

拡大体 \mathbb{F}_4 上の線形符号で符号化された 4PSK 信号の群共変性と通信路行列公式

情報科学科 田中 美波

指導教員：白田 毅

1 はじめに

通信システムの誤り率や相互情報量などの値は通信路行列から計算されるため、通信システムの性能の評価には通信路行列が必要となる。光の量子状態を通信媒体として古典情報を伝達する古典-量子通信では、汎用的なアルゴリズムにより通信路行列を求めることが計算量的に困難であるため、それを解析的に求めるための通信路行列公式が重要となり、その導出には量子信号系の“群共変性”という性質が用いられる。

本研究では、応用上有用となる拡大体 \mathbb{F}_q 上の線形符号により符号化された q -PSK コヒーレント状態信号 (q -PSK 信号とかく) の通信路行列を求めることを目的とし、まずは $\mathbb{F}_{2^2} = \mathbb{F}_4$ 上の線形符号により符号化された 4PSK 信号の群共変性について考察し、通信路行列公式の一例を示す。

2 $(G; \circ, \hat{\chi})$ -共変的信号

本研究で扱う $(G; \circ, \hat{\chi})$ -共変的信号の定義を以下に示す。

定義 1 : $(G; \circ, \hat{\chi})$ -共変的信号 [2]

$(G; \circ)$ を有限群とする。量子信号系 $\{|\psi_i\rangle \mid i \in G\}$ は、

$$\forall i, k \in G, \exists V_k, V_k|\psi_i\rangle = \hat{\chi}(k, i)|\psi_{koi}\rangle \quad (1)$$

であるとき、 $(G; \circ, \hat{\chi})$ -共変的であるという。ただし、 V_k はユニタリまたは反ユニタリ作用素である。また、 $\hat{\chi}(i, j)(i, j \in G)$ は $\hat{\chi}: G \times G \rightarrow \mathbb{U} = \{x \in \mathbb{C} \mid |x| = 1\}$ なる写像であり、 \mathbb{C} は複素数全体である。

3 R 上の符号で符号化された $(R, +; \hat{\chi})$ -共変的信号

R を整数剰余環 \mathbb{Z}_m または拡大体 \mathbb{F}_q とし、符号語を構成する R の要素に対応する各レター状態の集合 $\{|\psi_i\rangle \mid i \in R\}$ が $(R; +, \hat{\chi})$ -共変的であるとする。

V_k がユニタリとなる k の集合を H_U 、反ユニタリとなる集合を H_A と置くと、以下の命題が成り立つことがわかった。

命題 2 : $(C; +, \hat{\chi}')$ -共変的信号

R 上の線形符号 C で符号化された状態集合 $\{|\mathbf{v}\rangle \mid \mathbf{v} \in C\}$ は、以下の条件を満たすとき、 $(C; +, \hat{\chi}')$ -共変的となる。ここで、 $\hat{\chi}'$ は、 $\mathbf{v} = (a_0, a_1, \dots, a_{n-1})$ 、 $\mathbf{w} = (b_0, b_1, \dots, b_{n-1}) \in C$ に対して

$$\hat{\chi}'(\mathbf{v}, \mathbf{w}) = \prod_{x=0}^{n-1} \hat{\chi}(a_x, b_x) \quad (2)$$

のように定義される写像で、 $a_x, b_x \in R$ である。ただし、以下の条件が必要となる。

【条件】任意の符号語 $\mathbf{u}, \mathbf{v}, \mathbf{w} \in C$ をそれぞれ (i_0, \dots, i_{n-1}) 、 (j_0, \dots, j_{n-1}) 、 (k_0, \dots, k_{n-1}) とおき、対応する量子符号語を $|\mathbf{u}\rangle = |\psi_{i_0}\rangle \otimes \dots \otimes |\psi_{i_{n-1}}\rangle$ 、 $|\mathbf{v}\rangle = |\psi_{j_0}\rangle \otimes \dots \otimes |\psi_{j_{n-1}}\rangle$ 、 $|\mathbf{w}\rangle = |\psi_{k_0}\rangle \otimes \dots \otimes |\psi_{k_{n-1}}\rangle$ とするとき、式 (3) または (4) が常に成り立つ。

$$\prod_{\{x|k_x \in H_A\}} \langle \psi_{i_x} | \psi_{j_x} \rangle = \prod_{\{x|k_x \in H_A\}} \langle \psi_{j_x} | \psi_{i_x} \rangle \quad (3)$$

$$\prod_{\{x|k_x \in H_U\}} \langle \psi_{i_x} | \psi_{j_x} \rangle = \prod_{\{x|k_x \in H_U\}} \langle \psi_{j_x} | \psi_{i_x} \rangle \quad (4)$$

