7　量子通信技術

7 Quantum Communication Technologies

7-1　量子通信路符号化のための量子検出回路

7-1 Quantum detection circuit for quantum channel coding

佐々木雅英　　水野　潤　　藤原幹生
Masahide SASAKI, Jun MIZUNO, and Mikio FUJIWARA

要旨

現在の情報技術の主要な搬送媒体である光は、波であるとともにエネルギーの粒、光子の集合体でもある。現在の光通信技術は、光がエネルギーの束として伝播するという性質しか使っておらず、波としての性質すら使ってはいない。光の波の性質を積極的に活かした通信は、コヒーレント光通信として現在、研究が進展しつつある。従来の通信理論はコヒーレント光通信の領域までは問題なくカバーでき、明確な性能限界を与える。

しかし、光通信の最終的な性能限界は、光子の従う量子力学の法則によって課されることになる。こういった領域でのシステム設計と最終的な性能限界を与えるのは量子情報理論であり、従来理論の限界を超える新しい通信領域の可能性が予言されている。量子通信路の伝送容量を決めているのは、光の量子状態の識別限界である。本稿では、量子暗号等で用いられる最も基本的な信号系である単一光子の対称偏波変調信号を取り上げ、そこから取り出せる最大情報量とそのための最適検出法を明らかにする。通常、偏波変調信号の識別は偏光子を使って行うが、単一光子状態に対してはvon Neumannn測定と呼ばれる偏光子に基づく2値出力の検出器が標準的である。これに対して量子情報理論が与える最適解は、信号成分の数によらず3値の出力を有する検出器であり、偏波干渉系によって構成することができる。この最適検出回路を開発しvon Neumannn限界を凌駕し理論限界の96%まで迫る検出性能の実証に成功した。

Ligth, main carrier in the present information technology, is electromagnetic wave, and also an ensemble of energy quanta, photon as well. At present only the fact is used that light propagagtes as an energy flux, and the wave nature of light is never used any more so far. Conventionsl information theory is readily capable of designing communication system based on the wave nature of light, and providing its performance limit. However the ulitimate performace limit of optical communication is eventually given by the law of quantum mechanics that governs photon dynamics.

Quantum channel capacity is then determined by the distinguishability of optical quantum states. In this article we consider one of the most basic quantum signal system, symmetric states of a single photon polarization, which is often used for quantum key distributiontion. It is clarified what is the maximum amount of information that can be extracted from that source and how one can implement the optimal detector for attaing it. Conventionally detection of polarization modulation signals is made by using a polarizer. For a single photon state, the binary output detection based on a polarizer is the standerd mesurement, which is called the von Neumann measurement. On the other hand the optimal solution in quantum information theory is given by the detector with three outputs at most regardless of the munber of the signal components. This type of detector can be implemented by the polarization interferometer. We developed such a detector and could demondtrate the 96% of the predected limit which is superior to the conventional von Neumann limit.

PACS　numbers:

1 序論

現在の情報技術は、0と1という二つの数字による抽象化の上に成り立っている。情報は0と1からなる系列によって表現され、系列間の遷移によって情報の伝送や処理が行われる。この操作を乱す雑音は、0－1間の確率的遷移としてモデル化される。{0, 1} を担うのは多くの電子、あるいは光子の集合体であり、その物理的状態は雑音が小さい極限では完全に識別できるという仮定がなされる。また、そのような状態は複製や増幅も可能である。このような仮定に立って情報理論は、確率事象に伴う曖昧さとして情報量を定義することによって、外乱の下での最適な情報伝送と信号処理を設計する強力な手段を与えてきた。

しかし、情報技術は今や原子一個、電子一個、あるいは光子一個といった量子力学的対象を直接操作する領域に入りつつある。{0, 1} を担う媒体の量子力学的性質が顕在化する領域では、状態を変えることなく複製や増幅を行うことは不可能であり[3][4]、状態間の完全な識別も（直交状態でない限り）一般に不可能となる[8][9]。このことは、情報技術に新たな原理的な性能限界を課す一方で、量子暗号という頑健な情報セキュリティーの原理を提供することにもなる。また{0, 1}の系列間の遷移によって行われる情報の伝送や処理には、必然的に確率振幅レベルでの量子力学的干渉効果が内在し、それを最適に制御することで、従来理論から外挿される限界を凌駕する性能が予言されてくる。情報理論はこのような極限まで含めて、量子力学の言葉で抽象化されなければならない。

また、量子光学の進歩は、原子スケールに特徴的だった量子相関を数10kmにわたって展開することを可能にし、さらには、それが従来に類似のない転送技術や暗号技術、信号処理技術へ応用できることを明らかにしつつある[1]。こうした中で、従来の情報理論における情報操作のモデル化や情報量の定義は、実はほんの一つの可能性にしか過ぎず、もっと広い情報の定義、新しい伝送・処理の方式が可能であることがわかってきた。これまでの情報技術の指導原理であった情報理論は、量子力学と合流し量子情報理論として統一される時を迎えている。

この量子情報理論が描く新しい情報技術の全貌はまだその一端が見えはじめたに過ぎない[2]。実現に向けた実験的原理検証に至っては、さらにそのごく一部しか手がつけられていないのが現状である。特に、あらゆる情報技術の根幹にある、ものの識別、つまり量子状態の識別問題は理論、実験ともに最も重要な問題の一つである。本稿では、究極の通信路容量の実現を目指す符号技術で本質的な役割を果たす相互情報量の最適化という観点からこの問題を概説し、最も単純な量子状態信号を取り上げ、最新の理論的・実験的成果を解説していく。

2 量子信号検出の基礎と相互情報量

情報理論の主題は二つに整理される。「如何に効率よく与えられたメッセージを0, 1で表現するか」、及び「如何に正確に0, 1の記号系列を伝送するか」である。通信の基本的なモデルでは、送信者（業界ではなぜかアリスと呼ぶ）が情報源S（例えば、送信したい一冊の本の内容）を持っており、その構成要素（例えば、アルファベット）$\{a, b, \ldots z\}$と対応する先験確率 $\{P(a), P(b), \ldots P(z)\}$ が既知であるとする。情報源Sは確率変数 $S=\{a, b, \ldots z ; P(a) ; P(b), \ldots P(z)\}$ として記述される。

アリスは情報源から出てきたメッセージを与えられた文字の集合 $\{x_i\}$（例えば、通常用いられる {0, 1}）からなる系列で表現する。実際の通信路を伝わっていくのはこれらの文字記号である。おのおののメッセージを表す文字記号の系列を符号語と呼び、メッセージから文字記号への変換を情報源符号化と呼ぶ。情報源符号化の性能は、平均符号長をどれだけ短くできるかで測られ、それはシャノンエントロピー

$$H(S) = -\sum_{A=a,b,\ldots} P(A)\log_2 P(A)\,. \qquad (1)$$

によって与えられるというのが情報理論の主張である。

通信路には必ず何らかの雑音が伴うのが普通である。情報理論は、こういった雑音下でも符

号語に更に冗長性を持ち込めば、受信側で誤り訂正が可能となり、信頼性のある情報伝送ができることを教える。情報源符号語に冗長性を加え再度符号化する操作を通信路符号化と呼ぶ。できるだけ少ない冗長性で、できるだけ信頼性の高い伝送を行いたい。誤りゼロの伝送を実現するためにどれだけの冗長性を付加する必要があるか、これを定量化するのが相互情報量である。

