超ロバスト量子計算

今井浩

情報理工学系研究科コンピュータ科学専攻

概 要

本サブプロジェクトでは，量子状態のデコヒーレンスと操作エラーに基づく計算困難性を克服する研究と，デコヒーレンスによりもたらされる状態を活用する研究との両面から，超ロバスト量子計算について研究する．さらに，量子暗号・量子通信においても，ロバスト性の確立を目指している．本報告では，今年度理論解析を完結した量子数え上げアルゴリズムにおけるデコヒーレンス解析結果と，量子通信路容量計算法に関する成果について述べる．

1　はじめに

量子コンピュータは，量子力学原理に基づいて動作するコンピュータで，内部での情報表現として量子状態を用い，ある量子状態を他の量子状態に変換する量子的操作を計算手段とし，そして量子測定を情報獲得法としたものである．理論的には素因数分解を既存コンピュータより超高速に行えることが示され，現代の RSA 暗号や離散対数暗号など公開鍵暗号系のセキュリティに脅威を与えている一方，実現はまだ先だと思われている．その一因は，量子状態が脆く，外界と作用して生じるデコヒーレンスエラーや，計算や通信での操作エラーが存在する中で，ロバストで正しい計算ができる方式・解析が行われていないことにある．

本報告では，昨年度成果を発展させた量子数え上げにおけるデコヒーレンスの精緻な理論解析と，量子通信路容量を計算する方法についての成果を述べる．昨年度より取り組みを始めた Bell 不等式については次年度報告を予定する．

2　量子数え上げアルゴリズムのロバスト性: 理論的解析

量子数え上げ [1] は, データベース中の解の個数を求めるもので，Grover の量子探索アルゴリズムと量子フーリエ変換を組合せたアルゴリズムである．そのために，まず Grover の探索アルゴリズムを，全体の集合 $\mathcal{I}$ の中に条件を満たす解が t 個ある場合で解説しておく．集合 $\mathcal{I} := \{x_0, x_1, \ldots, x_{t-1}\}$ に対し関数 f を

$$f(x) = \begin{cases} 1 & (x \in \mathcal{I}) \\ 0 & (x \notin \mathcal{I}) \end{cases}$$

と定めて Grover の 1 反復の Grover 演算 G (これの詳細は略) を $\lceil \frac{\pi}{4}\sqrt{\frac{N}{t}} \rceil$ 回呼べば, 十分高い確率で $\frac{1}{\sqrt{t}} \sum_{i=0}^{t-1} |x_i\rangle$ を得ることが示せる．このアルゴリズムは 2 次元面内での回転とみなせる．Hilbert 空間を $\mathcal{H}_g := \operatorname*{span}_{x \in \mathcal{I}} \{|x\rangle\}$, $\mathcal{H}_b := \operatorname*{span}_{x \notin \mathcal{I}} \{|x\rangle\}$ の 2 つに分けて,

$$\begin{aligned} |g\rangle &:= \frac{1}{\sqrt{t}} \sum_{x \in \mathcal{I}} |x\rangle \in \mathcal{H}_g \\ |b\rangle &:= \frac{1}{\sqrt{N-t}} \sum_{x \notin \mathcal{I}} |x\rangle \in \mathcal{H}_b \end{aligned}$$

と状態を定義すれば, この正規直交基底 $\{|g\rangle, |b\rangle\}$ のもとで

$$\begin{aligned} G &\equiv \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \\ |s\rangle &= \sqrt{\frac{t}{N}}|g\rangle + \sqrt{\frac{N-t}{N}}|b\rangle \end{aligned}$$

となる. 回転角は $\sin(\theta/2) = \sqrt{t/N}$ で与えられていて, G を $\frac{\pi}{4}\sqrt{\frac{N}{t}}$ 回ほど作用させると, ほぼ $\pi/2$ 回転する仕組みである. この Grover 演算子 G を用いた数え上げ回路を図 1 に示す.

