapter 10.
- 15. Tanizawa, K.; Futami, F. Digital coherent PSK Y-00 quantum stream cipher with 2<sup>17</sup> randomized phase levels. *Opt. Express* **2019**, 27, 1071–1079. [CrossRef] [PubMed]
- 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] [PubMed]
- 17. Holevo, A.S. On asymptotically optimal hypotheses testing in quantum statistics. *Theor. Probab. Appl.* **1979**, 23, 411–415. 429–432. [CrossRef]
- Eldar, Y.C.; Forney, G.D., Jr. On quantum detection and the square-root measurement. *IEEE Trans. Inf. Theor.* 2001, 47, 858–872.
   [CrossRef]
- 19. Belavkin, V.P. Optimal multiple quantum statistical hypothesis testing. *Stochastics* 1975, 1, 315–345. [CrossRef]
- Hausladen, P.; Wootters, W.K. A "pretty good" measurement for distinguishing quantum states. J. Mod. Opt. 1994, 41, 2385–2390. [CrossRef]
- 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]
- 22. Tyson, J. Error rates of Belavkin weighted quantum measurements and a converse to Holevo's asymptotic optimality theorem. *Phys. Rev. A* 2009, *79*, 032343. [CrossRef]
- 23. Helstrom, C.W. Quantum Detection and Estimation Theory; Academic Press: New York, NY, USA, 1976; p. 113.

- 24. Holevo, A.S. Statistical Structure of Quantum Theory; Springer: Berlin, Germany, 2001; p. 53.
- 25. Charbit, M.; Bendjaballah, C.; Helstrom, C.W. Cutoff rate for the *M*-ary PSK modulation channel with optimal quantum detection. *IEEE Trans. Inf. Theor.* **1989**, *35*, 1131–1133. [CrossRef]
- 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]
- 27. Djordjevic, I.B. LDPC-coded *M*-ary PSK optical coherent state quantum communication. *J. Light. Technol.* **2009**, 27, 494–499. [CrossRef]
- 28. Cariolaro, G.; Pierobon, G. Performance of quantum data transmission systems in the presence of thermal noise. *IEEE Trans. Commun.* **2010**, *58*, 623–630. [CrossRef]
- 29. Kato, K.; Osaki, M.; Hirota, O. Derivation of classical capacity of a quantum channel for a discrete information source, *Phys. Lett. A* **1999**, 251, 157–163. [CrossRef]
- Kato, K. A Note on the Reliability Function for M-ary PSK Coherent State Signal. *Tamagawa Univ. Quant. ICT Res. Inst. Bulletin* 2018, *8*, 21–25. Available online: https://www.tamagawa.jp/research/quantum/bulletin/pdf/Tamagawa.Vol.8-5.pdf (accessed on 19 April 2022).
- 31. Glauber, R.J. Coherent and incoherent states of the radiation field. Phys. Rev. 1963, 131, 2766–2788. [CrossRef]