連続量変数の光量子計算と量子情報通信

武　岡　正　裕

Continuous-Variables Optical Quantum Computation and Quantum Communication

Masahiro TAKEOKA

We discuss the physical processes necessary for constructing continuous-variables (CV) optical quantum computing. Particularly, the importance of non-Gaussian quantum operations is pointed out. As a practical mean to implement such operations, we introduce a scheme of "measurement-induced nonlinearity." Finally, as an application of CV quantum computation, we discuss the topic of quantum communication which necessarily requires quantum computation on CV quantum states.

Key words: continuous-variables quantum computation, non-Gaussian operation, measurement-induced nonlinearity, quantum collective decoding, quantum optimal receiver

光を使った量子計算は，光子の偏光や位置などの離散的な自由度を使うアプローチに加えて，その一般化となる光の連続量を使ったアプローチも広く研究されている[1)]．連続量とは，連続的な値をもつ観測物理量を指し，光の電磁波としての直交位相振幅（複素振幅）などがこれに相当する．光の連続量量子状態の量子計算を追求する動機はいくつか挙げられる．まず，連続量の量子状態は，量子ビットのような離散量の自然な拡張であり，基礎学問的な興味があるだろう．任意の計算が可能な万能量子計算機を作るには，それを可能にする基本ゲートのセットが必要である[*1]．光の連続量量子状態のそれを明らかにすることは，結局あらゆる光の量子状態に対する任意のユニタリー変換（状態変換）を可能にする物理過程のセットを明らかにするという基本問題と等価である．

一方，実際上の面でも，高量子効率が容易に達成できるホモダイン検出が使えること，またいくつかの量子情報処理プロトコルでは，成功した事象のみを採用するポストセレクションとよばれる方法を必要としないことなどの利点がある．また，単一光子状態などの離散的光量子ビットの光源は人為的な工夫と技術の産物であるのに対し，現実の世界では，熱分布した光やレーザーのコヒーレント光など，多くの光は連続量にまたがる状態である．そして，実用上重要な点は，こうした連続量の光量子状態を用いざるを得ない応用があるという点である．

本稿では，連続量変数の量子計算について概説する．まず，連続量変数の万能量子計算を可能にする一般的な物理操作，特にガウス型操作と非ガウス型操作について整理する．後半ではその応用として，光の連続量量子状態制御を必要とする量子通信，特に量子符号化，量子受信機について紹介する．

1.　光の連続量万能量子計算

ここでは，光の量子状態およびその状態変換がガウス型，非ガウス型の2種類に分類されることと，万能量子計算機を構成するにあたってそれらの果たす役割について述べる．簡単のため，単一モードの光の量子状態を考えよ

（独）情報通信研究機構第一研究部門新世代ネットワーク研究センター（〒184-8795 小金井市貫井北町 4-2-1）　E-mail: takeoka@nict.go.jp

[*1] ゲートを直接必要としないクラスター量子計算の概念については，本特集号の解説記事を参照．最近では，連続量のクラスター量子計算も理論的に検討されている．

う．光（電磁波）の量子状態はさまざまな方法で記述できるが，量子状態の密度行列 $\hat{\rho}$ に対して，$W(x,p)=(2\pi)^{-1}\int_{-\infty}^{\infty}\mathrm{d}y e^{\mathrm{i}py}\langle x-y/2|\hat{\rho}|x+y/2\rangle$ のように定義されるウィグナー関数を用いると便利である．ここで x，p は電磁波の位相平面における cos，sin 成分の軸に対応する．ウィグナー関数は $\int\mathrm{d}x\int\mathrm{d}pW(x,p)=1$ のように規格化された関数であり，量子ゆらぎが位相平面においてどのように分布しているかを直感的に把握することができる．ただし，このウィグナー分布は正確には確率分布ではなく，光子数確定状態などのきわめて強い非古典性をもつ状態では，負の値をとることがある擬似確率分布である．また，例えば $P(x)=\int\mathrm{d}pW(x,p)$ のようにそのある 1 軸を積分すると，この $P(x)$ は確率分布となり，これはその状態に対してホモダイン測定を行った場合に得られる直交位相振幅の値の確率分布に対応している．

