

NISQ 時代とそれ以降の量子コンピューティングについて

ジョン・プレスキル

量子情報・情報研究所

カリフォルニア工科大学、パサデナ CA 91125、米国

2018 年 1 月 27 日

arXiv:1801.00862v2 [quant-ph] 2018 年 1 月 27 日

概要

近い将来、ノイズの下での中規模程度の量子技術 NISQ (Noisy Intermediate-Scale Quantum) が利用可能になるだろう。50~100qubit の量子コンピュータは、今日の古典的なデジタルコンピュータの能力を上回るタスクを実行する可能性を持つのだが、量子ゲートのノイズは、信頼性をもって実行できる量子回路のサイズを制限する。NISQ デバイスは、多体量子物理学の研究の有用なツールとなるだろう。その他の有用な応用もあるのだが、100qubit の量子コンピュータは、すぐには世界を変えないだろう。我々は、それを、将来のより強力な量子技術に向けた重要なステップとみなすべきである。量子技術者は、完全にフォールト・トレラントな量子コンピューティングを結果的に可能とする、より正確な量子ゲートの実現に向けて努力しなければならない。

この論文は、2017 年 12 月 5 日に開催された Quantum Computing for Business カンファレンスでの基調講演に基づいている。この集まりでのすべての講演のビデオについては、q2b.us を参照されたい。

1 はじめに

この会議の前提は、現在が、量子コンピューティングに関心を持つ研究者、起業家、経営者、投資家の間で、実りある議論をするふさわしい時期であるということである。大企業とスタートアップ企業の投資は最近急増しており、この傾向は、アカデミーの世界で働いている多くの量子技術の研究者を驚かせている。我々は、量子技術の商業的可能性を長い間認識してきたつもりだが、産業活動のこのような急速な増加は、我々の大部分が期待していたよりも早くそして突然に起こった。

量子コンピューティングの現在の状況と将来の可能性を評価するこの機会に参加できたことを、私は喜んでいる。量子コンピューティング技術は現在我々が使用している情報技術とは非常に異なるため、将来の応用を予想するのも、これらの応用が実現した際のプロジェクトを考えるのにも、我々は非常に限られた能力しか持っていない。この不確実性は楽観主義を助長するのだが、我々は、楽観主義を注意深く調整する必要がある。我々は、将来の数十年にわたって量子技術が社会に重要な影響を及ぼすと確信しているのだが、今後の5〜10年という短期間での量子技術の商業的可能性については、あまり自信を持っているとは言えないのだ。それが、私がこの話で伝えたい主なメッセージである。私は、この会議を組織したようなすべての利害関係者間の活発な議論が、将来の進展に向けての道筋を照らすと確信している。

2 エンタングルメントのフロンティアでの好機

私は粒子物理学と宇宙論をバックグラウンドとした理論物理学者なのだが、20年以上にわたり、私の研究の努力の多くは量子情報科学に向けられていた。私がこの分野にひきつけられたのは、我々が物理学の新しいフロンティア – 複雑性のフロンティアあるいはエンタングルメントのフロンティアとでもよぶべきもの – の探求の初期段階にいて感じていたからである。この新しいフロンティアは、素粒子論や宇宙論のフロンティアとは異なっているのだが、非常に基本的でエキサイティングである。我々は人類史上初めて、多くの粒子、非常に複雑で高度にもつれあった量子状態を構築し、それを正確にコントロールするためのツールを手に入れて完成させつつある。その状態は非常に複雑で、現在我々が持つ最良のデジタル・コンピュータでもシミュレートできず、既存の理論的道具では、それをうまく特徴付けることもできない。私のような物理学者が、量子コンピューティングについて本当に興奮しているのは、量子コンピュータが自然界で起こる全てのプロセスを効率的にシミュレートできると信じる十分な理由があるからである。これは、古典的(すなわち非量子)デジタルコンピュータでは当てはまらないことだ。古典的コンピュータは、高度にもつれあった量子システムをシミュレートすることができないのだ。量子コンピュータがあれば、きっと複雑な分子やエキゾチックな材料の特性をより深く探求することが可能になるだろう。それだけでなく、例えば、基本粒子の性質やブラックホールの量子的挙動やビッグバン直後の宇宙の進化をシミュレートすることで、新しいやり方で、基本的な物理学を切り開いていくだろう。

エンタングルメント(量子もつれ)の最前線の開拓が実り多いものであるという我々の確信は、次の二つの原理に基づいている。

- (1) 量子複雑性(量子コンピューティングが強力であるとする我々の考えの基礎)
- (2) 量子誤り訂正(量子コンピュータは、難しい問題を解決する大規模なデバイスに拡張可能であるという量子力学であるとする私たちの基礎)

これらの二つの原理の基礎となるのは、量子エンタングルメントの考え方である。エンタングルメントは、私たちが日常生活でであう相関とは全く異なる、量子システムの部分の間の特徴的な相関のために使用する言葉である。エンタングルメントの概念を理解するために、100 ページの長さの本など、多くの部分を持つシステムを想像してみよう。通常の古典的な 100 ページの本の場合、別の1ページを読むたびに、その書籍の内容の別の 1%を習得する。すべてのページを1ページずつ読んだら、本の中のすべてを知ることになる。しかし今、その本が古典的な普通の本ではなく、ページがお互いに非常にもつれあっている量子の本だとして。そこでは一度に 1 ページを見てもとランダムなちんぷんかんぷんな言葉しか見えない。すべてのページを1ページずつ読んでも、その本の内容はほとんど理解できない。それは、この量子書籍の情報が個々のページには印字されていないためである。そこでは情報は、あるページが他のページと互いにどのように相関しているかに従って、ほぼ完全に符号化されている。こうした量子の本を読みたいと思ったら、一度に多くのページを一括して観察する必要がある。これが量子系のエンタングルメント(もつれ合い)である。その本質的な特徴は、量子システムによって運ばれる情報を通常のデジタルコンピュータで処理される情報とは非常に異なるものになっている。

3 量子コンピューティングの可能性

3.1 なぜ量子コンピューティングが強力だと思うのか

通常のコンピュータは、ビットを処理する。ビットは、たかだか状態のオン・オフの二値の状態を表しているにすぎない。それに対して、量子コンピュータで基本的な情報を担っている量子ビット qubit は、相互にもつれあった(entangled)非常に複雑な量子システムである。量子ビットは、物理的には様々な方法で実現できる。量子ビットは、単一の原子、単一の電子、単一の光子によって担われることができるし、多くの電子が移動する、もっと複雑なシステムである、超低温の超電導回路によっても担われることができる。

「量子の複雑性」という時、まず心に浮かぶのは、通常の古典的なデータを利用して、たくさんの量子ビットからなる高度にもつれあった量子状態を記述しようとする際に現れる驚異的な複雑さである。ほんの数百の qubit であっても、それらの間の全ての相関の完全な記述を考えてみよう。それは、目に見える宇宙の全ての原子の数より大きなビット数を必要とする。これらを書き下すことも、古典的な言語を用いて数百の qubit の変化を忠実に記述することも、原理的にも、不可能である。この量子の世界の明らかに法外な複雑さは、非常に示唆的だが、そのことはそれ自体では、量子コンピュータが古典的なコンピュータより強力であることを保証するものではない。

しかし、量子コンピュータが古典的コンピュータを凌駕する能力を持つと考える、少なくとも三つの理由がある。

第一。我々は、古典的なコンピュータにとっては難しい問題だと信じられている幾つかの問題を知っている。しかし、それらを簡単に解くことができる量子アルゴリズムが発見されている。最もよく知られている問題は、大きな数の素因数を求める問題である[1]。優秀な人たちが何十年にもわたってより良い因数分解アルゴリズムを探し求めて来たのに成功しなかったことを見ればわかるように、因数分解は難しい問題である。おそらく、将来、高速の素因数分解の古典的アルゴリズムが発見されるかもしれないのだが、それは、大きな驚きにはならないだろう。

