3-5 Manipulation and Measurement of Quantum Signals via Non-Gaussian Operation

KITAGAWA Akira, TAKEOKA Masahiro, SASAKI Masahide, Anthony Chefles, and Norbert Lütkenhaus

On the current communication scheme, Gaussian coherent state signals play an important role. To make use of a potential of coherent state signals going beyond the shot noise limit, not only Gaussian operations, but also non-Gaussian operations, described as the third or higher order interactions with respect to the electric field amplitude, must essentially be applied. In this manuscript, we discuss our recent results on the enhancement of entanglement and quantum signal descrimination via the measurement-induced non-Gaussian operation with the photon detector and linear optics.

Keywords
Measurement-induced non-Gaussian operation, Photon detection, Entanglement enhancement, Quantum state discrimination

1 Introduction

Quantum coding is expected to overcome the performance limits of today's optical communications and to achieve the ultimate transmission performance permitted by quantum mechanics. To implement quantum coding, quantum technology on the receiver side is viewed as particularly important. This means that, while the carrier of the signal is the same coherent light pulse as in the ordinary classical communication system, the receiver performs quantum computing on the received optical pulses to decode the maximum information. This procedure enables quantum communications beyond the traditional "shot noise limit".

The coherent state, which corresponds to the coherent light, belongs to the Gaussian class, the quasi-distribution of which is described with the Gaussian form. The operation that transforms a Gaussian state to another Gaussian state is referred to as a Gaussian operation or a Gaussian transformation. For example, beam splitters, wave plates, homodyne detections, and second-order non-linear optical processes all belong to the class of Gaussian operations.

However, according to recent research on quantum information theory, operations other than Gaussian operations—that is, non-Gaussian operations—will be essential for numerous quantum information protocols to achieve breakthroughs beyond classical information processing, with the exception of a few applications such as quantum cryptography[1]. A non-Gaussian operation is a non-linear optical process of the third or higher order (i.e., a third- or higher-order non-linear process with respect to the creation and annihilation operators of the photons). In other words, in order to convert diverse optical quantum information processes into practical techniques, we need to generate and control non-Gaussian optical quantum states with non-linear processing strong enough even for weak light such as a state containing only a few photons.

A well-known example of a non-Gaussian quantum state is the Schrödinger cat state.

$$|K^{\pm}(\alpha)\rangle = \frac{|\alpha\rangle \pm |-\alpha\rangle}{\sqrt{2(1 \pm e^{-2|\alpha|^2})}} \quad (1)$$

These are the superposed states of two beams of macroscopic coherent light. $|K^{+}(\alpha)\rangle$ and $|K^{-}(\alpha)\rangle$ can be transformed into each other with annihilation operator of the photon given by $\hat{a}$.

$$\begin{cases} \hat{a}|K^{+}(\alpha)\rangle \propto |K^{-}(\alpha)\rangle \\ \hat{a}|K^{-}(\alpha)\rangle \propto |K^{+}(\alpha)\rangle \end{cases} \quad (2)$$

Figure 1 shows the Wigner quasi-probability distribution function of the Schrödinger cat state, $|K^{+}(\alpha)\rangle$. The bulges with the Gaussian shapes at the front left and back right express $|\alpha\rangle$ and $|-\alpha\rangle$, respectively, and the oscillation between them indicates the quantum interference between the wave functions of those two coherent states. The figure shows that the shape of the entire curve is completely different from that of a Gaussian curve.

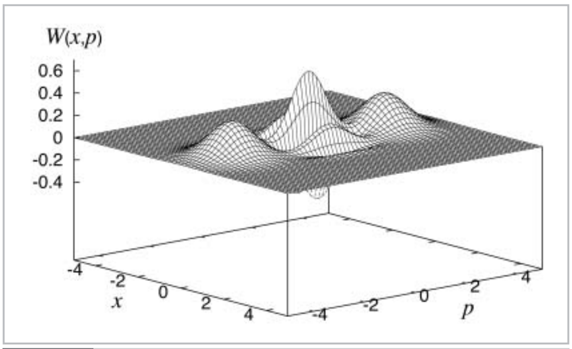

Fig. 1 Wigner quasi-probability distribution function of Schrödinger cat state

However, to generate this Schrödinger cat state, some third- or higher order non-linear process strong enough even for weak light containing only a few photons, is required. Unfortunately, no such device is yet available. Alternatively, the measurement-induced non-linear process, which is due to quantum entanglement and the photon-number resolving detector, is promising. A measurement-induced non-linear process is an operation that effectively causes non-linearity using quantum entangled states and photon-number resolving detectors. The photon-number state is an extreme non-Gaussian state; thus, the projection onto it, which is achieved through measuring photons, is the effective non-Gaussian operation. Once the quantum state is observed, however, it is converted into an electrical signal and the quantum character of the light is destroyed. To avoid this crucial difficulty for quantum state operation, quantum entanglement plays an essential role. When a fragment of an entangled state is measured with a photon counter, the remaining state is non-linearly transformed according to the result of the measurement. It is the measurement-induced nonlinear process that enables the effective non-linear operations at present.

