2/17 マルレク@DMM

量子コンピュータの現在

-- 量子優越性のマイルストーンの達成 --

2/17 マルレク Agenda

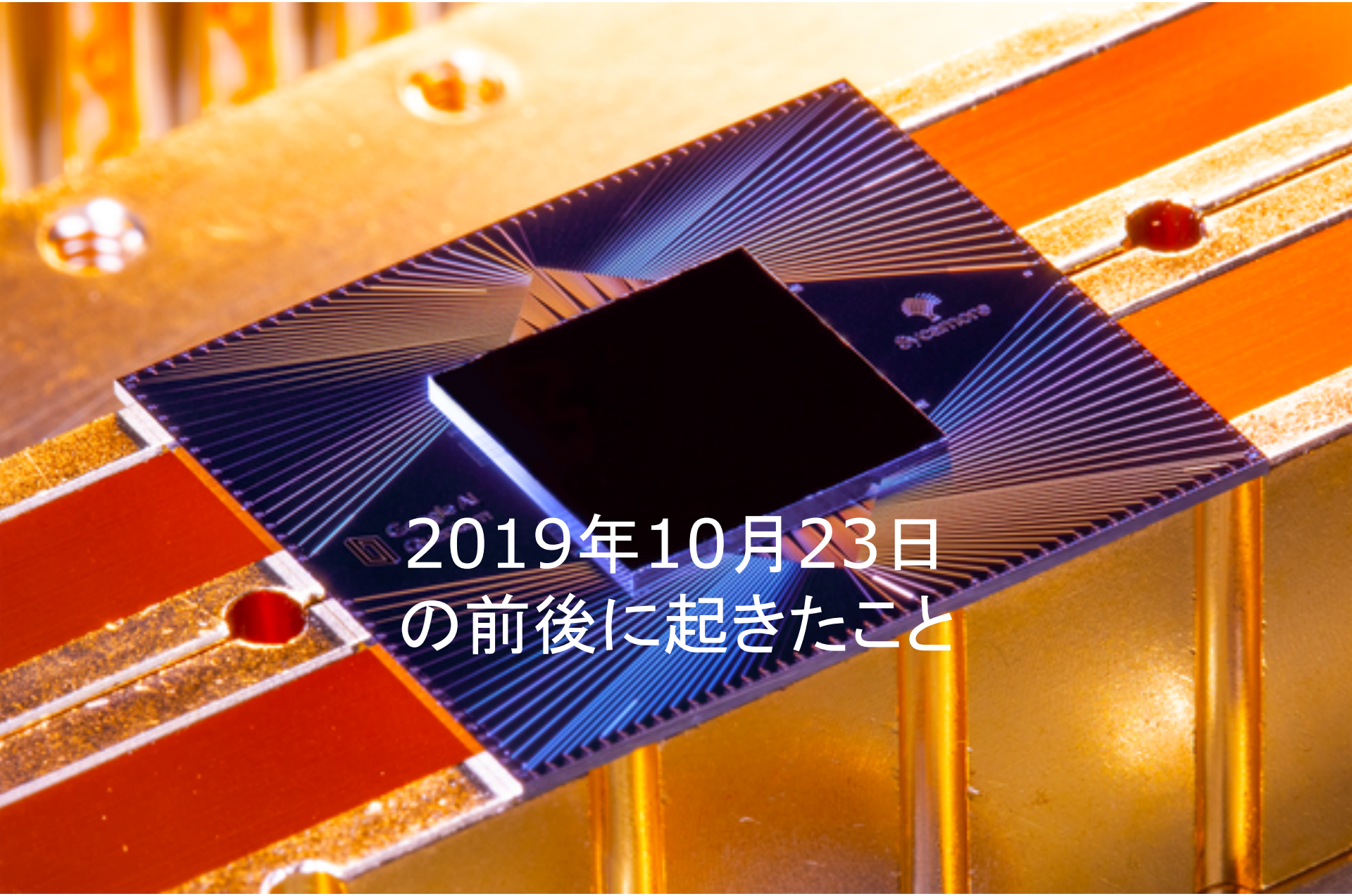
- 2019年10月23日の前後に起きたこと
- なぜ、量子優越性を示すことが重要だったのか？
  - 量子優越性とは何か？
  - 量子技術の発展
  - 量子優越性実証への関心の集中
  - 実験前夜　NISQ時代の課題

2/17 マルレク Agenda

- Googleはどんな実験をしたのか
  - Google論文の概要
  - 量子ビットについて基本的なことを確認しよう
  - ランダム量子回路
  - 量子コンピュータの動作を図解する
  - 量子優越性の実験はどのように行われたか
  - IBM論文の指摘
  - IBM論文に対するAaronsonの指摘
  - 科学・技術のマイルストーンを考える

2/17 マルレク Agenda

- 量子優越性をめぐる「論争」
  - 私はなぜそれを量子優越性と呼んだのか？
  - IBM Research Blogの二つの問題
  - 優越性は人種差別主義者のもの
  - ダボス会議でのIBM量子パネル
- 「拡大されたチャーチ＝チューリング・テーゼ」の終焉


2019年10月23日
の前後に起きたこと

Article | Published: 23 October 2019

Quantum supremacy using a programmable superconducting processor

Frank Arute, Kunal Arya, [...] John M. Martinis

Nature **574**, 505–510(2019) | Cite this article

Abstract

The promise of quantum computers is that certain computational tasks might be executed exponentially faster on a quantum processor than on a classical processor[1]. A fundamental challenge is to build a high-fidelity processor capable of running quantum algorithms in an exponentially large computational space. Here we report the use of a processor with programmable superconducting qubits[2,3,4,5,6,7] to create quantum states on 53 qubits, corresponding to a computational state-space of

2019年10月23日
Natureに論文発表

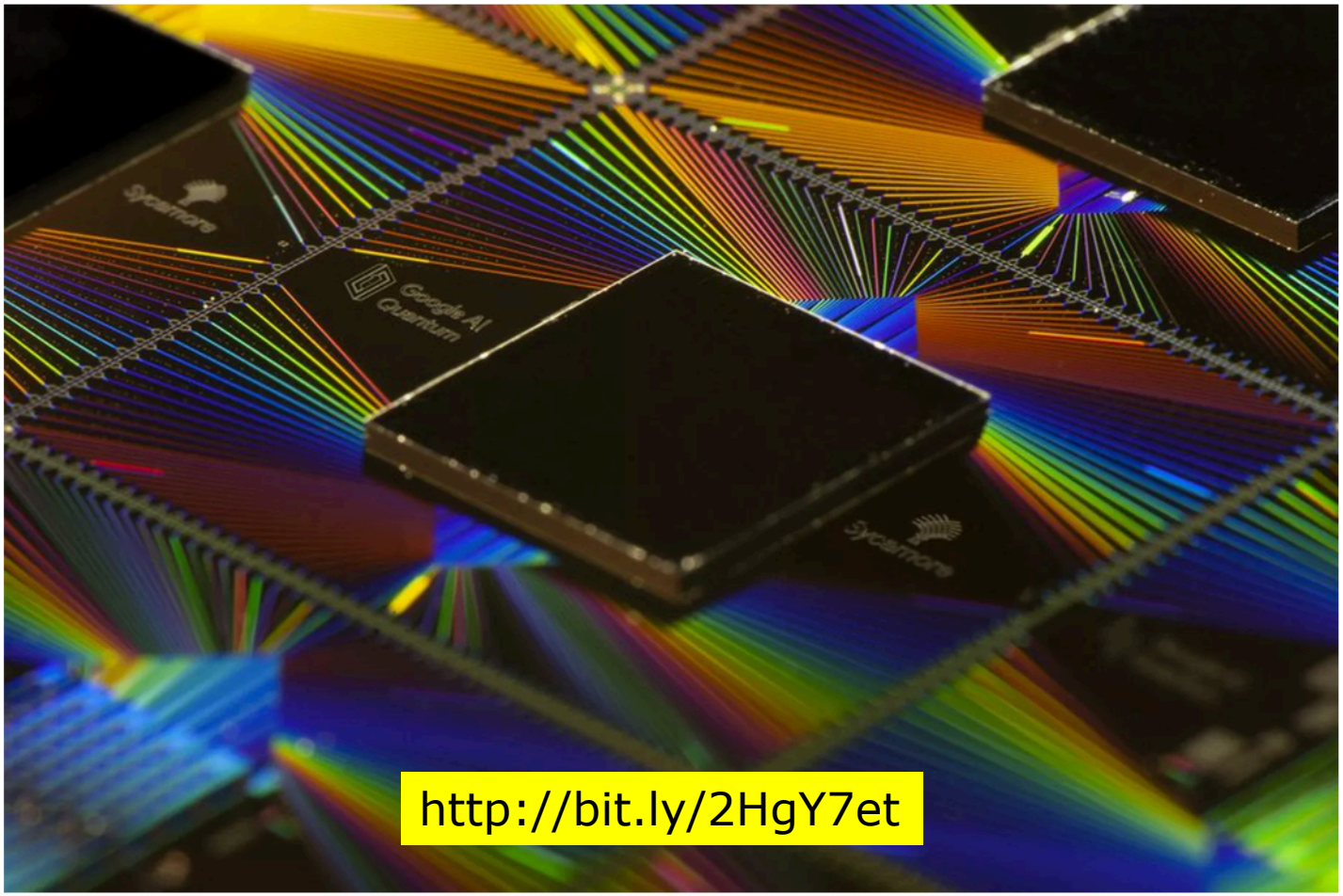
circuit a million times—our benchmarks currently indicate that the equivalent task for a state-of-the-art classical supercomputer would take approximately 10,000 years. This dramatic increase in speed compared to all known classical algorithms is an experimental realization of quantum supremacy[8,9,10,11,12,13,14] for this specific computational task, heralding a much-anticipated computing paradigm.

Google confirms 'quantum supremacy' breakthrough

Its research paper is now available to read in its entirety

By Jon Porter | @JonPorty | Oct 23, 2019, 6:31am EDT

SHARE



http://bit.ly/2HgY7et

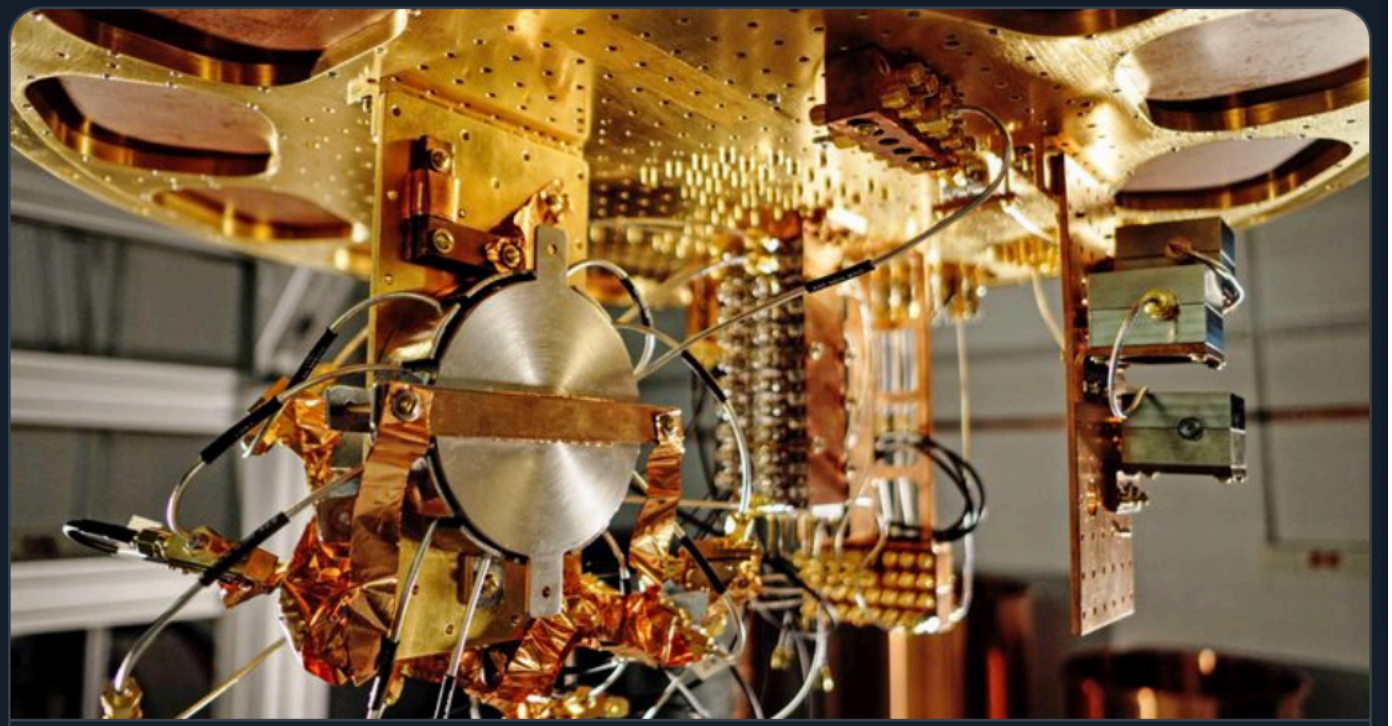
Andrew Yang 🧢 ✓
@AndrewYang

民主党の大統領候補の一人

Google achieving quantum computing is a huge deal. It means, among many other things, that no code is uncrackable.

クラックされないコードはない

ツイートを翻訳



Google reportedly attains 'quantum supremacy'
Its quantum computer can solve tasks that are otherwise unsolvable, a report says

Andrew Yang 🧢 ✔
@AndrewYang

We need to catch up with our approach to encryption

ツイートを翻訳

暗号へのアプローチを
変えないといけない

Quantum Computing and Encryption Standards - Yang2020 - Andrew Yang for P...
Our current encryption standards protecting sensitive national security and banking data, among other types, will one day be decryptable in a short time ...
🔗 yang2020.com

ビットコイン、7500ドル割れ　量子コンピューター警戒

2019/10/23 23:59

https://s.nikkei.com/2SgvCE0

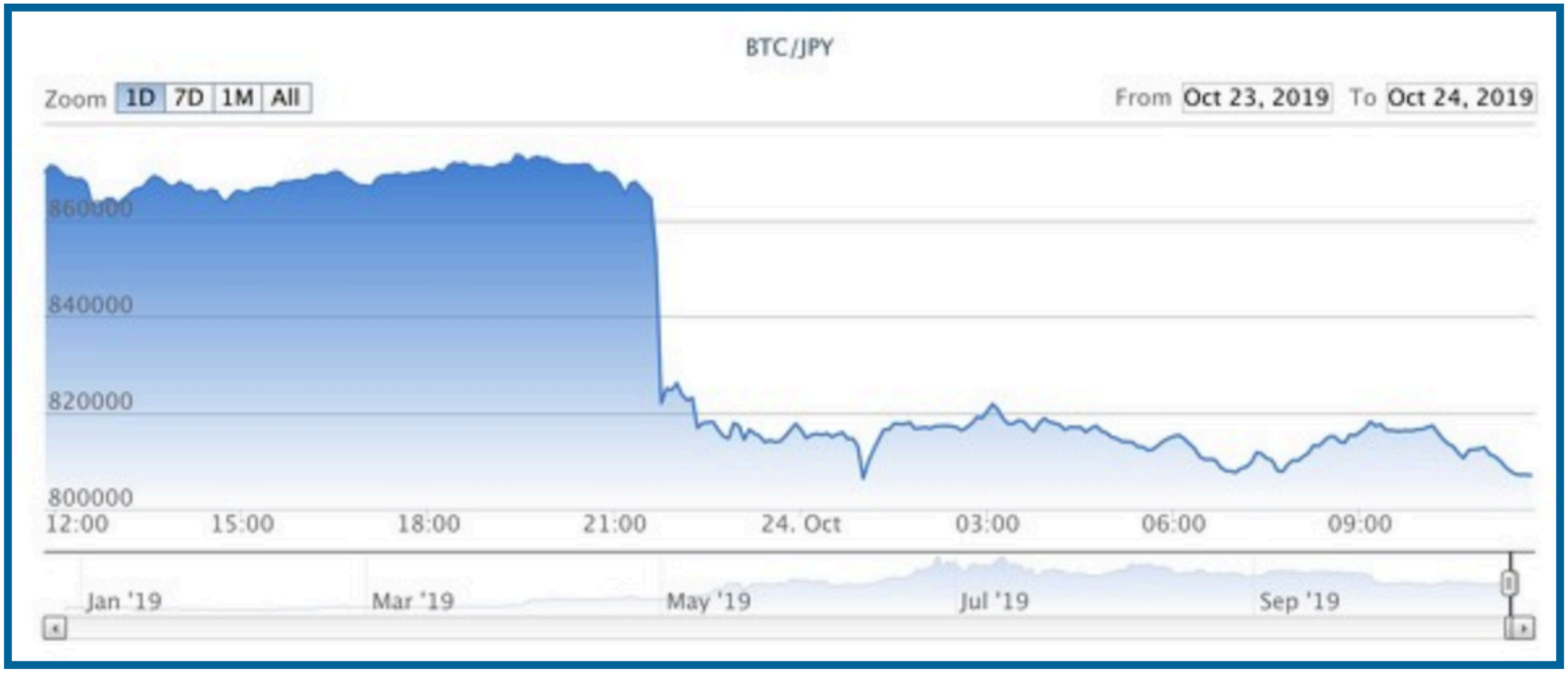
ビットコイン(BTC) 底割れ暴落、「量子超越」が取り沙汰される背景は？｜仮想通貨市況

CoinPost編集部

2019/10/24 12:03　2019/10/25 06:32　マーケット

https://coinpost.jp/?p=114188

ビットコイン価格が10月23日夜、急落し、1BTCあたり80万円に迫った。このところ80万円後半で推移していたが、一気に10%ほど下落した。これは、5カ月前の5月に80万円を割り込んだ時以来だ。



過去1日の円建てビットコイン価格の推移（=bitFlyer）

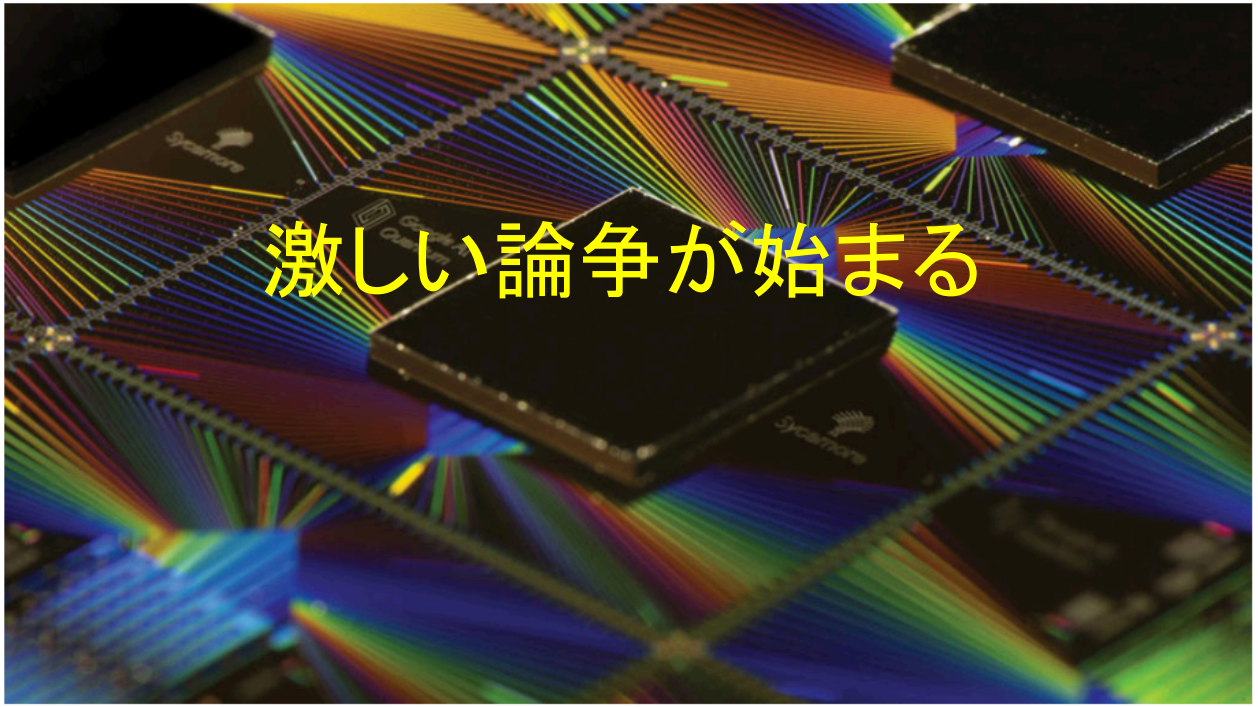
このあたりの議論は、以前のマルレク「暗号技術の現在 ― ポスト量子暗号への移行と量子暗号」を参照されたい。
https://www.marulabo.net/docs/cipher/

ScienceNews
INDEPENDENT JOURNALISM SINCE 1921

YEAR IN REVIEW QUANTUM PHYSICS

Google claimed quantum supremacy in 2019 — and sparked controversy

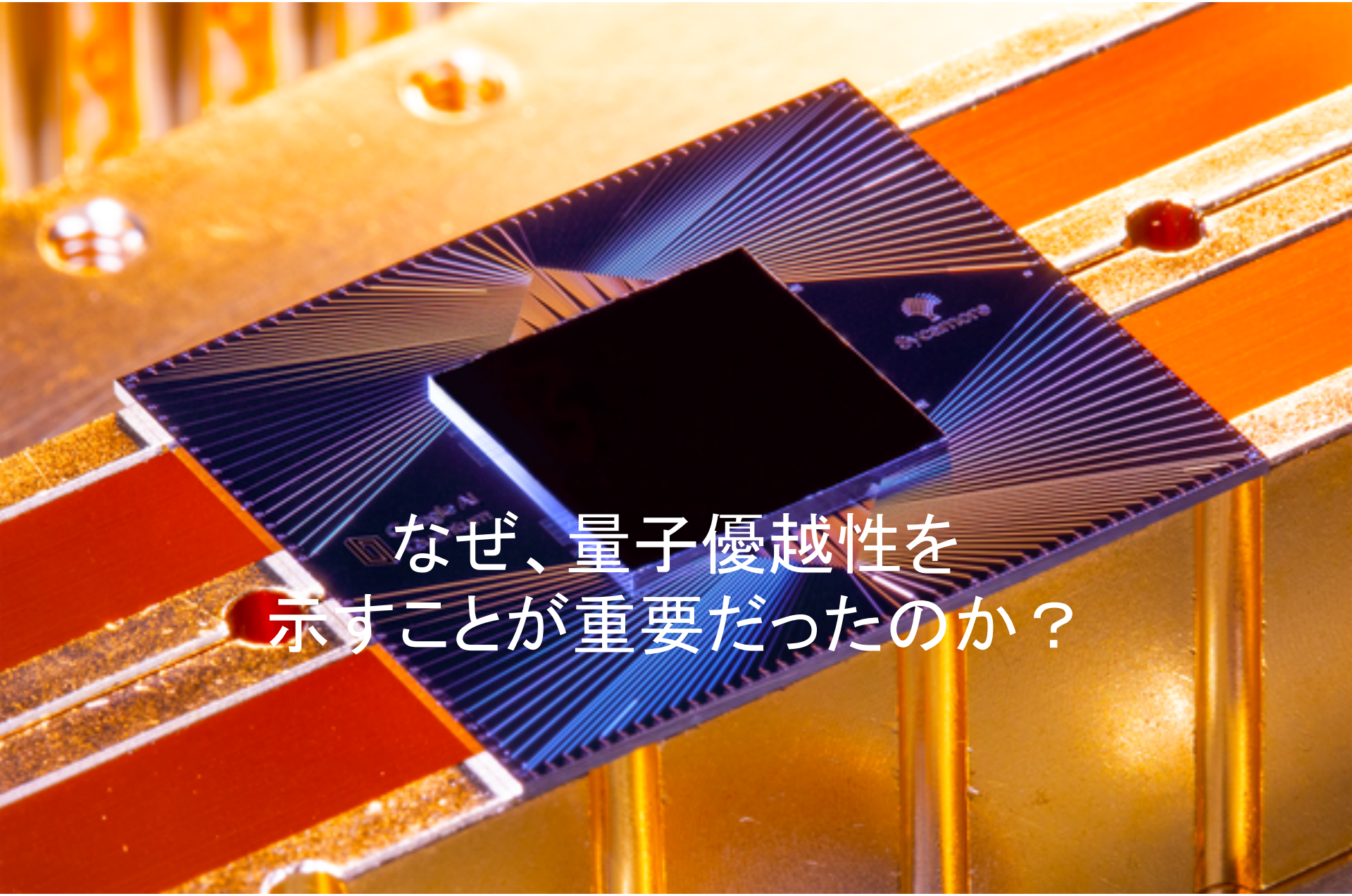
Competitors questioned whether the milestone had truly been achieved



Google's quantum computer Sycamore performed a calculation that would take thousands of years with a classical supercomputer, researchers claimed in 2019. An array of quantum computer chips is shown.

GOOGLE

http://bit.ly/31MgLV6


なぜ、量子優越性を
示すことが重要だったのか？

量子優越性とは何か？

1982年　ファインマン

2012年　プレスキル

量子優越性とは何か？

- 「量子優越性」という言葉は、2012年にプレスキルが論文 ”Quantum computing and the entanglement frontier” で提唱した造語です。
- 彼はこう言っています。

  Classical systems cannot in general simulate quantum systems efficiently.

