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

本年度の研究においては，量子情報処理が古典情報処理を凌駕するための資源として重要なエンタングルメントに着目し，エンタングルメントの性質を明らかにするためにBell不等式を現代的に見直すという観点から研究推進を行った．Bell不等式を満たすか破るかという二者択一の決定を数値計算等を通して行う難しさもこの中で起こっており，元来本研究が目指してきた量子状態の脆さから生じるロバスト処理の必須さの他にも種々の意味での超ロバスト的アプローチが必要となっている．

1 はじめに

量子情報処理においては，量子状態を用いて情報を表現・操作・伝送することによって情報処理を実現する．ここで重要なことは，これまでの情報処理が古典力学系に依存して展開されていたのに対して，量子状態を用いた場合の情報処理ではどのような新しいことができるかを解明することである．

本年度の研究では，古典力学系の状態では表現できない量子的相関について精緻に解析を行い，それを情報処理方式へと発展させることに重点を置いた．具体的には，量子力学において真の量子性を示すためのBell不等式の理論を現代の組合せ的凸多面体論と対話証明の枠組みを適用することによって研究を進めた．そこで，本報告では2節でBell不等式を現代的な観点からコンパクトに眺めた上で，3節で個別の成果について述べることとする．

2 現代Bell不等式論準備

Bell不等式について論じる上で必要な最小限の量子情報を準備するにあたり，まずは次の問題を考える．

$$P_N = \{\boldsymbol{x} \mid \boldsymbol{x} \in \mathbf{C}^N, |\boldsymbol{x}| = 1\}$$

$\boldsymbol{x}' \in P_{N^2}$ に対し $\boldsymbol{x}' = \boldsymbol{x}_1 \otimes \boldsymbol{x}_2$ 存在? $(\boldsymbol{x}_1, \boldsymbol{x}_2 \in P_N)$

ここで，$\mathbf{C}^N$ とは N 次元複素数ベクトル空間であり，$|\cdot|$はノルムを表す．P_Nのようなノルム1の複素ベクトルは純粋な量子状態を表す数理モデルであり，N準位系純粋量子状態という．量子力学では複数の量子状態の合成系は数理的にテンソル積で表される．すると，上の問題は N^2 準位系の純粋量子状態 $\boldsymbol{x}'$が，2つのN準位系の純粋量子状態 $\boldsymbol{x}_1$, $\boldsymbol{x}_2$ のテンソル積で合成として表されるかということを焦点にしている．そのように表現できる場合の N^2 準位系純粋量子状態を分離可能といい，どのような部分系を考えてもそのようには表せないときエンタングルしているという．古典系の状態を量子状態で表現した場合，分離可能となっており，したがってエンタングルしている量子状態に量子情報処理の本質の大部分があると思われている．

一方，量子状態は測定を行うと確率的に測定結果に従って次の状態が定まること，また外界 (環境系) との作用を考慮する必要等があることから，量子状態を表現する一般の数理モデルとして密度行列が用いられる．それを用いることにより，純粋状態でない量子状態 (混合状態と呼ぶ) を表すことができる．この場合，エンタングルしているかどうかという問題は次のように記述される．

$$S_N = \{\rho \mid \rho \in \mathbf{C}^{N\times N}, \rho = \rho^* \geq 0, \mathrm{Tr}\,\rho = 1\}$$

$\rho \in S_{N^2}$ に対し $\rho = \sum_i p_i(\boldsymbol{x}_i \boldsymbol{x}_i^*) \otimes (\boldsymbol{y}_i \boldsymbol{y}_i^*)$ 存在?

$$(\boldsymbol{x}_i, \boldsymbol{y}_i \in P_N, \textstyle\sum_i p_i = 1, p_i \geq 0)$$

ここで*は転置複素共役を表し，$\rho \geq 0$ はρが非負定値であることを意味する．S_Nの要素の行列を密度行列といい，状態は一般のN準位系量子状態で

ある．N 準位系純粋状態 $\boldsymbol{x}$ に対しては，$\boldsymbol{xx}^*$が対応する密度行列となる．上の問題で，N^2 準位系量子状態 ρ が純粋状態のテンソル積の確率混合によって表現できる場合その状態は分離可能であるとされる．そのように表せないとき，エンタングルしているという．