第二。コンピュータ・サイエンスの理論家たちは、複雑性の理論に基づいて、ある合理的な仮定のもとで、量子コンピュータで用意できる量子状態が、古典論的な性質を超える性質を持つことを示す議論を提供している。すなわち、特に関連のある確率分布からサンプリングで得られたある状態の全ての qubit を測定すると、それはいかなる古典的な手段によってもサンプリングできない状態を持つ[2, 3]。

第三。しかし、量子コンピュータが強力であるという、我々が持つもっとも説得的な議論は、単純に、デジタル・コンピュータを使ってどのように量子コンピュータをシミュレートすればいいかわからないということだと思う。このことは、物理学者たちが、今後数十年にわたって、量子システムをシミュレートするより良い方法を見つけようという試みを続けたとしても、変わらず、真実だろう。

もっとも驚くべきアイデアは、古典的に難しい問題と量子的に難しい問題の間には、違いがあるという要求である。そして、どのような問題が、古典的に難しいが量子的には容易であるか[4, 5]をよりよく理解することは、多くの人を動かしている挑戦的な課題である。我々は、量子コンピュータの力が無制限なものではないことを、特に、認識すべきである。例えば、我々は、巡回セールスマン問題のような NP-困難な問題を、量子コンピュータが効率的に解くだろうことを期待してはいない。このような困難な組合せ論的検索問題は、徹底的にしらみ潰しで検索する以外にいい解はないだろう。量子コンピュータは皆尽探索を高速化できるが[6]、その効果はほどほどのものである[7]。だから、NP-困難な問題は、古典的に困難なだけでなく、量子的にも困難であるように見える。

古典的には困難だが量子的には易しい問題を探している物理学者にとって、見るべき自然な場所は、多粒子量子系のシミュレーションである。偉大な二人の物理学者 Bob Laughlin と David Pines は、数年前にこう述べた[8]。「我々は、日常の生活に関連する『万物の理論』をもっている。我々はこの理論が正しいことに強い自信を持っている。また、その方程式を正確に書き下ろすことができる。-- その方程式とは、原子核と電子が電磁相互作用していることを記述している。しかし、我々は、その方程式を解くことができない。」 Laughlin と Pines は、次のようにも述べている。「我々は『万物の理論』をもっているのだが、それは、非常に重要さを持つ多くの物事については、全く何も教えてくれないことをみつけただ

けであった。」ここで彼らが重要なものとして思い描いているのは、エンタングルメントが重要な帰結を持つ量子世界の状況である。この仕事の豊かさを劇的に示すために、彼らは、次のように公言している。「現存するどんなコンピュータも、これから登場するだろうどんなコンピュータも、この障壁、多数のもつれあった粒子を記述する方程式の障壁を打ち破ることはできない。」

しかし、これらの言葉が述べられる前のことだが、ファインマンは、既に反論を明確に述べていた[9]。「自然は、全然、古典的な代物なんかじゃないんだ。もし、自然をシミュレートしたいと望むなら、量子力学的にシミュレートした方が、もっとうまくできるだろう。なんとまあ、それは素敵な問題なんだろう。というのも、それは簡単そうな問題には見えないから。」ファインマンは、物理学者や科学者がデジタル・コンピュータを使って解くのに失敗した量子物理の問題を、量子コンピュータを使って解くというビジョンを持っていた。ファインマンの提案から 35 年以上たった今、我々は、量子コンピュータが、難しい量子的問題に有用なソリューションを提供できるという最初の段階に到達しようとしているのだ。

3.2 量子コンピューティングがなぜ難しいのか

それでは、なぜ、そんなに時間がかかったのか？ 量子コンピュータがそんなに難しいのは、どんな問題があるのか？この問題の中核は、量子的世界の次のような基本的特徴から発したものだ。すなわち、我々は、そのシステムの内部にコントロール不能な混乱を生み出すことなしには、量子的システムを観測することができないのだ。このことは、もし、我々が量子的システムを、情報の蓄積や処理のために使うのならば、そのシステムをほぼ完全に外界から隔離する必要があることを意味する。同時に、それにもかかわらず、我々が情報を処理するためには、qubit たちが相互に強く作用することを望むことになる。さらに我々は、システムを外部からコントロール出来る必要がある。最終的には、計算の結果を見つけることができるためには、qubit を読み出すことになる。これらの要求をすべて満たす量子システムを構築するのは、極めて挑戦的な課題である。現在の我々の到達点に至るまでには、素材の面でもコントロールの面でも回路設計でも、その開発に多くの年月が費やされたのである。

最終的には、我々は、量子誤り訂正の原理[10]を用いて、量子システムを保護し規模拡大することを期待している。量子誤り訂正のアイデアのエッセンスは、もし我々が量子システムをダメージから守ろうとするなら、それは高度にもつれあった状態に符号化されるべきだということである。先に述べた 100 ページの本のように。この状態は、次のような特徴を持っている。すなわち、環境は、同時にはシステムの一つの部分としか相互作用しないので、エンコードされた情報を盗み見ることも、それゆえ、システムにダメージを与えることもできない。更に言えば、我々は、高度にもつれあった状態にエンコードされた量子情報を、どのように処理すべきかを、原理的には、理解している。残念なことに、量子誤り訂正を行うには、膨

大なオーバーヘッドのコストが必要になる。保護された量子情報を、高度にもつれあった本に書き出すには、多くの追加の物理的 qubit が必要になるのだ。そういうわけで、量子誤り訂正を利用した信頼性の高い量子コンピュータは、今すぐには、実用可能になるようには思えない。

4 NISQ 時代の展開

4.1 50 キュビットの障壁

フォールト・トレラントな量子コンピュータは、今では、まだ遠い夢だとしても、現在、我々は、量子技術における重要な新時代に入ろうとしている。この差し迫った新しい時代を表現するために名前が必要なので、私は NISQ という言葉を作った。これは、Noisy Intermediate-Scale Quantum の略である。ここで「Intermediate-Scale」とは、数年後に利用可能となる、量子ビット数が 50 から数百程度までの量子コンピュータのサイズを指す。50qubit は、重要なマイルストーンである。それは、最も強力な既存のデジタル・スーパーコンピュータを使用して力づくでシミュレートできるものを超えているからである。「Noisy」とは、我々がそれらの qubit を不完全にしかコントロールできないことを強調している。ノイズは、当面の量子デバイスが達成できることに、重大な制限を課すだろう。物理学者はこの NISQ 技術に興奮している。というのも、それが、多数のもつれた粒子の物理学を探索する新しいツールを我々に提供しているからである。この講演の聴衆(ビジネス・コミュニティ)に関心を持つような有用な応用があるかもしれないが、それについては、確かなことは分からない。我々は、NISQ それ自体を、世界を変えるものだと期待すべきではない。そうではなく、それは、将来において開発されるより強力な量子技術への一步と見なされるべきである。私は、最終的には、量子コンピュータが、社会を変えるような影響を与えているのだが、それにはまだ数十年かかるかもしれない。どれくらいの時間がかかるか、確かなことはわからない。

4.2 Qubit の「品質」

私は、古典的なデバイス上で量子コンピュータのシミュレーションを行うことがどれほど難しいかの尺度として qubit の数を強調したが、qubit の数だけが私たちが気にすべきものではない。qubit の品質、特に量子ゲートを実行する正確さ、すなわち qubit のペアたちに作用する、よく制御されたエンタングル処理についても気にしている。トラップ・イオン[14]や超伝導回路[15]をコントロールするための最良のハードウェアでは、2qubit のゲートの 1 ゲート当たりのエラー率は 0.1%レベルを上回る(しばしばさらに悪化する)。さらに、多くの qubit を有するより大きいデバイスでは、低いエラー率が維持できるかどうかはまだ分かっていない。おそらくすぐにわかるだろうが。これらのノイズ下のデバイスでは、1000 個以上のゲー