In principle, with such measurement-induced non-Gaussian operation, we can obtain a set of universal quantum gates that can perform any type of quantum operation. (See Reference[2] and Article **3-1**.) However, each of the components of the universal gates, such as the high-performance detector and squeezer, has challenging issues, making it quite difficult to construct a practical quantum device combining them.

On the other hand, we have been studying the theoretical superiority of non-Gaussian operations through measurement-induced processes for certain quantum protocols that will directly lead to demonstration experiments. This article reports on our recent research achievements in this regard.

The first half of this article discusses the generation of the Schrödinger cat state based on a measurement-induced non-Gaussian operation and enhancement of local quantum entanglement. The non-local correlation between the entangled states plays important roles in various quantum information processes. Combining two squeezed states, we can obtain an entangled state, which is the non-classical Gaussian state of light. A number of protocols based on the effects of quantum entanglement have been proposed and verified, such as quantum teleportation[3] and quantum dense coding[4]. Quantum entanglement decreases through interaction with the environment, and it is impossible to recover it with Gaussian local operations and classical communications only[5]. With the above measurement-induced non-Gaussian operation, however, the enhancement of entanglement is possible[6], as discussed earlier. We have recently shown that it is possible for mutual information to increase in the quantum dense coding channel due to this non-Gaussian operation[7]. We have further succeeded in directly evaluating mixed non-Gaussian entangled states[9] using logarithmic negativity, which is a suitable measure of quantum entanglement[8]. We will report on these achievements in the first half of this article.

In the latter half of this article, we discuss the usefulness of measurement-induced non-Gaussian operations in the measurement of, and discrimination among, quantum signals. In communication systems with quantum signals, a measurement in which information is derived maximally is required. In this kind of situation as well, non-Gaussian quantum measurement can be a powerful tool. Not only in regard to communication scheme, but also for various quantum information processing protocols, it is a quite important theoretical issue to study the implementation of the required measurement. A number of researchers have long been discussing these problems in detail. Reviewing their past achievements from a modern point of view provides us with valuable suggestions for a host of new possibilities. Based on this approach, we have proven that we can construct arbitrary binary projection measurements using photon detectors, linear optics, and classical feedforward control. This is discussed in the latter half of this article.

2 Enhancement of quantum entanglement by non-Gaussian operation

Now we consider that a part of the squeezed beam $|r\rangle$ (r is the degree of squeezing) is tapped off with a beam splitter and it is measured with a photon detector. Let us consider an event selection such that a photon is detected on the photon detector (Fig. 2). Beam splitting of the non-classical states brings quantum correlation between the resultant beams. When one of the beams is projected on a photon-number basis, which is a non-Gaussian process, the remaining beam is transformed into a non-Gaussian state. We obtain catlike states close to $|K^{-}(\alpha)\rangle$ when an odd number of photons is detected, and those close to $|K^{+}(\alpha)\rangle$ are obtained when an even number is detected. Practically, however, in cases where it has been difficult to identify photon numbers precisely, an alternative method such as the combination of a high-transmittance beam splitter (for example $T = 0.9$) and on/off photon detector is used, where the probability of two or more photon events is almost negligible, and the 'on' events are selected. As a result, the remaining mode is transformed into a state close to $|K^{-}(\alpha)\rangle$, where the probabilities of two or more photon events are not zero in a strict sense, so the generated state is more or less reduced to a mixed state.

This probabilistic non-Gaussian operation

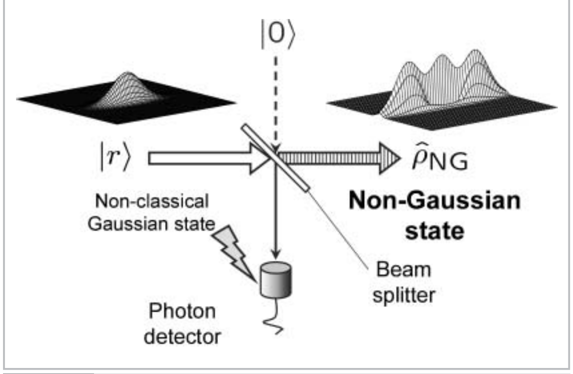

Fig.2 *Schematic diagram of Schrödinger-cat-like state generation scheme based on measurement-induced non-Gaussian operation using beam splitters and photon detectors*

with linear optics and photon detectors is also effective against the Gaussian entangled states. When two squeezed states $|r\rangle_A$ and $|-r\rangle_B$, the quantum fluctuations of which are squeezed along the x axis and the p axis, respectively, are combined with a balanced beam splitter, the resulting state is referred to as a two-mode squeezed state. The photons in each of paths A and B are correlated quantum mechanically, which realizes a Gaussian entangled state. The degree of entanglement is stronger with a higher degree of squeezing, r , and, at the limit of infinitely large squeezing, the ideal quantum correlation is obtained. However, the degree of squeezing practically available is limited, for technical and other reasons. Thus, we are led to consideration of whether or not the entanglement can be enhanced with local operations. However, it is known that the Gaussian entangled state cannot be enhanced with Gaussian local operations (i.e., performing independent operations on beams A and B correlated with each other) and classical communications only.