この回路は, 上側 p qubit を第一レジスタ, 下側 n qubit を第二レジスタと呼ぶことにすると, 次のように動く.

1. 初期状態を $|\psi_1\rangle := |0\rangle^{\otimes(p+n)}$ とする.

2. Hadamard 変換 $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ をそれぞれの qubit に作用させる. その結果, $|\psi_2\rangle := \frac{1}{\sqrt{P}}\sum_{m=0}^{P-1}|m\rangle\otimes|s\rangle$ となる. ここで, $P := 2^p$, $|s\rangle$ は前述の Grover 演算子が作用する, 第二レジスタの初期状態である.

3. 第一レジスタの内容 $|m\rangle$ に応じて第二レジスタに制御-G を作用させる.

$$|\psi_3\rangle := \frac{1}{\sqrt{P}}\sum_{m=0}^{P-1}|m\rangle\otimes G^m|s\rangle$$

回路では, m を 2 進表示 ($m \equiv \sum_{j=0}^{p-1} m_j 2^j$) したとき, $G^m = G^{m_{p-1}2^{p-1}}\cdots G^{m_1 2^1}G^{m_0 2^0}$ と構成している. 各 j に対し, m_j が 0 なら何もせず, 1 なら G^{2^j} を作用させるので, $G^{m_j 2^j}$ は制御-G^{2^j} を表している.

4. 第一レジスタをフーリエ変換する.

$$|m\rangle \mapsto \frac{1}{\sqrt{P}}\sum_{m'=0}^{P-1}\exp\left(2\pi i\frac{mm'}{P}\right)|m'\rangle$$

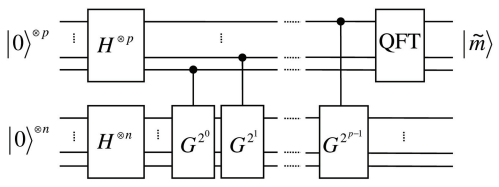


図 1: 量子数え上げ回路

この結果,

$$\begin{aligned}|\psi_3\rangle \;&\mapsto\; |\psi_4\rangle \\ &= \frac{1}{\sqrt{2}}\sum_{m'=0}^{P-1} e^{i\pi m'\frac{P-1}{P}}|m'\rangle \\ &\quad\otimes\left[e^{i\pi f}\frac{\sin\pi(m'+f)}{P\sin(\pi(m'+f)/P)}|\alpha\rangle\right. \\ &\quad\left.+\, e^{-i\pi f}\frac{\sin\pi(m'-f)}{P\sin(\pi(m'-f)/P)}|\beta\rangle\right]\end{aligned}$$

と変換される. ここで $f := P\theta/2\pi$, $|\alpha\rangle := \frac{-i|g\rangle+|b\rangle}{\sqrt{2}}$, $|\beta\rangle := \frac{i|g\rangle+|b\rangle}{\sqrt{2}}$ である.

5. 第一レジスタを測定して $|\tilde{m}\rangle$ を得る. $|\psi_4\rangle$ の確率振幅は $\tilde{m} \simeq f, P-f$ にピークを持つ ($P \gg 1$). このとき, $\tilde{t} := N\sin^2(\pi\tilde{m}/P)$ が, このアルゴリズムにより求められた正解 t の近似値である. P を $O(\sqrt{N})$ に選べば, 十分高い確率で t に近い値を得られることが保証されている [1].

