様　式　Ｆ－１９－２

科学研究費助成事業　　研究成果報告書

令和　　２ 年　　６ 月　　１ 日現在

機関番号：１３９０１
研究種目：国際共同研究加速基金（国際共同研究強化）
研究期間：2016～2019
課題番号：１５ＫＫ０００７

研究課題名（和文）マルチユーザ型量子ネットワーク（国際共同研究強化）

研究課題名（英文）Multi-user type quantum network(Fostering Joint International Research)

研究代表者
林　正人（Hayashi, Masahito）

名古屋大学・多元数理科学研究科・教授

研究者番号：４０３４２８３６

交付決定額（研究期間全体）：（直接経費）　　9,000,000円
渡航期間：　10ヶ月

研究成果の概要（和文）：本研究では，マルチユーザ型量子ネットワークの知見をもとに，自己精度保証が可能となる量子計算の研究を行った．このために，グラフ状態やハイパーグラフ状態などの巨大なエンタングル状態と局所測定の組み合わせで実現可能な測定型量子計算に注目した．そして，グラフ状態やハイパーグラフ状態などの純粋状態の検証について，様々な設定で研究を行った．特に，量子計算の自己精度保証のために，グラフ状態の特殊例である三角格子型クラスター状態の自己検証の方法を提案し，これを用いて，自己精度保証が可能となる量子計算の方法を提案した．

研究成果の学術的意義や社会的意義
近年、量子計算に関する研究の機運が高まっている．しかし，量子計算はノイズに弱いため，正しく所望の動作が物理的になされているか検証する必要がある．一般に，得られた計算結果だけから，その正しさを検証することは困難である．しかし，測定型量子計算の場合，その計算プロセスは，局所操作と形が決まっている巨大なエンタングル状態の組み合わせで得られる．したがって，局所操作と巨大なエンタングル状態の双方について検証を行えば，検証が可能となる．このような方法で検証を行うことで，量子計算の計算結果の信頼性を保証することができる．

研究成果の概要（英文）：In this study, based on the obtained result for a multi-user type quantum network, I studied a method for quantum computation with self-verification. For this aim, I focused on measurement-based quantum computation, which is composed of local measurement and a large entangled state, e.g., a graph state and a hypergraph state. Hence, I studied verification of pure states including graph states and hypergraph states under various formulations. Especially, for self precision-guaranteed quantum computation, I proposed a method for self-verification for triangle cluster state, which is a typical example of a graph state. Based on this method, I proposed a self precision-guaranteed method for quantum computation.

研究分野：量子情報

キーワード：測定型量子計算　グラフ状態　自己検証

様　式　Ｆ－１９－２

１．研究開始当初の背景

多端子系でのエンタングル状態の検定：基課題では最初に二端子系でのエンタングル状態の検定の基礎について研究し，定量的にエラーを評価するための枠組みを与えた．そして，多端子系でのエンタングル状態のうち，二部グラフからなるグラフ状態の場合での検定が，二端子系でのエンタングル状態の検定に帰着できることを示し，この場合について同様の成果を得た(Hayashi *et al* arXiv:1505.07535)．さらに，その成果をブランド量子計算に応用した．

ネットワーク符号の安全性評価：基課題では，ネットワーク符号，及び量子ネットワーク符号について研究し，一定の条件の下で安全となる符号の構成に成功した．これらのネットワーク符号において，有効に働く誤り訂正符号の構成法の一般論を与えた

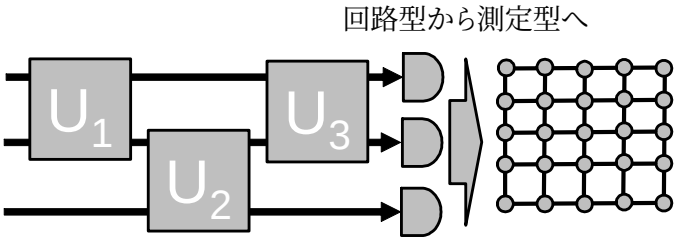
２．研究の目的

本研究では，基課題で得られた上述の成果をベースに，以下の新たなテーマに取り組む．すなわち，本研究の目的は，

定量的かつ厳密に精度保証が可能となる測定型量子計算機の理論的枠組みを構築する．

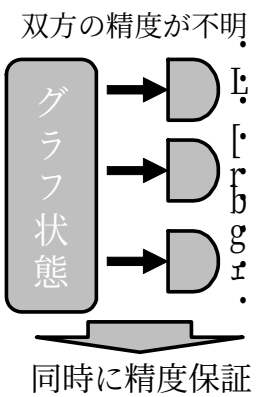
である．この研究は後に述べるように，上述の基課題の成果があって初めて研究が可能となるものである．

