2 次のレニー情報量を規準とした “けちん坊” 量子情報源に関する研究

情報科学科　佐藤 圭介　　指導教員：臼田 毅

1 はじめに

量子通信とは，情報の伝送に量子状態を使用する通信である．古典情報を量子状態に対応付けた量子通信を古典-量子通信と呼ぶ．量子通信では，量子情報源を固定し，測定を変化させることで得られる最大の相互情報量としてアクセシブル情報量が定義される．アクセシブル情報量の下界を達成する量子情報源を “Scrooge Ensemble”（以降，けちん坊量子情報源）と呼ぶ [1]．けちん坊量子情報源は，最も情報を与えないという意味で，セキュリティへの応用が期待される．けちん坊量子情報源は，従来，無限集合とされていたが，応用を考えるのであれば，有限集合が望まれる．したがって，本研究の目的は有限のけちん坊量子情報源の存在を調査することである．

けちん坊量子情報源を考えるためには，相互情報量の最大化を考える必要がある．しかし，相互情報量の定義式に含まれる対数ゆえに，直接，相互情報量を最大化するのは困難である．そこで，本研究では，相互情報量の上界である，2 次の相互レニー情報量に対して，測定に関する最大化を考える．具体的には，文献 [2] にある，群共変的信号に対する相互情報量の最大化に関する定理が 2 次のレニー情報量規準でも成り立つことを示した．

2 相互レニー情報量

アルファベット $\mathcal{X}$ の離散確率変数 X に対して，レニーエントロピー[*1] $R(Y)$ は，次のように定義される．

$$R(Y) := -\log_2 \left(\sum_{j\in\mathcal{Y}} P(j)^2 \right). \tag{1}$$

レニーエントロピーを用いて条件付きレニーエントロピーが $R(Y|X) := \sum_{i\in\mathcal{X}} P(i)R(Y|X=i)$ のように定義される．そして，相互レニー情報量 $I_R(Y;X)$ は，これらの差として $I_R(Y;X) := R(Y) - R(Y|X)$ のように定義される [3]．

一般に，相互レニー情報量は，シャノンの相互情報量とは異なり，対称性，加法性，また，凸性を持たない．本研究では，Y を測定結果に関する確率変数，X を信号に関する確率変数とし，$I_R(Y;X)$ を相互レニー情報量として用いる．

3 群共変的信号・測定

量子信号（測定）が群共変的であるとは，文献 [2] にて以下のように定義された．ただし，$(G;\circ)$ を有限群，U_g を $g\in G$ のユニタリ表現とする．

定義 1：**群共変的信号**

先験確率が等確率 $|G|^{-1}$ である信号系 $\{\rho_i : i\in G\}$ を考える．この信号系が次の性質を満たすとき，信号系は群共変的であるという．

$$U_g\rho_i U_g^\dagger = \rho_{g\circ i} \quad (\forall g, i\in G). \tag{2}$$

定義 2：**群共変的測定**

測定 $\Pi = \{\Pi_j : j\in G\}$ を考える．この測定が次の性質を満たすとき，測定は群共変的であるという．

$$U_g\Pi_j U_g^\dagger = \Pi_{g\circ j} \quad (\forall g, j\in G). \tag{3}$$

定義から分かるように，群共変的信号（測定）とは，任意の信号（決定作用素）の G 軌道と元の信号系（測定）が一致するような信号系（測定）である．

4 群共変的信号を用いた相互レニー情報量を最大化する測定

シャノン情報量を規準とした場合，既約なユニタリ表現を持つ群に関して群共変的な信号に対しては，ランク 1 の群共変的測定によって相互情報量が最大化されることが文献 [2] に示されている．本研究では，相互レニー情報量がシャノンの相互情報量にある性質（e.g., 加法性）を持たないにも関わらず，相互レニー情報量を規準とした場合にも，Davies が示した定理と同じ命題が成り立つことを示した（紙面の都合のため，証明は省略する）．

命題 3

信号が既約なユニタリ表現 U_g $(g\in G)$ を持つ有限群 G に関して群共変的であるとする．このとき，相互レニー情報量を最大にする測定として，ランク 1 の群共変的測定が存在する．

この命題により，仮定を満たす量子情報源の相互レニー情報量の最大値を求める際に，測定をランク 1 の群共変的測定に絞ることができる．また，群共変性から相互レニー情報量の解析が容易になる．

5 おわりに

信号が既約なユニタリ表現を持つある群 G に関して群共変的である場合，相互レニー情報量を最大化する測定として，ランク 1 の群共変的測定が存在することを示した．

今後の課題として，シャノン情報量規準において示されている「群が可約表現を持つ場合に，相互情報量を最大化する測定」についての定理 [4] が，レニー情報量規準においても成り立つのかを考える必要がある．

参考文献

[1] R. Jozsa, *et al.*, Phys. Rev. **A49**, pp.668-677, (1994).

[2] E.B. Davies, IEEE Trans. Inform. Theory **IT-24**, pp.596-599, (1978).

[3] C.H. Bennett, *et al.*, IEEE Trans. Inform. Theory **41**, pp.1915-1923, (1995).

[4] T. Decker, IEEE Trans. Inform. Theory **55**, pp.2375-2383, (2009).

公表論文

1. **佐藤 圭介**, 高比良 宗一, 臼田 毅, 平成 29 年度電気・電子・情報関係学会東海支部連合大会, E3-4, (2017).
2. **佐藤 圭介**, 高比良 宗一 臼田 毅, 第 40 回情報理論とその応用シンポジウム 予稿集, pp347-352, (2017).
3. **K. Sato**, S. Takahira, and T.S. Usuda, QCMC2018, accepted.

[*1] 2 次のレニーエントロピー，2 次の条件付きレニーエントロピー，また，2 次の相互レニー情報量を，しばしば “2 次の” を省略して呼ぶ [3] ため，本稿でも “2 次の” という言葉を省略する．