2.1 エラーモデル

現実には計算過程においてエラーの混入は不可避であるので, 何らかのデコヒーレンスのモデルを作り, その影響を考察することには意味がある. 様々なモデルの中から, ここで我々は depolarizing 通信路を用いることにする. $\mathbb{C}^2$ 上の密度行列に対し,

$$\begin{aligned}\rho \;&\mapsto\; (1-3d)\rho \\ &\quad + d(\sigma_x\rho\sigma_x + \sigma_y\rho\sigma_y + \sigma_z\rho\sigma_z) \quad (1) \\ &= (1-4d)\rho + 4d(\mathbf{1}_2/2) \quad (2)\end{aligned}$$

で通信路を定義する ($\mathbf{1}_2$ は 2×2 単位行列). これは ρ と最大混合状態 $\mathbf{1}_2/2$ の凸結合であり, Bloch 球による表示では原点へ向かう運動である. どのような性質のエラーが系に入るのか, 我々は知らないとしよう. そのような場合に, すべての方向に等方的なこの通信路は妥当だと考えられる. 単位時間当たりのエラーの大きさを d とし, シミュレーション及び計算の都合上, 時間変数は離散化してある. ところで, 式 (1) は密度行列の足し算の形を

しているので, 古典的な事象の足し合わせである. $(1-3d)$ の確率で ρ, d の確率で $\sigma_i\rho\sigma_i$ $(i=x,y,z)$ が混合されているので, 数値計算では通信路を, 純粋状態に対し確率 $1-3d$ で恒等写像, 確率 d で $\sigma_x, \sigma_y, \sigma_z$ を作用させ, 複数回の実験の平均を取ることでシミュレートしている.

図 2 に回路例を示す. この図の場合を幅 4, 深さ 3 と呼び, 図中の局所ユニタリ演算を隣の制御 NOT と同時に行えるとすると深さ 2 になる. このように「深さ」は量子回路の最適化によって変わるため, 回路の実装に依存する. また, エラーは各 qubit, 各深さごとに作用させるとする (図 2 の灰色で示した円部分).

2.2 量子数え上げに対するエラーの影響

図 1 に示した回路にエラーを入れる. ここではエラーの大きさを $d \ll 1$ とする.

まず, アルゴリズムの Step2 での Hadamard 変換は qubit ごとに並列に行なうと深さ 1 であり, また Step4 での QFT 回路は, たかだか深さ $O(p^2)$ である. これに対して Step3 の制御-G^m は深さ 2^p-1 なので, ここではこの制御-G の後だけにエラーが入ると近似することにする. エラーのない $d=0$ の場合はすでに示したとおりなので, 測定の結果得られる $\tilde{m}$ における d の 1 次の項を求めてみよう. 式 (1) から明らかに, 制御-G^m 回路の中に $\sigma_x, \sigma_y, \sigma_z$ いずれかがエラーとして 1 回だけ入る場合を考えればよい.

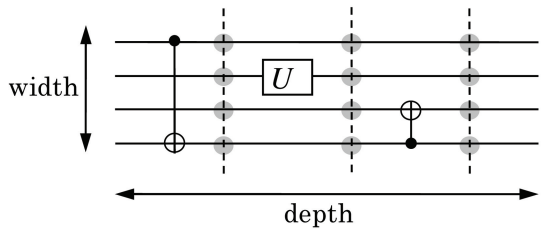


図 2: 回路の幅と深さ: qubit 数を幅, 演算のステップ数を深さと呼ぶ. 灰色の箇所に depolarizing 通信路を挿入する. 計算が終わるまでの全エラー量は回路の幅 × 深さに比例する.

2.2.1 第一レジスタに入るエラー

エラーが 1 回しか入らないと仮定したので, 第一レジスタにエラーが入る時, 第二レジスタではエラーが起こらない. 図 3 に, 第一レジスタの j 番目の qubit の k 番目の制御-G の後に σ_i が入った場合を図示した ($i=x,y,z$, $0 \le j \le p-1$, $0 \le k \le 2^j$). この変更のもとで測定結果 m' を得る確率を $Prob^{(i,j,k)}(m')$ とする. 少々計算すると

$$\sum_{i=0,x,y,z} Prob^{(i,j,k)}(m') \quad = \left[\frac{\sin\{\pi(m'+f)\}}{2^{p-j-1}\sin\{\pi(m'+f)/2^{p-j-1}\}} \times \frac{2^{p-j}\sin\left\{\pi(m'+f)/2^{p-j}\right\}}{2^p\sin\{\pi(m'+f)/2^p\}}\right]^2 + \left[\frac{\sin\pi(m'-f)}{2^{p-j-1}\sin\{\pi(m'-f)/2^{p-j-1}\}} \times \frac{2^{p-j}\sin\left\{\pi(m'-f)/2^{p-j}\right\}}{2^p\sin\{\pi(m'-f)/2^p\}}\right]^2$$