ト、すなわち、2 つの qubit の基本的操作を担う 1000 個以上の回路を実行することは期待できない。なぜなら、ゲートの数が 1000 個を超えると、ノイズが回路の信号よりはるかに大きくなり、それを圧倒するからである。この 1000 個のゲートという評価にしてもあまりに素朴すぎるので、この問題については後で触れる。この回路規模の制限は、NISQ 技術の計算力に上限を課している。最終的には、我々は量子エラー訂正技術を利用して、より大きな回路までスケールアップすることで、この問題に対処するだろう。しかし、すでに強調したように、量子エラー訂正は量子ビット数とゲート数に大きなオーバーヘッドコストを課するため、それを使ったスケールアップはもっと遠い目標となる。NISQ 時代を語るとき、私は、量子エラー訂正技術で保護されていないノイズの多いゲートの量子コンピュータを想定している。

qubit の数とゲートエラー率以外にも、我々が気にしている他の問題がある。単一ゲートの実行に要する時間は、量子コンピュータが問題を解決するのに必要な時間スケールを設定するためにも重要である。ここでは、超伝導回路がイオントラップ量子プロセッサより約 1000 倍高速であることは注目に値する。また、qubit を正確に準備し、測定することができる必要がある。現在、測定誤差の確率は、超伝導 qubit については約 1% であり、トラップ・イオンの場合に比べてはるかに良好である。デバイスの qubit ペアが正確な 2qubit ゲートを実行できるかという、qubit 間の接続性の問題もある。また、多数の qubit からなるデバイスを構築しようとするなら、いかに確実に qubit たちを組み上げるのか？ その qubit のうちどれだけが実用に耐えられるのか？ そうしたことを知ることは重要である。異なる量子コンピューティング・プラットフォーム間で比較を行う際には、これらも考慮に入れる必要がある。

5 私があまり話していないこと

この講演の主要なテーマに移る前に、誤解を避けるために弁明したいことがある。今回は、実際には話すことができないのだが、量子技術には、非常に興味深く重要ないくつかの側面がある。私が今回話さなかったことについて知ることができるように、それらを簡単に示しておこう。

(1) 量子耐性暗号

我々のプライバシーをどのように保護するかについていえば、我々は、量子コンピュータがそれに対して破壊的な影響を与えることを予見している。今日広く普及している公開鍵暗号システムは、十分に強力な量子コンピュータで簡単に破られるため、それは今後いつか時代遅れのものになるだろう。我々は、今後どのように我々のプライバシーを守るかについて考えなければならない。1 つの可能な方法は、既存の暗号システムを、量子コンピュータによる攻撃に耐性があると我々が確信している新しい暗号システムで置き換えることである[16]。

(2) 量子鍵配送、量子ネットワーク、量子リピータ

我々は、移動する qubit ー光子である可能性が高いのだが ーを利用して、暗号化と復号化に使用できる共有キーを作成することができる。量子鍵配布は、検出可能な乱れを生み出すことなく量子通信を盗聴することができないという原則を利用している[17]。しかし、我々は、量子もつれあい、それゆえ秘鍵を世界中に配布する技術をまだ持っていない。それはもう一つの興味深い技術的課題である[18]。鍵交換へのアプリケーション以外にも、グローバル量子ネットワークは、量子デバイス間で情報を共有するなど、他の目的にも使用できることも注目に値する。

(3) 量子センシング。

量子技術は、ある種のセンシングに利点がある。量子システムは、他のセンシング技術より優れた感度とより高い空間分解能で「弱い力」を感知することができる[19]。したがって、量子センシングは、比較的短期間で、例えば、医学などの分野で、影響の大きい応用を有する可能性がある。

量子通信、ネットワーキング、およびセンシングは、量子コンピューティングと明確に分離することはできない。なぜなら、同様の技術的課題に、これらの量子情報の目標すべてが直面しているからである。

6 量子スピードアップ？

ここでは、量子コンピュータが、特に比較的近い将来、広い応用を持つかどうかに関心を当てよう。主な質問は次のようなものだ。「量子コンピュータは、いつ古典的なコンピュータよりも早く我々が関心を持つ問題を解決できるのか？ また、それはどのような問題なのか？」少なくとも近い将来、量子コンピュータは、ほとんどのユーザがクラウドを介してアクセスする、特殊な目的のために利用されるデバイスになる可能性は高い。「量子高速化」について語る時、それは、典型的には、競合する古典的なコンピュータが、利用可能な最良のハードウェアを使用し、最良のアルゴリズムで同じタスクを実行したとして、量子コンピュータが、それよりも高速に問題を解決することを意味する。(量子ハードウェアが、より低コストで低消費電力であれば、古典的なスーパーコンピュータがより高速に動作しても、量子技術が望ましいという議論はあるかもしれないが) いずれにせよ、古典的なコンピュータのパワーは、増大を続けるので、数年後に予想されるシステムは、エグザ・スケールのシステム(10^{18} FLOPS を超える)になるだろうことを認識する必要がある。量子コンピュータは、古典的なハードウェアと古典的アルゴリズムの両方が絶え間なく改善されているという、動くターゲットに追いつくために努力しなければならない。

数年前に、私は人間文明の切迫したマイルストーンとして「量子優越性」について熱心に話した。[20] 量子デバイスで実行可能な計算タスクを特徴づける一つの方法としてこの用語を提案した。そこでは、

説得的に議論するために、既存の(または容易に予測しうる)どんな古典的なデバイスでも、同じタスクを実行できないとして、そのタスクが有用であるかどうかといった問題は無視した。この惑星上の技術の歴史を巨視的に眺めれば、現在は、特別な時期だと強調しようとして来た。そうしたことを後悔していない。しかし、商業的な観点からは、明らかに、タスクが有用かどうかに注意を払うべきである！「量子優越性」は、起業家や投資家にとっては、それほど注目すべき概念ではないかもしれないが、その本質的な重要性からというより、遥か遠くにあるより高い価値のある応用に向かう進歩の兆しとして、価値ある目標である。また、NISQ 技術の不完全なパフォーマンスのために、量子コンピュータが実際に正しい答えを与えていることを検証するのは難しいかもしれないことにも留意する必要がある。これは物理学者が興奮している量子シミュレーションの問題に特に当てはまる。したがって、研究者は量子コンピュータの出力を検証するためのより良い方法を探し続けることが重要である。

6.1 量子オプティマイザ

量子コンピュータが、組み合わせ最適化問題のような NP 困難な問題の最悪の場合を効率的に解くことを、我々は期待していないことは、すでに強調してきた。それでも、量子デバイスがより良い近似解を見つけたり、そのような近似解をより早く見つけれられることは、考えられる(保証されてはいないのだが)。例えば、 n 個のビットに m 個の制約を課して、 m 個の制約をできるだけ多く満たす n ビットの文字列を求めることができる。同時に満たすことができる制約の最大数 k を見つけることができれば、この最適化問題を正確に解決できたと言えるかもしれない。また、満たすべき制約の最大数が少なくともいくつかの k' に対して、 $k' < k$ であることを保証できれば、近似解を得たことになる。近似比 k'/k は、近似解の品質の尺度となる。

いくつかの最適化問題では、近似解が 1 に十分近くても近似解を見つけることさえ NP 困難である [21]。そのような場合には、量子計算機が、難しい問題の近似解を効率的に求めることは期待できない。しかし、多くの問題に対して、我々が現在知っている最高の古典的アルゴリズムによって達成される近似解と NP 困難との障壁との間には大きなギャップがある。だから、量子コンピュータが、近似解を見つけるという仕事には、古典的コンピュータよりも利点があることを発見することは衝撃的ではないだろう。

こうした量子の利点を実際に存在するかどうかは現在未解決の問題だが、量子ハードウェアを使用して実験的にこうした問題を探索する機会は、すぐに来るだろう。もちろん、近似最適化のための量子的利点があるとしても、NISQ 技術はその利点を実証するには不十分かもしれない。それでも、それを試して、それがどれほどうまくいくかを知ることは楽しいことだろう。

量子技術を用いた最適化問題を解決するため新登場のパラダイムは、量子・古典のハイブリッド・アルゴリズムである。このスキームでは、量子プロセッサを使用して n -qubit 状態を準備し、古典的オプティマイザを使用してすべての qubit を測定し、測定の出力を処理する。古典的オプティマイザは、量子プロセッサに、 n -qubit 状態がどのように準備されるかをわずかに変更するよう指示する。このサイクルは、近似解を抽出することができる量子状態に収束するまで何度も繰り返される。従来の組み合わせ論的最適化問題に適用すると、この手順は量子近似最適化アルゴリズム (QAOA) [22] という名前になる。しかし、これはまた、多粒子量子系 (例えば、大きな分子) の低エネルギー状態を見出すような量子問題にも適用することができる。量子問題に適用する場合、この量子・古典のハイブリッド手順は、Variation Quantum Eigensolver (VQE) [23] という名前で行われる。

