符号化を用いた量子信号系の対称化に関する研究

田中 美波　　指導教員：臼田 毅

1　はじめに

近年，従来通信の性能をはるかに上回る通信として，伝送媒体に量子状態を用いる量子通信が着目されている．その中でも，本研究で扱う古典-量子通信とは，従来通信において伝送される古典情報を量子状態を用いて伝送する通信である．

量子通信に関する研究の中で，誤り率最小化や相互情報量最大化などの性能向上のための研究では，“対称”な量子信号として定義される群共変的信号が重要となる．しかし，応用上有用な拡大体上の符号を古典情報とする量子信号系は，一般に群共変性を持たない．その原因として，レター状態として用いる PSK（Phase Shift Keying）コヒーレント状態信号が拡大体に関して群共変的でないことが考えられる．まず，4PSK コヒーレント状態信号が最も単純な拡大体 $\mathbb{F}_{2^2} = \mathbb{F}_4$ に関して群共変性をもつように符号化することを提案する．その後，群共変的信号を構成する拡大体上の符号の構成法を示す．

また，通信を実現する上で重要となる信号の中には，ASK（Amplitude Shift Keying）コヒーレント状態信号や QAM（Quadrature Amplitude Modulation）コヒーレント状態信号などの非対称信号も存在する．4PSK コヒーレント状態信号に対して用いた符号化というアイデアを，これらの非対称信号の対称化へ応用することを考える．本稿では，最も単純な非対称信号である 3ASK コヒーレント状態信号を対称化する方法を示し，対称化された信号系の性能についても述べる．

2　本研究で用いる量子信号系

量子状態集合を $\{|\psi_i\rangle\}_{i=0}^{m-1}$ とする．この量子状態集合をレター状態とよび，符号長 n の m 元符号 $C = \{\boldsymbol{w} = (w_1, \ldots, w_n)\}$ で符号化した場合，各符号語に対応する量子状態 $|\boldsymbol{w}\rangle$ は以下のようにテンソル積で構成される．

$$|\boldsymbol{w}\rangle = |\psi_{w_1}\rangle \otimes \cdots \otimes |\psi_{w_n}\rangle \tag{1}$$

また，本研究では，レター状態集合としてコヒーレント状態信号を用いる．コヒーレント状態は，レーザー光で近似される最も簡単な光の量子状態であり，複素振幅 α，光子数状態 $|n\rangle$ を用いて以下で表される．

$$|\alpha\rangle = \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} \mathrm{e}^{-\frac{1}{2}|\alpha|^2} |n\rangle \tag{2}$$

3　量子信号の対称性

量子信号系が群の構造を持つとき，量子信号は対称であると定義される．具体的に，対称な量子信号は群共変的信号と呼ばれ，以下のように定義される．

定義 1：群共変的量子信号 [1]

$(G;\circ)$ を有限群[*1]とする．量子信号系 $\{|\psi_i\rangle \mid i \in G\}$ は

$$U_k |\psi_i\rangle = |\psi_{k\circ i}\rangle\,,\ \forall k, i \in G \tag{3}$$

を満たすユニタリ作用素 U_k が存在するとき $(G;\circ)$ に関して群共変的であるという．

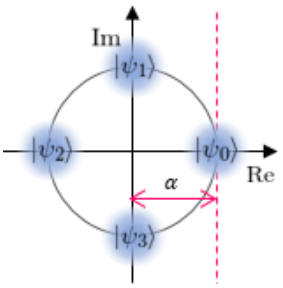

図 1　4PSK 信号

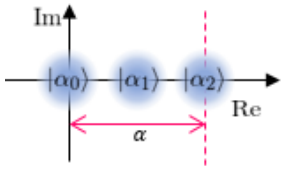

図 2　3ASK 信号

また，量子信号系が群共変であるかどうかを判断するための必要十分条件も以下に示す．

命題 2：群共変的量子信号の必要十分条件 [1]

量子信号系 $\{|\psi_i\rangle \mid i \in G\}$ が $(G;\circ)$ に関して群共変的であるための必要十分条件は，任意の $k \in G$ に対し，

$$\forall i, j \in G, \langle\psi_{k\circ i}|\psi_{k\circ j}\rangle = \langle\psi_i|\psi_j\rangle \tag{4}$$

が成り立つことである．

命題 2 より，量子信号の群共変性は，信号の内積で構成されるグラム行列 $\Gamma_{ij} = [\langle\psi_i|\psi_j\rangle]$ のみで決まる．

4　4PSK コヒーレント状態信号の対称化

q-PSK（Phase Shift Keying）コヒーレント状態信号は，振幅 α を用いて以下のように表される．

$$|\psi_i\rangle = \left|\alpha \exp\left[\mathbf{i}\frac{2\pi i}{q}\right]\right\rangle \tag{5}$$