を得る. ここで式を簡単にするために, $i=0$ として $\sigma_0 := \mathbf{1}_2$ も上式に含めてある (式 (2) の第 2 項に対応する). まずこれよりわかることは,

1. エラーの入る場所 k に依存しない. ただし, これは depolarizing 通信路と制御-G が交換することは意味しない.
2. エラーのないときの正しい解は $m' \simeq f, 2^p-f$ であるが, この正しい解に対し, $\pm 2^{p-j-1}$ だけずれたピークが主にあらわれる. 大まかに

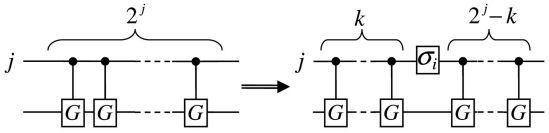


図 3: (左) 第一レジスタ j 番目の qubit を制御 qubit とする制御-G^{2^j}. (右) j 番目の qubit において k 番目の制御-G の後に $\sigma_i (i=x,y,z)$ が入った場合. 第一レジスタのその他 qubit は省略, 第二レジスタは簡略化して 1 本線で示した.

上式第一項は, $m'+f$ に対して周期 2^{p-j-1} の関数と, $|m'+f| \leq 2^{p-j}$ に大きな強度を持つエンベロープとの掛け算とみなせるからである.

図 4 に $\frac{1}{4p}\sum_{i=0,x,y,z}\sum_{j=0}^{p-1} Prob^{(i,j,k)}(m')$ のグラフを示した. $m' \simeq 38, 2^8-38=218$ が正解のピークであり, そこから 2 のベキだけずれたピークが見て取れる: 40, 42, 46, 54, 70, 90$(=218-128)$, 102 などが強度を持っている.

この 1 次のエラーの現れやすい場所は, $2^p(=O(\sqrt{N}))$ 箇所の中で高々$2p(=O(\log N))$ 箇所である. ランダムに現れるのではないという事は, デコヒーレンスの下でも繰り返し実験を行なうことにより, 推定精度を高めることができることを示している.

2.2.2 第二レジスタに入るエラー

次に第二レジスタに 1 回エラーが入る場合を考えよう. Grover 演算子は 2 次元の回転とみなせるが, デコヒーレンスによって状態が乱されるときはこの限りではない. 任意の状態 $|\phi\rangle \in \mathcal{H}$ を初期状態として, Grover のアルゴリズムを走らせる. オラクルによって, 集合 $\mathcal{I}$, 空間 $\mathcal{H}_g$, $\mathcal{H}_b$ は決められている. この時, Gram-Schmidt の直交化により次の一意な分解を得る.

$$|\phi\rangle \equiv u|g\rangle + v|b\rangle + u'|e_g\rangle + v'|e_b\rangle \qquad (3)$$

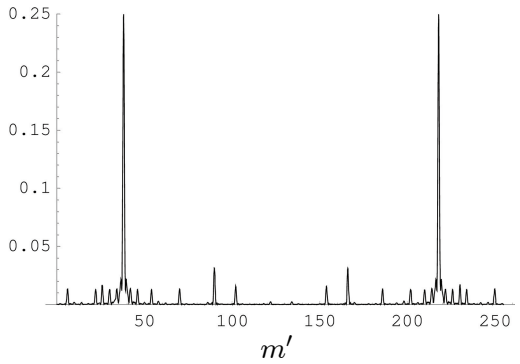


図 4: $\frac{1}{4p}\sum_{i=0,x,y,z}\sum_{j=0}^{p-1} Prob^{(i,j,k)}(m')$ のグラフ. $p=8$, $n=6$, $t=13$ で, $f \simeq 38.1$ である.

