複数の量子通信路を識別する量子アルゴリズムの誤り確率のより精密な下界

伊藤凌 [1]　　森立平 [1,2]

[1] 東京工業大学情報理工学院
School of Computing, Tokyo Institute of Technology
[2] 国立研究開発法人科学技術振興機構さきがけ
Japan Science and Technology Agency, PRESTO

1　導入

1.1　背景

既知の量子状態の有限族 $\{\rho_A^\xi\}_{\xi\in\Xi}$ の中の一つの ρ_A^ξ が測定可能な状態として与えられたとき, その状態の添字 ξ を決定する問題は量子状態識別問題と呼ばれ, 詳しく研究されている. 量子状態識別問題の中でも最も単純なものは二つの量子状態 $\{\rho_A^0, \rho_A^1\}$ を識別する問題であり, この問題に対する最小誤り確率とそれを達成する測定を構成する方法は広く知られている [1]. また複数の量子状態を適当な測定で識別したときに誤り確率が厳密に 0 になるための必要十分条件は, それらの状態が全て互いに直交していることである [2]. さらに複数の量子状態を識別する問題において最小誤り確率を達成する測定は半正定値計画問題の解として表すことが可能である [1].

量子状態の識別問題と密接に関連した問題として, 量子状態に対する物理的操作と同一視できる量子通信路の識別問題も近年研究が盛んである. 既知の量子通信路の有限族 $\{\mathcal{O}_{A\to B}^\xi\}_{\xi\in\Xi}$ の中の一つの $\mathcal{O}_{A\to B}^\xi$ が繰り返し使用可能なオラクルとして与えられたとき, そのオラクルの添字 ξ を決定する問題を量子通信路識別問題という. 量子通信路識別問題を解くアルゴリズムは与えられたオラクルに対するクエリ方法に応じて非適応的アルゴリズムと適応的アルゴリズムに分類される. 非適応的アルゴリズムでは予め定めた量子状態をオラクルに並列に入力する. 一方, 適応的アルゴリズムではオラクルの出力をオラクルの入力として再使用することが許される. 二つの量子通信路を非適応的アルゴリズムで識別する際の誤り確率については二つの量子状態を識別する際の誤り確率と同様に達成可能な下界が与えられており [1], その値は半正定値計画問題の最適値として表すことが可能である [3].

量子通信路の識別では一般的に補助空間（直接オラクルを適用しない空間）を使用することで最小誤り確率の値が改善されるため補助空間の次元についても研究がされている [1]. 一般の二つの量子通信路を非適応的アルゴリズムで識別する場合は, 補助空間の次元がオラクルの入力空間の次元以上であると最小誤り確率を達成するアルゴリズムが存在する [1]. さ

らに二つの等長通信路を非適応的アルゴリズムで識別する場合は補助空間を使用せずとも最小誤り確率を達成できる [1].

量子通信路にクエリする回数が多い程, 識別誤り確率は小さくなるため, そのトレードオフを明らかにすることは重要な問題である. 二つのユニタリ通信路の識別問題はよく研究されており, クエリ回数と識別誤り確率のトレードオフがほぼ完全に知られている [4]. このとき, 非適応的アルゴリズムがその最適なトレードオフを達成する. 一方, 一般の二つの量子通信路識別問題では適応的アルゴリズムが非適応的アルゴリズムよりも誤り確率が真に小さくなる例が知られている [5]. また一般の二つの量子通信路識別問題について, 十分な回数のクエリをした時に誤り確率が厳密に 0 になるための簡単な必要十分条件が知られている [6]. しかし, 量子通信路に仮定を置かずにクエリ回数と識別誤り確率のトレードオフを解析する研究は少ない [7]. 特に量子通信路の数が三つ以上の場合についての研究はほとんどない.

複数の量子通信路を識別する問題の簡単な一例として Grover の探索問題が挙げられる. Grover の探索問題において識別するオラクルが N 個であるとき $O(\sqrt{N})$ 回のクエリを用いる適応的アルゴリズムとして Grover 探索が知られている [8]. Grover 探索の漸近的な最適性, すなわち Grover の探索問題に対して高確率で正しい解を与えるには $\Omega(\sqrt{N})$ 回のクエリが必要であることは Bennett らにより証明されている [9]. クエリ回数を固定した際の Grover 探索の誤り確率の最適性は Zalka によって証明されている [10].

1.2 本研究の結果

本研究では量子通信路識別問題を一般化した量子通信路グループ識別問題を考え, 与えられたクエリ回数のもとでの最小誤り確率の下界を導出した. 本研究で用いる手法は Zalka がグローバー探索の最適性の証明に用いたものに関連している [10]. Zalka は純粋状態同士の距離の下界評価にノルムの三角不等式を用いる代わりに角度の三角不等式を用いること誤り確率の精密な下界を導出した. 一般の量子通信路の場合については混合状態を扱う必要があるが, 本研究では Bures 角という量に注目することで Zalka の結果を一般化する形で誤り確率の下界を導出した.

さらに識別する量子通信路が二つだけである場合に対しユニタリ通信路識別問題の誤り確率の下界の導出を一般化することで別の形の誤り確率の下界を与えた.

1.3 論文の構成

本論文の構成を説明する. まず 2 節では量子通信路グループ識別アルゴリズムの枠組みを定式化する. 3 節では本研究の主たる結果である量子通信路グループ識別問題の誤り確率の下界を紹介する. 4 節では 3 節で紹介した下界の具体的な計算例を与える. 5 節, 6 節では 3 節で与えた下界の証明を与える。 7 節ではまとめと今後の課題を述べる.

2 問題の定義

以下, Ξ, H は有限集合とし, A, B, C, E, R は有限次元の量子系とする. また単に作用素と表記した場合, 有限次元線形作用素を指すものとする. まず量子情報理論において基本的な概念である密度作用素, 量子通信路, POVM を以下のように定義する.

