（別紙5）

「量子と情報」研究領域 領域活動・評価報告書
－平成 18年度終了研究課題－

研究総括 細谷 暁夫

1. 研究領域の概要

この研究領域は、量子力学的現象を利用した情報処理を実現するために、量子力学と情報処理の間に横たわる諸問題の解決に資する研究を対象とするものです。

具体的には、量子もつれ効果の強さと情報処理能力の関係についての理論的・実証的な研究、新しいアルゴリズムの創出、量子状態の評価技術、記憶方法、量子情報の高密度伝送方式、通信における符号化・誤り訂正・情報セキュリティ等、安全かつ高速の情報処理を実現するための基盤を拡充する抜本的、革新的な研究を対象とします。

2. 研究課題・研究者名

別紙一覧表参照

3. 選考方針

選考の基本的な考えは下記の通り。

1） 選考は「量子と情報」領域に設けた選考委員 10 名と研究総括で行う。

2） 選考方法は、書類選考、面接選考及び総合選考とする。

3） 選考に当たっては、募集要項に示した選考基準を基本としたが、以下の点に特に留意した。

量子と情報の分野を広く捉えて、理論実験とも何かをやってくれる人であることを面接選考で十分に見たつもりである。国立大学・私立大学および企業の研究者のバランス、ジェンダー・年齢など特に考慮せずに選考したが、結果的にバランスが取れたと考える。

4. 選考の経緯

一応募課題につき領域アドバイザー3 名が書類審査し、書類選考会議において面接選考の対象者を選考した。続いて、面接選考および総合選考により、採用候補者を選定した。

選 考	書類選考	面接選考	採用者
対象者数	19 名	13 名	5 名

5. 研究実施期間

平成 15 年 10 月～平成 19 年 3 月

6. 領域の活動状況

領域会議：7 回

研究報告会：1 回

研究総括（または技術参事）の研究実施場所訪問：研究開始時に、研究総括と技術参事が全研究者を訪問し、研究目標に対する意気込みを伺い、それに対して研究総括から激励及びコメントを行なった。同時に研究環境を把握して、上司に協力を要請した。その後、年 1 回(年度末)は、研究総括と技術参事が、研究進捗の把握と支援を目的に訪問。また、研究実施場所の移動の際には、技術参事が適宜訪問。

7. 評価の手続き

研究総括が研究者からの報告・自己評価を基に、必要に応じて領域アドバイザーの協力を得て行った。また、研究終了報告会の参加者の意見も参考に行った。

（評価の流れ）

平成 18 年 11 月　　研究報告会開催
平成 19 年 2 月　　研究課題別評価提出
平成 19 年 3 月　　研究報告書提出

平成 19 年 3 月　　研究総括による評価
平成 19 年 3 月　　研究期間終了

8. 評価項目
（1） 研究開始時の研究構想を基準に研究の達成度
（2） 外部発表(学術論文、口頭発表など)、特許など研究成果の発信状況
（3） 学術賞、学会招待講演、新聞記事発表など外部からの評価状況
（4） 得られた研究成果の科学技術への貢献

9. 研究結果

9.1 理論的研究

石坂智研究者は、研究の進展の中で発見した束縛エンタングルメントの性質に関して重要な研究成果を上げました。それが、計画の本筋に関係の深い強単調性に結びついた点について、見事な研究展開と評価します。5編の論文のうち3編は単著であり、残りの2編も石坂智研究者の貢献が大であることは、石坂智研究者の力量をあらわしています。この分野に大きく貢献しました。

清水明研究者は、大きな量子計算の速さに対して「マクロにエンタングルした状態」が重要な役割をすると予想してはじめ、ほぼそれを実証した研究です。量子多体系との類推から、その判定をする指標を導入しシミュレーションを含む具体的に説得力ある議論を展開しました。一般的な証明までには至っていませんが、量子計算の速さを理解するための重要な知見であると考えます。何よりも、この研究の基本的なアイデアが日本発である点を高く評価します。

村尾美緒研究者の非対称な量子状態の共有に関する基礎的研究とその応用である量子鍵に関する仕事が、この分野で高く評価されています。他の仕事の出版も時間の問題でしょう。3年間の業績として申し分ありません。計画が目指していた量子状態自体を秘密鍵にして、量子計算機があっても安全な暗号システムについては、計画の終わり頃にエンジンがかかって一分野をなすような系統的な研究への大きな橋頭堡を築いているように見えます。この分野で喫緊に必要な若手の養成にも心を砕いている点も高く評価したいと思います。

9.2 実験的研究

北野晴久研究者の固有ジョセフソン接合の研究において、彼はメサ型IJJ素子を作成し電流分布測定をし、「大きい接合領域でのフラクソン励起」という予想に反する結果を得、そこから高温超伝導物質について物理的に興味深い知見を得ました。その成果を高く評価します。本来の研究目的のために、それをS字型に切り替えて MQT 状態の直接観測可能なところまで進めた研究推進力にも敬意を払います。高温超伝導量子ビットの可能性についての重要な成果と思いますので、今後の発展を期待します。

黒田隆研究者は物理的に単純明快なやりかたで、
（1）単一量子ドットの自然放射の減衰信号を初めて観測
（2）そのラビ振動
（3）励起子コヒーレンス時間の評価
を実験的に実証した点を高く評価します。

単一量子ドットによる量子計算素子の研究に関して大きな成果をあげたと思います。量子ドット複合構造があらたに見いだされたこともあり、今後の2ビットの量子ゲートの実証実験に期待します。

10. 評価者

研究総括 細谷 暁夫　　東京工業大学 大学院理工学研究科 教授

領域アドバイザー氏名（五十音順）

今井 浩	東京大学 大学院情報理工学系研究科 教授
井元 信之＊	大阪大学 大学院基礎工学研究科 教授
枝松 圭一	東北大学 電気通信研究所 教授
小澤 正直	東北大学 大学院情報科学研究科 教授
北川 勝浩	大阪大学 大学院基礎工学研究科 教授
佐々木 雅英	情報通信研究機構 新世代ネットワーク研究センター 研究マネジャー
高木 伸	富士常葉大学 環境防災学部 教授
竹内 繁樹	北海道大学 電子科学研究所 助教授
蔡 兆申	日本電気(株) 中央研究所 基礎・環境研究所 主席研究員
南 不二雄	東京工業大学 大学院理工学研究科 教授
山本 喜久	スタンフォード大学 応用物理・電気工学科 教授

＊平成 17 年 4 月から参画

（参考）

（1）外部発表件数

	国 内	国 際	計
論 文	0	30	30
口 頭	39	27	66
その他	4	0	4
合 計	43	57	100

※平成 19 年 3 月 31 日現在

（2）特許出願件数

国 内	国 際	計
1	0	1

（3）受賞等

・北野 晴久

Nano-Virtual-Labs Joint Workshop on Superconductivity (NVLS2005) ベストポスター賞（H17.12）

（4）招待講演

国際 2 件

国内 0 件

別紙

「量子と情報」領域　研究課題名および研究者氏名

研究者氏名 （参加形態）	研　究　課　題　名 （研究実施場所）	現　職 （応募時所属）	研究費 （百万円）
石坂　智 （兼任）	量子縺れ最適回復プロトコル導出を可能にする量子状態の判定・測定法 （日本電気(株) 中央研究所 基礎・環境研究所）	日本電気(株) 中央研究所 基礎・環境研究所 主任研究員 （日本電気(株) 基礎研究所 主任研究員）	11
北野 晴久 （兼任）	固有ジョセフソン接合と超伝導共振器を用いた量子状態制御の研究 （東京大学　大学院総合文化研究科）	東京大学　大学院総合文化研究科 助手 （同上）	57
黒田 隆 （兼任）	単一量子ドットにおける多光子量子操作 （物質・材料研究機構　量子ドットセンター）	物質・材料研究機構　量子ドットセンター　主任研究員 （物質・材料研究機構　ナノマテリアル研究所　主任研究員）	42
清水 明 （兼任）	多体量子系としての量子計算機の分析 （東京大学　大学院総合文化研究科）	東京大学　大学院総合文化研究科 教授 （同上　助教授）	40
村尾 美緒 （兼任）	量子鍵を用いた次世代量子暗号プロトコル （東京大学　大学院理学系研究科）	東京大学　大学院理学系研究科 助教授 （同上）	24

研究課題別評価

1　研究課題名：量子縺れ最適回復プロトコル導出を可能にする量子状態の判定・測定法

2　研究者氏名：石坂　智

3　研究のねらい：

量子縺れ（量子エンタングルメント）は量子情報処理にとって極めて重要な資源の一つである。量子通信の送信者と受信者の様に遠く隔てられた 2 つのパーティがエンタングルメントを共有する事を考えると、初期に量子状態が持っていたエンタングルメントの一部は伝送途中のデコヒーレンス等により破壊され、共有できるのは不完全にエンタングルした量子状態である。一方、局所操作と古典通信（LOCC）により、この不完全にエンタングルした状態を、元の完全にエンタングルした状態（EPR 状態）へと回復させることができる。この回復を行う LOCC プロトコルが、エンタングルメント回復プロトコルである。このプロトコルは量子暗号通信の中継に必須であり、他の多くの量子情報処理アプリケーションの動作効率を上げるなどの広範な応用性を持ち、極めて基本的なプロトコルである。

本研究では、エンタングルメント最適回復プロトコルの導出を将来目標に捉え、その基盤技術を拡充する為に、量子エンタングルメントに関する数理的研究を行う。

4　研究成果：

（1）Schmidt 階数と束縛エンタングルメント

A と B、2 つのパーティの系における任意のエンタングルした純粋状態$|\psi\rangle$は、EPR 状態

$$|\phi_2\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$$

と、確率 1 の LOCC で相互変換が可能である。しかし、この相互変換は$|\psi\rangle$の同一コピー数が無限大の漸近領域に限られる。もし、A と B が$|\psi\rangle$を単一コピーしか所有していないとすると、LOCC による状態変換は或る強い制限を受けることになる。それは『A と B は$|\psi\rangle$にどの様な LOCC を行っても、その重ね合わせの項数（Schmidt 階数、還元密度行列の階数）を増やす事ができない』という制限である。例えば、

$$|\phi_3\rangle = (|00\rangle + |11\rangle + |22\rangle)/\sqrt{2}$$

とすると、$|\phi_2\rangle \rightarrow |\phi_3\rangle$の変換は確率的にすら不可能である（図 1）。また、3 つのパーティの系における GHZ 状態

$$|GHZ\rangle = (|000\rangle + |111\rangle)/\sqrt{2}$$

と W 状態

$$|W\rangle = (|001\rangle + |010\rangle + |100\rangle)/\sqrt{3}$$

は、$|GHZ\rangle \rightarrow |W\rangle$の変換も$|W\rangle \rightarrow |GHZ\rangle$の変換も不可能であり、GHZ 型と W 型は比較不可能な異なるエンタングルメントであると言われる（図 2）。

これらの変換を行うのに必要な最小資源は何だろうか？この疑問に答える為に束縛エンタングルメントに着目する。本研究により、束縛エンタングルメントは純粋状態の変換に対して非常に強力な威力を持ち、上記 LOCC の制限を完全に取り除いてしまう効果がある事が判明した（図 1 および図 2）。

例えば、A と B の 2 つのパーティが$|\phi_2\rangle_{A3B3}$に加え、

$$E_{AB} = \frac{1}{7}|\phi_3\rangle\langle\phi_3|_{A1B1} \otimes |\phi_2\rangle\langle\phi_2|_{A2B2} + \frac{1}{28}(I - |\phi_3\rangle\langle\phi_3|)_{A1B1} \otimes (I - \phi_2\rangle\langle\phi_2|)_{A2B2}$$

の束縛エンタングル状態を共有していたとする。もし A と B が、それぞれ A2A3 と B2B3 に対しベル状態測定を行う

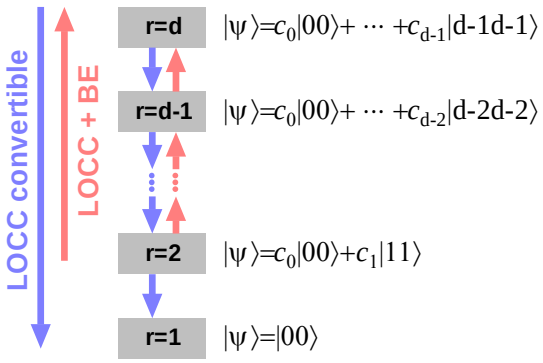


図 1. 純粋状態の LOCC 変換性と、それに対する束縛エンタングルメント(BE)の効果。LOCC は Schmidt 階数（r）を下げる青矢印の方向にのみ変換可能であるが、BE を利用する事により赤矢印方向の変換が可能になる。

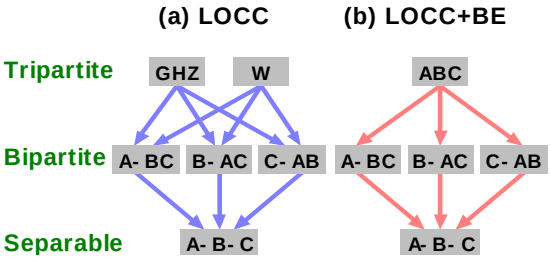


図 2.　（a）LOCC と（b）束縛エンタングルメント（BE）を利用した LOCC における 3 量子ビットの純粋状態の分類と変換性。

と、その結果として$|\phi_3\rangle_{A1B1}$を共有する事ができる。すなわち、E_{AB}の束縛エンタングルメントを利用する事で$|\phi_2\rangle \rightarrow |\phi_3\rangle$の変換が可能になる。同様にして、AとBは適切な束縛エンタングルメントを利用する事で、エンタングルした純粋状態のSchmidt階数を幾らでも増やす事ができる(図1)。

