

量子力学現象を利用した革新的コンピュータ

Innovative Computing with Quantum Mechanical Phenomena

松崎雄一郎 川畑史郎

Abstract

長年続いてきたムーアの法則の終えんが現実味を帯びてきた。そのため近年、汎用量子コンピュータや量子アニーリングマシンなどの量子力学現象を積極的に情報処理に利用したコンピュータに大きな注目が集められている。実際、Google, IBM, Intel, Microsoft といった世界的大企業及び D-Wave Systems, IonQ などのベンチャー企業が、汎用量子コンピュータや量子アニーリングマシンの開発を進めている。本稿においては、汎用量子コンピュータ、NISQ (Noisy Intermediate Scale Quantum Computer), 量子アニーリングマシンの基礎、最新研究開発動向、展望と課題について紹介する。

キーワード：汎用量子コンピュータ, NISQ, 量子アニーリング

1. はじめに

コンピュータは現代社会を支える必須のテクノロジーであり、その性能の向上のために多くのリソースが投入されてきた。しかしながら、半導体の微細加工技術による性能向上は限界に近付いてきている。そのため、従来とは異なるアプローチを用いてコンピュータの性能を飛躍的に向上させる手法が必要となってきた。

量子コンピュータは、現在の古典コンピュータとは全く異なる原理で動作して、理論的には高速計算が可能である。量子コンピュータは、量子力学に従って振る舞う状態のダイナミクスを巧みに用いることで問題の解を得る。

量子ハードウェアの方式には、大きく分けて、汎用量子コンピュータ、NISQ (Noisy Intermediate Scale Quantum computer), 量子アニーリングの三つが存在する (表 1)。本稿では、これらを解説する。

2. 汎用量子コンピュータ

2.1 汎用量子コンピュータの動作原理

2.1.1 古典ビットと量子ビットの違い

古典ビットは 0 か 1 の値しか取れないのに対して、量子ビットは 0 と 1 が共存するような、「重ね合わせの状態」を作り出すことができる。この古典と量子の違いは、ビットの数を大きくしたときに、極めて大きな差となって現れてくる。例えば、2 量子ビットであれば 00, 01, 10, 11 の四つの状態の重ね合わせを生成することができる。同様に、 L 個の量子ビットを用いた場合は、 2^L 個の状態の重ね合わせを生成することができる (図 1)。このような量子状態を、古典コンピュータ上で表現するには、指数関数的に多くのメモリが必要となる。そのために、古典コンピュータで大規模な量子コンピュータの振舞いを模倣することは極めて難しい。

2.1.2 量子コンピュータにおける入出力

汎用量子コンピュータにおいては、与えられた入力状態に、適切なゲート操作を印加していくことで、問題の解に対応する出力状態へと状態を推移させていき、最後に読出しを行う (図 2)。ゲート操作は、単一の量子ビットに対する回転ゲートと、2 量子ビット間の制御 NOT と呼ばれるゲートの、2 種類を組み合わせることで、任意のゲートが構成できることが知られている⁽¹⁾。

量子コンピュータは重ね合わせの状態を計算に利用している。量子力学の原理に従うと、重ね合わせの状態を読み出す場合、重ね合わされた状態の中の一つに、確率的に状態が確定される。例えば、2 量子ビットで、00,

松崎雄一郎 国立研究開発法人産業技術総合研究所ナノエレクトロニクス研究部門
E-mail matsuzaki.yuichiro@aist.go.jp
川畑史郎 国立研究開発法人産業技術総合研究所ナノエレクトロニクス研究部門
E-mail s-kawabata@aist.go.jp
Yuichiro MATSUZAKI and Shiro KAWABATA, Nonmembers (Nanoelectronics Research Institute, National Institute of Advanced Industrial Science and Technology, Tsukuba-shi, 305-8568 Japan).
電子情報通信学会誌 Vol.103 No.3 pp.267-274 2020 年 3 月
©電子情報通信学会 2020

表1 量子ハードウェアを実現するための三つの方式とその特徴

	特徴	長所	短所
汎用量子コンピュータ	量子ゲートの印加で計算を実行	原理的には、誤りが存在しても大規模計算が可能	必要な量子ビットの数が膨大
NISQ	量子ゲートと古典コンピュータを併用する	汎用形より実現が容易で、誤りの部分的修正も可能	・誤りを部分修正しかできない ・量子加速の有無が不明
量子アニーリング	ハミルトニアン of 自然な時間発展を計算に利用する	ゲート印加を必要とせず自然な時間発展を使うので実現が比較的容易	・誤りの修正方法が知られていない ・量子加速の有無が不明

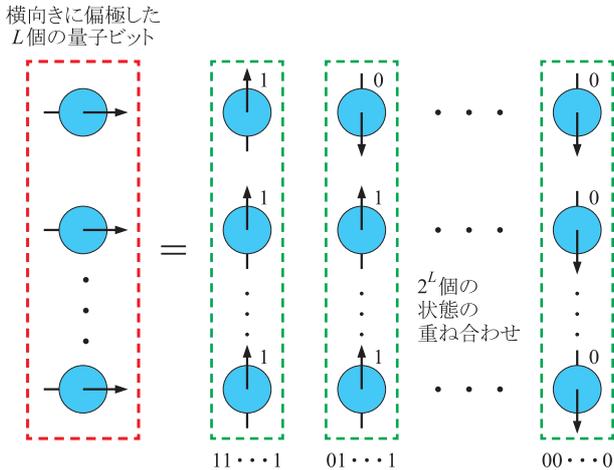


図1 L個の量子ビットの重ね合わせのイメージ図

01, 10, 11 の等しい重みで重ね合わせの状態を生成して、読出しを実行した場合、これらの状態のいずれかが25%の確率で出現する。よって、もし計算の出力が、指数関数的に多くの状態の重ね合わせを持つ場合は、その中の正解に対応する状態を読み出せる確率は、指数関数的に低くなってしまふ。そのため、高効率な計算を行うためには、出力の持つ重ね合わせの数は 2^L 個よりもはるかに少なくする必要がある。汎用量子コンピュータでは、無数の重ね合わせの中から、正解に対応する状態を「量子的な干渉性」などを利用して取り出す点に、大きな特徴がある。

