トレース距離を用いた最小誤り率の近似式提案と量子暗号の安全性評価への応用

浅野 駿吾　　　指導教員：臼田 毅

1　はじめに

量子情報理論において，与えられた量子信号に対する量子最適測定の発見と最小誤り率の計算は，量子通信の限界性能を明らかにするだけでなく，量子暗号の安全性を示すためにも非常に重要である [1]．しかし，たとえ最適測定を見つけたとしても，信号数が非常に多い場合，最小誤り率の計算は困難である．実際，先験確率が等確率である対称性を持つ純粋状態信号系に対しては，Square-root measurement(SRM)[2] が量子最適測定であることが知られているが，その最小誤り率を計算するためには，グラム行列の平方根を計算する必要があり，信号数が数千の場合でも困難である．

本研究ではトレース距離を用いた多元コヒーレント状態信号の最小誤り率の近似式を提案する．トレース距離は 2 量子状態の近さを表す指標であり，いくら信号数が増えようとも，純粋状態信号であれば容易に計算することができる．多元コヒーレント状態信号に対して，提案する近似式は信号数が多く誤り率の小さい領域で高精度であることを示す．また，量子暗号の安全性を示すために最小誤り率を計算するとき，提案する近似式が応用可能な例を紹介する．最後に，現在量子暗号の安全性評価指標としてトレース距離が注目されており，本研究の結果から，トレース距離を評価指標として導入する際の問題点を考察する．

2　コヒーレント状態信号に対する近似式の構成法

初めに，多元信号として 3 つのコヒーレント状態信号，M-PSK(Phase Shift Keying)，M-ASK(Amplitude Shift Keying)，M-QAM(Quadrature Amplitude Modulation) を考える．これらの多元信号に対して，量子最適測定を用いた平均誤り率，すなわち最小誤り率を $P_{\mathrm{e}}^{\mathrm{opt}}$ とする．

多元信号の中で最小のトレース距離を示す 2 信号 $\{\rho_j, \rho_l\}$ を識別する最小誤り率を $P_{\mathrm{e}}^{\mathrm{binary}}$ とする．ここで ρ は密度作用素である．ここでは $\{\rho_j, \rho_l\}$ を近接 2 信号と呼び，$P_{\mathrm{e}}^{\mathrm{binary}}$ はトレース距離 D を用いて次のように定義される．

$$P_{\mathrm{e}}^{\mathrm{binary}} = \frac{1}{2}\{1 - D(\rho_j, \rho_l)\} \tag{1}$$

さらに，与えられた信号に対して最も近い信号の数 $N(k)$ を考える．ρ_k について，これを次のように定義する．

$$D_{\mathrm{min}}(\rho_k) = \min_{j \neq k} D(\rho_k, \rho_j) \tag{2}$$

$$N(k) = \#\{j \mid D(\rho_k, \rho_j) = D_{\mathrm{min}}(\rho_k)\} \tag{3}$$

ここで，$\#S$ は集合 S の要素数を意味する．このとき，$N(k)$ を用いて最も近い信号の平均数 $\langle N \rangle$ が次のように定義することができる．

$$\langle N \rangle = \frac{1}{M}\sum_{k=0}^{M-1} N(k) \tag{4}$$

比 $P_{\mathrm{e}}^{\mathrm{opt}}/P_{\mathrm{e}}^{\mathrm{binary}}$ は，平均光子数 α が大きくなるにつれて $\langle N \rangle$ に収束する．従って，$P_{\mathrm{e}}^{\mathrm{binary}}$ を定数 $\langle N \rangle$ 倍した値が最小誤り率を近似することが考えられる．従って，最小誤り率の近似式 $P_{\mathrm{e}}^{\mathrm{approx}}$ を次のように定義する．

$$P_{\mathrm{e}}^{\mathrm{approx}} = \langle N \rangle P_{\mathrm{e}}^{\mathrm{binary}} \tag{5}$$

図 1,2 にぞれぞれ各コヒーレント状態信号の規格化近似精度を示す．規格化近似精度は近似式がどの程度良いかを示すため，次のように定義された値である．

$$\left| 1 - \frac{P_{\mathrm{e}}^{\mathrm{approx}}}{P_{\mathrm{e}}^{\mathrm{opt}}} \right| \tag{6}$$