On the contrary, it may be possible to enhance quantum entanglement if we use non-Gaussian operations. Thus, we consider performing measurement-induced non-Gaussian operations on the two-mode squeezed state (Fig. 3). Combining two beams of non-Gaussian entangled state on mode A and B with another balanced beam splitter, and measuring each of the output modes with the homodyne detection (continuous variable Bell measurement), we can see that the variance is suppressed more than the original squeezed state in $\tanh r \equiv \lambda \lesssim 0.67$ (Fig. 4). In other words, quantum fluctuation is more squeezed. This implies that entanglement has been enhanced.

When the on/off photon detector is used, the non-Gaussian entangled state is generated as a mixed state, similar to the generation of the catlike state. In fact, the evaluation of entanglement in a mixed state is a non-trivial task. Previously some entanglement measures such as the entanglement of formulation[11] had been proposed, however, almost all of them are practically impossible to calculate in a straightforward manner for mixed states. Alternatively, variable operational entanglement evaluation was proposed, such as the fidelity of continuous variable teleportation scheme[6] and the violation of Bell type inequality[12].We have recently applied non-Gaussian entangled states to a quantum dense coding channel and shown that the non-Gaussian operation can be improved for the mutual information[7] of this channel.

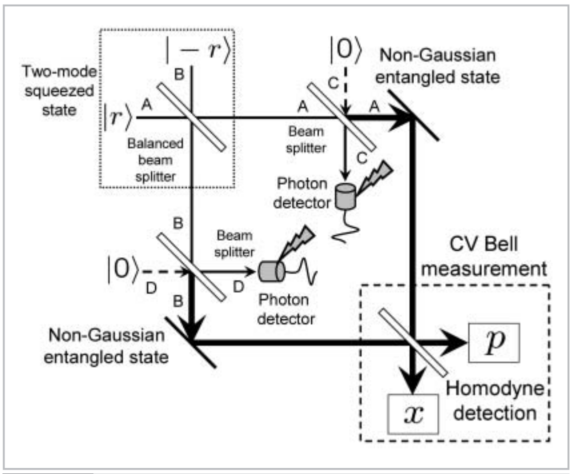

Fig.3 Non-Gaussian operation on Gaussian entangled states

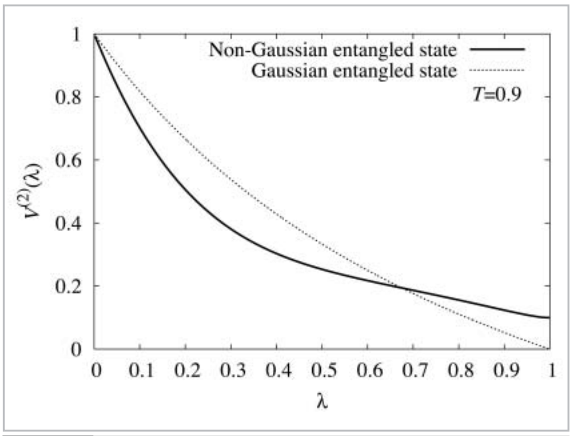

Fig.4 Variances before and after the non-Gaussian operation

Quantum dense coding is a protocol that improves performance of this channel using quantum channels based on entanglement (Fig. 5). The sender, Alice, and the receiver, Bob, share the entangled states in advance, and Alice encodes the classical message using amplitude/phase modulation. Here, we consider in particular Quaternary Phase Shift Keying (QPSK), a model in which four-value signals are encoded, and the maximum information that can be sent is two bits. Bob performs continuous variable Bell measurement between his fragment of entangled state and another sent from Alice in order to decode the information. The results of homodyne measurement obtained here correspond to the channel matrix. Given the signal modulation power β of the coding, we can calculate the performance of mutual information of this channel. Figure 6 shows the mutual information with the non-Gaussian entangled state and Gaussian two-mode squeezed state, respectively. This figure shows that the non-Gaussian operation brings the gain on this channel to $\lambda \leq \lambda_{\rm D}$. ($\lambda_{\rm D} \simeq 0.65$ when $\beta = 0.7$.)