連続量の量子状態は，ウィグナー関数がガウス分布で表されるような状態をガウス状態とよび，それ以外を非ガウス状態とよんでしばしば区別される．簡単のため，熱分布のような統計的混合状態を除いて，純粋状態に限ってこれらを分類してみる．レーザーから生成されるコヒーレント状態やその直交位相振幅がゼロの真空状態，そして直交位相振幅の片方の量子雑音を圧搾したスクイーズド状態がガウス状態に属する．一方，これらを除く状態はすべて非ガウス状態であり，有限の光子数確定状態や，異なる位相，振幅をもつコヒーレント状態の重ね合わせ状態（いわゆるシュレーディンガーの猫状態）などがこれに相当する．これらの定義は多モードの量子状態に対しても同様である．

概して（純粋状態では）非ガウス状態のほうがより非古典性の強く，実験的にも高い精度で生成することは難しい．また，ガウス状態は，通常のガウス分布がそうであるように期待値と分散，つまり一次と二次のモーメントのパラメーターさえわかれば一意に特徴づけられる．一方，非ガウス状態は一般にウィグナー関数の形がすべてわからなければならず，別のいい方をすれば，量子状態により多くの情報が含められているともいえる．

次に，これらの状態を量子計算の観点からより厳密に特徴づけよう．量子計算は量子状態の変換であると冒頭で述べたが，量子状態を変換する操作についても，先の状態同様に分類される．すなわち，ガウス状態を他のガウス状態へと変換するような操作はガウス型量子操作とよばれ，それ以外，つまりガウス状態を非ガウス状態へと変換するような操作は非ガウス型量子操作とよばれる．

光の量子状態におけるガウス型操作と非ガウス型操作の分類は，非線形光学過程と密接に対応している．ここでは簡単のため，ユニタリー変換についてのみ考えることにする．純粋状態のガウス状態は，上述のようにコヒーレント状態とスクイーズド状態のことであるから，これらの状態間を自在に変換するには，線形光学操作，およびスクイージング操作があればよい．具体的には，線形過程である位相シフト，ビームスプリッター，変位操作*2，そしてスクイージングを行う二次の非線形光学過程（光パラメトリック過程など）があれば，任意のガウス型操作が実現できる．また，ホモダイン検出も理想的には無限にスクイズされた状態への射影であり，ガウス型操作に相当する．これらはすべて技術的にもよく確立されている操作である．

非ガウス型操作は上記以外の操作なので，三次以上の非線形過程がすべて含まれることになる．例えば，三次の非線形過程の光カー効果などである．ガウス型操作だけでは万能量子計算機として片手落ちなことは明らかだが，加えてガウス型操作のみで構成された量子計算機では，古典計算機の計算速度をしのげないことがすでに明らかにされている[2)]．では，どのような非ガウス型操作が必要か，ということだが，実は何か 1 種類の非ガウス型操作さえあれば，それとガウス型操作を無数に組み合わせることで，原理的には任意の次数の非線形過程，つまり万能操作が実現できることが知られている[3)]．しかも，この非ガウス型操作は何でもよいので，例えば自己位相変調のような単一モードに対する操作でかまわない．

2. 測定誘起非線形過程

すると，次はどのような非ガウス型操作が実現できそうかということになる．しかし，三次以上の非線形光学過程を，光子レベルの微弱光に対して低損失で実現するのは現在の技術ではきわめて難しい課題である．そこで，この非線形過程を実効的に実現するために期待されているのが，測定誘起非線形過程とよばれる概念である．これは，量子状態の非局所的な相関（エンタングルメント）と非ガウス型の検出器を使って，実効的に強い非線形過程を誘起するという考え方である．例えば，光子数識別器，光子検出器などが非ガウス型検出器である．光子検出だけでは入力量子状態は破壊されてしまうが，エンタングルした 2 つのモードの間で片方に対して測定を行えば，その結果に応じて残ったモードの状態が非局所的に変化する．この性質を使えば，片方のモードで非ガウス型の測定を行うことで，残