量子状態から情報を得るには測定が必須であるが，一方その測定によって状態そのものが変わってしまう．与えられた量子状態が分離可能なのかエンタングルしているのかをその測定結果から判定する問題を考える．上述の測定によって状態そのものが変化する特性ゆえ，1 度の測定で判定を下すのは非常に困難である．したがって，元の量子状態は同じものを繰り返し生成することができると仮定し，その 1 つ 1 つに対して様々な測定を行うことによって測定結果を集積し，その結果全体からエンタングルしているかどうかを判定することが考えられてきた．また，これが実験的にも可能なスキームとなっていた．

ここでは膨大な量にのぼる測定の理論を詳細に述べることはできないので，抜粋して測定によって得られる情報の一部を直接的に式を用いて記すことにする．

$\mathbf{C}^{N(A)} \otimes \mathbf{C}^{N(B)}$ 上の量子状態 ρ

Alice側測定$M_i^{(A)} \in \mathbf{C}^{N(A) \cdot N(B)}$ $(i = 1, \ldots, m^{(A)})$,

Bob側測定 $M_j^{(B)} \in \mathbf{C}^{N(A) \cdot N(B)}$ $(j = 1, \ldots, m^{(B)})$

ここで，測定の条件として

$$0 \leq M_i^{(A)} = (M_i^{(A)})^* \leq I,$$

$$0 \leq M_j^{(B)} = (M_j^{(B)})^* \leq I$$

であり，これに対して相関表 $C(\rho)$を

$$C(\rho) = \{(p_{ij}) \mid i = 0, \ldots, m^{(A)},\ j = 0, \ldots, m^{(B)},\ (i, j) \neq (0,0)\}$$

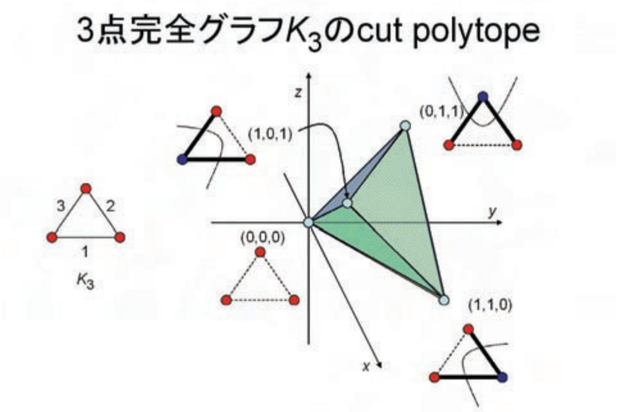
とし，ここで p_{ij} は

$$p_{ij} = \mathrm{Tr}(\rho(M_i^{(A)} \otimes M_j^{(B)}))$$

$$M_0^{(A)} = M_0^{(B)} = I$$

によって定める．

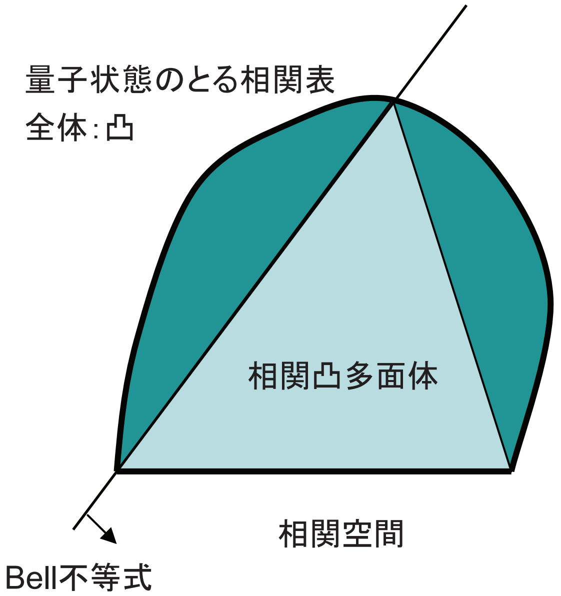
こうした情報を整理したうえで，測定が 2 値をとるのが規準的な場合であることに着目し，本研究では最初に次のことを確認した．分離可能量子状態 ρ 全体と測定全体に対する相関表の集合は，凸多面体をなす．この凸多面体はブール 2 次凸多面体や相関凸多面体として知られているもので，組合せ最適化・組合せ的凸多面体理論で精力的に研究がなされてきたグラフのカット凸多面体とアフィン同型である．具体的には，上記設定のもとの相関表全体がなす凸多面体は，2 部グラフ $\mathrm{K}_{m(A),m(B)}$ の相関凸多面体であり，3 部グラフ $\mathrm{K}_{1,m(A),m(B)}$のカット凸多面体にアフィン同型である．ここではカット凸多面体の例として，3 点の完全グラフに対するものを次図に示して説明としておく．



