データ工学のための量子コンピューティング

齋藤 和広† 別府 翔平† 黒川 茂莉† 山城 悠‡ 伊神 皓生† 成定 真太郎†

†株式会社 KDDI 総合研究所 〒356-8502 埼玉県ふじみ野市大原二丁目 1 番 15 号
‡株式会社 Jij 〒113-0031 東京都文京区根津 1-4-6 SB ビル 7F

E-mail: †{ku-saitou, sh-beppu, mo-kurokawa, ak-ikami, sh-narisada}@kddi.com, ‡y.yamashiro@j-ij.com

あらまし ムーアの法則の限界から従来のコンピュータの成長限界が見え始め，次世代のコンピュータの候補の一つとして量子コンピュータが注目されている． 量子コンピュータは，量子力学的な現象によって 0 と 1 の得られる確率で状態を表現する「量子ビット」を利用し，複数の情報を重ね合わせて同時並列的に計算を行う． 量子コンピュータの利用者は，この量子ビットの特性を有効活用した量子アルゴリズムを設計することで，大規模な計算を高速に解くことができる． 化学や金融の領域ではシミュレーションなどの大規模な計算において活用が検討されており，データ工学の領域においても，量子コンピュータの活用によるさらなる発展が期待できる．本チュートリアルでは，量子コンピューティングに関する基礎技術から始まり，データ工学に関連する量子アルゴリズムとして，量子機械学習手法，組合せ最適化問題の解法（量子アニーリング含む），及びデータ探索手法を紹介する．

キーワード 量子コンピューティング，機械学習，組合せ最適化，データ探索

1. はじめに

古典コンピュータは，0 か 1 のいずれかの状態を持つ「ビット」を利用して情報を表現し，逐次的に計算を行う．大規模な計算では，スーパーコンピュータなど多数の古典コンピュータを利用して並列計算する．一方，量子コンピュータは，量子力学的な現象によって，0 と 1 の得られる確率で状態を表現する「量子ビット」を利用し，複数の情報を重ね合わせて同時並列的に計算を行う．これにより n 量子ビットを備える量子コンピュータは，一度に最大 2^n 回計算できる．したがって，量子コンピュータは，量子ビットの数を増やすことで，古典コンピュータで実現できない超並列計算を実現することが期待される．

量子コンピュータの概念は，1985 年に理論的に定式化された[1]．その後，限定的な用途の量子コンピュータとして，D-Wave Systems により量子アニーリングマシン[2]が世界で初めて開発された．量子アニーリングマシンは，組合せ最適化問題の近似解を高速に解く汎用ソルバーとして活用検討が進められている．更に，古典コンピュータのように汎用的に利用可能な量子コンピュータも様々な実装方式で開発が進められ[3]，小規模な量子ビット数ながらクラウドを介して利用できる．

量子コンピュータの用途は，古典コンピュータで計算が困難もしくは長時間を要する計算があげられ，最適化問題，シミュレーション，AI，セキュリティなどが想定されている[4]．本チュートリアルでは，量子コンピュータを利用する方法として量子コンピューティングの概要を紹介し，特にデータ工学で重要な用途として，量子コンピュータにおける機械学習，組合せ最適化，及びデータ探索のアルゴリズムを解説する．

2. 量子コンピューティング概要

量子コンピュータは，量子ビットが持つ量子重ね合わせの特性を活用して，古典コンピュータに対する優位性を得る．量子ビットにおける 0 と 1 の重ね合わせ状態は，二つの複素ベクトルα,βを用いて表現される．$|\alpha|^2$が 0 を得る確率，$|\beta|^2$が 1 を得る確率を表し，$|\alpha|^2+|\beta|^2=1$が規格化条件である．古典ビットにおける 0 は$\alpha=1,\beta=0$となり，1 は$\alpha=0,\beta=1$となる．量子ビットψの状態ベクトルは，ブラケット表記によって以下のように表現される．

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

ここで$|0\rangle$は古典ビットにおける 0，$|1\rangle$は古典ビットにおける 1 に対応する．

量子ビットに対する演算は量子ゲートと呼ばれ，量子ビットの状態ベクトルを操作する．一つの量子ビットに対する量子ゲートの例として，0 と 1 の得られる確率を反転する X ゲートがあり，古典ビットの NOT ゲートに対応する．他に，重ね合わせ状態を作るアダマールゲート（H ゲート）など，量子コンピュータ固有の演算子も存在する．古典ビットにおける AND ゲートや OR ゲートのように，複数の量子ビットに対して作用する量子ゲートも存在する．