  （古典システムは、一般には、量子システムを効率的にはシミレートできない）

Quantum computing and the entanglement frontier

John Preskill 2012年

https://arxiv.org/pdf/1203.5813.pdf

量子優越性の考え方は、ファインマンの量子コンピューターのアイデアにさかのぼります

- あるシステムをシミレートするためには、一定の計算能力が必要です。これは、量子コンピュータは、古典コンピューターより、計算能力で優っていることを意味します。
- 古典システムと量子システムの複雑さを対比する、こうした考え方は、量子コンピュータのアイデアを初めて提案したファインマンの考えに遡るものです。彼は、1982年の論文”Simulating Physics with Computers” で、次のように述べていました。

自然をシミュレートするコンピュータ

コンピューターが、正確に自然と同じように振る舞う、正確なシミュレーションが存在する可能性について話そうと思う。
それが証明されて、そのコンピュータのタイプが先に説明したようなものであるなら、必然的に、有限の大きさの時空の中で起きる全てのものは、有限な数の論理的な操作で正確に分析可能でなければならないことになるだろう。

量子論的システムは、古典的なコンピューターでシミュレートされるか？

量子論的なシステムは、古典的な万能計算機で、確率論的にシミュレートされるだろうか？
別の言い方をすれば、コンピューターは、量子論的なシステムが行うのと、同じ確率を与えるだろうか？
コンピューターを今まで述べてきたような古典的なものだとすれば（前節で述べたような量子論的なものではないとすれば）、また法則はすべて変更されないままで、ごまかしもないとすれば、答えは明らかにノーである。

量子コンピュータ -- 万能量子シミュレーター

それは、新しいタイプのコンピューター、量子コンピューター？で可能になるだろう。
私が理解する限りでは、それは量子論的なシステムによって、量子コンピューターの要素によって、シミュレート出来るようになることは、いまや、明らかになった。それはチューリング・マシンではない。別のタイプのマシンである。

Simulating Physics with Computers

Richard P. Feynman, 1982年
http://www.cs.berkeley.edu/~christos/classics/Feynman.pdf

こうしたファインマンの考えは、そのままプレスキルに受け継がれています。

classical systems cannot simulate highly entangled quantum systems efficiently, and we hope to hasten the day when well controlled quantum systems can perform tasks surpassing what can be done in the classical world.

彼は、この考えをさらに具体的に進めます。

One way to achieve such "quantum supremacy" would be to run an algorithm on a quantum computer which solves a problem with a super-polynomial speedup relative to classical computers,

この時点では、プレスキルは、量子コンピュータを実際に作り上げることが、とてもとても難しいことをよく理解していました。あるいは、「とんでもないほど、笑えるほど難しいいのかも」

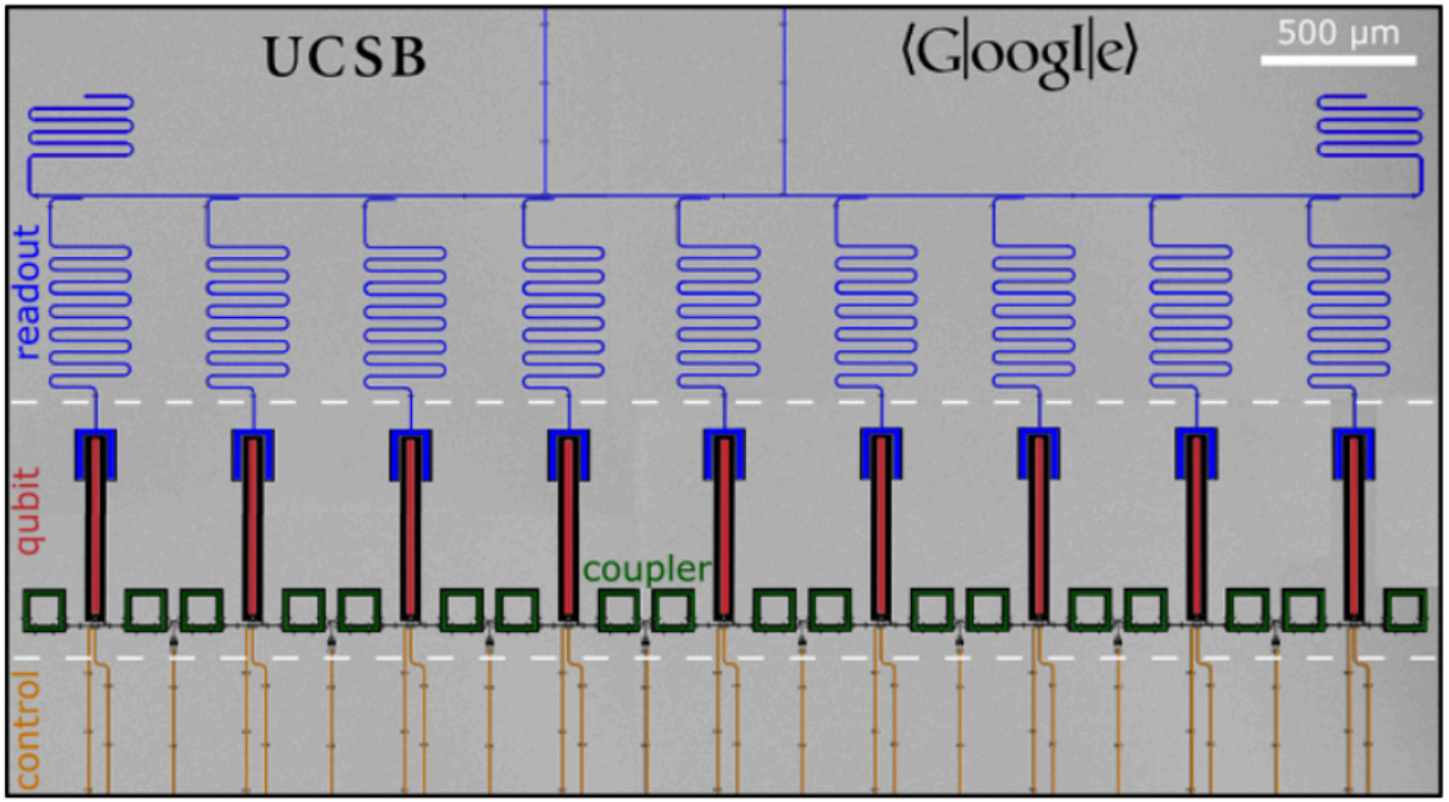
To operate a large scale quantum computer reliably we will need to overcome the debilitating effects of decoherence, which might be done using "standard" quantum hardware protected by quantum error-correcting codes, or by exploiting the nonabelian quantum statistics of anyons realized in solid state systems, or by combining both methods.

Classical systems cannot in general simulate quantum systems efficiently.

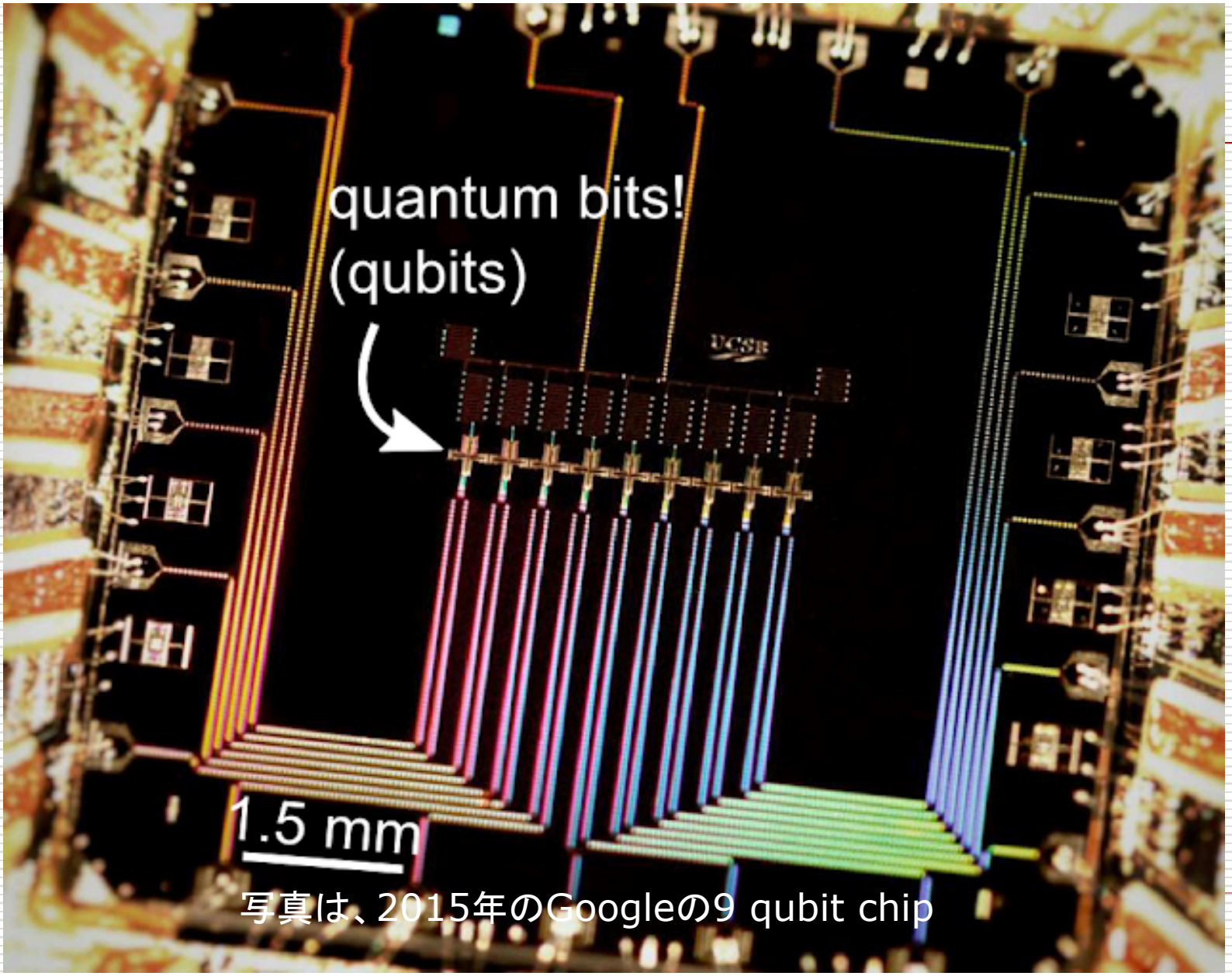
Is controlling large-scale quantum systems merely really, really hard, or is it ridiculously hard?

量子技術の発展

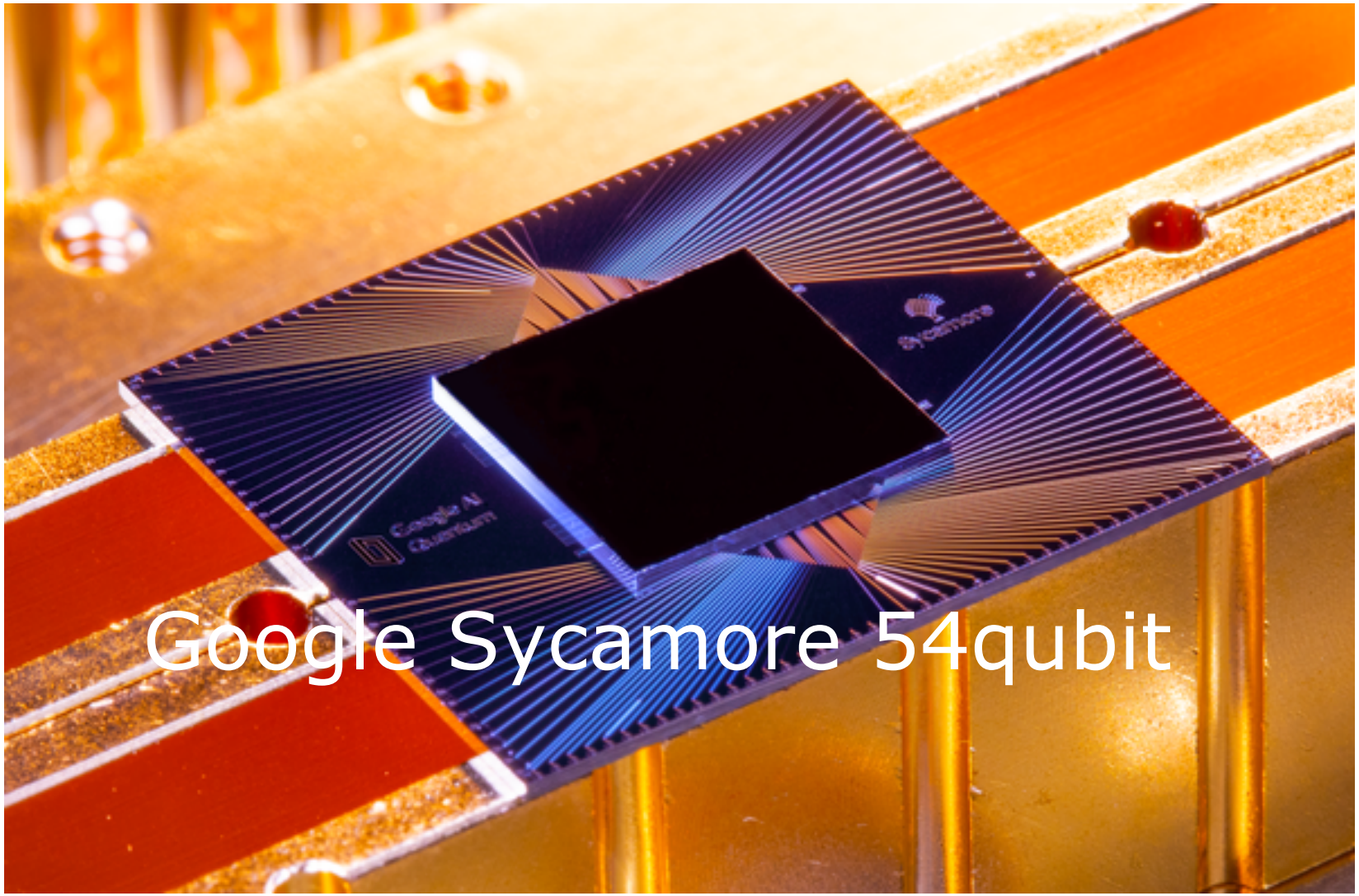
シリコン上にqubitを実装するのには、大きな困難があった。しかし、着実に前進を続けた。



写真は、2015年のGoogleの9 qubit chip

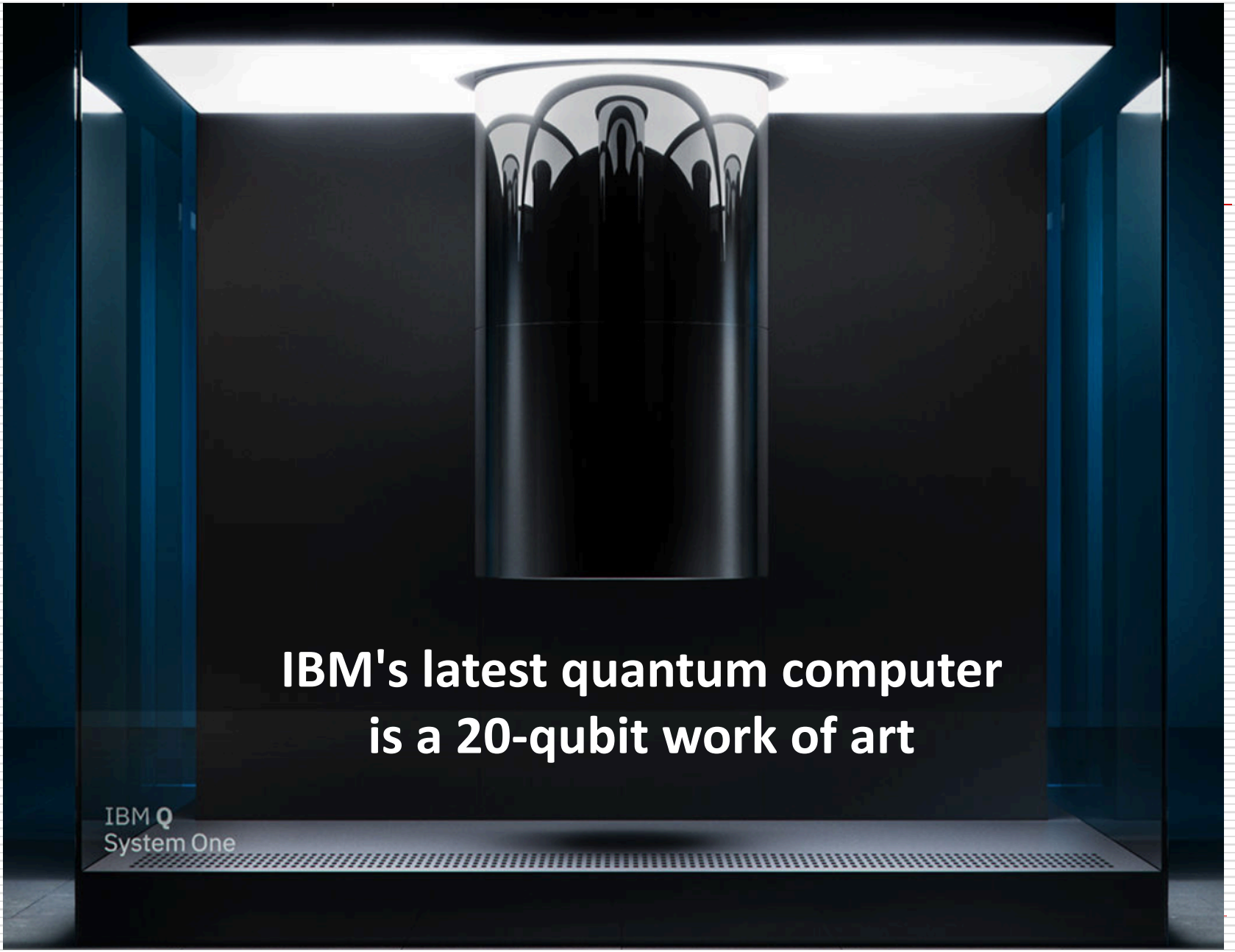


写真は、2015年のGoogleの9 qubit chip


Google Sycamore 54qubit

2018年
Google Bristlecone 54qubit

The Google AI lab introduced a 72-qubit quantum processor called Bristlecone in 2018.

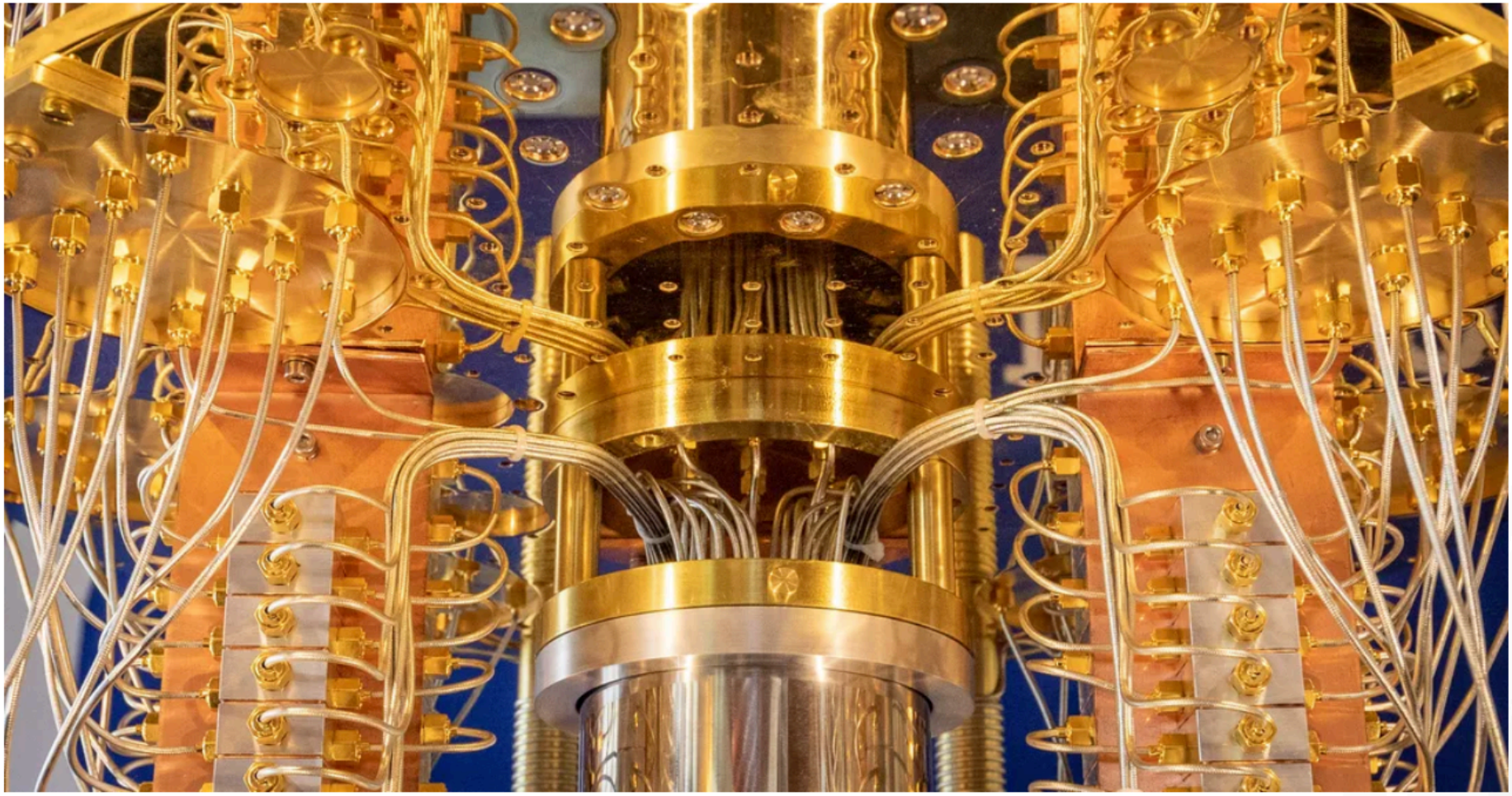


https://engt.co/37gydSA

2019/01/08

IBM's new 53-qubit quantum computer is its biggest yet

September 18, 2019



A close-up view of the IBM Q quantum computer. The processor is in the silver-colored cylinder.

https://cnet.co/2OQ4VE5

量子優越性実証への関心の集中

のちに見るプレスキルのNISQという時代の特徴づけから時間は少し遡るのだが、ここでは、まだノイズのもとに置かれた規模も小さい量子デバイスを使ってなにをなすべきかと量子コンピュータの研究者が考えてきたかを振り返ってみよう。

それは、急速に「量子優越性の実証」という課題に収斂していった。いくつかの動きを紹介する。

Characterizing Quantum Supremacy in Near-Term Devices

John M. Martinis et al. **2016/07/31**
https://arxiv.org/abs/1608.00263

- マルチネス率いるGoogleのチームの、近いうちに開発可能なデバイス（”near term device”。まだ “NISQ” という言葉は使われていない）で、エラー訂正ができなくとも、量子優越性の特徴づけができるのではという 2016年の問題提起。
- 当時は、9 qubitの量子デバイスしかなかった。この デバイスの動作は、簡単にコンピュータでシミレートできる。
  ただ、48 qubit , 40ステップ程度のランダム量子回路で、最新のスーパー・コンピュータでもシミレートできなくなるのではという予想を述べている。

- A critical question for the field of quantum computing in the near future is whether quantum devices without error correction can perform a well-defined computational task beyond the capabilities of state-of-the-art classical computers, achieving so-called quantum supremacy.
- In this paper we show how to estimate the cross entropy between an experimental implementation of a random quantum circuit and the ideal output distribution simulated by a supercomputer.
- We study the cost of all these algorithms and conclude that, with state-of-the-art supercomputers, they fail for universal random circuits with more than approximately 48 qubits and depth ~ 40

Complexity-Theoretic Foundations of Quantum Supremacy Experiments

Scott Aaronson, Lijie Chen, **2016/12/26**
https://arxiv.org/pdf/1612.05903.pdf

- アーロンソン達も、これに呼応して、量子優越性実験の「複雑性理論」からの基礎づけに取り組み始める。
- こうした実験は、完全な誤りのない汎用の量子コンピュータを作ることを目的としたものではなく、「単に」、ある量子アルゴリズムが、最速の古典コンピュータとその最良のアルゴリズムより高速であることを示すことを目的とする。その意味では、実用的な意味は持たない。
- 量子優越性は、量子コンピュータ技術がいまだ到達していない、中心的なマイルストーンである。しかし、それは、近い将来、きっと実現されるだろう。

- "quantum supremacy": that is, a clear quantum speedup for some task, motivated by the goal of overturning the Extended Church-Turing Thesis as confidently as possible.
- These experiments don't yet aim to build full, fault-tolerant, universal quantum computers, but "merely" to demonstrate some quantum speedup over the best known or conjectured classical algorithms
- The ECT is an asymptotic claim, which of course means that no finite experiment could render a decisive verdict on it, even in principle. But this hardly makes experiments irrelevant.
- In summary, we regard quantum supremacy as a central milestone for quantum computing that hasn't been reached yet, but that might be reached in the near future.

A blueprint for demonstrating quantum supremacy with superconducting qubits

Martinis et al. **2017/09/19**
https://arxiv.org/abs/1709.06678

- Googleチームの、超電導qubit で、量子優越性を実証するための計画書。この時点では、まだ、Googleには、9qubitのデバイスしかなかったのだが。

- Here, using 9 superconducting qubits, we demonstrate an immediate path towards quantum supremacy.
- By extending these results to a system of 50 qubits, we hope to address scientific questions that are beyond the capabilities of any classical computer.

Quantum Supremacy and the Complexity of Random Circuit Sampling

Vazirani et al. **2018/05/12**
https://arxiv.org/abs/1803.04402

- 「量子複雑性」の大家であるVaziraniら、UCB校のメンバーのコミット。量子優越性実験の手段としてフォーカスされてきた、「ランダム量子回路」の「サンプリング」についての、量子複雑性理論からの考察。

- A critical milestone on the path to useful quantum computers is quantum supremacy - a demonstration of a quantum computation that is prohibitively hard for classical computers. A leading near-term candidate, put forth by the Google/UCSB team, is sampling from the probability distributions of randomly chosen quantum circuits, which we call Random Circuit Sampling (RCS).
- In this paper we study both the hardness and verification of RCS. While RCS was defined with experimental realization in mind, we show complexity theoretic evidence of hardness that is on par with the strongest theoretical proposals for supremacy.
- While quantum devices capable of solving such important problems may still be far off, decades of work undertaken toward building scalable quantum computers have already yielded considerable progress in high-precision control over quantum systems.