同様の効果は3つのパーティの系にも存在する。束縛エンタングルメントを利用すると、LOCCで比較不可能だったGHZ状態とW状態でさえも相互に変換する事が可能になる。この事は、エンタングルメントの分類に対しても大きな意味を持つ。3量子ビットの系のエンタングルメントをLOCCで分類すると、3体のエンタングルメントとしてはGHZ型とW型の2つが存在するが、束縛エンタングルメントを利用したLOCCで分類を行うと、GHZ型とW型は同じ型に属してしまう事を意味している(図2)。一般に、N個のパーティの系におけるエンタングルメントをLOCCで分類すると、比較不可能な型が無限個存在する事になり、分類は極めて複雑になるが、束縛エンタングルメントを利用したLOCCで分類すると、それら異種エンタングルメントは全て同一の型に属する事になる。この様に、束縛エンタングルメントにはエンタングルメントの分類を著しく簡単化すると言う効果がある。

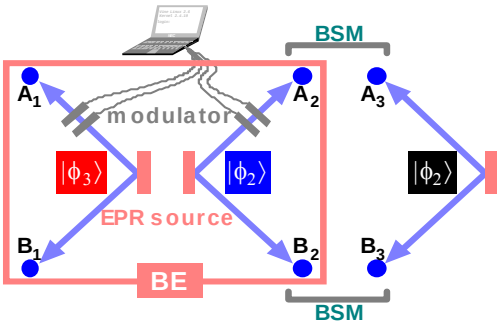


図 3. 束縛エンタングルメント(BE)を利用したLOCCによる$|\phi_2\rangle \rightarrow |\phi_3\rangle$の実験スキーム。

束縛エンタングルメントを利用したLOCCはPPT保存写像の一つであり、変換における最大確率はPPT保存写像を考える事で定量的に議論できる。この問題は、convex optimizationへと帰着させる事ができ、更に状態が持つ対称性を利用する事で上記変換の最大確率(P)を求める事ができる。結果のみを示すと、$|\phi_d\rangle \rightarrow |\phi_{d'}\rangle$に対しては

$$P = d(d-1)/(dd'+d'-2d),$$

$|GHZ\rangle \rightarrow |W\rangle$に対しては

$$P = \frac{1}{4}\left[(18+6\sqrt{3})^{1/3}+(18-6\sqrt{3})^{1/3}-2\right] \approx 0.75436\ldots$$

である。LOCCにおける$|GHZ\rangle \rightarrow |W\rangle$の最大変換確率がゼロ(変換不可能)である事を考えると、PPT保存写像における同変換の75%以上の変換確率は極めて大きなものであり、束縛エンタングルメントは定量的にも強力な威力を持っている事が分かる。

EPR光源を用いて束縛エンタングル状態を実験的に生成し、束縛エンタングルメントが持つ非局所性の威力を実験的にデモンストレーションする事も可能である。先に記したE_{AB}を利用する$|\phi_2\rangle \rightarrow |\phi_3\rangle$の変換に対応する実験スキームを図3に示す。この実験スキームにおいて量子ゲートは必要なく、線形光学の技術で実現が可能である。

(2)多体エンタングルメントの等価性

2つのパーティの系における任意のエンタングルした純粋状態$|\psi\rangle$は、nが無限大の漸近領域であれば

$$|\psi\rangle^{\otimes n} \leftrightarrow |\phi_2\rangle^{\otimes nE}$$

の相互変換が確率1のLOCCで可能である(Eは$|\psi\rangle$の還元密度行列のvon Neumannエントロピー)。これにより、全ての2体のエンタングルメントはEPR状態のエンタングルメントと等価であるとされる。ところが、3つのパーティの系では、$|GHZ\rangle^{\otimes n} \leftrightarrow |W\rangle^{\otimes nE}$のLOCCによる相互変換は、漸近領域においても不可能であると考えられている(厳密な証明はなされてはいないかった)。

一方、単一コピーの場合、PPT保存写像で$|GHZ\rangle \leftrightarrow |W\rangle$の確率的な相互変換が可能になる事を(1)で示した。では、PPT保存写像は漸近領域において$|GHZ\rangle^{\otimes n} \leftrightarrow |W\rangle^{\otimes nE}$の相互変換をも可能にするのだろうか?これは、エンタングルメントの等価性に関する基本的で重要な問題であると言える。

これを明らかにする為には、幾つかのエンタングルメント測度の値を漸近領域で求めなければならない。エンタングルメント測度の計算は一般的に困難であり、ましてや漸近領域での計算は極めて困難である。しかしながら、本研究では幾つかの状態クラスに対する漸近的エンタングルメント測度を計算する事に成功した。

まず、スピン0状態

$$|A\rangle = \frac{1}{\sqrt{6}}\sum_{ijk=1}^{3}\varepsilon_{ijk}\,|ijk\rangle$$

に対する3体の相対エントロピー・エンタングルメント測度E_3は

$$E_3(|A\rangle^{\otimes 2}) < 2E_3(|A\rangle)$$

を満たし、劣加法的である事が示せる。すなわち、一般に漸近的エンタングルメント測度は非漸近的測度の値とは

一致しない。そこで、$E_3(\sigma_{ABC})$とその漸近的測度 $E^{\infty}{}_3(\sigma_{ABC})$、2 体の漸近的測度 $E^{\infty}{}_2(\sigma_{AB})$、および von Neumann エントロピー$S(\sigma_{AB})$の間で成立する不等式

$$E_3(\sigma_{ABC}) \geq E^{\infty}{}_3(\sigma_{ABC}) \geq E^{\infty}{}_2(\sigma_{AB}) + S(\sigma_{AB})$$

に着目する。筆者が以前に得た 2 量子ビットにおける相対エントロピー・エンタングルメント測度の関係式を用いると、もし 2 量子ビットの混合状態σ_{AB}が、その最近接のエンタングルしていない状態と可換であれば、$E_2(\sigma_{AB})$が弱加法的になる事を示せる。この結果と上記不等式を用いると、W 状態に対する $E_3(W)$も弱加法的であり、$E^{\infty}{}_3(W)=\log(9/4)$である事が分かる。これより、GHZ 状態と W 状態に対する還元 von Neumann エントロピーは

$$S_A(GHZ) = 1 > 0.92 = S_A(W)$$

の不等式を満たし、$E^{\infty}{}_3$ は

$$E^{\infty}{}_3(GHZ) = 1 < \log(9/4) = E^{\infty}{}_3(W)$$

の不等式を満たす。もし、確率 1 の PPT 保存写像で$|GHZ\rangle^{\otimes n} \leftrightarrow |W\rangle^{\otimes nE}$の相互変換が可能であるとすると、全ての連続な漸近的エンタングルメント測度 R^{∞}に対し

$$R^{\infty}(GHZ) = \alpha \cdot R^{\infty}(W)$$

が成立する様な係数αが存在しなければならない。しかし、上記の S_A と $E^{\infty}{}_3$ の不等式により、その様なαは存在し得ず、GHZ 型と W 型のエンタングルメントは、PPT 保存写像においても等価にはなり得ないと結論できる。

同様にして、GHZ 型のエンタングルメントは、W 型と AB、AC、BC 間の EPR 型のエンタングルメントには分割不可能であるとの結論も得られる。LOCC は PPT 保存写像に含まれるので、これらの結論は LOCC でも成立する。

（3）強い単調性とエンタングルメント回復

先に述べた状態変換における制限、『どの様な LOCC も、純粋状態の Schmidt 階数を確率的にすら増やす事ができない』は、強い単調性の一つである。これを混合状態に拡張した強い単調関数は Schmidt 数と言われる。一方、PPT 保存写像は、これらの強い単調性を取り除いてしてしまう事を（1）で示した。これにより、エンタングルした純粋状態は全て確率的に相互変換可能になった。これは、純粋状態の変換に関する強い単調性が Schmidt 数しか存在しないからである。では、混合状態に関する変換では、どうなるのだろうか？この問題は単一コピーにおけるエンタングルメント回復と深く関係した重要な問題である。

混合状態から EPR 状態への変換（すなわち単一コピーのエンタングルメント回復）

$$\sigma \rightarrow |\phi_2\rangle$$

を考える。σを $C^d \otimes C^d$ 上の混合状態とすると、σの階数が

$$\mathrm{rank}(\sigma) \geq d^2 - 2$$

と高い場合、PPT 保存写像の下でも単一コピーのエンタングルメント回復が不可能である事を本研究で証明した。先に述べた通り、PPT 保存写像は Schmidt 数の強い単調性を取り除いてしまう。よって、上記の結論は、混合状態の変換においては、PPT 保存写像でも取り除けない強い単調性が残っている事、すなわち Schmidt 数と独立な強い単調性が存在している事を意味している。

そこで、本研究では幾何学的なアプローチにより、Schmidt 数とは独立な強い単調関数の導出も行った。まず、正行列の集合を考える。密度行列（σ）は（規格化条件を除いて）正行列（$\sigma \geq 0$）なので、正行列の集合は密度行列の集合に相当する。また、PPT 行列の集合を考える。PPT 行列とは、部分転置をすると正行列になる行列である。これら 2 つの集合の模式図を図 4 に示した。2 つの集合の共通部分は PPT 状態、すなわち Peres criterion を満たす状態で、典型的にはエンタングルしていない状態である（束縛エンタングル状態も一部含まれる）。

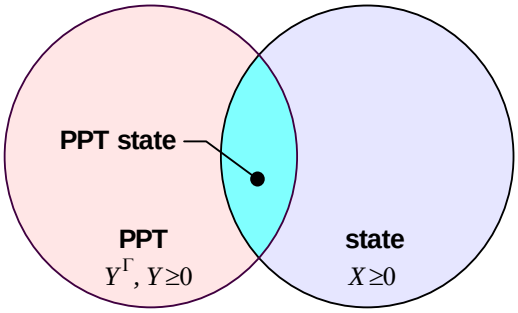


図 4. 密度行列(正行列)の集合と PPT 行列の集合の幾何学的模式図。共通部分は Peres criterion を満たす状態(PPT 状態)。

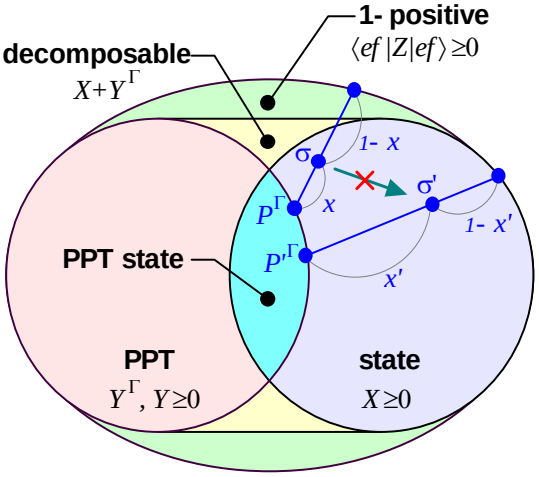


図 5. エルミート行列の集合の幾何学的模式図。密度行列と PPT 行列の集合は decomposable 行列と 1−positive 行列の集合の一部である。密度行列σを図の様に凸結合で表現した時の最小内分比 x は強い単調関数となる。

まず、この幾何学的構造に着目する事で、エンタングルメント理論における重要な未解決問題の一つ、binegativity problem を解決する事に成功した。すなわち、全ての 2 量子ビットの密度行列が、

$$|\sigma^{\Gamma}|^{\Gamma} \geq 0$$

を満たす事を厳密に証明した。

また、正行列と PPT 行列の凸結合で記述できる行列は decomposable 行列、直積状態による期待値が常に正（$\langle ef|X|ef\rangle \geq 0$）となる行列は 1−positive 行列と呼ばれる。全ての decomposable 行列は 1−positive 行列であるので、エルミート行列の集合は、図 5 の様な構造をしていると考えられる。

この幾何学的構造に着目し、混合状態の密度行列σを PPT 行列と 1−positive 行列の凸結合で表現する事を考える。その際、σ^{Γ}の Jordan 分解（直交分解）を

$$\sigma^{\Gamma} = P - Q$$

とし、PPT 行列は P^{Γ}に選ぶ。また、凸結合における 1−positive 行列δは、内分比 x が最小になる様に選ぶものとする(図 5)。この最小の内分比 x は、混合状態における強い単調関数の一つであり、LOCC では確率的にすら増やす事ができない。例えば、図 5 においてσ'を同様な凸結合で表現した時の最小内分比を x'とすると、$x' > x$ であるので、$\sigma \rightarrow \sigma'$の LOCC 変換は確率的にすら不可能であると結論できる。密度行列σを P^{Γ}と decomposable 行列の凸結合で表現した場合でも、その最小内分比は別の強い単調関数の一つとなる。大雑把に言うと、混合状態の LOCC 変換は、PPT 状態へと近づく方向へしか許されていない事になる。

これら最小内分比[以下 $M_1(\sigma)$とする]が強い単調関数の一つである事は、convex optimization における双対性を用いて証明する事ができる。また $M_1(\sigma)$は、全てのエンタングルしていない状態に対して 0 の値を取り、全てのエンタングルした純粋状態に対して 1 の値を取る。エンタングルメント回復とは、混合状態をエンタングルした純粋状態、すなわち $M_1=1$ の状態へと変換する事である。M_1 は LOCC で確率的にすら増やせないので、これより直ちに、エンタングルメント回復できる混合状態σは $M_1(\sigma)=1$ を満たさなければならない事が分かる。また、これらの状態は、1−positive 行列の集合の境界に位置しなければならない事も図 5 より直ちに分かる。これらは、単一コピーにおけるエンタングルメント回復が可能である為の必要条件である。なお、コピー数が n の状態のエンタングルメント回復は、$\rho = \sigma^{\otimes n}$の単一コピーのエンタングルメント回復と捉える事ができるので、ここで導出した必要条件は、コピー数が有限である場合のエンタングルメント回復全てに適用される。

5　自己評価：

状態空間の幾何学的構造の解析を通して量子エンタングルメントの基礎的性質を明らかにし、状態空間の幾何学的構造と量子情報処理の間の関係を解明する事が当初の研究計画であった。しかし、研究開始直後に束縛エンタングルメントの全く新しい性質を思いがけず発見した。この性質は、（1）パーティの数や系の次元に関係なく広く現れる一般的なものであり、（2）量子エンタングルメントの分類という基本的な事柄とも密接に関係しているものであった。そこで、これは重要な性質であると判断し、定量的解析や漸近領域における振舞い等の詳細な研究を行った。量子情報における理論研究の様な基礎研究では、必ずしも計画通りに研究が進む訳ではないので止むを得ない事だし、柔軟に対応する事が重要だと思っているが、当初の研究計画とは異なってしまったことは確かである。

