

研究種目：基盤研究(B)

研究期間：2005～2008

課題番号：17340021

研究課題名（和文） 量子情報と量子計算の数理解析的基礎研究

研究課題名（英文） Mathematical study of quantum information and quantum computing

研究代表者

小澤 正直 (Masanao Ozawa)

名古屋大学・大学院情報科学研究科・教授

研究者番号：40126313

研究成果の概要：量子コンピュータに代表される量子情報技術の理論的基礎を確立するために、数理物理学と数学基礎論の方法によって、量子測定、量子情報、量子計算に関する数学理論を構築し、本研究代表者が開発した量子測定理論と普遍的不確定性原理に基づいて、保存法則に由来する量子計算の精度の限界を明らかにし、量子計算の実現に伴う様々なモデルに対して、想定される不可避な誤差とそれを防ぐのに必要な物理的リソースの関係を明らかにした。

交付額

(金額単位：円)

	直接経費	間接経費	合計
2005年度	3,600,000	0	3,600,000
2006年度	3,400,000	0	3,400,000
2007年度	3,400,000	1,020,000	4,420,000
2008年度	3,400,000	1,020,000	4,420,000
総計	13,800,000	2,040,000	15,840,000

研究分野：数物系科学

科研費の分科・細目：数学・数学一般(含確率論・統計数学)

キーワード：数理物理学，数学基礎論，量子測定，量子情報，量子計算，不確定性原理，量子集合論，量子確率論

## 1. 研究開始当初の背景

(1) 1994年に Shor のアルゴリズムが発見され、量子コンピュータにより従来の計算機では解決困難な問題が多項式時間で解決可能であることが示されて以来、量子情報一般に関する数学的基礎理論を確立する必要性が明らかになってきた。

(2) Shor のアルゴリズムでは、任意の基本的計算素子が完全なユニタリ変換を実現すると仮定されている。しかし、実際は環境からのデコヒーレンスによりその仮定は現実的でなく、量子誤り訂正によってそれらの誤りが訂正できなければならない。

(3) この問題に対し、誤り耐性量子計算理論によれば、量子ゲートの誤り確率がある閾値以下ならば、誤り訂正が可能であることが示されている。しかし、その閾値は  $10^{-5}$ ～ $10^{-6}$  と非常に厳しいので、実際にこのような高い精度で量子ゲートにおける量子状態制御が可能かどうかを理論的に究明する必要がある。

(4) この問題に対して、研究代表者はこれまでの研究で、量子ゲートの制御系と量子ゲートの間の相互作用によりある不可避な誤差がもたらされることを発見し、それをモデルによらないで相互作用が満たす保存法則だけから導く理論的方法を発見した。

(5) また、研究代表者は、量子測定の数学理論を構築し、測定精度と擾乱に関する **Heisenberg** の不確定性原理の不備を明らかにし、小澤の不等式と呼ばれる測定精度と擾乱に関する普遍的な関係式を発見し、厳密な量子測定理論のもとで証明した。

## 2. 研究の目的

(1) 量子ゲートの不可避な誤差をモデルによらないで相互作用が満たす保存法則だけから導く研究代表者の理論的方法を小澤の不等式に基づく普遍的な不確定性原理によって基礎付け、量子測定理論と量子計算理論を結びつける新しい数学理論を構築することを目標とする。

(2) この理論のもとで従来、**Wigner-Araki-Yanase** の定理として知られてきた保存則のもとでの測定不可能性の定性的議論を一般化した定量的理論を構成することを目標とする。

(3) また、この理論を応用して、量子計算の実現に伴う様々なモデルに対して、想定される不可避な誤差とそれを防ぐのに必要な物理的リソースを明らかにすることを目標とする。

(4) 目標とする数学理論の計算論的基礎を量子計算量理論によって明らかにし、また、数理物理学的基礎を作用素環論及び量子確率論の手法で明らかにする。

## 3. 研究の方法

(1) 研究課題を以下のテーマに分類して、研究代表者、研究分担者の役割分担を定める。

① 計算論的研究：量子計算の計算量的基礎を計算理論、数理論理学的手法で研究する。代表者、分担者・田中一之が担当し、協力者・西村治道と共同研究を行う。

② 解析的研究：量子計算の数学的基礎を作用素環論及び量子確率論の手法で研究する。代表者及び分担者・日合文雄、尾畑伸明、金子誠が担当する。

③ 力学的研究：量子ゲートを物理的に実現する上で現れる誤差を量子力学系の状態変化から研究する。代表者、分担者・堀田昌寛が担当し、協力者 **Gea-Banacloche** と共同研究を行う。