但し，$\mathbf{i} = \sqrt{-1}$．本研究では，4PSK コヒーレント状態信号（図 1．以下，4PSK 信号）を扱う．4PSK 信号のグラム行列は

$$\Gamma_{\mathrm{4PSK}} = \begin{pmatrix} 1 & \kappa_1 & \kappa_2 & \kappa_1^* \\ \kappa_1^* & 1 & \kappa_1 & \kappa_2 \\ \kappa_2 & \kappa_1^* & 1 & \kappa_1 \\ \kappa_1 & \kappa_2 & \kappa_1^* & 1 \end{pmatrix} \tag{6}$$

である．但し，$\kappa_1 = \exp[(-1+\mathbf{i})\alpha^2]$，$\kappa_2 = \exp[-2\alpha^2]$ である．このグラム行列と式 (4) より，4PSK 信号は整数剰余環 $\mathbb{Z}_4$ に関して群共変的であり，拡大体 $\mathbb{F}_4$ に関しては群共変性をもたないことがわかるが，4PSK 信号に対して以下の命題が成り立つ．

命題 3：4PSK 信号の $\mathbb{F}_4$ に関する対称化 [B]

拡大体 $\mathbb{F}_4$ 上の群符号 $C_{\mathrm{sym1}} := \{00, 13, 22, 31\}$ で符号化された 4PSK 信号は，符号 C_{sym1} と $\mathbb{F}_4$ に関して群共変的となる．

この命題は，式 (1) に従って構成された，C_{sym1} に対応する符号語量子状態集合のグラム行列と，命題 2 から簡単に証明することができる．

[*1] ほとんどの場合で整数剰余環 $(\mathbb{Z}_m;+)$ もしくは拡大体 $(\mathbb{F}_q;+)$ を用いる．ただし，m は 2 以上の整数，q は素数べき．

次に，命題 4 に基づいて，$\mathbb{F}_4$ 上の (n,k)-線形符号 C から新しく符号長 $2n$ の符号を構成する．その準備として，以下の写像 $f:\mathbb{F}_4\to\mathbb{F}_4$ を定義する．

$$f(a)=\begin{cases} a & \text{if } a\in\{0,2\} \\ a+2 & \text{if } a\in\{1,3\} \end{cases} \tag{7}$$

この写像を用いて以下のように C の拡大符号を構成する．

定義 4：C_{sym1} を用いた $\mathbb{F}_4$ 上の線形符号の拡大 [B]

符号長 n の拡大体 $\mathbb{F}_4$ 上の線形符号に対し，拡大符号 $C^{\mathrm{ex}}_{\mathrm{sym1}}(C)\in\mathbb{F}_4^{2n}$ を以下のように定義する．

$$C^{\mathrm{ex}}_{\mathrm{sym1}}(C)=\{(\boldsymbol{a}|\boldsymbol{b})\ |\boldsymbol{a}=(a_1,\dots,a_n)\in C \\ \boldsymbol{b}=(f(a_1),\dots,f(a_n))\in\mathbb{F}_2^n\} \tag{8}$$

この拡大符号 $C^{\mathrm{ex}}_{\mathrm{sym1}}(C)$ に対して，以下の命題を得る．

命題 5：$\mathbb{F}_4$ に関して対称化された 4PSK 信号の符号化 [B]

C が (n,k)-線形符号であるとき，量子信号系 $\{|\boldsymbol{w}_i\rangle\ |\ \boldsymbol{w}_i\in C^{\mathrm{ex}}_{\mathrm{sym1}}(C)\}$ は $C^{\mathrm{ex}}_{\mathrm{sym1}}(C)$ と $\mathbb{F}_4^k$ に関して群共変的となる．

この命題は，$C^{\mathrm{ex}}_{\mathrm{sym1}}(C)$ と同値な符号と，[A] で示した命題を用いて証明されるが，本稿では紙面の都合上，証明は省略する．

上記の定義 4 と命題 5 によって，符号化された 4PSK 信号が群共変的となるような符号の構成法を示すことができた．

5　3ASK コヒーレント状態信号の対称化

m-ASK (Amplitude Shift Keying) コヒーレント状態信号は，最大コヒーレント振幅 α を用いて以下のように表される．

$$|\alpha_k\rangle=\left|\frac{k}{m-1}\,\alpha\right\rangle \tag{9}$$

本研究では，3ASK コヒーレント状態信号（図 2．以下，3ASK 信号）を扱う．3ASK 信号のグラム行列は

$$\Gamma_{\mathrm{3PSK}}=\begin{pmatrix} 1 & \kappa & \kappa^4 \\ \kappa & 1 & \kappa \\ \kappa^4 & \kappa & 1 \end{pmatrix} \tag{10}$$