しかし、混合状態の場合におけるこの性質の意味を落ち着いて考えて見ると、この性質は強い単調性を通して単一コピーのエンタングルメント回復と関係があることに気づいた。そこで、当初の研究計画に戻り、状態空間の幾何学的性質に着目し、新しい強い単調性の導出および単一コピーのエンタングルメント回復の必要条件の導出を行った。これにより、エンタングルメント回復と状態空間の幾何学的性質の関係の一つの側面を明らかにすることができた。この研究は研究計画に沿ったものではあったが、成果のインパクトや応用上の重要性（特に導出した強い単調関数の計算可能性）に関しては問題があったと思う。

また、この 3 年の短い研究期間の間で、量子情報の研究に対する学会や企業の姿勢が大きく変化したと感じた。以前にも増して、量子情報の新しい方向性や新しい応用先を必要としている様に思う。特に新しい応用先の発掘に関しては、企業のマネージメントサイドからも強く要望されているところである。この情勢の変化を踏まえ、最終年度の後半では、研究総括の許可を得て現代暗号量子プロトコルの研究に着手した。この研究に関しては、残念ながら期間中に成果を上げることはできなかったが、次のステップへの重要な足がかりを得ることができた期間になったと思う。

6　研究総括の見解：

研究の進展の中で発見した束縛エンタングルメントの性質に関して重要な研究成果を上げました。それが、計画の本筋に関係の深い強単調性に結びついた点について、見事な研究展開と評価します。

5編の論文のうち3編は単著であり、残りの2編も石坂智研究者の貢献が大であることは、石坂智研究者の力

量をあらわしています。この分野に大きく貢献しましたので、この人を研究者として採択したことは成功であったと思っています。

7 主な論文等:

論文: 6 件

[1] S. Ishizaka, "Binegativity and geometry of entangled states in two qubits", Phys. Rev. A **69**, 020301-1 – 020301-4 (Rapid communication) (2004)

[2] S. Ishizaka, "Bound entanglement provides convertibility of pure entangled states", Phys. Rev. Lett. **93**, 190501-1 – 190501-4 (2004)

[3] S. Ishizaka and M. B. Plenio, "Multiparticle entanglement manipulation under positive partial transpose preserving operations", Phys. Rev. A **71**, 052303-1 – 052303-13 (2005)

[4] S. Ishizaka and M. B. Plenio, "Multiparticle entanglement under asymptotic positive partial transpose preserving operations", Phys. Rev. A **72**, 042325-1 – 042325-5 (2005)

[5] S. Ishizaka, "Strong monotonicity in mixed-state entanglement manipulation", Phys. Rev. A **73**, 062308-1 – 062308-6 (2006)

特許: 0 件

受賞: 0 件

招待講演: 0 件

その他

解説: 2 件

[1] 石坂智、「束縛エンタングルメント」、数理科学、2005 年 2 月号

[2] 石坂智、「EPR パラドックス」、月刊オプトロニクス、2007 年 3 月号

チュートリアル講演・講師・レビュー講演: 3 件

[1] 石坂智、「混合状態のエンタングルメント」、第 11 回量子情報技術研究会

[2] 石坂智、「二者間および多者間エンタングルメントとその周辺」、第 14 回非平衡系の統計物理シンポジウム

[3] S. Ishizaka, "Theory of entanglement for mixed states", The 6th Workshop on Fundamental Problems and Applications of Quantum Field Theory

国内学会発表: 6 件

国際学会発表: 4 件

[1] S. Ishizaka, "Effect of bound entangled states on the convertibility of pure entangled states", The 7-th International Conference on Quantum Communication, Measurement and Computing 2004

[2] S. Ishizaka, "Binegativity and geometry of entangled states in two qubits", ERATO conference on Quantum Information Science 2004

[3] S. Ishizaka, "Bound entanglement and convertibility of pure states", ERATO conference on Quantum Information Science 2004

[4] S. Ishizaka, "Strong monotonicity in mixed-state entanglement manipulation", Asian Conference on Quantum Information Science 2006

研究課題別評価

1　研究課題名：固有ジョセフソン接合と超伝導共振器を用いた量子状態制御の研究

2　研究者氏名：北野　晴久

3　研究のねらい：

近年，量子コンピューターに関する研究への関心が増大しているが，ほとんどの実験は希釈冷凍機を用いて初めて到達可能な数十ミリケルビンという極低温下で行われており，周辺回路まで含めた将来の実用化を考えた際に大きな障害になるものと予想される．本研究では，高温超伝導体が潜在的に持つ従来超伝導体に対する優位性がこの状況を打開する可能性を秘めていると確信し，高温超伝導体に共通の固有ジョセフソン接合（以下，IJJと略記）を用いた「量子ビット」（特に位相量子ビット）の実現により、動作温度に関する制限の緩和を目指した．さらに、超伝導共振器内に生成される単一モード光子と IJJ 量子ビットを相互作用させることにより，量子計算に本質的とされる「量子もつれ合い状態」を生成することを目指した．

より具体的には，位相量子ビットの構築に必要な次の 3 つの実験的根拠，(i) 巨視的量子トンネル(以下，MQT と略記)の実現，(ii) MQT 状態における量子化準位の形成(以下，ELQ と略記)の観測，(iii) 量子化準位間のコヒーレントな量子振動（ラビ振動），を観測するための物理的基礎であるIJJの位相ダイナミクスの解明にまず取組んだ．また，空洞量子電磁力学(以下，cavity-QED と略記)で記述される超伝導共振器内の単一モード光子を量子ビットと結合させて量子もつれ合い状態を作り出す研究は，過去に Rydberg 原子など原子系量子ビットで行われた実績はあるが，超伝導体のジョセフソン接合（以下，JJと略記）を用いる位相量子ビットに対しても可能かどうかは全く不明であった．このため，本研究ではまず位相量子ビットが超伝導共振器内の電磁場と強く結合するための必要条件を検討し，共振器内部の電磁場を空間的に一点に集中させる手段を検討した．

本研究で高温超伝導体が量子コンピューターへ応用可能なことが示されれば，実現可能な量子ビットに新しい有力候補が加わるだけでなく，超伝導量子ビットの動作温度に関するこれまでの制限が一気に緩和され，実用化に向けた研究がさらに加速されるものと期待される．また，発見から 20 年が過ぎた今でも未解明部分が残る高温超伝導体がベースとなる IJJ では，ジョセフソン接合の物理としても興味深い新たな未知現象が発見されるものと期待される．

4　研究成果：

（1）メサ型 IJJ 素子のスイッチング電流分布測定

本研究では，IJJ 素子を用いた位相量子ビットの構築に向けて，まず基本となるIJJの位相ダイナミクスを把握するためにゼロ電圧状態から有限電圧状態へのスイッチング電流分布測定を行った．その結果，IJJ 素子の振舞いは従来の JJ に比べてはるかに複雑なことが判明し，位相量子ビット構築への最初のステップとなる MQT 状態を従来より高温で実現させるには，IJJ の素子サイズや素子構造が非常に重要になることが明らかになった．以下では，本研究で得られた実験結果から IJJ の本質的特徴を述べると共に，より高温で MQT 状態を実現させるための素子条件を示す．

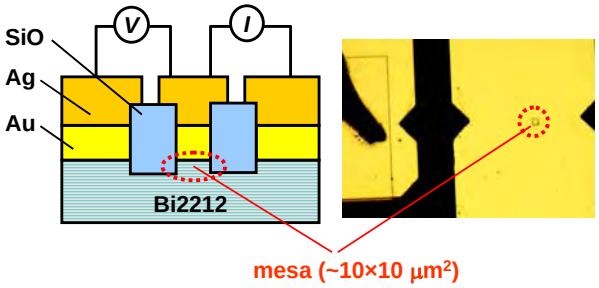


図 1　メサ型 IJJ 素子の素子構造（左）と光学顕微鏡写真（右）

測定には，非常に優れたIJJとして知られる高温超伝導体$Bi_2Sr_2CaCu_2O_y$単結晶を浮遊帯域溶融法で作製し，イオンミリング法を用いてメサ型構造（図 1）に微細加工した素子を用いた．図2にメサ型IJJ素子に対して測定された典型的なスイッチング電流分布を示す．メサ構造の作製には通常のフォトリソグラフィとArイオンミリングを用い，最小約 10 μm四方の接合面積と最小約 20 層の接合数にまで制御したメサ型IJJ素子の作製に成功した．

従来のJJの古典領域に対して用いられてきた熱活性的脱出モデル(以下，SJJモデルと略記)で図2(a)の実験結果を解析したところ，L=40 μm四方の接合サイズでは，SJJモデルは実験結果を全く説明できないことが判明した．詳細な解析の結果，これはIJJの起源が層状の結晶構造にあることに関連して，接合の特徴的長さスケールであるジョセフソン侵入長λ_Jが通常よりも著しく小さくなることに原因があることが分かった．つまり，図2(a)の素子サイズでは，従来のSJJモデルで仮定されていた位相の空間変化を無視できる「小さい接合($L<\lambda_J$)領域」の条件が満たされておらず，むしろ位相の空間変化が無視できずフラクソン励起（位相ソリトンの一種）が支配的となる「大きい接合($L>\lambda_J$)領域」に対応した脱出モデル(以下，LJJモデルと略記)を適用すべきであることが明らかになった．実際，図2(a)の測定結果をフラクソン励起を前提にしたLJJモデルで解析してみると、SJJモデルよりも定量的一致が良いことが示された．

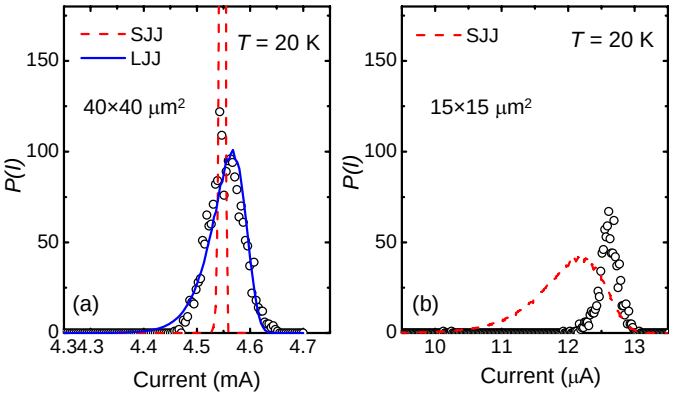


図2　メサ型IJJ素子のスイッチング電流分布
（a）40×40μm² (b) 15×15μm²

従来の人工的JJをベースに構築される現在の超伝導量子ビットでは，あらかじめ小さい接合として扱えるようなλ_Jの設計が可能である．しかしながら，IJJのλ_Jは物質定数であり，設計するには超伝導転移温度などの物質パラメーターを制御する必要がある．現状では，むしろ接合サイズLの方を設計して小さい接合領域を実現させることが重要である．このため，接合サイズの小さいL=15 μm四方のメサ型IJJ素子を作製し，スイッチング電流分布測定を行ったところ（図2(b)参照），予想に反して，SJJモデルよりもさらに分布幅が狭くなる実験結果を得た．これは上で述べた大きい接合の場合の振舞いとは全く逆である．通常，古典領域ではスイッチング電流の分布幅を決めるのは熱揺らぎであるため，測定温度から見積もられる分布幅より狭くなることはあり得ないと予想される．しかも，図3(a)に示すようにスイッチング電流の分布幅が温度減少と広がる振舞いは，通常の熱活性的脱出過程とは逆の振舞いであり，単一の熱活性的脱出過程を前提にしたSJJモデルやLJJモデルでは説明できない振舞いであることが明らかになっ

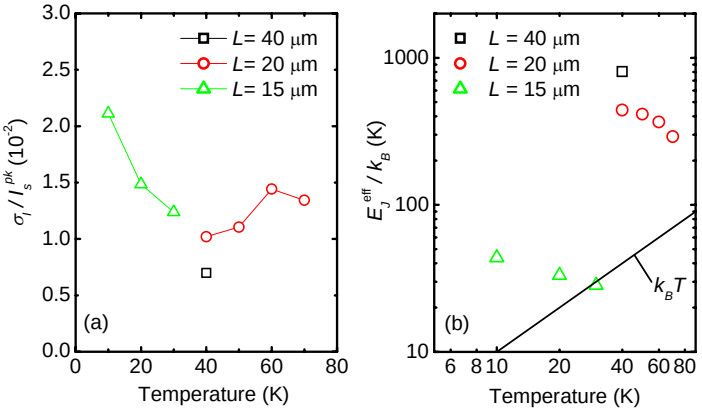


図3　(a)スイッチング電流分布幅の温度依存性
(b)実効的ジョセフソンエネルギーの温度依存性

た．こうした結果は，メサ型素子において接合サイズを小さくしても，直ちに従来のSJJモデルで説明されるような古典領域には至らず，したがってその低温側に存在するはずのMQT状態も観測が難しいことを示唆している．

この原因は，メサ型IJJ素子の実効的ジョセフソンエネルギーE_J^{eff}が接合サイズLの減少と共に急激に減少していることに起因することが分かった．ここでE_J^{eff}は，臨界電流I_cと接合サイズパラメーター$(\lambda_J/L)^2$に比例する量である．図3(b)に示すように，接合サイズをL=15 μmまで小さくすると，E_J^{eff}が温度のエネルギースケールk_BT程度と同程度になることが判明した．ごく最近，従来のJJでも図2(b)のような振舞いが$E_J^{eff} \lesssim k_BT$となる領域で観測されることが報告され，準安定状態であるゼロ電圧状態から脱出後に再び準安定状態に束縛される過程の影響が指摘された．このリトラッピング過程はSJJモデルやLJJモデルでは考慮されていない影響であり，L=15 μm四方のIJJ素子における異常な振舞いはE_J^{eff}減少に伴うリトラッピング過程の増大に起因するものと考えられる．接合サイズの減少に伴うE_J^{eff}の減少は，臨界電流密度$j_c(=I_c/L^2)$が接合サイズLに依存しない場合には生じない現象であり，何らかの理由でメサ型IJJ素子の臨界電流密度が接合サイズ減少と共に急激に劣化していることが明らかになった．