３．研究の方法



測定型量子計算：量子計算を実現するには様々な方法がある．伝統的には量子回路モデルが使われてきているが，そのほかにも，近年 D-wave 量子計算機で注目を集めている断熱量子計算モデルや，2001 年にドイツで提案され量子回路モデルと同等な性能を持つ測定型量子計算モデルが挙げられる．本研究では，測定型量子計算モデルに注目する．なぜならば，精度保証の目的にはこれが最も適しているからである．測定型量子計算では，始めにグラフから定義される多端子間でエンタングルした状態であるグラフ状態を準備する．グラフ状態はグラフで繋がったキュービット間でエンタングルするよう設計されている．このグラフ状態の下で，各キュービットを逐次的に測定することで，量子回路モデルと同等の量子計算が実現できる．一般に，キュービットの測定は簡単に行える場合が多く，とりわけ光系やイオントラップ系ではすでに多くの実験がなされている．一方で，規模の大きいグラフ状態を準備することは一般には難しく，多くのエラーに悩まされることになる．そこで，このグラフ状態の精度保証を行うことで，測定型量子計算における精度保証を行う．この方法が従来の量子回路モデルの精度保証と大きく違う点は，量子回路の場合，計算結果が予測できない量子回路の大規模な組み合わせの精度保証を行わなければならないが，測定型量子計算の場合，形が分かっている大規模なグラフ状態の精度保証のみを制限された測定の組み合わせで行えばよいので，はるかに簡単でありより厳密かつ詳細な分析が可能となる．

グラフ状態の自己精度保証：基課題では，グラフ状態の精度保証を最小限の測定手法の組み合わせで定量的に実現する手法を与えた．しかし，測定においてもエラーが入る可能性があるので，本研究では，測定によるエラーをグラフ状態の準備に組み込むことで，グラフ状態だけでなく測定についても精度保証を同時に実現する理論を構築する．このためには，測定基底の自己検証が必要である．本研究では，測定基底の自己検証とグラフ状態の精度保証を適切に組み合わせることで，測定基底とグラフ状態だけからそれ自身の精度保証を定量的に行う．これをグラフ状態の自己精度保証とよぶことにする．グラフ状態の自己精度保証をベースに，測定型量子計算機の計算結果の精度保証を与えるプロトコルを設計する．ここで与える精度保証は工業製品の統計的品質管理に用いられる仮説検定の枠組みで行う．そのため，有意水準付きの精度保証が得られ，現在の工業製品に適用されている品質管理と同レベルの精度保証が可能となる．



本研究を行うには通常の量子計算の技法よりも，量子論の基礎付けに関する議論と共に，量子系の統計的仮説検定に関する知識が必要となる．自己精度保証では，量子論の基礎に立ち戻って考え直す必要があり，量子論の基礎は大変重要である．一方で，扱っている対象が量子状態であるため，量子性を考慮した統計理論である量子系の統計的仮説検定が必要となる．なお，従来用いられてきた量子トモグラフィーは量子状態を

記述する全パラメータの推定を行うため，精度保証の目的から考えると不要な測定を沢山行っており，極めて効率が悪く，グラフのサイズが大きくなると実用的ではない．そこで得られる精度に関する議論にも不十分な点が多い．

４．研究成果

測定型量子計算の自己検証：当初の予定通り，シンガポール国立大学の Michal Hajdusek 博士と共同でグラフ状態の自己検証の方法を提案することができた．そして，これを用いて自己精度保証が可能となる測定型量子計算の方法を具体的に与えた．最初に Bell 状態の自己検証の方法を与えた．従来方法では，CHSH テストのみを用いていた．しかし，その方法では，自己検証のために必要なコピーの数が多くなる問題がある．そこでは，本研究では，スタビライザーテストを組み合わせることで，必要なコピーの数を減らすことに成功した．なお，スタビライザーテストだけでは，自己検証は不可能であるので，スタビライザーテストと CHSH テストを組み合わせることが重要である．
次に，ここで提案した Bell 状態の自己検証の方法を組み合わせることで，グラフ状態の自己検証の方法を提案した．すなわち，グラフ状態の色わけに注目し，それぞれの色ごとに局所的な測定基底を検証する方法を提案した．この方法では１つの色に注目した場合，互いに共通の近傍を持たない同じ色の qubit 系の測定基底を同時に検証できる利点がある．さらに，測定基底の自己検証に，測定型量子計算に用いるグラフ状態の検証を組み合わせることで，自己検証が可能となる測定型量子計算の方法を提案した．なお従来研究では，個々のコピーの間の独立同一性が仮定されていた．しかし，本研究では，この仮定を取り除き，ランダムサンプリングだけの仮定の下で，自己検証が可能であることをしめした．ただし，この単純な組み合わせでは，個々の qubit 系が独立に動作することを仮定する必要がある．この仮定を取り除き，巨大なグラフ状態を準備する player と，残りの qubit 系を測定する player の 2 者だけの間の独立性だけで，自己検証が可能となることを示した．そのために，前者の player から後者の player への巨大なグラフ状態の受け渡しにおいて，teleportation を巧妙に用いるアイデアを用いた．