量子優越性実験へ

Googleの実験と受け止められているかもしれないが、多くのアカデミーのメンバーが、この実験に協力している。

- Preskill(Caltech),
- Martinis(UCSB -> Google),
- Aaronson(MIT -> UTA),
- Vazarini(UCB),
- Farhi(MIT -> Google)

等の連携で、量子優越性実験の準備は進む。

実験前夜
NISQ 時代の課題

2018年　プレスキル

Quantum Computing in the NISQ era and beyond

John Preskill 2018/01/27

https://arxiv.org/abs/1801.00862v2

こうした時代を「NISQ 時代」と名付け、その課題を整理したのは、プレスキルの論文 “Quantum Computing in the NISQ era and beyond” だった。

彼は、「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」ことを指摘し、「量子複雑性」と「量子誤り訂正」の二つを、この時代の課題として提示した。

Quantum Computing in the NISQ era and beyond

John Preskill 2018/01/27

https://arxiv.org/abs/1801.00862v2

論文概要

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。

はじめに　突然の変化

このカンファレンスの前提は、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仕事をし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。

量子技術の商業的可能性について

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。

エンタングルメントのフロンティア

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、我々が物理科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ると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ィジタル・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。

現在のコンピュータでは
自然のシミュレートはできない

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。

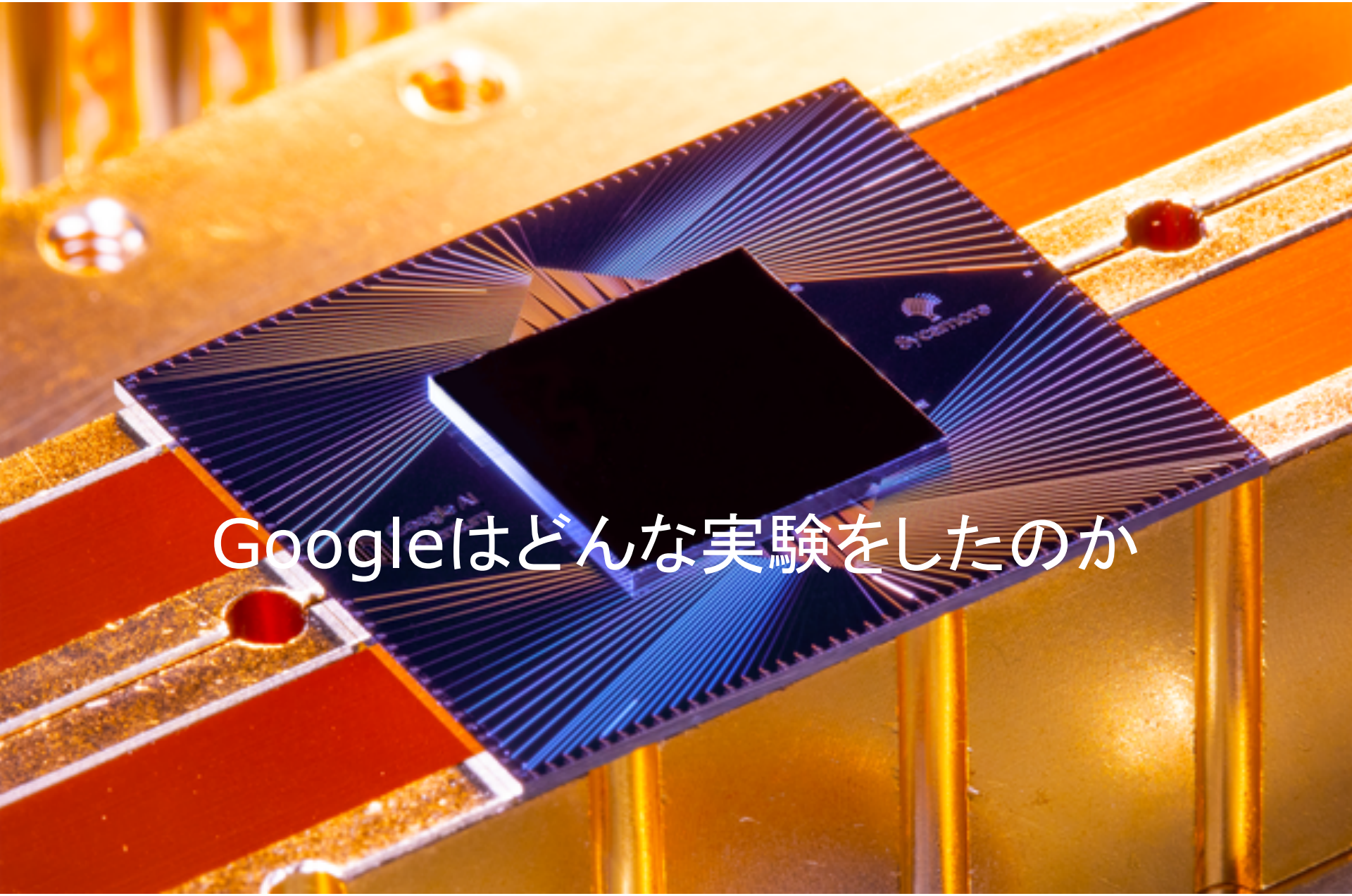
「量子複雑性」と「量子誤り訂正」という二つの原理

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考え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考える私たちの基礎）

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。


Googleはどんな実験をしたのか

Quantum supremacy using a programmable superconducting processor

2019/10/23

https://www.nature.com/articles/s41586-019-1666-5

Google 論文は、多くの著者の連名で書かれている

Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C. Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando G. S. L. Brandao, David A. Buell, Brian Burkett, Yu Chen, Zijun Chen, Ben Chiaro, Roberto Collins, William Courtney, Andrew Dunsworth, **Edward Farhi**, Brooks Foxen, Austin Fowler, Craig Gidney, Marissa Giustina, Rob Graff, Keith Guerin, Steve Habegger, Matthew P. Harrigan, Michael J.Hartmann, Alan Ho, Markus Hoffmann, Trent Huang, Travis S. Humble, Sergei V. Isakov, Evan Jeffrey, Zhang Jiang, Dvir Kafri, Kostyantyn Kechedzhi, Julian Kelly, Paul V. Klimov, Sergey Knysh, Alexander Korotkov, Fedor Kostritsa, David Landhuis, Mike Lindmark, Erik Lucero, Dmitry Lyakh, Salvatore Mandrà, Jarrod R. McClean, Matthew McEwen, Anthony Megrant, Xiao Mi, Kristel Michielsen, Masoud Mohseni, Josh Mutus, Ofer Naaman, Matthew Neeley, Charles Neill, Murphy Yuezhen Niu, Eric Ostby, Andre Petukhov, John C. Platt, Chris Quintana, Eleanor G. Rieffel, Pedram Roushan, Nicholas C. Rubin, Daniel Sank, Kevin J. Satzinger, Vadim Smelyanskiy, Kevin J. Sung, Matthew D. Trevithick, Amit Vainsencher, Benjamin Villalonga, Theodore White, Z. Jamie Yao, Ping Yeh, Adam Zalcman, Hartmut Neven & **John M. Martinis**

論文の概要

量子コンピューターが約束していることは、特定の計算タスクが古典プロセッサーよりも量子プロセッサー上では、指数関数的に高速に実行される可能性があることである。

基本的な挑戦は、指数関数的に大きな計算空間上で量子アルゴリズムを実行できる高い信頼性を持つプロセッサを構築することである。

この論文では、プログラム可能な超伝導量子ビットを備えたプロセッサを使用して、 53量子ビットの量子状態を作成したことを報告する。この量子状態は、次元2^{53}（約10^{16}）の計算状態空間に対応する。

繰り返される実験からの測定は、結果の確率分布をサンプリングすることで行われる。この結果は、古典的なシミュレーションを使用して検証する。

論文の概要

我々のSycamoreプロセッサでは、量子回路の1つのインスタンスを100万回サンプリングするのに約200秒を要した。

現在のベンチマークでは、最先端の古典的なスーパーコンピューターで同等のタスクを実行するには、約10,000年かかる。

すべての既知の古典的なアルゴリズムと比較して、この劇的な速度の向上は、この特定の計算タスクに対して量子優位性を実験的に実現したものとなる。この実験は、待望のコンピューティングパラダイムの先駆けである。

量子ビットについて基本的なことを確認しよう

- n個のqubitの状態の数
- n個のqubitの観測
- 量子ゲートの働き

この節で解説するのは、論文の「概要」のこの部分である

論文の概要

量子コンピューターが約束していることは、特定の計算タスクが古典プロセッサーよりも量子プロセッサー上では、指数関数的に高速に実行される可能性があることである。

基本的な挑戦は、指数関数的に大きな計算空間上で量子アルゴリズムを実行できる高い信頼性を持つプロセッサを構築することである。

この論文では、プログラム可能な超伝導量子ビットを備えたプロセッサを使用して、53量子ビットの量子状態を作成したことを報告する。この量子状態は、次元2^{53}（約10^{16}）の計算状態空間に対応する。

n個のqubitの状態の数

繰り返される実験からの測定は、結果の確率分布をサンプリングすることで行われる。この結果は、古典的なシミュレーションを使用して検証する。

この節で解説するのは、論文の「概要」のこの部分である

論文の概要

量子コンピューターが約束していることは、特定の計算タスクが古典プロセッサーよりも量子プロセッサー上では、指数関数的に高速に実行される可能性があることである。

基本的な挑戦は、指数関数的に大きな計算空間上で量子アルゴリズムを実行できる高い信頼性を持つプロセッサを構築することである。

この論文では、プログラム可能な超伝導量子ビットを備えたプロセッサを使用して、53量子ビットの量子状態を作成したことを報告する。この量子状態は、次元2^{53}（約10^{16}）の計算状態空間に対応する。

繰り返される実験からの測定は、結果の確率分布をサンプリングすることで行われる。この結果は、古典的なシミュレーションを使用して検証する。

n個のqubitの観測

n個のqubitの状態の数

一個のqubitの状態

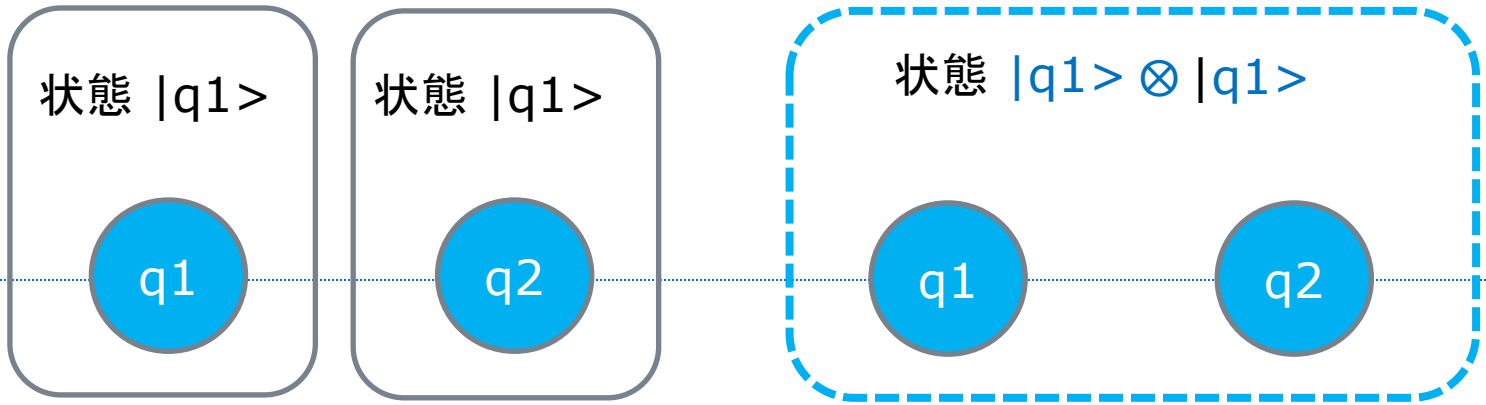
- 一個のqubitは、0の状態と1の状態の「重ね合わせ」の状態を持つ。二つの状態が重なり合っているが、一つの状態である。
- 0の状態を |0>
  1の状態を |1> で表す。
- qubitの重ね合わせの状態で、
  0らしさを表す数を a
  1らしさを表す数を b としたとき、
  このqubit q1の状態を次のように表すことにする。

  $$|q1\rangle = a|0\rangle + b|1\rangle$$

- 全てのqubitの状態は、二つの数 a, b と |0>, |1> を使って、先の形で表される。
- ただし、a, b には $|a|^2+|b|^2 = 1$ という条件がつく。

二個のqubitの状態

- 二つのqubit q1とq2があったとする。
- q1とq2の状態は、それぞれ、次のように表される。
  $|q1\rangle = a|0\rangle + b|1\rangle$
  $|q2\rangle = c|0\rangle + d|1\rangle$
- この時、二つのqubit q1とq2を、一緒に考えた状態を考えて、それを、状態 $|q1\rangle \otimes |q2\rangle$ と表すことにする。

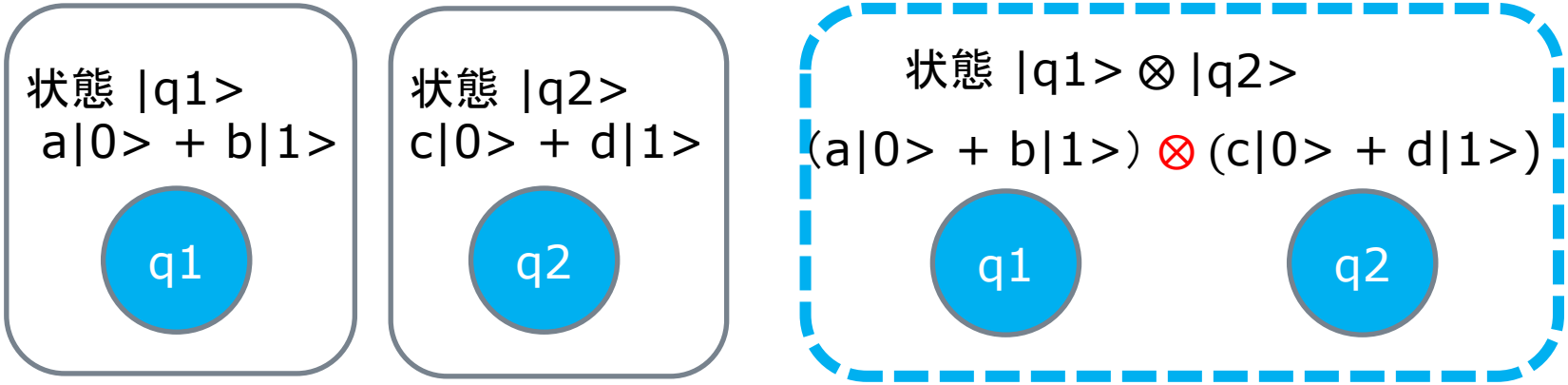


二個のqubitの状態の計算

- この時、|q1> ⊗ |q2> を、次のように計算する。

$$|q1\rangle \otimes |q2\rangle = (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle)$$

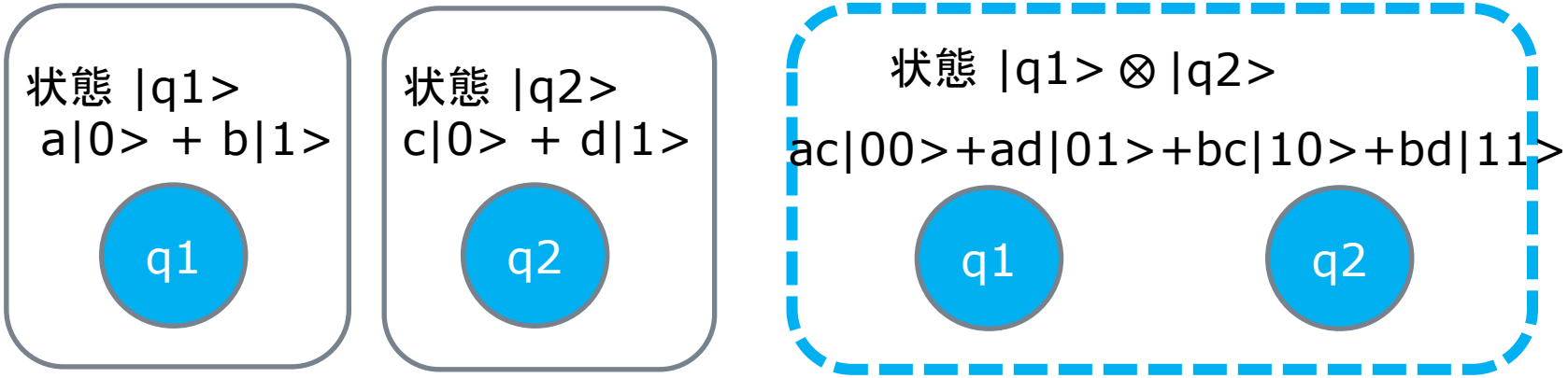
$$= ac|0\rangle\otimes|0\rangle + ad|0\rangle\otimes|1\rangle + bc|1\rangle\otimes|0\rangle + bd|1\rangle\otimes|1\rangle$$



二個のqubitの状態の数

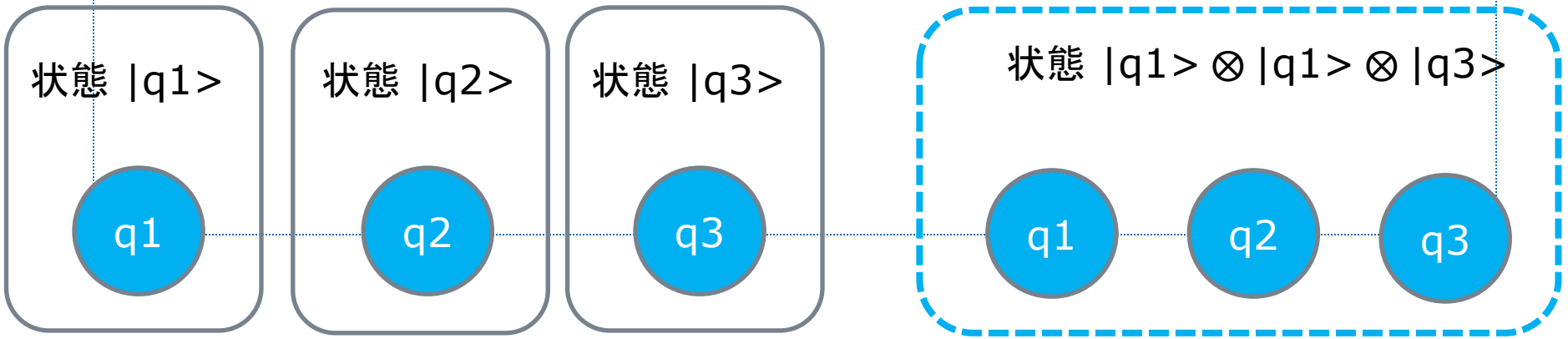
- 先の式で、|0>⊗|0>=|00>, |0>⊗|1>=|01>,
  |1>⊗|0>=|10>, |1>⊗|1>=|11>とすれば、
- |q1> ⊗ |q2> = (a|0> + b|1>) ⊗ (c|0> + d|1>)
  = ac|00>+ad|01>+bc|10>+bd|11>

- 二つのqubitの状態は、4つの状態の重ね合わせであることがわかる。



三個のqubitの状態

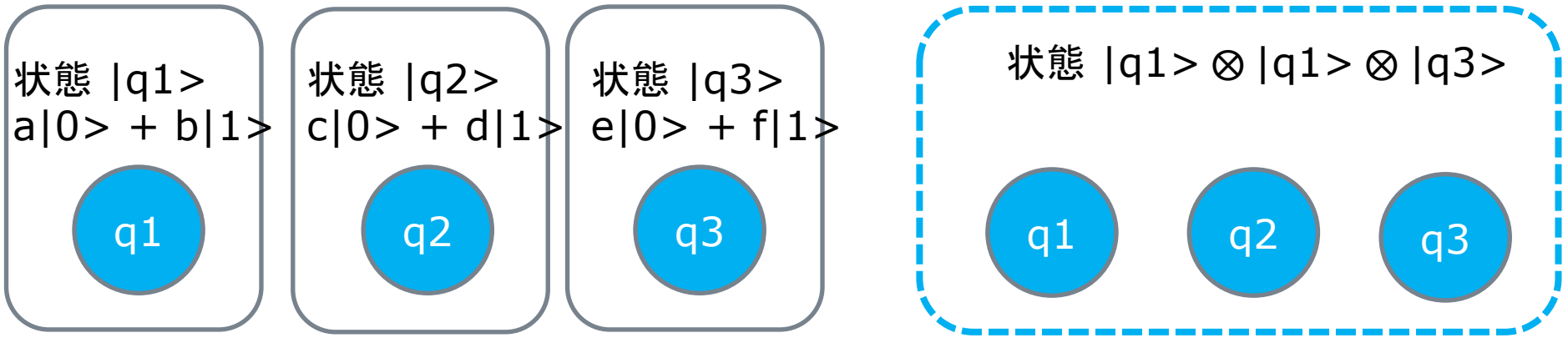
- 三つのqubit q1とq2とq3があったとする。
- q1,q2,q3の状態は、それぞれ、次のように表される。
  $|q1\rangle = a|0\rangle + b|1\rangle$
  $|q2\rangle = c|0\rangle + d|1\rangle$
  $|q3\rangle = e|0\rangle + f|1\rangle$
- この時、三つのqubit q1とq2とq3を、一緒に考えた状態を考えて、それを、状態 $|q1\rangle \otimes |q2\rangle \otimes |q3\rangle$と表すことにする。



三個のqubitの状態の計算

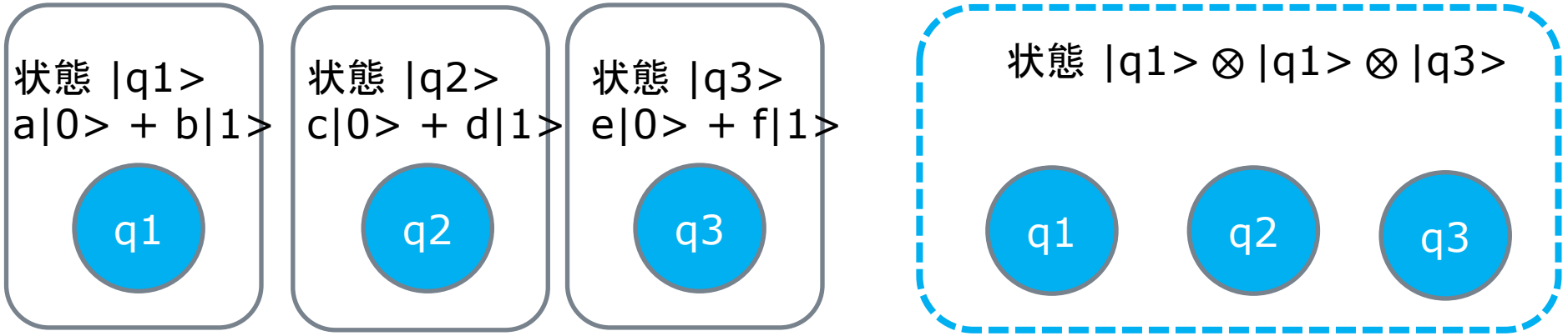
- この時、|q1> ⊗ |q2> ⊗ |q3>を、次のように計算する。

$$|q1\rangle \otimes |q2\rangle \otimes |q3\rangle$$
$$= (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle) \otimes (e|0\rangle + f|1\rangle)$$



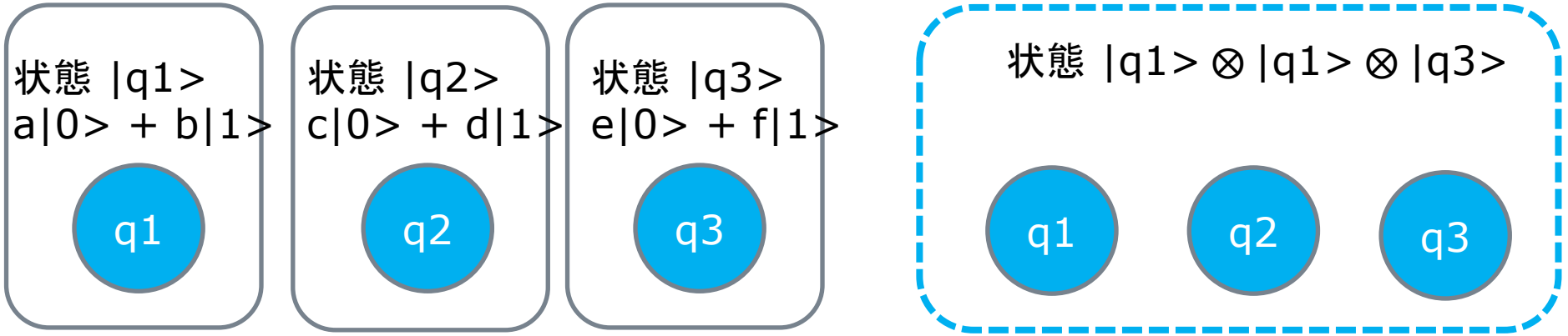
三個のqubitの状態の計算

- 先の式で、
  |0>⊗|0>⊗|0>=|000>, |0>⊗|1>⊗|0>=|010>,
  |1>⊗|0>⊗|0>=|100>, |1>⊗|1>⊗|1>=|111> …とすれば、
- |q1> ⊗ |q2 ⊗ |q3>
  = (a|0> + b|1>) ⊗ (c|0> + d|1>)⊗ (e|0> + f|1>)
  = ace|000>+acf|001>+ade|010>+adf|011>
  +bce|100>+bcf|101>+bde|110>+bdf|111>