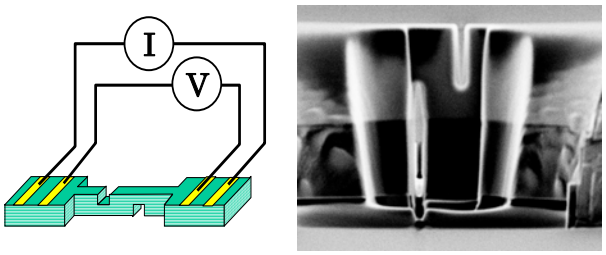


図 4　S 字型素子構造の模式図（左）と
走査型イオンビーム顕微鏡写真（右）

（2）S 字型 IJJ 素子のスイッチング電流分布測定

このような接合サイズ減少に伴う臨界電流密度の劣化は，素子構造に起因する可能性が高い．特にメサ型素子の場合には，メサ外周部のSiO絶縁層への漏れ電流やメサ上部電極からの準粒子注入の影響が懸念される．このため，本研究ではS字型構造（図4）のIJJ素子の作製にも着手した．この構造では，接合周辺部が真空のため漏れ電流の影響がなく，電極部が同じ超伝導体から形成されるため準粒子注入の影響も抑制できる利点がある．作製には，通常のイオンミリング装置よりさらに微細な加工ができる集束化イオンビーム(以下，FIBと略記)装置を用いた．図2に示したIJJ素子の接合サイズは約 0.9×0.8×0.09 μm^3であり，接合数は約 60 層と見積もられた．

図5にS字型IJJ素子に対するスイッチング電流の確率分布を示す．注目すべきは図3(b)に示したメサ型素子(15×15 μm^2)よりも接合面積が 1/200 以下になっているにも関わらず，スイッチング電流の大きさがほとんど変化していないことである．これはメサ型素子に比べてS

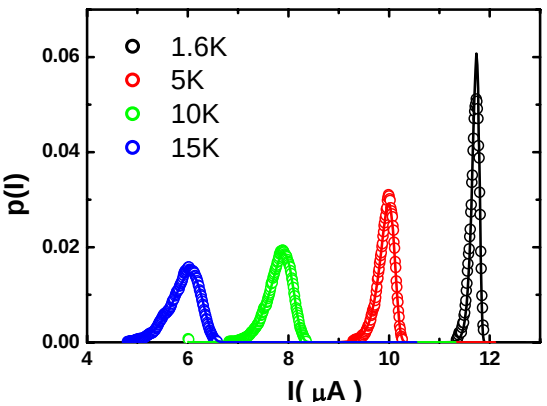


図5　S 字型 IJJ 素子のスイッチング電流分布確率．実線は SJJ モデルによるフィッティング結果．

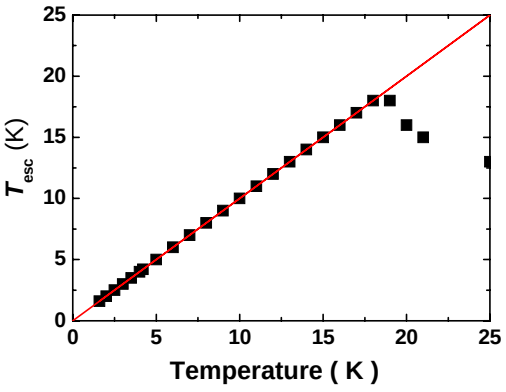


図6　S 字型 IJJ 素子のスイッチング確率から得られた脱出温度

字型素子のj_cが 2 桁以上向上していることを直接示している．また，図5の実線で示されるように，T=1.6 KからT=17 Kの温度範囲でスイッチング電流の確率分布はSJJモデルで定量的に説明できることが分かった．さらにSJJモデルとのフィッティングから得られる脱出温度T_{esc}はT=17 Kまで熱浴の温度とよく一致しており（図6），この領域では従来のJJで知られた小さい接合における古典領域とほぼ見なせることが明らかになった．

以上の研究から，高温超伝導体のIJJを用いて位相量子ビットを構築する場合の第一ステップであるMQT状態を実現するには，少なくとも以下の条件が必要であることが示された。即ち，(1) 接合サイズが 1 μm四方程度であること，(2) 臨界電流密度が 1kA/cm^{2}以上あること，の2つである．現在，T=1 K以下の極低温領域までスイッチング電流分布測定が可能な測定系を立ち上げ中であり，これによりMQT状態の直接観測が実際に可能になるものと期待される．

（3）超伝導共振器内の電磁場分布解析

超伝導共振器内の単一モード光子とIJJ 位相量子ビットを結合させて量子もつれ合い状態を作るには，両者の強結合条件が満たされなければならない．このため，本研究では様々な共振器構造に対して 3 次元電磁界解析シミュレーターによる電磁場分布解析を行い，共振器内の共振電場を空間的に一点に集中させて強結合条件を実現させる手段を検討してきた．その結果，図 7(a)に示す共振器構造が非常に有効なことが分かった．

この共振器は，円筒形のリエントラント型空洞共振器と類似の構造を持ち，共振器下部の金属ステージ上に IJJ 位相量子ビットとなる素子を設置し，共振器上部から伸びた金属探針を用いて共振電場を局所的に集中させる．実際に 3 次元電磁界解析シミュレーターを用いて共振器内に生じる共振電場の空間分布を調べたところ，金属探針の先端に共振電場が集中することが分かった（図7(b)参照）．

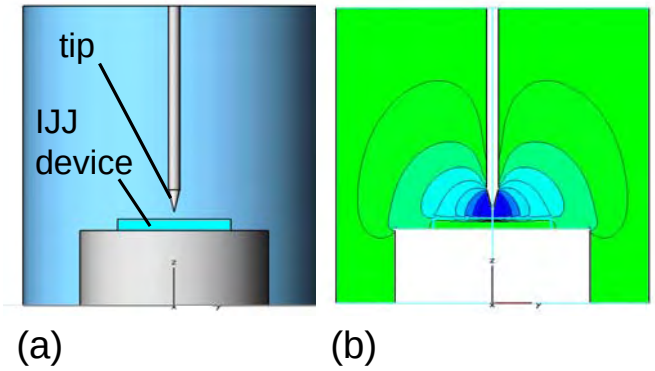


図7(a) 検討した超伝導共振器の模式図
(b) 電磁界解析から得られた共振電場の空間分布

金属探針により電界強度が増強される効果は，図8からも明らかである．この共振モードは，円筒の中心軸に平行な共振電場成分を持つため，IJJ 素子の接合面に垂直にマイクロ波電場を加えることが可能である．共振周波数に関しては，基本モードは円筒の直径や高さを調整することにより自由に設計できる他，高次モードの利用も可能なため，極低温用の測定インサートの先端に搭載しても 10 GHz から 100 GHz の周波数範囲を十分カバーできることが分かった．

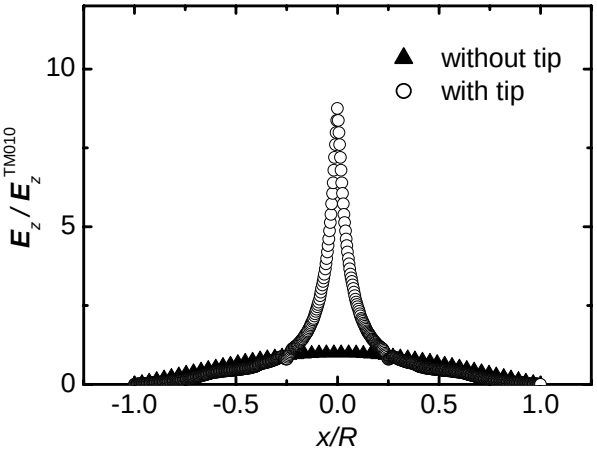


図8 電磁界解析から得られた電界虚度分布

図7に示す共振器構造では，金属探針を素子から 100 μm の距離にまで近づけることにより 1 光子当たりの電界強度を 100 mV/m 程度にまで強められることが数値解析から明らかになった．この値は従来の cavity-QED 実験で用いられた Nb 超伝導体のファブリ・ペロー型共振器に比べて 100 倍近い増倍であり，本研究開始後に報告されたコプラナー型ストリップライン共振器とジョセフソン電荷量子ビットによる cavity-QED 実験と同程度の電界強度である．したがって，本研究で得られた超伝導共振器構造が量子もつれ合い状態を生成するための cavity-QED 実験に十分適用可能なことが示された．

５ 自己評価：

本研究では，高温超伝導体のIJJを用いた位相量子ビットの構築に向けて，まず基本となるIJJの位相ダイナミクスを把握するためにゼロ電圧状態から有限電圧状態へのスイッチング電流分布測定を行った．その結果，IJJの位相ダイナミクスが当初予想していたよりもはるかに複雑なことが判明し，高温超伝導体の優位性を生かしてより高温でMQT状態を実現させるには，IJJの接合サイズや素子構造が非常に重要になることを見出した．具体的には，接合サイズが 1μm四方以下であること，臨界電流密度が 1kA/cm^{2}以上あること，の2つが必要条件であり，両者を満たす素子構造としてFIB加工によるS字型構造が優れていることが明らかになった．

本研究が目指した高温超伝導体を用いた量子ビットの実現は，まだ誰も成功していないが誰もが夢見る壮大な研究テーマである．本研究で独自に提案した IJJ を用いた位相量子ビットは，非常に挑戦的ではあっても最も実現可能性の高い量子ビット候補であると信ずる．本研究では，単結晶試料を微細加工して素子を作製するプロセスの構築や基本測定系の立ち上げから研究を開始し，約 3 年間で基本となる IJJ の位相ダイナミクスを把握し MQT 観測の一歩手前のところにまで辿り着いた．残念ながら，高温超伝導体の IJJ 素子における MQT の観測や ELQ の観測に関しては，S 字型構造から研究を始めた別の研究グループ（東北大通研と NIMS の共同グループ，独国 Erlangen 大グループ，産総研グループ）がつい最近報告してしまい一番乗りを逃してしまったが，本研究で得られた研究成果は彼らの観測結果とは相補的関係にあり，共に当初予想した高温超伝導体の IJJ の優位性を示す重要な研究成果であると見なせる．加えて，当初予想していなかった「大きい接合」領域でのフラクソン励起を利用した新しいフラクソン量子ビットの可能性を見出したという意味で，IJJ の新しい側面を切り拓く重要な研究成果も得られたと自負する．

本研究が目指したもう一つの研究テーマである cavity-QED の原理を利用した量子もつれ合い状態の生成に関しては，本研究の開始以前に超伝導量子ビットに適用した報告は一切なく，非常に画期的アイデアであったと自負している．本研究では，この cavity-QED 実験に適用可能な超伝導共振器構造を提案し，その電磁場分布を数値的に調べるに留まったが，本研究の開始後，別の研究グループ（Yale 大，Delft 工科大，NTT）から従来の人工的 JJ を用いた超伝導量子ビットと超伝導共振器を組み合わせた cavity-QED 実験が報告された．そこで用いられた超伝導共振器と本研究で提案したものを比べると，本研究で提案した構造の方が設計や制御性の自由度が高く，より高度な制御操作が可能である．特に本研究で示した超伝導共振器は，原理的に従来の人工的 JJ を用いた超伝導量子ビットにも十分適用可能である．したがって，今後は数値シミュレーションだけでなく，実際に超伝導共振器を作製し，その効果を実証していきたいと考えている．

６ 研究総括の見解：

固有ジョセフソン接合の研究において、北野晴久研究者はメサ型 IJJ 素子を作成し電流分布測定をし、「大きい接合領域でのフラクソン励起」という予想に反する結果を得、そこから高温超伝導物質について物理的に興味深い知見を得ました。その成果を高く評価します。

本来の研究目的のために、それをS字型に切り替えて MQT 状態の直接観測可能なところまで進めた研究推進力にも敬意を払います。高温超伝導量子ビットの可能性についての重要な成果と思いますので、今後の発展を期待します。

7 主な論文等:

論文 5 件

[1] H. Kitano, K. Ota, A. Maeda, "Study of switching events from zero-voltage state of Bi2212 intrinsic Josephson junctions", Supercond. Sci. Tech. **20**, S68-S73 (2007).

[2] K. Ota, H. Kitano, A. Maeda, "Escape rate from the zero-voltage state in the intrinsic Josephson junctions of $Bi_2Sr_2CaCu_2O_y$", Physica C **445-448**, 955-958 (2006).

[3] H. Kitano, K. Ota, A. Maeda, "Superconducting cavity resonator with a metallic tip for realizing strong coupling between superconducting qubits and microwave photons", American Institute of Physics Conference Proceedings **850,** 943-944 (2006).

[4] A. Maeda, H. Kitano, L. Gómez, T. Kubo, K. Ota, T. Ohashi, "High-Tc Josephson junction: towards improvement of IcRn product and realization of phase qubits", J. Phys. Conference Series **43**, 1151-1154 (2006).

[5] H. Kitano, K. Ota, A. Maeda, "Switching current distribution in large $Bi_2Sr_2CaCu_2O_y$ intrinsic Josephson junctions", Physica C, accepted for publication.