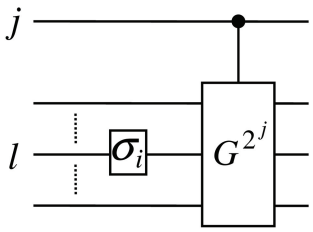


図 5: 第二レジスタにエラーが入った後に制御-G^{2^j} が作用する場合 $(0 \leq j \leq p-1)$.

ここで $u, u', v, v' \in \mathbb{C}$, $|e_g\rangle \in \mathcal{H}_g$, $|e_b\rangle \in \mathcal{H}_b$ は $|\phi\rangle$ に依り, $\langle g|e_g\rangle = \langle b|e_b\rangle = 0$ と選ぶ. すると基底を $\{|g\rangle, |b\rangle, |e_g\rangle, |e_b\rangle\}$ として G の作用は

$$G \equiv \begin{pmatrix} \cos\theta & \sin\theta & 0 & 0 \\ -\sin\theta & \cos\theta & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

と表せる. 数え上げするには回転角を知ればよく, その回転角は $\theta, 0, \pi$ である. この角度に対応する数え上げアルゴリズムの出力 $\tilde{t}$ はそれぞれ $t, 0, N/2$ となり, 正しい解 t 以外に 0 や $N/2$ の間違った出力が予想される.

第二レジスタにはこれまでと同様, エラーが 1 回しか入らないと仮定しよう. すると, エラーが

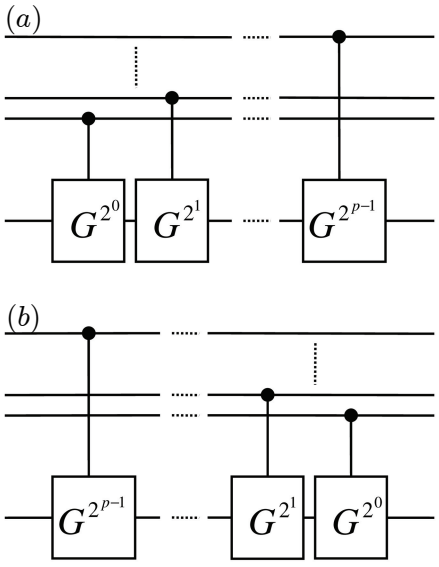
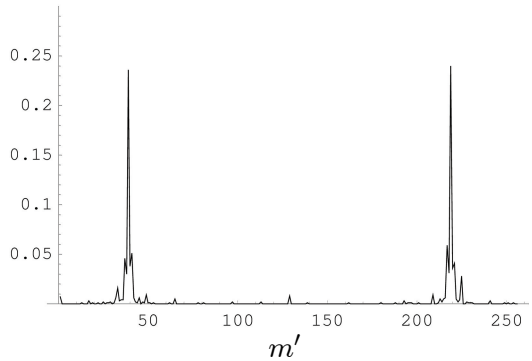
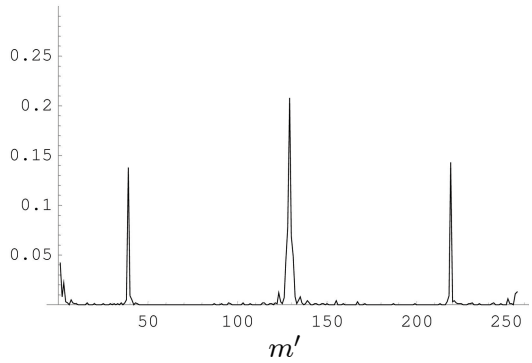


図 6: 制御-G^m の 2 種類の (デコヒーレンスなしなら等価な) 実装. (a) 昇順. (b) 降順.