情報源符号器からの出力は、文字 $\{x_i\}$ からなる系列であるが、そこに現れる各文字の出現頻度 $P(x_i)$ は、情報源が持つメッセージの特性と使用している情報源符号化の仕方に応じて決まってくる。結局、ここで情報源符号器からの出力を特徴付ける確率変数 $X=\{x_i\,;P(x_i)\}$ を定義することができ、これが通信路への入力源となる。通信路の数学的モデルは、出力しうる文字記号 $\{y_j\}$ と入出力間の条件付確率 $P(y_j|x_i)$ によって与えられる。通信路への入力源 X、出力文字 $\{y_j\}$、及び通信路行列 $[P(y_j|x_i)]$ が与えられたとき、要求される伝送性能を実現する符号化、復号化の方法が存在するか否かを見極めるのが情報理論の重要な主題であり、ここで相互情報量が重要な役割を演ずる。

相互情報量は入力変数 X と出力変数 $Y=\{y_j\,;P(y_j)\}$ の間で定義される。ここで

$$P(y_j)\equiv\sum_{x_i}P(y_j|x_i)P(x_i) \tag{2}$$

は y_j が出力される確率である。まず入力変数が持つ不確定さは、先に述べたシャノンエントロピー

$$H(X)=-\sum_i P(x_i)\log P(x_i) \tag{3}$$

で定義される。今、受信者（なぜかボブと呼ぶ慣習となっている）が出力信号 y_j を観測したとしよう。ボブから見た X の不確定さはこの知識によって減ることになる。y_j が得られた後でのボブからみた確率分布は

$$P(x_i|y_j)=\frac{P(y_j|x_i)P(x_i)}{P(y_j)}. \tag{4}$$

で与えられる。この新しい確率分布をもとに出力変数によって条件付けされたエントロピーを

$$H(X|Y)=-\sum_{y_j}P(y_j)\sum_{x_i}P(x_i|y_j)\log P(x_i|y_j). \tag{5}$$

で定義する。これが出力情報が得られた後で残る X の不確定さを定量化する量となる。したがって、ボブによって引き出される情報量の定義として、受信過程の後で減ったエントロピー

$$\begin{aligned}I(X:Y)&=H(X)-H(X|Y)\\&=\sum_{x_i,y_j}P(x_i)P(y_j|x_i)\log\left[\frac{P(y_j|x_i)}{\sum_{x_i}P(x_i)P(y_j|x_i)}\right].\end{aligned} \tag{6}$$

を採用するのは非常に自然なことである。これが X と Y の間の相互情報量である。

さて、次に長さ n のブロック符号化を考える。情報源符号器からの出力は長さ $k(<n)$ のメッセージブロックからなる系列である。それぞれのブロックに長さ $n-k$ の誤り訂正用ブロックを付加して符号化する。伝送用の長さ n のブロック符号語を $\{\mathrm{x}^p\}$ とする：

$$\begin{aligned}\mathbf{x}^p&=\overbrace{x^p{}_1x^p{}_2\cdots x^p{}_k}^{\text{message block}}\overbrace{x^p{}_{k+1}x^p{}_{k+2}\cdots x^p{}_n}^{\text{correction block}}\\&\quad(\text{for } p=1,2,\ldots,L^k),\end{aligned} \tag{7}$$

ここでおのおのの $x^p{}_l\,(l=1,\ldots,n)$ は文字集合 $\{x_i\,;i=0,1,\ldots,L-1\}$ のどれかである。

入力符号語 x^p は通信路で雑音の影響を受け、一般には入力とは異なった系列 $\mathbf{y}^q=y^q{}_1y^q{}_2\ldots y^q{}_n$ として出力される。通信路復号器は、適当な誤り訂正を行った後で適切な符号語に復元する。ここで復号誤り確率はできるだけ小さくしたいし、一方で冗長性 $n-k$ はできるだけ小さいことが望ましい。いい換えると伝送レートと呼ばれる比 $R=k/n$ をできるだけ高く保ちながら、一方で、復号誤り確率をできるだけ小さくしたい。

ここで符号語の集合 $\{\mathrm{x}^p\}$ に現れる x_i の頻度を一定に保ったままで符号化を行うこととする。情報理論によれば、伝送レートを $R<I(X:Y)$ となるように保てば、復号誤り確率をいくらでも小さくできる符号化が存在する。与えられた通信路行列 $[P(y_j|x_i)]$ に対して、我々はさらに相互情報量を最大化するように先験確率を $\{P(x_i)\}$ を選ぶことができる。このときの最大値

$$C^{c} = \max_{\{P(x_i)\}} I(X:Y) \tag{8}$$

が通信路容量と呼ばれる。ここで伝送レートを$R < C^{c}$に保てば、復号誤り確率をいくらでも小さくできる符号化が存在する、と主張するのが通信路符号化定理である[5][6][7]。このように相互情報量は符号化を用いた通信路の究極的な使用法に直接関係した量である。

こういった情報理論の基本的枠組みは量子限界にさらされた通信路に対しても当てはめることができる。しかし、従来の理論にはない新しい要素が顔を出す。その最たるものは受信過程における量子効果である。量子力学的な受信過程は、数学的には確率作用素測度、probability operator measure（POM）という概念によって記述される。これは以下のように単位分解を構成する非負のエルミート作用素である[8][10][11]：

$$\hat{\Pi}_j^{\dagger} = \hat{\Pi}_j, \quad \hat{\Pi}_j \geq 0 \quad {}^{\forall}j, \quad \sum_j \hat{\Pi}_j = \hat{I}. \tag{9}$$

それぞれの要素$\hat{\Pi}_j$は、出力値jに対応しており、出力文字y_jを出力する。簡単のため文字$\{x_i\}$が純粋状態$\{|\psi_i\rangle\}$によって運ばれる場合を考える。この文字状態は一般には非直交状態である。このとき通信路モデルを決めるのは、POM$\{\hat{\Pi}_j\}$と通信路行列$P(y_j|x_i) = \langle\psi_i|\hat{\Pi}_j|\psi_i\rangle$である。