量子ゲート操作の後に，量子ビットを測定することで出力結果を取り出す．このとき，出力結果は確率的であり，確率$|\alpha|^2$で 0 が得られ，確率$|\beta|^2$で 1 が得られる．つまり，所望の出力（例えば最適化問題の解となるビット値）が一度の測定で得られるとは限らない．意図した出力を高確率で得るよう設計された量子コンピュータ専用のアルゴリズムは，量子アルゴリズムと呼ばれる．量子アルゴリズムは量子ゲートを並べた量子回路として実装される．量子アルゴリズムの性能が，

同じ問題で最も良い性能の古典アルゴリズムを上回ることを量子加速 (quantum speedup) と呼び，多くの量子アルゴリズムで理論的に量子加速が証明されている[5]. 図 1 は，代表的な量子アルゴリズムの一つであるアダマールテストの量子回路である．各横線が量子ビット，箱が量子ゲートを表し，左から順に量子ゲートが対応する量子ビットに作用し，一番右のメーターの箱でその量子ビットを測定する.アダマールテストは，任意の量子ビット列$|\psi\rangle$に対して量子ゲート U を作用させたときの期待値を推定する.

量子コンピュータの重要な課題として，外的要因などによって量子状態が壊れる量子エラーがある．量子エラーを訂正するための仕組みとして量子誤り訂正符号が提案されている[6]. 量子誤り訂正を前提とした量子コンピュータを Fault-Tolerant Quantum Computer (FTQC) と呼び, FTQC での実行を前提とした量子アルゴリズムを Long-term アルゴリズムと呼ぶ．しかし量子誤り訂正符号は，符号化に多数の余剰量子ビットを必要とすること，量子ゲート操作のエラー率を十分下げなければ誤り訂正操作自体が新たな誤りを生んでしまうこと等の技術的な課題がある．現在の量子コンピュータで，これらの要件をクリアして誤り訂正しながら有用な計算を行うことは容易ではない．他方，現在利用可能な量子コンピュータは Noisy Intermediate-Scale Quantum (NISQ) デバイスと呼ばれ，量子ビット数が少なく誤り訂正機能を持たない.このような NISQ デバイスで，古典コンピュータを何らかの意味で上回る有用な計算が出来るかは自明ではないが，その可能性に期待して多くの NISQ アルゴリズムの提案と改善が進められている[7].

3. 量子機械学習アルゴリズム

量子機械学習[8]は，量子コンピュータを利用して機械学習タスクを実行するための量子アルゴリズム全般である．ここでは量子機械学習アルゴリズムにおける代表的な二種類を紹介する．一つは，古典機械学習における特定の計算部分を量子コンピュータで高速化する量子アルゴリズムで，もう一方は古典機械学習における表現（ニューラルネット，カーネル等）として量子系を使う量子アルゴリズムである．前者は，アダマールテストなどの量子加速に関する理論保証がある量子アルゴリズムを用いた Long-term アルゴリズムである．後者は量子エラーをある程度許容して動作可能な NISQ アルゴリズムである．これは量子系の特徴である高次元状態ベクトル空間やテンソル積構造に起因した非線形を表現として用いることで，古典コンピュータでは難しい複雑な表現を出来ることが期待されている.

量子機械学習の NISQ アルゴリズムの例として，

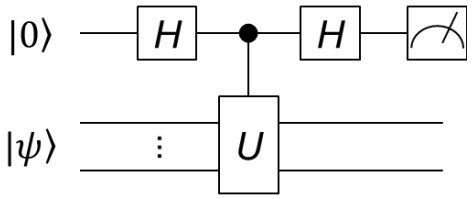

図 1 アダマールテストの量子回路

Quantum-enhanced Support Vector Machine (QSVM)[9]がある．QSVM はカーネル法ベースの教師あり機械学習として分類問題に適用可能な NISQ アルゴリズムである．QSVM では，入力データを量子ビットの状態ベクトルに埋め込み，状態ベクトル空間上でのベクトル内積をカーネル関数と定義する．このカーネル関数の値を用いてデータの分類を実行する．データの埋め込みからカーネル関数の計算までの処理は量子コンピュータで実行する．同様に NISQ アルゴリズムの例として，Quantum Circuit Learning (QCL)[10]があげられる．QCL は，ニューラルネットワークベースの教師あり機械学習の NISQ アルゴリズムである．量子ビットに埋め込まれたデータに対してパラメータを持つ量子回路を実行することで予測値を得る．このようなパラメータを持つ量子回路は変分量子回路または Ansatz と呼ばれる．学習時は，この回路の出力値と正解データから算出されるロスを最小化するパラメータを古典コンピュータで決定する.