QAOA または VQE を実行している NISQ 技術は、同じ問題に対するおおよその解決策を見出す古典的なアルゴリズムより優れた性能を発揮できるだろうか？誰も知らない。我々は、それを試して、どれくらいうまくいくかを見ていこう。これらの問題を解決するために使用する古典的な方法は、何十年にもわたって開発されて以来、磨きがかけているため、野心的な目標である。一方、たとえ初期の世代の NISQ デバイスが最高の古典的なコンピュータと競合する準備ができていなくても、実験結果は、QAOA や VQE が将来古典的な方法を上回るだろうという我々の期待を勇気づけるものになる可能性がある。そして、さらなる技術的改良に拍車がかかるだろう。

6.2 量子テストベッドがどのように役立つか

古典的コンピューティングの歴史は、ハードウェアが利用可能になると、新しいアルゴリズムの開発を刺激し加速すると教えている。実験的に発見されたヒューリスティックの例は数多くあり、理論家が最初に説明したことよりもそれがうまく動くのだ。我々は量子コンピュータでも同じことが起こるのを期待している。

例えば理論家は、最終的には、線形計画法のシンプレックス法がうまく機能する理由を説明したのだが [24]、それはそれが実験的に有用であることが判明してからずっと後のことだった。現在の例はディープ・ラーニングである [25]。そこでは、なぜそれがうまく機能するのかについての良い理論的説明が欠けている。量子の場合でも、実験でヒューリスティックなアルゴリズムの性能を検証することができる。ただ、ヒューリスティック・アルゴリズムが、なぜうまく機能するのか理解できていない。そういうことが、特に我々がテストしようとしている量子最適化アルゴリズムで起こるかもしれない。

しかし、NISQ システムの不完全なゲートは、多くのゲートを持つ回路が有用な結果をもたらすにはあまりにもノイズが多いため、計算能力が厳しく制限されていることを再度強調しなければならない。短期間の実験では、100qubit のオーダーと 100 以下の回路深度(タイムステップ数)で、できることを探求することになる。量子アルゴリズムの設計者とアプリケーション・ユーザーの間の活発な議論は、有望な方向にそれらの実験を向けさせるのに役立つ。今回のような会議の重要な目標は、そうした議論を促進し、刺激することである。

6.3 量子アニーリング

量子技術の現在のマイルストーンとして 50~100qubit を強調したが、実際には 2000qubit の量子デバイス、D-Wave 2000Q マシンがある。このマシンは、量子ゲート回路ベースの量子コンピュータではない。我々は、それをむしろ量子アニーラーと呼んでいる。量子回路の実行とは異なる方法を用いて最適化の問題を解こうとし、これらの問題を成功裏に解決することも多い。

しかし今のところ、量子アニーラーが、同じ問題に対して最良のアルゴリズムを実行する最高の古典的ハードウェアと比較して、解答までの時間を本当に高速化できるのかという点で説得力のある理論的議論や説得的な実験的証拠はない[26,27]。状況は少し微妙である。量子アニーラーは、断熱量子コンピューティング(adiabatic quantum computing)と呼ばれるもののノイズの多いバージョンである(D-Wave マシンの場合、量子ビットは、かなり品質は低い)[28]。ノイズのない量子ビットの場合、断熱量子コンピューティングが回路ベースの量子コンピューティングと同じくらい強力であることを示す理論的な議論が実際にある。しかし、断熱的方法と量子ゲート回路に基づく量子計算の等価性を示す議論は、断熱的方法が、量子的アニーラーが現在使用されている方法とはかなり異なる付加的な物理的量子ビットで高いオーバーヘッドコストを必要とする形式で実行される場合にのみ適用される[29]。いずれにしても、この正式な議論はノイズのない量子ビットにのみ適用され、回路ベースの量子コンピューティングとは対照的に、量子アニーリング装置がスケーラブルであることを証明する良い理論的議論はない。つまり、ノイズの多い量子ビットの場合、ノイズに対して頑強なものにする為のオーバーヘッドコストを受け入れたとしても、量子アニーラーが問題サイズの増加とともに正常に動作することを示す方法は分からないのだ。

今のところ量子アニーラーは、アニーリングが安定している場合に主に適用されている。このことは、古典的なコンピュータが量子アニーラーの動作をシミュレートすることは比較的容易だということを意味する[30]。間もなく予定されているのは、non-stoquastic な量子アニーラーである。これは、最高の古典的なアルゴリズムで可能な速度よりも高速化を達成する可能性がある。

理論家は量子アニーリングが強力であるかどうかを決定していないので、さらなる実験が必要である[31]。今後数年間の量子アニーラーの実験は、かなり有益である可能性が高い。特に、量子アニーラーの古典的な最適化問題への応用以外にも、量子シミュレーション問題への応用も検討すべきである。

6.4 ノイズ耐性量子回路

最終的には、我々は量子エラー訂正を使用して、ノイズの多い量子コンピュータを使用しながら、確実に実行できる計算のサイズを拡大していくだろうことを強調してきた。しかし、量子エラー訂正のオーバーヘッドコストが高いため、NISQ デバイスは近い将来には、それを使用しないだろう。それにもかかわらず、NISQ 時代には、ノイズの影響を緩和する方法が重要な検討事項になる。

素朴に考えれば、 G 個のゲートを備えた一般的な回路では、回路内のどこでも 1 つの失敗があると計算自体が失敗する可能性がある。そうであれば、ゲート当りの誤り率が $1/G$ よりもはるかに大きい場合、回路を確実に実行することができないことになる。しかし、少なくともいくつかの問題やアルゴリズムについていえば、この結論はあまりにも悲観的かもしれない。

特に、物理学者にとって興味のある量子シミュレーション・アルゴリズムのいくつかでは、欠陥のあるゲートによって計算がひどく失敗する可能性のある回路の場所は、比較的少数しかない。この特徴は、回路の深さが低いために発生している可能性がある。qubit 当たりのエラーの一定の確率だが、最終測定結果においてなら、我々は我慢できる。すなわち、回路で早い段階で発生したエラーに起因するダメージは、時間が経つと消えていくからである。このようなノイズ耐性は、Variant Quantum Eigensolver を用いて量子最適化問題を解くために呼び出すことができるいくつかのテンソルネットワーク構造の特徴である[32, 33]。

今後数年間にわたって協力しあえば、実験家や理論家には大きなチャンスがある。量子回路のノイズ耐性を向上させるための方法論を探求し、NISQ 技術の計算範囲を拡大するより良い方法を見つけるだろう。しかし、その潜在的なトレードオフとして、量子回路のノイズ耐性を高めることが、古典的なシミュレーションをも容易にするという可能性もあることも、意識したほうがいい。

6.5 量子ディープラーニング

機械学習は技術を変革し、科学にも大きな影響を与えている。それゆえ、量子技術と機械学習の組み合わせの可能性について、いろいろ考えるは当然である。「量子機械学習」には様々な概念がある。この主題に関する文献の多くは、線形代数とそれに関連するタスク[34, 35]を高速化する量子アルゴリズムをベースにしており、そのような応用については今後のサブセクションで取り上げたい。

まず最初に、量子ディープラーニング[36]の可能性について述べたい。ディープラーニングそのものは広い主題[25]を扱うのだが、ここでは、具体的には制限付きボルツマンマシン restricted Boltzmann machine (RBM)を検討しよう。制限付きボルツマンマシンは、低いがゼロではない温度で熱平衡状態にあるスピン系とみなされ、多くの隠れたスピン層が入力と出力を分離する。（「制限された」という言葉は、所与の層内のスピン間に結合がなく、連続する層のスピンのみが結合されることを意味している）システムは、入力と出力の間の望ましい結合確率分布を達成するために、訓練段階中に最適化される。訓練は教師付きで行われてもいい。例えば、ネットワークにラベル付けされた写真のセットを認識するように教えることができる。教師なしの場合、訓練の目標はラベルなしのトレーニングデータセットのパターンを識別することである。こうしたマシンの量子類似版は、古典的 RBM と類似の構造および機能を有することができる。ただし、スピンは古典的なビットではなく量子ビットである。量子ディープラーニング・ネットワークは古典的なものよりも利点があるかもしれない。たとえば、いくつかの目的のためには、量子版を訓練するほうが簡単かもしれない。しかし、我々はそれを本当に知っていない。それを試して、それがどれくらいまくいくかを試して見るいい機会である。