2.2 誤り耐性を持つ汎用量子コンピュータ

量子ゲートを印加するたびに誤りが蓄積するため、大規模量子計算を行うためには、量子誤り訂正と呼ばれる技術を用いて、誤りの修正を行う必要がある。このよう

用語解説

多項式時間 解くべき問題のサイズ L に対して、 L^2 や L^3 などの多項式で表される計算時間のこと。

磁界型の駆動ハミルトニアン 解きたい問題が埋め込まれているハミルトニアンHPは通常、「量子ビット間の相互作用」と「縦方向に印加された磁界による量子ビットのエネルギーシフト」の二つから構成される。一方で、HDは「横方向に印加された磁界による量子ビットのエネルギーシフト」で構成される。

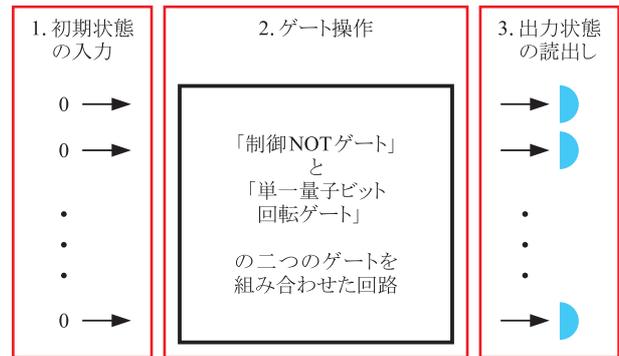


図2 汎用量子コンピュータの概要 初期状態入力、ゲート操作、出力状態読出し、の3ステップから成る。

な量子誤り訂正の機構を備えたものを、誤り耐性を持つ汎用量子コンピュータと呼ぶ。

2.2.1 量子誤り訂正の仕組み

古典の誤り訂正⁽²⁾と異なり、量子誤り訂正においてはno cloning定理⁽³⁾により量子状態の複製が不可能なこと、ビット反転雑音だけでなく位相反転雑音の影響も存在することから、複雑な冗長化が必要になる。量子誤り訂正において重要な概念として、誤りしきい値が存在する。量子誤り訂正を行っている途中にも誤りは起きるため、量子ゲート操作の誤り率が大き過ぎると、誤り訂正を行っている途中の誤り蓄積が無視できなくなる。そのため、大規模量子計算において任意の誤りを訂正するためには、量子ゲート操作の誤り率は、あるしきい値以下でなければいけない。このような量子誤りしきい値は、当初0.001%程度であったものが、現在は理論面の改善により、1%程度まで緩和された⁽⁴⁾。

2.2.2 汎用量子コンピュータの実現の難しさ

上述したように、量子ゲートの誤り率が1%未満であれば、量子誤り訂正で任意の誤りを訂正しつつ、現在の古典コンピュータでは実行の難しい規模の問題を解くことは原理的には可能である。しかし、複雑な冗長化が必要であるために、高度な量子アルゴリズム(例えば前述したような素因数分解)を行うには、数十億量子ビット程度が必要であると考えられている⁽⁵⁾。そのため、今後10数年程度では、大規模な誤り耐性量子コンピュータを実現するのは難しいと考えられている。

2.3 汎用量子コンピュータのアプリケーション

2.3.1 素因数分解

素因数分解は暗号の分野で重要な意義を持つ。古典コンピュータでは素因数分解を効率的に解けないことを前提に、現在の暗号システムの多くは構築されている。現在知られているベストの古典アルゴリズムで素因数分解を解く場合、入力サイズに対して指数関数的に多くのステップがかかることが知られている⁽⁶⁾。

汎用量子コンピュータを用いた Shor⁽⁷⁾のアルゴリズムは、入力サイズに対して多項式時間で素因数分解を実行できる。汎用形の量子コンピュータが実現された場合は、現在用いられている多くの暗号が解読されてしまう。そのために、汎用形の量子コンピュータの開発が進むにつれて、暗号システムの切替が加速されていくと予想される。実際に、汎用量子コンピュータで大規模な Shor のアルゴリズムが実装されたとしても安全性が保証される「耐量子計算暗号」の研究と開発が現在、精力的に進められている⁽⁸⁾。

2.3.2 量子化学計算

化学の分野では分子やたんぱく質の挙動をシミュレートすることで、創薬の開発を効率化できることが知られている⁽⁹⁾。しかしながら、このような分子やたんぱく質は、多数の電子が相互作用し合う極めて複雑な量子多体系である。その振舞いを予測するために、シュレーディンガー方程式を古典コンピュータで厳密に解こうとすると、分子やたんぱく質のサイズが大きくなるにつれて、指数関数的に膨大な時間がかかってしまう⁽¹⁰⁾。

古典コンピュータ上で計算するのが困難な量子多体系のシミュレートを、汎用量子コンピュータは効率的に実行することができる⁽¹¹⁾。特に、汎用量子コンピュータは、多数の電子を含むシュレーディンガー方程式を効率的に処理することができるために、系の状態のエネルギーや、分子構造、化学反応の様子などを効率的に予見できる。ここで「効率的に解く」と言っているのは、電子数の増加に対して、多項式時間^(用語)のタイムステップで解を得られるという意味である。汎用量子コンピュータは位相推定アルゴリズムと呼ばれる⁽¹²⁾、ハミルトニアン固有値を求める手法が知られており、量子状態の固有エネルギーを求めることができる。また、トロッター分解⁽¹³⁾、⁽¹⁴⁾と呼ばれる手法を用いることで、任意のハミルトニアンをゲート操作で表現することができるため、汎用量子コンピュータを用いると量子状態のダイナミクスを追うことができる⁽¹⁵⁾。このように、汎用量子コンピュータを用いて量子系のシミュレートすることで、材料設計や創薬に応用できると期待されている。