4. 量子組合せ最適化アルゴリズム

組合せ最適化問題は，最適化問題の一種で，離散的な集合から最適解を探索する問題である．代表的な組合せ最適化問題に，巡回セールスマン問題や最大フロー問題，彩色問題などがある．このうちいくつかの組合せ最適化問題は NP 困難であり，多項式時間で厳密解を得ることができない.NP 困難な組合せ最適化を効率的に解く手法として，近似解を高速に得るための近似アルゴリズムや機械学習アプローチがある.

量子コンピュータを用いた組合せ最適化では，近似アルゴリズムとしてメタヒューリスティックに近似解を得る手法が提案されている．量子アニーリング[11]は，量子組合せ最適化アルゴリズムの一つで，組合せ最適化問題をイジングモデルのエネルギー最小化問題として定式化し，量子効果を利用してイジングモデルの基底状態を探索する．D-Wave Systems が開発した量子アニーリングマシンは，量子アニーリング専用の計算機で，他の量子アルゴリズムの実行はできないが，利用者による量子回路の実装が不要でイジングモデルの構築のみにより利用できる．一方，汎用の量子コンピュータで実行可能な量子組合せ最適化アルゴリズムとして，Quantum Approximate Optimization Algorithm

(QAOA)[12]がある．QAOA は組合せ最適化の NISQ アルゴリズムで，量子アニーリングと同様にイジングモデルのエネルギーをコスト関数として組合せ最適化問題を解く．また，古典・量子のハイブリッド型のアルゴリズムであり，量子回路は QCL と同様に変分量子回路で構成され，コスト関数を最小化するパラメータの値を古典コンピュータで計算する．

5. 量子探索アルゴリズム

データ探索は，N 個の要素から解を見つける問題である．ここで要素のラベルを n 個のビット列とし，これから一つの解をデータ探索する場合に，探索回数は全探索によって$O(2^n)$となる．量子探索アルゴリズムである Grover のアルゴリズム[13]は，このデータ探索を$O(2^{n/2})$で求解し，二次の量子加速を実現できる．Grover のアルゴリズムでは，初めに $N = 2^n$個ある解の候補を n 量子ビットの重ね合わせ状態として表現する．続いて，与えられたビット列が解かどうかを検証する関数であるオラクルを構成する．オラクルは n 量子ビットに作用する量子ゲートで構成され，重ね合わせ状態に含まれている解の候補をいっぺんに検証することが出来る．このオラクルを何度も通すことで，重ね合わせ状態に含まれる解の状態の確率振幅だけを増幅することが出来る．十分に増幅した後に，測定を行うと，高い確率で解が出力される．

Grover のアルゴリズムおよびその発展形は，Long-term アルゴリズムとして様々な研究領域で活用されている．例えば，衝突問題[14]や充足可能性問題[15]，部分和問題[16]といった計算複雑性の分野における基礎的な問題に適用されている．また，機械学習の様々なアルゴリズム[17][18]や，最適化アルゴリズム[19]，データベースシステムのクエリ[20]などのデータ工学分野に加え，多変数多項式[21]や積分[22]などの数学の計算や，セキュリティの暗号解読[23]，通信の信号検出[24]などもユースケースとして挙げられる．今回のチュートリアルでは，部分和問題に対して Grover のアルゴリズムを量子コンピュータ上に実装した論文[25]を紹介する．

6. おわりに

本稿では，量子コンピューティングの概要について述べ，データ工学分野において重要な量子アルゴリズムとして，量子機械学習アルゴリズム，量子組合せ最適化アルゴリズム，及び量子探索アルゴリズムを紹介した．実際に利用可能な量子コンピュータの出現により，量子コンピューティングの研究開発は急速に加速している．本チュートリアルを通じて，データ工学分野において NISQ デバイスの活用や FTQC を見据えた研究開発が活発化し，データ工学分野がより発展することを期待する．

参 考 文 献

[1] D. Deutsch, “Quantum theory, the Church-Turing principle and the universal quantum computer,” in Proc. of the Royal Society of London A 400, pp. 97-117, 1985.