高信頼性通信の観点から，誤り率が 0.1 以下の場合を示しているが，信号数が大きく誤り率が小さい領域においては近似式が有用であると言える．実際，誤り率が 0.01 の場合には PSK と ASK の精度は 0.01 程度であるため，$P_{\mathrm{e}}^{\mathrm{approx}} \sim 0.99 P_{\mathrm{e}}^{\mathrm{opt}}$ である．また，図 1 に示す通り，PSK では信号数が増えるほど精度は良くなり，逆に ASK では信号数が増えるほど精度は悪くなっている．さらに，PSK と ASK の精度は信号数が増えるとある同じ値に収束していくことがわかる．図 2 では，QAM の精度は信号数によらずほとんど変わらないことがわかる．また，その精度は 4-PSK の場合とほとんど同じ値を示している．このことから，信号数が増えるに従って PSK のある性質が QAM から ASK へと近づくようなふるまいを示し，その性質に近似式が依存していると考えられる．

ここで，与えられた信号に対し，2 番目に近い信号に着目し，最も近い信号とのユークリッド距離を d_1，2 番目に近い信号との距離を d_2 とする．表 1 に比 d_2/d_1 を示す．このとき，信号数が増えるに従って PSK の比 d_2/d_1 の値が QAM の値から ASK の値に近づいていることがわかる．従って，近似式は 2 番目に近い信号に依存していると考えられる．

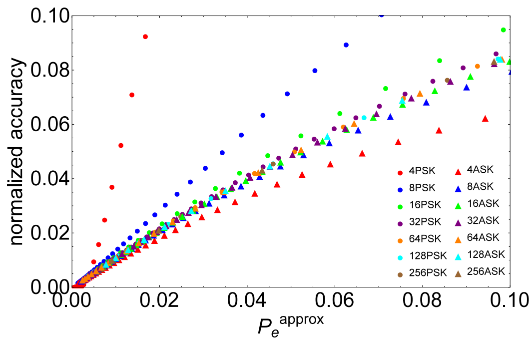

図 1　M-PSK と M-ASK の規格化近似精度

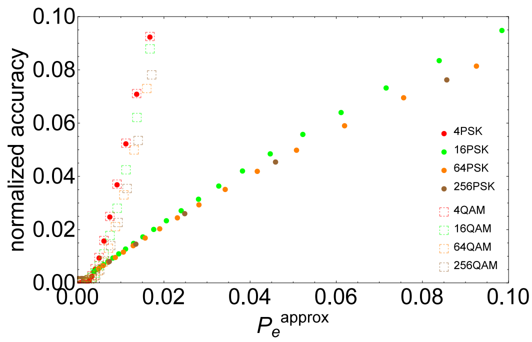

図 2　M-PSK と M-QAM の規格化近似精度

表 1　各コヒーレント状態信号の比 d_2/d_1

M	PSK	ASK	QAM
4	$\sqrt{2}$	2	$\sqrt{2}$
16	$2\cos\frac{\pi}{16} \sim 1.96157$	2	$\sqrt{2}$
64	$2\cos\frac{\pi}{64} \sim 1.99759$	2	$\sqrt{2}$
256	$2\cos\frac{\pi}{256} \sim 1.99985$	2	$\sqrt{2}$

3　量子暗号の安全性評価への応用

新量子暗号 Y-00 を提案した Yuen は，安全性評価として盗聴者に仮想的に有利な状況を想定した上で，受信者と盗聴者の誤り率の差を上界として評価する手法を提案している [3]．このとき誤り率の計算が必要になるが，Y-00 で用いられる信号数は 4000 元を超えるため計算が困難である．しかし，Y-00 は信号方式として PSK や ASK コヒーレント状態信号を用いるものもあり，提案する近似式が安全性評価のために応用できることがわかる．

また，2 量子状態を識別する最小誤り率はトレース距離を用いて表すことができるが，多元信号に対してはこの 2 つの間の関係は明らかとなっていない．現在，トレース距離は量子暗号の評価指標として注目されているが，安全性評価問題は多元信号の識別に関する問題のため，前述した関係を明らかにする必要がある．ここではトレース距離が多元信号の最小誤り率とどのような関係にあるかを考えるため，コヒーレント状態信号以外の信号として，以下の 3 つの信号系へ近似式を適用する．

1. 量子ビット系の多元純粋状態と対称混合状態 [4]
2. M 元直交信号
3. PSK 純粋状態の統計的重ね合わせによる混合状態 [5]

1 へ近似式を適用した場合の最小誤り率と近似式を図 3 に示す．信号数の多い場合，確かに近似式は真値に近づいている．しかし，量子ビット系の信号は二次元 Hilbert 空間で表されるため，最小誤り率が 1 に近づくことは自明である．従って，信号数が大きい場合に近似式が適用できることは明らかであり，それはトレース距離の性質以上に量子ビット系の性質が表れている結果であると言える．

