

量子限界における情報通信

佐々木 雅 英[†] 藤 原 幹 生[†] 武 岡 正 裕[†]

人間が直接認識できる文字、いわゆる「古典情報」を、量子通信路を通して伝送、処理する問題を考える。最近、ボソン系の線形損失通信路に対する通信路容量が明らかにされた。それを達成する最適解は、通報をコヒーレント状態のテンソル積に符号化して伝送し、受信側では十分大きなコヒーレント状態のテンソル積符号系列に量子一括測定を施して復号を行うというものである。このような量子一括測定を実現するための技術課題を整理して、その中でも特に根幹となる光子数識別技術について、最新の結果を紹介する。また、光子数識別技術にコヒーレント光、ビームスプリッタ、フィードフォワードを組み合わせて任意の2値のPOVMを実現するための設計理論を提案する。これは従来のショット雑音限界を克服するための具体的な方法を与えるもので、究極の通信路容量の実現に向けた一歩となる。

Info-communications at the Quantum Level

MASAHIDE SASAKI,[†] MIKIO FUJIWARA[†] and MASAHIRO TAKEOKA[†]

We consider a problem of transmitting and processing *classical information*, i.e. alphabet which human can directly recognize, over a quantum channel. Recently the channel capacity has been clarified for a linear lossy bosonic channel. The optimal solution to attain this capacity consists of the encoding with tensor products of coherent states, and the decoding by quantum collective measurement on large blocks of coherent state products. After reviewing technological targets in order to realize quantum collective measurement, we present recent development of photon number detector, which is at the heart of them. We also propose a design theory of arbitrary binary POVM using photon number detectors, coherent light, beamsplitters, and classical feedforward. This would provide a practical method to overcome conventional shot noise limit in communications, and thus be a first step toward achieving the ultimate channel capacity.

1. はじめに

現在のパソコンやインターネットの中を駆け巡っている情報の実体は、電気や光パルスの膨大な羅列であり、これらは0と1という記号の流れを表している。シャノンに始まる現代の情報理論は、情報の伝送や処理を(0, 1)の系列間の遷移ととらえ、雑音の効果は0-1間の確率的遷移として抽象的にモデル化することで、個々の物理系によらない汎用的なシステム設計を可能としている。一般に、通信路のモデル化とは、入力情報源 $X = \{x; P(x)\}$ に対応する出力文字 $\{y\}$ と、 x が入力されたときに y が出力される条件付き確率 $P(y|x)$ を与えることである。また、 $P(y) \equiv \sum_x P(y|x)P(x)$ から計算される出力文字の生起確率から出力情報源

$Y = \{y; P(y)\}$ が定義される。情報の操作はこれらの量のみを用いて抽象的に扱われる。記憶のない通信路に対する通信路容量は、相互情報量

$$I(X : Y) = \sum_{x,y} P(x)P(y|x) \log_2 \frac{P(y|x)}{P(y)}$$

という量を導入して

$$C_{1,1} \equiv \max_{P(x)} I(X : Y) \quad (1)$$

で与えられる¹⁾⁻³⁾。添え字 (1, 1) を付けた意味は後で明らかになる(式(9)の説明を参照)。

(0, 1)を担う媒体が少数の光子、電子といった量子力学的対象になると、情報の流れは量子状態 $\{|\psi_0\rangle, |\psi_1\rangle\}$ の量子力学的な時間発展として記述される。情報を取り出す測定過程も量子力学の言葉で直接書き換えられる。それは、ある直交基底、たとえば $\{|0\rangle, |1\rangle\}$ への射影という表現になる。信号量子状態 $\{|\psi_0\rangle, |\psi_1\rangle\}$ は、

[†] 情報通信研究機構

National Institute of Information and Communications Technology

損失などがある場合、受信器に届くころには非直交状態となって $\{|0\rangle, |1\rangle\}$ とは異なるのが普通である。媒体の量子的性質まで制御できる場合には、通信路行列の背後に遷移確率振幅という一段深い確率法則

$$P(y_1, y_2, \dots, y_n | x_1, x_2, \dots, x_n) = |\langle y_1, y_2, \dots, y_n | \hat{U} | \psi_{x_1}, \psi_{x_2}, \dots, \psi_{x_n} \rangle|^2 \quad (2)$$

が現れる。 \hat{U} は測定過程で信号に施す量子操作を意味する。もし、測定によって遷移する先の量子状態が

$$\hat{U}^\dagger |y_1, y_2, \dots, y_n\rangle = \sum_{x_1, \dots, x_n} c_{x_1, \dots, x_n} |\psi_{x_1}, \psi_{x_2}, \dots, \psi_{x_n}\rangle \quad (3)$$

のように複数の系列パターンの量子力学的重ね合わせ状態にあれば、遷移確率は式 (2) における複素振幅の絶対値の 2 乗という構造ゆえに、もはや個々の通信路の積にはならず、一般に

$$P(y_1, y_2, \dots, y_n | x_1, x_2, \dots, x_n) \neq P(y_1 | x_1) \cdots P(y_n | x_n) \quad (4)$$

となり、従来の枠組みでいう「記憶のある通信路」となる。式 (3) のような複数ビットの重ね合わせ状態は量子もつれ状態と呼ばれ、日常の感覚を超える現象を引き起こす。このような量子状態の干渉効果を直接的に制御することで、従来理論から外挿される限界を凌駕することが可能となる。

このように通信路行列の背後にある確率振幅を顕に考え、それを最適に制御することで可能になる情報通信技術とはどのようなものか、これが本論文の主題である。伝送対象は従来どおり人間が直接認識できる文字、いわゆる「古典情報」であるが、伝送媒体が光子や電子レベルの量子系となる。シャノン理論の基本的枠組みは踏襲しつつも、情報量やデータの圧縮率、通信路容量は量子力学の言語で直接与えられなければならない。これに対して、量子コンピュータの回路内を行き来する、一般には未知の量子状態そのもの、いわゆる「量子情報」を直接の伝送対象とする問題もあり、量子情報理論の新たな重要課題であるが、ここでは触れない。

量子通信路を介した古典情報伝送に関する問題は多くの読者には馴染みが薄いと思われるので、以下ではまず、その研究の背景と最近の結果について紙面を割いて概説する。次に、究極の通信路容量の達成に向けて、今後開発しなければならない重要な要素技術を整理する。鍵となるのは、高品質のスクィーズド光から作られる量子もつれ状態と高精度の光子数識別技術である。比較的開発が進んでいる量子もつれ状態の制御技術に対して、光子数識別技術は高い需要にもかかわらず通信応用に耐えうるレベルにはいまだに達してい

ない。我々は電荷蓄積型読み出し回路を用いた光子数識別技術の開発に取り組んでおり、その最新の成果を紹介する。最後に光子検出と線形光学素子および電氣的フィードフォワード操作のみを使って、任意の 2 値信号の量子最適受信器を設計する理論を提案する。

2. 量子通信路

古典情報の伝送を扱う量子情報理論において、最も第 1 原理的な出発点は量子状態間の写像としての量子通信路である。量子通信路の数学的表現は幾通りがあるがその 1 つに、信号を運ぶ系 Q と環境系 E を含めた系全体 QE の変化を記述する適当なユニタリ作用素 \hat{U}^{QE} を導入して、量子通信路からの出力の際に外部環境の情報を消去するという方法がある^{4),5)}。

$$\hat{\rho}_{\text{out}}^Q = \text{Tr}_E [\hat{U}^{QE} \hat{\rho}_{\text{in}}^Q \otimes \hat{\rho}_{\text{in}}^E \hat{U}^{QE\dagger}] \equiv \hat{L}^Q \hat{\rho}_{\text{in}}^Q \quad (5)$$