[2] M. W. Johnson et al., “Quantum annealing with manufactured spins,” Nature, vol. 473, no. 7346, pp. 194–198, 2011.

[3] T. D. Ladd et al., “Quantum computing,” Nature, vol. 464, no. 7285, pp. 45–53, 2010.

[4] “みんなの量子コンピューター ～情報・数理・電子工学と拓く新しい量子アプリ～”, https://www.jst.go.jp/crds/pdf/2018/SP/CRDS-FY2018-SP-04.pdf

[5] T. F. Rønnow et al., “Defining and detecting quantum speedup,” Science, vol. 345, no. 6195, pp. 420–424, 2014.

[6] D. Gottesman, “An introduction to quantum error correction and fault-tolerant quantum computation,” in Proc. of Symposia in Applied Mathematics, 2010.

[7] J. Preskill, “Quantum computing in the NISQ era and beyond,” Quantum, vol. 2, no. 79, 2018.

[8] J. Biamonte et al., “Quantum machine learning,” Nature, vol. 549, no. 7671, pp. 195–202, 2017.

[9] V. Havlíček et al., “Supervised learning with quantum-enhanced feature spaces,” Nature, vol. 567, no. 7747, pp. 209–212, 2019.

[10] K. Mitarai et al., “Quantum Circuit Learning,” Phys. Rev. A, vol. 98, no. 032309, 2018.

[11] T. Kadowaki and H. Nishimori, “Quantum annealing in the transverse Ising model,” Phys. Rev. E, vol. 58, no. 5, pp. 5355–5363, 1998.

[12] E. Farhi et al., “A Quantum Approximate Optimization Algorithm,” arXiv:1411.4028, 2014.

[13] L. K. Grover, “A fast quantum mechanical algorithm for database search,” in Proc. of the 28th Annual ACM Symposium Theory of Computing, pp. 212–219, 1996.

[14] H. Buhrman et al., “Quantum algorithms for element distinctness,” in Proc. of 16th Annual IEEE Conference on Computational Complexity, pp. 131-137, 2001

[15] Y. Wang and M. Perkowski, "Improved Complexity of Quantum Oracles for Ternary Grover Algorithm for Graph Coloring," in Proc. of 41st IEEE International Symposium on Multiple-Valued Logic, pp. 294-301, 2011.

[16] A. M. Childs, J. M. Eisenberg, “Quantum algorithms for subset finding,” Quantum Information and Computation, vol. 5, no. 593, pp 593–604, 2005.

[17] D. Anguita et al., “Quantum optimization for training support vector machines,” Neural Networks, vol 16, no. 5, pp. 763-770, 2003.

[18] A. Narayanan and T. Menneer, “Quantum artificial neural network architectures and components,” Information Sciences, vol 128, no. 3-4, pp. 231-255. 2000.

[19] A. Gilliam, et al., “Grover adaptive search for constrained polynomial binary optimization,” Quantum, vol. 5, no. 428, 2021.

[20] I. Hamouda et al., “Quantum databases: Trends and challenges,” in Proc. of 11th International Conference on Computer Engineering & Systems, pp. 275–280,

2016.

[21] P. Schwabe and B. Westerbaan, “Solving Binary MQ with Grover’s Algorithm,” in Proc. of Security, Privacy, and Applied Cryptography Engineering, 2016.

[22] K. Yu et al., "Practical numerical integration on NISQ devices," arXiv:2004.05739, 2020.

[23] S. Perriello et al., "A Complete Quantum Circuit to Solve the Information Set Decoding Problem," in Proc. of IEEE International Conference on Quantum Computing and Engineering, pp. 366-377, 2021.

[24] F. Li et al., "A quantum search based signal detection for MIMO-OFDM systems," in Proc. of 18th International Conference on Telecommunications, pp. 276-281, 2011.

[25] Q. Zheng et al., “Quantum algorithm and experimental demonstration for the subset sum problem,” Science China Information Science, vo. 65, no. 182501, 2022.