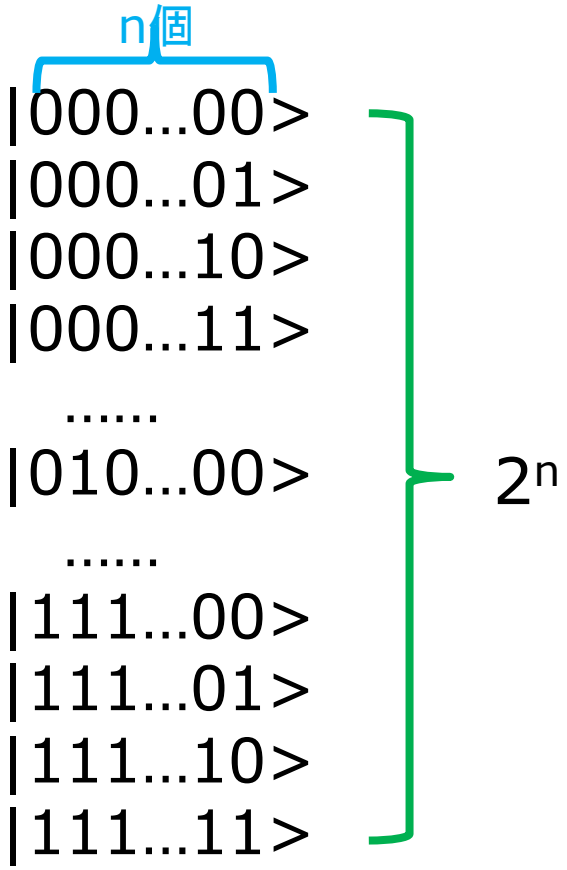
三個のqubitの状態の数

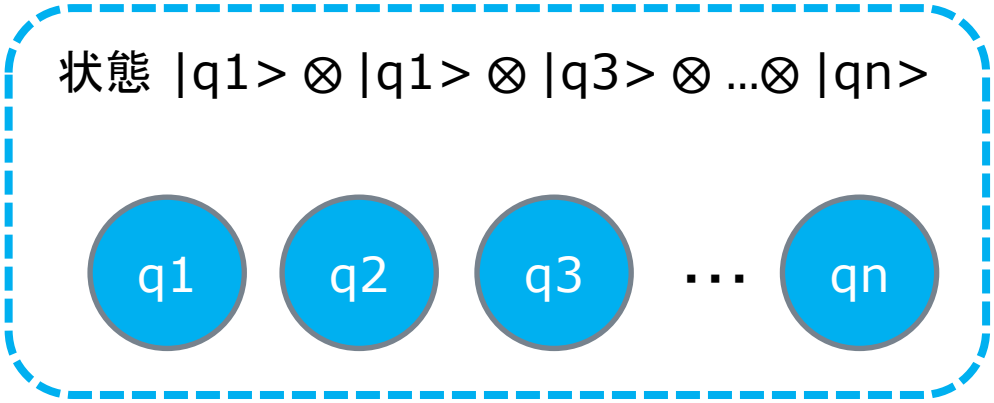
- よって、三個のqubitの状態は、
  |q1> ⊗ |q2 ⊗ |q3>
  = (a|0> + b|1>) ⊗ (c|0> + d|1>)⊗ (e|0> + f|1>)
  = ace|000>+acf|001>+ade|010>+adf|011>
  +bce|100>+bcf|101>+bde|110>+bdf|111>
  となって、
  |000>,|001>,|010>,|011>,|100>,|101>,|110>,|111>
  の8つの状態の重ね合わせになる。



n個のqubitの状態の数

- 一般に、n個のqubitの状態は、
  2^n個の状態の重ね合わせになる





n個のqubitの観測

一個のqubitの状態の観測

- 次の状態のqubit q1 があったとする。
  $|q1\rangle = a|0\rangle + b|1\rangle$
- このq1を観測すると、奇妙なことが起きる。
  q1の状態$|0\rangle$と状態$|1\rangle$ の重ね合わせの状態は失われ、
  0または1(普通のビット)が観測される。
  観測すると、元のq1が持っていた、a, bの情報は失われる。
- ただ、q1の状態を、くりかえし何度も観測できるとすると、
  0が観測される確率は、$|a|^2$
  1が観測される確率は、$|b|^2$ となる。
- 先に見た、$|a|^2+|b|^2 = 1$ という条件は、観測では、必ず、0または1が観測されることを意味する。

1 qubitの状態のサンプリングと分布

- 一回の観測では、0または1の値しか返らない。ただ、何度も観測して、観測結果のサンプルを増やすと、0または1が観測される頻度の分布が得られる。それが、元のqubitが持っていた情報を与えてくれる。

二個のqubitの状態の観測

- |q1> = a|0> + b|1>
  |q2> = c|0> + d|1>
  である二つのqubitの状態の観測をしてみよう。
- 先に見たように、この状態は、
  $|q1\rangle \otimes |q2\rangle = (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle)$
  $= ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle$
  で表され、四つの状態 |00>,|01>,|10>,|11>の重ね合わせである。
- 観測によって、重ね合わせの状態は失われて、
  四つの状態 |00>,|01>,|10>,|11>のうちの一つが観測される。

二個のqubitの状態の観測

- この時、
  $|00\rangle$が観測される確率は、$|ac|^2$
  $|01\rangle$が観測される確率は、$|ad|^2$
  $|10\rangle$が観測される確率は、$|bc|^2$
  $|11\rangle$が観測される確率は、$|bd|^2$ となる。
- また、$|ac|^2 + |ad|^2 + |bc|^2 + |bd|^2 = 1$ である。

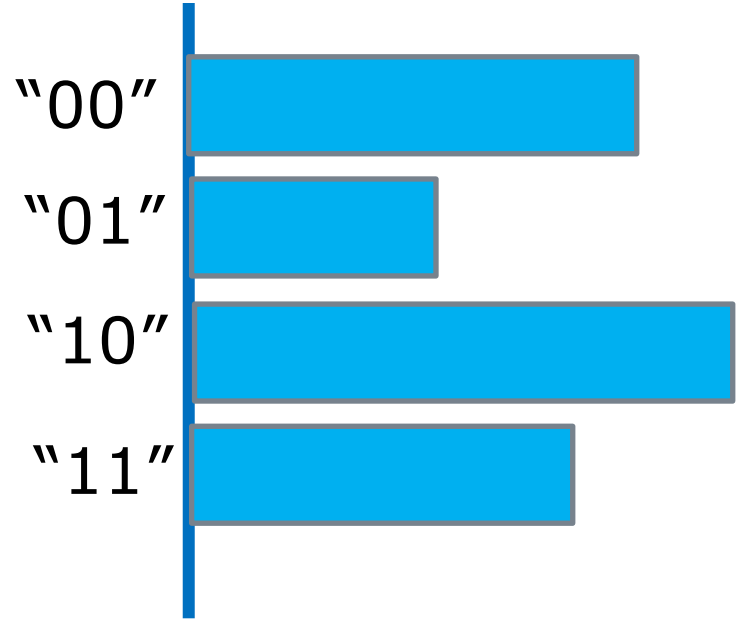
二個のqubitの状態の観測

- |00>が観測されるということは、
  q1が0と観測され、q2が0と観測されるということである。
  |01>が観測されるということは、
  q1が0と観測され、q2が1と観測されるということである。
  |10>が観測されるということは、
  q1が1と観測され、q2が0と観測されるということである。
  |11>が観測されるということは、
  q1が1と観測され、q2が1と観測されるということである。

- 二個のqubitの観測によって、結局
  “00”, “01”, “10”, “11” のうちいずれかの2ビット列が返ることになる。

2 qubitの状態のサンプリングと分布

- 一回の観測では、特定の値一個しか返らない。ただ、何度も観測して、観測結果のサンプルを増やすと、それぞれの値が観測される頻度の分布が得られる。それが、元のqubitが持っていた情報を与えてくれる。

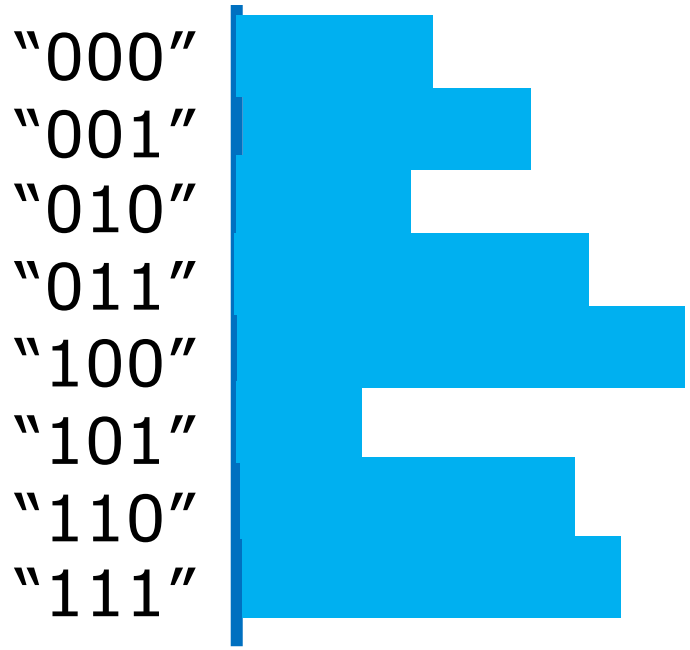


三個のqubitの観測

- 三個のqubitの状態は、
  |000>, |001>, |010>, |011>,
  |100>, |101>, |110>, |111>
  の8つの状態の重ね合わせである。
- ただし、観測によって重ね合わせの状態は失われ、
  |000>, |001>, |010>, |011>,
  |100>, |101>, |110>, |111>
  のうち、一つの状態だけが観測される。
- 三個のqubitの観測によって、
  “000”, “001”, “010”, “011”,
  “100”, “101”, “110”, “111”
  のうちいずれかの3ビット列が返ることになる。

3 qubitの状態のサンプリングと分布

- 一回の観測では、特定の値一個しか返らない。ただ、何度も観測して、観測結果のサンプルを増やすと、それぞれの値が観測される頻度の分布が得られる。それが、元のqubitが持っていた情報を与えてくれる。



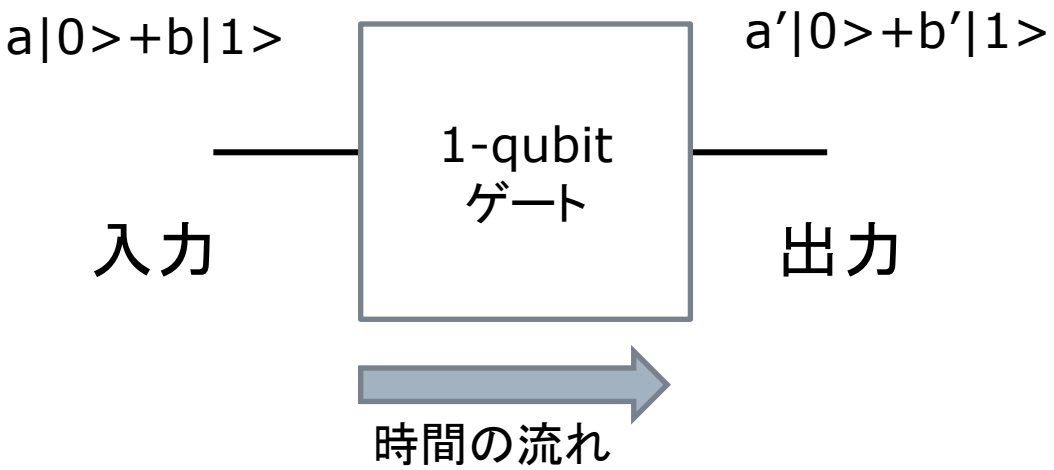
n個のqubitの観測

- n個のqubitの状態は、
  |0…00>, |0…01>, |0…10>, |0…11>, ……
  |1…00>, |1…01>, |1…10>, |1…11>
  の2^nの状態の重ね合わせである。
- ただし、観測によって重ね合わせの状態は失われ、
  |0…00>, |0…01>, |0…10>, |0…11>, ……
  |1…00>, |1…01>, |1…10>, |1…11>
  のうち、一つの状態だけが観測される。
- n個のqubitの観測によって、
  “0…00”, “0…01”, “0…10”, “0…11”, ……
  “1…00”, “1…01”, “1…10”, “1…11”
  のうちいずれかのnビット列が返ることになる。

量子ゲートの働き

1-qubit ゲート

- 1-qubitの状態　a|0>+b|1> を入力とし、
  他の 1-qubitの状態 a'|0>+b'|1>に変換して出力する
  回路を 1-qubit ゲートという。



- ただし、$|a|^2+|b|^2 = |a'|^2+|b'|^2 = 1$ である。

代表的な 1-qubitの回路

Bit Flipper

$a|0\rangle+b|1\rangle \rightarrow b|0\rangle+a|1\rangle$

Phase Flipper

$a|0\rangle+b|1\rangle \rightarrow a|0\rangle-b|1\rangle$

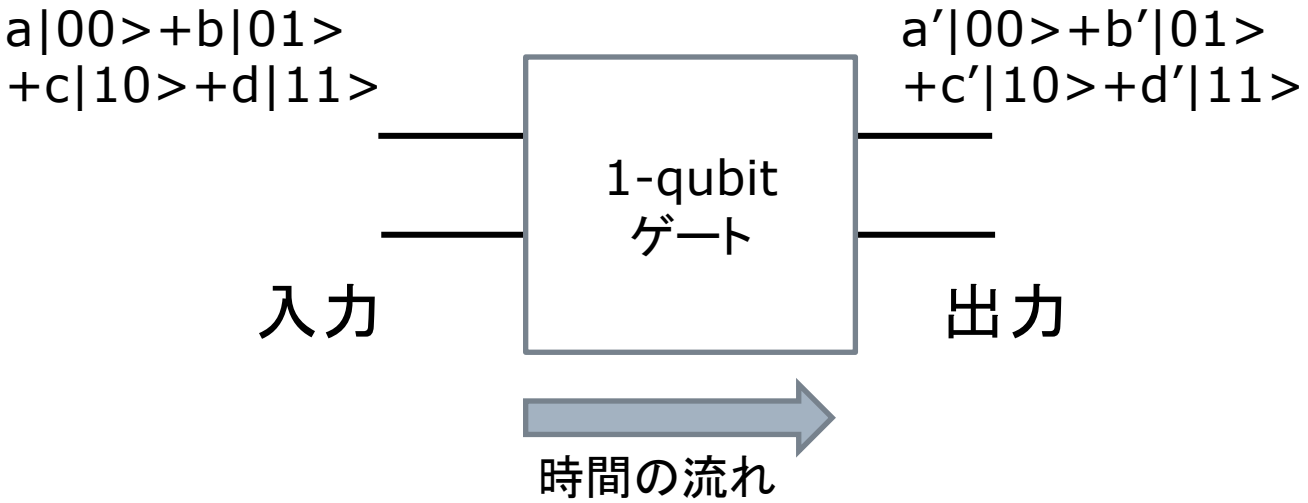
Hadamard

$a|0\rangle+b|1\rangle \rightarrow$

$\frac{1}{\sqrt{2}}(a+b)|0\rangle+\frac{1}{\sqrt{2}}(a-b)|1\rangle$

2-qubit ゲート

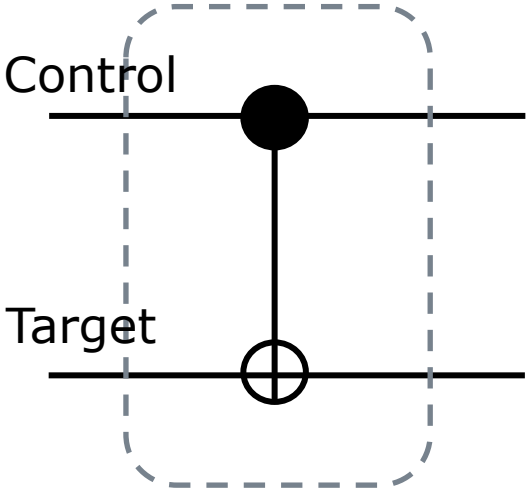
- 2-qubitの状態　a|00>+b|01>+c|10>+d|11> を入力とし、2-qubitの状態 a'|00>+b'|01>+c'|10>+d'|11> に変換して出力する回路を 2-qubit ゲートという。



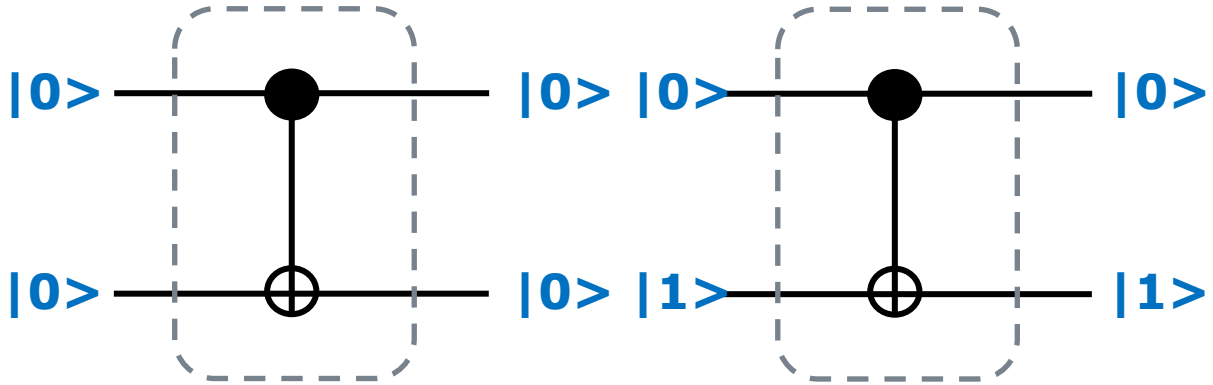
- ただし、$|a|^2+|b|^2+|c|^2+|d|^2=1$
  $|a'|^2+|b'|^2+|c'|^2+|d'|^2=1$ である。

2-qubitの回路の例
CNOT (Control-NOT)

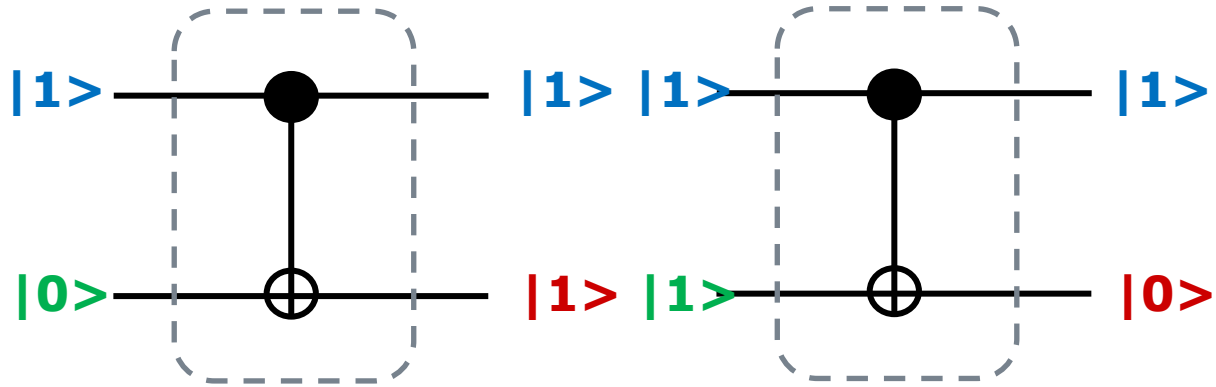
Control が |1> の時
Target のNOTをとる



Controlが |0>なら何もしない



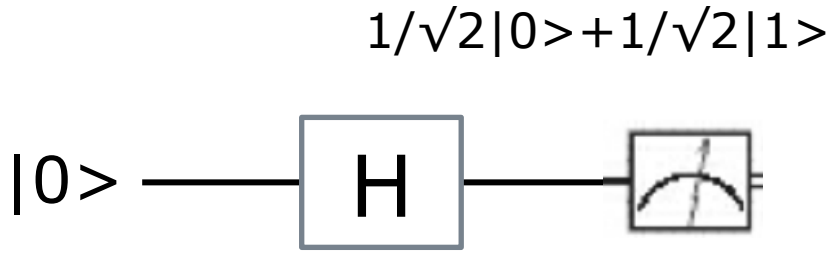
Controlが |1>ならNOT操作



ランダム量子回路

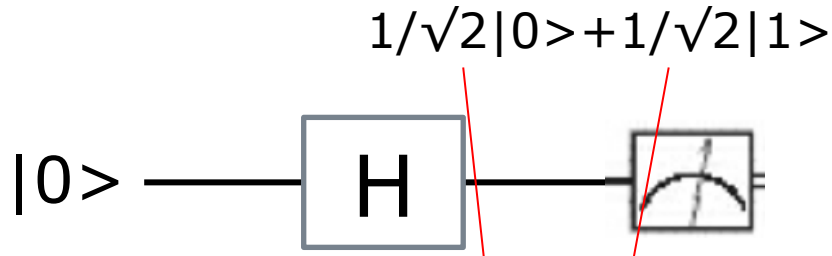
今回のGoogleの実験の一つのポイントは、量子優越性を実証するのに、「ランダム量子回路」という手法をとったことである。ここでは、それがどういうアイデアかを説明する。

つぎのように、アダマール・ゲートH 一つに、
初期値として |0>を与えた時、サンプリングで得られる分布を考えよう



Hは、|0>を
1/√2|0>+1/√2|1>
に変える

つぎのように、アダマール・ゲートH 一つに、
初期値として |0>を与えた時、サンプリングで得られる分布を考えよう

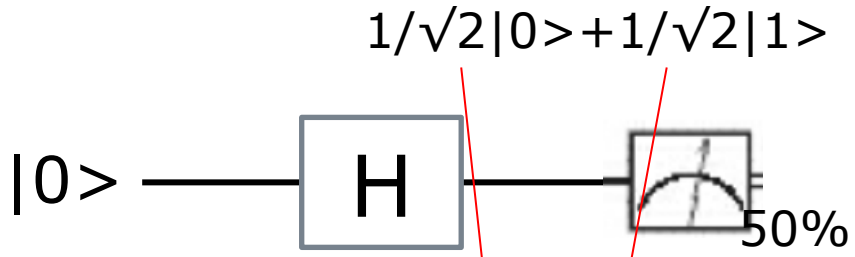


Hは、|0>を
1/√2|0>+1/√2|1>
に変える

この時、|0>が観測される確率は
$|1/\sqrt{2}|^2 = 1/2$
この時、|1>が観測される確率は
$|1/\sqrt{2}|^2 = 1/2$

よって、分布は次のようになる

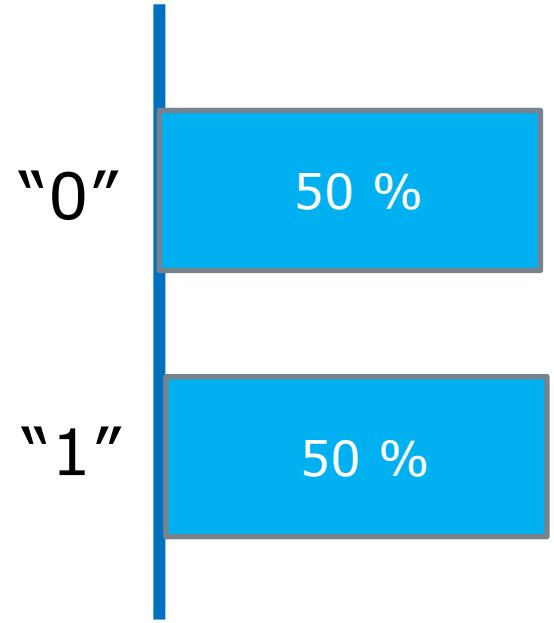
つぎのように、アダマール・ゲートH 一つに、
初期値として |0>を与えた時、サンプリングで得られる分布を考えよう



Hは、|0>を
1/√2|0>+1/√2|1>
に変える

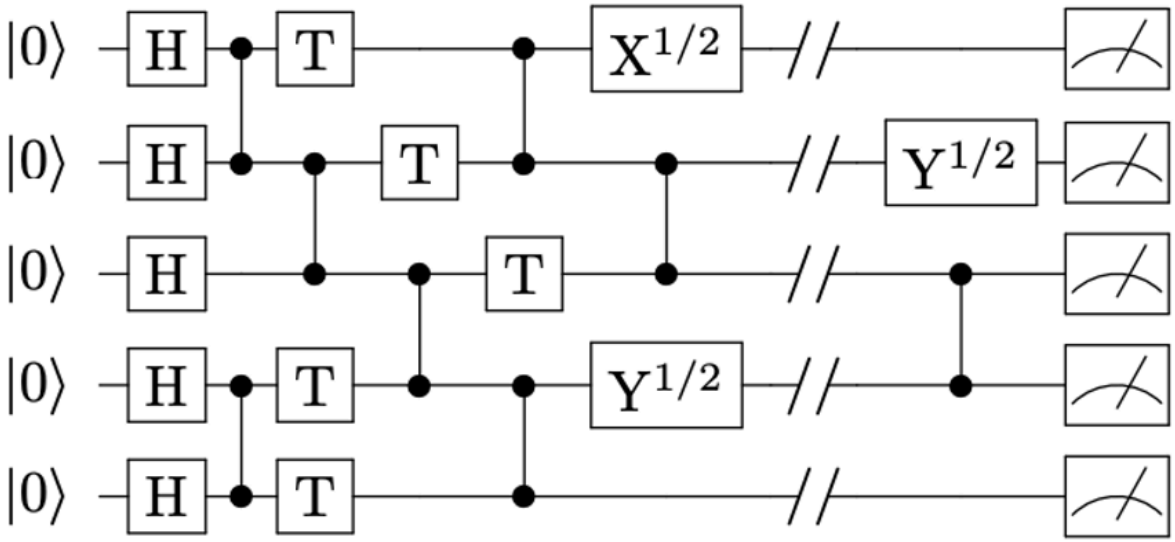
この時、|0>が観測される確率は
$|1/\sqrt{2}|^2 = 1/2$
この時、|1>が観測される確率は
$|1/\sqrt{2}|^2 = 1/2$