ここで、 $\hat{\rho}_{\text{in}}^Q$ と $\hat{\rho}_{\text{in}}^E$ は、それぞれ信号系と環境系の初期状態であり、 Tr_E は環境系に関する部分トレースを表す。この式で定義される写像 $\hat{L}^Q: \hat{\rho}_{\text{in}}^Q \rightarrow \hat{\rho}_{\text{out}}^Q$ が量子通信路を表す（以下、添え字 Q は省略する）。与えられた量子通信路に対して、入力も出力も量子力学が許すあらゆる可能性を考慮して最適化し、送れる情報伝送レートの上限を求めることが理論上の重要課題であり、そこで示された通信路容量にせまる通信システムを実現することが究極のゴールである。

3. 通信路容量

一般的な量子通信路に対して、通信路容量を直接 \hat{L} の関数として求めることはきわめて困難な問題である。歴史的には、まず、入力する量子状態の集合 $\{\hat{\rho}_x^{\text{in}}\}$ を固定したときの通信路容量に対して解答が与えられた。より正確には、量子通信路 \hat{L} 自体には記憶効果がないと仮定し、出力状態 $\hat{\rho}_x = \hat{L}(\hat{\rho}_x^{\text{in}})$ が分かっていると、そのもとの符号化を考える。入力状態 $\{\hat{\rho}_x^{\text{in}}\}$ と量子通信路 \hat{L} が定義される信号系のヒルベルト空間を \mathcal{H} とする。符号化はテンソル積状態

$$\hat{\Psi}_x = \hat{\rho}_{x_1} \otimes \hat{\rho}_{x_2} \otimes \cdots \otimes \hat{\rho}_{x_n} \quad (6)$$

に制限し（量子もつれ状態は考えない）、復号化は量子力学が許すあらゆる可能性を考慮して最適化する。そのような復号過程は、出力文字系列を $\mathbf{y} = (y_1, y_2, \dots, y_n)$ としたとき、 n 次拡大空間 $\mathcal{H}^{\otimes n}$ 上で

$$\hat{\Pi}_{\mathbf{y}} = \hat{\Pi}_{\mathbf{y}}^\dagger \geq 0, \quad \sum_{\mathbf{y}} \hat{\Pi}_{\mathbf{y}} = \hat{I} \quad (7)$$

という条件を満たす作用素、いわゆる確率作用素測度 (Positive Operator Valued Measure, POVM) に

よって表現される^(6),7)．特に，出力文字 y_j 間で量子もつれを形成しながら行う測定のことを量子一括測定と呼ぶ．符号語状態 $\hat{\Psi}_x$ に対する復号過程もまた通信路行列

$$P(y|x) = \text{Tr}(\hat{\Pi}_y \hat{\Psi}_x) \quad (8)$$

で表現される．式(1)に基づく n 次の相互情報量を，符号語の選択 $\mathcal{E}^n = \{x; P(x)\}$ と復号戦略 $\mathcal{D}^n = \{\hat{\Pi}_y\}$ に関して最大化した量を

$$C_{1,n} = \max_{\mathcal{E}^n, \mathcal{D}^n} I(X^n : Y^n), \quad (9)$$

と定義する．ここで添え字 $(1, n)$ のうち“1”は，符号化をテンソル積に制限し文字 x_i 間での量子もつれはないという制限を表す．一方，“ n ”は復号過程で長さ n の系列状態にわたる量子もつれ制御を含む一般的な量子測定（つまり，式(3)のような状態への射影）を許すことを意味する．

もし，量子もつれのない，文字ごとの個別測定に基づく従来どおりの復号戦略を用いる場合，量子通信路 \hat{L} 自体には記憶効果がないと仮定しているので， $I(X^n : Y^n) = nI(X : Y)$ すなわち $C_{1,n} = nC_{1,1}$ となり，通信路容量は

$$C_{1,\infty}^{(C)} = \lim_{n \rightarrow \infty} \frac{C_{1,n}}{n} = C_{1,1} \quad (10)$$

となって，符号化する前の個別測定に対する特性 $C_{1,1}$ で一意に決まることになる．

ところが，量子一括測定に基づく復号戦略では，符号語状態間の干渉効果が式(4)の意味での記憶効果として現れ，最大伝送情報量は一般に超加法的 $C_{1,n} \geq nC_{1,1}$ となる． $C_{1,n}$ の具体的な表式を求めることは一般に難しいが，幸い $n \rightarrow \infty$ の極限での通信路容量の表式について，最近

$$C_{1,\infty} = \max_{p(x)} \chi(\mathcal{E}), \quad (11)$$

という解が与えられた⁸⁾⁻¹⁰⁾．ここで，

$$\chi(\mathcal{E}) = S \left(\sum_x p(x) \hat{\rho}_x \right) - \sum_x p(x) S(\hat{\rho}_x), \quad (12)$$

は文字集合 $\mathcal{E} = \{\hat{\rho}_x; p(x)\}$ に対するホレボー情報量¹¹⁾，

$$S(\hat{\rho}) = -\text{Tr} \hat{\rho} \log_2 \hat{\rho} \quad (13)$$

はフォン・ノイマンエントロピーである．この通信路容量 $C_{1,\infty}$ のことを特に積状態容量と呼ぶ．

文字状態がすべて可換な場合 $[\hat{\rho}_x, \hat{\rho}_{x'}] = 0$ には，系列状態全体にわたる量子操作の効果は特に現れず，

最適な復号戦略は個別測定となって，通信路容量は式(10)に帰着する．従来の情報理論で扱われてきた問題は，この場合に相当する． $[\hat{\rho}_x, \hat{\rho}_{x'}] \neq 0$ という非可換な場合に，シャノン理論の枠組みの背後にある量子力学の法則にのっとって，通信路容量の顕な表式を与えたのが式(11)である．

次に，符号化を式(6)のようなテンソル積状態に制限しないで， m 次拡大空間 $\mathcal{H}^{\otimes m}$ 上で任意の状態を許す場合について考える．この拡大空間上で，文字 x を運ぶ量子状態を $\hat{\Phi}_x^{\text{in}}$ とする．これをまた1つの文字状態と見なして，長さ n のテンソル積状態からなる符号化を考えることができる．その場合の積状態容量は

$$C_{m,\infty} = \max_{p(x), \hat{\Phi}_x^{\text{in}}} \chi(\{p(x), \hat{L}^{\otimes m}(\hat{\Phi}_x^{\text{in}})\}) \quad (14)$$

で与えられる．物理的には，十分長い出力状態系列 $\hat{L}^{\otimes m}(\hat{\Phi}_{x_1}^{\text{in}}) \otimes \hat{L}^{\otimes m}(\hat{\Phi}_{x_2}^{\text{in}}) \otimes \dots \otimes \hat{L}^{\otimes m}(\hat{\Phi}_{x_n}^{\text{in}})$ に対する量子一括測定を行っていることに相当する．量子通信路 \hat{L} に対する最終的な通信路容量は，入力状態のサポート空間のサイズ m を十分大きくとった極限で

$$C = \lim_{m \rightarrow \infty} \frac{C_{m,\infty}}{m} \quad (15)$$

と定義される．

4. 線形損失通信路の通信路容量

古典情報の伝送に使われる実用的媒体である電磁場に対して通信路容量(15)を求めたい．この問題は式(11)の結果が得られた直後から，これを連続ガウス通信路へ適用する問題として調べられた¹²⁾⁻¹⁴⁾．この場合，通信路に入れる信号のエネルギーに拘束条件を課し，そのもとでの通信路容量を考える．量子通信路 \hat{L} が恒等作用素となる理想的な場合については，それ以前にすでに Yuen と Ozawa によって通信路容量 C の表式とそれを達成する方法が与えられている^{15),16)}．理想的な場合なので，誤り訂正のための符号化は考える必要がない．問題となるのは，与えられたエネルギー拘束条件のもとで，どのような変調を行えば最大の情報量を送ることができるかという点である．その方法とは，光子数状態に離散的な文字を載せて伝送し，光子数識別器で測定するというものである．各光子数状態を用いる頻度は，エネルギー拘束条件に一致する平均エネルギーを持つボーズ・アインシュタイン分布に従って決める．