④ 量子情報理論的研究：量子ゲートに現れる誤差を量子情報理論的に考察して、不確定性原理や保存法則により現れる不可避の誤差限界を研究する。代表者が担当し、協力者 **H.P. Yuen** , **Gea-Banacloche** と共同研究を行う。

## 4. 研究成果

(1) 2005 年度の研究において以下の成果を得た。

① 小澤は、量子完全相関の概念を新たに導入して、様々な数学的特徴付けを与えた。量子情報理論への応用として、**Hardy**

非局所性不成立問題の説明が量子完全相関の推移性から得られることを示し、また、量子測定が被測定物理量とその表示物理量との量子完全相関を実現することを示した。

② 小澤は、河野らと共同で **DiVincenzo** らの 3 量子ビット・デコヒーレンス・フリーシステムにおける 19 ゲート列量子演算実現法を研究し、これまで未解決であった **CNOT** 演算を実現する制御パラメータの厳密解の存在を証明した。更に、19 ゲート列により実現可能なゲートの全体が制御回転ゲートと局所的同等なゲートの全体と一致することを証明し、一般の制御回転ゲートを実現する制御パラメータを明らかにした。

③ 日合は、多変数の非可換確率変数に対して自由圧力関数を定義し、その **Legendre** 変換によって多変数の新しい自由エントロピーを導入し、多変数の自由エントロピーに対する **Voiculescu** の 2 通りの方法（行列近似の方法と非可換 **Hilbert** 変換の方法）に加えて、第 3 の方法を提起した。

④ 尾畑は、共同研究者とブラウン運動を分解（時間微分＋量子分解）して得られる「量子ホワイトノイズ」を理論の出発点とし、非線形ホワイトノイズ方程式を目標として、量子ホワイトノイズを基礎とする作用素論を発展させた。

⑤ 堀田と小澤は、環境系との相互作用による微小雑音を記述する量子チャンネルに対する量子推定問題の研究を行い、ノイズによって乱された量子状態を測定するときノイズの大きさを最適に推定する方法を **Fisher** 情報量理論に基づいて与えた。更に、アンシラ系との量子もつれを使用したとき、どの程度推定改良がなされるかを議論し、キュービット系に対して達成可能な改良因子の上限を与えることに成功した。

(2) 2006 年度の研究において以下の成果を得た。

① 遅延情報を持つ量子推定問題である **Mean King** 問題に対して、従来は直交ラテン方陣を利用した一般的解の構成法が知られていたが、これは任意レベルの問題に対して解の存在を保証しない。木村、田中、小澤は、直交配置を利用した解を構成して、任意レベルで常に解が存在することを示した。

② 小澤は、量子測定と量子オペレーションにおける誤差と擾乱の間の不確定性関係に関する新しい結果を示し、誤差のない位置測定において、運動量の擾乱をいくらかでも小さくできることを明らかにした。

- ③ **Gea-Banacloche** と小澤は、量子論理ゲートを実現するために量子化された電磁パルスで多くの量子系を同時に制御する場合に、誤差を軽減するために必要なエネルギーをそれらの系の間で共有することができないことを示した。
- ④ 量子 NOT ゲートを物理的に実装する際に不可避な誤差が現れるかどうかは、未解決だったが、唐澤と小澤は、新しい手法で制御系のサイズに反比例する誤差が現れることを示した。
- ⑤ 小澤は、一般の von Neumann 環の射影束を論理とする集合論を初めて展開し、ZFC の定理から量子集合論において真な命題を生成するための移行原理を確立した。これにより、量子集合論における実数と量子観測量が一対一に対応すること、量子相関が集合論の言語で記述できることなどを示した。
- ⑥ 日合, **Petz**, 植田は、ランダム行列近似の手法と特殊ユニタリ群の固有値分布に対する大偏差原理を用いて、単位円周上の確率測度に対する自由確率論的な対数ソボレフ不等式を証明した。