特許 なし

受賞 1 件

Nano-Virtual-Labs Joint Workshop on Superconductivity (NVLS2005) ベストポスター賞 (H17.12)

招待講演 なし

研究課題別評価

1　研究課題名：単一量子ドットにおける多光子量子操作

2　研究者氏名：黒田　隆

3　研究のねらい：

近年の結晶成長技術の進展により、10ナノメートル程度の微小な半導体結晶を作製することが可能となってきた。微結晶の大きさは、原子数にして 10^3個程度に相当する。このような微結晶を、異種の半導体中に、エピタキシャルに（結晶格子の切れ目なしに）埋め込むことにより、結晶の表面やその内部に格子欠陥が存在しない、高品質のナノ結晶（量子ドット）が実現できる。

量子ドット内部の伝導電子は、ナノメートル・スケールの微小空間に閉じ込められる結果、顕著な量子性を示す。例えば、バルク結晶で見られていたバンド的な電子構造は、量子ドットにおいては、原子の量子準位と似た離散的な線スペクトルになる。また、固体中の電子は、一般に、価電子や原子核など他自由度からのランダムな擾乱を受け、純粋な量子状態は極めて短時間に消失するが、量子ドットにおいては、システムのサイズダウンの結果、電子状態と相互作用する自由度が劇的に少なくなり、結果として量子状態が乱れることなく長時間に渡って保たれる。半導体量子ドットは、固体でありながら、真空中に孤立して置かれた原子に類した系であり、人工原子とも呼称する。顕著な量子性が長く保たれる特性は、固体の量子計算を実現するために理想的な対象といえる。

量子ドットを用いて量子ビットを構成する方法には、量子ドット内の伝導電子の有無を量子ビット準位に用いるもの、伝導電子のスピン準位を用いるもの、および、光学遷移である励起子を用いるものなどが知られている。それぞれ長所と短所があるが、本研究で着目する励起子を用いる方法は、光学手法を用いるため非接触的に量子ビットにアクセスでき、実験の構成が比較的簡単になること、超短パルスレーザーを用いるために高速のゲート処理が実現できること、量子通信など光ネットワークとの相性がいいこと、などの優位点がある。他方、欠点としては、量子ビットの寿命が、励起子の自然放出寿命で制限されることがある。広く用いられている III-V 族の半導体では、励起子寿命は100ピコ秒～1ナノ秒であり、全ての量子演算はこの時間内に終わらねばならない。この欠点は、しかしながら、先述のように毎ステップ1ピコ秒程度の高速処理が可能であことを考慮すれば、幾分緩和できる。これらの特徴から、励起子量子ビットは、大規模かつ長大な演算処理には不向きであるが、量子中継器など高速かつ小規模な量子情報処理ユニットに活用できると考えられる。

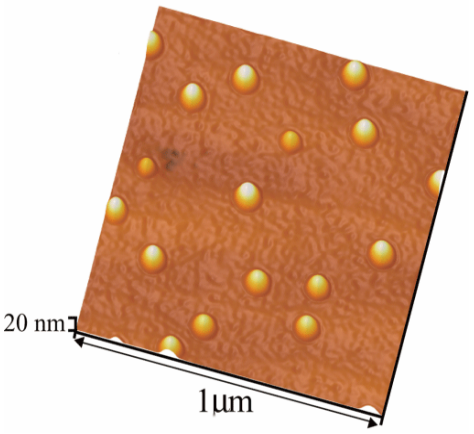


図 1　GaAs 量子ドットの原子間力顕微鏡写真

量子ドットの励起子を量子ビットに適用する試みは、プロジェクトの開始時点において既に、ラビ振動の観測（2001 年）、制御付量子ゲートの実験（2002 年）など報告があった。これらの先行実験では、励起子の量子ビット的な性質を、非線形光学手法や変調分光など、量子情報処理としては、やや冗長な手段を駆使して、ようやく検証に至っている。実験の困難さのために、残念ながら後続する研究例は多くはない。

本研究では、優れた性質を持つ励起子量子ビットを、実用に使える程度のレベルまでに展開することを目的とした。鍵となるのは、将来的にはシングル・ショット検知も可能な、高効率の読み出し手法を開発することである。そのため、自然放出をベースとした新しい読み出し手法を提

案した。また、条件付き量子ゲートを構成する空間的に近接した量子ドット複合体を作製し、その結合した電子準位を確証することに成功した。

4　研究成果：

【励起子量子ビットの読み出し手法の開発】

量子計算では、アルゴリズムに則って量子ゲートを施し、その後、個々の量子ビットの状態を演算結果として読み出す。励起子量子ビットの場合、量子ビットを担う2準位は、量子ドット内に励起子が「ある」状態と「ない」状態である。個々の量子ドットに対して、適切な波長、強度、位相に定めた光パルスの列で、多段的に量子遷移を引き起こし、最終的に励起子が存在するか、消えているかを、個々の量子ドットにおいて観測する。一般に、一個の量子ビットからの応答は極微なものであり、終状態の読み出しには、ごく高感度な計測が要求される。

励起子の有無を決める、最も直接的な方法は、自然放出光を検知することである。励起子が存在する場合に限り、再結合に伴って光子が放出される。従って、その光子を検知できれば、状態操作後の励起子の存在を確定できることになる（図3）。現在、光子用の検出器には、100%に近い効率のものが手に入る。そのため、この手法は、原理的にはシングル・ショットの状態検知も可能な、理想的な読み出し手法とみなすことが出来る。

しかし、実際に量子ドットからの自然放出を検出しようとすると、微弱な発光信号は、ゲート操作に用いた入射光に埋もれてしまい、判別できない場合が多い。1個の量子ドットの吸収断面積はごく小さく、量子遷移の操作には莫大な数の光子の照射が必要となる。対する発光信号は、1対の電子・正孔の再結合で生み出される1個の光子に過ぎず、波長が等しいこともあって、両者を分別することは不可能だと信じられていた。

我々は、このような一般認識を逆手にとり、入射ゲート光のもれ成分を丁寧に取り除くことで、単一の量子ドットからの自然放出光を観測することを試みた。基本的なアイデアは、広く用いられている共焦点的な顕微鏡配置を崩し、平面波的なゲート光を照射後、励起光とは異なるモード（伝搬方向）の自然放出を観測することである。そのため、量子ドット試料には、斜め方向から平面波に近い励起パルスを照射した。単一の量子ドットを共鳴的に励起し、その後の発光を対物レンズで捕集する。さらに、試料表面からの弾性散乱と共鳴的な信号を分別するため、時間分解計測を行った。

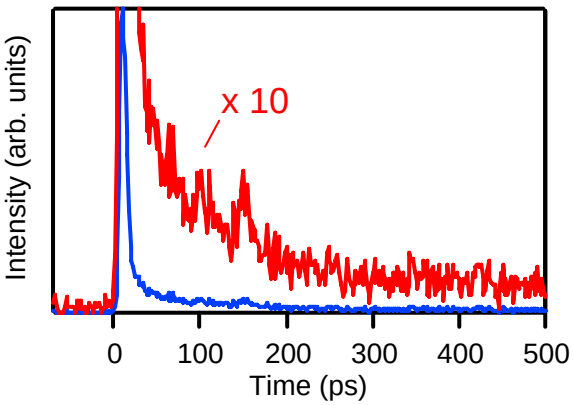


図2　単一量子ドットにおける共鳴パルス励起後の発光の時間発展。

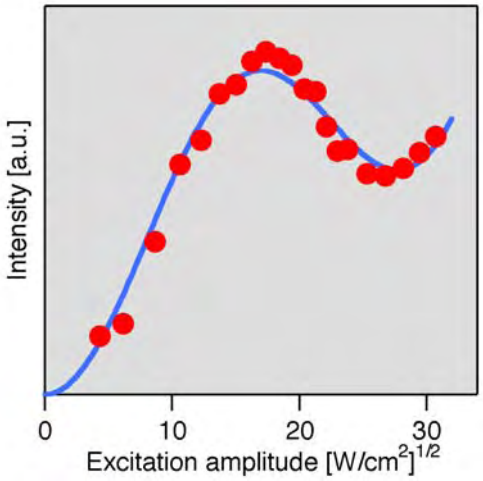


図3　共鳴励起後の発光信号の励起強度依存性。振動的な依存性は励起子のラビ振動を反映している。

図2は、単一の量子ドットを共鳴的にパルス励起し、その後の光放出信号を時間分解計測したものである。時刻0に現れるスパイク的な信号は、励起光の弾性散乱信号である。これに引き続き、単一量子ドットの自然放出に由来する減衰信号を、初めて観測することに成功した。

この実験では 10^9回もの試行を繰り返し、その結果を足し合わせて、自然放出の減衰曲線を

見出した。実際の量子計算では、放出寿命内に光子が検知できるかのみを確認すればよい。高効率の光子検出器と、光子の取り出し効率を高めた試料デザインを採用すれば、シングルショットに近い状況での状態読み出しが、今後可能になると考えている。

この読み出し手法を用いて、1量子ビットの回転ゲート操作であるラビ振動を見た結果が、図3である。光パルスを用いてラビ振動見出す場合、コヒーレントな相互作用の大きさ(パルス面積)を変えるために、励起パルスの入射強度を変化する。図3は、自然放出の信号強度を、励起強度の関数として図示したものである。振動的な依存性は、パルス励起後の量子状態が、基底状態と励起状態の間を往来していることを示しており、確かに回転ゲートが実現したことを確証づけた。

【励起子デコヒーレンス時間の評価】

固体凝縮系の電子状態のデコヒーレンスは、原子分光で知られたスペクトル衝突広がりとの類推で、他自由度や擬粒子との衝突過程として考えることが多い。しかしながら量子ドット内部に閉じ込められた電子は、空間的に局在した状態であり、衝突によるコヒーレンス破壊といった素朴な描像が立ちにくく、デコヒーレンス機構については未解明な部分が多い。この背景には、デコヒーレンス時間を決定する有力な方法がなく、実験研究が捗っていないことがある。

量子準位のデコヒーレンス時間は遷移スペクトルの線幅の逆数で与えられる。従って、1個の量子ドット発光線のスペクトル線幅が決定できれば、本来十分であるが、多くの場合、発光線幅は通常の分光装置の分解能以下であり、その決定には困難を極めていた。

そこで我々は、量子ドット発光の自己相関を観測することにより、分光器を用いることなく高分解に線幅を決めることを試みた。実験では、単一の量子ドットからの発光信号を、マイケルソン型の干渉計に導入し、可干渉度を測定する。一般のフーリエ分光とは異なり、毎秒数フォトン程度の微弱な信号を長時間積算するため、干渉計の内部には位相関係を保持するフィードバック機構を組み込んだ。

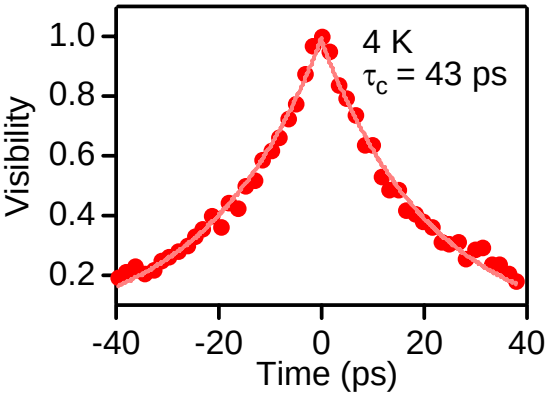


図4. 単一量子ドット発光信号の自己相関関数。

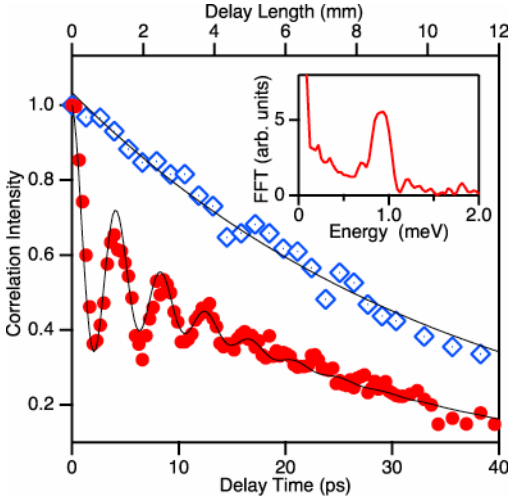


図5. 励起強度が 4 W/cm^2(青)と 40 W/cm^2(赤)での自己相関関数。

光学遅延を関数とした可干渉度が自己相関関数であり、そのフーリエ変換がスペクトル(線幅)を与える。結果を図4に示す。代表的な量子ドットにおいて、デコヒーレンス時間は 40 ps、線幅にして 30 meV と決定できた。相関関数は温度によらず、単一指数減衰を示す。またデコヒーレンス時間は検出する量子ドットによって著しく異なっており、統計的には6割程度の分散を持つことがわかった。この結果は、量子ドットのデコヒーレンスが、局所的な環境に強く依存することを示している。

図5は、異なる励起強度における自己相関関数の変化の様子を示す。弱励起時(青)には指数関数的な単調減少だったものが、強励起時(赤)には振動成分が重畳していることがわかる。この時、量子ドットには2個の励起子の複合体である励起子分子が形成される。励起子分子と

1励起子は、電子間相関の分、遷移エネルギーが異なる。両者の発光波長の違いを反映して、自己相関関数にうなりが生じる。うなりのフーリエ解析から、励起子分子の結合エネルギーやデコヒーレンス時間を評価することができる。

【量子ドット複合体の創生と光学評価】

1つの量子ビットは、1つの量子ドットで実現できる。多量子ビットを構成するには、複数の量子ドットを準備し、量子ビット間に相互作用を持つようにすればよい。例えば、量子ドットのペアを、波動関数の浸みだし程度の、ごく近傍に置くことが出来れば、制御ゲート(条件付ゲート)が実現できる。図6には、近接した量子ドット対における制御ゲートの概念図を示した。2つの量子ドットは、励起光の波長や偏光の違いを用いて、個別のアクセスが可能である。各々の量子ドットの遷移エネルギーは、電子相関の結果、相手方の量子ドットの状態(励起子の有無)に応じて僅かに異なる。そのため、励起光の波長を適切に設定することで、相手方の状態に応じて、もう片方の状態のみを制御すること(条件付きゲート)が可能となる。

自己形成的に作製する半導体量子ドットは、結晶学的には極めて高品質であるが、形状制御や配置制御は困難である。特に量子ドットの配列化は、ナノテク分野のフロンティア領域の一つであるが、現状では、分光探査に要求される高品質の試料は実現していない。