(a)



(b)

図 7: 測定結果 (シミュレーション, 10^3 回, $d = 10^{-3}$): (a) 昇順の回路, (b) 降順の回路

起こる前の第二レジスタは $\{|g\rangle, |b\rangle\}$ で張られた空間にいるが, エラー後には上で見たように 4 つの基底上での状態として表せる. もちろんこのとき $|e_g\rangle, |e_b\rangle$ は, エラーの種類 $(\sigma_x, \sigma_y, \sigma_z)$, エラーの入る qubit の場所 l, 目的のファイル集合 $\mathcal{I}$ に依存している.

図 5 に, 第二レジスタにエラーが入った後に制御-G^{2^j} が作用する場合の回路を示した. エラー後の状態は式 (3) のように表せて, G が作用したとき, それぞれの成分に応じて $\theta, 0, \pi$ 回転を起こす. ところが, 例えば π 回転を 2^j 回行なうと $j \geq 1$ のとき, 何もしないのと同じである. つまり, ここで回転角に対する推定に誤差が入ってくるわけである. もう少し正確に言うと, 今 $[0, 2\pi)$ の回転角を $P(= 2^p)$ 等分し m として表しているが, 各制御-G^{2^j} が下位 $(p-j)$ ビットを取り出している ($\equiv \bmod 2^{p-j}$).

図 6 に, 典型的な 2 つの制御-G^m の実装例を挙げる. デコヒーレンスがなければ, 明らかに等価な回路であるが, エラーが入るとどのようになるだろうか? シミュレーションの結果を図 7 に示す (前実験と同じパラメータとした). 図 7(a) では, 正しい解のみが大きなピークを持ち, そのまわりに幅を持って分布している. これに対し, 図 7(b) では, $m' \simeq 0, P/2(= 128)$ にも大きな強度で分布していることがわかる.

これらの出力の大きな違いは, 上述の理論解析より定性的に説明できる. 制御-G^{2^j} は回転角の情報の下位 $(p-j)$ ビットを取り出しており, 昇順の回路 (a) は回転角の情報を上位ビットから, 降順の回路 (b) は下位ビットから, 制御 qubit へ取り出している. デコヒーレンスは, 回路の実行中に時間とともに増大していく. より重要な情報は, アルゴリズムの中でなるべく早めに取り出すのが良い. 各制御-G^{2^j} の実行には 2^j 回のオペレーションが必要である. 回路 (b) では, 最下位の bit 情報のために実行時間の 1/2 を, 回路の最初で費やしている. こうして回路 (a) のほうが回路 (b) より優れていることが示せる.

このことは, 量子回路設計において, エラーなしでは等価な回路であっても, エラーありでは全く違う振る舞いを示すものがあることを示しており, 古典回路設計理論ではなかった新たな回路設計問題に取り組むことが必要であることを示している.

3 量子通信路容量計算

量子通信路容量の計算問題についても, 昨年度展開した内点法展開をさらにおしすすめ, 本年度では外近似による上界計算法を与えた. 量子通信路計算の色々なアルゴリズムのサーベイとともに, この方法について述べる.

3.1 既存の量子通信路容量計算法

量子通信路容量は, 量子情報理論における基本的問題であり, 量子状態を伝送する際の送信側・

受信側の条件等によって様々な場合が解析されている．Holevo 容量はその中でも代表的な環境下での量子通信路の容量であり，量子相互情報量を送信量子状態とその上の確率に関して最大化した量である．古典通信路容量は，古典相互情報量を送信符号上の確率に関して最大化したもので，相互情報量がその確率に関して凹関数になっているため，降下法によって数値的に求めることができる．Holevo 容量は，確率について凹性が成り立つものの，量子状態の変数については逆に凸性が成り立ち，そのために局所最適解が必ずしも大域的最適解にならず，その計算は難しいものとなる．