*2 位相平面上で状態をシフトする操作．補助的なコヒーレント局発光を 99：1 のような非対称なビームスプリッターで干渉させることにより実現できる．

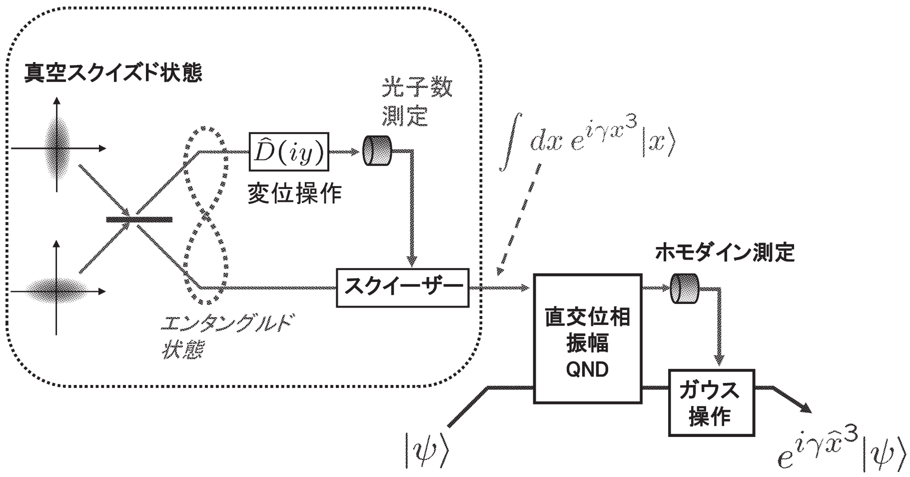

図1　三次位相ゲートの構成法．QND：量子非破壊測定．

ったモードに実効的に非線形な状態変換を施せるのである．

具体例を挙げる．ガウス状態である真空スクイーズド状態をビームスプリッターで分割すると，2つの出力はエンタングルする．このときの反射率を数% 程度にしてその反射光の光子を測定し，光子が検出された場合の透過モードの状態を選択的に取り出すと，光のシュレーディンガーの猫状態 $|\alpha\rangle \pm |-\alpha\rangle$ を近似的に生成することができる[4]．これは典型的な非ガウス状態であり，α や重ね合わせの符号は検出された光子数に依存して変化する．これは近年実験で実証されており（詳細，文献は本特集号の解説記事を参照），また最近では，光子を検出する前に干渉光を入れて検出光子数を不確定にし，異なる光子数状態の重ね合わせへ射影するより制御性の高い過程も提案され[5,6]，実験も実現しはじめている[7]．

以上の例は，ガウス状態の入力を非ガウス状態へと変換しているが，光子が検出されたときのみ動作することからわかるように本質的に確率的な状態変換である．しかし，このような確率的な変換では，失敗した場合の量子情報はすべて失われてしまうため，量子計算のゲートとして直接用いることはできず，少なくとも原理的には確率1で動作するゲートが求められる[*3]．実は測定を用いていても，原理的にはそれは可能である．そのようなゲート構成方法として，次に三次位相ゲート (cubic phase gate) とよばれるものを紹介する[8]．