量子機械学習の可能性に期待する理由の 1 つは、QRAM(量子ランダムアクセスメモリ)という概念にある。QRAM とは、 N 個の成分をもつベクトルを $\log N$ 個の qubit で符号化することで、大量の古典的データを非常に簡潔に表現することを意味する。しかし、量子機械学習の応用の典型的な提案では、厳しい入力/出力ボトルネックによって混乱することになる。大規模な古典的なデータセットへの応用では、QRAM への入力を符号化するコストを考慮に入れるべきであり、それが潜在的な利点を無効にする可能性がある。さらにいえば、量子ネットワークからの出力自体が量子状態である。すなわち、有益な情報を得るためには、この量子状態を測定する必要がある。 $\log N$ 個の qubit の一回の測定では、 $\log N$ ビット以上の古典的な情報を取得することはできない

これらのボトルネックは、古典的なデータの相関を知るために量子ネットワークを訓練しようとするときに発生する。おそらく、入力と出力の両方が量子状態であるという設定で、量子機械学習について考えてみるのが、より自然である。したがって、例えば、それが、複雑な量子システムを制御するために使用される場合、量子ネットワークが古典的ネットワークよりも利点があると期待することができる。より広く言えば、量子もつれが重要な役割を果たす確率分布を学習しようとする場合、量子ディープラーニングは古

典型的なそれよりも強力であると思われる。つまり、量子ディープラーニング・ネットワークは量子的なタスクに非常に適しているかもしれないのだが、今日広く普及しているディープラーニングのアプリケーションでは、量子ネットワークに利点があるのかどうかは不明である。

量子ディープラーニングの可能性を励ます側で述べれば、量子ディープラーニング・マシンは、必ずしも汎用回路ベースの量子コンピュータである必要はないという点に注目する価値がある。それは特別な目的のデバイスになるかもしれない。おそらく、ノイズが低いものであれば、量子アニーラーが、それにあたる可能性がある。

6.6 量子行列反転

QRAM は、量子アルゴリズムでは、さらに別の意味を持っている。特に、行列反転のタスクは、指数関数的な量子高速化を可能にし、多くの応用が可能である。

HHL[37]アルゴリズム（9年前に最初に議論した3人の著者 Hallow, Hassidim, Lloyd の名前をとった）は、簡潔に表現された非常に大きな $N \times N$ 行列 A を入力とする。 A は十分に疎で条件づけされているものとする。入力の N 個の成分をもつベクトル $|b\rangle$ は、QRAM で符号化され $\log N$ 個の qubit の量子状態にエンコードされる。量子アルゴリズムの出力は、小さな誤差で量子状態 $|A^{-1}b\rangle$ すなわち、入力ベクトル $|b\rangle$ に行列 A の逆行列を適用した結果である。この量子アルゴリズムは、古典的な行列反転に対して指数関数的に高速な時間 $O(\log N)$ で実行される。

ただ、行列 A はスパースであり条件がよくなければならないという注意点とは別に、入力ベクトル $|b\rangle$ と出力ベクトル $|A^{-1}b\rangle$ の両方が量子状態であることに留意されたい。いったん出力状態になると、出力ベクトル $|A^{-1}b\rangle$ の特徴を学ぶための測定を実行することができ、このスキームを何度も繰り返すことにより、出力ベクトルについてより詳細に知ることができる。しかし、この行列反転アルゴリズムを古典的な入力データに適用しようとする場合、その古典的なデータを QRAM にロードする潜在的なコストを考慮する必要がある。これは指数関数的な高速化を無効にする可能性がある。代わりに、QRAM に古典的なデータをロードすることは、データベースから入力するのではなく、量子コンピュータ上で $|b\rangle$ を計算することによって回避することができる。

この量子行列反転アルゴリズムは、我々が BQP-完全な問題と呼ぶものを解決するもので、強力なものであると信じる十分な理由がある。つまり、量子コンピュータで効率的に解決できるどんな問題も、この行列反転問題の一例として問題をエンコードすることができる。

また、潜在的に有用な多くのアプリケーションが提案されている。たとえば、この行列反転アルゴリズムを使用して、古典的な線形方程式[38](場を空間格子上で離散化し、適切な前処器を適用した後)に近似解を見つけることができる。この手順は、例えば、アンテナの性能を最適化するために、複雑な 3 次元形状の電磁気方程式を解くために使用することができる。

私は、HHL が最終的に影響の大きい応用を持つことを期待しているが、NISQ 時代には実現することはない。このアルゴリズムはおそらく、エラー訂正を使用しない量子コンピュータでうまく実行されるには高いものにつきすぎる。

6.7 量子リコメンデーション・システム

最近提案されたもう 1 つの量子アルゴリズム[39]は、有益なタスクのための現在知られている最高の古典的アルゴリズムよりも指数関数的な高速化を提供する。このアルゴリズムの目標は、顧客および他の顧客の好みの限られた知識に基づいて、顧客がおそらく好むであろう製品を顧客に推奨することである。

問題の簡略化されたバージョンを定式化するには、 m 人の顧客と n 個の製品を考え、 P を次のような二値の値をとる $m \times n$ の行列とする。顧客 a が製品 i を好む場合は $P_{ai} = 1$ 、顧客が製品 i を嫌う場合は $P_{ai} = 0$ となるようにする。実際には、 $m \approx 10^8$ 人のユーザーと $n \approx 10^6$ の製品を持つかもしれないが、行列のランク k は比較的小さく、おそらく $k \approx 100$ となる。このランクの小ささは、顧客のタイプの数に限られていることを示している。したがって、新しい顧客の好みのいくつかを知ったら、顧客が好む他の製品を正確に推奨することができる。

リコメンデーション・システムのためのアルゴリズムは 2 つの段階もつ。オフラインで実行される第 1 段階では、嗜好行列 P に対する低いランクの近似が構築される。第 2 段階では、オンラインで実施され、新しい顧客はいくつかの嗜好を明らかにし、システムは、その顧客が高い確率で好む推奨を出力する。量子スピードアップが認められるのはこの第 2 のオンラインステージである。量子ランタイムは $O(\text{poly}(k) \text{polylog}(mn))$ だが、既知の最良の古典的なアルゴリズムでは、 $\text{poly}(mn)$ が高い値の推奨値を返すために時間が必要となる。重要なのは、古典的アルゴリズムとは対照的に、量子アルゴリズムは完全な推奨行列を再構成しようとはしないということである。代わりに、 P の低ランクの近似から効率的にサンプリングをする。

これは、機械学習の現実の応用のための重要な量子高速化であり、こうした別の高速化が発見されるだろうという希望を励ますものだ。しかし、現在、量子リコメンデーションシステム($\text{polylog}(mn)$ 時間で高品質のリコメンドを返す)によって実行されるタスクが古典的に不可能であることを示す納得のいく理論的議論はない。そのような議論を定式化することは、量子コンピュータが機械学習に重大な影響を及ぼすという我々の自信を強めるだろう。しかし、ここでもこのアルゴリズムは NISQ 時代に確かに妥当性が確認されるには高価すぎるだろう。

6.8 半正定値プログラミング

半正定値プログラミングは、行列がある不等式の制約条件に従うという条件のもとで線形関数を最適化するタスクである。具体的には、 $m + 1$ 個の $N \times N$ のエルミート行列 $\{C, A_1, A_2, \dots, A_m\}$ および実数 $\{b_1, b_2, \dots, b_m\}$ が入力として与えられた時、制約条件 $\text{tr}(A_i X) \leq b_i$ に従う $\text{tr}(CX)$ を最大にする正の半正定値の $N \times N$ 行列 X を見つけるという問題である。このタイプの凸最適化問題は広範な応用を有し、古典的には $\text{poly}(m, N)$ 時間で解くことができる。