従来の枠組みでは通信路行列$[P(y_j|x_i)]$は、与えれる固定された量であったが、量子通信の領域では与えられた文字集合$\{|\psi_i\rangle\}$に対して最適な測定過程、つまりPOMがどのようになるかを問題とする。この問題は何段階かに分けて考えることができる。まず$\{|\psi_i\rangle\}$と$\{P(x_i)\}$を固定したときに、相互情報量を最大化するPOM$\{\hat{\Pi}_j\}$を探す必要がある。この最大値

$$I_{\mathrm{Acc}}\left(\{|\psi_i\rangle; P(x_i)\}\right) = \max_{\{\hat{\Pi}_j\}} I\left(\{|\psi_i\rangle; P(x_i)\}:Y\right) \tag{10}$$

は$\{|\psi_i\rangle; P(x_i)\}$に対する*accessible information*と呼ばれる。次にこのaccessible informationを先験確率$\{P(x_i)\}$で最大化した量を

$$C_1 = \max_{\{P(x_i)\}} I_{\mathrm{Acc}}\left(\{|\psi_i\rangle; P(x_i)\}\right). \tag{11}$$

と書く。ここまでは従来の単なる延長線上の話である。しかし、これが最終的な通信路容量になるわけではない。実際、量子力学的な復号過程では、量子状態間の干渉効果が存在し、これをうまく使うことによってさらに大きい通信路容量が予言されてくる。量子効果まで考慮した最終的な通信路容量はHausladenらによって与えられた[12]。混合状態まで含めた一般論はHolevo[13]とSchumacher及びWestmorelandによって与えられている[14]。

量子情報理論によって与えられたこの通信路容量に近い性能で、信頼性の高い情報伝送を実現するためには、実は復号の過程で量子計算が必要になる[15][16]。上記の通信路容量を与える符号化定理の証明の中では、暗黙のうちに文字状態信号間で行う量子計算の必要性が仮定されているのである。しかし、この復号過程で必要になる量子計算は、現在の技術水準に照らすと、その実現ははるか先の話になるほど困難なものである。量子計算が不可能な現状では、各文字状態信号ごとに直接、光－電気変換を行う個別量子測定に頼るしかない。その場合の、通信路容量の限界はI_{Acc}若しくはC_1によって与えられることになる。ここで再び符号語集合$\{\mathbf{x}^{p}\}$の中でx_i（つまり$\{|\psi_i\rangle\}$）の出現確率が$P(x_i)$となるような符号化を考える。$X=\{|\psi_i\rangle; P(x_i)\}$に対するaccessible informationを達成する信号検出過程の数学解（確率作用素測度、POM）を$\{\hat{\Pi}_j\}$とし、各文字状態信号に$\{\hat{\Pi}_j\}$を個別に施して復号を行うものとする。その際の出力系列を$\{y_{j1}y_{j2}\ldots y_{j_n}\}$とする。ここでもし伝送レートを$R < I_{Acc}$に保てば、適切な従来の古典的符号化法を用いて誤り確率をいくらでもゼロに近づけられることが保証されるわけである。この個別量子最適測定$\{\hat{\Pi}_j\}$と古典的符号化法を組み合わせたものが、当面の最高の通信性能を保証する方式となってくる。したがって、個別量子最適測定$\{\hat{\Pi}_j\}$を理論的に明らかにし、実験的に検証し、デバイス化していくことが重要な課題となってくる。

Accessible information達成のための最適検出過程を求める問題は、他の規範に基づく最適化問題とも関連している。受信者ボブにとってのおそらく最も基本的な最適化問題は、信号セット$\{|\psi_i\rangle\}$の各要素を最小の誤り確率P_eで識別する、というものであろう[17][18]。もう一つの重要

な規範としてボブが確率的で良いから、ある事象を一切の曖昧さなく確定したい、というものがある。この場合、あるフラッグのもとでは、受信信号は$|\psi_i\rangle$でしかありえないというように断定できるが、一方で別のフラッグが立てばなんら判断を下せないあいまいな状況を許すというシナリオになる[19]～[26]。この場合、断定不可能なフラッグが立つ確率P_iを最小化することになる。このタイプの信号検出は量子鍵配布で用いられる[27]。

一方、実際のメッセージの伝送では、むしろボブはアリスからできるだけ多くのメッセージを復元したいわけで、このことは必ずしもPe あるいはPi を最小化すればよいということを意味しない。この場合、直接的にはアリスの有する情報源、つまり確率変数$X=\{x_i, P(x_i)\}$の不確定さをできるだけ減らす測定法が最適となる。これこそが通信の最終的な性能を決する規範となり、具体的には効果的な符号化法の設計として表現されることになる。それを測るのが上で述べた相互情報量である。

ちなみに誤り確率最小化のための最適条件は良く知られているが[17][18]、これらの条件から最適解を導くのは一般にはかなり難しい問題である。実際、最適解は2元純粋状態や対称的信号といったごく限られた例でしか知られていない[15][17][18][28][29][30]。断定的測定でのP_i最小化については[25][26]にて議論が行われている。これに対して$I(X:Y)$を最大化する問題は、P_eやP_iの最小化問題に比べはるかに難しい問題である。それは$I(X:Y)$に含まれる対数関数という非線形関数をPOMといういわば行列を変数として最適化しなければならないからである。現在知られている最適解は、2元純粋状態[31][32]と実対称qubit信号[33][34]に限られている。

直観的にはより多くの情報を取り出すためには、P_eやP_iを最小化するのが良いように思われる。実際、2元純粋状態に対しては平均誤り確率最小化と相互情報量最大化は同じ最適解に帰着する。しかしながら、$I(X:Y)$、P_e、P_iいずれの最適化も全く異なるPOMによって実現される例も確実に存在する[33][34][35]。

こういった最適量子信号検出の実験的検証もいくつか報告されている。例えば、単一光子の

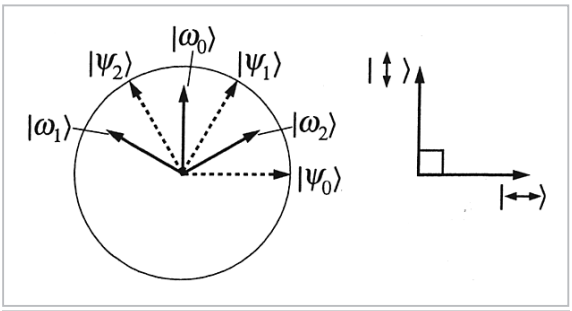


図1 3元信号の最適測定の測定ベクトル(実線)と信号ベクトル(点線)

偏波状態から作った2元状態信号識別の最小誤り確率[36]、同様の信号に対する断定的測定でのP_iの最小化[37][38]、3値、4値対称偏波信号の断定的測定[39]などである。