となる．但し，$\kappa=\exp[-(1/8)\alpha^2]$．上記のグラム行列より，3PSK 信号はどのような $(G;\circ)$ に対しても式 (2) の必要十分条件は満たさない．

この 3ASK 信号に対して，以下の命題が成立する．

命題 6：3ASK 信号の対称化 [C]

拡大体 $\mathbb{F}_4$ 上の群符号 $C_{\mathrm{sym2}}:=\{00,01,20,21\}$ で符号化された 3ASK 信号は，拡大体 $\mathbb{F}_4$ に関して群共変となる．

上記の命題は，以下のように計算される対称化された 3ASK 信号 $\{|\boldsymbol{x}\rangle\ |\ \boldsymbol{x}\in C_{\mathrm{sym2}}\}$ のグラム行列

$$\Gamma_{C_{\mathrm{sym2}}}=\begin{pmatrix} 1 & \kappa & \kappa^4 & \kappa^5 \\ \kappa & 1 & \kappa^5 & \kappa^4 \\ \kappa^4 & \kappa^5 & 1 & \kappa \\ \kappa^5 & \kappa^4 & \kappa & 1 \end{pmatrix} \tag{11}$$

より明らかである．

対称化された 3ASK 信号の通信路容量を図 3 のグラフに示す．

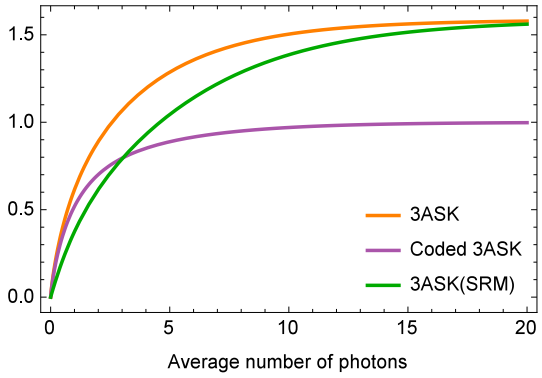

図 3　符号化された 3ASK 信号の通信路容量

紫線が対称化された 3ASK 信号の通信路容量である．比較として，橙線は元の 3ASK 信号のフォンノイマンエントロピー（先験確率に関して最適化をすれば通信路容量），緑線は誤り率に関して準最適測定である Square-root measurement（SRM）を用いて 3ASK 信号を測定したときの相互情報量である．このグラフより，平均光子数が小さいときには，対称化された 3ASK 信号は元の 3ASK 信号の通信路容量をほぼ達成することがわかる．

さらに，対称化された 3ASK 信号に対して以下が示される．

命題 7：対称化された 3ASK 信号の符号化 [C]

対称化された 3ASK 信号 $\{|\boldsymbol{x}\rangle\ |\ \boldsymbol{x}\in C_{\mathrm{sym2}}\}$ は，$\mathbb{F}_4$ 上の (n,k)-線形符号で符号化されると符号 C と $\mathbb{F}_4^k$ に関して群共変となる．

これは，命題 5 と同様に，[A] で示した命題を用いて証明される．

6　おわりに

本研究では，符号化を行うことによって，4PSK 信号が拡大体 $\mathbb{F}_4$ に関して群共変的となることを示し，その上で，符号化された 4PSK コヒーレント状態信号が群共変的となるような $\mathbb{F}_4$ 上の符号の構成法を示した．さらに，非対称信号である 3ASK 信号に対しても，符号化を行うことで群共変的となることを示し，対称化された 3ASK 信号は平均光子数が小さいとき，元の 3ASK 信号の通信路容量を達成する可能性を示した．

今後の課題として，今回の対称化の方法を，元数の大きい PSK 信号や ASK 信号へ拡張していくこと，また，レートの高い対称化する符号を探すことなどが挙げられる．

参考文献

[1] T. S. Usuda and I. Takumi, QCMC2, Plenum Press, New York, pp.37-43, (2000).

公表論文

[A] **M. Tanaka**, T. Sogabe, K. Shiromoto, T. S. Usuda, Proceedings of ISITA2014, p.348, (2014).

[B] **M. Tanaka**, A. Ohashi, and T. S. Usuda, Proceedings of ISITA2016, pp.692-696, (2016).

[C] **田中**, 大橋, 臼田, 第 39 回情報理論とその応用シンポジウム (SITA2016), pp.354-359, (2016).

他 5 件 (筆頭著者)，3 件 (第二以降著者)