ノイズがある設定での量子計算の検証：しかしながら，上記のように測定基底を信用せず，測定基底まで検証する自己検証の方法は，コストがかかりすぎて実用的とは言えない．特に，この方法では，少しでもノイズがあると不正とみなし，動作しない問題点がある．実用的な設定としては，測定基底を信用する代わりに，少しのノイズを不正とみなさず，ノイズとして受け入れ，そのようなノイズの下でも機能する方法である．このような設定を扱う方法として，fault-tolerant 型量子計算に注目し，これを測定型量子計算に組み合わせることで，測定基底を信用した場合に機能する，検証可能な fault-tolerant 型測定型量子計算を提案した．この方法では，検出されたノイズが fault-tolerant 型測定型量子計算で訂正可能であるか否か検証することになる．なお，測定基底のノイズを状態に対するノイズとみなすことにより，この手法は測定基底にノイズがある場合にも適用できる．おそらく，実用的にはこちらの方法が有効であると考えられる．

量子状態の検証：そのほか，測定基底を信用するが，測定の方法に一定の制約がある場合に，一般の純粋状態の検証方法についても研究を行った．この設定においては，上記の議論に比べて扱いやすい設定であるため，より緻密な最適化の議論を行った．すなわち，一定の有意水準を達成するために必要最小限のコピー数を導出した．この議論は，グラフ状態の検証のみならず，ハイパーグラフ状態，重みつきグラフ状態の検証にも適用できる．さらに，一般の qubit 純粋状態の検証についても扱った．最大エンタングル状態も separable でない qubit 純粋状態においては，双方向の通信を行うことで，一方向の通信のみを用いた時の性能を上回ることを示した．

量子超越性への応用：重みつきグラフ状態は、量子超越性を実現すると考えられる量子計算に用いられることが知られている．したがって，重みつきグラフ状態の検証は量子超越性の検証に応用可能である．近年 google による量子超越性実現の議論があるが，様々な反論が起こっている．その原因の１つは，本当に量子超越性が実現されたか否かを厳密に判定する基準が，与えられていなかったことが挙げられる．したがって，本研究のように，厳密な基準の下での検証がなされたのであれば，事情が異なっていたと考えられる．

測定型量子計算への展開：測定型量子計算は，上で述べたように，量子計算の検証において中心的役割を果たした．従来の測定型量子計算では，最低でも 3 種類の測定が必要であるか，もしくは，標準的な Pauli 行列以外の物理量の測定が必要であった．より少ないコストで測定型量子計算を実現するには，２つの Pauli 行列の測定だけで実現できるのが望ましい．本研究では，PauliX,Z 行列の測定のみで測定型量子計算を実現するスキームを提案した．すなわち，

PauliX,Z 行列の測定のみでユニバーサル測定型量子計算を実現するハイパーグラフ状態を提案した．サーバーがハイパーグラフ状態を準備し，ユーザが測定を行うだけで量子計算を行うスキームでは，上記の性質を持つハイパーグラフ状態をサーバーが実現すれば，ユーザは極めて実現が容易な PauliX,Z 行列の測定さえ準備すればよいので，ユーザ側のコストを抑えることができる．

今後の展開：なお、本国際共同研究の終了後 2020 年 4 月 1 日から名古屋大学を休職し，本研究での共同研究先である南方科技大学で勤務することになった．本国際共同研究の成果は南方科技大学で研究において発展させることが期待できる．

５．主な発表論文等

〔雑誌論文〕　計10件（うち査読付論文　10件／うち国際共著　8件／うちオープンアクセス　2件）

１．著者名 Masahito Hayashi and Michal Hajdusek	４．巻 97
２．論文標題 Self-guaranteed measurement-based blind quantum computation	５．発行年 2018年
３．雑誌名 Physical Review A	６．最初と最後の頁 52308
掲載論文のDOI（デジタルオブジェクト識別子） 10.1103/PhysRevA.97.052308	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