本論文では、実対称qubit 信号に対してRef.[34]で明らかにされた相互情報量最大化のための最適測定の実験的検証について解説する。3値信号については、すでにClarke *et al*が一部実証実験を行っている[39]。今回我々のグループでは測定精度を大幅に改善し、まだ実証されていなかった5値信号に対しての従来測定に対する測定利得の確認も行った。実対称qubit信号は、実用的には量子暗号鍵配布に使われる最も簡単な信号系のひとつである[40][41]。基礎的な興味としてはDavies の定理[33]の予言、相互情報量最適測定の出力数Nは信号空間の次元dによって$d \leq N \leq d^2$のようにバウンドされる、という効果を直接実験で検証するという意義がある。実信号に対してはこのバウンドはさらに$d \leq N \leq d(d+1)/2$まできつくする事ができる[34]。したがって、単一光子の偏波信号に対しては、信号数がいくつであっても常に最大3出力の測定を用意すれば、必ず最適解を構成できることが原理的には保証されている。

3 実対称qubit信号と最適測定

単一光子の線形偏波に基底を$\{|\leftrightarrow\rangle, |\updownarrow\rangle\}$とする。実対称信号は次のように定義される。

$$|\psi_i\rangle = \cos\frac{i\pi}{M}|\leftrightarrow\rangle + \sin\frac{i\pi}{M}|\updownarrow\rangle \quad (i=0,\ldots,M-1). \tag{12}$$

それぞれの要素は等確率$1/M$で用いられるものとする。この信号セットが現在唯一相互情報量

最大化の最適解が知られている信号系である[31]～[34]。

M＞2であればこれらの信号を誤りゼロで識別することは原理的に不可能である。最小誤り確率は

$$P_e = 1 - \frac{2}{M}, \tag{13}$$

であり、それを実現するPOM $\{\hat{\Pi}_j\}$ は[8][29]

$$\hat{\Pi}_j = |a_j\rangle\langle a_j| \quad \text{with} \tag{14}$$

$$|a_j\rangle = \sqrt{\frac{2}{M}}\left(\cos\frac{j\pi}{M}|\leftrightarrow\rangle + \sin\frac{j\pi}{M}|\updownarrow\rangle\right) \tag{15}$$

$$(j = 0, \ldots, M-1).$$

で与えられる。出力数は信号数と同じである。

表1 3元信号の場合の通信路行列

	$\|\psi_0\rangle$	$\|\psi_1\rangle$	$\|\psi_2\rangle$
$\|\omega_0\rangle$	0	0.5	0.5
$\|\omega_1\rangle$	0.5	0	0.5
$\|\omega_2\rangle$	0.5	0.5	0

これに対して相互情報量最大化のためのPOMは三つのランク1の作用素からなる[34]。しかし、信号数と同数の出力数を持つ最適解も存在する。ただ、実際のデバイス化においては、出力数が小さい方が良いことはいうまでもない。

Mが偶数であれば、出力数は2で十分でありこの場合の測定は従来型のvon Neumann測定である。Mが奇数であれば、最低でも三つ以上の出力が必要になり、従来型のvon Neumann測定では最大情報を引き出すことは不可能となる。そのような最適POM $\{\hat{\Pi}_j\}$ は次のように与えられる。

$$\hat{\Pi}_j = |\omega_j\rangle\langle\omega_j| \tag{16}$$

$$\text{with} \quad \begin{cases} |\omega_0\rangle = -\sin\frac{\gamma}{2}|\updownarrow\rangle \\ |\omega_1\rangle = \frac{1}{\sqrt{2}}\left(-|\leftrightarrow\rangle + \cos\frac{\gamma}{2}|\updownarrow\rangle\right) \\ |\omega_2\rangle = \frac{1}{\sqrt{2}}\left(|\leftrightarrow\rangle + \cos\frac{\gamma}{2}|\updownarrow\rangle\right) \end{cases} \tag{17}$$

ここでγは

$$\cos\frac{\gamma}{2} = \cot\frac{m\pi}{M}, \quad \sin\frac{\gamma}{2} = -\sqrt{1 - \cot^2\frac{m\pi}{M}} \tag{18}$$

から決められる。mは$\frac{M}{4} < m < \frac{M}{2}$なる整数である。

M=3（3元信号）の場合、最適POMはm=1で与えられ、長さの等しい三つの測定状態ベクトルで与えられる（図.1）。この図では、矢印は偏光の方向を表し、紙面上の水平、垂直方向が2つの単位ベクトル$|\leftrightarrow\rangle$と$|\updownarrow\rangle$に対応する。矢印の長さは状態ベクトルのノルムを表している。M=3の場合の最適測定では、$|\psi_i\rangle$と$|\omega_j\rangle$が直交する。したがって

$$P(y_j|x_j) = \langle\psi_j|\hat{\Pi}_j|\psi_j\rangle = 0. \tag{19}$$

であり、他の二つの出力は等確率で生じる。出力確率を表1にまとめる。

M=5とM=7の場合、式(17)は、ノルムの違う三つの測定ベクトルで与えられる。M=5の場合の信号と測定ベクトルの配置を図2に示す。この場合の通信路行列を表2へ示す。7元信号の場合、2種類の最適な3値出力測定が存在する（式(17)。それぞれ式(18)でm=2とm=3に対応している。図3と表3及び4に測定ベクトル、通信路行列を示す。どちらの場合も$P(y_j|x_i)$=0となる組(i, j)がある。

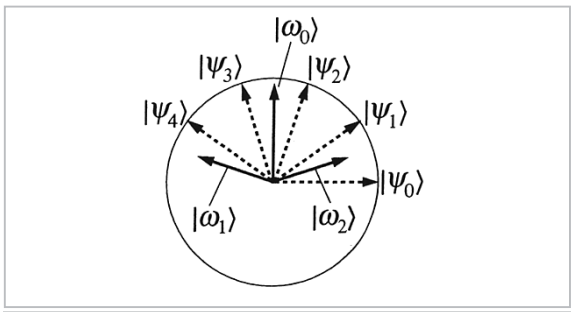


図2 5元信号の最適測定の測定ベクトル(実線)と信号ベクトル(点線)

表2 5元信号の場合の通信路行列

	$\|\psi_0\rangle$	$\|\psi_1\rangle$	$\|\psi_2\rangle$	$\|\psi_3\rangle$	$\|\psi_4\rangle$
$\|\omega_0\rangle$	0	0.309	0.809	0.809	0.309
$\|\omega_1\rangle$	0.5	0.191	0	0.191	0.5
$\|\omega_2\rangle$	0.5	0.5	0.191	0	0.191

表3 7元信号の場合の通信路行列（m=2）

	$\|\psi_0\rangle$	$\|\psi_1\rangle$	$\|\psi_2\rangle$	$\|\psi_3\rangle$	$\|\psi_4\rangle$	$\|\psi_5\rangle$	$\|\psi_6\rangle$
$\|\omega_0\rangle$	0	0.069	0.223	0.346	0.346	0.223	0.069
$\|\omega_1\rangle$	0.5	0.154	0	0.154	0.5	0.777	0.777
$\|\omega_2\rangle$	0.5	0.777	0.777	0.5	0.154	0	0.154

