

令和 6 年 6 月 10 日現在

機関番号：33910

研究種目：基盤研究(C)（一般）

研究期間：2021～2023

課題番号：21K11764

研究課題名（和文）量子古典ハイブリッドアルゴリズムを用いた機械学習

研究課題名（英文）Machine Learning using Quantum-Classical Hybrid Algorithms

研究代表者

河野 泰人（Kawano, Yasuhito）

中部大学・理工学部・教授

研究者番号：40396180

交付決定額（研究期間全体）：（直接経費） 3,100,000円

研究成果の概要（和文）：機械学習から派生した組み合わせ最適化問題として知られるLWE問題の量子古典ハイブリッドシステムを用いた解法を研究した。まず、LWE問題を最大独立集合問題に変換する古典アルゴリズムを開発した。この古典アルゴリズムを計算サーバに実装し、40次元のLWEチャレンジ問題を量子アニーリングマシン上で解くために必要な量子ビット数が約4万であることを示した。さらに、開発した古典アルゴリズムを改良し、ゲート型量子コンピュータでLWE問題を解く量子古典ハイブリッドアルゴリズムを開発した。

研究成果の学術的意義や社会的意義

量子コンピュータは重ね合わせ状態が利用できるため、人工知能や機械学習で扱う組み合わせ最適化問題が得意であると予想されている。本研究では、代表的な組み合わせ最適化問題として知られるLWE問題を解く量子古典ハイブリッドアルゴリズムを新たに開発した。本研究で得られた量子古典ハイブリッドアルゴリズムを量子古典ハイブリッドシステムに実装することにより、人工知能や機械学習への応用が期待できる。

研究成果の概要（英文）：We have been studying a method for solving the LWE problem, which is known as a combinatorial optimization problem derived from machine learning, using a quantum-classical hybrid system. First, we developed a classical algorithm to convert an LWE problem into a set of maximum independent set problems. We implemented this classical algorithm on a classical computer and demonstrated that the number of qubits required to solve a 40-dimensional LWE challenge problem on a quantum annealing machine is approximately 40,000. Next, we improved the classical algorithm and developed a quantum-classical hybrid algorithm to solve the LWE problem on a gate-type quantum computer.

研究分野：量子情報科学

キーワード：量子コンピュータ 量子アルゴリズム 機械学習 人工知能 LWE問題 組み合わせ最適化問題 耐量子暗号 次世代公開鍵暗号

科研費による研究は、研究者の自覚と責任において実施するものです。そのため、研究の実施や研究成果の公表等については、国の要請等に基づくものではなく、その研究成果に関する見解や責任は、研究者個人に帰属します。

1. 研究開始当初の背景

2019年、Googleは量子超越性の実証実験に成功し、特定の問題に対して量子コンピュータ専用アルゴリズムを用いれば古典コンピュータよりも高速に計算できることを示した。しかし、この研究で使用された問題(ランダム回路のサンプリング問題)の応用範囲は限定的で、たとえば人工知能や機械学習で研究される「組み合わせ最適化問題」などの、広範囲に応用可能な問題に対する量子超越性の実現および実社会への応用が望まれていた。

2. 研究の目的

本科学研究の目的は、組み合わせ最適化問題などの実用的な問題に対する量子古典ハイブリッドアルゴリズムを開発し、計算効率に関する理論的な解析と、量子コンピュータおよび古典コンピュータ上での実装により、実社会に応用可能な量子古典ハイブリッドシステムを構築することである。

3. 研究の方法

組み合わせ最適化問題の一種として知られるLWE問題と呼ばれる問題に注目し、この問題を解く量子古典ハイブリッドアルゴリズムを開発する。LWE問題に注目するのは、以下の理由による。

1. LWE問題は機械学習から派生した問題であるため、開発した量子古典ハイブリッドアルゴリズムが機械学習に応用しやすい
2. LWE問題は次世代の公開鍵暗号候補に利用されており、暗号の安全性を保障する鍵長の計算に利用できる
3. Darmstadt大学が提供するLWEチャレンジ問題により、古典コンピュータと性能を比較しやすい。LWEチャレンジの古典コンピュータによる未解決問題が、開発した量子古典ハイブリッドシステムで解決できれば、量子超越性が結論できる