定義 2.1. 条件 $\mathrm{Tr}\,(\rho_A) = 1$ を満たす半正定値作用素 ρ_A を密度作用素という．密度作用素 ρ_A が $\mathrm{rank}(\rho_A) = 1$ を満たすとき ρ_A は純粋状態であるという．

定義 2.2. 線形写像 $\Phi_{A\to B}$ が任意の作用素 X_A に対して $\mathrm{Tr}\,(\Phi_{A\to B}(X_A)) = \mathrm{Tr}\,(X_A)$ を満たし, かつ任意の有限次元恒等写像 $\mathbb{I}_C$ と任意の半正定値作用素 P_{AC} に対して $(\Phi_{A\to B}\otimes\mathbb{I}_C)\,(P_{AC})$ が半正定値作用素であるとき $\Phi_{A\to B}$ を量子通信路という．

定義 2.3. 半正定値作用素の族 $\{M_A^\eta\}_{\eta\in H}$ が条件 $\sum_{\eta\in H} M_A^\eta = I_A$ を満たすとき $\{M_A^\eta\}_{\eta\in H}$ を測定, または POVM という．

さらに ρ_A が密度作用素のとき確率質量関数 $\Pr(X=\eta) = \mathrm{Tr}\left(M_A^\eta\rho_A\right)$ に従う確率変数 X を「状態 ρ_A に POVM $\{M_A^\eta\}_{\eta\in H}$ を適用したときの観測値」という．$\{M_A^\eta\}_{\eta\in H}$ に対して集合 H を測定結果といい, 各 M_A^η を観測値 η に対応する測定作用素という．

本研究で取り扱う量子通信路識別問題を以下のように定義する．

定義 2.4. (量子通信路識別問題) 既知の量子通信路の有限族 $\{\mathcal{O}^\xi_{A\to B}\}_{\xi\in\Xi}$ の中の一つの $\mathcal{O}^\xi_{A\to B}$ が確率分布 $\{q_\xi\}_{\xi\in\Xi}$ に従って, 繰り返し使用可能なオラクルとして与えられるとする．このとき, 与えられたオラクルの添字 ξ を決定する問題を「確率分布 $\{q_\xi\}$ に従うオラクル $\{\mathcal{O}^\xi_{A\to B}\}$ の量子通信路識別問題」といい, $\mathrm{QCDP}(\{q_\xi\},\{\mathcal{O}^\xi_{A\to B}\})$ と表記する．

量子通信路識別問題の自然な一般化として, 量子通信路グループ識別問題を以下のように定義できる．

定義 2.5. (量子通信路グループ識別問題) $\{C_\eta\}_{\eta\in H}$ を Ξ の部分集合の族とし, 識別問題 $\mathrm{QCDP}(\{q_\xi\},\{\mathcal{O}^\xi_{A\to B}\})$ と同様にオラクル $\mathcal{O}^\xi_{A\to B}$ が与えられるとする．このとき $\eta\in C_\eta$ を満たすような部分集合の添字 $\eta\in H$ を決定する問題を「$\{C_\eta\}$ でグループ化され, 確率分布 $\{q_\xi\}$ に従うオラクル $\{\mathcal{O}^\xi_{A\to B}\}$ の量子通信路グループ識別問題」と呼び, この問題を $\mathrm{QCGDP}(\{q_\xi\},\{\mathcal{O}^\xi_{A\to B}\},\{C_\eta\})$ と表記する．ここで $\{C_\eta\}_{\eta\in H}$ は Ξ の分割とは限らず, $\xi\in C_\eta$ を満たす $\eta\in H$ が複数ある場合はどの η を出力しても構わない．$\xi\in C_\eta$ を満たす $\eta\in H$ が存在しない場合はどの η を出力しても識別失敗となる．

量子通信路グループ識別問題を解くアルゴリズムを考える．オラクルを並列に使用するアルゴリズムは非適応的アルゴリズムと呼ばれ, そうでないアルゴリズムは適応的アルゴリズムと呼ばれる．適応的アルゴリズムは一般的に以下のように記述される．

1. 量子計算機に初期状態 $\rho^{\mathrm{init}}_{AR}$ をセットする．
2. 与えられたオラクル $\mathcal{O}^\xi_{A\to B}$ と適切な量子通信路を交互に適用する．
3. 測定 $\{M^\eta_{BR}\}_{\eta\in H}$ を状態に適用し, 観測値 $\eta\in H$ を出力する．

つまり適応的アルゴリズムは初期状態 $\rho^{\mathrm{init}}_{AR}$, 各ステップで用いられる量子通信路, そして測定 $\{M^\eta_{BR}\}_{\eta\in H}$ により一意に定まる．そのため適応的アルゴリズムは以下のように定義できる．

定義 2.6. (適応的アルゴリズム) $\rho^{\mathrm{init}}_{AR}$ を密度作用素, $\{\Phi^k_{BR\to AR}\}_{k=1}^{n-1}$ を量子通信路の族, そして $\{M^\eta_{BR}\}_{\eta\in H}$ を POVM とする．このとき三つ組 $(\rho^{\mathrm{init}}_{AR},\{\Phi^k_{BR\to AR}\},\{M^\eta_{BR}\})$ を適応的アルゴリズムと呼ぶ．

任意の非適応的アルゴリズムは適当な計算 $\{\Phi^k_{BR\to AR}\}$ を用いることで適応的アルゴリズムに変換できるので, 以下では適応的アルゴリズムのみを考える.

オラクルの添字 $\xi\in\Xi$ に対しアルゴリズムの出力 $\eta\in H$ が $\xi\in C_\eta$ を満たすとき, またそのときに限りアルゴリズムは成功したとされる. QCGDP の最小誤り確率は以下のように定義される.

定義 2.7. (QCGDP の最小誤り確率) 三つ組 $(\rho^{\mathrm{init}}_{AR},\{\Phi^k_{BR\to AR}\},\{M^\eta_{BR}\})$ を識別問題 $\mathrm{QCGDP}(\{q_\xi\},\{\mathcal{O}^\xi_{A\to B}\},\{C_\eta\})$ に対するアルゴリズムとする. さらにそれぞれの $\xi\in\Xi$ に対し以下のように密度作用素を定義する.

$$\rho^{k,\xi}_{AR}\coloneqq\begin{cases}\rho^{\mathrm{init}}_{AR} & (k=0),\\ \Phi^k_{BR\to AR}\circ\mathcal{O}^\xi_{A\to B}(\rho^{k-1,\xi}) & (1\le k\le n-1),\end{cases}$$

$$\rho^{\mathrm{fin},\xi}_{BR}\coloneqq\mathcal{O}^\xi_{A\to B}(\rho^{n-1,\xi}_{AR}).$$

識別問題 $\mathrm{QCGDP}(\{q_\xi\},\{\mathcal{O}^\xi_{A\to B}\},\{C_\eta\})$ のクエリ回数 n の適応的アルゴリズムの最小誤り確率 $p_{\mathrm{err}}(n)$ を以下のように定義する.

$$p_{\mathrm{err}}(n)\coloneqq 1-\max_{\rho^{\mathrm{init}}_{AR},\{\Phi^k\},\{M^\eta_{BR}\}}\sum_{\xi\in\Xi}q_\xi\sum_{\eta:\xi\in C_\eta}\mathrm{Tr}\left(\rho^{\mathrm{fin},\xi}_{BR}M^\eta_{BR}\right).$$

識別問題 $\mathrm{QCDP}(\{q_\xi\},\{\mathcal{O}^\xi_{A\to B}\})$ に対する最小誤り確率も同様に定義される.