図1は，三次位相ゲートの構成方法である．基本的な考え方は，まず非ガウス型の補助状態を確率的な方法で準備し，これを入力の状態と（確率的でない）ガウス型操作で相互作用させることにより，実効的に非ガウス型操作を入力状態に施すというものである．補助状態には計算途中の量子情報は何も含まれていないので，その生成に失敗しても何ら問題なく，いわば計算のオンライン上ではなく，オフラインにおいて確率的な操作をすませてしまうというものである．具体的には，まず2つのスクイーズド状態を使ってガウス型のエンタングルド状態を作り，その一方に変位操作を施してから光子数を測定する．測定された光子数が変位量とほぼ等しい場合，もう片方の状態にさらに適当なスクイージングを施すことで，$\int dx \exp(i\gamma x^3)|x\rangle$ という直交位相振幅 x に対する三次の非ガウス状態が生成される．まずは，この補助状態の生成に成功するまでこの過程を繰り返し，成功したらそれと入力の信号状態を（直交位相振幅の）量子非破壊測定とよばれるガウス型操作で相互作用させる．さらに，2つの出力のうち片方をホモダイン測定して，その結果に応じてもう片方の出力に適当なガウス操作を施してやれば完成である．このゲートにより，出力には，入力状態に $\hat{U}=\exp(i\gamma\hat{x}^3)$ という直交位相振幅に対する三次の非線形位相シフトが施された状態が現れる．

以上をまとめると，原理的には，線形素子，ホモダイン検出器，スクイージングを組み合わせれば任意のガウス型量子ゲートが可能で，これに光子数識別器を組み合わせれば，原理的には確率1の非ガウス型量子ゲートが実現できる．そして，さらにこれらガウス型・非ガウス型の量子ゲートを適切に組み合わせることで，連続量における任意の量子操作，すなわち万能量子計算が可能となる．

[*3] 実際には実験上の不完全性によるデコヒーレンスがあるが，それはある程度までは量子誤り訂正によって回避できる．

3. 連続量量子計算と量子情報通信

前章では，光の連続量万能量子計算に必要な物理過程と，万能量子ゲート構成の一例を紹介した．連続量の光量子計算が，将来素因数分解等のいわゆる量子計算を行う最有力候補かどうかはわからない．例えば，連続量ではどのような状態に情報をエンコードするのかという問題がある．理論的には，直交位相振幅の固有状態（無限にスクイズされた状態）を用いるのが見通しがよいが，現実にはスクイズできる量は有限なので，その実現化は必ずしも容易ではない．では，非ガウス型操作を含む連続量の量子情報処理は実際にはまずどのような場面で役に立つのか．ここではその一例として，通信に関する量子符号化，量子受信機の概念について紹介する．

このため，量子計算から少し離れて，問題の背景から述べる．現在の光通信では，レーザー光を強度変調し直接検波する方式が主流だが，さらに次世代の方式として光の波の性質まで利用したコヒーレント光通信も実用化されつつある．コヒーレント光通信で用いるホモダイン検波では局発光との干渉によりレーザーや検出器の雑音が除去され，受信感度は光自身がもつ量子ゆらぎによる制限，すなわちショット雑音限界まで比較的容易に到達可能である．さらに通信システム全体では，これらの送受信機の前後でメッセージを符号化，復号化することで誤り訂正を行い，その性能で通信路容量が決まっている．ショット雑音の影響は微弱信号の領域で顕著であり，実用上では，深宇宙通信など超長距離で減衰（線形損失）の著しい通信路において重要な課題である．最近の衛星通信のフィールド試験では，すでに受信端で平均100光子を切るような量子レベルに近い微弱光が用いられている．

しかし，上記のコヒーレント光通信は，光信号のもつ量子ゆらぎを極限まで制御したものとはいえない．こうしたコヒーレント光通信の性能限界を打破し，量子力学で許される最大の通信性能を実現するのが，量子符号化技術である．量子ゆらぎの支配的な微弱光領域において極限的な性能を達成するためには，与えられた量子通信路に対して，送信キャリヤー，受信方式，さらには符号化・復号化まですべてを含めて量子力学的に最適化する必要がある．この最適化は一般的には非常に難しい数学問題だが，先の例の線形損失通信路では，最近になって厳密な解答が与えられている[9]．これは，物理的なキャリヤーが量子力学に従った振る舞いをする限り超えられない通信限界であり，その意味である種究極の通信路容量といえる．その数学的な内容は文献に譲ることとして，ここではその性能限界の達成に必要な物理過程について述べる．