最近発見された量子アルゴリズム[40, 41]は、 $\text{polylog}(N)$ 時間で近似解を発見する。これは指数関数的な高速化である。この量子アルゴリズムでは、出力は量子状態を表す密度演算 ρ であり、それが最適な行列 X を近似することになる。この量子状態は、 X に関する情報を抽出するために測定することができ、その手順は詳細な情報を得る為、何回も繰り返される。

しかし、この量子アルゴリズムの解析では、ある特定の形式の量子初期状態が利用可能であることを仮定している。その状態である熱的 Gibbs 状態は、半正定値プログラムの入行列の線形結合であるハミルトニアンに関連付けられている。指数関数的な高速化が実際に実現できるかどうかは、このギブス状態が量子コンピュータを用いて効率的に準備できるかどうかにかかっている。正しい構造の半正定値プログラムの場合、ギブス状態の効率的な準備が可能である。したがって、指数関数的な高速化が実際に可能となる。特に、半正定値プログラムのすべての入行列が低いランクを有する場合、すなわち対応するハミルトニアンシステムが急速に熱平衡化する場合、量子アルゴリズムは指数関数的な高速化を達成する。これらの特性が実質的に関心のある半正定値的なプログラムにどの程度適用されるかはまだ明らかではない。この問題を明確にすることが、さらなる研究の重要な目標である。

この量子アルゴリズムの重要なステップが、非ゼロ温度での熱的平衡状態の準備であることは興味深いことである。これは、このアルゴリズムが熱的ノイズに対して本質的な頑健性を有すること、また、このア

ルゴリズムの熱的平衡化の段階が量子アニーリングによって実行可能であることを示唆することができ
る。おそらく、半正定値的プログラムのための量子ソルバーは、NISQ 技術の範囲内にあるかもしれない

6.9 量子シミュレーション

私がすでに強調しているように、量子コンピュータは、多くの粒子の非常にもつれあったシステムの特
性を研究するのに非常に適していると考えている。以前に引用した Laughlin と Pines[8]が強調したように、
このような「強く相関する」問題をシミュレートするのは難しい計算問題であると考えている。実際、多くの
非常に優れた物理学者が数十年間それを解決しようとしてきて成功しなかったのだから。したがって、
Feynman が主張しているように[9]、非常にもつれあった量子物質のシミュレーションは、量子コンピュ
ータが古典的なものよりも明確な利点を有するように見える自然な場である。

長期的には、量子コンピュータを用いた量子シミュレーションは、世界に広い影響を与える可能性が大
きい[42, 43, 44]。量子コンピューティングによって容易なものになった量子化学の進歩は、新しい医薬
品や、窒素固定または炭素捕捉の効率を改善する新しい触媒の設計を大いに進めると可能性がある。
また、量子シミュレーションから生じる新しい材料は、より効果的な送電または太陽エネルギーの収集の
改善につながる可能性がある。我々は、よりパワフルな量子シミュレータから生まれて来る、最も世界を
変えるような発見を予期する想像力が不足している。しかし、大規模な分子やエキゾチックな物質を正
確にシミュレートするための量子アルゴリズムは、エラー訂正なしで成功するには高価すぎるかもしれな
いので、この約束は NISQ 時代には実現しそうにない。

古典的なコンピュータは、特に、量子力学をシミュレートすること、つまり、もつれあった量子状態が時間
とともにどのように変化するかを予測するのに、ひどく向いていない。それに対して、量子コンピュータは
その仕事には大きな利点があり、物理学者は NISQ 技術を使って、比較的短い期間のうちに、量子力
学についての興味深いことを学ぶことを望んでいる。古典的なカオス理論(古典力学系の初期条件に
対する極端な影響の受けやすさ、それが 2 週間以上先の天気予報ができないことを説明するのだが)
は、60 年代と 70 年代に、古典的なコンピュータを使ってカオス的な力学系をシミュレートすることが可
能になってから急速に進展した。(エンタングルメントが非常に急速に広がる)カオス量子システムをシミ
ュレートする新たな能力が、量子カオスの理解の進歩を促進することが予想される。すでに、貴重な洞
察が、100 qubit のオーダーのノイズのあるデバイスを使用して収集されている可能性がある。

6.10 デジタル対アナログ量子シミュレーション

量子力学をシミュレートする潜在的な価値を強調したので、アナログとデジタルの量子シミュレーションの違いについてもコメントする必要があるだろう。アナログ量子シミュレータについて言えば、それは、我々が、研究して理解しようとしているモデルシステムのダイナミクスに類似したダイナミクスを持つ、多くの量子ビットを持つシステムを意味する。対照的に、デジタル量子シミュレータは、適切にプログラムされた場合に任意の物理的システムをシミュレートするために使うことができるゲートベースの汎用量子コンピュータであり、他の目的にも使用することができる。

アナログ量子シミュレーションは、過去 15 年間、非常に活発な研究領域だったが、汎用回路ベースの量子コンピュータによるデジタル量子シミュレーションが今や始まろうとしている。しかし、イオン・トラップや超伝導回路などの同じ実験プラットフォームのいくつかは、両方の目的に使用できる。アナログ量子シミュレータは、より洗練されてきており、古典的なシミュレータの到達範囲を超えた枠組みで量子力学を研究するためにすでに採用されている[45, 46]。しかし、アナログ量子シミュレータは、不完全なコントロールしかできないことで、その機能は妨げられている。実験室の実際の量子システムは、対象のモデルシステムの荒い近似でしかない。このため、アナログシミュレータは、小さな誤差が入り込むことについては比較的堅牢な、物理学者が「普遍的」な特性と呼ぶ物理的特性を研究するのに最も適している。

アナログ量子シミュレータは最終的に時代遅れになることが予想される。それらは制御が難しいため、量子エラー訂正を使用して確実に制御することができるデジタル量子シミュレータによって、ある日乗り越えられるだろう。しかし、量子エラー訂正のオーバーヘッドコストが非常に高いため、アナログ量子シミュレータの時代は長年にわたって続く可能性がある。したがって、量子技術の短期間の応用を目指す場合、アナログ量子シミュレータの潜在的な可能性を見落とすべきではない。

6.11 量子ゲーム

古典的コンピューティングの進歩は、数百万の人の人生に触れ、何十億ドルもの収益を生み出すデジタルゲームの新しい世界を生み出した。量子コンピュータは同じことができるのだろうか？

物理学者はしばしば、量子世界は、直感に反しているという。なぜなら、それは日常の経験とは非常に異質であるからである。それは今のところ本当なのだが、将来それは違うかもしれない可能性はないだろうか？おそらく、量子ゲームをプレイする子供たちは、私たちの世代に欠けている量子現象の内在的な理解を得るだろう。量子もつれあい不可欠な役割を果たす状況の中で、チャンスをうまく掴めば、ゲームを有利に進められるといった量子ゲームができれば、それは、量子機械学習法の新領域を開くことができる可能性だってあるかもしれない。

7 スケーラビリティへの困難な挑戦

困難な問題を解決するフォールト・トレラントな量子コンピュータが登場するまでには、おそらく長い時間がかかることを繰り返し強調してきた。それにもかかわらず、我々は、量子エラー訂正符号を用いた比較的小規模の実験によって導かれ、量子エラー訂正を実現するためのより良い方法とハードウェアを開発することで、近い将来に著しい進歩を遂げることができるだろう。今後数年間で、誤り訂正された量子ビットの強化された制御が初めてラボで確かに実証されることを期待している。量子エラー訂正を探索する、当面のさらなる実験は、量子デバイスにおけるノイズの理解を促進し、ノイズ軽減[47]およびデバイス検証[48, 49]のためのより効果的な手法を提案することに結びついている。

それにもかかわらず、フォールト・トレラント量子コンピューティングを使用した実際の難しいな問題(数千ビットの素因数分解)を解決することは、必要な物理 qubit の数が多いためしばらくは起こりそうにもない。数千のエラー保護された qubit を含むアルゴリズムを実行するには、数百万かそれ以上の数の物理的 qubit が必要[50]であるからである。これは、今後数年間で我々が到達するであろう数百 qubit のオーダーからは、非常に大きな飛躍である。数百の物理 qubit から数百万の物理 qubit へと「量子カズム」を越えるには時間がかかるだろうが、最終的には、我々はそこに行き着くだろう。