4 \mathbb{F}_4 上の符号で符号化された 4PSK 信号

命題 2 より、4PSK 信号が $(\mathbb{F}_4; +, \hat{\chi})$ -共変的であれば \mathbb{F}_4 上の符号で符号化された 4PSK 信号も群共変的であることがいえる。ここで、定義 1 における V_k をユニタリに限定する場合と、反ユニタリまで考慮する場合の二種類の定義に基づいて群共変性を考察する。

ユニタリに限定した場合

ユニタリに限定した場合については、4PSK 信号の平均光子数を $N_S = \frac{\pi}{2}$ に固定した場合、群共変的となることが分かった。具体例をあげると、 $N_S = \frac{\pi}{2}$ とすると、命題 2 より \mathbb{F}_4 上の $(3,1)$ 線形符号 $C = \{000, 121, 232, 313\}$ で符号化された 4PSK 信号は群共変的となる。通信路行列は信号系のグラム行列の平方根を求めることにより計算されるため、グラム行列の固有値 λ と固有ベクトル $\boldsymbol{\lambda}$ の解析解を求めれば、それが通信路行列公式となる。この例について通信路行列公式を求めると、

$$\lambda = \begin{cases} 1 - a \pm (b + c) \\ 1 + a \pm (b - c) \end{cases} \quad (5)$$

$$\boldsymbol{\lambda} = \begin{pmatrix} 1 \\ 1 \\ \mathbf{i} \\ \mathbf{i} \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ -\mathbf{i} \\ -\mathbf{i} \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ \mathbf{i} \\ -\mathbf{i} \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ -\mathbf{i} \\ \mathbf{i} \end{pmatrix} \quad (6)$$

のように求めることができる。ただし、 $a = e^{2\pi}$ 、 $b = e^{-5\pi/2}$ 、 $c = e^{-3\pi/2}$ である。これは、すでに一般の通信路行列公式が導出されている狭義群共変的信号の通信路行列公式 [1] と類似している。具体的には式 (6) の \mathbf{i} がすべて 1 に置き換わると一致する。

反ユニタリまで考慮する場合

ユニタリに限定した場合には平均光子数に制約があるのに対して、反ユニタリまで考慮すると 4PSK 信号は常に群共変的となることを示した。しかしながら、本質的な \mathbb{F}_4 上の符号で命題 2 の条件を満たす符号の例は見つかっていない。

5 まとめ

命題 2 を示し、これより \mathbb{F}_4 上の符号で符号化された 4PSK 信号が群共変となる例、通信路行列公式の例を示した。今後の課題として、反ユニタリまで考慮する場合に条件を満たす \mathbb{F}_4 上の符号を探るか存在しないことを示すこと、[1] を参考に一般の線形符号に対する通信路行列公式の導出を目指すことがあげられる。

参考文献

- [1] S. Usami, T.S. Usuda, I. Takumi, and M. Hata, IEICE Trans. Fundamentals. E82-A, no.10, pp.2185-2190, (1999).
- [2] T.S. Usuda, Y. Ishikawa, and K. Shiromoto, Abst. of Papers of QCMC2012, p.361, (2012).

公表論文

- 1) 田中, 岩田, 曾我部, 白田, 平成 26 年度電気・電子・情報関係学会東海支部連合大会 講演論文集, J1-2, (2014).
- 2) 田中, 曾我部, 城本, 白田, 第 37 回情報理論とその応用シンポジウム (SITA2014), pp.242-247, (2014).
- 3) M. Tanaka, T. Sogabe, K. Shiromoto, and T.S. Usuda, Proc. of ISITA2014, p.348, (2014).