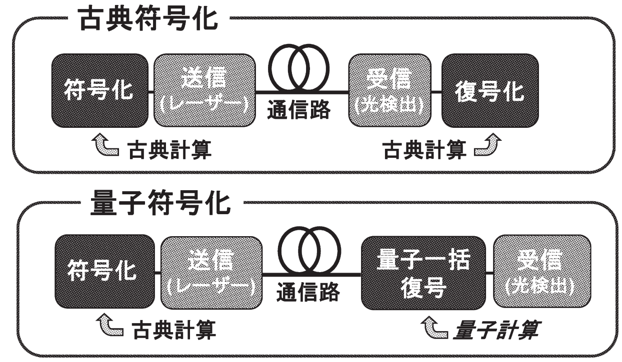

図2　古典符号化（上）と量子符号化（下）の概念図．

まず，送信側の最適な信号は，コヒーレント状態からなるテンソル積状態，つまり通常のレーザー光のパルス列をガウス分布に従う連続変数で変調して符号化を行えばよいことがわかっている．非古典的な状態はむしろ損失にきわめて弱くすぐに壊れてしまうため，通信のキャリヤーに向かないのである．しかしながら，コヒーレント状態自身のもつ量子ゆらぎは避けられない．信号を劣化させる量子ゆらぎは，$\langle\alpha|-\alpha\rangle=\exp(-2|\alpha|^2)$ のように状態ベクトル間が互いに非直交であることに由来している．

この量子ゆらぎによる信号識別性能の劣化を極限まで抑えて最大の通信路容量を達成するためには，むしろ受信および復号操作を量子力学的に最適化する必要がある．具体的には，受信端に入ってきたコヒーレント光パルスを個別に測定して古典的計算機で復号化するのではなく，量子計算を行いながら復号していくというものである．この復号は，数学的にはコヒーレント信号列 $|\alpha_1\rangle\otimes\cdots\otimes|\alpha_n\rangle$ の重ね合わせ，すなわち $\sum_x|\alpha_1^x\rangle\otimes\cdots\otimes|\alpha_n^x\rangle$ のように信号全体にわたりエンタングルした直交基底への射影測定の形で書かれ，量子一括復号，または量子一括測定などとよばれている．実際にはこの一括測定は，個々のパルス間に何らかの相互作用を順次施していくことで構成されると考えられ，また信号はコヒーレント状態の連続的な振幅に符号化されているから，これは連続量に対する量子計算にほかならない．線形損失通信路は現実的かつ非常に汎用的なモデルであり，連続量の量子計算が，素因数分解等のいわゆる量子計算のアルゴリズム以外でも応用上非常に重要であることを示す一例である．古典符号化と量子符号化の概念を図2で比較する．

ところで，古典情報理論における連続通信路の通信路容量が漸近論による理想的な性能限界であるのと同様に，上述の量子符号化における通信路容量も無限に長い符号と量子復号を仮定しており，現実には離散的な変調（ただしコヒーレント光自身は連続量量子状態）と有限の長さの量子

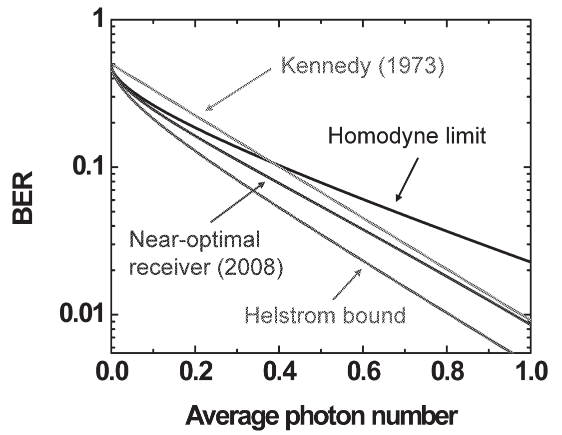

図3　各種測定のビットエラーレートと量子限界．BER：ビットエラーレート，Average photon number：信号の平均光子数，Helstrom bound：ヘルストローム限界（量子限界），Homodyne limit：ホモダイン限界，Kennedy (1973)：ケネディの準最適量子受信機，Near-optimal receiver (2008)：筆者らの提案する準最適量子受信機．