１．著者名 Tomoyuki Morimae, Yuki Takeuchi, and Masahito Hayashi	４．巻 96
２．論文標題 Verification of hypergraph states	５．発行年 2017年
３．雑誌名 PHYSICAL REVIEW A	６．最初と最後の頁 62321
掲載論文のDOI（デジタルオブジェクト識別子） 10.1103/PhysRevA.96.062321	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Keisuke Fujii and Masahito Hayashi	４．巻 96
２．論文標題 Verifiable fault tolerance in measurement-based quantum computation	５．発行年 2017年
３．雑誌名 PHYSICAL REVIEW A	６．最初と最後の頁 030301(R)
掲載論文のDOI（デジタルオブジェクト識別子） 10.1103/PhysRevA.96.030301	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Kun Wang and Masahito Hayashi	４．巻 100
２．論文標題 Optimal verification of two-qubit pure states	５．発行年 2019年
３．雑誌名 PHYSICAL REVIEW A	６．最初と最後の頁 32315
掲載論文のDOI（デジタルオブジェクト識別子） 10.1103/PhysRevA.100.032315	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

1．著者名 Huangjun Zhu and Masahito Hayashi	4．巻 99
2．論文標題 Optimal verification of two-qubit pure states	5．発行年 2019年
3．雑誌名 PHYSICAL REVIEW A	6．最初と最後の頁 52346
掲載論文のDOI（デジタルオブジェクト識別子） 10.1103/PhysRevA.99.052346	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

1．著者名 Huangjun Zhu and Masahito Hayashi	4．巻 123
2．論文標題 Efficient Verification of Pure Quantum States in the Adversarial Scenario	5．発行年 2019年
3．雑誌名 PHYSICAL REVIEW LETTERS	6．最初と最後の頁 260504
掲載論文のDOI（デジタルオブジェクト識別子） 10.1103/PhysRevLett.123.260504	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

1．著者名 Huangjun Zhu and Masahito Hayashi	4．巻 100
2．論文標題 General framework for verifying pure quantum states in the adversarial scenario	5．発行年 2019年
3．雑誌名 PHYSICAL REVIEW A	6．最初と最後の頁 62335
掲載論文のDOI（デジタルオブジェクト識別子） 10.1103/PhysRevA.100.062335	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

1．著者名 Huangjun Zhu and Masahito Hayashi	4．巻 12
2．論文標題 Efficient Verification of Hypergraph States	5．発行年 2019年
3．雑誌名 PHYSICAL REVIEW APPLIED	6．最初と最後の頁 54047
掲載論文のDOI（デジタルオブジェクト識別子） 10.1103/PhysRevApplied.12.054047	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

1．著者名 Masahito Hayashi and Yuki Takeuchi	4．巻 21
2．論文標題 Verifying commuting quantum computations via fidelity estimation of weighted graph states	5．発行年 2019年
3．雑誌名 New Journal of Physics	6．最初と最後の頁 93060
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.1088/1367-2630/ab3d88	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

1．著者名 Yuki Takeuchi, Tomoyuki Morimae, and Masahito Hayashi	4．巻 9
2．論文標題 Quantum computational universality of hypergraph states with pauli-X and Z basis measurements	5．発行年 2019年
3．雑誌名 Scientific Reports	6．最初と最後の頁 13585
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.1038/s41598-019-49968-3	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

〔学会発表〕　計22件（うち招待講演　12件／うち国際学会　21件）

1．発表者名 Masahito Hayashi
2．発表標題 Measurement-Based Quantum Computation and Its Verification
3．学会等名 Second Hong Kong-Shenzhen Workshop on Quantum Information Science（招待講演）（国際学会）
4．発表年 2018年

1．発表者名 Masahito Hayashi
2．発表標題 Finite-length security analysis in quantum key distribution
3．学会等名 中国電子学会2019量子信息技術学術交流大会（招待講演）
4．発表年 2019年

１．発表者名
Masahito Hayashi

２．発表標題
Various security in quantum information

３．学会等名
Nagoya-SUSTech Quantum Information Workshop（国際学会）

４．発表年
2019年

１．発表者名
Masahito Hayashi

２．発表標題
Asymptotic decoupling property, mixing condition and Hidden Markovian Process in quantum system

３．学会等名
Mathematical Aspects in Current Quantum Information Theory（招待講演）（国際学会）

４．発表年
2019年

１．発表者名
Masahito Hayashi

２．発表標題
Discrimination in general probability theory

３．学会等名
Interactions between Noncommutative Analysis and Quantum Information Theory（招待講演）（国際学会）