2.3.3 機械学習

機械学習は、自動車、材料、創薬、物流、金融、通信

など幅広い分野で極めて大きな需要を持つ。機械学習においては、データをベクトルとして保存して、そのベクトルに対して行列計算などの演算を行っていくことで、データの分類やフィッティングを行う。このような行列計算は、入力サイズに対して、古典コンピュータでも多項式時間で処理を行うことができる。しかしながら、扱うデータの数が膨大になるにつれて、実用的な時間で計算を終えることが難しくなってくる。

量子機械学習⁽¹⁶⁾では、量子状態が、量子ビットの数に対して指数関数的に多くの情報を保存できることを利用して、データの処理を高速で行うことができる^{(17)~(20)}。機械学習は現代の IT 社会を支える重要な技術であるので、より高速に機械学習を実行できる手法が開発されれば、産業界に与えるインパクトは極めて大きい。

しかしながら量子機械学習では、古典データを量子的なデータに変換する必要がある。より具体的には、量子的な形で蓄えられたデータを格納できて、かつ任意のタイミングでその量子情報を取り出せる Quantum Random Access Memory (QRAM) を必要とする⁽²¹⁾。データの処理自体を汎用量子コンピュータで高速に行っても、このようなデータの古典・量子変換にかかるステップ数が多いと、量子機械学習の有用性が失われてしまう。この QRAM を効率的に構成する方法は、幾つかの理論提案はあるが、この分野でまだ主要なテーマの一つとして研究が続けられている。

3. N I S Q

3.1 NISQ の動作原理

3.1.1 汎用量子コンピュータと NISQ の違い

NISQ とは近未来に実現する誤り訂正機能を有していない中規模でノイズな量子コンピュータを指す⁽²²⁾。NISQ は汎用量子コンピュータに比べると、少ない量子ビットで動作が可能であり、実現性のたやすさから注目を集めている。NISQ の動作方法は、与えた入力状態に対して量子ゲートを印加していくことで、量子状態を変化させていく点は汎用量子コンピュータと同じであるが、大きな違いが2点ある。一つ目は、NISQ では計算の途中で量子状態の読出しを行う必要がある。二つ目は、NISQ では、古典コンピュータとの併用が本質的な役割を果たす。一方で、汎用量子コンピュータでは原理的には最終的な出力状態に到達するまでは状態の読出しを行う必要がなく、古典コンピュータの併用も本質的には必要ない^(注1)。

(注1) ただし、量子誤り訂正を行う場合は、汎用量子コンピュータでも、誤りの検知のために計算途中で部分的に読出しを行い、誤りの場所を特定する。更にその読出しの結果を古典コンピュータで処理する。しかし簡単のため、ここでは、誤りのない理想的な場合での比較を行っている。

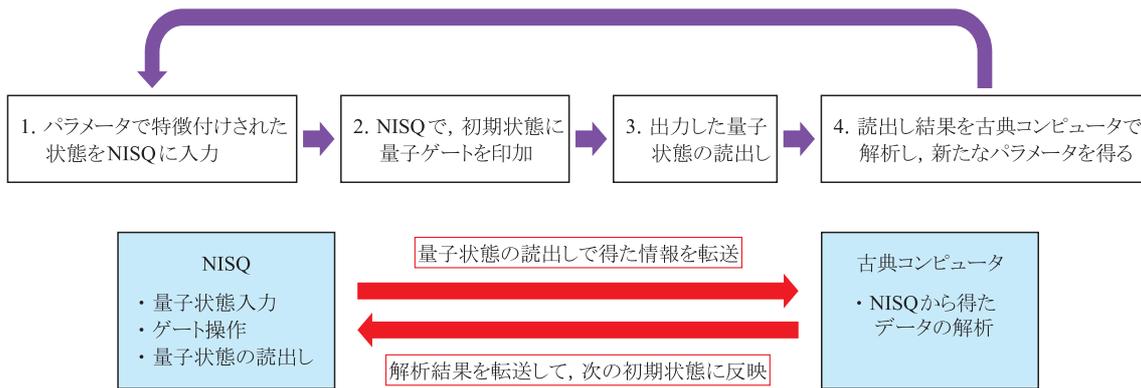


図3 NISQの動作方法の概略図 NISQでは、古典コンピュータとの併用が本質的な役割を果たす。

3.1.2 NISQの動作方法

より具体的に、NISQの動作方法を解説する(図3)。NISQでは、問題のサイズに対して多項式程度の数のパラメータ θ を用いて、量子状態を特徴付ける。①あるパラメータ(例えば θ_0)で特徴付けられた初期状態をNISQに入力する、②複数の量子ゲートを作用する、③量子状態を読み出す、④読出しの結果を古典コンピュータに入力して解析(例えば最適化処理)を行うことで、新しいパラメータ θ_n を得る、⑤NISQの新しい入力状態用に、 θ_n で特徴付けられる量子状態を生成する、⑥①~⑤を N 回繰り返して、最後に得られた(パラメータ θ_N で特徴付けられる)量子状態を読み出して、解を得る。

3.1.3 NISQの問題点とその対策

NISQにおいても、量子状態の操作に量子ゲート操作の印加を用いるために、量子ゲートが完全でない限り、誤りの問題は避けられない。更にNISQでは、量子誤り訂正を行うことを想定していないために、計算の規模を大きくしていくと、量子ゲートの誘発する誤りが蓄積していき、正解を得ることが難しくなる。

このような誤りの蓄積の問題を緩和する方法としてerror mitigationと呼ばれる技術が提案されている^{(23)~(25)}。量子ゲートの誤りは、実験的に取り除くことが難しい雑音が存在するために、任意に小さくすることはできない。しかし、誤りの種類をあらかじめ同定しておくことで、誤り率を人為的に増加させることはできる。量子ゲートの誤り率を変えてNISQを動作させて解を得て、得られた解を誤り率に対して外挿することで、正解を推定することが原理的には可能であり、この手法をerror mitigationと呼ぶ(図4)。

しかしながら、error mitigationも、計算の規模が大きくなるにつれて必要なリソースが増加していくために、大規模量子計算をNISQで実行するのは現実的ではない。NISQが実用的に意味を持つのは、error mitigationで誤りの影響を抑えられる程度の、例えば数百から