アルゴリズムの集合はコンパクトであるから各 QCGDP に対して最小誤り確率を達成するアルゴリズムが存在する. 最小誤り確率 $p_{\mathrm{err}}(n)$ の下界を与えるのが本研究の目的である.

3 本研究の結果

本研究で導出した QCGDP の誤り確率の下界を与えるために, まず二つの密度作用素の類似度を測る量であるフィデリティを導入する.

定義 3.1. 作用素 ρ_A,σ_A を密度作用素とする. このとき $F(\rho_A,\sigma_A)\coloneqq\|\sqrt{\rho_A}\sqrt{\sigma_A}\|_1$ で定義される関数 F を密度作用素のフィデリティという. ここで $\|\cdot\|_1$ は作用素のトレースノルムである.

本研究では QCGDP の誤り確率の下界をフィデリティを用いて以下のように与えた.

定理 3.2. 識別問題 $\mathrm{QCGDP}(\{q_\xi\},\{\mathcal{O}^\xi_{A\to B}\},\{C_\eta\})$ の最小誤り確率を $p_{\mathrm{err}}(n)$ とし, さらに

$$\theta_F\coloneqq\arccos\max_{\Psi_{AR\to BR}}\min_{\rho_{AR}}\sum_{\xi\in\Xi}q_\xi F\left(\Psi_{AR\to BR}(\rho_{AR}),\mathcal{O}^\xi_{A\to B}(\rho_{AR})\right)\tag{3.1}$$

$$\theta_q\coloneqq\arcsin\sqrt{\max_{\eta\in H}\left(\sum_{\xi\in C_\eta}q_\xi\right)}.$$

と定義する. ここで $\Psi_{AR\to BR}$ は量子通信路, ρ_{AR} は密度作用素である. 条件 $n\theta_F+\theta_q\in[0,\pi/2]$ が成り立つとき以下の不等式が成り立つ.

$$p_{\mathrm{err}}(n)\ge\cos^2\left(n\theta_F+\theta_q\right).$$

さらに識別する量子通信路が 2 つのみの場合に対し, 以下のような下界を与えた.

定理 3.3. 識別問題 QCDP($\{q_0, q_1\}, \{\mathcal{O}^0_{A\to B}, \mathcal{O}^1_{A\to B}\}$) の最小誤り確率を $p_{\mathrm{err}}(n)$ とし, さらに

$$\tau \coloneqq \arccos \min_{\rho_{AR}} F\left(\mathcal{O}^0_{A\to B}(\rho_{AR}), \mathcal{O}^1_{A\to B}(\rho_{AR})\right).$$

とする. ここで ρ_{AR} は密度作用素である. 条件 $n\tau \in [0, \pi/2]$ が成り立つとき以下の不等式が成り立つ.

$$p_{\mathrm{err}}(n) \geq \frac{1}{2}\left(1 - \sqrt{1 - 4q_0q_1\cos^2(n\tau)}\right).$$

5 節で定理 3.2, 6 節で定理 3.3 の証明をそれぞれ与える.

4 本研究の応用例

定理 3.2 を用いて $p_{\mathrm{err}}(n)$ の下界を計算する例を紹介する.

例 4.1. (Grover の探索問題) A を $|H|$ 次元の量子系とし, その計算基底を $\{|\eta\rangle_A\}_{\eta\in H}$ とする. また m を $1 \leq m \leq |T|/2$ を満たす整数とする. さらに $\{P_\xi\}_{\xi\in\Xi}$ を $|P_\xi| = m$ を満たす H の部分集合全体の族とする. $\{O^\xi_A\}_{\xi\in\Xi}$ を $O^\xi_A \coloneqq I - 2\sum_{u\in P_\xi} |u\rangle\langle u|$ $(\xi \in \Xi)$ を満たすユニタリ作用素の族とし, さらに $\mathcal{O}^\xi_A$ を

$$\mathcal{O}^\xi_A(\rho_A) \coloneqq O^\xi_A \rho_A O^{\xi\dagger}_A,$$

とする. また $\{C_\eta\}_{\eta\in H}$ を $C_\eta = \{\xi \in \Xi \mid \mathcal{O}^\xi_A(|\eta\rangle\langle\eta|_A) = -|\eta\rangle\langle\eta|_A\}$ を満たす Ξ の部分集合族とする. このとき QCGDP($\{1/|\Xi|\}, \{\mathcal{O}^\xi_A\}, \{C_\eta\}$) は Grover の探索問題と呼ばれる. ここでユニタリ作用素 $\{O^\xi_A\}_{\xi\in\Xi}$ に対して以下の不等式が成り立つ.

$$\begin{aligned}\frac{1}{|\Xi|}\sum_{\xi\in\Xi} O^\xi_A &= \binom{|H|}{m}^{-1}\left(\binom{|H|-1}{m} - \binom{|H|-1}{m-1}\right) I_A \\ &= \left(1 - \frac{2m}{|H|}\right) I_A.\end{aligned}$$