表4　7元信号の場合の通信路行列（m=3）

	$\|\psi_0\rangle$	$\|\psi_1\rangle$	$\|\psi_2\rangle$	$\|\psi_3\rangle$	$\|\psi_4\rangle$	$\|\psi_5\rangle$	$\|\psi_6\rangle$
$\|\omega_0\rangle$	0	0.178	0.579	0.901	0.901	0.579	0.178
$\|\omega_1\rangle$	0.5	0.322	0.099	0	0.099	0.322	0.5
$\|\omega_2\rangle$	0.5	0.5	0.322	0.099	0	0.099	0.322

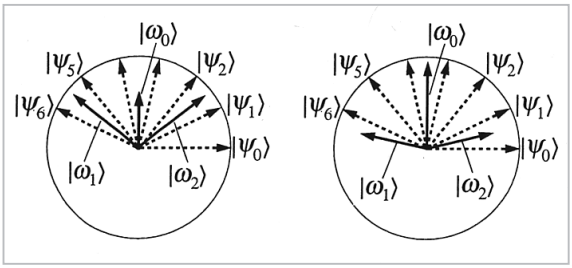


図3　7元信号の場合の最適測定ベクトル
左が$m=2$、右が$m=3$の場合に対応。

以上述べた3値出力の最適測定の実現方法はRef.[34]で詳しく述べられている。非直交の測定ベクトルを、補助系を導入して拡大空間の上で直交化して、標準のvon Neumann測定として実現するという方法である。

これは実際には図4に示したMach-Zehnder干渉系によって実現される。この系は $\{|\leftrightarrow\rangle_a, |\updownarrow\rangle_a, |\leftrightarrow\rangle_b, |\updownarrow\rangle_b\}$ なる基底によって張られる4次元空間を構成する。a，bは光学パスを表す添え字である。もともとの信号状態はこれらの最初の二つの基底ベクトルで張られる空間に存在する。空間の拡大は新たに真空ポート図4のbを加えることで実現する。

Mach-Zehnder干渉部でのunitary変換、図4の$\hat{U}$は

$$A'_{\mathrm{H}}|\leftrightarrow\rangle_a + A'_{\mathrm{V}}|\updownarrow\rangle_a + B'_{\mathrm{H}}|\leftrightarrow\rangle_b + B'_{\mathrm{V}}|\updownarrow\rangle_b$$
$$= \hat{U}\left(A_{\mathrm{H}}|\leftrightarrow\rangle_a + A_{\mathrm{V}}|\updownarrow\rangle_a + B_{\mathrm{H}}|\leftrightarrow\rangle_b + B_{\mathrm{V}}|\updownarrow\rangle_b\right) \quad (20)$$

$$\text{with} \begin{bmatrix} A'_{\mathrm{H}} \\ A'_{\mathrm{V}} \\ B'_{\mathrm{H}} \\ B'_{\mathrm{V}} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos\gamma/2 & \sin\gamma/2 & 0 \\ 0 & -\sin\gamma/2 & \cos\gamma/2 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} A_{\mathrm{H}} \\ A_{\mathrm{V}} \\ B_{\mathrm{H}} \\ B_{\mathrm{V}} \end{bmatrix}$$

のように表される。ここで$\gamma/2$は半波長板HWP1の回転角の2倍である。このセットアップでは入力は$B_{\mathrm{H}}=B_{\mathrm{V}}=0$であり、したがって、図4は実際には3次元空間を構成する。

PD_0は$|\leftrightarrow\rangle_b$成分を検出するがその振幅は

$$B'_{\mathrm{H}} = -\sin(\gamma/2)A_{\mathrm{V}}\,. \quad (21)$$

で与えられる。この出力が出ない場合は信号は$|\psi_0\rangle$ではなかったことになる。一方、$|\leftrightarrow\rangle_a$と$|\updownarrow\rangle_a$成分はさらにHWP2とPBS3で干渉し

$$\frac{1}{\sqrt{2}}\left(A'_{\mathrm{H}} \pm A'_{\mathrm{V}}\right) = \frac{1}{\sqrt{2}}\left[A_{\mathrm{H}} \pm \cos\frac{\gamma}{2}A_{\mathrm{V}}\right] \quad (22)$$

という振幅へと変換されPD1とPD2へ到達する。式(21)と(22)からわかるように式(17)の$|\omega_j\rangle$が再現されることになる。

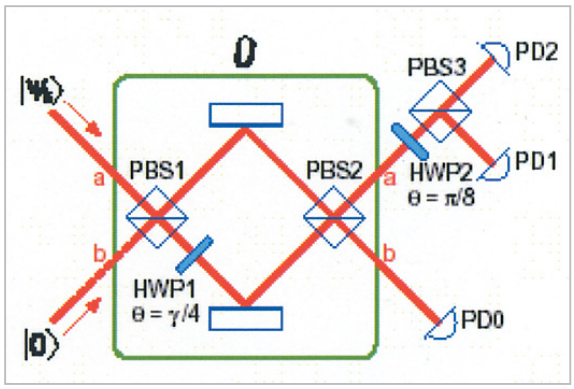


図4　最適POMを実現する検出回路の概念図
PBSは偏光ビームスプリッター、HWPは半波長板、θはその回転角、PDは光検出器である。

4　実験

実際の実験では偏光の基底$\{|\leftrightarrow\rangle, |\updownarrow\rangle\}$はP－（図5の紙面内）とS－（図5の紙面に垂直）偏光に対応する。光源は波長632.8nm帯のHe-Neレーザ（Spectra-Physics, model117A）である。光出力1mWを減衰器ATN1でファクタ10^6だけ減らし、偏光ビームスプリッタPBS0で水平偏光に初期化する。波長板HWP0はステッピングモータで制御し、信号の変調を行い$\{|\psi_i\rangle\}$を生成する。光ビームはさらに減衰器ATN2で因子10^4だけさらに減衰させられる。Mach-Zehnder干渉系への入力点では、光パワーは10^4pW（$\approx 3\cdot 10^5$photon/sec）程度となる。これは1メートルに光子10^3個程度に対応し、検出回路内に2光子以上存在する確率はほとんど無視できる。

偏光Mach-Zehnder干渉系を構成する偏光ビームスプリッタは、消光比1:1000程度達成できるよう、並行配置からわざと若干ずらしてアラインメントをとってある。つまり、通常の$\pi/4$入

射の角からわざと≈0.02radほど傾けて入射させることでPBSのコントラストを≈0.998まで上げている。結果的に干渉系は図5のように若干ひしゃげた干渉系となる。干渉系の各アームには半波長板HWP1とHWP1′が挿入されている。HWP1は光の偏光を$\gamma/2$だけ回転させる。HWP1′は対称性を保つために挿入したもので、光の偏光は変えない。二つの光路からのビームはPBS2で合波し、二つのビームに分かれて一つは光路bからポート0へ入る。光路aの光はHWP2で偏光を$\pi/8$だけ回転してからPBS3へ向い、最終的にポート1と2で検出される。