通信路に損失がある場合，この方法は最適解にはならない．最も簡単で現実的にも意味のある通信路は，線形損失通信路である．これは式(5)において環境系

の初期状態を真空状態とし、信号系がユニタリ作用素

$$\hat{U} = \exp \left[\sum_k \theta_k (\hat{a}_k^\dagger \hat{b}_k - \hat{b}_k^\dagger \hat{a}_k) \right] \quad (16)$$

によって環境系と混合するモデルで表される。 \hat{a}_k, \hat{b}_k はそれぞれ信号系、環境系の電磁場モード k に対する消滅作用素である。写像表現は

$$\hat{L}(\hat{a}_k) = \sqrt{\eta_k} \hat{a}_k + \sqrt{1 - \eta_k} \hat{b}_k \quad (17)$$

となる。ここで $\eta_k = \cos^2 \theta_k$ である。

最近、この線形損失通信路に対する通信路容量が求められた¹⁷⁾。エネルギー拘束条件

$$\sum_k \hbar \omega_k N_k = \bar{E}, \quad N_k = \langle \hat{a}_k^\dagger \hat{a}_k \rangle \quad (18)$$

のもとで通信路容量は

$$C_{\infty, \infty} = \max_{N_k} \sum_k g(\eta_k N_k) \quad (19)$$

で与えられる。ここで

$$g(x) = (x+1) \log_2(x+1) - x \log_2 x \quad (20)$$

である。この結果の証明では、式(14)の容量が

$$C_{1, \infty} \leq \frac{C_{m, \infty}}{m} \leq \max_{N_k} \sum_k g(\eta_k N_k) \quad (21)$$

のような不等式で挟まれ、ここでの上限と下限が一致することを用いている¹⁸⁾⁻²⁰⁾。特に、ここでの下限は入力をコヒーレント状態からなるテンソル積状態とし、その振幅の先験確率を

$$p_k(\alpha) = \frac{1}{\pi N_k} \exp \left(-\frac{|\alpha|^2}{N_k} \right) \quad (22)$$

というガウス分布としたときの積状態容量である。

したがって、入力側では量子もつれや光子数状態のような非古典的状态は必要なく、単にコヒーレント状態のテンソル積によって符号化を行えばよいことになる。実際、コヒーレント状態 $|\alpha\rangle$ は、位相のそろった古典的に最も綺麗な波で、振幅と位相の量子揺らぎの積も最小不確定状態にあり、これは線形損失を受けても変わらない。これが、入力側でコヒーレント状態が最適解となる理由であろう(ただし、これは必ずしも非古典的入力を否定するものではない。まだ、具体例は知られていないが、非古典的入力をうまく使って、より優れた漸近的特性で同じ通信路容量を達成する別の方法も存在しうる)。

一方、復号過程では、やはり量子一括測定が必要となる。実際、異なる振幅・位相を持つコヒーレント状態は一般に非可換 $[[|\alpha\rangle\langle\alpha|, |\beta\rangle\langle\beta|]] \neq 0$ で、このような状態はどんな理想的状況でも完全な識別は原理的に不可能である。最小の誤り率で信号を識別するために

は、受信過程で量子干渉効果をうまく活用する必要もある。系列状態を最適に復号するためにも、系列全体にわたる量子干渉効果を引き起こす必要がある。

ただし、許される信号エネルギー(エネルギー拘束条件(18)の \bar{E}) が大きい極限では非可換性の度合いが小さくなり、ヘテロダイン検波に基づく個別測定で漸近的にほぼ $C_{\infty, \infty}$ が達成できるようになる。量子一括測定による利得の効果は、 \bar{E} が小さくなるほど顕著になるが、それでも、通信路容量の値そのものは、式(19)の $C_{\infty, \infty}$ と従来のホモダイン検波に基づく個別測定での通信路容量 $C_{1,1}^{(H)}$ との間で数倍程度しか変わらない(\bar{E} が小さくなるとヘテロダイン検波よりホモダイン検波の方が有利になる)。

この数倍程度の容量の違いが実際の通信性能にどのように効いてくるのか、その答えは単純ではない。無限に速いデバイスで信号を処理できれば、単に通信速度が数倍程度改善されるだけだが、実際のデバイスの処理速度は有限で、しかも微弱な信号になるほど、信頼性を確保するために符号長を長くとる必要がある。符号長が長くなれば、それだけ復号に要する計算ステップ数も増えてゆくため、通信に時間がかかることになる。現在使われている接続符号の復号計算量は $O(n^2 \log^2 n)$ の程度であり、このような復号計算量まで考慮して実際の通信性能を評価する必要がある。想定する状況によって答えは千差万別であり、これ自体がまだ研究対象である。ここでは \bar{E} が非常に小さい場合に、入力を2値のコヒーレント状態で近似して大まかな外挿を試みる。変調方式はレーザ光の位相を 180° ずらすことで0, 1を変調する方式を取り上げ、受信側の信号パワーがパルスあたり平均0.4光子という極端に微弱な状況を想定する。深宇宙光通信などで直面する状況である。当然、手の込んだ符号化が必須となる。符号化効率を表すレートとして、現在の光符号の上限に近い値 ($R=0.635$ ビット/シンボル) を想定する。誤り率 10^{-9} という通常のエラーフリーの基準値まで達しようと思うと、従来の光符号では33万桁もの長さの符号を用いなければならないが、 $C_{\infty, \infty}$ (ここでは2値コヒーレント信号に対する $C_{1, \infty}$) を達成できる量子一括測定を用いると550桁で済んでしまうという予測となる。このような大幅な符号長の短縮は、復号計算量が $O(n^2 \log^2 n)$ 程度とすると実効的な伝送速度を100万倍程度改善できることになる。ただし、量子一括測定を構成する量子ゲートが現在のトランジスタの処理速度と同程度といったちょっと無理な仮定がなされている。このような予測が現実のものになるのはいつの時代か定かではないが、たとえ小規

モードでも量子一括測定が実現できれば、従来の光符号と組み合わせることで、通信性能は着実に向上してゆく。

5. 量子一括測定

量子一括測定とは、一言でいえば式 (3) のような量子もつれ状態への射影である。測定器への入力のコヒーレント状態のテンソル積からなる符号系列であり、それを量子もつれ状態へ射影する過程とは、入力のテンソル積状態に適切なユニタリ変換を施して量子もつれ状態を形成してから、あるテンソル積状態へ射影する、つまり個別測定を行う過程と読み替えることができる。それはコヒーレント状態に対して行う量子計算そのものといってよい。コヒーレント状態に対しては、量子計算はおろか単純な重ね合わせ状態すらまだ生成されていない。したがって、技術的にはまったくの未踏領域である。

一方、理論上も、POVMとして与えられた量子一括測定を具体的な量子回路として構成的に書き下す方法はまだ見つかっていない。量子一括測定の典型的な例として、平方根測定というものがある。それは、信号状態 $\{|\Psi_x\rangle\}$ に対して

$$|\Pi_x\rangle \equiv \left(\sum_y P(y) |\Psi_y\rangle \langle \Psi_y| \right)^{-\frac{1}{2}} \sqrt{P(x)} |\Psi_x\rangle \quad (23)$$