(3) 2007 年度の研究において以下の成果を得た。

- ① これまでの研究で、スピン量子ビット上のアダマール・ゲート、否定ゲートなどを角運動量保存法則のもとで実装する場合のゲート非忠実度（1 からゲート忠実度の 2 乗を引いた値）の一般的な下限が得られたが、本研究において、唐澤と小澤は、任意の自己共役ゲート（1 量子ビットの自己共役なユニタリ変換）の任意の保存法則のもとでの実装に関するゲート非忠実度の一般的な下限を得た。この結果により、スピン 1/2 の量子ビット上の任意の自己共役ゲートを  $N$  量子ビットのアンシラ、または、スピン  $N/2$  系のアンシラと回転不変な相互作用で実装すると非忠実度が  $1/(4+4N^2)$  以上になることが導かれる。
- ② 木村, **Meister**, 小澤は、測定相互作用に関する加法的保存量と非可換な物理量の正確な測定の不可能性を示す **Wigner-Araki-Yanase** の定理を乗法的保存量に拡張して、乗法的保存量と非可換な物理量の正確な測定の不可能性を証明した。更に、乗法的保存量が存在する場合の測定における平均 2 乗誤差の下限を求め、誤差を小さくするためには、加法的保存量の場合には装置系に含まれる保存量の分散を小さくする必要があったが、乗法的保存量の場合には変動係数（相対揺らぎ）を小さくする必要があることを明らかにした。
- ③ 日合, **Mosonyi**, 小川は、スピン・チェ

イン上の並行移動不変な有限距離の相互作用のギブス状態に対して大偏差原理を証明し、さらに、スピン・チェーン上の相関のあるギブス状態や有限相関状態に対して、量子仮説検定のチャーノフ型、ヘフディング型、シュタイン型の誤り確率の漸近挙動を統一的な方法で明らかにした。

(4) 2008 年度の研究において以下の成果を得た。

- ① 唐澤, **Gea-Banacloche**, 小澤は、任意のユニタリゲートの任意の保存法則のもとでの実装に関するゲート忠実度の一般的上限を得て、それがブロッホ球における保存量とユニタリゲートの幾何学的関係と制御系のサイズに依存することを示した。
- ② 量子チューリング機械と一様量子回路族の計算量的同等性は、量子計算量理論の基本問題であるが、これまで **BQP** クラス以外の **EQP** や **ZQP** クラスに対しては未解決であった。西村と小澤は、有限生成一様量子回路族という新しい回路族のクラスを定めて、量子チューリング機械と有限生成一様量子回路族が完全に計算量的に同等であり、**BQP**, **EQP**, **ZQP** 等、全ての対応する計算量クラスに対して計算量的同等性が成立することを示した。
- ③ 日合グループは、自由確率、量子情報理論について研究し、以下の成果を得た。(1)射影作用素に対して自由エントロピーを導入し、2つの射影作用素の自由エントロピーと相互自由フィッシャー情報量の間に対数ソボレフ型不等式を示した。(2)量子共分散と量子フィッシャー情報量との関係を考察し、不確定性原理と関連して知られていた不等式を一般化した。(3)サイト間に相関がある **KMS** 状態と有限相関状態に対する量子仮説検定について、各種の漸近エラー限界に関する統一的な研究を行った。
- ④ 尾畑グループは、ボゾンフォック空間上の非有界作用素の生成・消滅作用素に関する微分を導入し、それらの双対として従来の量子確率積分を拡張し、量子マルチンゲール表現定理や作用素の量子確率積分表示を得た。
- ⑤ 田中グループは、ランダム性に関する計算量的研究を行い、無限列およびランダム実数の計算量変動、及び、部分ランダム性の諸定義の擬同値性に関する成果を得た。
- ⑥ 堀田は、**LOCC** と基底状態の量子もつれを用いてエネルギーを転送できる量子プロトコル、量子エネルギーテレポーテーションを提案した。

5. 主な発表論文等

(研究代表者, 研究分担者及び連携研究者には下線)