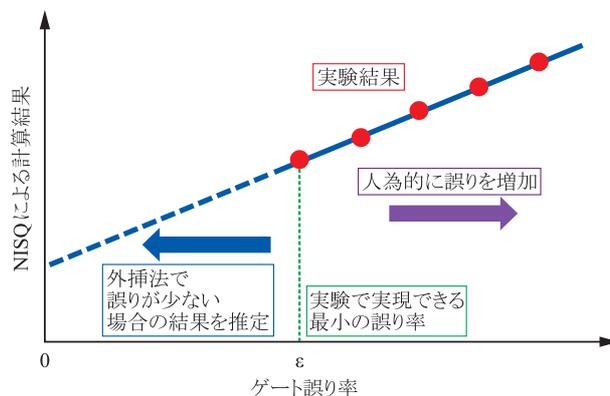


図4 NISQにおけるerror mitigationのイメージ図 人為的に誤りを大きくして計算を行い、そこからデータを外装することで、誤りのない理想的な場合の計算結果を推定する。

数千程度の量子ビットを用いた中規模な量子コンピュータだと考えられている。NISQを用いた中規模な計算で、実用的な問題を解けるかどうかは、この分野で極めて重要な課題であり、世界中で検討が続けられている。

3.2 NISQのアプリケーション

3.2.1 NISQによる量子化学計算

NISQを用いた実用的なアプリケーションとして、Variational Quantum Eigensolver (VQE)と呼ばれる、量子化学計算における量子状態のエネルギーを計算する手法が存在する^{(26), (27)}。汎用量子コンピュータでも量子化学計算は実行できるが、NISQを用いる場合は量子誤り訂正を実装する必要がないために、比較的少ない量子ビット数で実現できる点が大きな特徴である。VQEでは、複数のパラメータで特徴付けられた試行波動関数を使い、その波動関数のエネルギーが小さくなるようにパラメータを更新しながら計算を行う。一般的には、用いる試行関数が真の波動関数に近いほど、解が収束するまでの時間は短くて済む。そのため、古典コンピュータを用いて、精度の良い試行関数をあらかじめ求めておくことが重要となる。例えば数百量子ビット程度のNISQで

も、幾つかの分子に関しては実用上意味のある量子化学計算ができると考えられている⁽²⁸⁾。

3.2.2 NISQ による組合せ最適化

NISQ を用いたアプリケーションとして、Quantum Approximated Optimization Algorithm (QAOA) と呼ばれる組合せ最適化問題を解く手法も存在する⁽²⁹⁾。

組合せ最適化問題は、状況に応じて与えられたコスト関数を最小化する変数の組を見つける問題である⁽³⁰⁾。例えば、巡回セールスマン問題は、組合せ最適化問題の代表的な例である⁽³¹⁾。この問題では、セールスマンが訪れるべき都市が与えられており、都市間の距離も決められている。その際に、全ての都市を一度ずつ訪れて出発した都市に再び戻るのに必要な距離が、最短になる経路を求める。この場合は、セールスマンの移動する距離の総和がコスト関数となる。また、組合せ最適化問題の対象として、金融資産のポートフォリオの最適化や、交通渋滞の解消など、様々な応用が期待されている。

QAOA では、組合せ最適化問題の解を「イジング模型」と呼ばれるハミルトニアン基底状態にマップして、その基底状態の探索を行うことで、問題を解いていく⁽³²⁾。具体的には、QAOA では、複数のパラメータで特徴付けられた試行波動関数のエネルギーを、小さくなるようにパラメータを更新しながら計算を行う。その点では、VQE と共通点がある。更に近年になり、機械学習における分類問題が、組合せ最適化問題の一種として定式化ができることが示されたので、QAOA を機械学習に応用することが可能になった⁽³³⁾。ただし、QAOA による機械学習は、古典的機械学習よりも優れているとの証明はまだないので、その優位性を確認するためには、NISQ の実機を用いた検証を注意深く行っていく必要がある⁽³⁴⁾、⁽³⁵⁾。

4. 量子アニーリング

次に量子アニーリングについて解説する。

4.1 量子アニーリングの動作原理

4.1.1 汎用量子コンピュータと量子アニーリングの違い

量子アニーリングマシン^{(34)~(37)}は、汎用形や NISQ に代表されるゲートを用いる量子コンピュータとは、根本的に異なる手法で計算を実行する。汎用量子コンピュータと NISQ では、初期状態に対してゲート操作を印加して行くことで量子状態を変化させて、終状態へ発展させていく。一方で量子アニーリングは、ゲート操作を必要としない点が大きく異なる。量子アニーリングは元々、物性物理分野から生まれた計算手法であり、スピングラス模型などにおける熱平衡状態を効率的に計算できる古

典ヒューリスティックアルゴリズムである「シミュレーテッドアニーリング」を量子的に拡張したものと位置付けられる⁽³⁸⁾。

4.1.2 量子アニーリングの動作原理

量子アニーリングでは、人間がイジングハミルトニアンを設計した後は、初期状態をシュレーディンガー方程式に従う時間発展に任せて自然に推移させていき、終状態を得る。そのため、量子アニーリングでは、最終的に得られる状態が計算の解を与えるようにイジングハミルトニアンを設計する。汎用量子コンピュータのように、逐一、ゲート操作を行う必要がなく、ハミルトニアン設計後は、系の自然な時間発展を利用して問題を解くことができるために、実験的な実現が比較的容易である。

量子アニーリングを実行するためのハミルトニアンは以下のようにして構築する。まずは基底状態が解きたい問題の解となるようなイジングハミルトニアン H_P と、その H_P と非可換な駆動ハミルトニアン H_D を選ぶ。全体のハミルトニアンは $H = s H_P + (1-s) H_D$ とする。