のように定義される $POVM\{|\Pi_x\rangle \langle \Pi_x|\}$ で表される。式 (11) の結果を導く際に復号戦略として用いられた測定でもある。 $|\Psi_x\rangle = |\rho_{x_1}\rangle \otimes \dots \otimes |\rho_{x_n}\rangle$ のような系列状態に対して、 $POVM\{|\Pi_x\rangle \langle \Pi_x|\}$ を実現するにはどうしたらよいのか。 $n = 2, 3$ までのごく限られた例で、その回路構成が示されているだけである^{(21)~(23)}。

量子一括測定に関するこれまでの実験的研究は、我々による光子の偏光や経路の自由度を使った2モードの制御にとどまっている。それは最も簡単な超加法的符号化利得 $C_{1,2} > 2C_{1,1}$ を実験的に実証するもので、究極の通信路容量の実現を目指すうえでの最初の一步である⁽²³⁾。文字状態として2次元系の3値信号 $|\psi_0\rangle = |0\rangle$, $|\psi_1\rangle = -\frac{1}{2}|0\rangle - \frac{\sqrt{3}}{2}|1\rangle$, $|\psi_2\rangle = -\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$ を用いるペレス-ウッターズ (Peres-Wootters) 符号を取り上げる⁽²⁴⁾。この3元対称信号 $\{|\psi_x\rangle \langle \psi_x|\}$ は互いに非可換である。非可換な量子状態で運ばれる信号は、雑音がまったくない理想的な状況でも原理的に完全に識別することは不可能である^{(6),(7)}。このような文字状態を接続してできる系列状態の最適な復号は量子一括測定となる。一方、個別測定による従来限界は $C_{1,1} = 0.645$ [bit] であることが知られている⁽²⁵⁾。こ

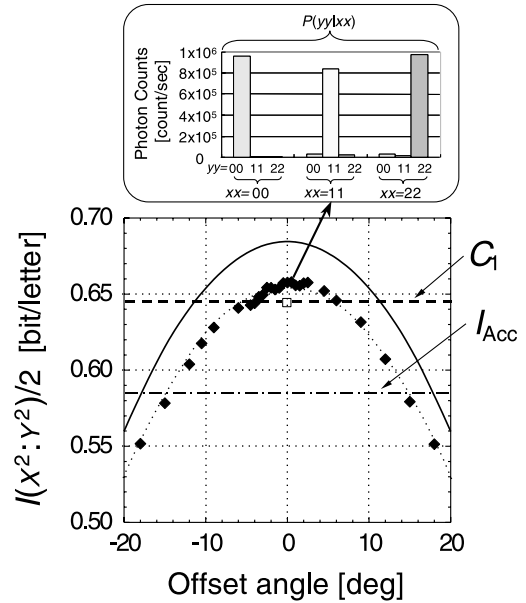


図1 上図：通信路行列 $P(yy|xx)$ に対するヒストグラム。下図：超加法的量子符号化利得の実験結果
Fig.1 Upper: Histogram of the channel matrix $P(yy|xx)$. Lower: Experimental result of the superadditive quantum coding gain.

れらの文字状態を2つ接続してできる合計9種類の積状態の中から

$$|\Psi_{xx}\rangle = |\psi_x\rangle \otimes |\psi_x\rangle, (x = 0, 1, 2) \quad (24)$$

の3つを選んで符号語とし、それぞれ先験確率 $1/3$ で用い、式 (23) の平方根測定によって復号する。このような符号化によって、 $I(X^2 : Y^2) = 1.3690$ [bit]、すなわち $I(X^2 : Y^2)/2 - C_{1,1} = 0.0391$ [bit] という超加法的符号化利得が得られる。 $C_{1,2} > I(X^2 : Y^2)$ という自明の関係から、 $I(X^2 : Y^2)/2 > C_{1,1}$ を実験的に実証すればよい。

この長さ2の符号化を、光子の偏光 (P) と経路 (L) の自由度を使って $|\Psi_{xx}\rangle = |\psi_x\rangle_P \otimes |\psi_x\rangle_L$ のように構成して、光子の偏光と経路間にわたる量子もつれの制御を行ったあとで光子検出を行う。そのための量子回路は、偏光マッハ-ツェンダー干渉系となる⁽²³⁾。単一光子による符号化-復号化の試行を何度も繰り返した統計的なデータから、通信路行列を見積もり、そこから相互情報量が求められる。図1が最終的に得られた実験データである。縦軸が取り出された情報量を自由度あたりに換算して表したもので、横軸が実験のパラメータで、信号ベクトルと測定ベクトル間の相対的なオフセット角度を、理想値の 0° からわざと前後に振らせて情報量の変化を見ている。実線が理論曲線で黒の点が実験データ、水平の破線が従来理論の限界

(シャノン限界 $C_{1,1}$) である。破線の上にわずかに飛び出ているギャップが超加法的量子符号化利得の証拠である。つまり、光子の符号空間を 2 倍にしたとき、2 倍以上の情報量が伝送されていることを示している。

現在の技術でできる量子的な符号化操作はここまでである。残念ながら実際の通信で使われる信号フォーマットからはほど遠いし、単一光子といってもレーザー光を十分弱く減衰させたものを用いているため、信号パルスのタイミングを定期的に制御できていない。ランダムに到来する光子を用いて量子復号回路のシミュレーションを行っているレベルである。

実用的なコヒーレント状態に対する量子符号化のためには、制御されたタイミングで入ってくるパルス列 $|\alpha_1\rangle \otimes \dots \otimes |\alpha_n\rangle$ に量子操作を施し、いくつか候補となる符号語パターンからなる適切な重ね合わせ状態（量子もつれ状態） $\sum_{x_1, \dots, x_n} c_{x_1, \dots, x_n} |\alpha_{x_1}\rangle \otimes \dots \otimes |\alpha_{x_n}\rangle$ を生成する必要がある。これはとりもなおさず、多モードのシュレーディンガの猫状態を受信器の中に作るということにほかならない。光の伝播モードでシュレーディンガの猫状態を生成することは、量子光学における積年の夢であり、そのような状態を量子回路で自在に生成して処理することは、量子情報科学の長期的な目標の 1 つである。しかし、そのためにはまだまだ明らかにならなければならない多くの問題がある。

6. 光のガウス操作と非ガウス操作

まず簡単のため、 $\{0, 1\}$ を 2 値の位相変調信号 $\{|\alpha\rangle, |-\alpha\rangle\}$ (α は実数) で伝送する方式を考える。現在最も高い感度の検出方式はホモダイン検波である。これは生成・消滅作用素 \hat{a}, \hat{a}^\dagger から $\hat{X} \equiv (\hat{a} + \hat{a}^\dagger)/\sqrt{2}$ と定義される直交振幅作用素の固有基底 $|x\rangle$ ($\hat{X}|x\rangle = x|x\rangle$) に射影する操作として表現され、出力はガウス分布

$$|\langle x|\pm\alpha\rangle|^2 = \frac{1}{\sqrt{\pi}} \exp\left[-\frac{(x \mp \sqrt{2}\alpha)^2}{2}\right] \quad (25)$$

に従う。0, 1 の生起確率が等しい場合、ビット誤り率は

$$P(1|0) = P(0|1) = P_e^{(H)} = \frac{1}{2} \operatorname{erfc}(\sqrt{2}\alpha) \quad (26)$$