以上が分離可能量子状態に対する相関表全体を考えた場合である．したがって，もしある量子状態に対してある測定が存在し，それによる相関表が上述の凸多面体の中に入らないことが示されれば，そのもとの量子状態は分離可能でなく，エンタングルしていることがわかる．凸多面体は，ファセットを定める不等式の共通部分として表され，凸多面体の外の点に対しては必ずあるファセットを定める不等式が存在して，その外点ではその不等式が満たされない (不等式が破れる) ものが存在する．タイトな Bell 不等式とは，相関凸多面体のファセットを定める不等式のことであり，上述の性質を用いて，それを測定とうまく組合せるとエンタングルしているかどうかを調べることができる．

次の図でその概念を示す．量子状態の空間は数理的には扱えるものの実験的には直接に触れることはできないが，測定によって観測結果を得た空間(図ではそれを相関空間と呼んでいる)においては具体的なものとして捉えることができる．その相関空間においては，分離可能な量子状態の相関表全体からなる相関凸多面体に対して，量子状態全体に対する相関表全てはそれを真に含む凸集合となっており，図のように相関凸多面体のファセットを定めるタイトなBell不等式でエンタン

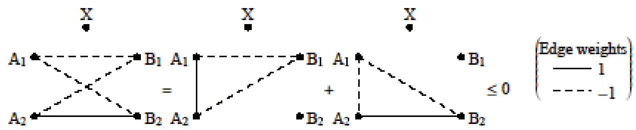
グルしているかどうかを判定できる．



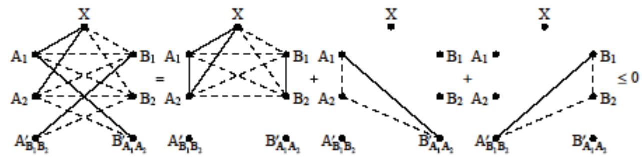
3 これまでの研究成果

(1) 本年度では，Avis, Imai, Ito, Sasaki の 4 名の共著で初期の成果をまとめたものを Journal of Physics A: Mathematical and General に投稿し掲載まで至ることができた．この論文では，上述の分離可能状態の相関表全体が凸多面体が 3 部グラフのカット凸多面体であることを指摘し，組合せ的凸多面体論で詳細に調べられているカット凸多面体の結果をこの Bell 不等式の場合に適用することを試みた．具体的には，従来研究で完全グラフのカット凸多面体のファセットは K_9 くらいまで調べ上げられていることに鑑み，それらファセットを完全 3 部グラフ $K_{1,m(A),m(B)}$のファセットに変換する汎用的手法として 3 角消去 (Triangular Elimination) を提案した．

3 角消去のうちの「3 角」は，カット凸多面体の理論が距離埋め込みとも直結していて，いわゆる距離の 3 角不等式に対応する不等式がカット凸多面体のファセットを定めることから来ている．3 角消去の「消去」は凸多面体論での一般的技法である Fourier-Motzkin 消去に由来している．3 角消去は Fourier-Motzkin 消去を一方の不等式を 3 角不等式にして適用したものであるが，Fourier-Motzkin 消去が単にファセットを表現する不等式を足し合わせただけではファセットを導出する不等式に必ずしもならないのに対し，3 角消去では土台の完全グラフにはない点を絡ませた 3 角不等式を用いることで，導出された不等式が必ずファセットを定義することが保証できるようになっている．



例として Bell 不等式の最も基本的なものである CHSH 不等式の場合の説明図を示す．CHSH 不等式は，カット凸多面体の理論では $K_{1,2,2}$ の最も非自明なファセットに対応し，上図のように 2 つの 3 角不等式の和として最も左の図のように表わされる．



もう 1 つの例として，上図は左から 2 番目の K5 の不等式に 3,4 番目の 3 角不等式を加えて，左から 1 番目の不等式を得る過程を示す．

この論文ではさらに 3 角消去により膨大な数の Bell 不等式が系統的に獲得できることを具体的に示し，またカット凸多面体の超幾何不等式クラス等に対応する無限個からなる Bell 不等式のクラスが構成できることを示した．またこの問題の背景にある対称性に関して，違う過程を経て得られる 3 角不等式同士が異なるものになっていることを示すことも行っている．

(2) グループメンバによる結果であるが，Avis, Ito は arXiv:math.CO/0505143 において，Collins, Gisin がその従来研究から出てきた未解決問題としていた I_{mm22} という不等式系がタイトな Bell 不等式となっているのかというものについて，カット凸多面体の理論を用いて肯定的に解決した．