[雑誌論文] (計 43 件)

- [1] T. Karasawa, M. Ozawa, and K. Nemoto, Theoretical constraints on implementations of arbitrary single-qubit gates under conservation laws, AIP Conference Proceedings 1110, 411-414 (2009). 査読有.
- [2] M. Hotta and M. Ozawa, A Protocol of Quantum Authentication with Secure Quantum Passwords, AIP Conference Proceedings 1110, 388-391 (2009). 査読有.
- [3] T. Karasawa, J. Gea-Banacloche, and M. Ozawa, Gate fidelity of arbitrary single-qubit gates constrained by conservation laws, J. Phys. A: Math. Theor. 42, 225303 (1-16) (2009). 査読有.
- [4] H. Nishimura and M. Ozawa, Perfect computational equivalence between quantum Turing machines and finitely generated uniform quantum circuit families, Quantum Inf. Process. 8, 12-24 (2009). 査読有
- [5] T. Karasawa, M. Ozawa, J. Gea-Banacloche, and K. Nemoto, Quantum precision limits for any implementation of single qubit gates under conservation laws, Int. J. Quant. Inf. 6, 701-706 (2008). 査読有
- [6] G. Kimura, B.K. Meister, and M. Ozawa, Quantum limits of measurements induced by multiplicative conservation laws: Extension of the Wigner-Araki-Yanase Theorem, Phys. Rev. A 78, 032106 (1-7) (2008). 査読有.
- [7] F. Hiai, M. Mosonyi and T. Ogawa, Error exponents in hypothesis testing for correlated states on a spin chain, Journal of Mathematical Physics 49 (2008) 007803 (1-22). 査読有.
- [8] M. Mosonyi, F. Hiai, T. Ogawa and M. Fannes, Asymptotic distinguishability measures for shift-invariant quasi-free states of fermionic lattice systems, Journal of Mathematical Physics 49 (2008) 072104 (1-11). 査読有.
- [9] F. Hiai and Y. Ueda, A log-Sobolev type inequality for free entropy of two projections, Ann. Inst. H. Poincaré Probab. Statist. 45 (2009) 239-249. 査読有.
- [10] P. Gibilisco, F. Hiai and D. Petz, Quantum covariance, quantum Fisher information and the uncertainty principle, IEEE Trans. Inform. Theory 55 (2009) 439-443. 査読有.
- [11] F. Hiai and D. Petz, Riemannian metrics on positive definite matrices related to means, Linear Algebra Appl. 430 (2009) 3105-3130. 査読有.
- [12] U. C. Ji and N. Obata, Annihilation-derivative, creation-derivative and representation of quantum martingales, Commun. Math. Phys. 286 (2009) 751-775. 査読有.
- [13] U. C. Ji and N. Obata, Quantum stochastic integral representations of Fock space operators, Stochastics (2009) 掲載決定. 査読有.
- [14] C.G. Liu, K. Tanaka, and T. Yamazaki, Generalization of complexity oscillations in infinite sequences, 4rd International Conference on Natural Computation (ICNC'08), IEEE (2008) 299-303. 査読有.
- [15] C.G. Liu, K. Tanaka, and T. Yamazaki, The quasi-equivalence between the definitions of partial randomness, 4rd International Conference on Natural Computation (ICNC'08), IEEE (2008) 371-375. 査読有.
- [16] C.G. Liu and K. Tanaka, Complexity Oscillations in Random Reals, IEICE Transactions on Information and Systems 91 (2008) 2517-2518. 査読有.
- [17] M. Hotta, Quantum measurement information as a key to energy extraction from local vacuums, Physical Review D 78 (2008) 045006 (1-9). 査読有.
- [18] M. Hotta and T. Karasawa, Channel estimation theory of low-noise multiple parameters: Attainability problem of the Cramér-Rao bounds, Physical Review A 78 (2008) 012332(1-10). 査読有.
- [19] A. Hora and N. Obata, Asymptotic spectral analysis of growing regular graphs, Trans. Amer. Math. Soc. 36 (2008) 899-923. 査読有.
- [20] M. Ozawa, Simultaneous measurability of non-commuting observables and the universal uncertainty principle, Proc. 8th Int. Conf. on Quantum Communication,