ここで s は 0 から 1 の値をとる、時間に依存する変数である。初期時刻 $t=0$ では $s=0$ をとり、終時刻 $t=T$ では $s=1$ をとり、ここで $s=0$ では H_D の基底状態を用意する。このとき、 s を十分にゆっくりと変化させた場合は、系は断熱的な時間発展を行うために、常にハミルトニアンの基底状態にとどまることが知られている。ここで、「十分にゆっくり」というのは、数学的には、基底状態のエネルギーと第一励起状態のエネルギー差の逆数よりも十分に長い時間をかけてパラメータを変化させることに対応する。このような操作を行うことで、 $s=1$ では H_P の基底状態を得ることができる。直感的には、 H_P は問題の構造を表すポテンシャルを与えて、 H_D はそのポテンシャルをトンネリングさせて状態を移動させる役割を担う。トンネリングを弱めていくことで、次第に、系をポテンシャルの基底状態へと推移させていくことができる (図 5)。

4.1.3 量子アニーリングの問題点とその対策

量子アニーリングで実用的な問題を解く上で克服しなければならない課題は、ハミルトニアン設計の不完全性から生じる誤りである。解きたい問題がハミルトニアン H_P に埋め込まれるという性質上、アニーリング方式量子コンピュータの実際のデバイスのハミルトニアンが、理想的なものとは異なっている場合には、正解を得ることが難しくなる。しかも、ゲート誤りの影響を原理的に取り除ける量子誤り訂正を搭載する汎用量子コンピュータ (あるいはゲート誤りの影響を部分的には抑制できる NISQ) と異なり、量子アニーリングにおいては、ハミルトニアン設計の不完全性に由来する誤りを抑える有効な手法は現状では見つかっていない。そのため、ア

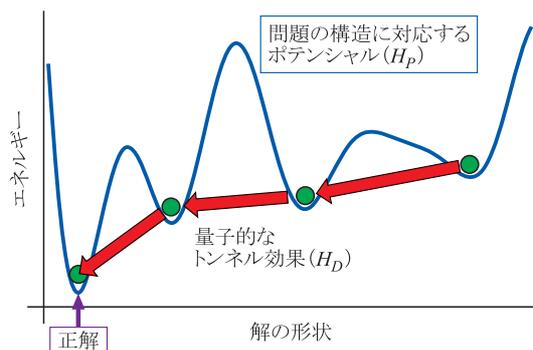


図5 量子アニーリングの原理のイメージ図 量子的なトンネル効果でエネルギーの最小になる解を探索する。

アニーリング方式の量子コンピュータを大規模化すると、正確に解を得ることが極めて困難となる。

また、現状で実装されている量子アニーリングの多くは、 H_D として横磁界型の駆動ハミルトニアン^(注2)を、 H_P として古典的イジングハミルトニアン^(注2)を選ぶという、非常に単純な場合で計算を行っている。この場合は、量子アニーリングは、量子モンテカルロ法と呼ばれる古典アルゴリズムでそのシミュレートが効率的に可能であることが知られている。更に、横磁界型の駆動ハミルトニアンを用いた通常の量子アニーリング (Stoquastic 量子アニーリング) においては、多くの場合、基底状態と励起状態のギャップが問題サイズとともに指数関数的に閉じてしまう。その結果、高い正答率で計算を行うためには、指数関数的に膨大な計算時間が必要となる。つまり、Stoquastic 量子アニーリングにおいては、多くの場合、指数関数的量子加速は期待できない。

そのため、量子アニーリングが古典ベストアルゴリズムを超える処理速度で計算を行うには、 H_D 若しくは H_P の選び方を工夫する必要がある。例えば、古典コンピュータで模倣のできないような H_D は non-stoquastic ハミルトニアンと呼ばれる^{(39)~(45)}。原理的にはこの項の導入により計算時間が指数関数的に高速化される可能性が数値的に示されている^(注3)。そのため、non-stoquastic ハミルトニアンの実装が量子アニーリングマシンでは大きな研究テーマとなっている。あるいは、 H_P として非可換な項を含む量子的なハミルトニアンを用いる場合は、量子アニーリングを古典コンピュータで模倣することは難しい。

しかし、non-stoquastic な H_D 、若しくは量子的な H_P を導入できたとしても前述した「ハミルトニアンの設計

誤り」は、少なくとも現状では回避する方法は知られていない。そのため、量子アニーリングが実用的に意味を持つのは、non-stoquastic な H_D 若しくは量子的な H_P を導入した上で、ハミルトニアンの設計誤りが支配的にならない程度の中規模のサイズの問題を解く場合に限られるであろう。

4.2 量子アニーリングのアプリケーション

量子アニーリングにより組合せ最適化問題を解くことができる。具体的には、 H_P としてイジングハミルトニアンを選ぶ。解く問題の情報は、古典イジングハミルトニアンにマップされているが、駆動ハミルトニアン H_D 及び $0 < s < 1$ での全ハミルトニアン H の固有状態は重ね合わせを含むので、量子性が現れると考えられている。

しかし近年、量子アニーリングの原理に着想を得て、このような組合せ最適化問題を高速^(注4)に解く新しい古典アルゴリズムも開発されている^{(48)~(51)}。古典アルゴリズムも極めて早いスピードで進化を遂げているために、量子アニーリングが古典コンピュータを超えて、真に実用的な問題を高速に解くことができるかどうかは、現状では分かっていない。

また量子アニーリングを利用することで、量子化学計算における、系の基底状態のエネルギーを求めることができる^{(42), (52)}。 H_P として、分子やたん白質などの解きたい電子系のハミルトニアンを選ぶ。すると、量子アニーリングマシンを断熱的に動かすことで、 H_P の基底状態が得られる。この状態に対して測定を行うことで、基底エネルギーを求めることができる。

5. 量子コンピュータ開発の現状

ゲート方式の量子コンピュータの開発に関しては2014年に非常に大きなブレイクスルーがあった。当時、アメリカのカリフォルニア大学サンタバーバラ校に在籍していた Martinis のグループが、5個の超伝導量子ビットを用いて、99%を超える精度での量子ビット操作と測定を実現した⁽⁵³⁾。量子ビットの数はまだ十分でないものの、精度の点では量子誤り訂正を可能にするレベルが実現されており、ゲート量子コンピュータへの開発に加速がついた。Martinis のグループは同年、Google に引き抜かれて、引き続き超伝導量子ビットの開発に取り組んでいる。現在72個の超伝導量子ビットの作製に成功しており、その性能を評価しているとの報告がある⁽⁵⁴⁾。更に、2019年にGoogleは、53個の超伝導量子ビットを