よって、分布は次のようになる



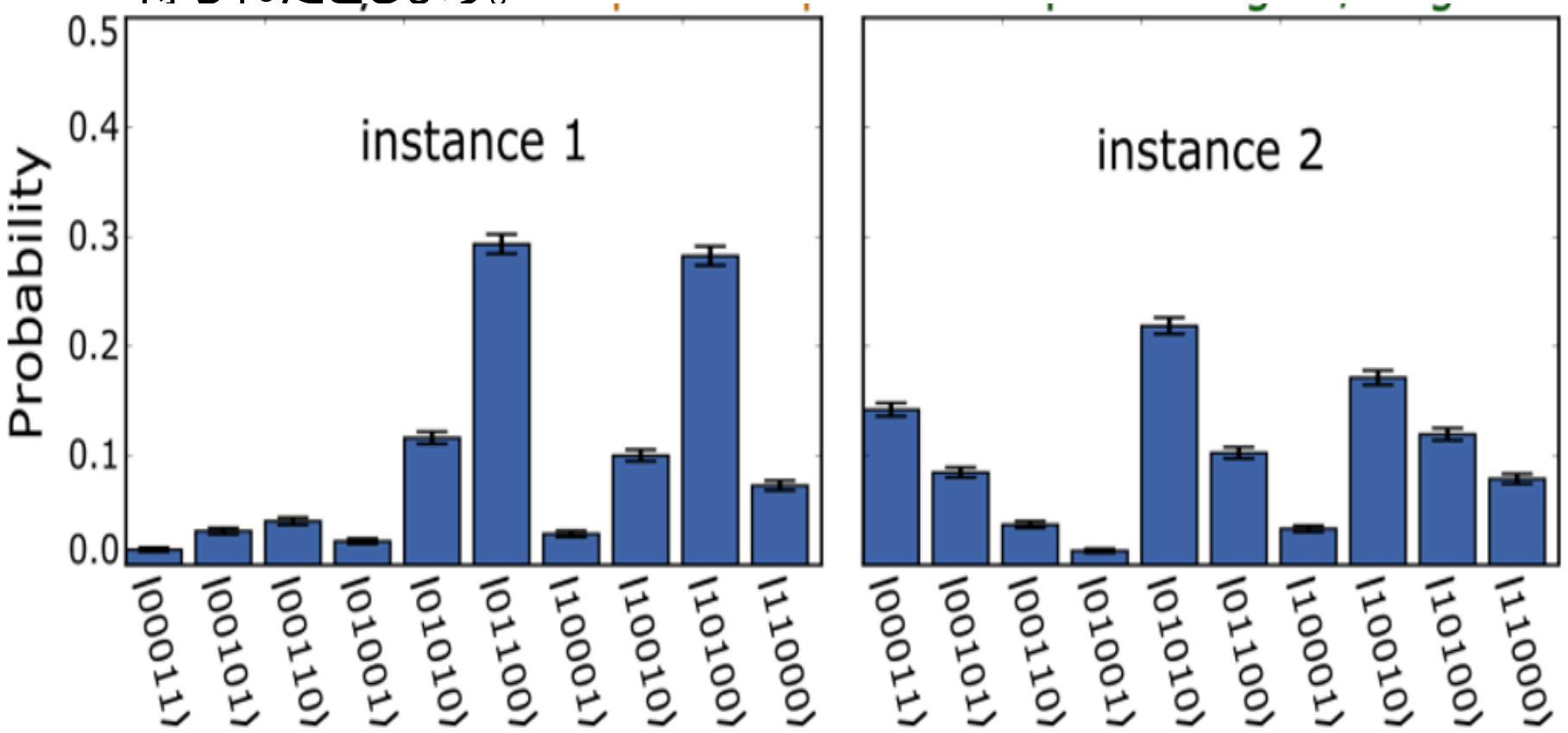
ランダムに量子回路を生成する

- ランダムに量子回路を生成する。この回路が何を計算しているかは考えない。
- 二つの別のランダム量子回路を、インスタンス1とインスタンス2としよう。



ランダム量子回路の出力をサンプリングし、出力の分布をチェックする

- 二つの量子回路の出力をサンプリングして、次のような分布が得られたとしよう。



得られた分布は、回路の特徴を反映している

- インスタンス1の回路と、インスタンス2の回路は、どちらもランダムに作られたものだが、それぞれ異なった回路である。その回路の違いが、分布の違いに反映している。
- サンプリングの数を増やしていけば、それぞれの回路に固有な分布の特徴は、いっそうはっきりしたものになってゆくだろう。

回路図が与えられれば、コンピュータを使って出力をシミレートできる

- もしも、インスタンス1とインスタンス2の回路図が与えられれば、コンピュータを使って、その出力をシミレートでき、サンプリングの数を増やせば、量子回路を使わなくても、正確な分布を得ることができるだろう。

- 問題は、これからである。
  量子回路の出力のサンプリングで作られた分布と、コンピュータの回路シミレートのサンプリングで作られた分布は、サンプル数を増やせば、基本的に同じものになるはずである。
- 量子回路もコンピュータでのシミレーションも、基本的には、「同じ仕事」をしたと考えることができる。それでは、この同じ仕事に要した時間は、それぞれ、どれくらいかかるのだろう？

ランダム量子回路を使った、量子優越性の実証

- 今回のGoogleの実験は、ランダム量子回路の出力を直接サンプリングする方が、コンピュータを使ってシミレートするよりも、圧倒的に速いことを示そうとしたものである。

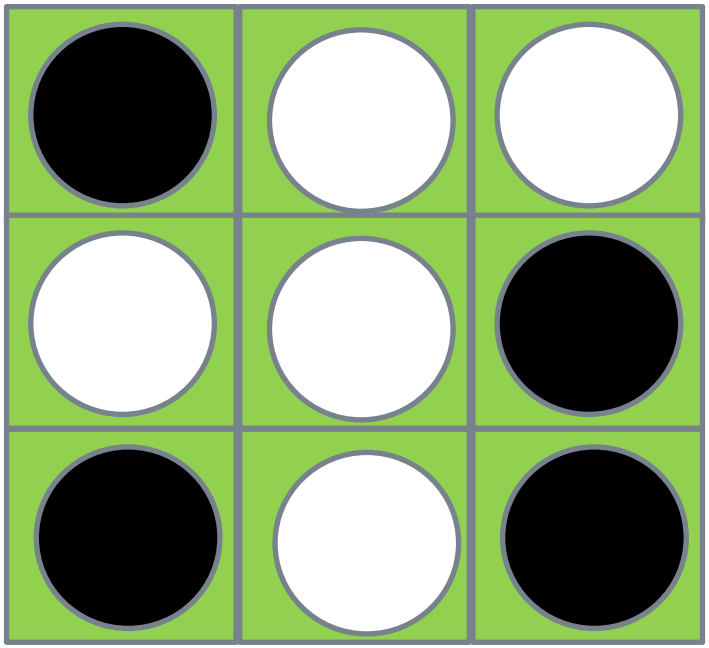
- 実際、実験では、53qubit x 20段（これを「深さ」という）上の量子回路の100万回のサンプリングを 200秒で終えた。
- スーパーコンピュータが、この回路のシミレーションを行おうとすると、膨大な時間がかかる。論文では、それを「1万年」と見積もったが、そこは違っていたようだ。IBMの見積もりによると、「2.5日」だという。

量子コンピュータの動作を図解する

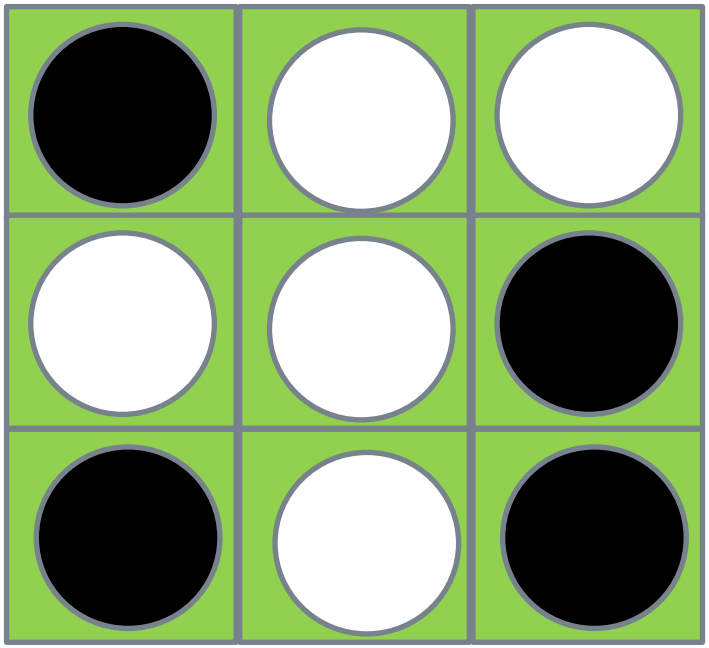
基本的には、「量子優越性」実験を行ったGoogleの量子プロセッサー sycamoreの構造を念頭に置いて、n個のqubit(量子ビット)から構成される量子コンピュータの動作を図解します。

量子プロセッサー上での
qubitの配置について

量子プロセッサーのチップの上では、
n個のqubitが、碁盤の目状に並べられています。

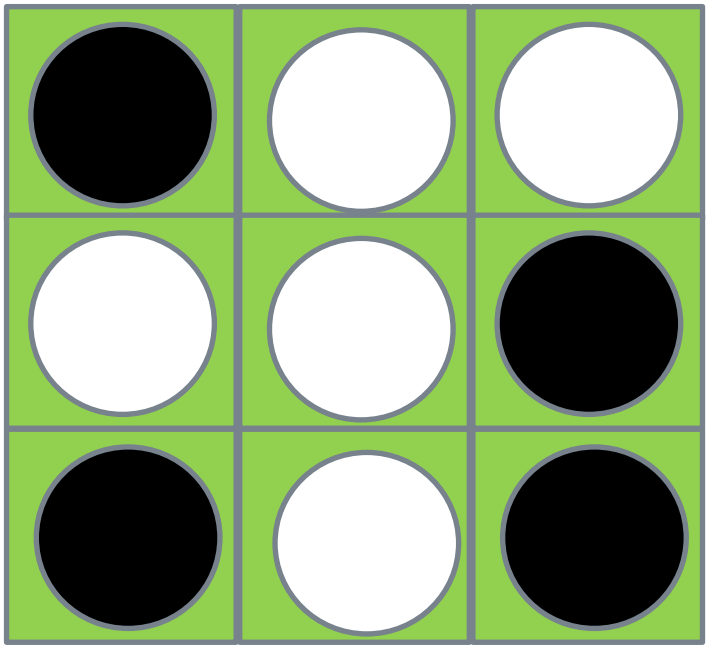


量子プロセッサーのチップの上では、
n個のqubitが、碁盤の目状に並べられています。



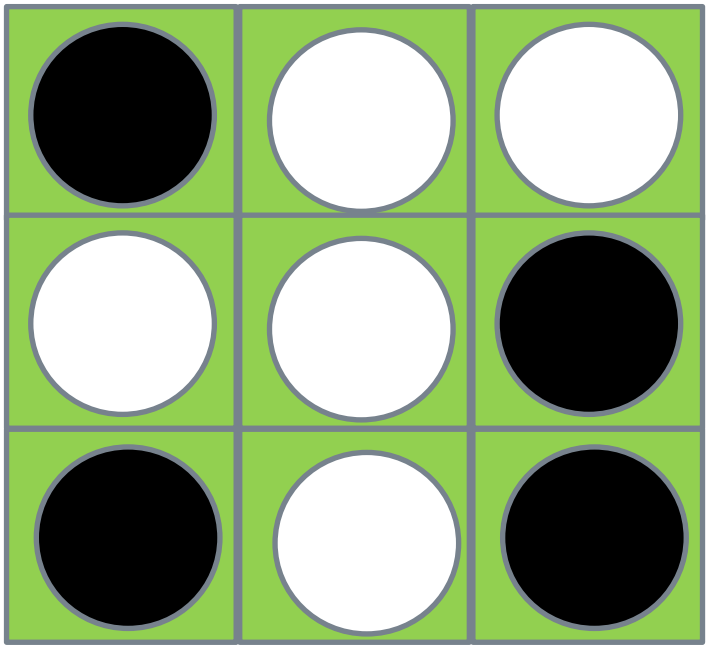
この例では、9個のqubitが、3 x 3 のマス目の上に
置かれています。

量子プロセッサーのチップの上では、
n個のqubitが、碁盤の目状に並べられています。



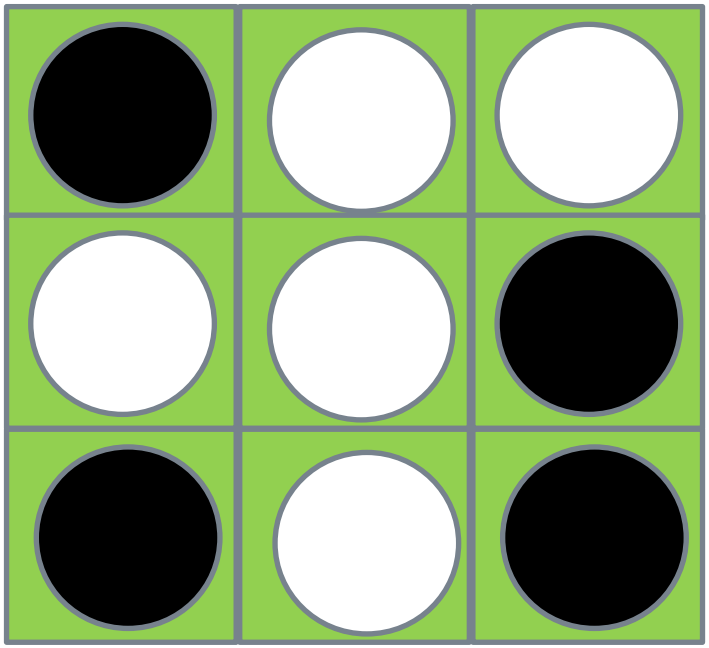
この例では、9個のqubitが、3 x 3 のマス目の上に置かれています。石の色（白・黒）は、qubitの状態を表しています。

量子プロセッサーのチップの上では、
n個のqubitが、碁盤の目状に並べられています。



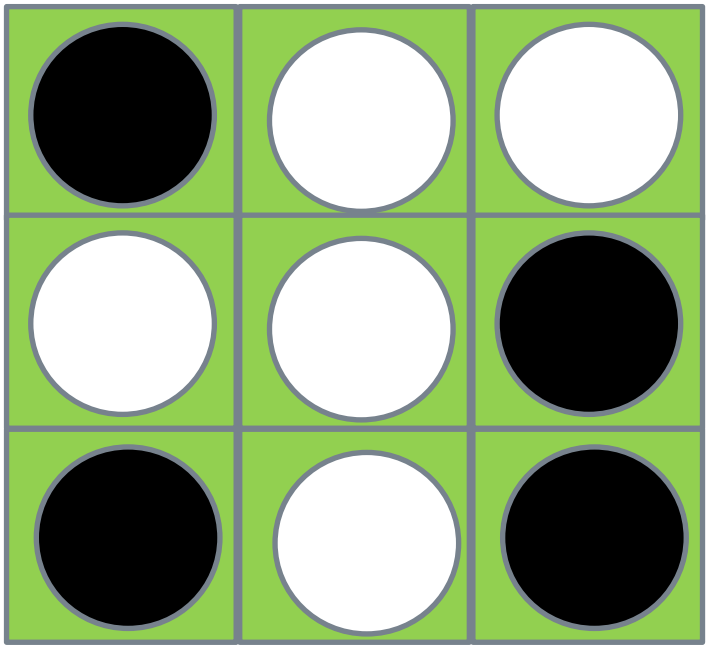
量子コンピュータにとって
大事なことが二つあります。

量子プロセッサーのチップの上では、
n個のqubitが、碁盤の目状に並べられています。



量子コンピュータにとって
大事なことが二つあります。
一つは、量子の状態を維持
し続けることができること
です。

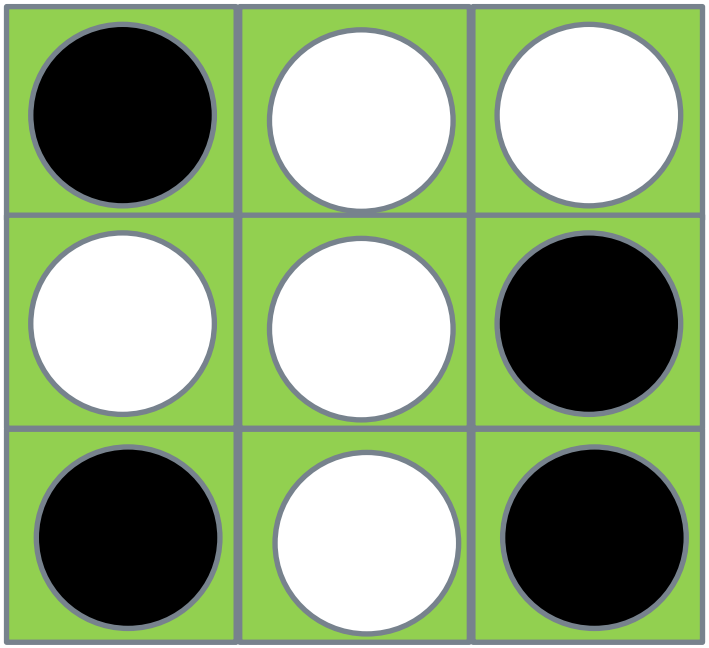
量子プロセッサーのチップの上では、
n個のqubitが、碁盤の目状に並べられています。



量子コンピュータにとって
大事なことが二つあります。
一つは、量子の状態を維持
し続けることができること
です。

この石の白・黒の色の状態を、ずっと維持できるということです。
量子の状態は不安定なので、これは実は、とても難しいこと
なのです。

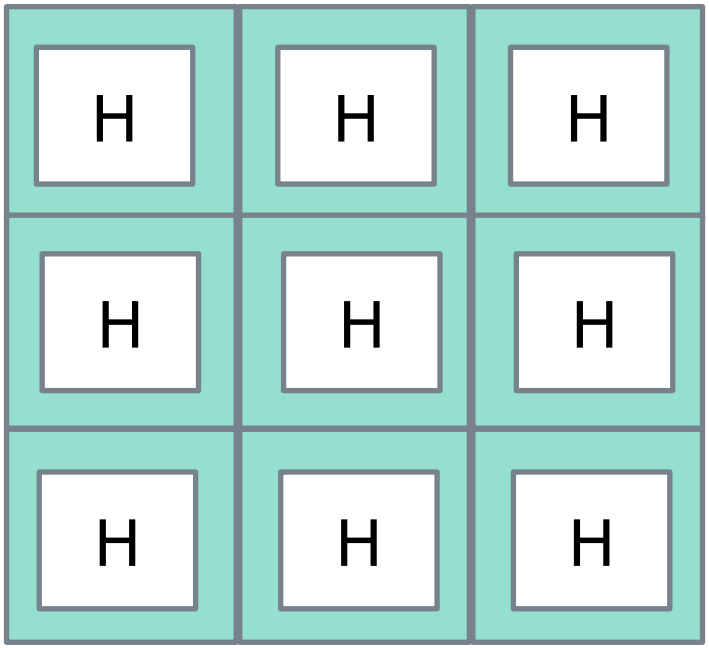
量子プロセッサーのチップの上では、
n個のqubitが、碁盤の目状に並べられています。



量子コンピュータにとって
大事なことが二つあります。
一つは、量子の状態を維持
し続けることができること
です。

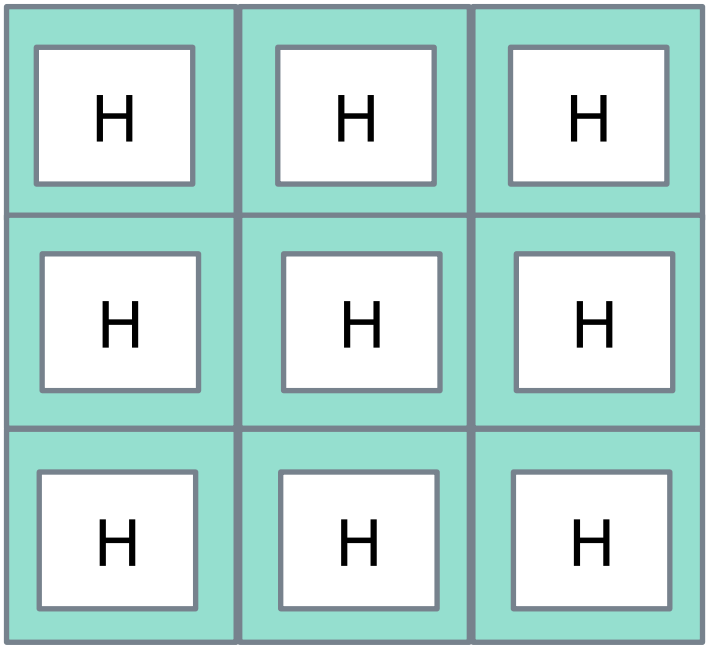
大事な注意：量子の状態は、白・黒の二色では表せません。

量子プロセッサーのチップの上では、
n個のqubitが、碁盤の目状に並べられています。



量子コンピュータにとって
大事なことが二つあります。
一つは、量子の状態を維持
し続けることができること
です。
もう一つは、どのqubitに
対しても、そのqubitを操作
して、その状態を変える
ゲートの機能を組み込む
ことができることです。

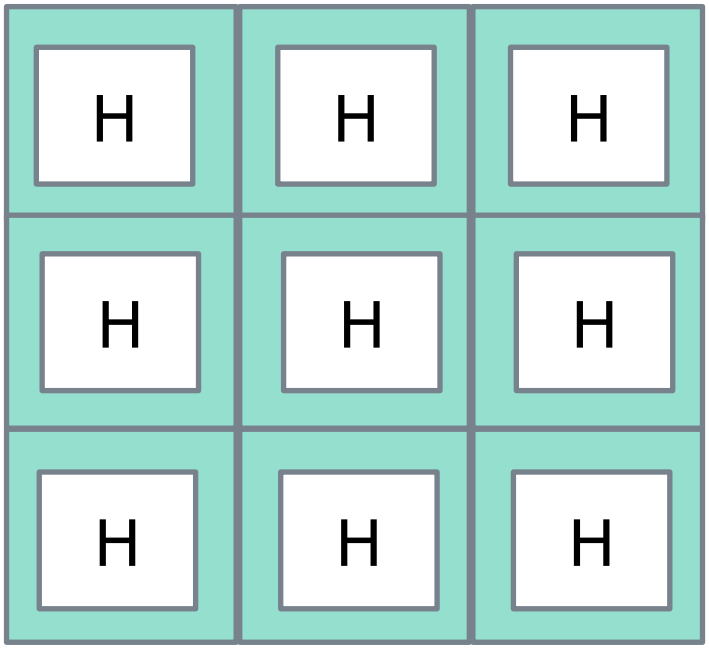
量子プロセッサーのチップの上では、
n個のqubitが、碁盤の目状に並べられています。



量子コンピュータにとって
大事なことが二つあります。
一つは、量子の状態を維持
し続けることができること
です。
もう一つは、どのqubitに
対しても、そのqubitを操作
して、その状態を変える
ゲートの機能を組み込む
ことができることです。

注意：量子コンピュータでは、qubitの状態を直接操作します。それがゲートの
役割を果たします。実際には、この図のように明示的にゲートが配置される
わけではないのですが、わかりやすくする為、ここではゲートを使って説明します。

量子プロセッサーのチップの上では、
n個のqubitが、碁盤の目状に並べられています。



量子コンピュータにとって
大事なことが二つあります。
一つは、量子の状態を維持
し続けることができること
です。
もう一つは、どのqubitに
対しても、そのqubitを操作
して、その状態を変える
ゲートの機能を組み込む
ことができることです。