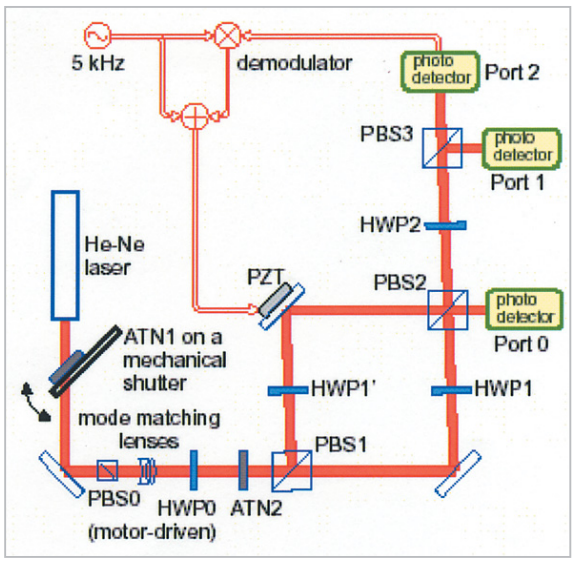


図5 実験系

記号は図4と同じ。ポート0、1、と2にはAPDとa silicon photodiodeが含まれ機械的シャッティングでこれらへの光路の切り替えが為される。すべてのPBSは消光比が最大となるよう並行配置から若干ずらしてアラインメントをとってある(≈0.02rad)。

偏光Mach-Zehnder干渉系の行路長はPZTアクチュエータで適切な操作点にロックされる。ロックがかかった後で、信号取得に入るが、この際の取得時間間隔は20－30秒である。光検出器としてはsilicon photodiodeとAPD(avalanche photodiode, EG & G, SPCM-AQ-141-FC)の2種類があるが前者は明光によるアラインメント用に用い、後者が単一光子検出用であり、マルチモード光ファイバへ集光されAPDへ導かれる。APDの出力はカウンター(EG& G ORTEC, model 995)で計数される。二つの検出器への光

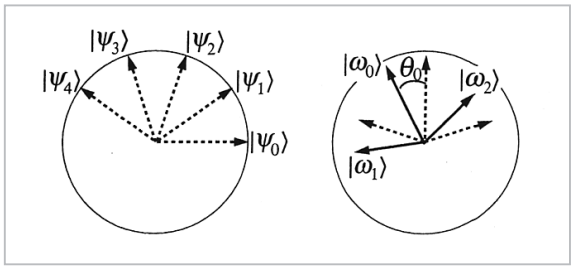


図6 測定ベクトルと信号ベクトルの間に加える相対角θ_0。$M=5$の場合の図。

の切り替えは機械的なシャッティングで行う。光ファイバへの結合効率は0.75－0.8である。カウンターは約1秒間動作させデータを収集し、これを5回繰り返し通信路行列に対応する統計データにする。このステップを各信号$|\psi_i\rangle$ $(i=0,\ldots,M-1)$に対して実行し相互情報量を算出する。

後に**5**で議論するが、相互情報量を増やす効果的な方法は実は可能性のある信号の一つを完全に排除することである。その意味で出力が出ないはずのポートへの光の漏れを如何に低く抑えるかが重要な点となる。しかし、現実のシステムでは不完全性から誤差が免れない。その主要因はここではAPDの暗電流(APD error)とPBSでの不完全な消光比からくる漏れ(PBS error)である。APD errorは光をシャットアウトした時のレベルで100 count/secである。なお、完全なダークニングの後でも300 count/secのレベルの背景光が観測された。信号光入射後は、干渉系とPBS自身の不完全性からの光の漏れがこれに加わる。このレベルが、出力が出ないはずのポートで大体1000 count/secである。(表1～4参照。)信号光が出るべきポートでのカウント数は105 count/sec程度でありAPDの線形領域の範囲に収まるようになっている。実際に得られた干渉精度は

$$\frac{P_{\max}-P_{\min}}{P_{\max}+P_{\min}} \approx 0.98\,, \tag{23}$$

程度である。

検出回路の性能を解析するため、相互情報量の最大値のみならず、信号状態と$\{|\psi_i\rangle\}$と測定ベクトル$\{|\omega_j\rangle\}$の間の相対角度$\theta_0=0$を変えながら

$$|\psi_i'(\theta_0)\rangle = \cos\left(\frac{i\pi}{M}+\theta_0\right)|\leftrightarrow\rangle + \sin\left(\frac{i\pi}{M}+\theta_0\right)|\updownarrow\rangle \quad (24)$$
$$(i=0,\ldots,M-1),$$

なる信号に対する相互情報量の変化を測定した。最適点は$\theta_0=0$である。図6を参照。実際の測定ではθ_0は$\pi/90$radian（2度）刻みで変えている。

5　結果

図7は3元信号の場合の三つのAPDでの相対出力強度である。相対出力強度が入射単一光子に対して各ポートに検出される確率に対応する。

偏光角が$\{-\pi/6,\ \pi/6,\ \pi/2\}$の時には、誤り確率最小化の測定に対応し、偏光角が$\{-\pi/3,\ 0,\ \pi/3\}$の場合には断定的測定に対応し、Ref.[39]でのtrine及びanti-trine測定といっているものに対応する。Clarkeらは、表1の理想値からの*rms*分散として3.8%の値を報告しているが、我々の実験では1.1%と、より低い値となっている。これは主に偏光ビームスプリッタの誤差が減っているためである。図7のデータから計算される相互情報量を図8に示す。最適点での相互情報量は明らかに理想的von Neumann測定による理論値より大きくなっており、量子最適測定の優位性が確認された。また、我々の得た最大相互情報量はClarke *et al.*[39]のものより更に大きくなっている。これは前述のごとく偏光ビームスプリッタの誤差が減っているためで、理論値からの減少分は、主に偏光ビームスプリッタの残存誤差