古典通信路容量の場合の有名な Arimoto-Blahut アルゴリズムを Holevo 容量の場合に拡張したアルゴリズムが Nagaoka [3] により提案され，Osawa, Nagaoka [4] により実装されて，Holevo 容量の加法性に関する予備的実験がなされている．しかし，上述したことにより，降下法であるこの方法では，大域的最適解が得られるとは限らない．

Shor [6] は，離散個の量子状態を用いて Holevo 容量計算の部分問題を線形計画問題で表し，無限にある量子状態から適当なものを部分最適化問題を解くことによって生成し，それを加える列生成法を用いたアルゴリズムを提案しているが，列生成での最適化や収束性に関する性質は具体的には与えられていない．

昨年度の研究成果で Hayashi, Imai ら [2] は，1 量子ビット通信路の場合，純粋状態に対応する Bloch 球面をメッシュ点で近似することにより，確率変数に関する凹関数最大化を非線形計画法で解くことにより，メッシュの粗さに応じた近似解が得られることを実験的に報告している (なお，本年度より林は特任助教授として本 COE に参加している)．さらに，本年度の成果として Oto, Imai ら [5] はその近似精度が Taylor 展開により最適解に十分近い近傍では説明できることを示した．そこでは，古典の場合と同様に，Holevo 容量計算がが量子ダイバージェンスに関する最小包含球計算に帰着できること，および計算幾何アルゴリズムが適用できることについて触れている．これらの研究で，近似精度を保証するためには，Bloch 球面全体を均一に近似することが必要であり，具体的に与えられた通信路に対して通信路容量を達成するには明らかに不要な状態を考慮しないですむ仕組みは与えられていない．この点は，Shor の論文 [6] で，Holevo 容量よりも古典通信路に近い容量のアクセス情報量を計算する場合でも問題点として指摘されており，またそれが Shor が Holevo 容量計算で列生成法を提案する理由でもあった．

3.2 外近似計算法

本年度の研究では，Hayashi ら [2] の方法が球をその球面上の均一な有限点集合の凸包で近似する内近似法であるのに対して，その球を含む凸多面体で近似する外近似法を示し，外近似法において平面切除法を用いると適応的に所望の近似精度で計算を行うのに必要な有限離散個の点を生成しながら近似解を求めることができることを示した．外近似のためには，球面上の点集合に対して，各点での接平面により構成される球を含む半空間の交わりとしての凸多面体を利用する．内近似に比べ，外近似は実行可能でない点，また近似精度が対応する有限点集合の内近似解よりも悪いという欠点があるが，一方で最適解の上界を与える始めての方法になっている．

本報告では，1 量子ビットの通信路の場合について記述する．多量子ビットの場合も，次元を考慮すれば拡張ができる部分がある．

1 量子ビット状態は，3 次元 (x, y, z) 空間の原点を中心とし半径 1 の Bloch 球 B の点と同一視できるので，以降 1 量子ビット全体を B で表す．量子通信路は，ある条件を満たすアフィン変換 $\Gamma\colon B \to B$ で与えられ，その条件によって値域 $\Gamma(B)$ は Bloch 球の内部の楕円体に変換される．このとき，古典のダイバージェンス球に対応して，Holevo 容量は次の式でも与えることができる．

$$\chi(\Gamma) = \min_{\sigma\in B} \max_{\rho\in B} D(\Gamma(\rho)||\Gamma(\sigma))$$

ここで，$D(\cdot||\cdot)$ は量子ダイバージェンスである．

Hayashi ら [2] は，Bloch 球面を均一な n 点の集合 S で，球面上のどの点からも Euclid 距離で

$\sqrt{\epsilon}$ ($\epsilon = O(1/n)$) 以内に S の点があるような配置に対して，Holevo 容量の計算の ρ の定義域を S に限った近似量 $\underline{\chi}(\Gamma, S)$ を計算することを提案している．これは球を S の凸包で近似する内近似 (inner approximation) になっている．Oto らは，十分に n が大きい場合には，適当な仮定の下，

$$\underline{\chi}(\Gamma, S) \leq \chi(\Gamma) \leq \underline{\chi}(\Gamma, S) + O(\epsilon)$$