Although the above results are significant in the sense that the enhancement of quantum entanglement is clarified from the viewpoint of informatics, they depend on the modulation intensity, and thus this method is also no more

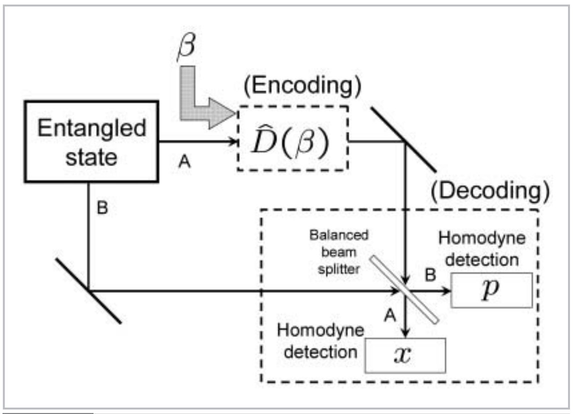

Fig.5 Schematic diagram of quantum dense coding channel

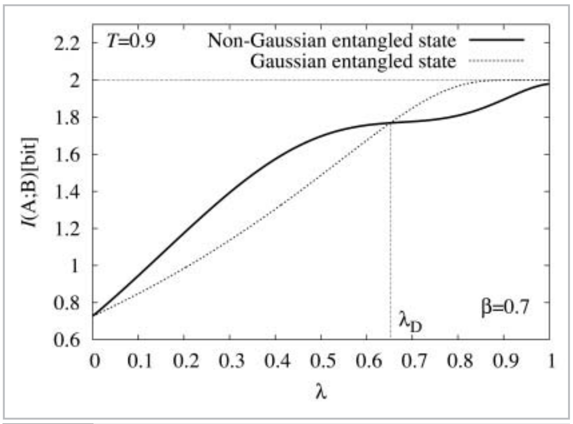

Fig.6 Mutual information for four-value coding model $(\beta = 0.7)$

than an indirect evaluation. Accordingly, we need a measure for which a calculation method is uniquely defined, and further is also "entanglement monotone". Recently, one such monotone measure, logarithmic negativity[8], has been introduced, based on Peres' separability criterion[13].

$$E_{\mathcal{N}}(\hat{\rho}) = \log_2 ||\hat{\rho}^{PT}||. \qquad (3)$$

Here, $\hat{\rho}^{PT}$ shows the partial transposition on one mode only (for example, B) of the density operator. $||\cdot||$ is the sum of the absolute values of the eigenvalues of the operator. As no physical process corresponds to partial transposition, negative eigenvalues can appear due to the effects of entanglement. The magnitudes of these negative eigenvalues correspond to the strength of the entanglement. This quantity can be calculated using the linear algebra packages. As this method has been proved to be an entanglement monotone, it is a useful measure. We have found a method of efficiently calculating the logarithmic negativity for the non-Gaussian entangled states generated in Fig. 3. Figure 7 shows the results of numerical calculation. The larger logarithmic negativity is, the larger entanglement is, thus we can conclude that entanglement is actually enhanced by non-Gaussian operation in the region indicated by $\lambda \leq \lambda_{\rm LN}$.

How is this evaluation related to the result by quantum dense coding protocol discussed earlier? In fact, in the limit of the signal intensity of coding, $\beta \to 0$, we find that the limit to

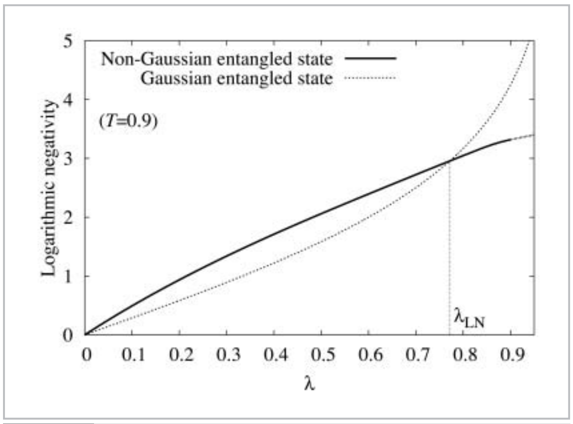

Fig.7 Evaluation of entanglement with logarithmic negativity

improving the mutual information based on a non-Gaussian operation converges to a fixed value (Fig. 8), and this value is very close to the one based on the logarithmic negativity $(\lambda_{\rm D} \simeq \lambda_{\rm LN})$. This is considered to be due to the fact that decreasing the modulation intensity of the signal to an ultimately weak value increases the role of entanglement in this channel, thus bringing us close to a situation in which the pure relative merits of entanglement can be evaluated. In other words, this method optimizes the quantum dense coding channel for an evaluation of entanglement. If the performance of the quantum dense coding channel is improved as a result of this process, we can conclude that the non-Gaussian operation has actually enhanced quantum entanglement. Although the mathematical relationship between logarithmic negativity and evaluation by quantum dense coding unfortunately remains unclear, this is an interesting topic both theoretically and experimentally.