このゲートの働きと配置については、次に説明します。

qubitの状態は
どのように変化するのか？

qubitの状態は
どのように変化するのか？

qubitの計算（ゲートの作用による状態の変化）は、qubitの配置された平面上で進行するわけではありません。この平面とは垂直な方向で進行します。

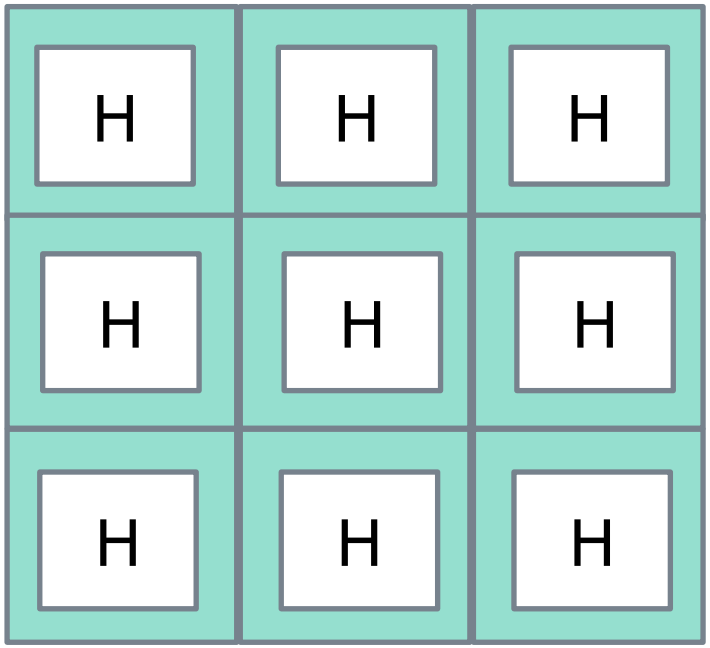
qubitの状態は
どのように変化するのか？

qubitの計算（ゲートの作用による状態の変化）は、qubitの配置された平面上で進行するわけではありません。この平面とは垂直な方向で進行します。

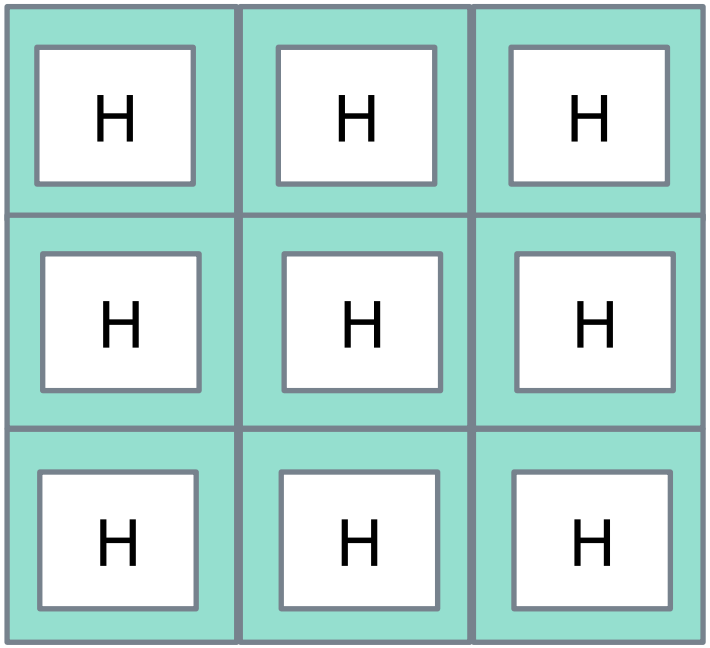
どこに垂直な方向があるのでしょう？

それを説明したいと思います。

量子プロセッサーのチップの上では、
ゲートが、碁盤の目状に並べられています。

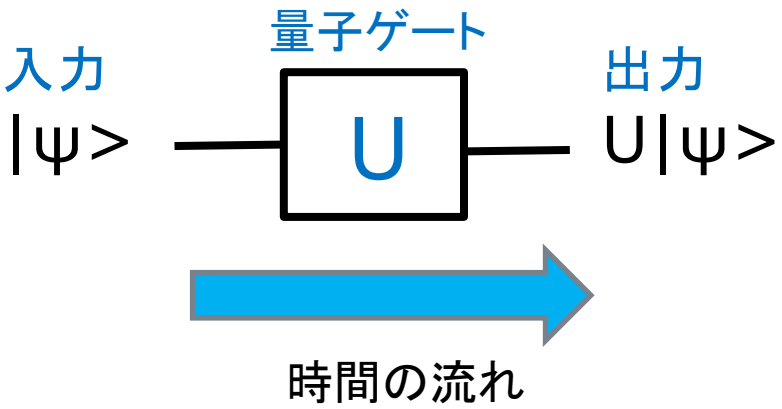


量子プロセッサーのチップの上では、
ゲートが、碁盤の目状に並べられています。

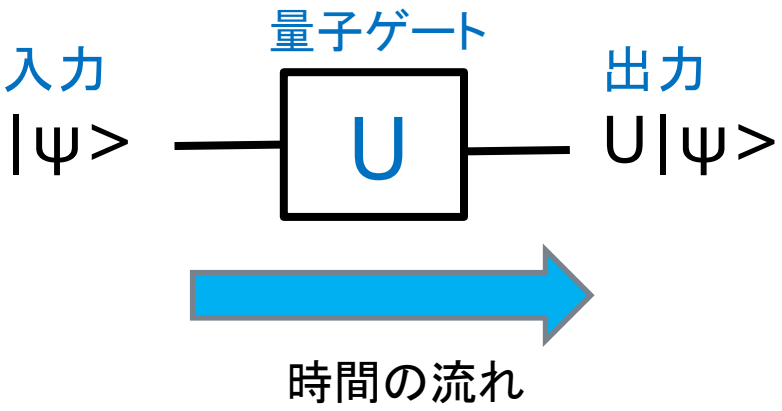


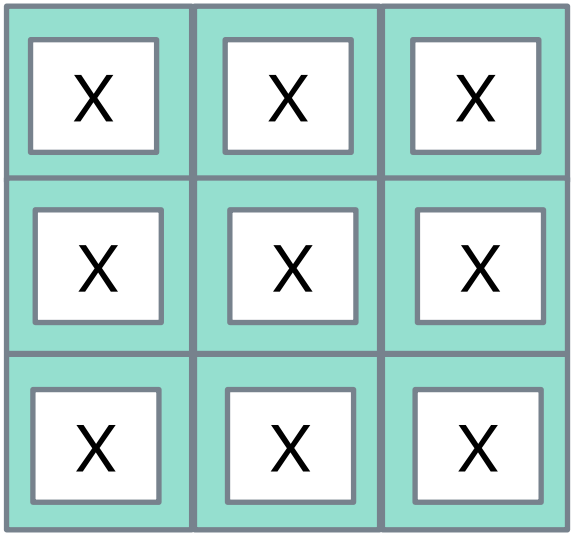
ここでは、全てのqubitに、Hゲートの機能が組み込まれています。

1-qubitの入力を持つゲートの場合、入力|Ψ>は、
ゲートUの働きによって、出力U|Ψ>に変換されます。



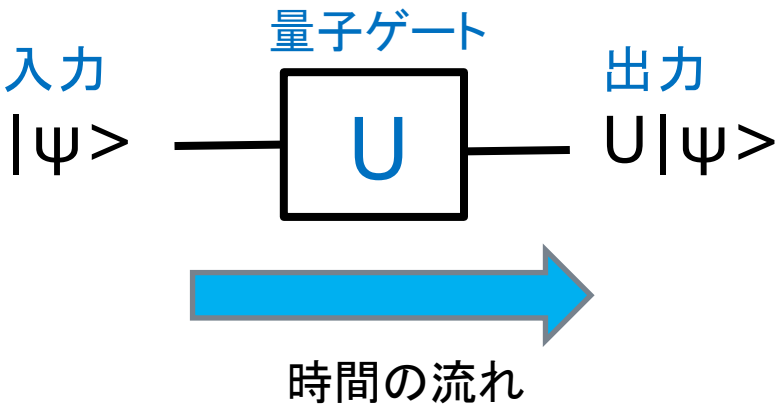
1-qubitの入力を持つゲートの場合、入力|Ψ>は、
ゲートUの働きによって、出力U|Ψ>に変換されます。

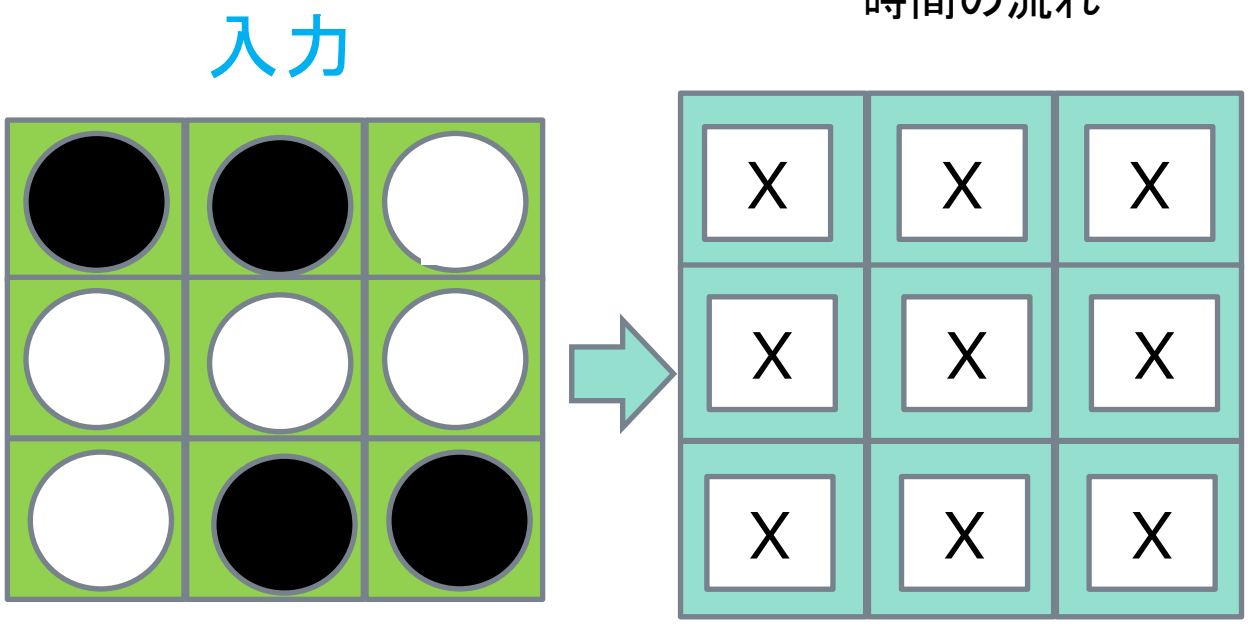




この例では、チップの上に、格子状に
Xゲートが並んでいます。

1-qubitの入力を持つゲートの場合、入力|Ψ>は、
ゲートUの働きによって、出力U|Ψ>に変換されます。

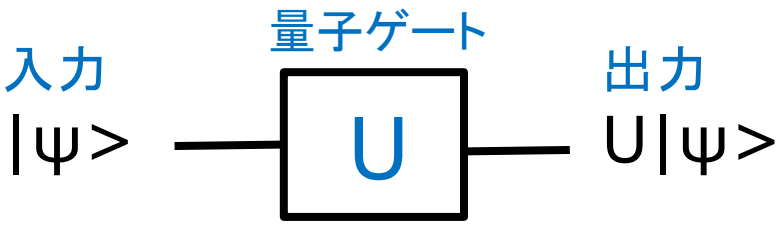




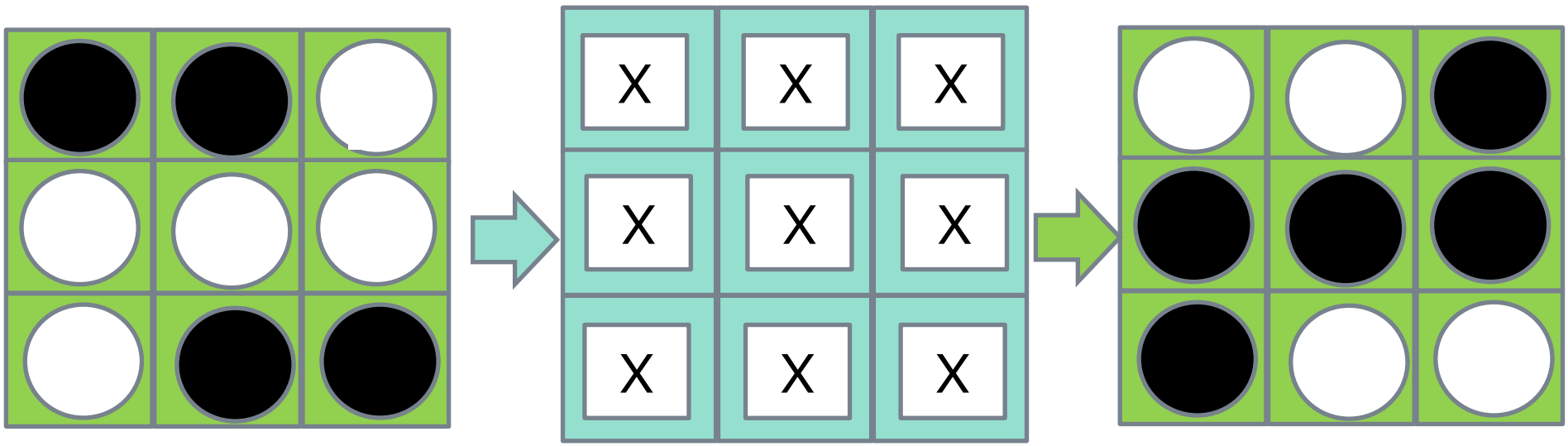
一つ前の
qubitの状態

時間的に一つ前のqubitの状態が
対応するゲートに入力として渡されます

1-qubitの入力を持つゲートの場合、入力|Ψ>は、
ゲートUの働きによって、出力U|Ψ>に変換されます。



入力

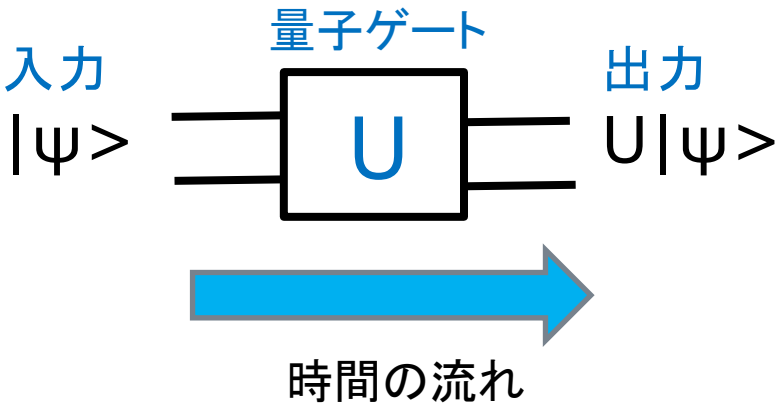


出力

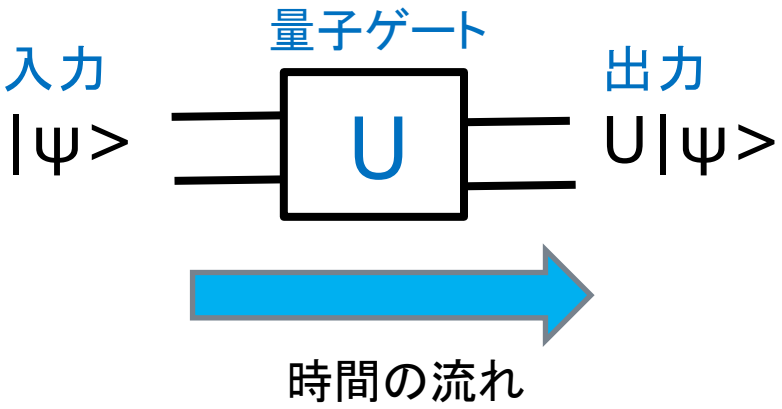
一つ前の
qubitの状態

対応するゲートの作用による出力で、
格子上のqubitの状態は、変化します

2-qubitの入力を持つゲートの場合も、ほとんど同じです。
2-qubitの入力|Ψ>は、2-qubitのゲートUの働きによって、
2-qubitの出力U|Ψ>に変換されます。

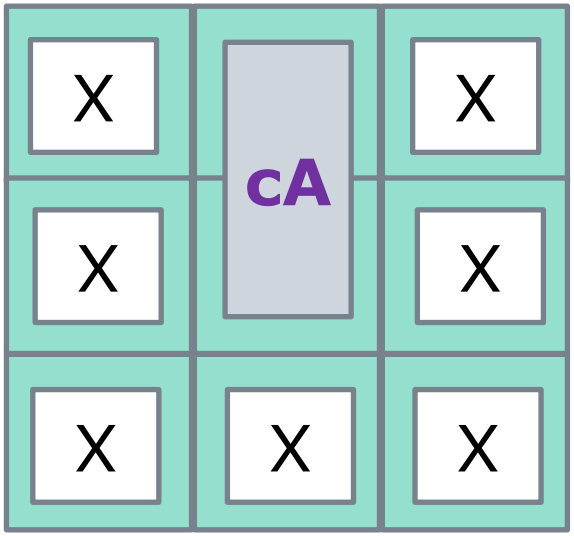


2-qubitの入力を持つゲートの場合も、ほとんど同じです。
2-qubitの入力|Ψ>は、2-qubitのゲートUの働きによって、
2-qubitの出力U|Ψ>に変換されます。

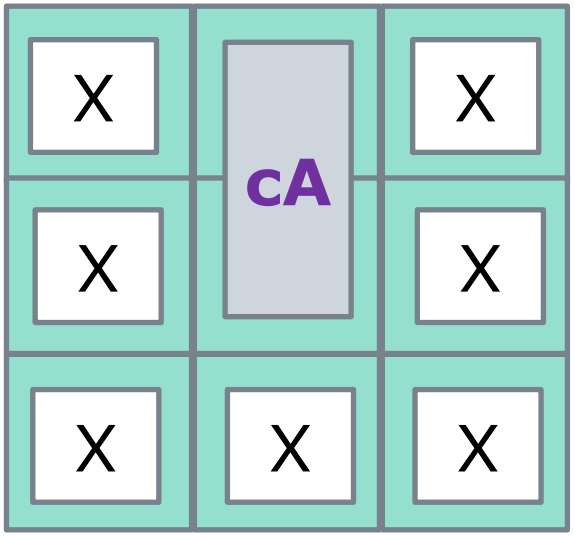


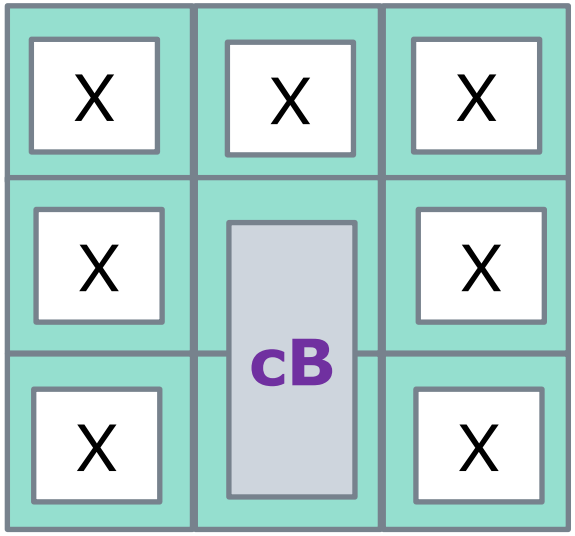
GoogleのSycamore量子プロセッサーの場合
隣り合う二つのqubit上に、2-qubitの入力を持つ
CNOTやControl-Zといった2-qubitゲートを構成
できます。