このことから

$$\begin{aligned}\theta_F &= \arccos \max_{\Psi_{AR\to BR}} \min_{\rho_{AR}} \sum_{\xi\in\Xi} \frac{1}{|\Xi|} F\left(\Psi_{AR\to BR}(\rho_{AR}), \mathcal{O}^\xi_A(\rho_{AR})\right) \\ &\leq \arccos \min_{|\phi_{AR}\rangle} \sum_{\xi\in\Xi} \frac{1}{|\Xi|} F\left(|\phi\rangle\langle\phi|_{AR}, \mathcal{O}^\xi_A(|\phi\rangle\langle\phi|_{AR})\right) \\ &= \arccos \min_{|\phi\rangle} \sum_{\xi\in\Xi} \frac{1}{|\Xi|} \left\langle \phi \middle| O^\xi_A \middle| \phi \right\rangle_{AR} \\ &\leq \arccos\left(1 - \frac{2m}{|H|}\right).\end{aligned}$$

となり, さらに

$$\begin{aligned}\theta_q &= \arcsin\sqrt{\max_{\eta\in H}\left(\sum_{\xi\in C_\eta}\frac{1}{|\Xi|}\right)} \\ &= \arcsin\sqrt{1-\frac{m+1}{|H|}} \\ &= \arccos\sqrt{\frac{m+1}{|H|}}\end{aligned}$$

が成り立つから定理 3.2 より以下の下界を得る.

$$p_{\mathrm{err}}(n) \geq \cos^2\left(n\arccos\left(1-\frac{2m}{|H|}\right)+\arccos\sqrt{\frac{m+1}{|H|}}\right).$$

Zalka は $m=1$ の場合のみこの問題の誤り確率の下界を示したが [10], 定理 3.2 によって与えられる下界は Zalka によって与えられた下界と一致している. さらに Grover 探索はこの下界を達成するアルゴリズムである.

定理 3.3 の応用例を考えるための準備としてまず以下の補題を与える.

補題 4.2. $\xi\in\{0,1\}$ に対して $\mathcal{O}^{\xi}_{A\to B}$ を量子通信路とし, さらに等長作用素 $O^{\xi}_{A\to BE}$ が $\mathcal{O}^{\xi}_{A\to B}(\rho_A)=\mathrm{Tr}_E\left(O^{\xi}_{A\to BE}\rho_A O^{\xi\dagger}\right)$ を満たすとする. $\dim A\leq\dim R$ のとき以下の不等式が成り立つ.

$$\min_{\sigma_{AR}} F\left(\mathcal{O}^0_{A\to B}(\sigma_{AR}),\mathcal{O}^1_{A\to B}(\sigma_{AR})\right)=\min_{\rho_A}\left\|\mathrm{Tr}_B\left(O^1_{A\to BE}\rho_A O^{0\dagger}\right)\right\|_1.$$

ここで ρ_A,σ_{RA} は密度作用素である.

証明. $\hat{\sigma}_{AR}$ を左辺の最小値を達成する密度作用素とし, さらに $\hat{\sigma}_{AR}=\sum_i\lambda_i|\phi_i\rangle\langle\phi_i|_{AR}$ とスペクトル分解する. このとき以下の不等式を得る.

$$\begin{aligned}F\left(\mathcal{O}^0_{A\to B}(\hat{\sigma}_{AR}),\mathcal{O}^1_{A\to B}(\hat{\sigma}_{AR})\right) &\geq \sum_i\lambda_i F\left(\mathcal{O}^0_{A\to B}(|\psi_i\rangle\langle\psi_i|),\mathcal{O}^1_{A\to B}(|\psi_i\rangle\langle\psi_i|)\right) \\ &= \sum_i\lambda_i\left\|\mathrm{Tr}_{BR}\left(O^1_{A\to BE}|\psi_i\rangle\langle\psi_i|_{AR}O^{0\dagger}\right)\right\|_1.\end{aligned}$$

ここで不等号はフィデリティの凹性から成り立ち, 等号は以下のフィデリティの恒等式から成り立つ.

$$F\left(\mathrm{Tr}_E\left(|\psi\rangle\langle\psi|_{CE}\right),\mathrm{Tr}_E\left(|\varphi\rangle\langle\varphi|_{CE}\right)\right)=\left\|\mathrm{Tr}_C\left(|\varphi\rangle\langle\psi|_{CE}\right)\right\|_1.$$

ここで複素数 $\{\alpha_{j\ell}\}_{j,\ell}$ と計算基底 $\{|j\rangle\}_j,\{|\ell\rangle\}_\ell$ に対して線形写像 $|\cdot\rangle\!\rangle$ を $|\sum_{j,\ell}\alpha_{j\ell}|j\rangle\langle\ell|\rangle\!\rangle:=\sum_{j,\ell}\alpha_{j\ell}|j\rangle|\ell\rangle$ により定義する. さらに $|\psi_i\rangle_{AR}=|K^i_{R\to A}\rangle\!\rangle$ が成り立つような作用素の族 $\{K^i_{R\to A}\}_i$ をとると

$$\begin{aligned}\sum_i\lambda_i\left\|\mathrm{Tr}_{BR}\left(O^1_{A\to BE}|\psi_i\rangle\langle\psi_i|_{AR}O^{0\dagger}\right)\right\|_1 &= \sum_i\lambda_i\left\|\mathrm{Tr}_{BR}\left(|O^1_{A\to BE}K^i\rangle\!\rangle\langle\!\langle O^0_{A\to BE}K^i|\right)\right\|_1 \\ &= \sum_i\lambda_i\left\|\mathrm{Tr}_B\left(O^1_{A\to BE}K^iK^{i\dagger}O^{0\dagger}\right)\right\|_1 \\ &\geq \min_{\rho_A}\left\|\mathrm{Tr}_B\left(O^1_{A\to BE}\rho_A O^{0\dagger}\right)\right\|_1,\end{aligned}$$

ここで二つの等号は $|\cdot\rangle\!\rangle$ の性質より成り立つ.

次に, $\hat{\rho}_A$ を右辺の最小値を達成する密度作用素とする. このとき条件 $\dim A \leq \dim R$ より $\hat{\rho}_A = K_{R\to A}K^\dagger$ を満たす作用素 $K_{R\to A}$ が存在するから以下の不等式が成り立つ.

$$\begin{aligned}\left\|\mathrm{Tr}_B\left(O^1_{A\to BE}\hat{\rho}_A O^{0\dagger}\right)\right\|_1 &= \left\|\mathrm{Tr}_{BR}\left(O^1_{A\to BE}\,|K_{R\to A}\rangle\!\rangle\langle\!\langle K_{R\to A}|\,O^{0\dagger}\right)\right\|_1 \\ &= F\left(\mathcal{O}^0_{A\to B}(|K\rangle\!\rangle\langle\!\langle K|), \mathcal{O}^1_{A\to B}(|K\rangle\!\rangle\langle\!\langle K|)\right) \\ &\geq \min_{\sigma_{RA}} F\left(\mathcal{O}^0_{A\to B}(\sigma_{AR}), \mathcal{O}^1_{A\to B}(\sigma_{AR})\right).\end{aligned}$$

□

定理 3.3 と補題 4.2 を用いることにより二つの振幅減衰通信路の識別誤り確率の下界を以下のように求めることができる.