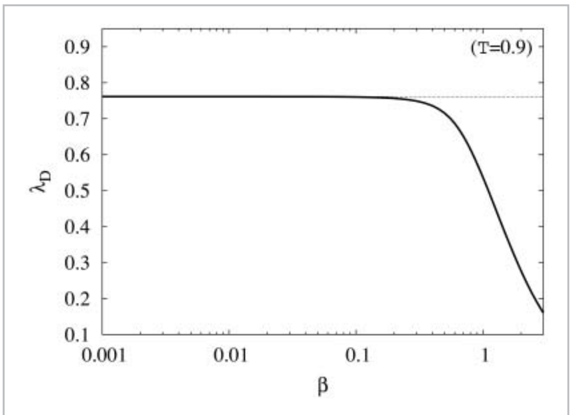

Fig.8 Behavior of $\lambda_{\rm D}$ in the limit as $\beta \to 0$

3 Detection of quantum signals with photon detectors, based on non-Gaussian quantum measurement

Up to the previous section, we discussed how we might control quantum signals using measurement-induced non-Gaussian quantum operations. On the other hand, if we think of the quantum signals as carriers for the classical information, that we directly use, we see that these signals must be detected by a receiver after they are manipulated, modulated, and transmitted. As the carriers we use in communication—electrons and light—are quantum signals that follow quantum mechanics in the microscopic (weak) region, the problem of quantum signal detection as such represents an extremely general problem with implications on overall communication theory.

In the latter half of this article, we address the discrimination of coherent states in the optical domain. Optical coherent states play a central role in communication. We provide an overview of the differences in performance of a Gaussian receiver, which represents today's leading technology, and an optimal quantum receiver incorporating non-Gaussian operation. We then discuss a design theory we are proposing for a photon-detector-based optimal quantum receiver capable of discriminating arbitrary binary optical quantum signals.

3.1 Optimal quantum receiver for coherent signal discrimination

Let us consider the simple problem of coherent optical communication in which information represented by $\{0,1\}$ is carried on signals obtained by phase-shifting the coherent state using $\{|\alpha\rangle, |-\alpha\rangle\}$ (α is a real number). Here, we assume that the occurrence probabilities of $0, 1$ are equal. The most basic Gaussian quantum receivers for such a signal are a homodyne detector and a heterodyne detector. The homodyne detector is mathematically expressed as a projection operation described by the eigenbases $|x\rangle$ corresponding to the quadrature amplitude operator

$$\hat{X} \equiv (\hat{a} + \hat{a}^\dagger)/\sqrt{2}\,, \tag{4}$$

where $(\hat{X}\,|x\rangle = x\,|x\rangle)$ and $\{\hat{a}, \hat{a}^\dagger\}$ pare the creation and annihilation operators.

The output probability distribution is given by

$$|\langle x|\alpha\rangle|^2 = \frac{1}{\sqrt{\pi}} \exp\left[-\frac{(x-\sqrt{2}\alpha)^2}{2}\right]. \tag{5}$$

As such, the coherent state is a typical Gaussian state for which the homodyne detector probability distribution follows a Gaussian distribution. When detecting the phase-shifted binary signals using a homodyne detector, the bit error probability is proportional to the area of overlap between the two distributions $|\langle x|\alpha\rangle|^2$ and $|\langle x|-\alpha\rangle|^2$, and given as

$$P_{\rm e}^{\rm (H)} = \frac{1}{2}{\rm erfc}(\sqrt{2}\alpha) \quad (6)$$

Various quantum operations may be performed along the way to improve on this error probability. However, it may be impossible to overcome the error probability limit of the homodyne detector by using only Gaussian operations. This is the final limit of conventional optical communications, where the shot noise limit applies to all communication performance.

On the other hand, if we allow all quantum operations in the receiving process, including non-Gaussian operations, we can in principle achieve an error probability beyond the limit of Equation (6). In 1967, Helstrom formulated the problem of calculating the minimum error probability allowed by quantum mechanics. For the phase-shifted binary coherent signals discussed above, the minimum error probability is given as

$$P_{\rm e}^{\rm min} = \frac{1}{2}\left(1-\sqrt{1-|\kappa|^2}\right) \quad (7)$$

where $\kappa \equiv \langle\alpha|-\alpha\rangle$. It has been shown that quantum measurement that achieves this minimum error probability is expressed as a projection onto the orthonormal bases consisting of the superposition of the signal states themselves[14], as

$$|\omega_0\rangle = \sqrt{\frac{1-P_e^{\rm min}}{1-\kappa^2}}|\alpha\rangle - \sqrt{\frac{P_e^{\rm min}}{1-\kappa^2}}|-\alpha\rangle \quad (8)$$

$$|\omega_1\rangle = \sqrt{\frac{P_e^{\rm min}}{1-\kappa^2}}|\alpha\rangle + \sqrt{\frac{1-P_e^{\rm min}}{1-\kappa^2}}|-\alpha\rangle \quad (9)$$

Although this expression is mathematically simple, its physical meaning is not clear. Thus, a physical mechanism providing an error probability close to $P_{\rm e}^{\rm min}$ was pursued as early as 1970.

Kennedy showed that it is possible to obtain an error probability characteristic as close as approximately twice the Helstrom limit of Equation (7)[15],

$$P_{\rm e}^{\rm (K)} = \frac{1}{2}{\rm e}^{-2|\alpha|^2} \quad (10)$$

In Kennedy's method, the signal state and strong coherent light are interfered by an asymmetric beam splitter to shift $\{|\alpha\rangle, |-\alpha\rangle\}$ to $|0\rangle, |-2\alpha\rangle$, and the photon detector determines only the presence or absence of the photons.