2-qubitゲートを含む回路の例を見ておきましょう。

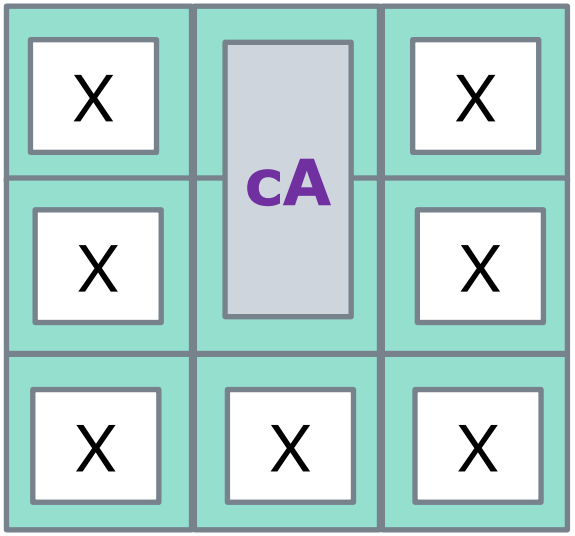


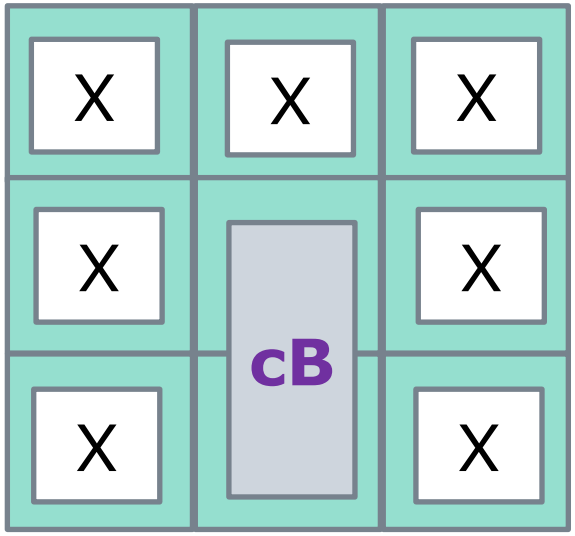
2-qubitゲートを含む回路の例を見ておきましょう。

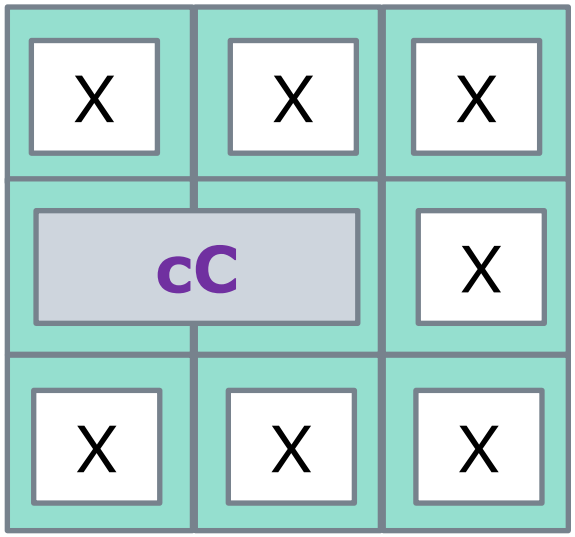




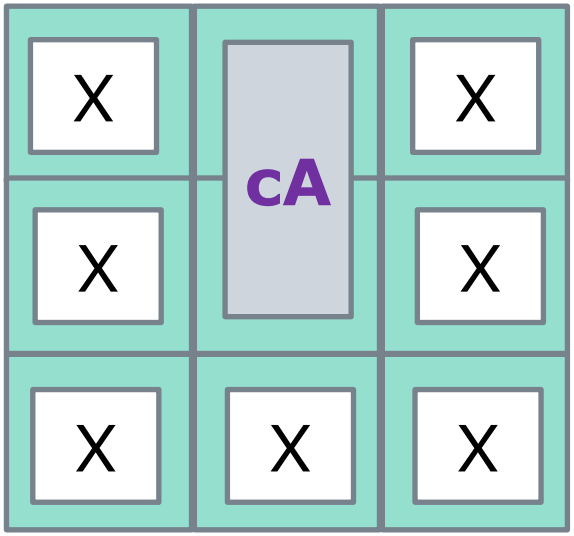
2-qubitゲートを含む回路の例を見ておきましょう。

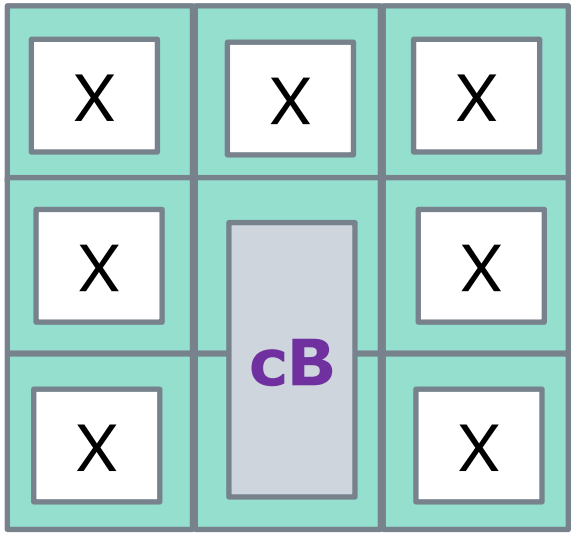


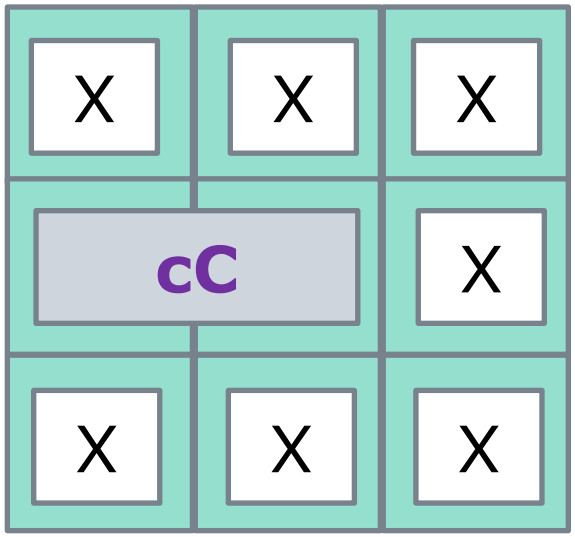


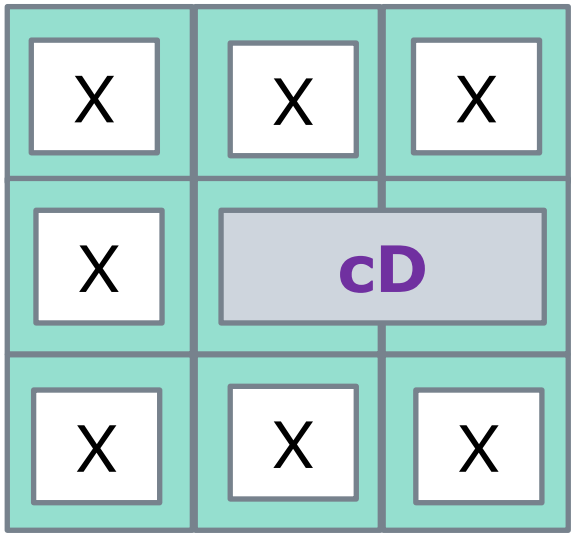


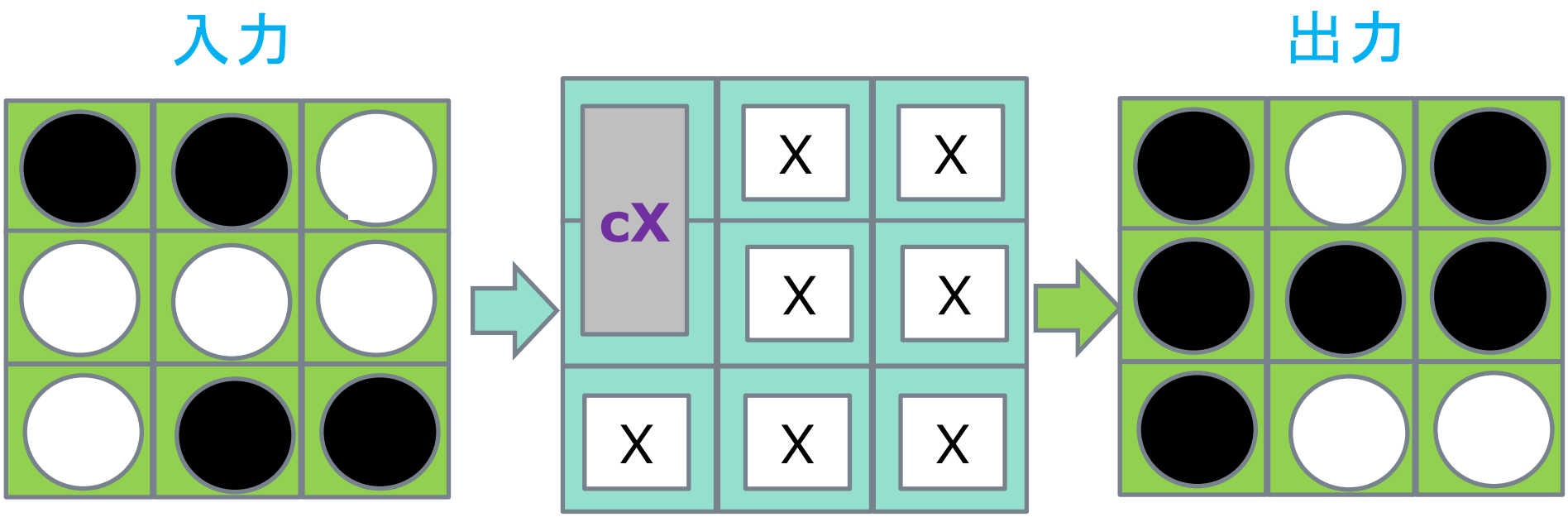
2-qubitゲートを含む回路の例を見ておきましょう。



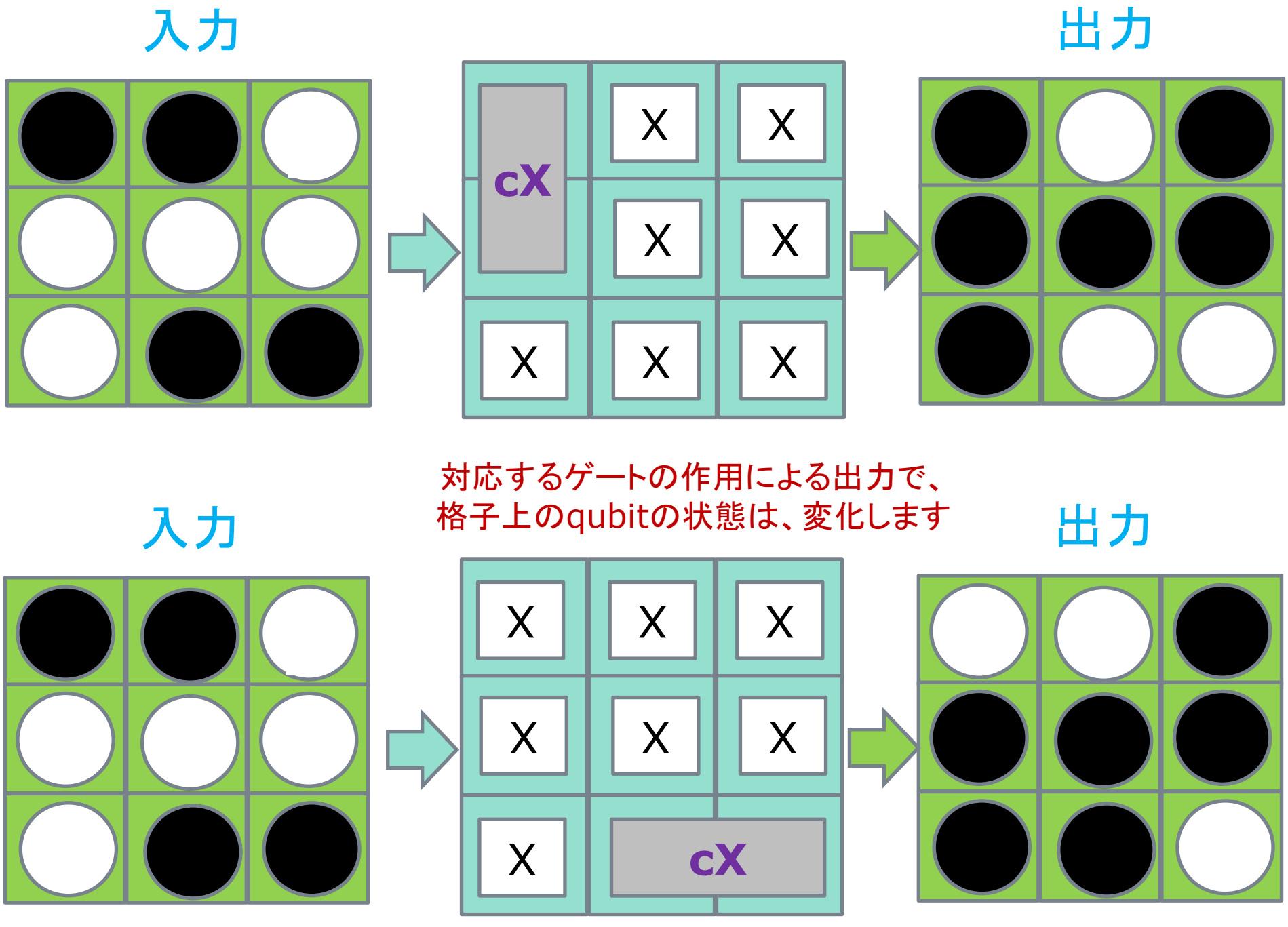








対応するゲートの作用による出力で、
格子上のqubitの状態は、変化します


入力
cX
X
出力
対応するゲートの作用による出力で、
格子上のqubitの状態は、変化します
入力
cX
X
出力

量子プロセッサーは
どのように「計算」をするのか？

量子プロセッサーは
どのように「計算」をするのか？

先に、qubitの「計算」（ゲートの作用による状態の変化）は、qubitの配置された平面上で進行するわけではなく、この平面とは垂直な方向で進行すると述べました。

量子プロセッサーは
どのように「計算」をするのか？

先に、qubitの「計算」（ゲートの作用による状態の変化）は、qubitの配置された平面上で進行するわけではなく、この平面とは垂直な方向で進行すると述べました。

どこに垂直な方向があるのでしょう？

量子プロセッサーは
どのように「計算」をするのか？

先に、qubitの「計算」（ゲートの作用による状態の変化）は、qubitの配置された平面上で進行するわけではなく、この平面とは垂直な方向で進行すると述べました。

どこに垂直な方向があるのでしょう？

それは、時間の進む方向です。

量子プロセッサーは
どのように「計算」をするのか？

量子プロセッサーにも、「クロック」に相当するものがあって、そのステップに同期して、チップ全体の状態が変わって行きます。それが「計算」です。

量子プロセッサーは
どのように「計算」をするのか？

量子プロセッサーには、「クロック」に相当するものがあって、そのステップに同期して、チップ全体の状態が変わって行きます。それが「計算」です。

普通のコンピュータでは、チップ上でのゲートの集積が目立つかもしれないのですが、CPUの中核であるレジスターの状態の時間変化に注目すれば、原理的には同じことですね。

量子プロセッサーは
どのように「計算」をするのか？

量子プロセッサーには、「クロック」に相当するものがあって、そのステップに同期して、チップ全体の状態が変わって行きます。

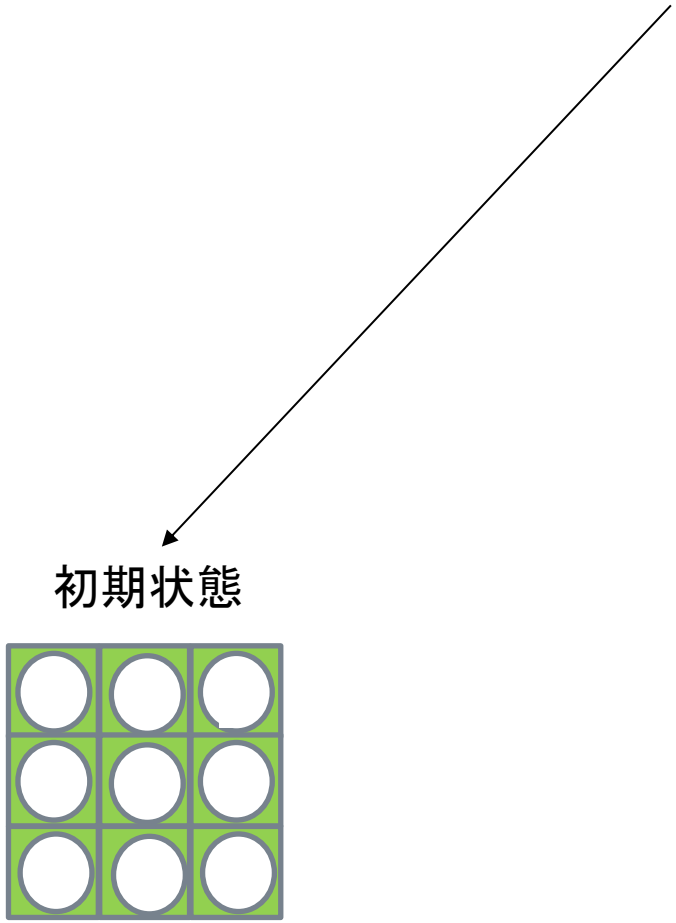
普通のコンピュータでは、チップ上でのゲートの集積が目立つかもしれないのですが、CPUの中核であるレジスターの状態の時間変化に注目すれば、原理的には同じことですね。

このことを、簡単な例で見てみましょう。

「計算」は、時間の進行とともに進みます。ここでは、
その時間の単位を「ステップ」と呼ぶことにします。

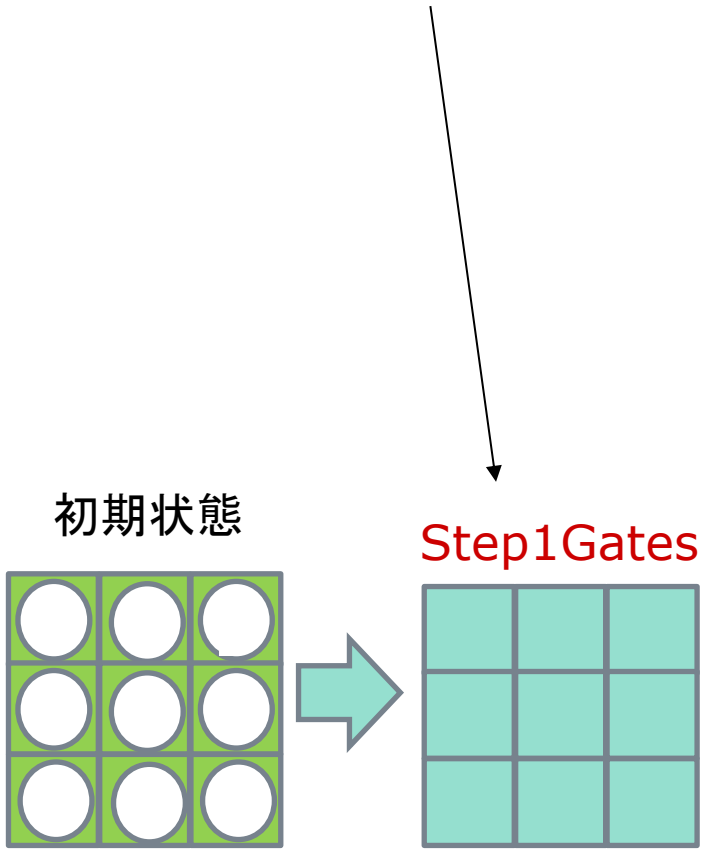
「計算」は、時間の進行とともに進みます。ここでは、
その時間の単位を「ステップ」と呼ぶことにします。

n個のqubitの最初の状態は、



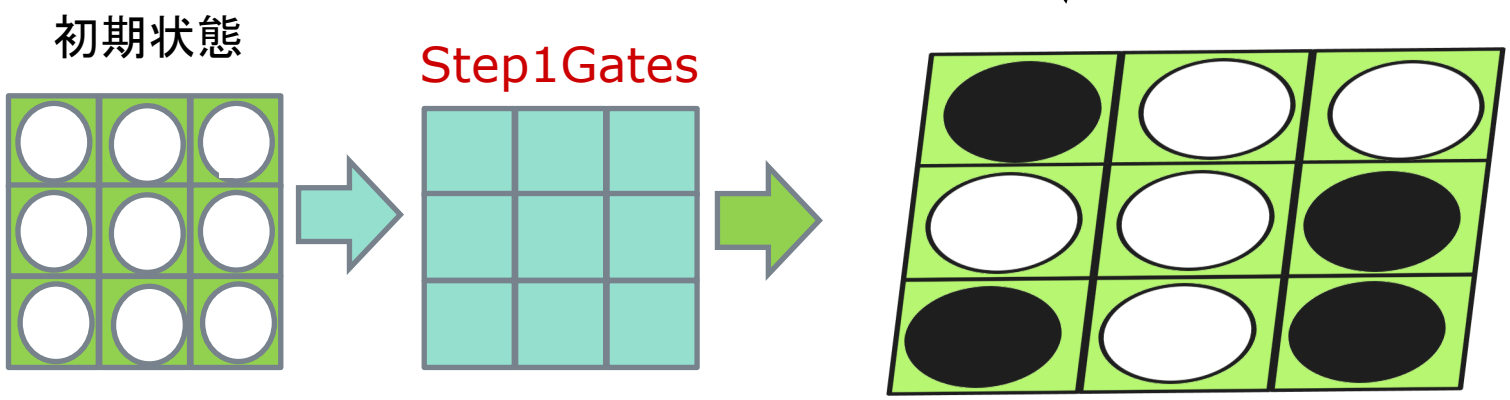
「計算」は、時間の進行とともに進みます。ここでは、その時間の単位を「ステップ」と呼ぶことにします。

n個のqubitの最初の状態は、Step1のために構成されたゲートに渡されて、



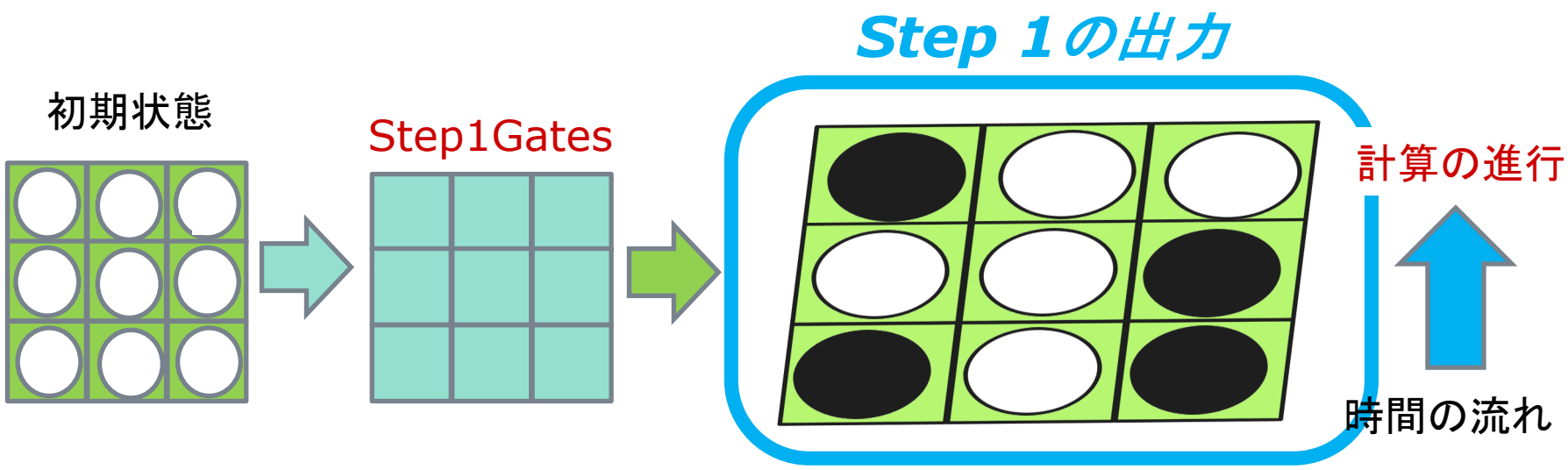
「計算」は、時間の進行とともに進みます。ここでは、その時間の単位を「ステップ」と呼ぶことにします。

n個のqubitの最初の状態は、Step1のために構成されたゲートに渡されて、その出力として、n個のqubitの状態は変化します。



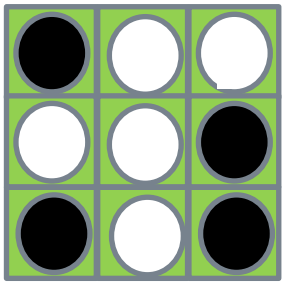
「計算」は、時間の進行とともに進みます。ここでは、その時間の単位を「ステップ」と呼ぶことにします。

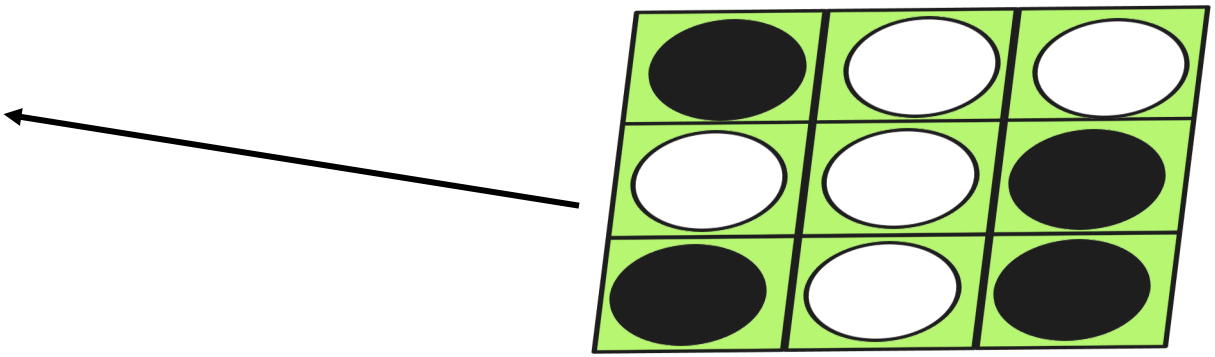
n個のqubitの最初の状態は、Step1のために構成されたゲートに渡されて、その出力として、n個のqubitの状態は変化します。これが、Step2のゲートの入力になります。