と与えられる。

一方、入ってきた信号状態をいったん適切なユニタリ変換 \hat{U} によって変換してからホモダイン検波を施す場合、出力確率分布は $|\langle x|\hat{U}|\pm\alpha\rangle|^2$ となる。もし、 \hat{U} を生成するハミルトニアンが少なくとも生成・消滅演算子の 3 次以上の非線形過程を含む場合には、ホモダイン検波の誤り率限界を超えられることが知られて

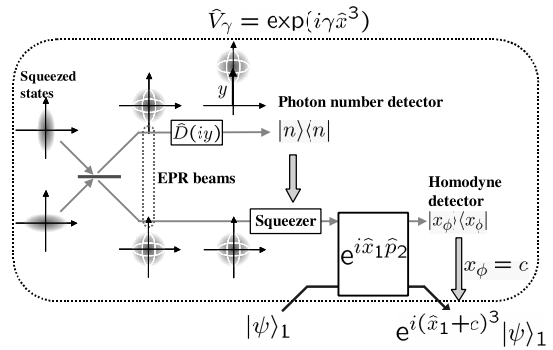


図 2 3 次の位相ゲートをスクィーズド光と光子数識別器およびホモダイン測定に基づいて実現する方法
Fig. 2 Realization method of the cubic phase gate using squeezed lights, photon number detector, and homodyne detector.

いる²⁶⁾⁻²⁸⁾。逆に、生成・消滅演算子の 2 次までの過程で生成される変換 $\hat{U}^{(2)}$ では、 $|\langle x|\hat{U}^{(2)}|\pm\alpha\rangle|^2$ はガウス分布のままであり、その枠内で通信路行列の扱いをいくら工夫しても、従来のホモダイン検波の限界を超えることはできない。その場合、通信路容量は式 (26)、式 (1) で与えられる $C_{1,1}$ となり、これが現在の光通信の最終的限界となる。

量子通信の領域に入るためには、生成・消滅演算子の 3 次以上の非線形過程を含む操作、いわゆる非ガウス操作が必要となる。実際には、生成・消滅演算子の 3 次以上を含むハミルトニアン、たとえば、3 次の位相ゲート $\hat{V}_\gamma = \exp(i\gamma\hat{x}^3)$ やカー効果 $\hat{U}_\gamma = \exp(i\gamma\hat{a}^\dagger\hat{a}^2)$ など、どれか 1 つでも手に入れば、それを従来のガウス型制御と組み合わせることで任意の次数の非線形ハミルトニアン、つまりは任意の量子回路を原理的に実現できることが知られている²⁹⁾。したがって、まずはこのような非線形ゲート実現することが重要な課題となる。このような非線形過程を光子レベルで低損失で実現する必要があるが、自然の材料や人工的なデバイスでは至難の技である。

そういった中で、現在考えられている方法は測定誘起型非線形過程である³⁰⁾。それは光子数測定が持つ非線形性を使おうというものである。実際、光子数状態への射影は高次のモーメントが関与する非線形な量子状態変換を引き起こす。これを用いて 3 次の位相ゲートを実現する方法を図 2 に示す³¹⁾。まず、2 つのスクィーズド光をビームスプリッタで合波して量子もつれ状態 (EPR ビームとも呼ばれる) を生成し、一方のビームに位相平面状でのシフト操作 $\hat{D}(iy)$ を加えてから、光子数測定を行う。測定結果に応じたスクィージングをもう一方のビームに施してやってから、実際

に処理したい信号状態 $|\psi\rangle_1$ をガウス型のハミルトニアンを通じて相互作用させてやり、今度は一方のビームをホモダイン測定してやると、その結果に応じて、3 次の位相シフトを引き起こすことができるというものである。点線の部分は、オフラインで実行すればよいので、3 次の位相シフトをユニタリな過程として誘起できることになる。こういった操作で鍵となるのは、高品質の量子もつれ状態の生成と高精度の光子数識別技術である。

スクィーズド光からなる量子もつれ状態は、これまでに量子テレポーテーション³²⁾ や量子稠密符号化³³⁾ といった量子プロトコルで使われ、その技術レベルも年々向上している。これに対して光子数識別技術は、その重要性にもかかわらずまだまだ多くの開発課題を残している。

7. 光子数識別技術

光子数識別技術に対しては、これまでいろいろな方式が試されている。特に、可視帯ではこれまでで最も高い量子効率で、非古典的な光子統計を評価できる光子数識別器 (VLPC) が報告されている³⁴⁾。ほかには量子ドット配列を組み込んだ電界効果トランジスタ (FET) による光子検出器³⁵⁾、超伝導エッジセンサ³⁶⁾、市販の Si-APD をカスケードに配列した光子検出器^{37),38)} などがあり、それぞれにメリットとデメリットとがある。

現在、我々が取り組んでいるのはこれらとは異なり、低雑音の光電変換と電荷蓄積型の読み出し回路を用いた光子数識別器で Charge Integration Photon Detector の頭文字をとって CIPD と呼んでいる。図 3 に示すように、最初の受光部では雪崩増幅ではなく線形増幅による低雑音の光電変換を行う。出てきた光電子は低雑音の積分型読み出し回路で電圧信号のステップへ変換し、このステップの飛びから光子数を読み出すという方式である。出力電圧はだまかには

$$V_{\text{Sig}} = \frac{Q \cdot G_M}{C_S} \quad (27)$$

で与えられる。 Q は光電子の電荷、 G_M は初段アンプの変換特性を決めるゲイン、 C_S は回路全体の浮遊容量である。 V_{Sig} が回路全体の電圧雑音 V_{Noise} より十分大きくなっていれば高い SN 比で光子数を識別できる。したがって、 G_M をできるだけ高く、 C_S と V_{Noise} をできるだけ小さく抑えることになる。

CIPD は、VLPC で問題となっていた高い暗計数を、時間幅の長い光パルスに対しても十分低く抑えられる点、量子ドット配列 FET や超伝導エッジセンサ

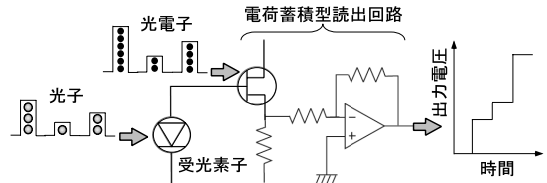


図 3 電荷蓄積型光子数識別器 (CIPD) の回路構成図
Fig. 3 Schematic of the charge integration photon detector.

では達成が難しい高量子効率を実現できる点、読み出し回路は現在の半導体デバイスで実装でき、受光デバイスを付け替えることで広い波長領域をカバーできる点などのメリットを有している。ただし、動作温度は 77 K あるいは 4 K という低温で、動作速度も現在のところまだ数 10 Hz と遅い。

ここでは、通信波長帯用 CIPD について紹介する。このほか、可視・近赤外帯用の CIPD にも取り組んでいるが、詳細は文献 39) に譲る。受光部は InGaAs の p-i-n フォトダイオードを、初段のアンプには GaAs JFET を使用し、熱雑音や漏れ電流の低減化を図るために液体ヘリウム温度まで冷却する。フォトダイオードの量子効率は現在 80% 強である。この波長帯では、読み出し速度が現在 40 Hz 程度であるが、光子数分解能が 1 光子を切って光子数識別できる領域に入ってきた。 $G_M \approx 1$ 、 $C_S = 0.057$ pF であり、1 電荷で発生する電圧ステップは $3 \mu\text{V}$ 程度である。識別感度は、SN 比で 2 以上、暗計数は 0.14 個/秒まで下げること成功した。超伝導を使わないタイプでは、世界最高レベルの低雑音特性である⁴⁰⁾。