例 4.3. A と E を 2 次元の量子系とする. $\xi \in \{0,1\}$ に対して $r_\xi \in [0,1]$ とし, さらに $\mathcal{O}^\xi_A(\sigma_A)$ を振幅減衰通信路

$$\begin{aligned}O^\xi_{A\to AE} &\coloneqq (|0\rangle\langle 0|_A + \sqrt{1-r_\xi}\,|1\rangle\langle 1|_A)\otimes|0\rangle_E + (\sqrt{r_\xi}\,|0\rangle\langle 1|_A)\otimes|1\rangle_E \\ \mathcal{O}^\xi_A(\sigma_A) &\coloneqq \mathrm{Tr}_E\left(O^\xi_{A\to AE}\sigma_A O^{\xi\dagger}\right)\end{aligned}$$

とする. 識別問題 $\mathrm{QCDP}(\{q_0,q_1\},\{\mathcal{O}^0_A,\mathcal{O}^1_A\})$ に対して定理 3.3 の τ の上界を計算すると

$$\begin{aligned}\tau &= \arccos\min_{\sigma_A}\left\|\mathrm{Tr}_A\left(O^1_{A\to AE}\sigma_A O^{0\dagger}_{A\to AE}\right)\right\|_1 \\ &= \arccos\min_{\sigma_A}\left\|\begin{pmatrix}\langle 0\,|\,\sigma_A\,|\,0\rangle_A + \sqrt{1-r_0}\sqrt{1-r_1}\,\langle 1\,|\,\sigma_A\,|\,1\rangle_A & \sqrt{r_0}\,\langle 0\,|\,\sigma_A\,|\,1\rangle_A \\ \sqrt{r_1}\,\langle 1\,|\,\sigma_A\,|\,0\rangle_A & \sqrt{r_0}\sqrt{r_1}\,\langle 1\,|\,\sigma_A\,|\,1\rangle_A\end{pmatrix}\right\|_1 \\ &\leq \arccos\min_{\sigma_A}\left|\langle 0\,|\,\sigma_A\,|\,0\rangle_A + (\sqrt{r_0}\sqrt{r_1}+\sqrt{1-r_0}\sqrt{1-r_1})\,\langle 1\,|\,\sigma_A\,|\,1\rangle_A\right| \\ &= \arccos\left(\sqrt{r_0}\sqrt{r_1}+\sqrt{1-r_0}\sqrt{1-r_1}\right)\end{aligned}$$

となる. ここで不等号はトレースノルムの単調性より成り立つ. また $\sigma_A = |1\rangle\langle 1|_A$ でこの上界を達成する. 以上より条件 $n\arccos\left(\sqrt{r_0}\sqrt{r_1}+\sqrt{1-r_0}\sqrt{1-r_1}\right) \in [0,\pi/2]$ が成り立つとき

$$p_{\mathrm{err}}(n) \geq \frac{1}{2}\left(1-\sqrt{1-4q_0q_1\cos^2\left(n\arccos\left(\sqrt{r_0}\sqrt{r_1}+\sqrt{1-r_0}\sqrt{1-r_1}\right)\right)}\right)$$

が成り立つ.

5 定理 3.2 の証明

この節では定理 3.2 の証明を与える. そのためにいくつかフィデリティの性質を紹介する. まずフィデリティは以下のような単調性・凹性を持つことが知られている.

補題 5.1. (フィデリティの単調性) 任意の量子通信路 $\Phi_{A\to B}$, 密度作用素 ρ_A,σ_A に対して $F\left(\Phi_{A\to B}(\rho_A),\Phi_{A\to B}(\sigma_A)\right) \geq F\left(\rho_A,\sigma_A\right)$ が成り立つ.

補題 5.2. (フィデリティの凹性) 任意の確率分布 $\{q_\xi\}_{\xi\in\Xi}$ と任意の密度作用素の族 $\{\rho_A^\xi\}_{\xi\in\Xi}, \{\sigma_A^\xi\}_{\xi\in\Xi}$ に対して

$$F\left(\sum_{\xi\in\Xi} q_\xi \rho_A^\xi, \sum_{\xi\in\Xi} p_\xi \sigma_A^\xi\right) \geq \sum_{\xi\in\Xi} q_\xi F\left(\rho_A^\xi, \sigma_A^\xi\right)$$

が成り立つ.

フィデリティから誘導された距離関数は密度作用素の識別可能性を考える際にとても有用である. そういった距離関数の 1 つとして以下に定義する Bures 角が知られている [11].

補題 5.3. (Bures 角) ρ と σ を密度作用素とする. このとき関数 $A(\rho,\sigma) \coloneqq \arccos F(\rho,\sigma)$ は ρ と σ の Bures 角と呼ばれ, 密度作用素の集合上で距離の公理を満たす.

ここで Bures 角は線形作用素全体で定義された距離関数ではないことに注意せよ.

以上の補題 5.1, 5.2, 5.3 を用いて定理 3.2 の証明を以下に与える.