This is the simplest example of non-Gaussian manipulation to overcome the conventional error probability limit, $P_{\rm e}^{\rm (H)}$, caused by the shot noise. Based on Kennedy's scheme, Dolinar proved that the Helstrom limit can be achieved by the feedforward of the intensity and phase of the coherent light, according to the results of photon detection[16] (Note that the Helstrom limit may also be achieved by cleverly operating a complicated non-Gaussian unitary transformation before homodyne detection[17]. However, in this case, the configuration of a feasible physical system remains unclear.).

These proposals by Kennedy and Dolinar represented pioneering, revolutionary developments in that they provided the first specific methods for exceeding the performance limit of optical communications. However, the technical requirements were far beyond the levels of electrical control and light-detection technologies at the same time, so few studies were conducted in this field. However, these proposals are beginning to be recognized as important problems that merit re-examination, primarily for the following two reasons[18][19]. First, we have recently seen considerable advances in quantum electronics as a whole, and in photon detection technology in particular (see other articles in this issue), and these proposals are now within reach. Progress in these technologies has also pushed optical communications technology based on homodyne detectors close to the theoretical limit. Second, theoretical studies concerning all areas of quantum information have advanced greatly in the past 20 years. It has become clear that the detection of quantum states, going beyond the detection of coherent signals, will play an important role in all areas of quantum information processing technology.

3.2 Design theory of optimal quantum receiver for arbitrary pure binary quantum signals

We will now discuss our recent activities and achievements with regard to the designing strategies of this optimal quantum receiver. In the physical model based on the feedforward discussed above, Dolinar derived the parameters that will minimize error probability in the detection of binary coherent states using optimal control theory, including dynamic programming, and showed that the parameters will approach the Helstrom limit. On the other hand, we have used the fact that quantum measurement achieving the minimum error probability is described by a projection measurement, and then shown that Dolinar's method may be derived in a simpler manner that does not require complicated optimization theory[19].

The problem can be formulated as whether a given two orthogonal states can be detected with a combination of photon-number resolving detectors, coherent states (as a supplementary system), beam splitters, and high-speed electric feedforward control. Here, we take the binary coherent signals discussed above as an example. The signals themselves are mutually non-orthogonal coherent states. However, the measurement is expressed as projections onto orthogonal state vectors, $\{|\omega_0\rangle, |\omega_1\rangle\}$. In other words, the measuring instrument that we want to produce need only be capable of perfect discrimination of the two orthogonal states $|\omega_0\rangle$ and $|\omega_1\rangle$. Such a measuring instrument will also be able to detect the original non-orthogonal signal states with the minimum error probability. For the perfect discrimination of orthogonal states, $\{|\omega_0\rangle, |\omega_1\rangle\}$, these states need to maintain orthogonality during the measurement process. An approach that uses the orthogonal condition can allow not only for discussion of the optimal measurement of binary coherent states but also of the problem of detecting arbitrary optical quantum states. In other words, we can also discuss whether perfect discrimination is possible with the above physical system for an arbitrary pair of orthogonal states, which are not restricted to $\{|\omega_0\rangle, |\omega_1\rangle\}$.

In addition, using this approach, we succeeded in proving that the perfect discrimination of two pairs of orthogonal quantum states is possible using the above physical system alone, by indicating a specific measuring scheme[20]. This achievement represents the generalization of the theory of the Dolinar receiver. Furthermore, our approach shows that if a sufficient number of photon detectors, linear optics, and feedforward mechanisms are provided, the photon detector does not need to be able to perform complete photon-number detection; instead, it is enough that the detector be able to detect the arrival of a photon with the highest possible quantum efficiency and the lowest possible dark count.

Let us denote the two orthogonal states as

$$|\Psi\rangle = \sum_{m=0}^{\infty} c_m |m\rangle \qquad |\Phi\rangle = \sum_{m=0}^{\infty} d_m |m\rangle, \quad (11)$$

Here, $|m\rangle$ is the m -photon state and $\langle\Psi|\Phi\rangle = \sum_{m=0}^{\infty} c_m^* d_m = 0$. As shown in Fig. 9, this state is divided evenly with $N-1$ sets of beam splitters such that the power reflectance of each beam is $1/N$. These split beams are measured sequentially. Each port interferes the tapped beam and the coherent state $|\beta_n\rangle$ of the auxiliary system using a beam splitter with sufficiently low reflectivity. Such an operation corresponds to a shift operation described as $\hat{D}(\beta_n/\sqrt{N})$ and finally, one performs photon detection. β_n is determined based on the history of photon detection up to the previous stage.