LWE問題を解く量子古典ハイブリッドシステムを、以下の3段階で開発する。

第1段階では量子アニーリングマシンの使用を想定した量子古典ハイブリッドシステムを構築する。第1段階で量子アニーリングマシンの使用を前提にシステムが構築されるのは、以下の理由による。

1. ゲート型量子コンピュータより量子アニーリングマシンの方が現時点で利用できる量子ビット数が多く、LWE問題のエンコードが容易である
2. 量子アニーリングマシンの場合、量子アルゴリズムを作る必要がなく、研究途中の結果を論文にまとめやすい

現在使用できる量子コンピュータの量子ビット数はLWE問題に比べて少ないため、LWE問題の分割が必須となる。第1段階における量子古典ハイブリッドシステムでは、この分割アルゴリズムの研究が主要な研究テーマとなる。量子アニーリングマシンはゲート型量子コンピュータに比べるとたくさんの量子ビットが使用できるが、古典コンピュータと比べて速く計算できるという理論的な保証はない。

第2段階では、第1段階で開発したシステムを拡張し、量子アニーリングマシンの代わりにゲート型量子コンピュータの使用を想定したシステムを構築する。第2段階においては、分割したLWE問題をゲート型量子コンピュータで解く量子アルゴリズム(量子回路)の開発が必要になる。現在、ゲート型量子コンピュータは量子アニーリングよりも量子ビット数が少なく、大規模な計算を長時間実行する場合は量子エラー訂正が必要となるが、量子アルゴリズムの設計自由度が高く、計算量の理論的評価もしやすいという利点がある。現在、量子コンピュータのハードウェア開発競争においてもゲート型量子コンピュータが中心となっており、実用的なシステム開発においてゲート型量子コンピュータを用いた量子古典ハイブリッドシステムの研究が必須である。

第3段階では、第1,2段階で開発したシステムを古典コンピュータおよび量子コンピュータ上で実装し、LWEチャレンジ問題を利用して量子コンピュータの超越性を実証する。この段階では理論研究を離れてハードウェア上での実装が必要である。古典コンピュータにおける実装は計算サーバを用いて行い、量子アニーリングマシンおよびゲート型量子コンピュータにおける実装は古典コンピュータによるシミュレーションを行う。

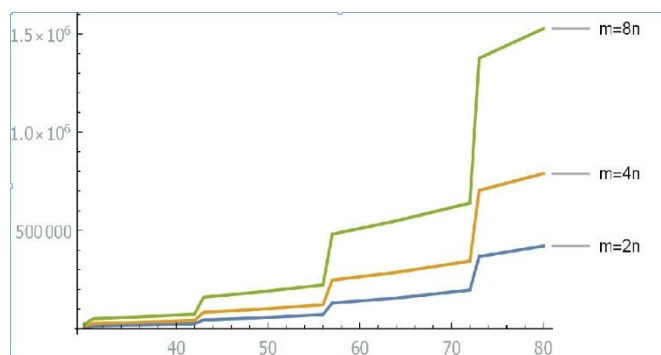
4. 研究成果

研究の結果、以下の成果を得た。

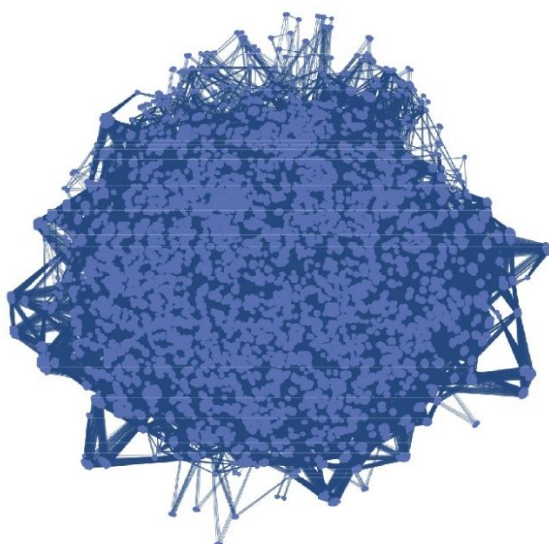
量子アニーリングマシンを用いて LWE 問題を解く量子古典ハイブリッドアルゴリズムを開発した。