定理 *3.2* の証明. 識別問題 QCGDP$(\{q_\xi\}, \{\mathcal{O}^\xi_{A\to B}\}, \{C_\eta\})$ の最小誤り確率 $p_{\mathrm{err}}(n)$ を達成するアルゴリズムを $(\rho_{AR}^{\mathrm{init}}, \{\Phi^k_{BR\to AR}\}, \{M^\eta_{BR}\})$ とする. さらに C を 2 次元の量子系とし $\xi\in\Xi$ に対し量子通信路 $\mathcal{M}^\xi_{BR\to C}$ を

$$\mathcal{M}^\xi_{BR\to C}(\rho_{BR}) \coloneqq \mathrm{Tr}\left(\sum_{\eta:\xi\in C_\eta} M^\eta_{BR}\rho_{BR}\right)|1\rangle\langle 1|_C + \mathrm{Tr}\left(\sum_{\eta:\xi\notin C_\eta} M^\eta_{BR}\rho_{BR}\right)|0\rangle\langle 0|_C$$

と定義する. θ_F の定義式 (3.1) の max を達成する量子通信路を $\Psi_{AR\to BR}$ とし, さらに以下のような密度作用素を定義する.

$$\begin{aligned}
\rho^i_{AR} &\coloneqq \begin{cases} \rho^{\mathrm{init}}_{AR} & (i=0), \\ \left(\Phi^i_{BR\to AR}\circ\Psi_{AR\to BR}\right)(\rho^{i-1}_{AR}) & (1\leq i<n), \end{cases} \\
\rho^{\mathrm{fin}}_{BR} &\coloneqq \Psi_{AR\to BR}(\rho^{n-1}_{AR}), \\
\rho^{i,k,\xi}_{AR} &\coloneqq \begin{cases} \rho^i_{AR} & (0\leq i=k<n), \\ \left(\Phi^k_{BR\to AR}\circ\mathcal{O}^\xi_{A\to B}\right)(\rho^{i,k-1,\xi}_{AR}) & (0\leq i<k<n), \end{cases} \\
\rho^{i,\mathrm{fin},\xi}_{BR} &\coloneqq \begin{cases} \mathcal{O}^\xi_{A\to B}(\rho^{i,n-1,\xi}_{AR}) & (0\leq i<n), \\ \rho^{\mathrm{fin}}_{BR} & (i=n) \end{cases} \\
\rho^{i,\mathrm{fin}}_C &\coloneqq \sum_{\xi\in\Xi} q_\xi \mathcal{M}^\xi_{BR\to C}\left(\rho^{i,\mathrm{fin},\xi}_{BR}\right).
\end{aligned}$$

このとき密度作用素の列 $|1\rangle\langle 1|_C, \rho_C^{0,\mathrm{fin}}, \rho_C^{1,\mathrm{fin}}, \ldots, \rho_C^{n,\mathrm{fin}}, |0\rangle\langle 0|_C$ に Bures 角の三角不等式を用いることにより以下の不等式を得る.

$$\begin{aligned}
\frac{\pi}{2} &= A\left(|1\rangle\langle 1|_C, |0\rangle\langle 0|_C\right) \\
&\leq A\left(|1\rangle\langle 1|_C, \rho_C^{0,\mathrm{fin}}\right) + \sum_{i=0}^{n-1} A\left(\rho_C^{i,\mathrm{fin}}, \rho_C^{i+1,\mathrm{fin}}\right) + A\left(\rho_C^{n,\mathrm{fin}}, |0\rangle\langle 0|_C\right).
\end{aligned}$$

この不等式の各項は以下のように評価される. まず

$$\begin{aligned} A\left(|1\rangle\langle 1|_C, \rho_C^{0,\mathrm{fin}}\right) &= \arccos F\left(|1\rangle\langle 1|_C, \sum_{\xi\in\Xi} q_\xi \mathcal{M}^\xi_{BR\to C}\left(\rho_{BR}^{0,\mathrm{fin},\xi}\right)\right) \\ &= \arccos\sqrt{\sum_{\xi\in\Xi} q_\xi \sum_{\eta:\xi\in C_\eta} \mathrm{Tr}\left(\rho_{BR}^{0,\mathrm{fin},\xi} M_{BR}^\eta\right)} \\ &= \arccos\sqrt{1-p_{\mathrm{err}}(n)}. \end{aligned}$$

が成り立つ. さらに

$$\begin{aligned} A\left(\rho_C^{i,\mathrm{fin}}, \rho_C^{i+1,\mathrm{fin}}\right) &= \arccos F\left(\sum_{\xi\in\Xi} q_\xi \mathcal{M}^\xi_{BR\to C}\left(\rho_{BR}^{i,\mathrm{fin},\xi}\right), \sum_{\xi\in\Xi} q_\xi \mathcal{M}^\xi_{BR\to C}\left(\rho_{BR}^{i+1,\mathrm{fin},\xi}\right)\right) \\ &\le \arccos\left(\sum_{\xi\in\Xi} q_\xi F\left(\mathcal{M}^\xi_{BR\to C}\left(\rho_{BR}^{i,\mathrm{fin},\xi}\right), \mathcal{M}^\xi_{BR\to C}\left(\rho_{BR}^{i+1,\mathrm{fin},\xi}\right)\right)\right) \\ &\le \arccos\left(\sum_{\xi\in\Xi} q_\xi F\left(\mathcal{O}^\xi_{A\to B}\left(\rho^i_{AR}\right), \Psi_{AR\to BR}(\rho^i_{AR})\right)\right) \\ &\le \theta_F \end{aligned}$$

が成り立つ. ここで最初の不等式はフィデリティの凹性から成り立ち, 二つ目の不等式はフィデリティの単調性から成り立つ. 最後に以下の不等式が成り立つ.

$$\begin{aligned} A\left(\rho_C^{n,\mathrm{fin}}, |0\rangle\langle 0|_C\right) &= \arccos\sqrt{\sum_{\xi\in\Xi} q_\xi \left\langle 0\middle|\, \mathcal{M}^\xi_{BR\to C}\left(\rho_{BR}^{n,\mathrm{fin},\xi}\right)\middle|\, 0\right\rangle_C} \\ &= \arcsin\sqrt{\mathrm{Tr}\left(\sum_{\xi\in\Xi} q_\xi \sum_{\eta:\xi\in C_\eta} M_{BR}^\eta \rho_{BR}^{\mathrm{fin}}\right)} \\ &= \arcsin\sqrt{\mathrm{Tr}\left(\sum_{\eta\in H}\left(\sum_{\xi\in C_\eta} q_\xi\right)\mathrm{Tr}\left(M_{BR}^\eta \rho_{BR}^{\mathrm{fin}}\right)\right)} \\ &\le \theta_q. \end{aligned}$$

従って、

$$\frac{\pi}{2} \le \arccos\sqrt{1-p_{\mathrm{err}}(n)} + n\theta_F + \theta_q$$

が得られる。これらのことから $n\theta_F + \theta_q \in [0, \pi/2]$ が成り立つとき

$$\begin{aligned} 1-p_{\mathrm{err}}(n) &\le \cos^2\left(\frac{\pi}{2} - n\theta_F - \theta_q\right) \\ &= \sin^2\left(n\theta_F + \theta_q\right) \end{aligned}$$