図 4 (a) に 40 Hz の繰返しで微弱光パルスを測定した際の出力電圧ステップのヒストグラムを示す。図中の 0, 1 は対応する光子数 (正確には入力換算光電子数) である。分布の広がりを読み出し回路の雑音による。この識別性能を基に微弱光領域での Poisson 光子統計分布の測定の結果を図 4 (b) に示す。パルスあたりの平均光電子数が 1.58 から 10.2 の例を示しており、図中の破線は Poisson 分布の理論曲線である。ヒストグラムと理論曲線により一致が見られ、光強度を高い線形性で検出できていることが分かる。今後の課題は、光子数分解能と繰返しレートをさらに向上させ高量子効率化を図って、光子対状態やスクィーズド状態の非古典的光子統計を直接計測することである。

8. POVM の実現化理論

このような光子数識別技術を量子もつれ状態と組み合わせると汎用的な量子情報操作が原理的に可能にな

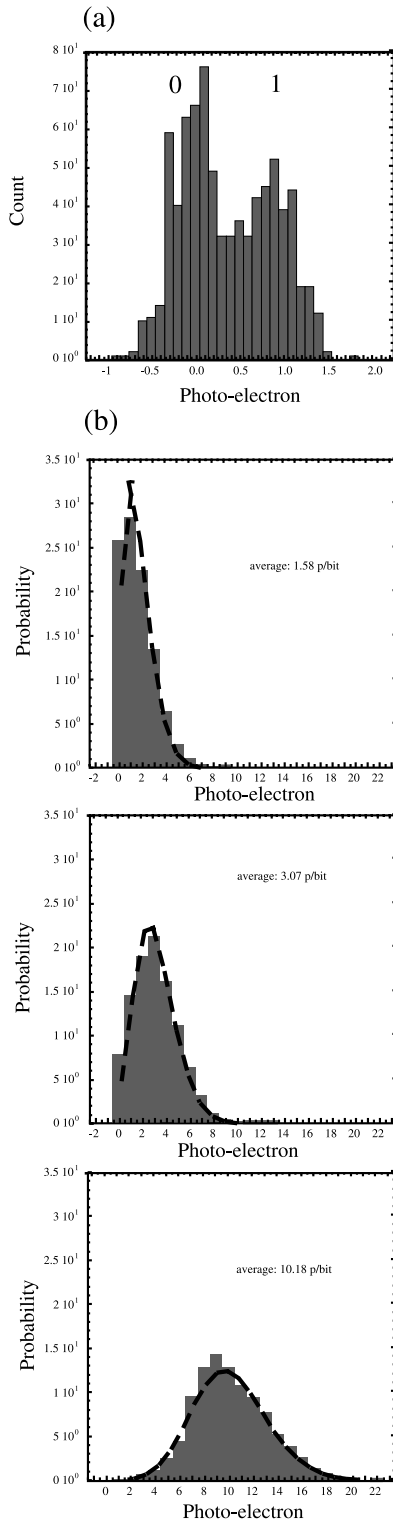


図 4 (a) 40 Hz における出力電圧ステップのヒストグラム . (b) 微弱光領域での Poisson 光子統計分布

Fig. 4 (a) Histogram of output voltage steps at 40 Hz. (b) Poisson photon number statistics in a faint light region.

る．それに先立って光子数識別技術と従来のコヒーレント光通信の技術を組み合わせるだけでも、実は重要な量子操作を実現できることが分かってきた．それは、任意の 2 値量子測定が、光子数識別器、補助系としてのコヒーレント状態、ビームスプリッタ、および高速の電気的フィードフォワード制御の組合せで実現できるというものである．特に、この場合、光子数識別器は完全な光子数分解能を持つ必要はなく、できるだけ高い量子効率とできるだけ低い暗計数で光子の到来を識別できれば十分である．

この知見につながる基本的なアイデアは、2 値位相変調コヒーレント信号 $\{|\alpha\rangle, |-\alpha\rangle\}$ を最小のビット誤り率で識別する方法として、すでに 1973 年に Dolinar によって提案されていた⁴¹⁾．その最小誤り確率は、1967 年 Helstrom によって

$$P_e^{\min} = \frac{1}{2} \left(1 - \sqrt{1 - |\kappa|^2} \right), \quad (28)$$

で与えられ (ただし $\kappa \equiv \langle \alpha | -\alpha \rangle$)、これを達成する測定は

$$\begin{aligned} |\alpha\rangle &= \sqrt{1 - P_e^{\min}} |\omega_0\rangle - \sqrt{P_e^{\min}} |\omega_1\rangle, \\ |-\alpha\rangle &= \sqrt{P_e^{\min}} |\omega_0\rangle - \sqrt{1 - P_e^{\min}} |\omega_1\rangle, \end{aligned} \quad (29)$$

で定義される正規直交基底 $\{|\omega_0\rangle, |\omega_1\rangle\}$ への射影となることが示されていた⁶⁾．この記述は数学的には簡潔だが物理的意味が判然としない．これに対して Kennedy は、信号状態を非対称なビームスプリッタを介して強いコヒーレント光と合波させ、 $\{|\alpha\rangle, |-\alpha\rangle\}$ をいったん $\{|0\rangle, |-2\alpha\rangle\}$ という状態にシフトさせてから、光子の有無を検出すれば、ヘルストローム限界とわずかに 2 倍程度しか変わらない誤り率特性 ($P_e^{(K)} = e^{-2|\alpha|^2}/2$) を実現できることを示した⁴²⁾．ドリナーは、このケネディ方式の中で、コヒーレント光の強度と位相を光子検出結果に応じてフィードフォワードすることで、ヘルストローム限界を厳密に実現できることを証明した．ちなみに、6 章で出てきたユニタリ変換 \hat{U} をうまく選んでやることで、やはりヘルストローム限界を実現できることが示されている⁴³⁾．

ドリナーは動的計画法などの最適制御理論を使って、フィードフォワードのパラメータを導出し、ヘルストローム限界に到達できることを証明した．一方、我々は複雑な最適化法を必要としないより簡単な設計指針によってドリナー方式が導かれることを示した⁴⁴⁾．

問題の定式化は、与えられた 2 つの「直交状態」の識別が、光子数識別器、補助系としてのコヒーレント状態、ビームスプリッタ、および高速の電気的フィードフォワード制御の組合せで実現できるかという形

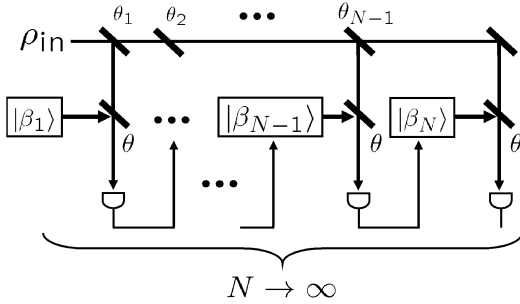


図5 光子検出，補助のコヒーレント状態，フィードフォワードによる2つの直交状態の識別

Fig.5 Discrimination of binary orthogonal states using photon detection, ancillary coherent states and feed-forward controls.