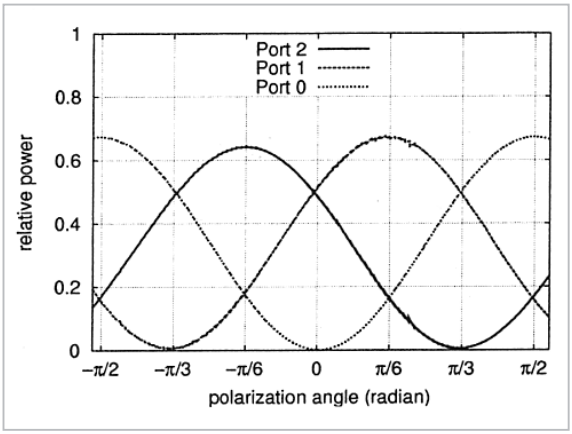


図7　三つのAPDでの相対出力強度。3元信号の場合

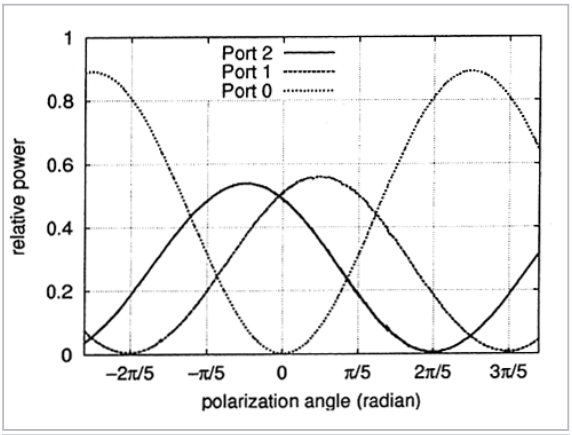


図9　5元信号の場合の三つのAPDでの相対出力強度

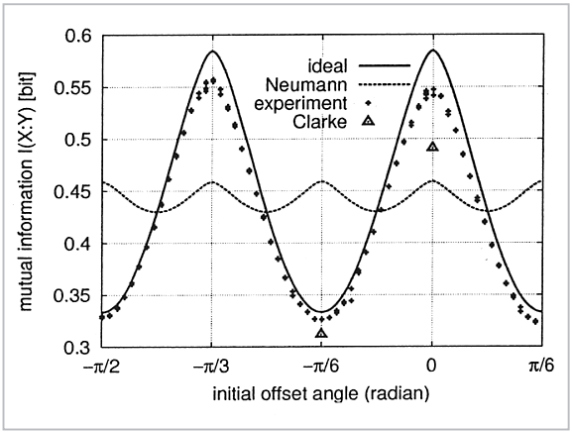


図8　相互情報量のθ_0依存性。3元信号の場合
＋が実験値、実線が理論値、点線が理想的von Neumann測定による相互情報量。三角印はClarkeらによって行われた実験値39（$\theta_0=0$と$-\pi/6$に相当）。

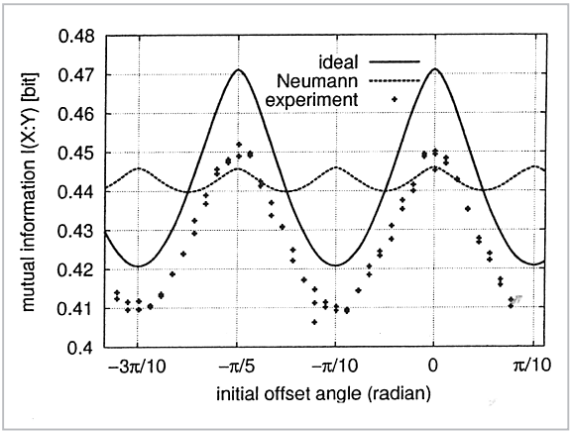


図10　5元信号の場合の相互情報量のθ_0依存性。
記号の定義は図8と同じ。

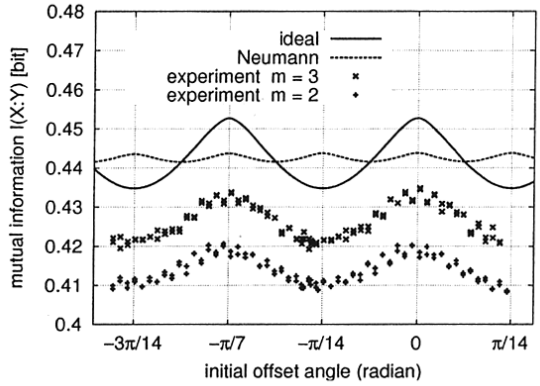


図11　7元信号の場合の相互情報量のθ_0依存性。
xは$m=2$、＋は$m=3$の解に対応する。他の記号の定義は図8と同じ。

約0.1%に起因するものである。

図9は5元信号の場合の三つのAPDでの相対出力強度、図10はそれから計算された相互情報量である。この場合の理想的von Neumann測定による理論値からの利得はわずかなものである。5元信号では、3元信号の場合より信号の識別性は著しく劣化しており、相互情報量そのものの値が小さくなる。前述したとおり相互情報量を増やすためには、可能性のある信号のうちのどれか一つを確実に排除できると良いが、3値出力の検出で排除でる信号の数は限られるため、信号の元の数が増えると必然的に最大相互情報量は頭打ちとなる。そこに偏光ビームスプリッタの誤差が加わり、最大相互情報量とvon Neumann測定の理論値との差が小さくなってしまう。ただ理論上の最大相互情報量からの実験値の減少の絶対値自身は3元、5元信号とも≈0.02である。

図11は7元信号の場合の二つの最適解（xは$m=2$、＋は$m=3$の解）に対する相互情報量の変化である。この場合、実験の最大相互情報量はもはやvon Neumann測定の理論値を上回ることはできなくなっている。$m=3$の場合の実験的相互情報量は$m=2$のものより若干大きくなっている。理想的にはこれらは同じ相互情報量を与えるはずのものであるが、実際の検出回路では、$m=2$と$m=3$で干渉する光の絶対量が違うため、そこに不完全な干渉コントラストが影響し非対称性が出でしまっている。

6　結語

非直交量子状態を使って情報伝送を行う量子通信路では、非直交量子状態が完全には識別不可能であることから、たとえシステムがどんなに完全でも正確に送れる伝送の容量に限界が課される。これは古典的な情報理論には考慮されていない点である。この別な側面としてno-cloning定理という原理が出てきて完全な安全性を原理的に保障する量子暗号鍵配布が可能となる[40][41]。

量子通信路を最適に使うためには、その通信路を特徴付ける相互情報量が最大となるよう信号検出や符号化を工夫しなければならない。特に、信号検出を最適したときの相互情報量の最大値がaccessible informationであり、この具体的最適解はほんの限られた例でしか知られていないのは、初めに述べたとおりである[31]～[34]。その中で、符号化も含めて理論・実験両面から研究を進められる数少ない信号系の一つが実対称qubit信号であった[34]。

この論文では、実対称qubit信号に対してaccessible informationを実現するための偏光Mach-Zehnder干渉系からなる最適検出回路を試作し、従来検出方式von Neumann測定からの検出利得の検証を行った。3元信号に対しては理論限界の96%まで迫る相互情報量の達成が現在の技術で可能であることを示した。残るギャップを生じさせている原因は偏光ビームスプリッタの不完全性からくる光の漏れである。これもアラインメントの角度を最適に選ぶことで、市販品の性能表を上回る精度で使うことができる。こう言った工夫の結果、我々の実験値は先に行われたClarkeらの実験値[39]を上回った。この3元信号での実験結果は同様の信号に基礎を置く量子暗号鍵配布Phoenix-Barnett-Chefles protocol[41]がすでに実用的な技術領域に入っていることを意味している。