であることを示しており，近似誤差については Hayashi らの実験である程度の大きさの n からこのオーダで精度が増していくことが観察されている．しかし，この理論的解析で用いる Taylor 展開では，詳細な点を配置する必要がない部分を判定するにはさらに精緻な近似解析をして，その条件を実際に計算で判定することが必要であると思われる．また，このような内近似による解は，最適解の下界を与えるのみで，上界の評価にはさらなる計算を要する．

次に，Holevo 容量の外近似計算について述べる．点集合 S による内近似に対応して，外近似 (outer approximation) を次のように考えることができる．S の各点の Bloch 球での接平面を考え，球を含む側の半空間の交わりで構成される凸多面体の端点集合を $\bar{S}$ とすると，

$$(S \text{の凸包}) \subseteq B \subseteq (\bar{S} \text{の凸包})$$

という関係が成り立ち，B を外近似することができる．量子通信路 Γ による値域の楕円体が B の真に内部になっており，点数 n が十分ある場合には，$\bar{S}$ の Γ で写像された先は B に入っている．このとき，量子ダイバージェンスに関する最小包含球を求めることは，内近似の場合と同様にでき，その外近似による値は真の容量値の上界となる．外近似は絶対誤差では内近似より悪い値を与えるが，次のように切除平面アルゴリズムを構成できる．

Bloch 球面上の点集合 S に関して，外近似の方が内近似より精度が悪い計算結果を見たが，数理計画での常套手段として，外近似を用いた場合には適応的な切除平面を求めることが可能となる．半径を量子ダイバージェンスとした時の $\bar{S}$ に対する最小包含球で，その最小包含球上に載っている点を p とする．このとき，p と最小包含球内部の点 (典型的には中心) を結ぶ線分と最小包含球面との交点で接平面をとると，それにより定まる最小包含球を含む半空間は，$\bar{S}$ が外近似であることから $\Gamma(B)$ を含み，一方で p を含まないので，p を切除して実行可能領域を保存する切除平面となっている．

すると，切除平面アルゴリズムとして，$\bar{S}$ が B 内に入るような小規模な外近似から始めて，アルゴリズムの各ステップで最小包含球上に載っている全点についての切除平面を加えるといった切除平面法が考えられる．

本年度の成果でさらに，この外近似による切除平面法は，本当に近似精度を上げるのに必要なところを適応的に点を詳細にとっていくことを，単位的通信路を例として理論的に示した．

参考文献

[1] G. Brassard, P. Høyer and A. Tapp: Quantum Counting. *Proc. 25th International Colloquium on Automata, Languages and Programming (ICALP'98)*, Lecture Notes in Computer Science, Vol.1443, 1998, pp.820–831. arXiv:quant-ph/9805082.

[2] M. Hayashi, H. Imai, K. Matsumoto, M. B. Ruskai and T. Shimono: Qubit Channels Which Require Four Inputs to Achieve Capacity. *Quantum Information and Computation*, to appear. arXiv:quant-ph/0403716

[3] H. Nagaoka: Algorithms of Arimoto-Blahut Type for Computing Quantum Channel Capacity. *Proc. 1998 IEEE International Symposium on Information Theory*, 1998, p.354.

[4] S. Osawa and H. Nagaoka: Numerical Experiments on the Capacity of Quantum Channel with Entangled Input States. *IEICE Trans. Fundamentals*, Vol.E84-A, No.10 (October 2001), pp.2583–2590.

[5] M. Oto, H. Imai, K. Imai and T. Shimono: Computational Geometry of Bloch Sphere. *Proc. ERATO Conference on Quantum Information Science (EQIS 2004)*, 2004, pp.156–157.

[6] P. W. Shor: Capacities of Quantum Channels and How to Find Them. *Mathematical Programming*, Vol.97 (2003), pp.311–335.