(注2) ここで、古典的なハミルトニアンとは、全ての固有状態が、0若しくは1の基底で、重ね合わせを用いずに記述できる場合を指す。

(注3) ただし、non-stoquastic ハミルトニアンを用いたとしても、高速化されないケースも数値的に見つかっている。つまり、non-stoquastic ハミルトニアンを使ったとしても、必ずしも計算が指数関数的に加速されるわけではない点に注意が必要である^{(40), (46), (47)}。

(注4) ここで「高速」というのは、従来に知られていたベストアルゴリズムよりも(定数倍の加速を含め)早く問題の解を与える、という意味である。

用いて、量子超越性を達成したと発表をしている⁽⁵⁵⁾。

IBMもゲート方式の量子コンピュータの開発を精力的に行っている⁽⁵⁶⁾。2016年に、ゲート量子コンピュータのクラウドサービスであるIBMQを発表した。現在IBMQは20個の超伝導量子ビットを搭載している。また、2019年には、ゲート方式としては世界初の、量子コンピュータの商用化を発表した。こちらも超伝導量子ビットを20個搭載している。

Intelもゲート量子コンピュータの開発に取り組んでおり、2018年に49個の超伝導量子ビットを搭載するチップの作製に成功している。またIntelはシリコンを用いた量子ビットの研究・開発も行っている。シリコン量子ビットは原理的にはトランジスタと同様のプロセスで製造ができるために、大規模化が比較的容易になる可能性がある点で、優位性があると考えられている。

Microsoftはトポロジカル量子ビットと呼ばれる、誤りに対して極めて耐性の強い形式を用いたゲート量子コンピュータの実現に取り組んでいる。しかしながらトポロジカル量子ビットの作製は極めて難しく、まだその実証は1量子ビットですらできていないのが現状である。

量子コンピュータ実現のためには、イオントラップによる量子コンピュータの研究・開発も行われている。イオン化された原子を捕捉して、レーザーで制御を行うベンチャー企業IonQが2018年に160量子ビットを捕捉して、79量子ビットに対して操作を行うことに成功するなど、着実に量子コンピュータ実現のための歩みが続けている。

アニーリング方式の量子コンピュータは、D-Wave社が商用マシンを販売している。2011年に128個の超伝導量子ビットを搭載するモデルを発表してから、その数を増やしていき、現在は2,000個の超伝導量子ビットを備えている商品を販売している。

6. ま と め

本稿では、汎用量子コンピュータ、NISQ、量子アニーリングの三つの量子ハードウェアを紹介して、これらの動作原理と応用、そして研究開発動向について解説した。大規模な量子ハードウェアが実現されると社会に大きなインパクトを与えるが、現状では実現に向けた課題も非常に多く残されている。真に実用的な量子ハードウェアが商用化されるには、今後、更なる研究・開発の加速が望まれる。

文 献

- (1) D.E. Deutsch, A. Barenco, and A. Ekert, "Universality in quantum computation," Proc. R. Soc. Lond. A, Math. Phys. Eng. Sci., vol. 449, no. 1937, pp. 669-677, 1995.
- (2) A.Y. Kitaev, "Quantum computations: algorithms and error correction," Uspekhi Matematicheskikh Nauk, vol. 52, no. 6, pp. 53-112,

- 1997.
- (3) W.K. Wootters and W.H. Zurek, "A single quantum cannot be cloned," Nature, vol. 299, no. 5886, p. 802, 1982.
- (4) R. Raussendorf and J. Harrington, "Fault-tolerant quantum computation with high threshold in two dimensions," Phys. Rev. Lett., vol. 98, no. 19, 190504, 2007.
- (5) N.C. Jones, R. Van Meter, A.G. Fowler, P.L. McMahon, J. Kim, T.D. Ladd, and Y. Yamamoto, "Layered architecture for quantum computing," Phys. Rev. X, vol. 2, no. 3, 031007, 2012.
- (6) D.E. Knuth, The Art of Computer Programming vol. 2, Seminumerical Algorithms, Addison-Wesley, Reading, Massachusetts, 1998.
- (7) P.W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," Proc. the 35th Annual Symposium on the Foundations of Computer Science, pp. 124-134, Los Alamitos, CA, 1994.
- (8) D.J. Bernstein, "Introduction to post-quantum cryptography," Post-quantum Cryptography, pp. 1-14, Springer, Berlin, Heidelberg, 2009.
- (9) T. Helgaker, P. Jorgensen, and J. Olsen, Molecular Electronic-structure Theory, John Wiley & Sons, Hoboken, New Jersey, 2014.
- (10) A. Szabo and N.S. Ostlund, Modern Quantum Chemistry: Introduction to Advanced Electronic Structure Theory, Courier Corporation, Chelmsford, Massachusetts, 2012.
- (11) A. Aspuru-Guzik, A.D. Dutoi, P.J. Love, and M. HeadGordon, "Simulated quantum computation of molecular energies," Science, vol. 309, no. 5741, pp. 1704-1707, 2005.
- (12) A.Y. Kitaev, "Quantum measurements and the Abelian stabilizer problem," arXiv: quant-ph/9511026, 1995.
- (13) H.F. Trotter, "On the product of semi-groups of operators," Proc. Am. Math. Soc., vol. 10, no. 4, pp. 545-551, 1959.
- (14) M. Suzuki, "Relationship between d-dimensional quantum spin systems and (d+1)-dimensional Ising systems: equivalence, critical exponents and systematic approximants of the partition function and spin correlations," Progress of Theoretical Physics, vol. 56, no. 5, pp. 1454-1469, 1976.
- (15) S. Lloyd, "Universal quantum simulators," Science, vol. 273, no. 5278, pp. 1073-1078, 1996.
- (16) C.M. Bishop, Pattern Recognition and Machine Learning, Springer, New York, New York, 2006.
- (17) J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, and S. Lloyd, "Quantum machine learning," Nature, vol. 549, no. 7671, pp. 195-202, 2017.
- (18) S. Lloyd, M. Mohseni, and P. Rebentrost, "Quantum algorithms for supervised and unsupervised machine learning," arXiv preprint arXiv: 1307.0411, 2013.
- (19) P. Rebentrost, M. Mohseni, and S. Lloyd, "Quantum support vector machine for big data classification," Phys. Rev. Lett., vol. 113, no. 13, 130503, 2014.
- (20) A.W. Harrow, A. Hassidim, and S. Lloyd, "Quantum algorithm for linear systems of equations," Phys. Rev. Lett., vol. 103, no. 15, 150502, 2009.
- (21) V. Giovannetti, S. Lloyd, and L. Maccone, "Quantum random access memory," Phys. Rev. Lett. vol. 100, no. 16, 160501, 2008.
- (22) J. Preskill, "Quantum computing in the NISQ era and beyond," Quantum, vol. 2, pp. 1-79, 2018.
- (23) Y. Li, and S.C. Benjamin, "Efficient variational quantum simulator incorporating active error minimization," Phys. Rev. X, vol. 7, no. 2, 021050, 2017.
- (24) K. Temme, S. Bravyi, and J.M. Gambetta, "Error mitigation for short-depth quantum circuits," Phys. Rev. Lett., vol. 119, no. 18, 180509, 2017.
- (25) S. Endo, S.C. Benjamin, and Y. Li, "Practical quantum error mitigation for near-future applications," Phys. Rev. X, vol. 8, no. 3, 031027, 2018.
- (26) A. Peruzzo, J. McClean, P. Shadbolt, M.-H. Yung, X.-Q. Zhou, P.J. Love, A. Aspuru-Guzik, and J.L. O'Brien, "A variational eigenvalue solver on a photonic quantum processor," Nature communications, vol. 5, 4213, 2014.
- (27) A. Kandala, A. Mezzacapo, K. Temme, M. Takita, M. Brink, J.M. Chow, and J.M. Gambetta, "Hardware-efficient variational quantum eigensolver for small molecules and quantum magnets," Nature, vol. 549, no. 7671, pp. 242-246, 2017.