NISQ 時代には、さまざまな量子プラットフォームでより低いゲートエラー率を目指すことが重要である。より正確な量子ゲートにより、誤り訂正を行わずに動作する量子コンピュータは、より大きな回路を実行することによってさらに進歩することができる。将来的にフォールト・トレラントな量子コンピューティングに移行する際に、より良いゲートを使用することで、量子誤り訂正のオーバーヘッドコストを削減できる。(トポロジカル量子コンピューティングの前進に焦点を当てたマイクロソフトの現在のプログラム[51]は、将来的には低いゲートエラー率が成功するという考えに基づいている。)

十分にスケーラブルなフォールト・トレラント量子コンピュータを実現するためには、基本的な科学とシステム工学の重要な進歩が必要であることを認識することが重要である。それゆえ、スケーラビリティへの挑戦は、科学者やエンジニアにとって魅力的な問題を提起している。我々は、まだまだ遠くに進んでいく必要があるのだ。だから、新らしい洞察や開発そしてイノベーションが、長期的な見通しを大きく変える可能性がある。

8 まとめ

この論文は落ち着いた妥協の産物である。技術的な知識のある読者のために有用なオーバービューを提供することを望みながら、広い層が関心を失ったり当惑しないように難しい専門用語や技術的な詳細を最小限に抑えようとした。私は参考文献の包括的なリストをつくろうとしなかった。代わりに、私が強調し明確にしたかったことを示すいくつかの論文を引用した。それは、今後、さらにどのような論文を読むべきを示唆してくれると思う。貴重な貢献を適切に触れることができなかった多くの同僚にお詫びしようと思う。

今回、私が伝えようとした主な点を要約しよう。

- NISQ の時代 (NISQ: noisy intermediate-scale quantum = ノイズのある中規模の量子コンピュータ) を目の当たりにしている現在は、科学技術史の中で特別な時代である。我々は、すぐにでも NISQ 技術を実験する機会を得て、それで何ができるかを見ることになるだろう。おそらく、NISQ は、近い将来のうちに、広い範囲の問題の解決の時間を早めることを可能にするだろう。ただ、それが実際に起こるかどうかはまだ分からない。
- ある分野では、我々が試したいと思っている具体的なアイデアがある。古典論的・量子論的双方の最適化の問題を解決するための量子古典ハイブリッド・アルゴリズムは、そうしたものだ。
- 量子コンピュータでの実験によって、量子アルゴリズムの開発が加速することを期待できる。有用な問題を解決するために新しいヒューリスティクスが発見されるかもしれない。ただ、そのヒューリスティクスが、なぜうまく働くのかを、少なくともすぐには説明することが出来ないかもしれないのだが。
- おそらく、NISQ 時代のデバイスをノイズから保護するために、本格的な量子誤り訂正技術を利用することはできないのだが、当面は、ノイズ耐性を念頭においた量子アルゴリズムを設計する必要がある。ノイズ耐性アルゴリズムを賢く設計することが、NISQ デバイスの計算能力を拡張する可能性がある。
- 古典的なコンピュータは、とりわけ、非常にもつれあった多数の粒子からなる量子システムの力学をシミュレートするのに、全く向いていない。したがって、量子力学は、量子コンピュータが古典的なコンピュータより著しい利点を有する、特別に有望な分野である。

- 我々は、より低いゲート誤り率をもつ量子ハードウェアの構築に引き続き焦点を当てるべきである。改善された量子ゲートの正確さは、最終的に実現されるとき量子誤り訂正のオーバーヘッドコストを低減する。近い将来には、より正確なゲートにより、より大きな量子回路を実行することができ、NISQ 技術のパワーを拡張することが可能になるだろう。
- NISQ が、世界全体を変える可能性はほとんどないように見える。その代わりに、近い将来の量子プラットフォームの第一の目標は、その先にあるより高度な量子デバイスが実現するより大きな利益のための道を開くことである。
- 未来の真の世界を変える量子技術はフォールト・トレラントなものでなければならない。量子エラー訂正のオーバーヘッドコストが非常に高いため、フォールト・トレラントな量子コンピューティングの時代はまだ遠いかもしれない。実際には、誰もそこに着くのにかかるのにかかるの時間がかかるとは知らないのだ。量子コミュニティは、NISQ デバイスを実験する差し迫った機会を熱烈に手に入れようとしているのだが、我々はフォールト・トレラント時代の始まりを早めるという本質的な長期目標を見失わないようにしなければならない。

私はこの論文での発言には注意深い立場を取ってきた。なぜなら、我々は NISQ 時代の始まりに、十分な根拠に基づいた期待をもって直面すべきだと考えているからである。しかし、私のことを誤解しないで欲しい。皆さんと同じように、私は今後数年間での NISQ 時代の展開に引き続く様々の発見に熱烈に期待している。量子技術には明るいチャンスが広がっており、その前途には多くの興奮するような驚きがあるのは確かである。しかし、私たちが直面している課題は依然として手強いものである。すべての量子力学者は、我々の分野では何十年にもわたる持続的でインスパイアされた努力によってのみその可能性を発揮できることを認識しなければならない。我々がその代償を支払うとき、究極の報酬は我々の努力を証明する以上のものになるだろう。

謝辞

この刺激的なカンファレンスを組織し、私に参加を呼びかけてくれた Matt Johnson に感謝する。ここで私の発言は、多くの同僚との議論の影響を受けている。しかし、私は、Scott Aaronson, Sergio Boixo, Fernando Brandao, Elizabeth Crosson, Toby Cubitt, Eddie Farhi, Steve Flammia, David Gosset, Daniel Gottesman, Stephen Jordan, Jordan Kerenidis, Isaac Kim, Seth Lloyd, Shaun Maguire, Oskar Painter, David Poulin, Peter Shor, Brian Swingle, Matthias Troyer, Umesh Vazirani, Thomas Vidick による洞察力から特に利益を得ている。この作業の一部は、Kavli 理論物理学研究所 (KITP) の量子物理

学に関する 2017 年のプログラムに参加している間に行われた。ARO、DOE、IARPA、NSF、Simons Foundation のサポートに感謝する。量子情報研究所 (IQIM) は、Gordon and Betty Moore Foundation の支援を受けている NSF 物理フロンティアセンターである。

参考文献

- [1] P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM Rev. 41, 303-332 (1999).
- [2] A. P. Lund, M. J. Bremner, and T. C. Ralph, Quantum sampling problems, BosonSampling, and quantum supremacy, npj Quantum Information 3: 15 (2017), arXiv:1702.03061.
- [3] A. W. Harrow and A. Montanaro, Quantum computational supremacy, Nature 549, 203-209 (2017).
- [4] S. P. Jordan, Quantum algorithm zoo, <http://math.nist.gov/quantum/zoo/>.
- [5] A. Montanaro, Quantum algorithms: an overview, npj Quantum Information, 15023 (2016), arXiv:1511.04206.
- [6] L. Grover, Quantum mechanics helps in searching for a needle in a haystack, Phys. Rev.Lett. 79, 325 (1997), arXiv:quant-ph/9706033.
- [7] C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani, Strengths and weaknesses of quantum computing, SIAM J. Comput. 26, 1510-1523 (1997), arXiv:quant-ph/9701001.
- [8] R. B. Laughlin and D. Pines, The theory of everything, PNAS 97, 28-31 (2000).
- [9] R. P. Feynman, Simulating physics with computers, Int. J. Theor. Physics 21, 467-488 (1982).
- [10] D. Gottesman, An introduction to quantum error correction and fault-tolerant quantum computation, Proceedings of Symposia in Applied Mathematics 68 (2010), arXiv:0904.2557.
- [11] S. Boixo, S. V. Isakov, V. N. Smelyansky, R. Babbush, N. Ding, Z. Jiang, M. J. Bremner, J. M. Martinis, H. Neven, Characterizing quantum supremacy in near-term devices, arXiv:1608.00263 (2016).
- [12] S. Aaronson and L. Chen, Complexity-theoretic foundations of quantum supremacy experiments, arXiv:1612.05903 (2017).
- [13] E. Pednault, J. A. Gunnels, G. Nannicini, L. Horesh, T. Magerlein, E. Solomonik, and R. Wisnieff, Breaking the 49-qubit barrier in the simulation of quantum circuits, arXiv:1710.05867 (2017).
- [14] C. J. Ballance, T. P. Harty, N. M. Linke, M. A. Sepiol, and D. M. Lucas, High-fidelity quantum logic