が成り立つ. □

6　定理 3.3 の証明

識別すべき量子通信路オラクルが二つしかない場合は以下の補題を用いることで三つ以上の場合とは異なる下界を与えることができる．この節では定理 3.3 の証明を与える．そのためにまずいくつか補題を説明する．

補題 6.1. ([1]) ρ_A^0, ρ_A^1 を密度作用素とし，さらに 非負実数 q_0, q_1 が $q_0 + q_1 = 1$ を満たすとする．このとき任意の POVM $\{M_A^0, M_A^1\}$ に対して，以下の不等式が成り立つ．

$$\sum_{\xi\in\{0,1\}} q_\xi \mathrm{Tr}\left(M_A^\xi \rho_A^\xi\right) \leq \frac{1}{2}\left(1 + \left\|q_0\rho_A^0 - q_1\rho_A^1\right\|_1\right).$$

また，適切に POVM $\{M_A^0, M_A^1\}$ を選択することで等号を達成することができる．

二つの密度作用素 ρ_A, σ_A に対して成り立つ不等式 $\|\rho_A - \sigma_A\|_1 \leq 2\sqrt{1 - F\left(\rho_A, \sigma_A\right)^2}$ は Fuchs–van de Graaf の不等式として知られており，フィデリティとトレース距離の関係として有用である [12]．次に示す補題はこの不等式の一般化である．

補題 6.2. a, b を非負実数とし，さらに ρ_A, σ_A を密度作用素とする．このとき以下の不等式が成り立つ．

$$\|a\rho_A - b\sigma_A\|_1 \leq \sqrt{(a+b)^2 - 4abF\left(\rho_A, \sigma_A\right)^2}.$$

証明. 以下の証明は Fuchs–van de Graaf の不等式の一般化である [1]．Uhlmann の定理により，単位ベクトル $|\phi\rangle_{AR}, |\psi\rangle_{AR}$ であって $\mathrm{Tr}_R\left(|\phi\rangle\langle\phi|_{AR}\right) = \rho_A$, $\mathrm{Tr}_R\left(|\psi\rangle\langle\psi|_{AR}\right) = \sigma_A$, および $|\langle\phi\,|\,\psi\rangle_{AR}| = F(\rho_A, \sigma_A)$ を満たすものが存在する．従って以下の不等式が成り立つ．

$$\begin{aligned}
\|a\rho_A - b\sigma_A\|_1 &= \|a\mathrm{Tr}_R\left(|\phi\rangle\langle\phi|_{AR}\right) - b\mathrm{Tr}_R\left(|\psi\rangle\langle\psi|_{AR}\right)\|_1 \\
&\leq \|a\,|\phi\rangle\langle\phi|_{AR} - b\,|\psi\rangle\langle\psi|_{AR}\|_1 \\
&= \sqrt{(a+b)^2 - 4ab\,|\langle\phi\,|\,\psi\rangle_{AR}|^2} \\
&= \sqrt{(a+b)^2 - 4abF\left(\rho_A, \sigma_A\right)^2},
\end{aligned}$$

ここで不等号はトレースノルムの単調性から成り立ち，二つ目の等号は任意の非負実数 a, b と単位ベクトル $|\phi\rangle, |\psi\rangle$ に対して成り立つ恒等式である． □

以上の補題を用いて定理 3.2 を証明する．

定理 *3.3* の証明．識別問題 $\mathrm{QCDP}(\{q_0, q_1\}, \{\mathcal{O}_{A\to B}^0, \mathcal{O}_{A\to B}^1\})$ の最小誤り確率を達成するアルゴリズムを $(\rho_{AR}^{\mathrm{init}}, \{\Phi_{BR\to AR}^i\}, \{M_{BR}^0, M_{BR}^1\})$ とする．さらに

$$\begin{aligned}
\rho_{AR}^i &\coloneqq \begin{cases} \rho_{AR}^{\mathrm{init}} & (i=0), \\ \left(\Phi_{BR\to AR}^i \circ \mathcal{O}_{A\to B}^0\right)\left(\rho_{AR}^{i-1}\right) & (1 \leq i < n), \end{cases} \\
\rho_{BR}^{\mathrm{fin}} &\coloneqq \mathcal{O}_{A\to B}^0(\rho_{AR}^{n-1}), \\
\rho_{AR}^{i,k} &\coloneqq \begin{cases} \rho_{AR}^i & (i=k), \\ \left(\Phi_{BR\to AR}^k \circ \mathcal{O}_{A\to B}^1\right)\left(\rho_{AR}^{i,k-1}\right) & (i < k < n), \end{cases} \\
\rho_{BR}^{i,\mathrm{fin}} &\coloneqq \begin{cases} \mathcal{O}_{A\to B}^1(\rho_{AR}^{i,n-1}) & (0 \leq i < n), \\ \rho_{BR}^{\mathrm{fin}} & (i=n) \end{cases}
\end{aligned}$$

と定義する. このとき以下の不等式を得る.

$$\begin{aligned} A\left(\rho_{BR}^{n,\mathrm{fin}}, \rho_{BR}^{0,\mathrm{fin}}\right) &\leq \sum_{i=0}^{n-1} A\left(\rho_{BR}^{i+1,\mathrm{fin}}, \rho_{BR}^{i,\mathrm{fin}}\right) \\ &\leq \sum_{i=0}^{n-1} A\left(\mathcal{O}_{A\to B}^0(\rho_{AR}^i), \mathcal{O}_{A\to B}^1(\rho_{AR}^i)\right) \\ &\leq n\tau. \end{aligned}$$

ここで最初の不等号は Bures 角の三角不等式から成り立ち, 二つ目の不等号はフィデリティの単調性により成り立つ. よって, $n\tau \in [0, \pi/2]$ のとき, $F\left(\rho_{BR}^{n,\mathrm{fin}}, \rho_{BR}^{0,\mathrm{fin}}\right) \geq \cos(n\tau)$ が成り立つ. これらのことから以下の不等式を得る.