- Measurement and Computing, NICT Press, Tokyo, 363-368 (2007). 査読有.
- [21] M. Hotta, T. Karasawa, K. Matsumoto, and M. Ozawa, Low-noise channel estimation, Proc. 8th Int. Conf. on Quantum Communication, Measurement and Computing, NICT Press, Tokyo, 319-322 (2007). 査読有.
- [22] G. Kimura, H. Tanaka, and M. Ozawa, Comments on “Best conventional solutions to the King’s problem,” Z. Naturforsch. 62a, 152-156 (2007). 査読有.
- [23] M. Ozawa, Transfer principle in quantum set theory, J. Symbolic Logic 72, 625-648 (2007). 査読有.
- [24] T. Karasawa, and M. Ozawa, Conservation-law-induced quantum limits for physical realizations of the quantum NOT gate, Phys. Rev. A 75, 032324 (2007). 査読有.
- [25] I. Csiszar, F. Hiai, and D. Petz, A limit relation for entropy and channel capacity per unit cost, J. Math. Phys. 48 (2007) 092102 (1-10). 査読有.
- [26] F. Hiai, M. Mosonyi, and T. Ogawa, Large deviations and Chernoff bound for certain correlated states on a spin chain, J. Math. Phys. 48 (2007) 123301 (1-19). 査読有.
- [27] Y. Kawano and M. Ozawa, Quantum gates generated by rotationally invariant operators in a decoherence-free subsystem, Phys. Rev. A 73, 012339 (1-8) (2006). 査読有.
- [28] R. Rahimi, K. Takeda, M. Ozawa, and M. Kitagawa, Entanglement witness derived from NMR superdense coding, J. of Phys. A: Math. Gen. 39, 2151-2159 (2006). 査読有.
- [29] M. Ozawa, Quantum perfect correlations, Annals of Physics 321, 744-769 (2006). 査読有.
- [30] G. Kimura, H. Tanaka, and M. Ozawa, Solution to the mean King’s problem with mutually unbiased bases for arbitrary levels, Phys. Rev. A 73, 050301(R) (1-4) (2006). 査読有.
- [31] M. Ozawa, Noise and disturbance in quantum measurements and operations, Proceedings of SPIE 6244, 62440Q (1-9) (2006). 査読有.
- [32] M. Ozawa, Defense of “Impossibility of distant indirect measurement of the quantum Zeno effect,” Phys. Lett. A 356, 411-413 (2006). 査読有.
- [33] M. Hotta, T. Karasawa, and M. Ozawa, N-body-extended channel estimation for low-noise parameters, J. Phys. A: Math. Gen. 39, 14465-14470 (2006). 査読有.
- [34] J. Gea-Banacloche and M. Ozawa, Minimum-energy pulses for quantum logic cannot be shared, Phys. Rev. A 74, 060301(R) (1-4) (2006). 査読有.
- [35] F. Hiai, D. Petz and Y. Ueda, A free logarithmic Sobolev inequality on the circle, Canad. Math. Bull. 49 (2006) 389-406. 査読有.
- [36] F. Hiai and Y. Ueda, Free transportation cost inequalities for non-commutative multi-variables, Infinite Dimensional Analysis, Quantum Probability and Related Topics 9 (2006) 391-412. 査読有.
- [37] F. Hiai and D. Petz, Large deviations for functions of two random projection matrices, Acta Sci. Math. (Szeged) 72 (2006) 581-609. 査読有.
- [38] M. Ozawa, Universal uncertainty principle in measurement operator formalism, J. Opt. B: Quantum Semiclass. Opt. 7, S672-S681 (2005). 査読有.
- [39] M. Hotta, T. Karasawa, and M. Ozawa, Ancilla-assisted enhancement of channel estimation for low-noise parameters, Phys. Rev. A 72, 052334 (1-11) (2005). 査読有.
- [40] J. Gea-Banacloche and M. Ozawa, Constraints for quantum logic arising from conservation laws and field fluctuations, J. Opt. B: Quantum Semiclass. Opt. 7, S326-S332 (2005). 査読有.
- [41] Y. Kawano, K. Kimura, H. Sekigawa, M. Noro, K. Shirayanagi, M. Kitagawa, and M. Ozawa, Existence of the exact CNOT on a quantum computer with the exchange interaction, Quantum Inf. Process. 4, 65-85 (2005). 査読有.
- [42] F. Hiai, Free analog of pressure and its Legendre transform, Comm. Math. Phys. 255, 229-252 (2005). 査読有.
- [43] N. Akiho, F. Hiai and D. Petz, Equilibrium states and their entropy densities in gauge-invariant C\*-systems, Rev. Math. Phys. 17, 365-389 (2005). 査読有.