- LWE 問題を別の LWE 問題に帰着する (LWE 帰着と呼ぶ) 古典アルゴリズムを開発した。このアルゴリズムのパラメータを変えることにより、与えられた LWE 問題を様々な別の LWE 問題に帰着できる。このアルゴリズムを使うと、LWE 問題のパラメータ変更や分割が可能になる。
- LWE 帰着を 2 回用いて、LWE 問題を独立最大集合問題(Maximum Independent Set problem, MIS)に帰着するアルゴリズムを開発した。帰着する過程で LWE 問題を分解するため、LWE 問題を単純にエンコードするよりも少ない量子ビット数でコーディングできる。ただし、多項式時間の帰着ではない。
- MIS を QUBO(Quadratic Unconstrained Binary Optimization problem)と呼ばれる問題に帰着する。ここで、QUBO は量子アニーリングマシン上で解ける問題である。この帰着は既知のアルゴリズムを使用する。
- 得られた QUBO を量子アニーリングマシンを用いて解く。
- 量子アニーリングマシンで得られた解から元の LWE 問題の解を計算する。

以上の量子古典ハイブリッドアルゴリズムで n 次元 LWE 問題を解いた場合、必要な量子ビット数は $2^{O(\sqrt{n})}$ であることを示した。すなわち、次元の準指数個の量子ビットを用いれば解が得られることが期待できる。下のグラフは次元に対して必要な最小量子ビット数を計算した例である。 n は次元数、 m はサンプル数を意味し、グラフの縦軸は必要な量子ビットの最小数である。



グラフから、LWE チャレンジ問題の最小次元 (40 次元) 問題を解く場合に必要な最小量子ビット数は約 40000 であることがわかる。下のグラフは、開発した帰着アルゴリズムを古典コンピュータに実装して 40 次元の LWE チャレンジ問題を MIS 問題に帰着した結果である。



グラフの頂点数は 36,664、結線数は 1,982,176 である。この MIS 問題は 10 万ノードの量子アニーリングマシンでコーディング可能なので、LWE チャレンジ問題の最小次元問題は、近い将来、量子コンピュータの射程圏内に入ることが予想される。

5. 主な発表論文等

〔雑誌論文〕 計4件（うち査読付論文 4件/うち国際共著 1件/うちオープンアクセス 3件）

1. 著者名 Kawano Yasuhito	4. 巻 13
2. 論文標題 A reduction from an LWE problem to maximum independent set problems	5. 発行年 2023年
3. 雑誌名 Scientific Reports	6. 最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.1038/s41598-023-34366-7	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 -
1. 著者名 Ozawa Masanao	4. 巻 394
2. 論文標題 Logical Characterization of Contextual Hidden-Variable Theories based on Quantum Set Theory	5. 発行年 2023年
3. 雑誌名 Electronic Proceedings in Theoretical Computer Science	6. 最初と最後の頁 1~12
掲載論文のDOI（デジタルオブジェクト識別子） 10.4204/EPTCS.394.1	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 -
1. 著者名 Ozawa Masanao	4. 巻 -
2. 論文標題 Quantum Measurement Theory for Systems with Finite Dimensional State Spaces	5. 発行年 2023年
3. 雑誌名 The Quantum-Like Revolution: A Festschrift for Andrei Khrennikov. A. Plotnitsky, E. Haven (eds.). Springer, Cham.	6. 最初と最後の頁 191~214
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-12986-5_9	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 Masanao Ozawa, Andrei Khrennikov	4. 巻 112
2. 論文標題 Nondistributivity of human logic and violation of response replicability effect in cognitive psychology	5. 発行年 2023年
3. 雑誌名 Journal of Mathematical Psychology	6. 最初と最後の頁 102739
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.jmp.2022.102739	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18件（うち招待講演 12件 / うち国際学会 5件）

1. 発表者名 河野泰人
2. 発表標題 量子アルゴリズム2「量子位相推定アルゴリズム」
3. 学会等名 2023年度 量子コンピュータ・ハンズオンワークショップ（招待講演）
4. 発表年 2024年

1. 発表者名 Yasuhito Kawano
2. 発表標題 A reduction from an LWE problem to maximum independent set problems
3. 学会等名 Chubu University International Symposium 2023
4. 発表年 2023年

1. 発表者名 小澤正直
2. 発表標題 不完全性定理から誤り耐性型汎用量子コンピュータへ:歴史的俯瞰
3. 学会等名 ムーンショット目標 6 誤り耐性型汎用量子コンピュータの実現に向けた数理科学ワークショップ（招待講演）
4. 発表年 2023年