- gates using trapped-ion hyperfine qubits, *Phys. Rev. Lett.* 117, 060504 (2016), arXiv:1512.04600.
- [15] 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* 508, 500-503 (2014), arXiv:1402.4848.
- [16] D. J. Bernstein, J. Buchmann, E. Dahmen, editors, *Post-Quantum Cryptography*, Springer (2009).
- [17] R. Alléaume, C. Branciard, J. Bouda, T. Debuisschert, M. Dianati, N. Gisin, M. Godfrey, P. Grangier, T. Langer, N. Lütkenhaus, C. Monyk, P. Painchault, M. Peev, A. Poppe, T. Pornin, J. Rarity, R. Renner, G. Ribordy, M. Riguiedel, L. Salvail, A. Shields, H. Weinfurter, and A. Zeilinger, Using quantum key distribution for cryptographic purposes: a survey, *Theoretical Computer Science* 560, 62-81 (2014), arXiv:quant-ph/0701168.
- [18] S. Muralidharan, L. Li, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, Efficient long distance quantum communication, *Scientific Reports* 6, 20463 (2016), arXiv:1509.08435.
- [19] C. L. Degen, F. Reinhard, and P. Cappellaro, Quantum sensing, *Rev. Mod. Phys.* 89, 035002 (2017), arXiv:1611.04691.
- [20] J. Preskill, Quantum computing and the entanglement frontier, 25th Solvay Conference on Physics (2011), arXiv:1203.5813.
- [21] S. Khot, Hardness of approximation, *International Congress of Mathematicians* (2014).
- [22] E. Farhi, J. Goldstone, and S. Gutmann, A quantum approximate optimization algorithm, arXiv:1411.4028 (2014).
- [23] J. R. McClean, J. Romero, R. Babbush, and A. Aspuru-Guzik, The theory of variational hybrid quantum-classical algorithms, *New J. Phys.* 18, 023023 (2016), arXiv:1509.04279.
- [24] D. A. Spielman and S.-H. Teng, Smoothed analysis of algorithms: why the simplex algorithm usually takes polynomial time, *Journal of the ACM* 51, 385-463 (2004), arXiv:cs/0111050.
- [25] Y. LeCun, Y. Bengio, and G. Hinton, Deep learning, *Nature* 521, 436-444 (2015).
- [26] T. F. Rønnow, Z. Wang, J. Job, S. Boixo, S. V. Isakov, D. Wecker, J. M. Martinis, D. A. Lidar, and M. Troyer, Defining and detecting quantum speedup, *Science* 345, 420-424 (2014).
- [27] S. Mandrà, H. G. Katzgraber, and C. Thomas, The pitfalls of planar spin-glass benchmarks: raising the bar for quantum annealers (again), *Quantum Sci. Technol.* 2, 038501 (2017), arXiv:1703.00622.
- [28] T. Albash and D. A. Lidar, Adiabatic quantum computing, arXiv:1611.04471 (2016).

- [29] D. Aharonov, W. van Dam, J. Kempe, Z. Landau, S. Lloyd, and O. Regev, Adiabatic quantum computation is equivalent to standard quantum computation, *SIAM Rev.* 50, 755-787 (2008), arXiv:quant-ph/0405098.
- [30] S. Bravyi, D. DiVincenzo, R. I. Oliveira, B. M. Terhal, The complexity of stoquastic local Hamiltonian problems, *Quant. Inf. Comp.* 8, 0361-0385 (2008), arXiv:quant-ph/0606140.
- [31] R. Harris et al., unpublished (2017).
- [32] I. H. Kim, Noise-resilient preparation of quantum many-body ground states, arXiv:1703.00032 (2017).
- [33] I. H. Kim and B. Swingle, Robust entanglement renormalization on a noisy quantum computer, arXiv:1711.07500 (2017).
- [34] J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, and S. Lloyd, Quantum machine learning, *Nature* 549, 195-202 (2017), arXiv:1611.09347.
- [35] S. Aaronson, Read the fine print, *Nature Physics* 11, 291-293 (2015).
- [36] X. Gao, Z. Zhang, and L. Duan, An efficient quantum algorithm for generative machine learning, arXiv:1711.02038 (2017).
- [37] A. W. Harrow, A. Hassidim, and S. Lloyd, Quantum algorithm for linear systems of equations, *Phys. Rev. Lett.* 103, 150502 (2009), arXiv:0811.3171.
- [38] B. D. Clader, B. C. Jacobs, and C. R. Sprouse, Preconditioned quantum linear system algorithm, *Phys. Rev. Lett.* 110, 250504 (2013), arXiv:1301.2340.
- [39] I. Kerenidis and A. Prakash, Quantum recommendation systems, arXiv:1603.08675 (2016).
- [40] F. G. S. L. Brandão and K. Svore, Quantum speed-ups for semidefinite programming, *Proceedings of FOCS 2017*, arXiv:1609.05537 (2017).
- [41] F. G. S. L. Brandão, A. Kalev, T. Li, C. Y.-Y. Lin, K. M. Svore, and X. Wu, Exponential quantum speed-ups for semidefinite programming with applications to quantum learning, arXiv:1710.02581 (2017).
- [42] M. Reiher, N. Wiebe, K. M. Svore, D. Wecker, and M. Troyer, Elucidating reaction mechanisms on quantum computers, *PNAS* 117, 7555-7560 (2017), arXiv:1605.03590.
- [43] D. Wecker, M. B. Hastings, N. Wiebe, B. K. Clark, C. Nayak, and M. Troyer, Solving strongly correlated electron models on a quantum computer, *Phys. Rev. A* 92, 062310 (2015), arXiv:1506.05135.
- [44] J. Olson, Y. Cao, J. Romero, P. Johnson, P.-L. Dallaire-Demers, N. Sawaya, P. Narang, I. Kivlichan, M. Wasielewski, A. Aspuru-Guzik, Quantum information and computation for chemistry, NSF Workshop

Report, arXiv:1706.05413 (2017).

[45] H. Bernien, S. Schwartz, A. Keesling, H. Levine, A. Omran, H. Pichler, S. Choi, A. S. Zibrov, M. Endres, M. Greiner, V. Vuletić, M. D. Lukin, Probing many-body dynamics on a 51-atom quantum simulator, *Nature* 551, 579-584 (2017), arXiv:1707.04344.

[46] J. Zhang, G. Pagano, P.W. Hess, A. Kyprianidis, P. Becker, H. Kaplan, A. V. Gorshkov, Z.-X. Gong, C. Monroe, Observation of a many-body dynamical phase transition with a 53-qubit quantum simulator, arXiv:1708.01044 (2017).

[47] E. T. Campbell, B. M. Terhal, and C. Vuillot, The steep road towards robust and universal quantum computation, arXiv:1612.07330 (2016).

[48] J. J. Wallman and J. Emerson, Noise tailoring for scalable quantum computation via randomized compiling, *Phys. Rev. A* 94, 052325 (2016), arXiv:1512:01098.

[49] J. Combes, C. Granade, C. Ferrie, and S. T. Flammia, Logical randomized benchmarking, arXiv:1702.03688 (2017).

[50] A. G. Fowler, M. Mariantoni, J. M. Martinis, and A. N. Cleland, Surface codes: towards practical large-scale quantum computation, *Phys. Rev. A* 86, 032324 (2012), arXiv:1208.0928.

[51] S. Das Sarma, M. Freedman, and C. Nayak, Majorana zero modes and topological quantum computation, *npj Quantum Information* 1, 15001 (2015), arXiv:1501.02813.