For a sufficiently large N, the probability that two or more photons will be detected in a port can be ignored. In such case, the state after the beam passes through the first beam splitter is expressed as

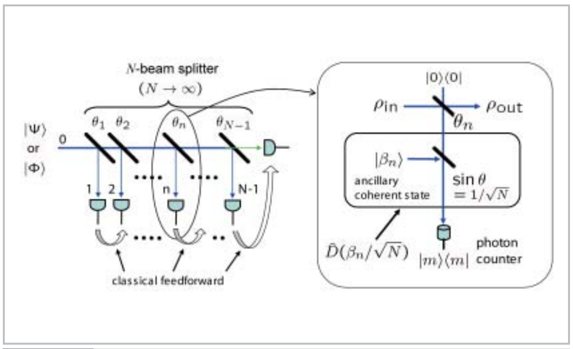

Fig.9 Photon detection, auxiliary coherent states, and feedforward detection of two orthogonal states

$$\hat{B}_{1,0}(\theta_1)|0\rangle_1|\Psi\rangle_0 \approx |0\rangle_1|\eta_0\rangle_0 + \frac{1}{\sqrt{N}}|1\rangle_1|\eta_1\rangle_0 , \quad (12)$$

$$\hat{B}_{1,0}(\theta_1)|0\rangle_1|\Phi\rangle_0 \approx |0\rangle_1|\nu_0\rangle_0 + \frac{1}{\sqrt{N}}|1\rangle_1|\nu_1\rangle_0 , \quad (13)$$

where $\langle\eta_0|\nu_0\rangle + \langle\eta_1|\nu_1\rangle/N \approx 0$ holds. The measurement at mode 1 is designed in a manner such that the post-measurement states $|\Psi'\rangle$ and $|\Phi'\rangle$ corresponding to the two inputs $|\Psi\rangle$ and $|\Phi\rangle$, respectively, are orthogonal. It is clear that such measurement is specifically given by the projection measurement of the form,

$$|\pi_0\rangle = \mathcal{N}_{p0}\left\{|0\rangle - (X + O(X^2))|1\rangle\right\}, \quad (14)$$

$$|\pi_1\rangle = \mathcal{N}_{p1}\left\{(X^* + O(X^2))|0\rangle + |1\rangle\right\}, \quad (15)$$

where $\mathcal{N}_{p0}$ and $\mathcal{N}_{p1}$ are the normalization constants and the parameter X depends on the orthogonal states $|\Psi\rangle$ and $|\Phi\rangle$ and is determined as

$$X = \frac{2(\langle\nu_0|\eta_1\rangle\langle\eta_1|\nu_1\rangle - \langle\eta_0|\nu_1\rangle\langle\nu_1|\eta_1\rangle)}{\sqrt{N}(|\langle\eta_0|\nu_1\rangle|^2 - |\langle\eta_1|\nu_0\rangle|^2)} . \quad (16)$$

In fact, this measurement can be implemented with the shift operation $\hat{D}(\beta_n/\sqrt{N})$ and photon detectors, as discussed above. The first-stage measurement (shown in Fig. 9) is thus expressed with the vector

$$\hat{D}^\dagger\left(\frac{\beta_1}{\sqrt{N}}\right)|0\rangle \approx e^{-|\beta_1|^2/2N}\left(|0\rangle - \frac{\beta_1}{\sqrt{N}}|1\rangle\right) , \quad (17)$$

$$\hat{D}^\dagger\left(\frac{\beta_1}{\sqrt{N}}\right)|1\rangle \approx -e^{-|\beta_1|^2/2N}\left(\frac{\beta_1^*}{\sqrt{N}}|0\rangle + |1\rangle\right) , \quad (18)$$

and we can approximately implement the measurement device expressed in Equations (14) and (15) if we select β_1 to make N sufficiently large. In addition, the post-measurement quantum states $|\Psi'\rangle$ and $|\Phi'\rangle$ can be formally expressed by

$$|\Psi'\rangle = \sum_{m=0}^{\infty} c'_m|m\rangle \qquad |\Phi'\rangle = \sum_{m=0}^{\infty} d'_m|m\rangle , \quad (19)$$

for both cases of measurement results. Thus, the second-stage and subsequent measurements may repeat the process according to the same strategy. The error probability for discriminating $\{|\Psi\rangle, |\Phi\rangle\}$ in the last N th-stage projection measurement can be made to approach zero asymptotically within the limit of a sufficiently large N.

The discussion above concerns single-mode optical quantum states. Nevertheless, the conclusion is the same for multi-mode states, where, for example, the two orthogonal states are in the entangled states. It is already known that all binary orthogonal states can be discriminated only by a local projection measurement for each mode[21]. Thus, it is sufficient to repeat the above measurement strategy sequentially. See Reference[20] for a more detailed discussion and derivation of the upper bound of the error probability for a finite N.

4 Conclusions

This article reports on the theoretical research achievements related to the non-Gaussian quantum operations based on a measurement-induced nonlinear process using photon detectors and beam splitters. For the Gaussian entanglement, conditional operation using on/off photon detectors—which determine only the presence or absence of photons—generates mixed non-Gaussian entangled states. It is generally difficult to evaluate the degree of entanglement for mixed non-Gaussian states. Nevertheless, we have found that the logarithmic negativity, a measure of entanglement, can be directly calculated for these states. We also conducted a numerical evaluation. The logarithmic negativity is an entanglement monotone. Since this quantity becomes large as a result of the non-Gaussian operation, we can directly conclude that entanglement is enhanced.