一括復号を行うことになる．量子一括復号による利得の実験的検証は，最もシンプルな長さ2の符号を光子の偏光等を用いて構成することによりなされている[10)]．しかし，これはまだ原理実証の段階で，実用的なコヒーレント信号に関しては，量子計算を行う基本ゲートの具体的な構成もまだ不透明であり，量子一括復号の実験も未だ実現されていない．

現時点で問題がある程度具体化され，また実現の可能性も高いのは，1つのコヒーレント光パルスに対する最適な量子測定であろう．これは量子一括復号ではないが，1つの信号に対する量子計算ということができるし，また本質的に非ガウス操作を必要とする．最も簡単な具体例は，等しい先験確率で飛来する二値位相変調（BPSK）信号 $\{|\alpha\rangle, |-\alpha\rangle\}$ を最小のビットエラーレート（BER）で識別する，というものである．先のコヒーレント通信では，ガウス操作であるホモダイン測定により識別され，理想的なBERは $P_e^{\mathrm{H}}=(1/2)\mathrm{erfc}(|\alpha|^2)$ となることはよく知られている．しかも，このホモダイン限界は，ガウス操作のみをいくら組み合わせても超えられないことが最近証明されている[11)]．だが，もちろんこれは本当の量子限界ではない．ヘルストローム限界とよばれる量子力学的に許される最小の誤り率は，

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

$$|\omega_1\rangle=\sqrt{\frac{P_e^{\min}}{1-\kappa^2}}\,|\alpha\rangle-\sqrt{\frac{1-P_e^{\min}}{1-\kappa^2}}\,|-\alpha\rangle \qquad (2)$$

のような重ね合わせ状態への射影測定で実現される（詳細や原著論文は文献12）などを参照）．これは非ガウス操作である．ただし $\kappa=|\langle\alpha|-\alpha\rangle|$，$P_e^{\min}=(1-\sqrt{1-\kappa^2})/2$ は最小誤り率である．

問題は，現実のデバイスでこれをどのように近似的に実現するかである．実はこのような量子受信機の実現化は，1970年代の先駆的な研究でいくつか提案されていたが（詳細，原著論文等は文献12）などを参照），検出器の性能などの問題もあり，実際にホモダイン限界を超えるBERを示した実験は未だに実現されていない．筆者らは最近，これらの先行研究をもとにして，現在の先端技術でホモダイン限界を超えることが可能な量子受信機を提案している[11)]．それは70年代にケネディによって提案された方式[12)]を改良したもので，次のように構成される．まず，非ガウス操作には，光子の有無のみを検出する光子検出器を用いる．これは理想的には，真空とそれ以外の光子数 $\{|0\rangle\langle 0|, \sum_{n=1}^{\infty} 1|n\rangle\langle n|\}$ へと射影する検出器である．信号は，まず前述の変位操作により位相平面の実軸上で γ だけシフトした後に，光子検出される．したがって，全体ではコヒーレント状態 $|\gamma\rangle$ とそれに直交する状態の空間への射影測定になっている．シフト量 γ は，測定の誤り率が最小になるように最適化する．

この量子受信機の設計の基本概念は，以下のようなものである．式（1），（2）の最適な射影測定は連続量だが，ここで問題としているのは微弱信号，特に平均光子数が1以下となるようなものである．そこで，$|\omega_0\rangle$ を光子数基底で $|\omega_0\rangle\propto|0\rangle+(\sqrt{1-P_e^{\min}}+\sqrt{P_e^{\min}})/(\sqrt{1-P_e^{\min}}-\sqrt{P_e^{\min}})\,\alpha|1\rangle+\cdots$ のように展開する．一方，提案する量子受信機も同様に $|\gamma\rangle\propto|0\rangle+\gamma|1\rangle+\cdots$ と展開できるから，$\gamma\to(\sqrt{1-P_e^{\min}}+\sqrt{P_e^{\min}})/(\sqrt{1-P_e^{\min}}-\sqrt{P_e^{\min}})$ と選ぶことで，0，1光子状態に関しては近似的に最適な量子測定が実現できるのである．厳密には多光子状態の係数も考慮に入れると，$\alpha=\gamma\tanh(2\alpha\gamma)$ を満たす γ が最適な値となる．それぞれの測定が理想的な場合のBERの比較を図3に示す．