でなされる．実際，2値コヒーレント信号を例にとると，式(29)から分かるように，直交状態 $\{|\omega_0\rangle, |\omega_1\rangle\}$ を完全に識別できれば，もともとの非直交な信号状態も最小誤り率で識別できることになる．直交状態 $\{|\omega_0\rangle, |\omega_1\rangle\}$ を完全に識別するためには，測定過程の途中においてこれらの状態がつねに直交性を保たなければならない．この直交条件が基本的な設計指針である．

さらにこの方法を使うと，任意の直交する2組の量子状態の完全な識別が上記の物理系のみで実現できることを示すことができる．今，2つの直交状態を

$$|\Psi\rangle = \sum_{m=0}^{\infty} c_m |m\rangle_0, \quad |\Phi\rangle = \sum_{m=0}^{\infty} d_m |m\rangle_0, \quad (30)$$

と表す．ここで $|m\rangle$ は m 光子状態で $\langle\Psi|\Phi\rangle = \sum_{m=0}^{\infty} c_m^* d_m = 0$ である．この状態を図5のような反射率 $\sin^2\theta = 1/N$ の非対称な $N-1$ 個のビームスプリッタからなる光学回路で N 個のモードに分離する．分離された状態は

$$\begin{aligned} & \hat{B}_{N-1,0}(\theta_{N-1}) \cdots \hat{B}_{1,0}(\theta_1) |0\rangle^{\otimes N-1} |\Psi\rangle_0 \\ &= e^{-\hat{a}_{N-1}^\dagger \hat{a}_0} \cdots e^{-\hat{a}_1^\dagger \hat{a}_0} \\ & \times e^{\hat{a}_0^\dagger \hat{a}_0 \ln(1/\sqrt{N})} |0\rangle^{\otimes N-1} |\Psi\rangle_0, \end{aligned} \quad (31)$$

のように書かれる．ここで

$$\hat{B}_{n,0}(\theta_n) = \exp[\theta_n (\hat{a}_n^\dagger \hat{a}_0 - \hat{a}_n \hat{a}_0^\dagger)] \quad (32)$$

$$\tan\theta_n = \frac{1}{\sqrt{N-n}}. \quad (33)$$

である．それぞれのポートでは，タップしたビームを反射率 $\sin^2\theta = 1/N$ のビームスプリッタを介して補助系のコヒーレント状態 $|\beta_n\rangle$ と合波させ， $\hat{D}(\beta_n/\sqrt{N})$ で記述されるシフト操作を施してから光子検出を行う．

β_n は，前段までの光子検出履歴に応じて決定する．十分大きな N に対しては，各ポートで2個以上の光子が検出される確率は無視できて，たとえば，1段目のビームスプリッタ通過後の状態は

$$\hat{B}_{1,0}(\theta_1) |0\rangle_1 |\Psi\rangle_0 \approx |0\rangle_1 |\eta_0\rangle_0 + \frac{1}{\sqrt{N}} |1\rangle_1 |\eta_1\rangle_0, \quad (34)$$

$$\hat{B}_{1,0}(\theta_1) |0\rangle_1 |\Phi\rangle_0 \approx |0\rangle_1 |\nu_0\rangle_0 + \frac{1}{\sqrt{N}} |1\rangle_1 |\nu_1\rangle_0. \quad (35)$$

と書かれる．ここで $\langle\eta_0|\nu_0\rangle + \langle\eta_1|\nu_1\rangle/N \approx 0$ となる．次にモード1を測定するが，その際，2つの入力 $|\Psi\rangle$ ， $|\Phi\rangle$ に対応する測定後の状態 $|\Psi'\rangle$ ， $|\Phi'\rangle$ が直交するよう測定過程を設計する．具体的には，

$$|\pi_0\rangle = M_c |0\rangle - \frac{M_s e^{i\varphi}}{\sqrt{N}} |1\rangle, \quad (36)$$

$$|\pi_1\rangle = \frac{M_s e^{-i\varphi}}{\sqrt{N}} |0\rangle + M_c |1\rangle, \quad (37)$$

なる形の射影測定を行えばよい．ここで M_s, M_c, φ は $c_i^* d_j$ の関数である．実はこの測定が，上述のシフト操作 $\hat{D}(\beta_n/\sqrt{N})$ と光子検出器で構成できる．実際，図5の1段目の測定はベクトル

$$\hat{D}^\dagger\left(\frac{\beta_1}{\sqrt{N}}\right) |0\rangle \approx e^{-|\beta_1|^2/2N} \left(|0\rangle - \frac{\beta_1}{\sqrt{N}} |1\rangle \right), \quad (38)$$

$$\hat{D}^\dagger\left(\frac{\beta_1}{\sqrt{N}}\right) |1\rangle \approx -e^{-|\beta_1|^2/2N} \left(\frac{\beta_1^*}{\sqrt{N}} |0\rangle + |1\rangle \right), \quad (39)$$

で表され， β_1 を適切な選ぶことで式(36)，(37)の測定を構成できることが分かる．さらに，測定後の量子状態 $|\Psi'\rangle$ ， $|\Phi'\rangle$ は測定結果がどちらであった場合でも

$$|\Psi'\rangle = \sum_{m=0}^{\infty} c'_m |m\rangle, \quad |\Phi'\rangle = \sum_{m=0}^{\infty} d'_m |m\rangle. \quad (40)$$

の形式で記述できるので，2段目以降の測定も同様の戦略で繰り返してゆけばよく， N の十分に大きい極限ならば最後の N 段目の射影測定により $\{|\Psi\rangle, |\Phi\rangle\}$ を誤りなく識別できるのである．

以上の議論では単一モードの光の量子状態について論じたが，2つの直交状態がエンタングルド状態にあるなど多モードにわたっていても結論は変わらない．あらゆる2値の直交状態はモードごとの局所的な射影測定のみで識別できることがすでに知られているので⁴⁵⁾，上記の N 分割による測定をモードごとに順次行っていけばよいのである．

9. ま と め

電磁場を伝送媒体とする線形損失通信路のモデルは、きわめて汎用的なモデルである。その通信路容量に到達するための究極の通信システムを実現する鍵は、入力側での量子的制御ではなく、受信側におけるコヒーレント状態に対する量子一括測定である。量子一括測定は、たとえ小規模でも従来の光符号化と組み合わせることで通信性能を大きく改善する。このいわゆる量子-古典ハイブリッド符号化は、量子的処理の性能と規模が向上するにつれ、着実に通信性能の改善が期待できる。

超加法的符号化利得の原理実証を終えて、現在はコヒーレント信号に対する小規模量子一括測定を実現するため研究フェーズに入っている。その第一歩として、測定誘起型非線形過程の概念を述べ、その中でも今後の重要課題として我々が取り組む光子数識別器の結果について議論した。

また、その最初の応用例として、任意の2つの光の量子状態を識別する量子最適受信器の構成理論を提案した。それは、高い量子効率と低い暗計数のオンオフ検出器と補助系としてのコヒーレント状態、ビームスプリッタ、および高速の電気的フィードフォワード制御を組み合わせるものである。光の2値測定は、デジタル通信の最も基礎的な技術であるし、量子情報光学の分野でもベル不等式の破れの検証など重要な応用があり、それが光子数識別器と現在の技術を組み合わせて実現できるという知見の意義はきわめて大きい。