$$\begin{aligned} 1 - p_{\mathrm{err}}(n) &= q_0 \mathrm{Tr}\left(M_{BR}^0 \rho_{BR}^{n,\mathrm{fin}}\right) + q_1 \mathrm{Tr}\left(M_{BR}^1 \rho_{BR}^{0,\mathrm{fin}}\right) \\ &= \frac{1}{2}\left(1 + \left\| q_0 \rho_{BR}^{n,\mathrm{fin}} - q_1 \rho_{BR}^{0,\mathrm{fin}} \right\|_1\right) \\ &\leq \frac{1}{2}\left(1 + \sqrt{1 - 4q_0 q_1 F\left(\rho_{BR}^{n,\mathrm{fin}}, \rho_{BR}^{0,\mathrm{fin}}\right)^2}\right) \\ &\leq \frac{1}{2}\left(1 + \sqrt{1 - 4q_0 q_1 \cos^2(n\tau)}\right), \end{aligned}$$

ここで二つ目の等号は補題 6.1 から成り立ち, 一つ目の不等号は補題 6.2 から成り立つ. □

Kawachi らはオラクルの分布が一様 (すなわち $q_0 = q_1 = 0.5$) で識別する量子通信路がユニタリ通信路である場合の誤り確率の下界を求めた [4]. 上で与えた定理 3.3 は Kawachi らの結果の一般化になっている. 定理 3.3 の系として, オラクルの分布が一様ではないときのユニタリ通信路識別問題の誤り確率の下界を与えることができる. このための下準備として, まずは covering angle という概念を導入する.

定義 6.3. (Covering angle) 複素数 z に対して $\arg_{\geq 0}(z) \coloneqq \min\{\tau \geq 0 \mid z = |z| \exp(i\tau)\}$ とする. このとき集合 $\Theta \coloneqq \{\exp(i\theta_1), \ldots, \exp(i\theta_n)\}$ に対して下式を満たす θ_{cover} を covering angle という.

$$\theta_{\mathrm{cover}} \coloneqq \min_{k\in\{1,\ldots,n\}} \max_{\ell\in\{1,\ldots,n\}} \{\arg_{\geq 0}(\exp(i(\theta_\ell - \theta_k)))\}.$$

この covering angle の概念を用いて, ユニタリ通信路の識別問題の誤り確率の下界は以下のように表すことができる.

系 6.4. ユニタリ作用素 O_A^ξ ($\xi \in \{0,1\}$) に対して $\mathcal{O}_A^\xi(\rho_A) = O_A^\xi \rho_A O_A^{\xi\dagger}$ が成り立つようなユニタリ通信路 $\{\mathcal{O}_A^0, \mathcal{O}_A^1\}$ をとる. さらに識別問題 $\mathrm{QCDP}(\{q_0, q_1\}, \{\mathcal{O}_A^0, \mathcal{O}_A^1\})$ の最小誤り確率を $p_{\mathrm{err}}(n)$ とし, 作用素 $O_A^{0\dagger} O_A^1$ の固有値集合の covering angle を θ_{cover} とする. 条件 $n\theta_{\mathrm{cover}}/2 \in [0, \pi/2]$ が成り立つとき, 以下の不等式が成り立つ.

$$p_{\mathrm{err}}(n) \geq \frac{1}{2}\left(1 - \sqrt{1 - 4q_0 q_1 \cos^2 \frac{n\theta_{\mathrm{cover}}}{2}}\right).$$

系 6.4 は $\tau = \theta_{\mathrm{cover}}/2$ が成り立つことから得られる (詳細は [4] 参照).

7　まとめ

本研究では Bures 角の三角不等式を用いて, 量子通信路識別アルゴリズムの誤り確率の下界を与えた. 今回与えた下界は Zalka による Grover の探索問題の誤り確率の下界を含んでいる.

今回与えた下界の式の θ_F, τ を解析的に求めることができるための条件, および少ないコストで数値的に計算するための手法, 条件については明らかではないので, 今後の課題としたい.

謝辞

本研究は JST さきがけ JPMJPR1867, JSPS 科研費 JP17K17711, JP18H04090, JP20H04138, JP20H05966 の助成を受け, さらに国際共同利用・共同研究拠点である京都大学数理解析研究所から支援を受けたものである。

参考文献

[1] John Watrous. The Theory of Quantum Information. Cambridge University Press, 2018.

[2] Michael A. Nielsen and Isaac L. Chuang. Quantum Computation and Quantum Information: 10th Anniversary Edition. Cambridge University Press, 2010.

[3] John Watrous. Semidefinite programs for completely bounded norms. arXiv preprint arXiv:0901.4709, 2009.

[4] Akinori Kawachi, Kenichi Kawano, François Le Gall, and Suguru Tamaki. Quantum query complexity of unitary operator discrimination. IEICE TRANSACTIONS on Information and Systems, Vol. 102, No. 3, p. 483, 2019.

[5] Aram Harrow, Avinatan Hassidim, Debbie Leung, and John Watrous. Adaptive versus nonadaptive strategies for quantum channel discrimination. Physical Review A, Vol. 81, No. 3, p. 032339, 2010.

[6] Runyao Duan, Yuan Feng, and Mingsheng Ying. Perfect distinguishability of quantum operations. Physical Review Letters, Vol. 103, No. 21, p. 210501, 2009.

[7] Stefano Pirandola, Riccardo Laurenza, Cosmo Lupo, and Jason L. Pereira. Fundamental limits to quantum channel discrimination. npj Quantum Information, Vol. 5, No. 1, p. 1, 2019.

[8] Lov K. Grover. A fast quantum mechanical algorithm for database search. In Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, p. 212, 1996.

[9] Charles H. Bennett, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani. Strengths and weaknesses of quantum computing. SIAM journal on Computing, Vol. 26, No. 5, p. 1510, 1997.

[10] Christof Zalka. Grover's quantum searching algorithm is optimal. Physical Review A, Vol. 60, No. 4, p. 2746, 1999.

[11] Zhihao Ma, Fu-Lin Zhang, and Jing-Ling Chen. Fidelity induced distance measures for quantum states. Physics Letters A, Vol. 373, No. 38, p. 3407, 2009.

[12] Christopher A. Fuchs and Jeroen Van De Graaf. Cryptographic distinguishability measures for quantum-mechanical states. IEEE Transactions on Information Theory, Vol. 45, No. 4, p. 1216, 1999.