この方式で実験系の不完全性も含めた数値計算を行うと，ホモダイン限界を超えるためには，おおまかにいって量子効率90%，ダークカウント 10^{-3} の光子検出，局発光との99.5%程度のモード整合が必要であることがわかる．これらの達成は現在の技術でも決して楽な数字ではないが，最近の超伝導光子数識別器などの開発の進展[13)]をみれば，十分期待がもてる．量子受信機は現在の光通信から量子通信，そして連続量計算による量子情報処理へとつながる自然な研究の道のりであろう．

本稿では，連続量光量子計算の基本的な枠組みと，そのひとつの応用となる量子情報通信について紹介した．連続量光量子計算の理論は，光の量子状態を任意に制御する際に必要な物理過程を体系的に明らかにするものであり，量子計算そのものの実現に向けた研究も興味深いが，通信をはじめさまざまな光量子情報プロトコルを設計する際の基本的な指針を提供するものとしても大いに期待される．

文　　献

1) S. L. Braunstein and P. van Loock: "Quantum information with continuous variables," Rev. Mod. Phys., **77** (2005) 513–577.
2) S. D. Bartlett, B. Sanders, S. L. Braunstein and K. Nemoto: "Efficient classical simulation of continuous variable quantum information processes," Phys. Rev. Lett., **88** (2002) 097904.
3) S. Lloyd and S. L. Braunstein: "Quantum computation over continuous variables," Phys. Rev. Lett., **82** (1999) 1784–1787.
4) M. Dakna, T. Anhut, T. Opatrný, L. Knöll and D.-G. Welsch: "Generating Schrödinger-cat-like states by means of conditional measurements on a beam splitter," Phys. Rev. A, **55** (1997) 3184–3194.
5) M. Takeoka and M. Sasaki: "Conditional generation of an arbitrary superposition of coherent states," Phys. Rev. A, **75** (2007) 064302.
6) A. E. B. Nielsen and K. Mølmer: "Transforming squeezed light into a large-amplitude coherent-state superposition," Phys. Rev. A, **76** (2007) 043840.
7) H. Takahashi, K. Wakui, S. Suzuki, M. Takeoka, K. Hayasaka, A. Furusawa and M. Sasaki: "Generation of large-amplitude coherent-state superposition via ancilla-assisted photon-subtraction," Phys. Rev. Lett., **101** (2008) 233605.
8) D. Gottesman, A. Kitaev and J. Preskill: "Encoding a qubit in an oscillator," Phys. Rev. A, **64** (2001) 012310.
9) V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, J. H. Shapiro and H. P. Yuen: "Classical capacity of the lossy bosonic channel: The exact solution," Phys. Rev. Lett., **92** (2004) 027902.
10) M. Fujiwara, M. Takeoka, J. Mizuno and M. Sasaki: "Exceeding classical capacity limit in quantum optical channel," Phys. Rev. Lett., **90** (2003) 167906.
11) M. Takeoka and M. Sasaki: "Discrimination of the binary coherent signal: Gaussian-operation limit and simple non-Gaussian near-optimal receivers," Phys. Rev. A, **78** (2008) 022320.
12) 佐々木雅英，松岡正浩監修：量子情報通信（オプトロニクス社，2006）第1部第4章，第4部第3章など．
13) A. E. Lita, A. J. Miller and S. W. Nam: "Counting near-infrared single-photons with 95% efficiency," Opt. Express, **16** (2008) 3032–3040.

（2008年9月3日受理）