参 考 文 献

- 1) Shannon, C.E.: *Bell System Tech. J.*, Vol.27, pp.379-423 (Part I), pp.623-656 (Part II) (1948).
- 2) Gallager, R.G.: *Information Theory and Reliable Communication*, J. Wiley, New York (1968).
- 3) Cover, T. and Thomas, J.: *Elements of Information Theory*, John Wiley and Sons, New York (1991).
- 4) Kraus, K.: *States, Effects and Operations*, Springer-Verlag, Berlin (1983).
- 5) Nielsen, M.A. and Chuang, I.L.: *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge (2000).
- 6) Helstrom, C.W.: *Quantum Detection and Estimation Theory*, Academic Press, New York (1976).
- 7) 広田 修: 光通信理論, 森北出版 (1985).
- 8) Hausladen, P., et al.: *Phys. Rev.*, A54, 1869 (1996).
- 9) Holevo, A.S.: *IEEE Trans. Inf. Theory* IT-44, 269 (1998).
- 10) Schumacher, B. and Westmoreland, M.: *Phys. Rev.*, A56, 131 (1997).
- 11) Holevo, A.S.: *Probl. Peredachi Inform.*, 9(3), 3 (1973).
- 12) Holevo, A.S.: *Tamagawa University Research Review*, 4, 1 (1998); (extended version, LANL e-print arXiv:quant-ph/9809023).
- 13) Holevo, A.S., Sohma, M. and Hirota, O.: *Phys. Rev.*, A59, 1820 (1999).
- 14) Sohma, M. and Hirota, O.: *Recent Research and Developments in Optics*, Vol.1, p.146, Research Signpost, Trivandrum, India (2001).
- 15) Yuen, H.P. and Ozawa, M.: *Phys. Rev. Lett.*, 70, 363 (1993).
- 16) Caves, C.M. and Drummond, P.D.: *Rev. Mod. Phys.*, 66, 481 (1994), and referebces therein.
- 17) Giovannetti, V., Guha, S., Lloyd, S., Maccone, L., Shapiro, J.H. and Yuen, H.P.: *Phys. Rev. Lett.*, 92, 027902 (2004).
- 18) Holevo, A.S. and Werner, R.F.: *Phys. Rev.*, A63, 032312 (2001).
- 19) Giovannetti, V., Lloyd, S., Maccone, L. and Shor, P.W.: *Phys. Rev. Lett.*, 91, 047901 (2003); *Phys. Rev.*, A68, 062323 (2003).
- 20) Bennett, C.H., DiVincenzo, D.P. and Smolin, J.A.: *Phys. Rev. Lett.*, 78, 3217 (1997).
- 21) Sasaki, M., Kato, K., Izutsu, M. and Hirota, O.: *Phys. Rev.*, A58, 146 (1998).
- 22) Sasaki, M., Usuda, T.S., Izutsu, M. and Hirota, O.: *Phys. Rev.*, A58, 159 (1998).
- 23) Fujiwara, M., Takeoka, M., Mizuno, J. and Sasaki, M.: *Phys. Rev. Lett.*, 90, 167906 (2003).
- 24) Peres, A. and Wootters, W.K.: *Phys. Rev. Lett.*, 66, 1119 (1991).
- 25) Osaki, M., Ban, M. and Hirota, O.: *Quantum Communication, Computing and Measurement 2*, Kumar, P., D'Ariano, G.M. and Hirota, O. (Eds.), Kluwer academic/Prenum publishers, New York, 17 (2000).
- 26) Usuda, T.S. and Hirota, O.: *Quantum Communication and Measurement*, Belavkin, Hirota and Hudson (Eds.), pp.419-427, Plenum Publishing, New York (1995).
- 27) Sasaki, M., Usuda, T.S. and Hirota, O.: *Phys. Rev.*, A51, 1702 (1995).
- 28) Sasaki, M. and Hirota, O.: *Phys. Rev.*, A54, 2728 (1996).
- 29) Lloyd, S. and Braunstein, S.L.: *Phys. Rev. Lett.*, 82, 1784 (1999).
- 30) Knill, K., Laflamme, R. and Milburn, G.J.: *Nature*, 409, 46 (2001).

- 31) Gottesman, D., Kitaev, A. and Preskill, J.: *Phys. Rev.*, A64, 012310 (2001).
- 32) Furusawa, A., Sørensen, J.L., Braunstein, S.L., Fuchs, C.A., Kimble, H.J. and Polzik, E.S.: *Science*, 282, 706 (1998); Zhang, T.C., Goh, K.W., Chou, C.W., Lodahl, P. and Kimble, H.J.: *Phys. Rev.*, A67, 033802 (2003); Bowen, W.P., Treps, N., Buchler, B.C., Schnabel, R., Ralph, T.C., Bachor, H.A., Symul, T. and Lam, P.K.: *Phys. Rev.*, A67, 032302 (2003).
- 33) Li, X., Pan, Q., Jing, J., Zhang, J., Xie, C. and Peng, K.: *Phys. Rev. Lett.*, 88, 047904 (2002). Mizuno, J., Wakui, K., Furusawa, A. and Sasaki, M.: *Phys. Rev.*, A71, 012304 (2005).
- 34) Waks, E., Diamanti, E., Sanders, B.C., Bartlett, S.D. and Yamamoto, Y.: *Phys. Rev. Lett.*, 92, 113602 (2004).
- 35) Shields, A.J., O'Sullivan, M.P., Farrer, I., Ritchie, D.A., Hogg, R.A., Leadbeater, M.L., Norman, C.E. and Pepper, M.: *Appl. Phys. Lett.*, 76, 3673 (2000).
- 36) Miller, A.J., Nam, S.W., Martinis, J.M. and Sergienko, A.V.: *Appl. Phys. Lett.*, 83, 791 (2003).
- 37) Achilles, D., Silberhorn, Ch., Sliwa, C., Banaszek, K. and Walmsley, I.A.: *Opt. Lett.*, 28, 2387 (2003).
- 38) Fitch, M.J., Jacobs, B.C., Pittman, T.B. and Franson, J.D.: *Phys. Rev.*, A68, 043814 (2003).
- 39) Akiba, M., Fujiwara, M. and Sasaki, M.: *Opt. Lett.*, 30, 123 (2005).
- 40) Fujiwara, M. and Sasaki, M.: *Appl. Phys. Lett.*, 86, 111119 (2005).
- 41) Dolinar, S.J.: *Quarterly Progress Report*, No.111, p.115, Research Laboratory of Electronics, MIT (1973). 詳細は文献 6), 44) や Geremia, J.M.: quant-ph/0407205 (2004) などを参照.
- 42) Kennedy, R.S.: *Quarterly Progress Report*, No.108, pp.219–225, Research Laboratory of Electronics, MIT (1973).
- 43) Sasaki, M. and Hirota, O.: *Phys. Lett.*, A210, pp.21–25 (1996).
- 44) Takeoka, M., Sasaki, M., van Loock, P. and Lütkenhaus, N.: *Phys. Rev.*, A71, 022318 (2005).
- 45) Walgate, J., Short, A.J., Hardy, L. and Vedral, V.: *Phys. Rev. Lett.*, 85, 4972 (2000).

(平成 17 年 6 月 28 日受付)

(平成 17 年 7 月 4 日採録)



佐々木雅英

昭和 37 年生・平成 4 年東北大学大学院理学研究科物理学専攻課程修了, 博士(理学). 同年日本鋼管(株)(現 JFE ホールディングス)綾瀬研究所入社. Si MOS デバイスの研究に従事. 平成 8 年郵政省通信総合研究所(現独立行政法人情報通信研究機構)入所. 光変調器, 量子情報通信の研究に従事. 現在, 同機構基礎先端部門量子情報技術グループリーダー. 日本物理学会会員.



藤原 幹生

昭和 42 年生・平成 4 年名古屋大学大学院工学研究科電子工学専攻修士課程修了. 同年郵政省通信総合研究所(現独立行政法人情報通信研究機構)入所. 以来, 遠赤外検出器, クライオジェニックエレクトロニクス, 微弱光検出研究開発に従事. 博士(理学). 電子情報通信学会, 応用物理学会, 日本物理学会各会員.



武岡 正裕

昭和 48 年生・平成 13 年慶應義塾大学大学院理工学研究科修了, 博士(工学). 同年総務省通信総合研究所(現独立行政法人情報通信研究機構)入所. 量子情報理論とその実験的実証, 量子光学等の研究に従事. 日本物理学会会員.