非対称量子信号に対する通信路行列計算の簡単化

情報科学科　宮崎 龍輔　　指導教員：臼田 毅

1　はじめに

量子通信システムの信頼性あるいは安全性を評価する上で，量子信号検出限界を明らかにすることは重要である．量子暗号において，PSK，ASK，QAM など，ディジタル通信でもよく知られている変調方式が利用されている．これらのうち，対称信号 (PSK コヒーレント状態信号など) については，量子信号検出限界を達成する量子最適測定が，SRM[1] であることが明らかにされている [2]．また，量子信号検出限界の限界値そのものを計算するための公式も得られている．

それに対し，非対称信号 (ASK コヒーレント状態信号など) に対しては，信号数が大規模な場合，量子信号検出限界を達成する測定が分かっておらず，通信路行列公式も得られていない．このため，非対称信号に対しては数値計算により，SRM による誤り率などの計算が試みられているが，計算量や所要メモリによる制限のため，1000 を大きく超える信号数を扱うことは，極めて困難である．そのため，非対称信号に対する通信路行列公式の導出は課題となっている．

本研究は，M 元非対称信号に対する通信路行列公式を与えることを目的としている．現在，成果として，1 次元で表される $M = 2m$ 元の ASK 信号に対し，その部分的な対称性に着目することで，問題の規模を半分の m にできることを明らかにした．また，その次のステップとして，2 次元の信号である AMPM 信号に対して，$M = 4m$ の場合，問題の規模を $\frac{1}{4}$ の m にすることができることを明らかにした．本稿では，本研究の基礎である ASK 信号に関する成果について述べる．

2　$M = 2m$ 元の ASK コヒーレント状態信号とその固有値，固有ベクトル

2.1　ASK コヒーレント状態信号とそのグラム行列

本稿で扱う $2m$ 元の ASK 信号を図 1 のように表す．ここで，信号の順番が左から $1, 2, ..., 2m$ となっていない点に注意されたい．

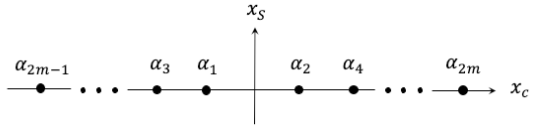

図 1　$2m$ 元の ASK コヒーレント状態信号

この $M = 2m$ 元の ASK 信号のグラム行列は

$$\Gamma^{(2m)} = \begin{bmatrix} 1 & \langle\alpha_1|\alpha_2\rangle & \cdots & \langle\alpha_1|\alpha_{2m}\rangle \\ \langle\alpha_2|\alpha_1\rangle & 1 & \cdots & \langle\alpha_2|\alpha_{2m}\rangle \\ \vdots & \vdots & \ddots & \vdots \\ \langle\alpha_{2m}|\alpha_1\rangle & \langle\alpha_{2m}|\alpha_2\rangle & \cdots & 1 \end{bmatrix} \quad (1)$$

のようになる．Γ の上付き添え字 $(2m)$ は行列サイズを表し，$\Gamma^{(2m)}$ が $2m$ 次の正方行列であることを意味している．

量子測定に SRM を用いる場合，グラム行列の平方根より通信路行列が得られることが知られている [1]．そのため，通信路行列を得るには，グラム行列の固有値，固有ベクトルを求める必要がある．

2.2　グラム行列の分解

ここで，本稿におけるメインアイデアを述べる．図 1 の $2m$ 元の ASK 信号をよく見ると，m 個の BPSK 信号の集まりとなっていることがわかる．BPSK 信号は典型的な対称信号であるので，$2m$ 元 ASK 信号は 2 個ずつ区切った信号が対称であるという意味で部分的な対称性を持つと言える．この特徴を利用するため，$\Gamma^{(2m)}$ を 2 次の正方行列 $\Gamma^{(2)}_{k,l}$ を用いてブロック分割することを考える．ただし，$k, l \in \{1, 2, \ldots, m\}$．ブロック行列 $\Gamma^{(2)}_{k,l}$ は対角成分が等しい行列であり，その固有値 $x_i^{(k,l)}$，固有ベクトル $|x_i\rangle$ を簡単に求めることができる．ただし，$i \in \{1, 2\}$．また，$\{|x_i\rangle\}$ は正規直交している．このとき， $\Gamma^{(2)}_{k,l}$ は

$$\Gamma^{(2)}_{k,l} = \sum_{i=1}^{2} x_i^{(k,l)} |x_i\rangle\langle x_i| \quad (2)$$

と書ける．これより $\Gamma^{(2m)}$ は

$$\Gamma^{(2m)} = \sum_{i=1}^{2} A_i \otimes |x_i\rangle\langle x_i| \quad (3)$$

と書ける．A_i は $x_i^{(k,l)}$ を (k, l) 成分に持つ m 次のエルミート行列であり，スペクトル分解可能である．A_i の固有値，固有ベクトルをそれぞれ $a_j^{(i)}, |a_j^{(i)}\rangle$ と書くと $\Gamma^{(2m)}$ は

$$\Gamma^{(2m)} = \sum_{i=1}^{2}\sum_{j=1}^{m} a_j^{(i)} |a_j^{(i)}\rangle\langle a_j^{(i)}| \otimes |x_i\rangle\langle x_i| \quad (4)$$

となる．ただし，$\{|a_j^{(i)}\rangle\}$ は正規直交する．式 (4) より，グラム行列 $\Gamma^{(2m)}$ の固有値，固有ベクトルが，それぞれ $a_j^{(i)}, |a_j^{(i)}\rangle \otimes |\lambda_i\rangle$ となることがわかる．つまり，$2m$ 次のエルミート行列である $\Gamma^{(2m)}$ の固有値，固有ベクトルを求めるには，m 次のエルミート行列である A_i の固有値，固有ベクトルを求めれば十分である．

3　おわりに

本稿では，M 元非対称信号に対する通信路行列公式を与えることを目的とし，$M = 2m$，すなわち偶数元の場合の ASK 信号について，信号の部分的な対称性を利用することで，問題の規模を半分の m にすることができることを示した．

参考文献

[1] P. Hausladen, R. Jozsa, B. Schumacher, M. Westmoreland, and W. K. Wootters, Phys. Rev. **A54**, pp.1869-1876, (1996).

[2] M. Ban, K. Kurokawa, R. Momose, and O. Hirota, Int. J. Theor. Phys. **36**, no.6, pp.1269-1288, (1997).

公表論文

1. **宮崎**, 吉田, 臼田, 令和元年度電気・電子・情報関係学会東海支部連合大会, F5-4, (2019).
2. **宮崎**, 吉田, 臼田, 第 42 回情報理論とその応用シンポジウム, 予稿集 2.3.3, (2019).
3. **宮崎**, 吉田, 王, 臼田, WiNF2019, P218, (2019).