

## コヒーレント状態信号に対する最小誤り率の近似式の古典及び量子の特性比較

情報科学科 西境 浩平

指導教員：白田 毅

## 1 はじめに

量子暗号の 1 つに QKD(Quantum Key Distribution) があり, これは 2 者間で鍵を共有するためのプロトコルである. QKD に対する安全性評価指標としてトレース距離が注目されており, トレース距離は 2 元決定問題に対して最小誤り率を導く性質を持つ. しかし, 暗号の分野では 2 元ではなく多元の決定問題に対する性質が重要となる. 先行研究として, 多元決定問題におけるトレース距離の性質を考察している研究 [1] がある. この研究では, 多元コヒーレント状態信号の中で最も近い 2 信号の最小誤り率の性質を考察し, その結果から多元信号の最小誤り率の近似式を提案している.

この研究を受けて, 本研究では, 多元決定問題におけるトレース距離の性質を考えるアプローチの一つとして, トレース距離の古典版である変動距離に着目する. この変動距離の性質を考察することでトレース距離の性質を明らかにできるのではないかと考える. そこで, 先行研究と同様の手法に従い, 変動距離を用いた古典最適測定における誤り率の近似式を構成し, トレース距離を用いた誤り率の近似式の結果と比較することで変動距離の性質とトレース距離の性質の関係や違いを考察する.

## 2 古典最適測定における誤り率の近似式の適用

先行研究 [1] にて提案されている近似式の構成方法を古典最適測定の場合に適用する. 本研究では,  $M$  相 PSK(Phase Shift Keying) コヒーレント状態信号  $|\alpha_k\rangle = |\alpha \exp[i\frac{2\pi k}{M}]\rangle$  と  $M$  元 ASK(Amplitude Shift Keying) コヒーレント状態信号  $|\alpha_k\rangle = |\frac{k}{M-1}\alpha\rangle$  を対象とする ( $k = 0, 1, \dots, M-1$ ). ここで,  $\alpha$  は複素振幅をあらわす. また, 信号の先験確率を等確率とする.

$M$  元信号における平均誤り率を  $P_e^M$  とする. また,  $M$  個の信号の中で最も近い 2 つの信号を近接 2 信号と呼び, その誤り率を  $P_e^B$  とする.  $P_e^B$  について, 量子最適測定の場合はトレース距離を用いて表すことができる. そして, 古典最適測定の場合には変動距離を用いて表すことができる.

先行研究 [1] では,  $P_e^B$  と  $P_e^M$  の比が近接信号の平均数  $\langle N \rangle$  に収束することを利用して近似式を構成している. 古典最適測定の場合も, この 2 つの誤り率は近接信号の平均数  $\langle N \rangle$  に収束する. すなわち, PSK 信号の場合は  $\langle N \rangle = 2$ , ASK 信号の場合は  $\langle N \rangle = \frac{2(M-1)}{M}$  に収束する. よって, 古典最適測定における誤り率の近似式は, 次のように構成される.

$$P_e^{\text{approx}} = \langle N \rangle P_e^B \quad (1)$$

## 3 近似式精度

文献 [1] では, 提案した近似式の精度を定量的に求めるために, 式 (2) に示す規格化近似精度を用いている. 近似式  $P_e^{\text{approx}}$  が真値  $P_e^M$  に近いほどこの値は小さくなり, 精度が良いことを示す. 本研究でもこの規格化近似精度を用いて評価を行う.

$$\left| 1 - \frac{P_e^{\text{approx}}}{P_e^M} \right| \quad (2)$$

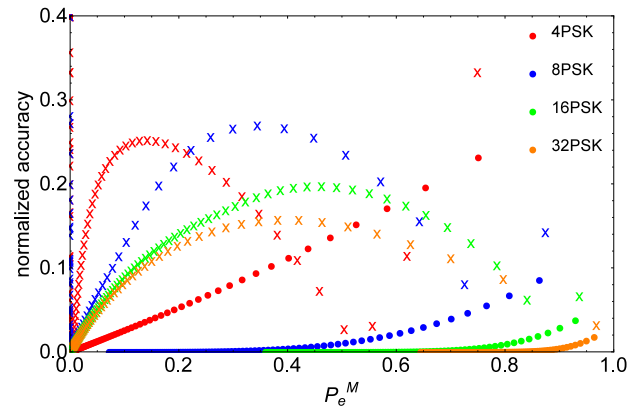


図1 PSK 信号における規格化近似精度の比較

## 4 結果

PSK コヒーレント状態信号に対する誤り率の規格化近似精度を比較したグラフを図 1 に示す. 横軸は多元信号における誤り率, 縦軸は規格化近似精度であり, 丸印は古典最適測定における精度,  $\times$ 印は量子最適測定における精度を示している. 図 1 より, 古典最適測定の場合において, その精度は元数の増加にしたがって向上していることが確認できる. 量子最適測定の場合も, 誤り率が低いところでは同様の性質が見られる. しかし, 量子最適測定における近似精度は, 誤り率の増加にしたがって一度悪くなってから再び良くなるという挙動を示している. そして, 再び良くなっていく部分では, 元数によって精度が向上するといった特徴が見られなくなっている. こういった挙動, 特徴が古典最適測定の場合には見られないことから, ここに量子特有の性質があらわれていると考えることができる.

ASK コヒーレント状態信号における近似精度について, 古典最適測定の場合は  $P_e^B$  と  $P_e^M$  の比が常に一定となることから近似式は真値に一致し, それゆえ 0 となる. 一方で, 量子最適測定の場合には上記のような挙動, 特徴があらわれる.

## 5 まとめ

本研究では, 多元決定問題におけるトレース距離の性質を考察する一つのアプローチとしてトレース距離の古典版である変動距離に着目し, 古典最適測定における誤り率について, 先行研究に倣って近似式を構成した. そして, 両測定における近似精度の比較を行い, 共通点と相違点を確認した. しかし, 相違点である量子特有の振る舞いの詳細については明らかにできていない. そのため, この振る舞いを明らかにし, トレース距離の多元決定問題における性質を明らかにすることが今後の課題である.

## 参考文献

[1] S. Asano, K. Nakahira, and T.S. Usuda, Proceedings of AQIS2014, pp.171-172, (2014).

## 公表論文

1. 西境浩平, 浅野駿吾, 角谷昭仁, 白田毅, 平成 27 年度電気・電子・情報関係学会東海支部連合大会, K1-6, (2015).
2. 西境浩平, 浅野駿吾, 角谷昭仁, 白田毅, 第 38 回情報理論とその応用シンポジウム (SITA2015), pp.457-462, (2015).