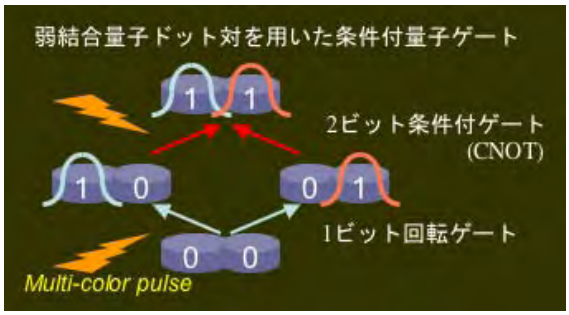
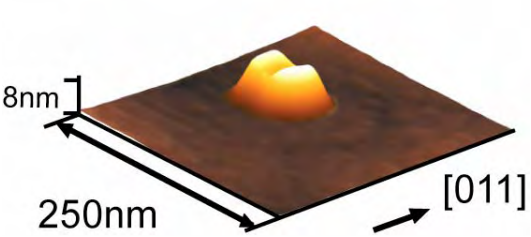


図6. 近接しておかれた量子ドット対を用いる2量子ビット条件付きゲート。



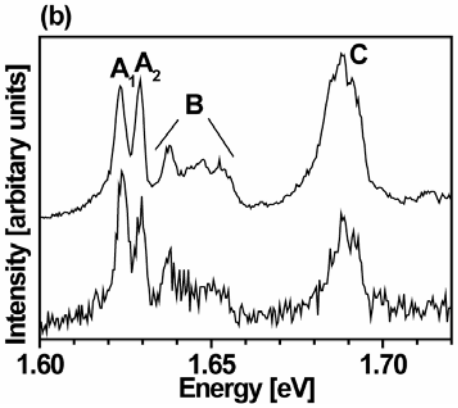


図7. 自己形成的に作製した量子ドット分子の原子間力顕微鏡写真(上)と光学遷移スペクトル(下)。

我々は、液滴エピタキシー手法に特有な、自己形成的に作製できる複合的な量子ドット構造に着目し、これらの成長過程の観測および光学評価を進めた。

図7には、試料面内方向に分割して形成した量子ドットの例を示す。面内の［011］方向と［0−11］方向では、結晶成長時における吸着原子の拡散速度がわずかに異なる。この異方性が大きくなるような条件に設定することにより、面内に分割した量子ドット対を作製することができた。下段には、分割量子ドットからの発光スペクトルを示している。比較的再現性よく、発光線(図の A1, A2)の対が見出され、これは、分子軌道的な結合状態、反結合状態からの発光と考えられる。スペクトル分裂の大きさは数値シミュレーションの結果ともよく合致していた。

5 自己評価:

プロジェクト申請段階で、1)高効率の励起子量子ビットの読み出し手法を確立し、2)2〜3量子ビット程度の量子ゲート操作を実現することを目標に掲げていた。1)は完遂できたものの、2)は手つかずの状況である。この理由は、申請時のプランニングにおける読みの甘さもあるが、

期間中に、量子ドット複合構造が新たに見出されたことなど、当初予定になかった発展があったからである。現在、2量子ビット系の準備も整った状況なので、今後、多波長・多パルスの励起レーザー光を用いた、条件付き量子ゲートの実証実験に着手する。また同時測定計測により、量子もつれの大きさを定量評価したいと考えている。

さきがけ研究では、励起子量子計算のための要素技術を、単純明快に探求してきた。固体量子情報のトレンドを見てみると、それぞれの分野・それぞれの量子ビットで、量子性をフルに取り扱う洗練した方策が探求されてきたと思う。極限技術の開発は、それ自身で面白い研究対象であるが、他方、ブレークスルーのためには、近未来、複雑にもつれ合う量子情報ネットワークの中で、個々の技術に望まれる要求仕様を、確かに見定めることが不可欠であると思う。今後も他分野の動向を踏まえつつ、自身の研究を展開していきたい。

6 研究総括の見解:

物理的に単純明快なやりかたで、

（1）単一量子ドットの自然放射の減衰信号を初めて観測

（2）そのラビ振動

（3）励起子コヒーレンス時間の評価

を実験的に実証した点を高く評価します。

単一量子ドットによる量子計算素子の研究に関して大きな成果をあげたと思います。量子ドット複合構造があらたに見いだされたこともあり、今後の2ビットの量子ゲートの実証実験に期待します。

7 主な論文等:

【論文】 11 件

[1] T. Kuroda, T. Mano, T. Ochiai, S. Sanguinetti, K. Sakoda, G. Kido, N. Koguchi: Optical transitions in quantum ring complexes; Phys. Rev. B 72, 205301 (2005); cond-mat/0509625.

[2] K. Kuroda, T. Kuroda, K. Sakoda, K. Watanabe, N. Koguchi, G. Kido: Excitonic and biexcitonic decoherence in self-assembled GaAs quantum dots as observed by phase-locked interferography; Appl. Phys. Lett. 88, 124101 (2006).

[3] M. Yamagiwa, T. Mano, T. Kuroda, T. Tateno, K. Sakoda, G. Kido, N. Koguchi, F. Minami: Self-assembly of laterally aligned GaAs quantum dot pairs; Appl. Phys. Lett. 89, 113115 (2006); cond-mat/0607549.

[4] T. Kuroda, T. Mano, T. Ochiai, S. Sanguinetti, T. Noda, K. Kuroda, K. Sakoda, G. Kido, N. Koguchi: Excitonic transitions in semiconductor concentric quantum double rings; Physica E, 32, pp. 46-48 (2006).

[5] K. Kuroda, T. Kuroda, K. Watanabe, T. Mano, K. Sakoda, G. Kido, N. Koguchi: Final-state read-out of exciton qubits by observing resonantly excited photoluminescence in quantum dots; Appl. Phys. Lett. in press; cond-mat/0612629.

【特許】 1 件

・特願 2004-127226(平成16年4月22日)

黒田隆、黒田圭司、迫田和彰、木戸義勇「レーリー散乱光除去方法及びその装置」

【受賞】 なし

【招待講演】 なし

【解説】 1 件

黒田圭司，黒田隆，迫田和彰，小口信行，木戸義勇

GaAs 量子ドット励起子の単一光子フーリエ分光
固体物理, Vol.41, No.12, 919(2006).

【プレス発表】 1 件
・物質・材料研究機構・JST 共同プレス発表(2006 年 3 月 17 日)
「量子コンピュータ素子の性能評価に世界で初めて成功」(日刊工業新聞、日経産業新聞)

研究課題別評価

1　研究課題名：多体量子系としての量子計算機の分析

2　研究者氏名：清水　明

3　研究のねらい：

量子計算機と古典計算機の性能の差が顕著に出るのは、大きなデータを扱うときであるから [1]、意味のある量子計算機には多くの量子状態が必要である。これを実現するための物理系は、原理的には多準位の1自由度系（たとえば1個の水素原子）でも構わないのだが、様々な要素を勘案すると、少数の準位を持つ系（たとえば2準位系＝キュービット）が空間的に広がって配置されている系を想定するのが自然である。つまり、量子計算機の物理的実態は、多体量子系と考えるのが自然である。

量子計算機にはエンタングルメントが現れるが、上記のような多体量子系のエンタングルメントは、量子情報理論で言うところの「多地点のエンタングルメント」になるので、「2地点のエンタングルメント」とは違って、無数の種類がある。その中のどんな種類のエンタングルメントが、量子計算機の（古典計算機に比べての）スピードアップに本質的な役割を演じているのかはよくわかっていない。

この基本的な問題に対して、筆者は次のような予想を発表した（正確な表現は[9]に記した）[2]：ある計算問題を古典計算機よりもずっと速く解くような量子計算機は、マクロに異なる状態たちの重ね合わせ（これを筆者はマクロにエンタングルした状態と呼んでいる）を計算の途中に使うのであろう。そしてそれが量子計算機のスピードアップに本質的な役割を演じているのであろう。

本研究の目的は、この予想の真偽を調べて上記の基本的な問いかけに解答を与えることと、多体量子系のマクロエンタングルメントの物理を明らかにすることにある。そもそも、「マクロに異なる状態たちの重ね合わせ」という概念自体が曖昧なものであったが、これについてもきちんとした定義を与え、その物理を調べる。

4　研究成果：

多体量子系の「マクロに異なる状態たちの重ね合わせ」を最初に問題にしたのは、シュレディンガーであった [3]。それ以来このような状態は多くの人々の興味を引き、今日までずっと研究が続いている。最初のうちは、現実の物理とは結びつきにくいような議論がなされることも少なくなかったが、1980 年前後から、A. J. Leggett の有名な Leggett プログラム[4] のように、現実の物理の問題として論じられるようになってきた。しかしながら、「マクロに異なる状態たちの重ね合わせ」の定義からして曖昧なものであり、それを明確化しようとして Leggett が導入した disconnectivity という量も（Leggett 自身も述べているように）不定性の大きな曖昧な量になってしまっていた。また、「そのような状態はノイズにより極めて速くデコヒアーするであろう」という予想をきちんと示そうという仕事も多くのグループ（例えば Zurek ら）により試みられ、確かにそれを示したと主張されたが、実際には少数自由度系のモデルを採用したために、環境との相互作用のモデルを取り替えると答えが簡単に変わってしまうような有様だった。それでは何も示せていないし、後述のように、実はこの予想は一般には正しくない。

そこで筆者らは、本研究課題が採択される前に、まず次のような内容の一般論を構築した[5]：

(i) 多体量子系の純粋状態について、「マクロに異なる状態たちの重ね合わせ」を曖昧さなく定義し、そのような状態（「マクロにエンタングルした状態」と呼んだ）を p=2 として示す指標 p (1 ≦ p ≦ 2)を導入した。

(ii) p=1 の状態のデコヒーレンス・レートは、決して異常に大きくなることがないことを、環境との相互作用のモデルの詳細に依らずに一般的に示した。

(iii) p=2 の状態のデコヒーレンス・レートは、環境の性質に依存して、異常に大きくなることも

あればそうでないこともある（マクロにエンタングルした状態は、ノイズに対して格別に不安定というわけでは、必ずしもない）。
(iv) しかし、p=2 の状態は、適当な局所的な測定に対しては不安定である（状態を大きく変えるような局所測定が常に存在する）。
これは一般論であるから、様々な多体量子系に応用できる。そこで、量子計算機への応用として、上述の予想を発表した。そして、この予想の真偽を調べる第一段階として、Shor の因数分解アルゴリズムにおいて確かにこの予想が真であることを確かめることができた [6]。

しかしながら、次のような多くの課題が残っていた：

1. 因数分解はいわゆる構造のある問題 [1]であるが、構造のない問題を解くときにも予想は真なのか。
2. 文献[6]の段階では、一般の純粋状態について指標 p を計算する方法が見つかっていなかったために、手探りで調べて、計算ステップの中の2カ所について、マクロにエンタングルした状態が現れることを示しただけだった。他のステップではどうなっているのか。
3. p という指標は、純粋状態にしか使えない。一般の状態（混合状態）ではどのような指標を用いればよいのか。
4. マクロにエンタングルした状態を実験的に検出するには何を測ればよいのか。
5. 量子計算機以外の多体量子系には、マクロにエンタングルした状態は、いつどのようなときに現れるのか。

そこで本研究課題では、次のような方法でこれらの課題を克服していった。まず、一般の純粋状態について指標 p を計算する方法を開発した。大きな自由度の多体量子系にこの方法を適用するには大量のメモリーを積んだ高速の計算機が必要となるので、それを何台か購入し、数値計算を実行した。また、特殊な場合には手計算でも p が計算できる場合があるので、その場合は手計算を行った。これにより、1，2，5の研究を遂行することができた。また、様々なアイデアを試行錯誤し、時には数値計算の結果を参照することにより、遂に3，4も大きな成果が得られた。

まず、一般の（実効的に並進対称な）純粋状態について指標 p を計算する方法を開発し、Variance-Covariance Method (VCM)と名付けた [7]。そして、この方法をまず、強磁性体にマグノンがマクロに励起された状態に適用し、以下のことを示した [7]：
(i) 同じ濃度のマグノンを励起しても、どんな一体状態たちに励起するかで、p の値は大きく変わる。
(ii) 2地点エンタングルメントが最大なのにマクロエンタングルメントがない状態とか、2地点エンタングルメントが小さいのにマクロエンタングルメントがある状態が見つかった。つまり、エンタングルメントの大小は、どんな種類のエンタングルメントを見るかで全く異なる。

次に、多体の量子カオス系のエネルギー固有状態の p を計算した [8]。それまでは、量子カオス状態はエンタングルメントが大きくてノイズに対して脆弱であろうと想像されていたが、そうではないことが判った。即ち、2地点エンタングルメントは最大に近いがマクロエンタングルメントはなく、従って文献 [5]の一般論（上記）から、ノイズに対して格別に脆弱ということはあり得ないことが判った。また、多地点相関についても多くのことが判った。

続いて、量子計算機の p を計算した [9]。構造のある問題の代表としては Shor の因数分解アルゴリズムを、構造のない問題の代表としては Grover の量子探索アルゴリズムを選んだ。その結果、どちらについても我々の予想が真であることが判った。また、両アルゴリズムについて、各ステップにおいてどんな物理量がマクロに揺らいでいるか（p=2 をもたらすか）を明らかにした。今までに、量子計算のスピードアップのためには、2地点エンタングルメントも十分な量だけ必要であることが示されていたが、それは必要条件ではなく、十分条件である。p=2 の状態を使うことも、必要条件であって十分条件ではない。これらを含む必要条件をいくつも明らかにしてゆくことによって、やがては、必要十分条件に近いものが知れるようになると期待できる。

さらに、（実効的に並進対称な）混合状態について、それがマクロにエンタングルしているか（マクロに異なる重ね合わせ状態を含んでいると言えるか）否かを判定する新しい指標 q を

提案し、それがきわめて自然な指標になっていることを示した [10]。(定義するだけなら何でもいいわけだから、自然な指標になっていることが重要)これにより、
(i) 量子計算機の解析に少しでも現実味を加味すると混合状態になってしまうが、それがマクロにエンタングルしているかどうかが判定できるようになった。
(ii) マクロにエンタングルした状態を実験的に検出するには何を測ればよいのかが明らかになった。
(iii) 純粋状態の指標 p は2局所点相関の総和だが、なぜ2局所点相関で全体のエンタングルメントについて強いことが言えたのかが明らかになった。つまり、q の方は多局所点相関であるから全体のエンタングルメントについて強いことが言えるが、実は、純粋状態に限れば p=2 が q=2 を意味することが判り、「純粋状態である」という情報があれば、2局所点相関から多局所点相関について強いことが言えたのであった。