2 へ近似式を適用した場合の規格化近似精度を図 4 に示す．M 元直交信号は全ての信号が直交するため，与えられた信号に対して他の全ての信号が最も近い信号になる．従って，信号数が増えるほど精度が悪くなり，近似式は有用でないと言える．

3 へ近似式を適用した場合の比 $P_e^{\mathrm{opt}}/P_e^{\mathrm{binary}}$ を図 5 に示す．ϵ は統計的重ね合わせが起きている確率であり，$\epsilon = 0$ の場合には純粋な PSK 信号を意味する．$\epsilon \neq 0$ の場合には，比が $\langle N \rangle$ に収束しないため，近似式が適用できないことがわかる．

このように，多元信号に対しては信号系毎にトレース距離は異なるふるまいを示すことがわかる．トレース距離を安全性評価指標として導入するためには，信号系に依存しないユニバーサルな性質を明らかにすると共に，その性質が真に安全性評価に用いることができるかを議論しなければならない．

4　まとめ

本研究では，多元信号の中で最も近い 2 信号に着目し，その性質から構成できる最小誤り率の近似式を提案した．純粋な多元コヒーレント状態信号に対して，近似式は信号数が大きく誤り率の小さい領域で有用であることがわかった．また，量子暗号の安全性評価への応用例と，トレース距離を評価指標として用いる場合の問題点を考察した．今後の課題として，最も近い 2 信号以外のトレース距離の考察と，近似式の理論的な精度保証が挙げられる．

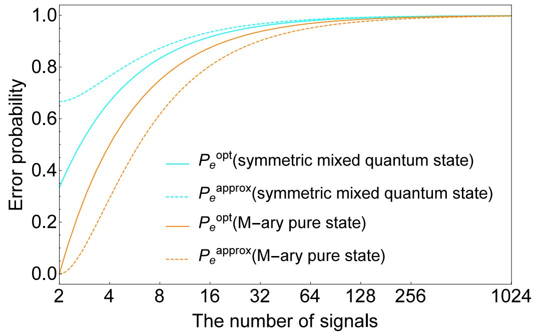

図 3　量子ビット系の信号の最小誤り率と近似式

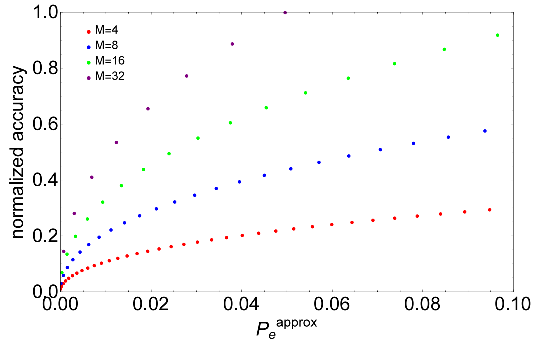

図 4　M 元直交信号の規格化近似精度

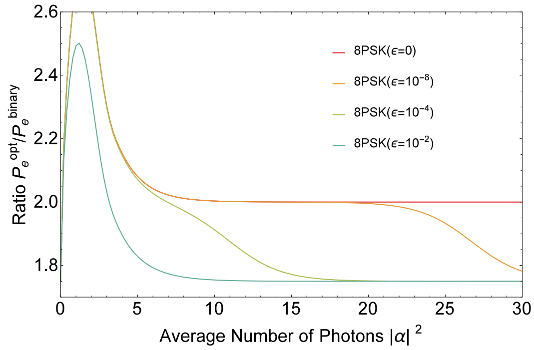

図 5　PSK 純粋状態の統計的重ね合わせによる混合状態信号の最小誤り率と近接 2 信号の最小誤り率の比

参考文献

[1] C.W. Helstrom, *Quantum detection and estimation theory*, Academic Press, New York ,(1976).

[2] P. Hausladen, *et.al.*, Phys. Rev. **A54**, pp. 1869-1876, (1996).

[3] H.P. Yuen, arXiv:quant-ph/0311061v6, (2004).

[4] C.-L. Chou and L. Y. Hsu, Phys. Rev. **A68**, 042305, (2003).

[5] 藤原 祐二, 臼田 毅, 内匠 逸, 畑 雅恭, No.1, pp.63-72, (2001).

公表論文

A) **S. Asano**, *et.al.*, Proc. of AQIS2014, pp.171-172, (2014).

B) **S. Asano**, *et.al.*, Proc. of ISITA2014, pp.254-258, (2014).

C) **S. Asano**, *et.al.*, Proc. of AQIS2015, pp.181-182, (2015).

D) **浅野 駿吾**, 臼田 毅, SITA2015 予稿集, 6.4.2, (2015).