- (28) N. Moll, P. Barkoutsos, L.S. Bishop, J.M. Chow, A. Cross, D.J. Egger, S. Filipp, A. Fuhrer, J.M. Gambetta, M. Ganzhorn, A. Kandala, A. Mezzacapo, P. Müller, W. Riess, G. Salis, J. Smolin, I. Tavernelli, and K. Temme, "Quantum optimization using variational algorithms on near-term quantum devices," *Quantum Science and Technology*, vol. 3, no. 3, 030503, 2018.
- (29) E. Farhi, J. Goldstone, and S. Gutmann, "A quantum approximate optimization algorithm," arXiv preprint arXiv : 1411.4028, 2014.
- (30) A. Lucas, "Ising formulations of many np problems," *Frontiers in Physics*, vol. 2, no. 5, pp. 1-15, 2014.
- (31) N. Christofides, Worst-case Analysis of a New Heuristic for the Travelling Salesman Problem, no. RR-388, Defense Technical Information Center, Fort Belvoir, Virginia, 1976.
- (32) E. Farhi, J. Goldstone, and S. Gutmann, "A quantum approximate optimization algorithm applied to a bounded occurrence constraint problem," MITCTP/4628, arXiv : 1412.6062, 2014.
- (33) J.S. Otterbach, R. Manenti, N. Alidoust, A. Bestwick, M. Block, B. Bloom, S. Caldwell, N. Didier, E. Schuyler Fried, S. Hong, P. Karalekas, C.B. Osborn, A. Papageorge, E.C. Peterson, G. Prawiroatmodjo, N. Rubin, C.A. Ryan, D. Scarabelli, M. Scheer, E.A. Sete, P. Sivarajah, R.S. Smith, A. Staley, N. Tezak, W.J. Zeng, A. Hudson, B.R. Johnson, M. Reagor, M.P. da Silva, and C. Rigetti, "Unsupervised machine learning on a hybrid quantum computer," arXiv preprint arXiv : 1712.05771, 2017.
- (34) T. Kadowaki and H. Nishimori, "Quantum annealing in the transverse Ising model," *Phy. Rev. E, Stat. Nonlinear Soft Matter Phys.*, vol. 58, no. 5, 5355, 1998.
- (35) E. Farhi, J. Goldstone, S. Gutmann, and M. Sipser, "Quantum computation by adiabatic evolution," arXiv preprint quant-ph/0001106, 2000.
- (36) E. Farhi, J. Goldstone, S. Gutmann, J. Lapan, A. Lundgren, and D. Preda, "Quantum adiabatic evolution algorithm applied to random instances of an NP-complete problem," *Science*, vol. 292, no. 5516, pp. 472-475, 2001.
- (37) D. Preda, "A quantum adiabatic evolution algorithm applied to random instances of an np-complete problem," *Science*, vol. 292, no. 5516, pp. 472-475, 2001.
- (38) S. Kirkpatrick, C.D. Gelatt, and M.P. Vecchi, "Optimization by simulated annealing," *Science*, vol. 220, no. 4598, pp. 671-680, 1983.
- (39) Y. Seki and H. Nishimori, "Quantum annealing with antiferromagnetic fluctuations," *Phys. Rev. E, Stat. Nonlinear Soft Matter Phys.*, vol. 85, no. 5, 051112, 2012.
- (40) L. Hormozi, E.W. Brown, G. Carleo, and M. Troyer, "Nonstoquastic Hamiltonians and quantum annealing of an Ising spin glass," *Phys. Rev. B, Condens. Matter Mater. Phys.*, vol. 95, 184416, 2017.
- (41) H. Nishimori and K. Takada, "Exponential enhancement of the efficiency of quantum annealing by nonstoquastic Hamiltonians," *Frontiers in ICT*, vol. 4, no. 2, 2017.
- (42) R. Babbush, P.J. Love, and A. Aspuru-Guzik, "Adiabatic quantum simulation of quantum chemistry," *Scientific Reports*, vol. 4, 6603, 2014.
- (43) D. Aharonov, W. van Dam, J. Kempe, Z. Landau, S. Lloyd, and O. Regev, "Adiabatic quantum computation is equivalent to standard quantum computation," *SIAM J. Comput.*, vol. 37, no. 50, pp. 755-787, 2007.
- (44) J.D. Biamonte and P.J. Love, "Realizable Hamiltonians for universal adiabatic quantum computers," *Phys. Rev. A, At. Mol. Opt. Phys.*, vol. 78, no. 1, 012352, 2008.
- (45) S.P. Jordan, D. Gosset, and P.J. Love, "Quantum-MerlinArthur-complete problems for stoquastic Hamiltonians and Markov matrices," *Phys. Rev. A, At. Mol. Opt. Phys.*, vol. 81, no. 3, 032331, 2010.