On the other hand, we also report on a design theory based on a number of devices—including photon detectors and linear-optic equipment—for the sort of non-Gaussian quantum measuring instrument that will be required in quantum communications. A measuring instrument that can detect quantum signals is a basic elementary tool for all parts of quantum information technology. In particular, we have theoretically proven that the most basic quantum measurement of all, binary projection measurement, can be established using the above devices only. Few have predicted that a wide class of quantum measurement, such as arbitrary binary projection measurement, could be implemented with such limited physical processes. A basic design theory for quantum receivers—with a view to the creation of practical devices—is anticipated as an important basic theory that will bring us closer to the future technical implementation of quantum coding.

References

1 S. D. Bartlett, B. C. Sanders, S. L. Braunstein, and K. Nemoto, Phys. Rev. Lett. 88, 97904, 2002.

2 D. Gottesman, A. Kitaev, and J. Preskill, Phys. Rev. A 64, 012310, 2001.

3 A. Furusawa, J. L. Sørensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and E. S. Polzik, Science 282, 706, 1998.

4 X. Li, Q. Pan, J. Jing, J. Zhang, C. Xie, and K. Peng, Phys. Rev. Lett. 88, 047904,2002; J. Mizuno, K. Wakui, A. Furusawa, and M. Sasaki, Phys. Rev. A 71, 012304, 2005.

5 J. Eisert, S. Scheel, and M. B. Plenio, Phys. Rev. Lett. 89, 137903, 2002; J. Fiurášek, ibid., 89, 137904, 2002; G. Giedke and J. I. Cirac, Phys. Rev. A 66, 032316, 2002.

6 T. Opatrný, G. Kurizki, and D.-G. Welsch, Phys. Rev. A 61, 032302, 2000; S. Olivares, M. G. A. Paris, and R. Bonifacio, ibid., 67, 032314, 2003.

7 A. Kitagawa, M. Takeoka, K. Wakui, and M. Sasaki, Phys. Rev. A 72, 022334, 2005.

8 G. Vidal and R. F. Werner, Phys. Rev. 65, 032314, 2002.

9 A. Kitagawa, M. Takeoka, M. Sasaki, and A. Chefles, Phys. Rev. A 73, 042310, 2006.

10 M. Dakna, T. Anhut, T. Opatrný, L. Knöll, and D.-G. Welsch, Phys. Rev. A 55, 3184, 1997.

11 C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wooters, Phys. Rev. A 54, 3824, 1996; W. K. Wooters, Phys. Rev. Lett. 80, 2245, 1998.

12 H. Nha and H. J. Carmichael, Phys. Rev. Lett. 93, 020401, 2004.

13 A. Peres, Phys. Rev. Lett. 77, 1413, 1996.

14 C. W. Helstrom, “Quantum Detection and Estimation Theory”, Academic Press, New York, 1976.

15 R. S. Kennedy, Quarterly Progress Report No. 108, Research Laboratory of Electronics, MIT, pp219-225, 1973.

16 S. J. Dolinar, Research Laboratory of Electronics, MIT, Quarterly Progress Report, No.111, p. 115, 1973.

17 M. Sasaki and O. Hirota, Phys. Lett. pp.21-25, 1996.

18 JM Geremia, Phys. Rev. A 70, 062303, 2004.

19 M. Takeoka, M. Sasaki, P. van Loock, and N. Lütkenhaus, Phys. Rev. A 71, 022318, 2005.

20 M. Takeoka, M. Sasaki, N. Lütkenhaus, e-print quant-ph/0603074, 2006.

21 J. Walgate, A. J. Short, L. Hardy, and V. Vedral, Phys. Rev. Lett.85, 4972, 2000.

***KITAGAWA Akira**, Dr. Eng.*

Limited Term Reseacher, Advanced Communications Technology Group, New Generation Network Research Center (former: Expert Researcher, Quantum Information Technology Group, Basic and Advanced Research Department)

Quantum Optics, Quantum Information Theory

***TAKEOKA Masahiro**, Dr. Eng.*

Reseacher, Advanced Communications Technology Group, New Generation Network Research Center (former: Expert Researcher, Quantum Information Technology Group, Basic and Advanced Research Department)

Quantum Optics, Quantum Information Theory

***SASAKI Masahide**, Ph.D.*

Research Manager, Advanced Communications Technology Group, New Generation Network Research Center (former: Group leader, Quantum Information Technology Group, Basic and Advanced Research Department)

Quantum Information Theory

***Anthony Chefles**, Ph.D.*

Quantum Information Processing Group, Hewlett Packard Labs.

Quantum Information Theory

***Norbert Lütkenhaus**, Ph.D.*

Professor, Institute for Quantum Computing, University of Waterloo

Quantum Optics, Quantum Information Theory