そして、この成果をすぐさま量子計算機に応用した。量子計算機の実装法として、一方向量子計算という実装法が有力視されているが、その場合にもマクロにエンタングルした状態が現れるかどうかは、混合状態のマクロエンタングルメントを調べる必要があった。それは上記の q で調べられる。そうして調べて見たところ、やはりマクロにエンタングルした状態が、今度は混合状態として、現れることが判った [11]。

また、今までに述べたような系に現れる「マクロにエンタングルした状態」というのは、いわゆる「シュレディンガーの猫状態」のような単純な状態ではなく、非常に多くのマクロに異なる状態の重ね合わせになっていることが多い。それを判りやすく可視化する方法が望まれる。そこで、測定の解像度を落とせば非可換な物理量も同時確率分布を持つようになることに着眼し、可視化する方法を開発した [12]。それによって Grover の量子探索アルゴリズムの途中に現れる状態を可視化したものを下図に示す。

さらに、量子計算機ではなく、短距離相互作用しかもたない自然なハミルトニアンによる時間発展で、多項式時間でマクロにエンタングルした状態がつくれるかどうかを調べ、それが可能であることをい示した [13]。

また、量子情報理論においては測定理論が重要な役割を演じることが多いが、量子ゼノ効果という測定理論の典型的な舞台に、現代的な測定理論を適用し、従来の安易な測定理論の結論とは全く違う結論が得られることを示した [14]。これに関連する仕事は、権威ある総合報告誌である Physics Reports 誌の招待総合報告になった [15]。特に、この総合報告の第 4 節は、量子ゼノ効果に限定しない、現代的な測定理論の総合報告になっているので、これから現代的な測定理論を研究に使う人にとっても役立つのではないかと思う。

以上についての参考文献:

[1] M.A. Nielsen and I.L. Chuang, Quantum Computation and Quantum Information (Cambridge University Press, 2000).
[2] 清水明, 第4回量子効果等の物理現象シンポジウム (December 20-21, 2000, Tokyo) 口頭発表; 清水明, 第 56 回日本物理学会(2001) 28pYN-6.
[3] E. Schroedinger, Naturwissenschaften 23 (1935) 807, 823, 844.
[4] 高木伸「巨視的トンネル現象」(岩波書店)など。
[5] A. Shimizu and T. Miyadera, Phys. Rev. Lett. 89 (2002) 270403.
[6] A. Ukena and A. Shimizu, Phys. Rev. A 69, 022301 (2004).
[7] T. Morimae, A. Sugita and A. Shimizu, Phys. Rev. A 71 (2005) 032317.
[8] A. Sugita and A. Shimizu, J. Phys. Soc. Jpn. 74 (2005) 1883.
[9] A. Ukena and A. Shimizu, quant-ph/0505057.
[10] A. Shimizu and T. Morimae, Phys. Rev. Lett. 95 (2005) 090401.
[11] Y. Matsuzaki and A. Shimizu, in preparation.
[12] T. Morimae and A. Shimizu, Phys. Rev. A 74 (2006) 052111.
[13] T. Morimae and A. Shimizu, in preparation.
[14] K. Koshino and A. Shimizu, Phys. Rev. Lett. 92 (2004) 030401.

[15] K. Koshino and A. Shimizu, Physics Reports 412 (2005) 191–275.
[16] A. Shimizu, Statistical Physics (eds. M. Tokuyama and H. E. Stanley, American Institute of Physics, 2000), 611–620.

５ 自己評価：

研究成果の中には、発足時の目標を達成した部分と、発足時にはなかった新たな研究課題が浮かび上がってきてそれをクリアーした部分もある。

まず達成した部分であるが、「量子計算のスピードアップにはマクロに異なる重ね合わせ(マクロエンタングルメント)を使うことが必要ではないか」という予想について、それが正しいことを強く示唆する結果が得られた。他のグループも別の必要条件を得ているが、それらは2地点エンタングルメントに関するものであり、我々のマクロエンタングルメントとは質的に全く異なるものである。異なる必要条件たちの共通部分が、より強い（核心に迫る）必要条件であるから、他のグループとは質的に全く異なる必要条件を得ることができたことは、大きな成果だと考えている。

また、量子計算中に現れる状態のマクロエンタングルメントの特徴を抽出する系統的な手法であるVariance-Covariance Methodを発見でき、それによって状態の特徴付けが出来た。A. Shimizu and T. Miyadera, Phys. Rev. Lett. 89 (2002) 270403により、この特徴付けがそのまま、「どの状態がどんなノイズに弱いか」という問いかけの答えになっている。しかし、そこから何かもう一歩進んだことが言えたかというと、それはできなかったので、それが不満点である。

一方、発足時にはなかった新たな研究課題については、混合状態へのマクロエンタングルメントの拡張をはじめ、予想よりも大きな成果を得ることができた。

以上を総合すると、十分な成果を得ることができたと言って良いと思う。

６ 研究総括の見解：

大きな量子計算の速さに、「マクロにエンタングルした状態」が重要な役割をすると予想してはじめ、ほぼそれを実証した研究です。量子多体系との類推から、その判定をする指標を導入しシミュレーションを含む具体的に説得力ある議論を展開しました。

一般的な証明までには至っていませんが、量子計算の速さを理解するための重要な知見であると考えます。何よりも、この研究の基本的なアイデアが日本発である点を高く評価します。この日本発の研究を勇気を持って採択したことは成功だったと思います。

７ 主な論文等：

論文：7件

A. Shimizu and T. Morimae, Detection of Macroscopic Entanglement by Correlation of Local Observables, Phys. Rev. Lett. 95 (2005) 090401.

K. Koshino and A. Shimizu, Quantum Zeno Effect by General Measurements, Physics Reports 412 (2005) 191–275 (invited review paper).

A. Sugita and A. Shimizu, Correlations of observables in chaotic states of macroscopic quantum systems, J. Phys. Soc. Jpn. 74 (2005) 1883.

T. Morimae and A. Shimizu, Visualization of superposition of macroscopically distinct states, Phys. Rev. A 74 (2006) 052111.

K. Koshino and A. Shimizu, Quantum Zeno Effect for Exponentially Decaying Systems, Phys. Rev. Lett. 92 (2004) 030401.

特許:なし

受賞:なし

招待講演:2 件

Akira Shimizu, Quantum Zeno effect by general measurements, 36th Winter Colloquium on The Physics of Quantum Electronics (Snowbird, Utah, USA, January 2-6, 2006).

Akira Shimizu, マクロにエンタングルした状態 s, International Conference on Quantum Information -- mathematical, physical engineering and industrial aspects (Tokyo, 1-3, November, 2003).

研究課題別評価

1　研究課題名：量子鍵を用いた次世代量子暗号プロトコル

2　研究者氏名：村尾　美緒

3　研究のねらい：

量子鍵配布に代表される従来の量子暗号のプロトコルは、量子状態を用いることで古典情報の安全な通信を可能とするものであった。一方、量子情報科学技術が進めば、量子情報そのものの安全な通信のために「量子情報のための暗号」が必要となる。そこで、量子情報を主体とした次世代の量子情報処理への手がかりとして、量子力学特有の性質である量子もつれの性質を解明し、その性質を量子情報のための暗号鍵（量子鍵）へと応用した、次世代の量子暗号プロトコルを探索する。

本研究は暗号プロトコルの提案という量子情報処理の応用研究的な側面を持つと共に、量子もつれを中心とした、量子力学的な非局所性と情報処理との関連の解明という基礎研究的な側面も持つ。基礎研究と応用研究との相互的発展によって、量子情報を用いることで何ができ何はできないのか、量子情報の優位性を保つためには何が必要なのか、という理論的基盤の構築に貢献を目指すものである。

4　研究成果：

4．1　基礎研究の成果

遠隔操作量子情報抽出と遠隔操作量子情報破壊

多量子ビット量子もつれを用いて2量子ビットに符号化した1量子ビットの量子情報が、LOCCのみで量子情報の抽出が可能であるための必要十分条件を、作用素代数的な方法を用いて求めた。この条件を用いて、どちらか一方には LOCC のみで量子情報を抽出することができるが他方には抽出できない、というような量子情報の二者間での非対称な共有方法（遠隔操作量子情報集約）を見出すことに成功した。

量子情報の共有には、量子もつれを持つ純粋状態を符号化の基底として用いており、どのような性質の量子もつれ状態を基底として用いるか、ということが、量子状態の共有の性質を決める。純粋状態の場合、2者間の量子もつれ自体は2者間に対称的に存在することが知られており、この類推から、量子情報の共有についての非対称性を分析した研究はこれまでにほとんどなかったため、本研究における非対称性の発見は重要な意義を持つものと考える。

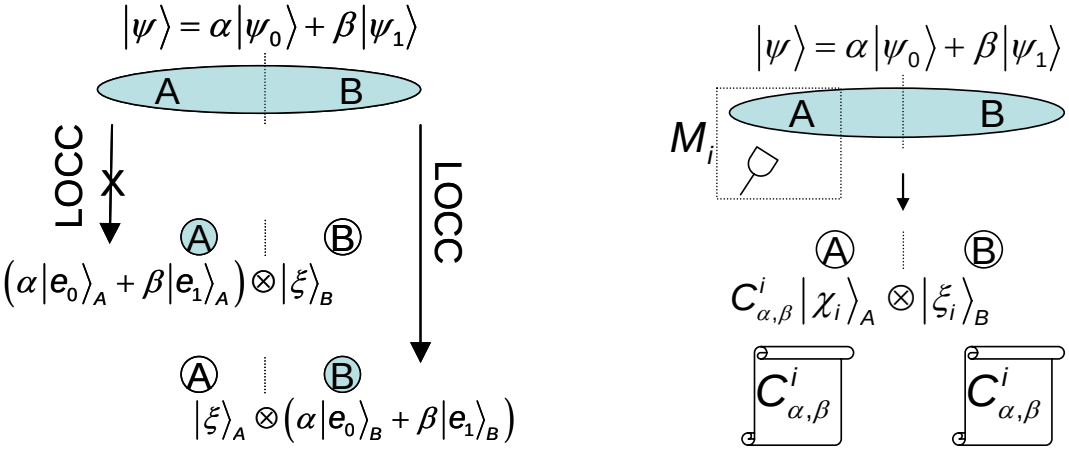
更に、遠隔操作量子情報抽出とは逆のタスクとも考えられる、遠隔操作量子情報破壊が可能であるための必要十分条件を求めた。これは、2者間で共有する量子情報を、どちらか一方の局所的操作のみによって、測定後の状態には量子情報が存在しないように破壊するタスクである。その結果、量子もつれを持つ状態を符号化基底として用いる場合、遠隔操作量子情報破壊が可能であるためには、量子情報を2者間で対称的に共有しなければならないこと示した。

非対称遠隔量子もつれ操作

純粋状態を用いて量子情報を2者間で共有する場合には、遠隔操作量子情報破壊の条件の制約により、遠隔操作量子情報抽出と遠隔操作量子情報破壊のどちらも非対称にすることは不可能となる。そこで、混合状態を用いた量子情報の共有を行うことによって、局所的操作の選択に応じて、非対称な遠隔操作量子情報抽出と遠隔操作量子情報破壊を選ぶことができる方法を見出した。

さらに、LOCCによる量子情報の変換と、拡張された系におけるLOCCの下での量子もつれの変換を結びつけることによって、A と B と C の3者間で共有する量子もつれから、B が局所操作を選び実行し、C が古典通信による回復量子操作を行なうことで、A と C との間で遠隔操作によって

量子もつれを抽出したり、量子もつれを破壊したりすることが可能である条件を得た。そして、混合状態の作用により、A と B の間では、量子もつれを抽出することが不可能であるが、A と C との間では量子もつれを抽出することが可能であるような、非対称遠隔量子もつれ操作を考案した。



遠隔操作量子情報集約（左）と遠隔量子情報破壊(右)の概念図

無限準位系に特有な量子もつれの性質の発見

従来、エネルギーが有限で有限情報のやりとりしか含まないような物理的に可能な条件下においては、無限準位系においても有限準位系の量子もつれと性質には大きな違いがないと考えられていた。我々は、有限・無限の次元性の違いによる量子物理の基盤的な量子もつれ構造（全順序・半順序構造の違い）に相違が生じることを示した。更に、無限準位系においては、物理的に可能な状況下においても相互に変換不可能な状態が無限に存在することを示した。この予想外の性質は、数学的性質の違いによる量子物理の基盤的な構造の違いを示し、量子情報処理への応用も期待されるものである。

LOCC 状態識別と量子もつれ量の関係

量子計算や量子通信は量子情報の演算や操作を扱うものであるが、情報処理の最終段階（出力過程）においては、我々が扱うことのできる古典情報に変換する必要がある。出力過程は、量子情報から古典情報への変換過程となっており、量子状態に符号化された古典情報をいかにうまく引き出すか、すなわち、異なる古典情報が符号化された量子状態をいかに識別するか、という問題が非常に重要となる。

そこで、LOCC 変換よりひとつ大きな量子操作の集合である Separable 変換に着目し、状態の量子もつれの量のみで定まる識別性の限界を求めた。そして、一般的な多粒子状態の空間において、大局的量子もつれ頑強性、相対エントロピーを用いた量子もつれ測度や幾何学的量子もつれ測度などの幾何学的に定義される量子もつれの量が、LOCC で識別可能な状態の数に上限を与えることを証明した。また、N 粒子の W 状態が N 粒子の GHZ 状態よりも LOCC 状態識別の視点では非局所性が高いことを示した。

この研究成果は、これまでにほとんど知られていなかった、操作的な観点からの多粒子量子もつれの定量化を与えるものであり、量子暗号等への応用が期待される。一方、量子もつれの距離的測度の大きい状態を探索することで、量子秘密共有などの量子暗号プロトコルへの応用研究へと発展する可能性がある。