４．発表年
2019年

１．発表者名
Masahito Hayashi

２．発表標題
Semi-Finite Length Analysis for Secure Random Number Generation

３．学会等名
2019 IEEE International Symposium on Information Theory（国際学会）

４．発表年
2019年

１．発表者名
Masahito Hayashi

２．発表標題
Secure list decoding

３．学会等名
2019 IEEE International Symposium on Information Theory（国際学会）

４．発表年
2019年

１．発表者名
Masahito Hayashi

２．発表標題
Quantum network coding

３．学会等名
Summer Workshop on Quantum Algorithm and Quantum Software（招待講演）（国際学会）

４．発表年
2019年

１．発表者名
Masahito Hayashi

２．発表標題
Quantum Private Information Retrieval

３．学会等名
the 2019 workshop on probability and information theory（招待講演）（国際学会）

４．発表年
2019年

１．発表者名
Yuuya Yoshida, Man-Hong Yung, and Masahito Hayashi

２．発表標題
Optimal Mechanism for Randomized Responses under Universally Composable Security Measure

３．学会等名
2019 IEEE International Symposium on Information Theory（国際学会）

４．発表年
2019年

１．発表者名
Masahito Hayashi

２．発表標題
Verification of Measurement-Based Quantum Computation

３．学会等名
IHP conference on Quantum Information Theory（招待講演）（国際学会）

４．発表年
2017年

１．発表者名
Masahito Hayashi

２．発表標題
Verification of Measurement-Based Quantum Computation

３．学会等名
International Workshop on Quantum Computing and Quantum Information Processing 2017（招待講演）（国際学会）

４．発表年
2017年

１．発表者名
Masahito Hayashi

２．発表標題
Role of Hypothesis Testing in Quantum Information Theory

３．学会等名
Asian Conference on Quantum Information Science (AQIS 17)（招待講演）（国際学会）

４．発表年
2017年

１．発表者名
Masahito Hayashi

２．発表標題
Verification of Measurement-Based Quantum Computation

３．学会等名
Trustworthy Quantum Information,（招待講演）（国際学会）

４．発表年
2017年

１．発表者名
Masahito Hayashi and Michal Hajdusek

２．発表標題
Self-guaranteed measurement-based quantum computation

３．学会等名
Asian Conference on Quantum Information Science (AQIS 17)（国際学会）

４．発表年
2017年

１．発表者名
Keisuke Fujii and Masahito Hayashi

２．発表標題
Verifiable fault-tolerance in measurement-based quantum computation

３．学会等名
Asian Conference on Quantum Information Science (AQIS 17)（国際学会）

４．発表年
2017年

１．発表者名
Masahito Hayashi and Michal Hajdusek

２．発表標題
Self-guaranteed measurement-based quantum computation

３．学会等名
The International Conference on Quantum Communication, Measurement and Computing (QCMC2016)（国際学会）

４．発表年
2016年

１．発表者名
H. Zhu and M. Hayashi

２．発表標題
Efficient Verification of Pure Quantum States in the Adversarial Scenario

３．学会等名
Quantum Information Processing 2020 (QIP)（国際学会）

４．発表年
2020年

１．発表者名
M. Hayashi

２．発表標題
Verification of Graph state, Hypergraph state, and Weighted graph state

３．学会等名
Beyond iid Conference（国際学会）

４．発表年
2019年

１．発表者名
M. Hayashi

２．発表標題
Verification of commuting quantum computations via fidelity estimation of weighted graph states

３．学会等名
Mini-Workshop on Quantum Verification（招待講演）（国際学会）

４．発表年
2019年

１．発表者名
M. Hayashi

２．発表標題
Verification of commuting quantum computations via fidelity estimation of weighted graph states

３．学会等名
Quantum information and string theory 2019（招待講演）（国際学会）

４．発表年
2019年

１．発表者名
Yuuya Yoshida, Man-Hong Yung and Masahito Hayashi

２．発表標題
Optimal Mechanism for Randomized Responses under Universally Composable Security Measure

３．学会等名
IEEE International Symposium on Information Theory (ISIT2019)（国際学会）

４．発表年
2019年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

6．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
主たる渡航先の主たる海外共同研究者	ハドゥシェック　ミカエル (Hajdusek Michal)	シンガポール国立大学・Centre for quantum technologies・Research fellow	
主たる渡航先の主たる海外共同研究者	ユン　マンホン (Yung Man-Hong)	南方科技大学・物理学科・准教授	
主たる渡航先の主たる海外共同研究者	ワン　クン (Wang Kun)	南方科技大学・量子科学与工程研究院・博士研究員	
その他の研究協力者	ズウ　ホンジャン (Zhu Huangjun)	復旦大学・物理学科・教授	