“けちん坊”量子情報源に近い特性を持つ有限集合

情報科学科　玉腰 友也　　指導教員：臼田 毅

1　はじめに

量子状態を用いた古典情報の伝送を古典-量子通信と呼ぶ．通信性能を評価する指標の一つに相互情報量がある．量子測定過程を通して得られる相互情報量の最大値をアクセシブル情報量という．このアクセシブル情報量の最良の上界と下界として，von Neumann エントロピーとサブエントロピーが知られている．この下界を達成するものとして Scrooge ensemble（けちん坊量子情報源）[1] は定義される．けちん坊量子情報源は，いかに量子測定を工夫しても，ほとんど情報が得られないという意味で，情報を漏らさないことが要求されるセキュリティへの応用が期待される．

従来の常識では，けちん坊量子情報源は無限集合とされていたが，本研究では，応用のため，有限のけちん坊量子情報源が存在するか否かを追求する．まず，本稿では，Weyl-Heisenberg 共変的信号 [2] という，状態数が 4 個に制限されたクラスを扱い，アクセシブル情報量を最小とする量子情報源を明らかにする．

2　アクセシブル情報量の下界 [1]

n 次元ヒルベルト空間 $\mathcal{H}_n$ における m 元の量子状態 $|\psi_i\rangle$ がそれぞれ確率 p_i で発生する量子情報源 $\mathcal{E}$ を考える．ただし，$i = 1, 2, \ldots, m$．$\mathcal{E}$ を測定過程 $\Pi = \{\hat{\Pi}_j \mid 1, \ldots, r\}$ で測定したときの相互情報量を $I(\mathcal{E}, \Pi)$ と表すと，アクセシブル情報量は，

$$I_{\rm ac} = \max_{\Pi} I(\mathcal{E}, \Pi) \tag{1}$$

により定義される．$\mathcal{E}$ の密度作用素 $\rho = \sum_{i=1}^{m} p_i |\psi_i\rangle\langle\psi_i|$ を用いてサブエントロピー $Q(\rho)$ は以下のように計算される．

$$Q(\rho) = -\sum_{k=1}^{n} \left(\prod_{l \neq k} \frac{\lambda_k}{\lambda_k - \lambda_l} \right) \lambda_k \ln \lambda_k \tag{2}$$

ただし，λ_k $(k = 1, 2, \ldots, n)$ は ρ の固有値である．

3　Weyl-Heisenberg (WH) 共変的量子状態集合

本稿では，信号のクラスとして生起確率が等確率である 2 次元の Weyl-Heisenberg (以降，WH) 共変的量子状態集合 [2] を扱う．2 次元の WH 共変的量子状態集合は，基点ベクトル

$$|f(\theta, \phi)\rangle = \begin{pmatrix} \cos\theta \\ e^{i\phi} \sin\theta \end{pmatrix}, (i = \sqrt{-1}) \tag{3}$$

を用いて以下のように定義される．

$$\{|\psi_i\rangle\} = \{|\psi_0\rangle, X|\psi_0\rangle, Z|\psi_0\rangle, XZ|\psi_0\rangle\} \tag{4}$$

$$|\psi_0\rangle = |f(\theta, \phi)\rangle \tag{5}$$

ただし，X と Z はパウリ作用素である．信号が群共変的であるとき，アクセシブル情報量を達成する測定も群共変的となることが知られている．しかし，測定に関しては，基点ベクトルが一般には複数必要であり，厄介である．本研究では，WH 共変的信号に対しては，測定に対する基点ベクトルが一つで十分であることを証明した（詳細は略）．このため，信号も測定も各一つの基点ベクトルで特徴付けることができる．本稿では，信号と測定に対応する基点ベクトルをそれぞれ，$|f(\theta, \phi)\rangle$ と $|f(\theta', \phi')\rangle$ と表す．

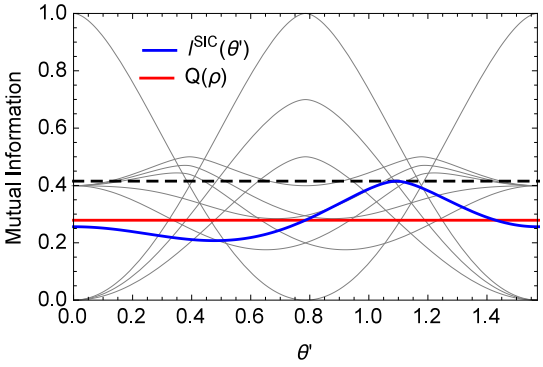

図 1　Weyl-Heisenberg (WH) 共変的信号の相互情報量

4　アクセシブル情報量の最小値

基点ベクトルを変化させて生成される全ての WH 共変的信号に対してアクセシブル情報量を計算したとき，最も下界に近くなる値，すなわち，最小値

$$I_{\rm ac}^{(\rm min)} = \min_{\mathcal{E}} \max_{\Pi} I(\mathcal{E}, \Pi) \tag{6}$$

を考える．$\mathcal{E}$, Π はそれぞれ (θ, ϕ), (θ', ϕ') の関数である．式 (6) を数値的に求めると，$I_{\rm ac}^{(\rm min)} = 0.41504$ となった．これは，WH 共変的信号が SIC (Symmetric Informationally Complete) 集合 [2] となる場合 ([3] の式 (23)) のアクセシブル情報量と一致する．図 4 に $I_{\rm ac}^{(\rm min)}$(黒破線) といくつかの WH 共変的信号の相互情報量を示す．赤線は $Q(\rho)$，青線は SIC 集合の相互情報量 $I^{\rm SIC}(\theta')$，その他は θ，ϕ を $0 \sim \pi/2$ まで $\pi/16$ 刻みで変化させた WH 共変的信号の相互情報量である (ただし，すべての場合で $\phi' = \phi$)．青線の最大値が黒破線と一致，その他の線の最大値は，いずれも黒破線よりも大きくなっていることが確認できる．

5　おわりに

信号のクラスとして 2 次元の Weyl-Heisenberg 共変的信号を用いて，アクセシブル情報量が最小となるものを数値計算により求めた．その結果，SIC 集合と呼ばれる量子状態集合の相互情報量に一致した．下界を達成する情報源は無限集合とされていたが，2 次元を考えたとき SIC 集合を用いると，アクセシブル情報量がもっとも下界に近くなることがわかった．SIC 集合による量子測定は，完全に情報を引き出せるという性質がある．それに対し，SIC 集合による信号は，逆にもっとも情報を与えないということは，非常に興味深い．今後は，信号数を増やした場合のアクセシブル情報量の最小値について調査し，信号数毎に最もけちん坊量子情報源に近い集合の条件を明らかにする．

参考文献

[1] R. Jozsa *et al.*, Phys. Rev. **A49**, pp.668-677, (1994).
[2] C.A. Fuchs, QCMC2010, Prize Talk, (2010).
[3] J.M. Renes *et al.*, J. Math. Phys. **45**, pp.2171-2180, (2004).

公表論文

1. 玉腰友也，田中美波，臼田毅，平成 28 年度電気・電子・情報関係学会東海支部連合大会，B3-2，(2016).