- (46) E. Crosson, E. Farhi, C.Y.-Y. Lin, H.-H. Lin, and P. Shor, "Different strategies for optimization using the quantum adiabatic algorithm," arXiv preprint arXiv : 1401.7320, 2014.
- (47) Y. Seki and H. Nishimori, "Quantum annealing with antiferromagnetic transverse interactions for the hopfield model," *J. Physics A, Mathematical and Theoretical*, vol. 48, no. 33, 335301, 2015.
- (48) H. Goto, K. Tatumura, and A.R. Dixon, "Combinatorial optimization by simulating adiabatic bifurcations in nonlinear Hamiltonian systems," *Science advances*, vol. 5, no. 4, pp. 1-8, 2019.
- (49) M. Yamaoka, C. Yoshimura, M. Hayashi, T. Okuyama, H. Aoki, and H. Mizuno, "A 20k-spin Ising chip to solve combinatorial optimization problems with CMOS annealing," *IEEE J. Solid-State Circuits*, vol. 51, no. 1, pp. 303-309, 2015.
- (50) T. Inagaki, Y. Haribara, K. Igarashi, T. Sonobe, S. Tamate, T. Honjo, A. Marandi, P.L. McMahon, T. Umeki, K. Enbutsu, O. Tadanaga, H. Takenouchi, K. Aihara, K.-I. Kawarabayashi, K. Inoue, S. Utsunomiya, and H. Takesue, "A coherent Ising machine for 2000-node optimization problems," *Science*, vol. 354, no. 6312, pp. 603-606, 2016.
- (51) M. Aramon, G. Rosenberg, E. Valiante, T. Miyazawa, H. Tamura, and H.G. Katzgraber, "Physics-inspired optimization for quadratic unconstrained problems using a digital annealer," (2018) ; arXiv : 1806.08815.
- (52) A. Perdomo-Ortiz, N. Dickson, M. Drew-Brook, G. Rose, and A. Aspuru-Guzik, "Finding low-energy conformations of lattice protein models by quantum annealing," *Scientific reports*, vol. 2, 571, 2012.
- (53) R. Barends, J. Kelly, A. Megrant, A. Veitia, D. Sank, E. Jeffrey, T.C. White, J. Mutus, A.G. Fowler, B. Campbell, Y. Chen, Z. Chen, B. Chiaro, A. Dunsworth, C. Neill, P. O'Malley, P. Roushan, A. Vainsencher, J. Wenner, A.N. Korotkov, A.N. Cleland, and J.M. Martinis, "Superconducting quantum circuits at the surface code threshold for fault tolerance," *Nature*, vol. 508, no. 7497, 500-503, 2014.
- (54) B.M. Terhal, "Quantum supremacy, here we come," *Nature Physics*, vol. 14, no. 6, pp. 530-531, 2018.
- (55) F. Arute, K. Arya, R. Babbush, D. Bacon, J.C. Bardin, R. Barends, R. Biswas, S. Boixo, F.G.S.L. Brandao, D.A. Buell, B. Burkett, Y. Chen, Z. Chen, B. Chiaro, R. Collins, W. Courtney, A. Dunsworth, E. Farhi, B. Foxen, A. Fowler, C. Gidney, M. Giustina, R. Graff, K. Guerin, S. Habegger, M.P. Harrigan, M.J. Hartmann, A. Ho, M. Hoffmann, T. Huang, T.S. Humble, S.V. Isakov, E. Jeffrey, Z. Jiang, D. Kafri, K. Kechedzhi, J. Kelly, P.V. Klimov, S. Knysh, A. Korotkov, F. Kostritsa, D. Landhuis, M. Lindmark, E. Lucero, D. Lyakh, S. Mandrà, J.R. McClean, M. McEwen, A. Megrant, X. Mi, K. Michielsen, M. Mohseni, J. Mutus, O. Naaman, M. Neeley, C. Neill, M.Y. Niu, E. Ostby, A. Petukhov, J.C. Platt, C. Quintana, E.G. Rieffel, P. Roushan, N.C. Rubin, D. Sank, K.J. Satzinger, V. Smelyanskiy, K.J. Sung, M.D. Trevithick, A. Vainsencher, B. Villalonga, T. White, Z.J. Yao, P. Yeh, A. Zalcman, H. Neven, and J.M. Martinis, "Quantum supremacy using a programmable superconducting processor," *Nature*, vol. 574, no. 7779, pp. 505-510, 2019.
- (56) J.M. Gambetta, J.M. Chow, and M. Steffen, "Building logical qubits in a superconducting quantum computing system," *npj Quantum Information*, vol. 3, no. 1, pp. 1-7, 2017.

(2019年10月3日受付 2019年10月21日最終受付)



まつぎき ゆういちろう
松崎 雄一郎

2011 オックスフォード大博士課程了。同年日本電信電話株式会社 NTT 物性科学基礎研究所入社。2019 から産業技術総合研究所。現在同所主任研究員。量子情報理論の研究に従事。



かわはた しろう
川畑 史郎

1998 阪市大大学院工学研究科博士課程了。博士 (工学)。同年電子技術総合研究所入所。2001 から産業技術総合研究所。現在同所研究グループ長。物性理論、量子情報処理、デバイス物理の研究に従事。現在、文部科学省光・量子飛躍フラッグシッププログラム Q-LEAP 量子情報処理サブプログラムディレクター。