1. 発表者名 Masanao Ozawa (presenter), Andrei Khrennikov
2. 発表標題 Quantum Instruments in Cognitive Science: Question Order Effect and Non-Bayesian Belief Update
3. 学会等名 'Category Theory for Consciousness Science' Workshop (国際学会)
4. 発表年 2023年

1. 発表者名 Masanao Ozawa
2. 発表標題 Quantum Perfect Correlations, Measurement, and Disturbance
3. 学会等名 The 23rd International conference on Quantum Foundations, Quantum Information and Probability: from Foundations to Engineering (QIP23) (招待講演) (国際学会)
4. 発表年 2023年

1. 発表者名 Masanao Ozawa
2. 発表標題 Sensation, Perception, Quantum Instruments, and Question Order Effect
3. 学会等名 3rd Quantum Cognition Workshop at QST (QCW 2023) (招待講演)
4. 発表年 2023年

1. 発表者名 Masanao Ozawa
2. 発表標題 Quantum instrument models in cognitive science: question order effect and non-Bayesian belief update
3. 学会等名 4th Models of Consciousness conference (MoC4) (国際学会)
4. 発表年 2023年

1. 発表者名 Masanao Ozawa
2. 発表標題 Quantum root-mean-square error and disturbance
3. 学会等名 Chubu Quantum Workshop 2023: New developments in quantum instrument theory (招待講演)
4. 発表年 2023年

1. 発表者名 Masanao Ozawa
2. 発表標題 Modeling question order effect with quantum instruments: Towards measurement theory of minds and consciousness
3. 学会等名 Workshop on Quantum-Like Revolution 2023 (招待講演)
4. 発表年 2023年

1. 発表者名 小澤 正直
2. 発表標題 量子インストルメント理論の展開: 量子測定から量子認知へ
3. 学会等名 RIMS 共同研究 (公開型) 量子場の数理とその周辺 (招待講演)
4. 発表年 2023年

1. 発表者名 小澤 正直
2. 発表標題 量子インストルメント理論
3. 学会等名 第2回数理の勉強会 (理化学研究所) (招待講演)
4. 発表年 2024年

1. 発表者名 Masanao Ozawa
2. 発表標題 The Value Reproducibility and the Intersubjectivity of Quantum Measurements based on the Theory of Quantum Perfect Correlations
3. 学会等名 International Conference on Photonics, Quantum Information, and Quantum Communication (招待講演)
4. 発表年 2024年

1. 発表者名 小澤 正直
2. 発表標題 不確定性原理と量子測定
3. 学会等名 量子科学技術研究開発機構 量子生命科学研究所 特別講義1 (招待講演)
4. 発表年 2024年

1. 発表者名 小澤 正直
2. 発表標題 質問順序効果と量子認知
3. 学会等名 量子科学技術研究開発機構 量子生命研究所 特別講義 (招待講演)
4. 発表年 2024年

1. 発表者名 小澤 正直
2. 発表標題 量子コンピュータ研究の歴史的俯瞰
3. 学会等名 2023年度 量子コンピュータ・ハンズオンワークショップ (招待講演)
4. 発表年 2024年

1. 発表者名 Masanao Ozawa
2. 発表標題 Logical Characterization of Contextual Hidden-Variable Theories based on Quantum Set Theory
3. 学会等名 19th International Conference on Quantum Physics and Logic (QPL 2022) (国際学会)
4. 発表年 2022年

1. 発表者名 Haruki Emori, Masanao Ozawa, Akihisa Tomita
2. 発表標題 Disturbance Evaluation Circuit in Quantum Measurement
3. 学会等名 Asian Conference on Quantum Information Science 2022 (AQIS 2022) (国際学会)
4. 発表年 2022年

1. 発表者名 河野泰人
2. 発表標題 Quantum-Classical Hybrid Algorithm for LWE Problems
3. 学会等名 電子情報通信学会第44回量子情報技術研究会 (QIT44)
4. 発表年 2021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
研究 分担 者	小澤 正直 (Ozawa Masanao) (40126313)	中部大学・AI数理データサイエンスセンター・特任教授 (33910)	

7. 科研費を使用して開催した国際研究集会

〔国際研究集会〕 計0件

8. 本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関
---------	---------