量子もつれ頑強性と低階数ノイズ

量子もつれ頑強性(Robustness of entanglement)は、ノイズに対する量子状態の量子もつれ保

持性を表す測度である。ノイズが量子状態に及ぼす効果は、その量子状態を表す密度演算子に別の密度行列を混合することでモデル化できる。混合する密度行列の階数は、ノイズによって引き起こされる可能性のあるユニタリ変換の数を示すものである。低階数の密度行列で表されるノイズにによる影響を考察することによって、多者間量子もつれの一つの指標である、シュミット数から1を引いた階数を持つようなノイズは、量子状態の多者間量子もつれを完全には破壊することができないことを示した。

熱平衡状態における多者間量子もつれ

ここ数年、量子情報科学のみならず、物理の様々な分野で量子もつれの存在とその役割を理解するための多大なる努力がなされてきた。例えば、凝縮系物理の臨界現象や高エネルギー物理での対称性の破れ、ホーキング放射などにも量子もつれの存在が関連づけられてきており、マクロな系でも量子もつれが絶対零度以外で存在し得ることが証明された。

そこで我々は、マクロな系における多者間量子もつれの性質をよりよく理解するために、有限温度の熱平衡状態における多者間量子もつれ保持性を、量子もつれの距離的測度を用いて解析した。その結果、量子もつれの距離的測度である量子もつれ頑強性の大きな基底状態を持つ熱平衡状態において、量子もつれの存在を保証する臨界温度を導出することに成功した。マクロスコピック熱平衡状態における量子もつれの見積りは、ノイズの影響を受ける現実的な系における量子情報処理の研究に欠かせないものであり、量子もつれ頑強性による解析は、広い分野へ応用可能であると考える。

局所演算による量子状態への古典情報符号化

量子もつれを持つ量子状態に対して、その量子状態の次元と同じ数の古典情報を、局所演算のみによって符号化する方法および、そのような符号化が可能である量子もつれを持つ量子状態の条件を求めた。その結果、クリッフォード群に属する演算によってゼロ状態（量子ビットがすべてゼロからなる積状態）から作られる量子もつれをもつ状態は、局所演算による量子状態への古典情報符号化が可能であることを示した。また、クリッフォード群には属さないが、局所演算による量子状態への古典情報符号化が可能であるような擬クリッフォード集合の存在を提示し、W状態などの非クリッフォード群状態での局所演算による古典情報符号化の方法を示した。

4．2　応用研究

量子情報のための量子鍵プロトコル・遠隔量子情報スイッチプロトコル

2 者間非量子情報分配の研究出られた成果を用いて、二者のうち一方が持つ量子情報は、他方への量子情報復元のための鍵（量子鍵）としかなり得ない、というような量子情報の「不公平」分配のプロトコルを提案した。

更に、純粋状態のみならず混合状態の量子鍵を考察することにより、さらに安全性を高めた量子鍵プロトコルである遠隔量子情報スイッチプロトコルを提案した。このプロトコルは、送信者・受信者・情報通信の是認者(approver)の三者からなるプロトコルであり、この当事者以外の信頼できる第三者の存在を不要としながらも、情報通信の是認者が承認した時のみ送信者から受信者への量子通信が可能となる一方、是認者が承認しない場合には、古典的限界を超えて量子情報を送信者から受信者に送ることが不可能となるもので、是認者が量子情報の伝達を「遠隔スイッチ」で制御することができるプロトコルとなっている。

量子錠プロトコル

量子情報における暗号的応用分野では、量子状態を用いて古典情報である乱数共有を行うBB84 プロトコルなどの量子鍵配送が成功している。我々は、量子情報そのものを用いた暗号プロトコルの可能性を模索し、群論的アプローチによる一方向性量子計算の暗号的応用の一例として、認証者を通じて証明者と確認者の間で認証を行うための量子錠プロトコルを提案した。このプロトコルでは、全行程を通してクローン禁止原理を持つ量子情報を用いることで、複製による情報漏

洩の可能性が非常に低くなっていることが特色である。

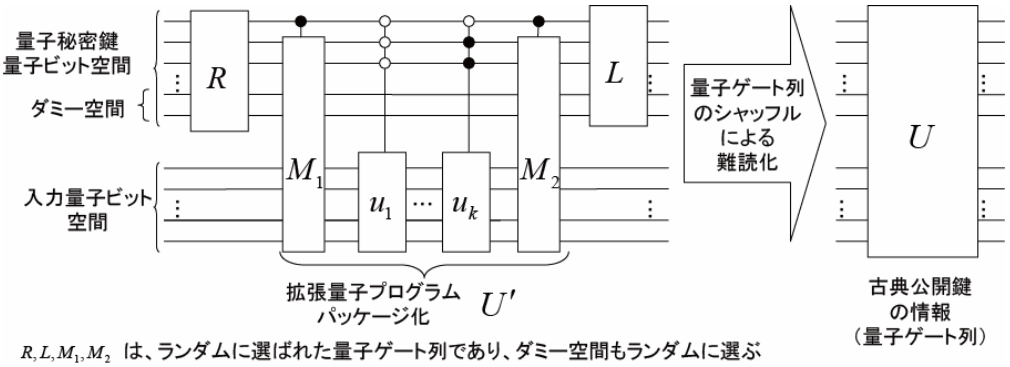
プロトコルは、証明者に配布される量子状態である量子鍵、確認者が持つ量子状態である量子確認鍵、認証者によって作成される最大エンタングル状態である量子錠からなる。そして、証明者が提出した量子鍵が量子確認鍵と同一の状態であることが確認者によって確認されれば、認証が成功することになる。ここで、量子鍵は認証者の行うパウリ群の演算によって暗号化されており、同じパウリ群の演算が組み込まれた量子錠によってのみ復号化することができる。一方、量子錠は、確認者の行うクリッフォード群の演算によって暗号化されており、認証者の知識のみでは、量子鍵と量子確認鍵を一致させることは不可能となっている。

計算量的秘匿量子演算

公開通信路を通じて古典情報を安全に送るために現在広く用いられている公開鍵暗号は、古典計算機による計算量によって安全が保障されているものであり、量子計算機が実現されると安全ではなくなる。そこで、量子系を用いて秘密鍵の共有を行う量子鍵分配が提案された。量子鍵分配では、認証が正しく行われていれば無条件安全性が保障される。しかしながら、現在用いられている認証プロトコルは公開鍵暗号と同様の性質を用いており、量子計算機が実現されると安全性が保障されない。量子計算機が実現しても安全性が保障されるような量子系を用いた公開鍵暗号プロトコルについては、河内らによる先駆的な研究(A. Kawachi et al, Proc. EUROCRYPT 2005, LNCS 3494, 268, 2005)があるが、量子状態を公開鍵として用いているため、認証プロトコルとして用いるには困難があった。一方、量子計算機が実現された場合には、量子情報の保全だけではなく、量子計算を行うためのソースプログラム(量子ゲート列)の暗号化も必要となる。このような課題に対処する方法も知られていなかった。

そこで、量子計算機が実現されても計算量的に安全性が保障される可能性が高い量子暗号要素技術(暗号プリミティブ)を考察するために、秘匿量子計算の概念を提唱した。秘匿量子演算は、ユニタリ演算を複数組み込み、さらに暗号化を行った拡張量子プログラムの量子ゲート列に難読化(obfuscation)を施すことによって得られた量子ゲート列を古典情報からなる公開鍵とし、量子状態からなる量子秘密鍵と組み合わせることによって、量子秘密鍵が指定するユニタリ演算で表される量子計算を任意の入力量子情報に対して実行するものである。

量子計算の実行者は、難読化の効果により、量子計算機を用いても古典公開鍵の情報から多項式時間でユニタリ演算を特定することができず、また、量子秘密鍵の量子状態の特定も、多項式時間の量子計算によっては不可能となる。この秘匿量子計算を用いると、量子秘密鍵を用いずに多項式時間で量子計算を実行することが可能であるのは、古典公開鍵の作成者だけとなる。そのため、量子計算機が実現されても計算量的に安全性が保障される可能性が高い量子暗号要素技術(暗号プリミティブ)となり得る。



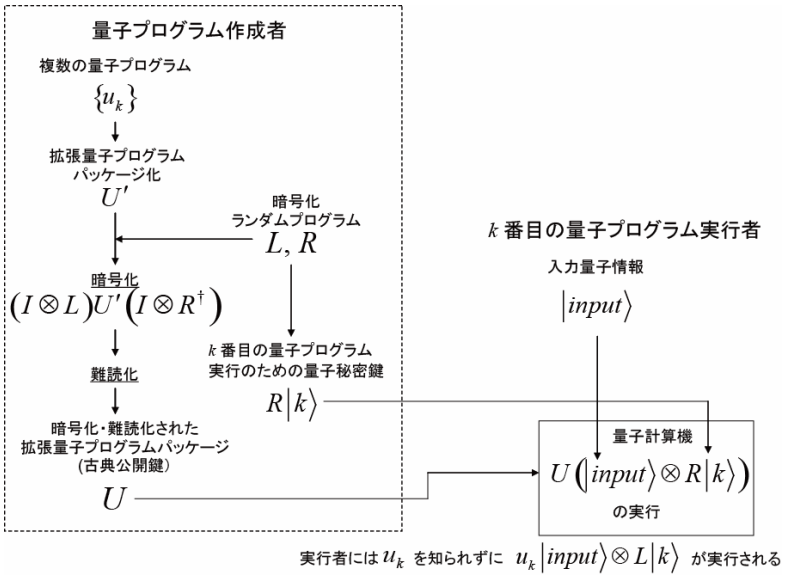
古典公開鍵の作成方法

計算量的秘匿量子演算を利用した量子公開鍵暗号システム

計算量的秘匿量子演算は、暗号要素技術(暗号プリミティブ)として、3種類の量子公開鍵暗号シ

ステム（量子計算機が実現してもなお計算量的に安全が保障される認証プロトコル、量子情報を安全に通信するための暗号システム、量子計算のソースプログラム暗号化方法）を構築することが可能となることを示した。これらの量子公開鍵暗号システムの特徴は、量子秘密鍵が再利用可能であり、量子メモリーが完全であるならば、秘密量子鍵配送のための量子通信を繰り返す必要がないという点である。また、量子プログラムから拡張量子プログラムを作る際に、複数の量子プログラムをまとめた量子プログラムパッケージを作成することも可能となる。このため、A と B の2者間のみならず、A と C、A と D など A に対して多者間で秘匿量子計算を行うことができる。

本研究は量子プログラム（量子ゲート列）の難読化(obfuscation)という新たな研究課題を提起するものであり、効率よく難読化を行うためのアルゴリズムなど、今後の量子情報の研究発展の新たな方向性を提供するものである。



多者間での計算量的秘匿量子計算

5　自己評価：

本研究は、基礎研究で得られた知見を応用研究に生かし、さらに基礎研究にフィードバックを行なうという研究方法をとって行った。量子もつれの性質および、量子情報の非局所的な性質について知見を得ることが先行し、応用研究である量子暗号プロトコルについては、なかなか画期的な研究成果を挙げることができなかったが、最終的には、基礎研究の成果をふまえて、量子もつれ状態を量子秘密鍵とし、古典公開鍵と組み合わせることによって認証を行うという、まったく新しいアイディアの量子暗号プロトコルを考案することができ、当初の目的はほぼ達成したのではないかと考える。

一方、本研究では、積極的に大学院生を研究補助者として採用し指導することにより、人材育成に努めた。このため、多くの研究テーマを同時進行で行うことになった。大学院生が飛躍的に力を発揮することによって研究自体は大きく進展したが、その研究成果を論文にまとめることに手間取り、本研究で得られた多くの研究成果が未発表であることは、反省するべき点であると考える。今後、早急に研究成果を論文としてまとめる予定である。

6　研究総括の見解：

非対称な量子状態の共有に関する基礎的研究とその応用である量子鍵に関する仕事が、この分野で高く評価されています。他の仕事の出版も時間の問題でしょう。3年間の業績として申し分ありません。

計画が目指していた量子状態自体を秘密鍵にして、量子計算機があっても安全な暗号シス

テムについては、計画の終わり頃にエンジンがかかって一分野をなすような系統的な研究への大きな橋頭堡を築いているように見えます。この分野で喫緊に必要な若手の養成にも心を砕いている点も高く評価したいと思います。

7 主な論文等:

論文(発表済2件、投稿中3件、投稿準備中3件)

1. Owari Masaki, Keiji Matsumoto and Mio Murao, Entanglement convertibility for infinite dimensional pure bipartite states, Phys. Rev. A 70, 050301 (2004)
2. M. Hayashi, D. Markham, M. Murao, M. Owari and S. Virmani, Bounds on Multipartite Entangled Orthogonal State Discrimination Using Local Operations and Classical Communication, Phys. Rev. Lett. 96, 040501 (2006)
3. D. Markham, J. Anders, V. Vedral, M. Murao, Survival of entanglement in thermal states, quant-ph/0606103
4. Masaki Owari, Samuel L. Braunstein, Kae Nemoto, Mio Murao, ε-convertibility of entangled states and extension of Schmidt rank in infinite-dimensional systems, quant-ph/0609167
5. Yu Tanaka, Damian Markham, Mio Murao, Local encoding of classical information onto quantum states, quant-ph/ 0702190

特許(特許出願準備中1件)
発明者: 村尾美緒、田中雄
発明の名称: 古典公開鍵と量子秘密鍵を用いた計算量的秘匿量子計算

受賞 なし

招待講演 なし

国際会議一般講演(11 件)

1. Yu Tanaka, Masaki Owari, Mio Murao, A quantum lock protocol, The Ninth Workshop on Quantum Information Processing (QIP2006), 2006
2. Mio Murao, Yoshiko Ogata, Mixed state asymmetric qubit information sharing, The Ninth Workshop on Quantum Information Processing (QIP2006), 2006
3. M. Hayashi, D. Markham, M. Murao, M. Owari, S. Virmani, Local Discrimination and Multipartite Entanglement Measures, ERATO conference on Quantum Information Science 2005
4. Yoshiko Ogata, Ryu Ebisawa and Mio Murao, Asymmetric quantum information sharing between two parties, Gordon Research Conference on Quantum Information Science 2004
5. Masaki Owari, Kenji Matsumoto and Mio Murao, Entanglement convertibility for infinite-dimensional pure bipartite states, ERATO conference on Quantum Information Science 2004.