〔学会発表〕(計7件)

- [1] M. Ozawa, Quantum measurement theory: mathematical and conceptual foundations, UK-Japan Quantum Information Workshop, 23 January 2009, Tokyo, Japan.
- [2] M. Ozawa, Uncertainty Principle, Conservation Laws, and the Size of Quantum Controllers, Workshop: Osamu Hirota, A True Quantum Communications, 26 June 2008, Waterloo, Canada.
- [3] M. Ozawa, Classification of Quantum Instruments, 28th Conference on Quantum Probability and Related Topics, 6 September 2007, Guanajuato, Mexico.
- [4] M. Ozawa, Simultaneous measurability and uncertainty principle, Workshop on Theory of Quantum Computation, Communication and Cryptography (TQC2006), 23 February 2006, Atsugi, Japan.
- [5] M. Ozawa, Universal Uncertainty Principle and Quantum State Control,” Satellite Symposium of XIIth International Congress of Quantum Chemistry Material-oriented Quantum Chemistry, 28 May 2006, Osaka, Japan.
- [6] M. Ozawa, Simultaneous measurability of non-commuting observables and the universal uncertainty principle, 8th International Conference on Quantum Communication, Measurement and Computing, (QCMC2006), 29 November 2006, Tsukuba, Japan.
- [7] M. Ozawa, Operational Uncertainty Relations: Recent Development, 9 th International Conference on Squeezed States and Uncertainty Relations, 2-6 May 2005, Besancon, France.

〔産業財産権〕

○出願状況 (計2件)

- [1] 名称: 量子認証方法, 量子認証システム及び量子認証装置  
発明者: 小澤正直, 堀田昌寛  
権利者: 東北大学

種類: 特許

番号: 特願 2007-255159, 特開 2009-88916  
出願年月日: 2007年9月28日  
国内外の別: 国内

[2] 名称: 制御回転ゲート, その決定装置, その決定方法, そのプログラム及びその記録媒体

発明者: 河野泰人, 小澤正直

権利者: NTT, 東北大学

種類: 特許

番号: 特願 2006-202080, 特開 2008-28320  
出願年月日: 2006年7月25日  
国内外の別: 国内

## 6. 研究組織

### (1)研究代表者

小澤 正直 (Masanao Ozawa)

名古屋大学・大学院情報科学研究科・教授

研究者番号: 40126313

### (2)研究分担者 (2005年度~2007年度)

日合 文雄 (Fumio Hiai)

東北大学・大学院情報科学研究科・教授

研究者番号: 30092571

尾畑 伸明 (Nobuaki Obata)

東北大学・大学院情報科学研究科・教授

研究者番号: 10169360

田中 一之 (Kazuyuki Tanaka)

東北大学・大学院理学研究科・教授

研究者番号: 70188291

堀田 昌寛 (Masahiro Hotta)

東北大学・大学院理学研究科・助手

研究者番号: 60261541

金子 誠 (Makoto Kaneko)

東北大学・大学院情報科学研究科・教授

研究者番号: 10007172

### (3)連携研究者 (2008年度)

日合 文雄 (Fumio Hiai)

東北大学・大学院情報科学研究科・教授

研究者番号: 30092571

尾畑 伸明 (Nobuaki Obata)

東北大学・大学院情報科学研究科・教授

研究者番号: 10169360

田中 一之 (Kazuyuki Tanaka)

東北大学・大学院理学研究科・教授

研究者番号: 70188291

堀田 昌寛 (Masahiro Hotta)

東北大学・大学院理学研究科・助手

研究者番号: 60261541