また、この論文ではまだ検証されていなかった5元信号、7元信号についても、最適解の検証と従来測定に対する測定利得の確認も行った。これはDaviesの定理[33]の予言、相互情報量最適測定の出力数Nは信号の元の数によらず信号空間の次元dによって$d \leq N \leq d^2$のようにバウン

ドされる、という効果を直接実験で検証した初めての例となった。特に、実信号に対してはこのバウンドは更に$d \leq N \leq d(d+1)/2$となり[34]、単一光子の偏波信号に対しては、信号数がいくつであっても常に最大3出力の測定を用意すれば、必ず最適解を構成できることが原理的には保証されており、これを実際に構成し、相互情報量で5元信号までは従来測定に対する測定利得が見られることを確認した。最適解としては信号と同じ元数、対称性を持つ群共変最適解も存在し、このクラスの検出回路と3出力最適測定との実験的比較などは今後の課題である。

今後はこういった結果に基づき、いよいよ量子符号化利得の実験的検証に進むことになる。まだ、だれも足を踏み入れたことのないShannon理論の容量限界を超えた新しい通信領域への一歩を目指した研究となる。

謝辞

最後に、有意義な議論と励ましを頂いた井筒博士と広田教授、Riis教授、Clarke博士に感謝いたします。

参考文献

1 C. H. Bennett and P. Shor, "Quantum Information theory," IEEE Trans. Inform. Theory, IT-44, No. 6, pp2724-2742 (1998).
2 佐々木雅英，番雅司，量子情報理論，－量子効果を使う新しい情報操作とその限界を明らかにする理論－：，物理学会誌，Vol. 57, N0. 1, 9-21 (2002).
3 W. K. Wootters and W.H. Zurek, Nature 299, 802 (1982).
4 H. P. Yuen, Phys. Lett. A, 113, 405 (1986).
5 C.E. Shannon, Bell System Tech. J. 27, 379 (Part Ⅰ) and 623 (Part Ⅱ) (1948).
6 R.G. Gallager: *Information Theory and Reliable Communication* (John Wiley and Sons, New York, 1968).
7 T. Cover and J. Thomas: *Elements of Information Theory* (John Wiley and Sons, New York, 1991).
8 C.W. Helstrom, *Quantum Detection and Estimation Theory* (Academic Press, New York, 1976).
9 広田修，光通信理論（森北出版，1985).
10 A.S. Holevo : *Probabilistic and Statistical Aspects of Quantum Theory* (North-Holland, Amsterdam, 1982).
11 A. Peres: *Quantum Theory: concepts and methods,* 279 (Kluwer Academic Publishers, Dortrecht, 1993).
12 P. Hausladen, R. Jozsa, B. Schumacher, M. Westmoreland, and W.K. Wootters, Phys. Rev. A54, 1869 (1996).
13 A.S. Holevo, IEEE Trans. Inf. Theory IT-44, 269 (1998).
14 B. Schumacher and M. Westmoreland, Phys. Rev. A56, 131 (1997).
15 M. Sasaki, K. Kato, M. Izutsu, and O. Hirota, Phys. Rev. A58, 146 (1998).
16 M. Sasaki, T.S. Usuda, M. Izutsu, and O. Hirota, Phys. Rev. A58, 159 (1998).
17 A.S. Holevo, J. Multivar. Anal. 3, 337 (1973).
18 H.P. Yuen, R.S. Kennedy, and M. Lax, IEEE Trans. Inf. Theory 21(2), 125 (1975).
19 I.D. Ivanovic, Phys. Lett. A123, 257 (1987).
20 D. Dieks, Phys. Lett. A126, 303 (1988).
21 A. Peres, Phys. Lett. A128, 19 (1988).
22 G. Jaeger and A. Shimony, Phys. Lett. A197, 83 (1995).
23 S.M. Barnett, Phil. Trans. R. Soc. Lond. A255, 2279 (1997).
24 A. Chefles and S.M. Barnett, J. Mod. Opt., 45, 1295 (1998).
25 A. Chefles, Phys. Lett. A239, 339 (1998).
26 A. Chefles, Contemp. Phys. 41, 401 (2000) and references therein.

27 B. Huttner and A. Peres, J. Mod. Opt. 41, 2397 (1994).

28 M. Osaki, M. Ban, and O. Hirota, Phys. Rev. A54, 1691 (1996).

29 M. Ban, K. Kurokawa, R. Momose, and O. Hirota, Inter. J. Theor. Phys. 36, 1269 (1997).

30 S.M. Barnett, Phys. Rev. A 64, 030303(R) (2001).

31 L.B. Levitin, *Quantum Communication, and Measurement* (Eds. V.P. Belavkin, O. Hirota, and R.L. Hudson, Prenum, New York, 1995), 439.

32 M. Osaki, M. Ban, and O. Hirota, *Quantum Communication, Computing, and Measurement 2* (Eds. P. Kumar, G M. D'Ariano, and O. Hirota, Kluwer academic/ Prenum publishers, New York, 2000) 17.

33 E.B. Davies, lEEE Trans. lnf. Theory IT-24, 596 (1978).

34 M. Sasaki, S.M. Barnett, R. Jozsa, M. Osaki, and O. Hirota, Phys. Rev. A59, 3325 (1999).

35 P.W. Shor, "On the Number of Elements Needed in a POVM Attaining the Accessible Information", to appear in *Quantum Communication, Computing, and Measurement 3* (Eds. O. Hirota and P. Tombesi, Kluwer, Dordrecht, 2001). Also available as ArXiv:quant-ph/0009077.

36 S.M. Barnett and E. Riis, J. Mod. Opt. 44, 1061 (1997).

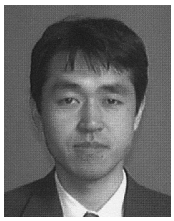
37 B. Huttner, A. Muller, J.D. Gautier, H. Zbinden, and N. Gisin, Phys. Rev. A54, 3783 (1996).

38 R.B.M. Clarke, A. Chefles, S.M. Barnett, and E. Riis, Phys. Rev. A63, 040305 (2001).

39 R.B.M. Clarke, V.M. Kendon, A. Chefles, S.M. Barnett, E. Riis, and M. Sasaki, Phys. Rev. A64, 012303 (2001).

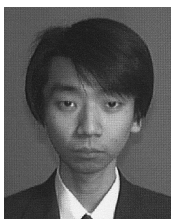
40 S.J.D. Phoenix and P.D. Townsend, Comtemp. Phys. 36, 165 (1995) and references therein.

41 S.J.D. Phoenix, S.M. Barnett, and A. Chefles, J. Mod. Opt. 47, 507 (2000).



佐々木雅英（ささきまさひで）
基礎先端部門量子情報技術グループリーダー　博士（理学）
量子情報理論

水野　潤（みずのじゅん）
基礎先端部門量子情報技術グループ専攻研究員　ph. D
光計測、重力波検出



藤原幹生（ふじわらみきお）
基礎先端部門量子情報技術グループ主任研究員　博士（理学）
光検出デバイス技術