(3) Avis, Imai, Ito は量子性に関してさらに研究を推し進めることにより，Bell inequalities stronger than the Clauser-Horne-Shimony-Holt inequality for three-level isotropic States という論文を Physical Review A に投稿，採択されるまでに至った．量子情報で有名な Werner 状態等の量子特有の対称性を満たす量子状態について，これまでは CHSH 不等式より強力なものが知られていなかったが，この論文ではそのような Bell 不等式が存在するかという未解決問題に対して肯定的な解決を与えることに成功した．具体的には，本研究の過程で得

られた Bell 不等式を系統的に調べ，測定数が相対的に少ない 89 個の不等式に着目し，その上で精緻な数値計算を行うことによって，3 準位系の isotropic 状態という対称性をもつ量子状態に対して，5 つの Bell 不等式が CHSH 不等式より強力であることを示した．すなわち，その 5 つの Bell 不等式それぞれに対して isotropic 状態なある量子状態が存在し，それに対してうまく測定して相関表を得るとその Bell 不等式が破れるが，CHSH 不等式に対してはどのような測定をしても決して CHSH 不等式は破れないという状態が存在し得るということである．本研究で調査できたものはまだまだ限られているが，その中で本質的に CHSH 不等式よりも強力なものが 5 つも発見できたということは，傾向としてどのような Bell 不等式についてもそれが最強である量子状態が存在する可能性を提示していると思われる．凸多面体の場合，ファセットを決定する不等式はすべて有効であり，それを除いてしまうと凸多面体が膨らんでしまうが，相関空間でも同様なことが成り立っている可能性が高い．この問題は，量子状態とその測定に関する非線形性から理論的にそれを示すのは非常に困難と考えられてきたが，本研究の成果はその解決に向けての一歩といえるだろう．

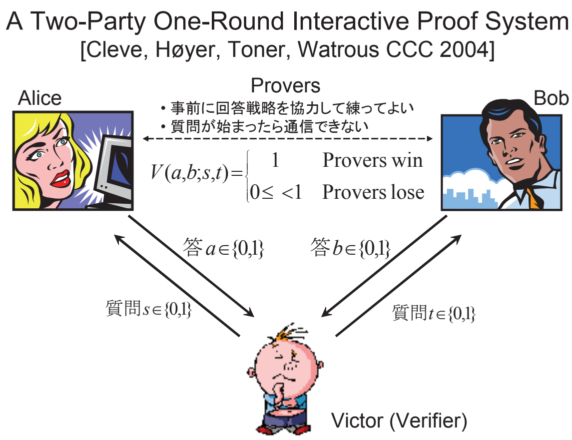
一方で，大きな未解決問題としては上記肯定的結果は 3 準位系では得られたものの，2 準位系に限った場合においては，同じ対象とした 89 個の Bell 不等式についてかなり詳細に数値計算したもののそのような結果については得ることができていないことが挙げられる．この数値計算は，双線形半定値計画問題となっていて全域的な最適解を求めるのが非常に困難なものとなっている．実際には双線形性を活用して，片方の変数を固定すると半定値計画（しかも制約が簡単なため，固有値問題に帰着されるもの）になることからそれを解き，次は他方を固定して片方の変数を最適化という交代型の局所最適化を行っており，この点の全域的最適化さらにはロバスト計算の観点からの精度保証を行うことが望まれる．

また，従来量子計算では 2 準位系量子状態を 1 量子ビットと呼び，ほぼこれに限ってアルゴリズムや情報量の理論を展開しているが，このように多準位系を基礎としてそのテンソル積空間を考えることが 2 準位系とそのテンソル積空間でのみ発想する場合と違った様相を示すことに繋がることを示したことで，従来のアプローチ法に対する反省を促す知見を与えるものになっているかもしれない．

(4) Bell 不等式から対話証明への拡張について．これもメンバの成果であるが，Avis, Hasegawa, Kikuchi, Sasaki は arXiv:quant-ph/0509047 において，Bell 不等式の中でもより情報処理的な側面を調べる研究として Hadamard グラフの量子彩色ゲームを擬似テレパシー (pseudo-telepathy) ゲームとの関係で調査を行い，その成果は IECE Trans. Fundamentals の 2006 年 5 月号に掲載予定である．

Bell 不等式を用いて量子状態がエンタングルしているかどうかを判定するには，同じ量子状態を繰り返し生成し，種々の測定を適用して，その観測結果から相関表の要素を経験分布で推定し，その上で不等式判定を推定誤差を考慮して行うという過程を経る必要があった．それに対して成功確率は小さくなるかもしれないが，誤差が生じない一度の実験で Bell 不等式の破れに相当することを判定できないかという思考実験がなされており，実はそれこそがコンピュータ科学での対話証明の枠組みを Bell 不等式に適用するものとなっている．

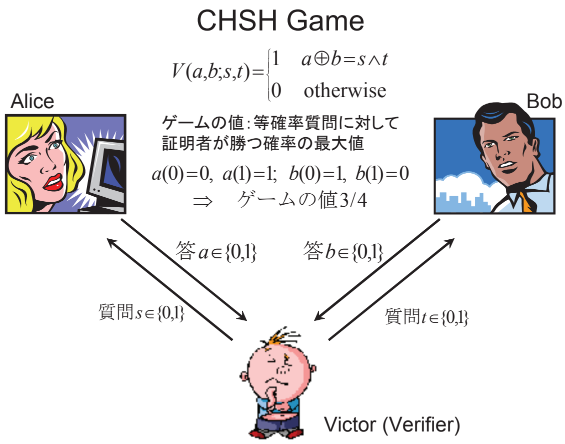
その概要を対話証明の観点から図式化したものが次の図である．



この図では，検証者 (verifier) の Victor が，Alice, Bob という 2 人の証明者 (prover) にそれぞれ質問し，Alice と Bob の答えを照らし合わせてその問題に対する答えの正しさを検証しようとしている．ここで，Alice と Bob は質問される前には結託して戦略等練ってもよいが，質問が開始されると通信は禁じられ協力をすることはできないルールとなっている．Victor の方はそれぞれへの質問を工夫することによって，自分が正しく検証できる確率を上げるようにする．それに対して，Alice と Bob は古典情報処理の枠組みではできな

いことでも，量子情報処理の枠組みを活用することにより事前協力してエンタングルしている量子状態をもつようにすることで，質問後の通信なしでより強力な何かをできることを模索することになる．

次の図は，Bell 不等式の最も基本的なものでありかつ重要なCHSH不等式の場合にこのゲームを考えたものである．



このような若干不思議なゲーム値の設定に対するものが，CHSH 不等式に対応している．この場合，Alice と Bob がエンタングルしている状態をもつことによって，証明者が勝つ確率を古典の場合の最大値の 3/4 から真に大きくすることができる．

本研究では，エンタングルしている状態を持っている場合には証明者が確率 1 で勝つことができるのに対し，古典情報処理の枠組みではそうはできない問題として最初に提示された Hadamard グラフの彩色問題に着目し，これまでの結果で限定されていた条件を Hadamard 変換の代わりに量子 Fourier 変換を用いてはずすとともに，Hadamard グラフでこのようなことができる最小の場合を示すことに成功している．これはグラフ理論的にも彩色問題での新しい問題を提示するものとなっている．

発表論文

M. Hayashi, H. Imai, K. Matsumoto, M. B. Ruskai and T. Shimono: Qubit Channels which Require Four Inputs to Achieve Capacity: Implications for Additivity Conjectures. *Quantum Information and Computation*, Vol. 5 (2005), pp. 13－31.

T. Yamasaki, H. Kobayashi and H. Imai: Quantum versus Deterministic Counter Automata. *Theoretical Computer Science*, Vol. 334, Issues 1-3 (2005), pp. 275－297.

大音真由美，今井桂子: Holevo 容量を求める外近似切除平面アルゴリズム．電子情報通信学会和文論文誌 A，Vol. J88-A，No. 8（2005），pp. 922－925.

K. Kato, M. Oto, H. Imai and K. Imai: Voronoi Diagrams for 1-qubit Pure Quantum States. *Proceedings of the 2nd International Symposium on Voronoi Diagrams*, Seoul, Korea, October 2005, pp. 293－299.

D. Avis, H. Imai, T. Ito and Y. Sasaki: Two-Party Bell Inequalities Derived from Combinatorics via Triangular Elimination. *Journal of Physics A: Mathematical and General*, Vol. 38 (2005), pp. 10971－10987.

T. Ito, H. Imai and D. Avis: Bell Inequalities stronger than the Clauser-Horne-Shimony-Holt Inequality for Three-Level Isotropic States. *Physical Review A*, 2006, to appear.

D. Avis, J. Hasegawa, Y. Kikuchi and Y. Sasaki: A Quantum Protocol to Win the Graph Colouring Game on All Hadamard Graphs. *IEICE Trans. Fundamentals*, May 2006, to appear.