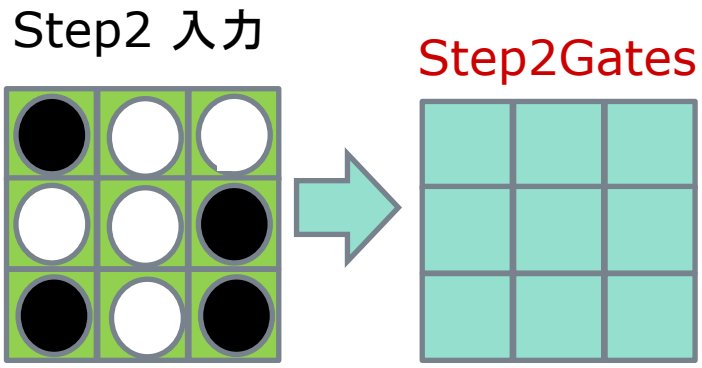
Step1の出力は、Step2の入力になります。

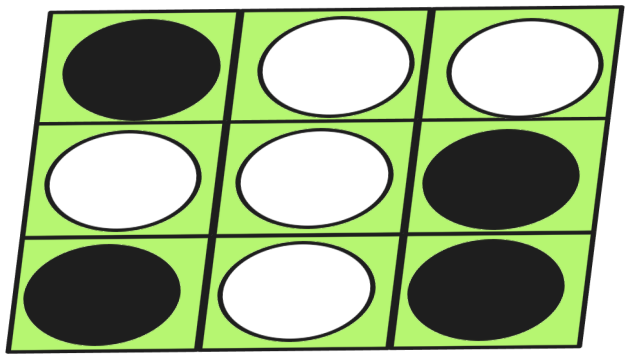
Step2 入力



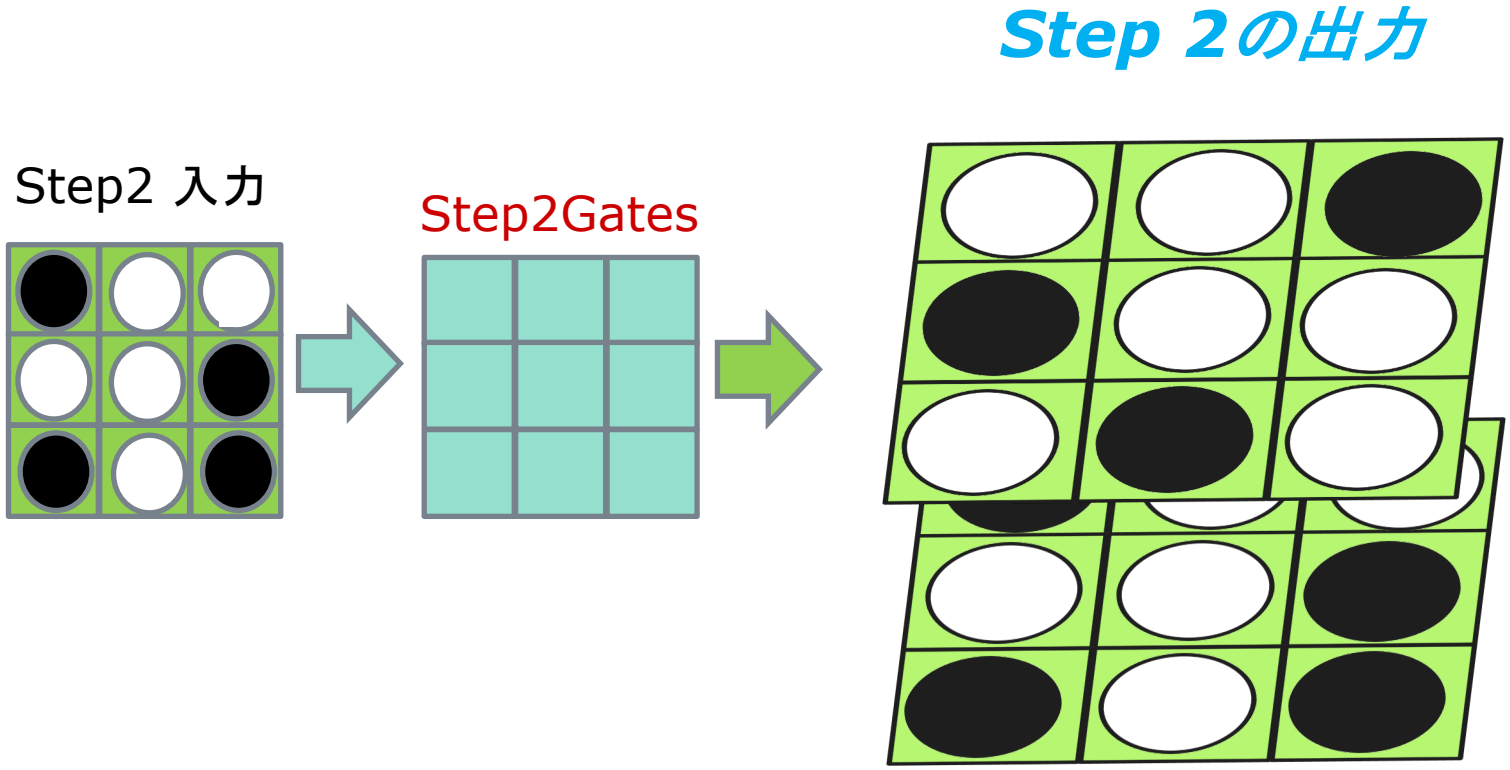


Step1の出力は、Step2の入力になります。
それはStep2のゲートに渡されて、



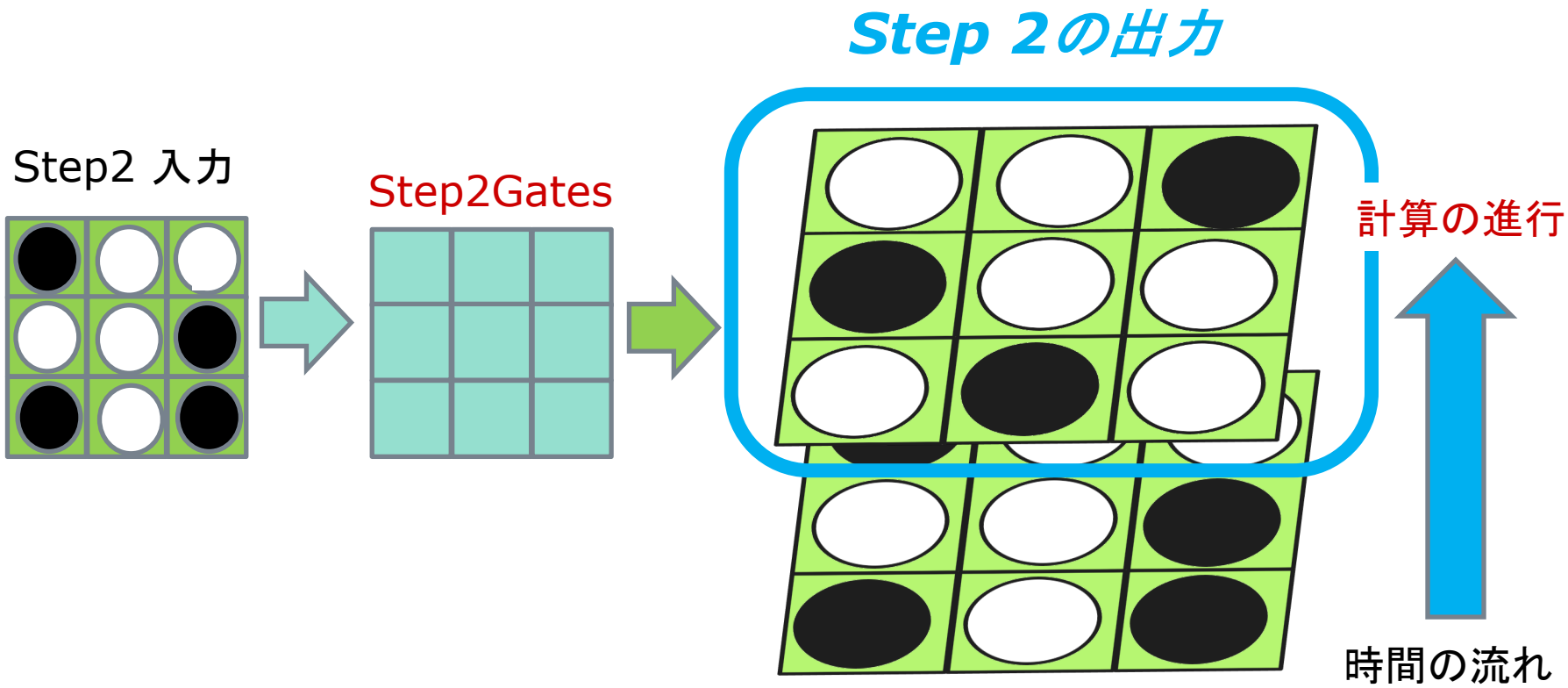


Step1の出力は、Step2の入力になります。
それはStep2のゲートに渡されて、Step2の出力を生み出します。

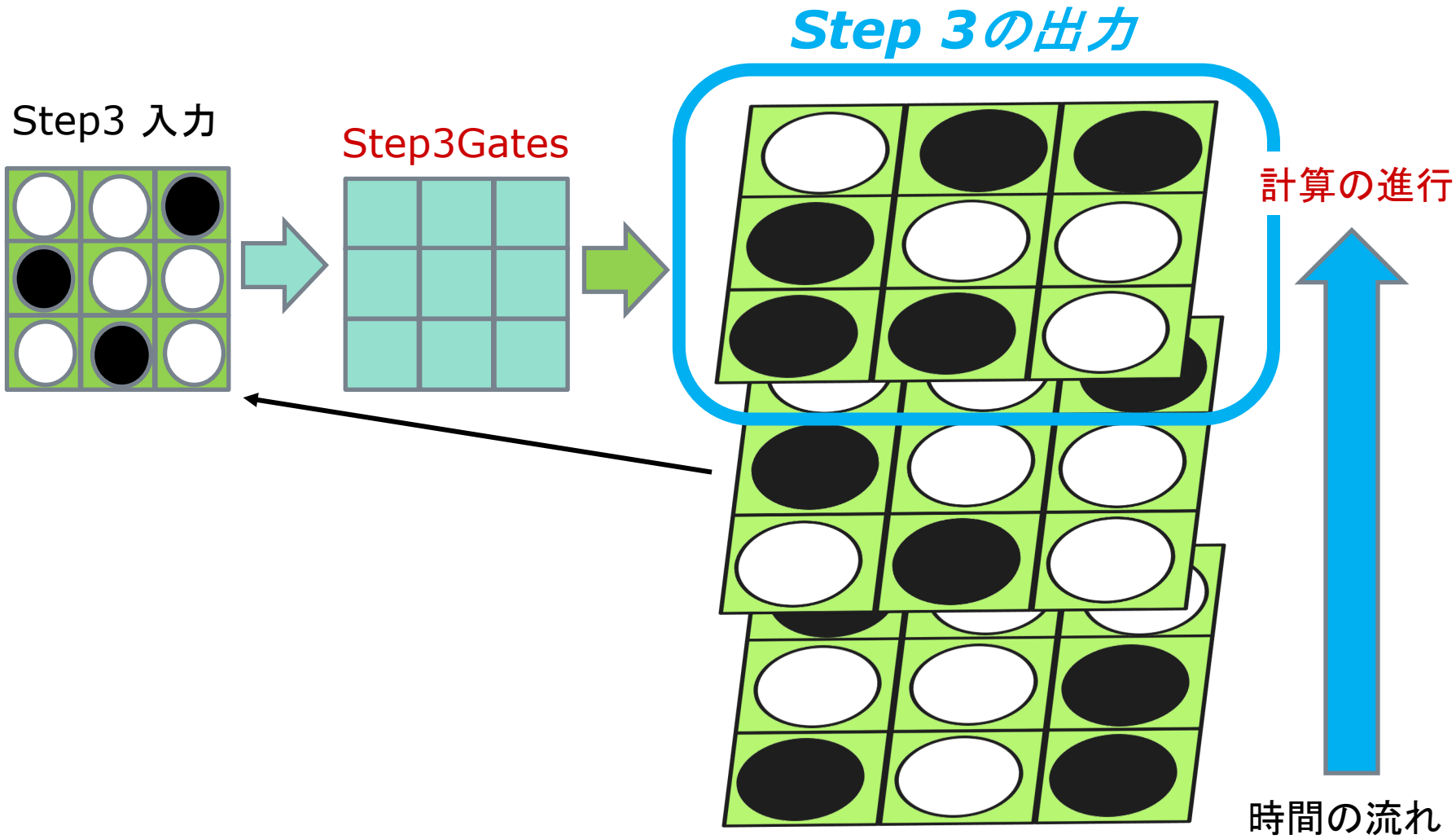


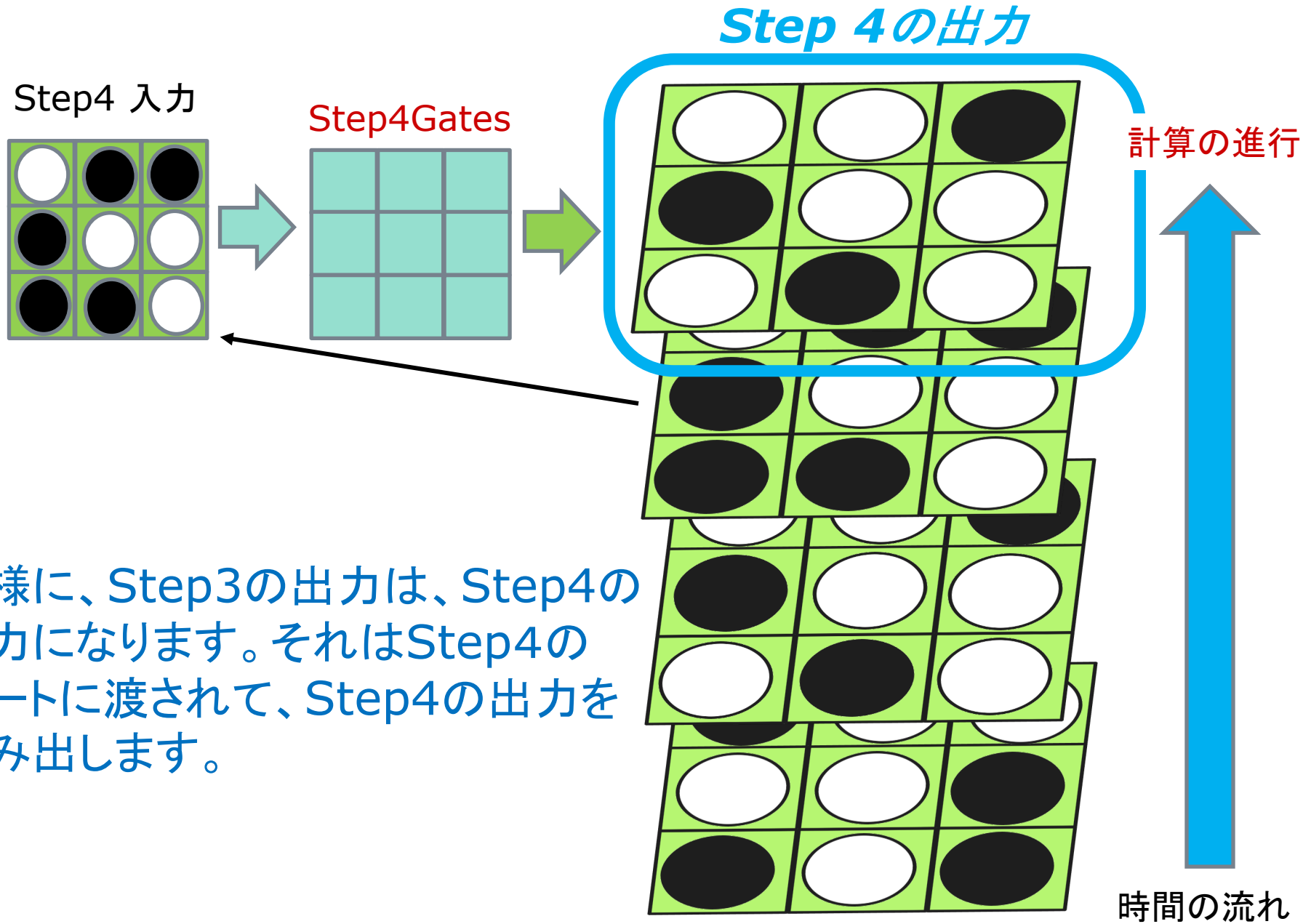
Step1の出力は、Step2の入力になります。
それはStep2のゲートに渡されて、Step2の出力を生み出します。

こうして、計算が進行します。

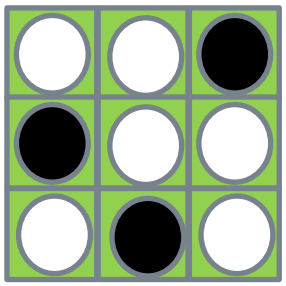


Step2の出力は、Step3の入力になります。
それはStep3のゲートに渡されて、Step3の出力を
生み出します。

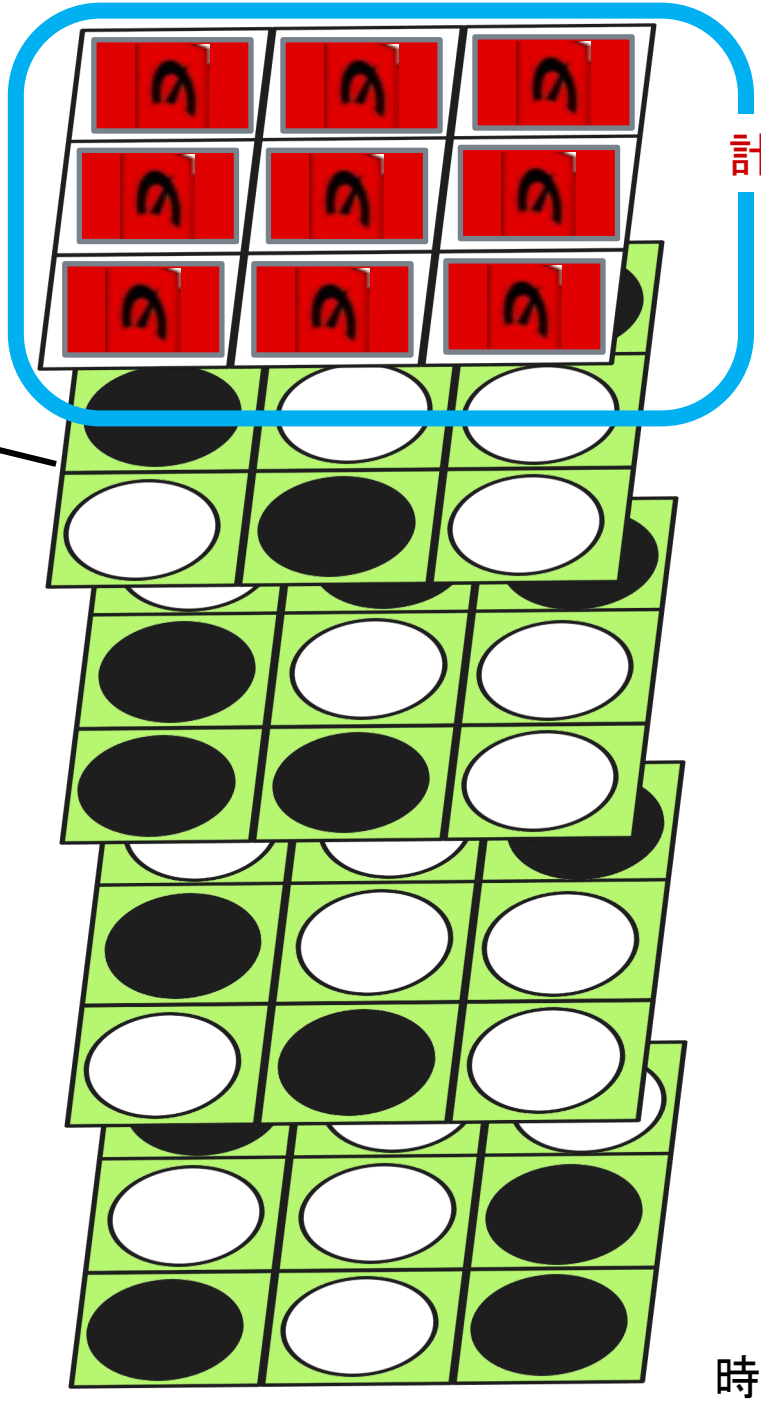




同様に、Step3の出力は、Step4の入力になります。それはStep4のゲートに渡されて、Step4の出力を生み出します。



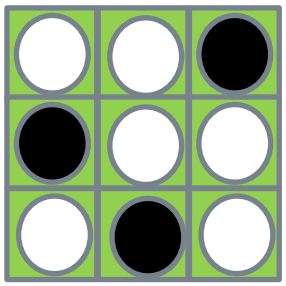
測定



計算結果

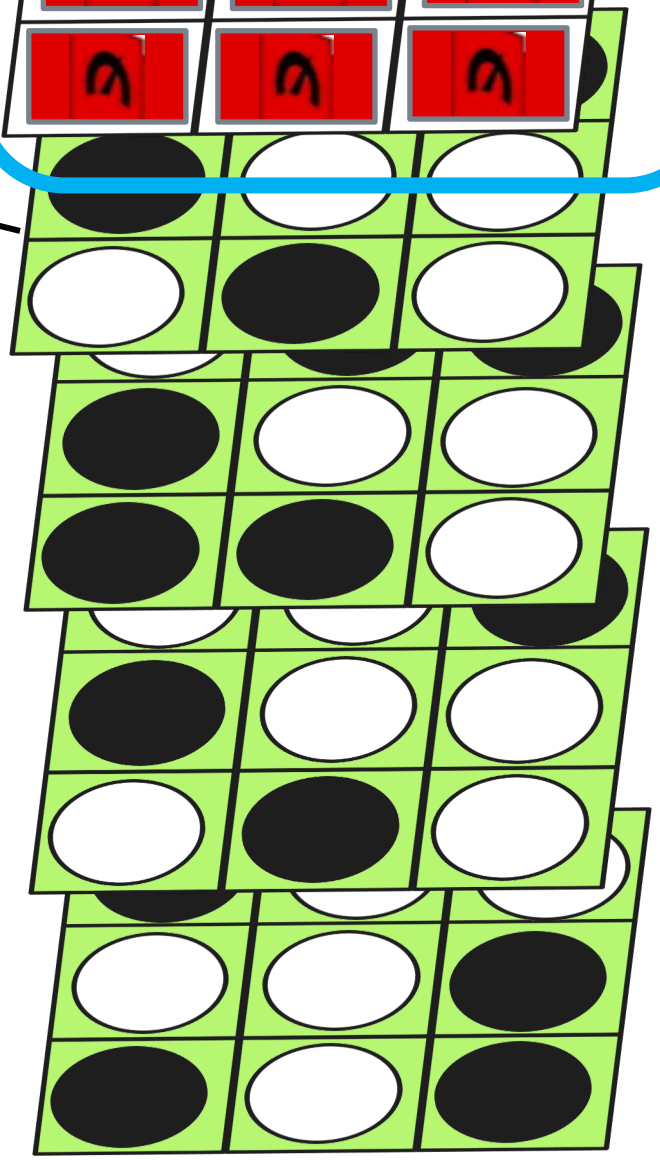
時間の流れ

この例では、Step4に進んだ所で
計算を止めています。



測定

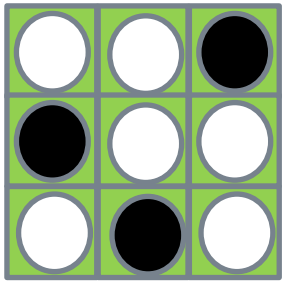
計算結果

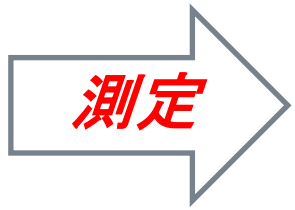


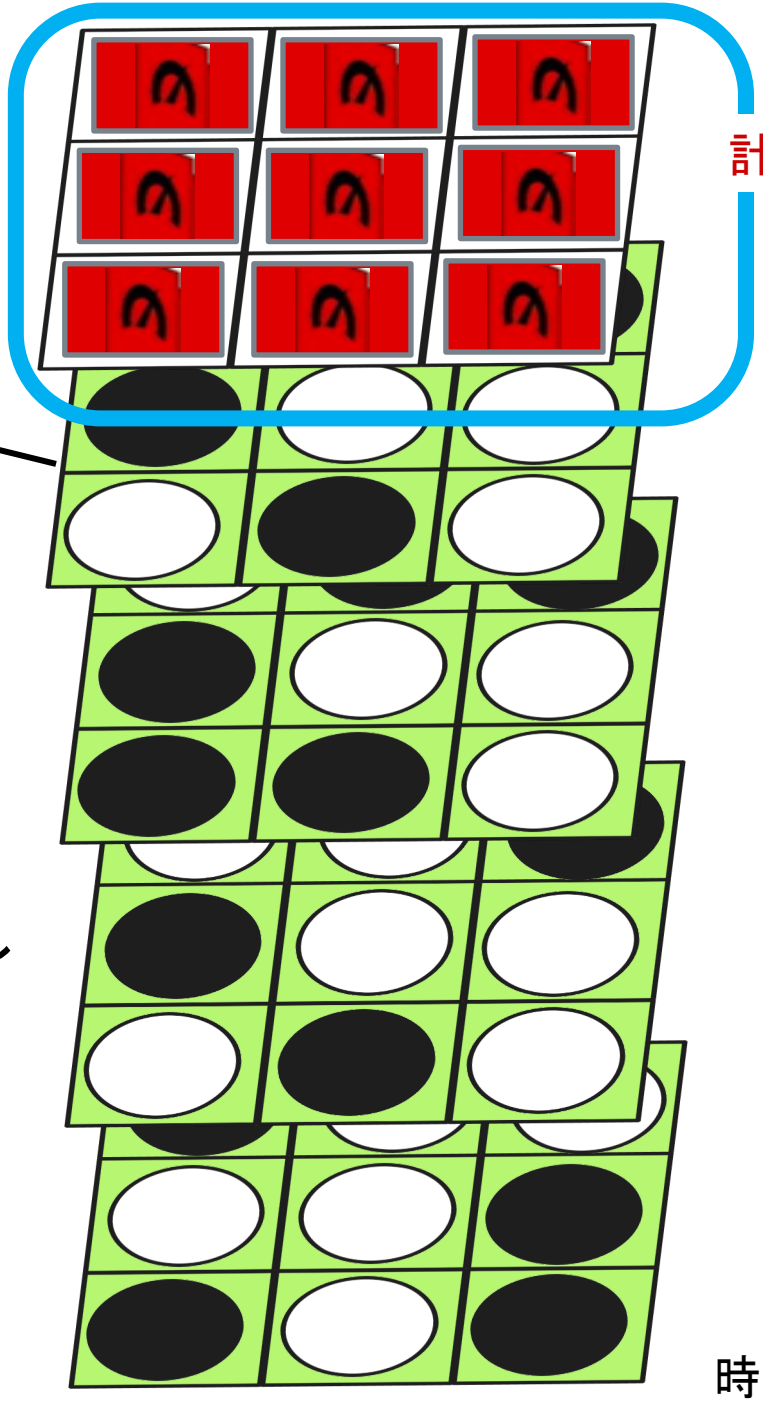
時間の流れ

この例では、Step4に進んだ所で計算を止めています。

計算結果を得るためには、3 x 3の9個のqubitを一つずつ、観測し測定します。







この例では、Step4に進んだ所で計算を止めています。

計算結果を得るためには、3 x 3の9個のqubitを一つずつ、観測し測定します。

観測で得られるのは、0(白)または1(黒)からなる、9bitの長さのbit列です。これが計算結果です。

量子優越性の実験は、どのように行われたか

量子優越性の実験に使われたGoogleのsycamore プロセッサーは、53-54 qubitです。それは、8 x 8 で 64個のマス目を持つオセロゲームより、少し小さい配置スペースを持ちます。

量子優越性の実験に使われたGoogleのsycamore プロセッサーは、53-54 qubitです。それは、8 x 8 で 64個のマス目を持つオセロゲームより、少し小さい配置スペースを持ちます。

「量子優越性」の実験では、20ステップまで計算を続けましたた。オセロの盤面を20個重ねたものをイメージしても、いいかもしれません。ハードウェアの構成は、極めてシンプルに思えます。

量子優越性の実験に使われたGoogleのsycamore プロセッサーは、53-54 qubitです。それは、8 x 8 で 64個のマス目を持つオセロゲームより、少し小さい配置スペースを持ちます。

「量子優越性」の実験では、20ステップまで計算を続けましたた。オセロの盤面を20個重ねたものをイメージしても、いいかもしれません。ハードウェアの構成は、極めてシンプルに思えます。

20ステップで観測をすると、各qubitは、0 または 1の値を返します。20ステップの計算をワンセットとした観測で、53個の各qubitの観測の結果として、53bit長ののの0と1のビット列を得ることになります。

実験では、同じ初期条件、各ステップのゲート配置を同一にして、20ステップの同一の計算を100万回繰り返しました。100万回の実行に要した時間は、約200秒でした。極めて高速です。

100万回の計算の繰り返しで、観測結果の53ビットのビット列を、100万個得たことになります。

前節での「計算」の説明では、「状態」の時間的推移を中心に図示をしました。ただ、「オセロの盤面 20段重ね」という比喩は、分かりやすいですが、正確なものではありません。

前節での「計算」の説明では、「状態」の時間的推移を中心に図示をしました。ただ、「オセロの盤面 20段重ね」という比喩は、分かりやすいですが、正確なものではありません。

だいいち、 各ステップで計算途中の量子の状態は、白・黒の二つの値で表されるわけではありません。最後に観測されて、はじめて 0または1の値を返すことになるのですが。

前節での「計算」の説明では、「状態」の時間的推移を中心に図示をしました。ただ、「オセロの盤面 20段重ね」という比喩は、分かりやすいですが、正確なものではありません。

だいいち、 各ステップで計算途中の量子の状態は、白・黒の二つの値で表されるわけではありません。最後に観測されて、はじめて 0または1の値を返すことになるのですが。

それに、先の状態の推移の図では、各ステップごとのゲートの配置の内容が、ほとんど省略されています。

次に、ゲートの配置を表現した図を紹介します。

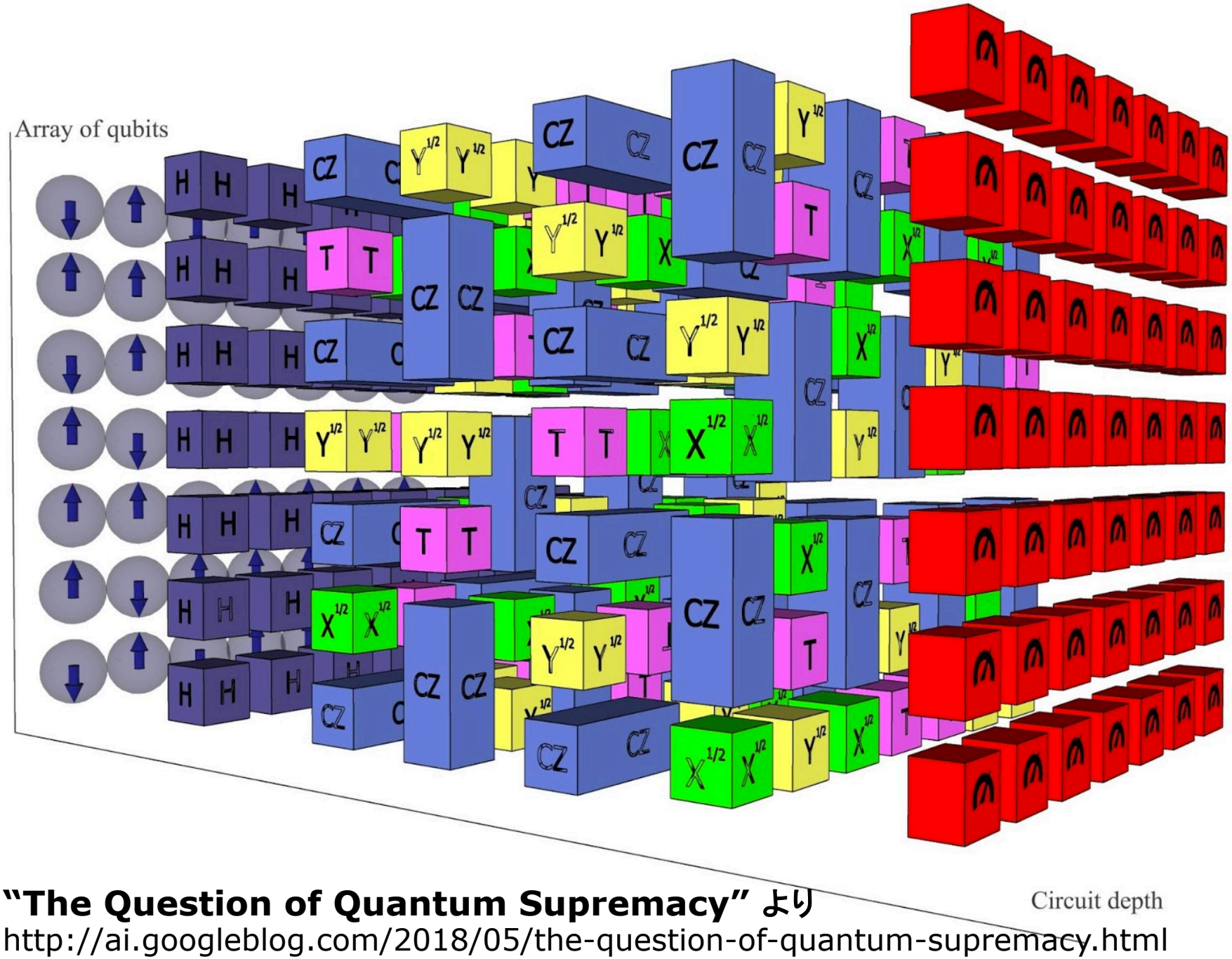
この図は、7 x 7 のマス目上に 49個のqubitを配置し、
5ステップの計算を実行し49個のbit列を観測する過程を、
ゲートの配置にフォーカスして図示したものです。

次に、ゲートの配置を表現した図を紹介します。

この図は、7 x 7 のマス目上に 49個のqubitを配置し、
5ステップの計算を実行し49個のbit列を観測する過程を、
ゲートの配置にフォーカスして図示したものです。

ここでは、時間は左から右に流れています。
2-qubitの入力をもつゲートは、紫色で表されています。

なかなか複雑ですね。



“The Question of Quantum Supremacy” より
http://ai.googleblog.com/2018/05/the-question-of-quantum-supremacy.html

IBM論文の指摘

"Leveraging Secondary Storage to Simulate Deep 54-qubit Sycamore Circuits"

Edwin Pednault, John A. Gunnels, Giacomo Nannicini, Lior Horesh, Robert Wisnieff **2019/10/22**

https://arxiv.org/abs/1910.09534

最強のスーパーコンピュータを使えば、10,000年ではなく、2.5日でシミレートできる

- Googleの発表の一日前に公開されたIBMの5名の研究者による論文は、興味深いものである。
- 彼らは、オークリッジの国立研にある、世界最強のスーパーコンピュータであるSummitを使えば、Google の 53-54 qubitのSycamore プロセッサーの出力のシミレートを、Googleのいう10,000年ではなく、2.5日でシミレートできるという。

- これは、本当かもしれない。

2^{53} 個の量子の状態を、メモリー上ではなく、250ペタバイトのディスク上に置く

- 彼らのアイデアは、シミレートすべき2^{53} 個の量子の全状態を、メモリー上ではなく、Summitの250ペタバイトのディスク上に置くというものであった。（Googleのスーパーコンピュータでのシミレートは、量子の状態をメモリーの上に置いていた。）
- もちろん、シミレーションのアルゴリズムも、違ったものになる。ただ、それによって、Sycamoreのシミレーションは、10,000年ではなく、2.5日で可能になるという。

- 本当かもしれない。

チェックしてみよう

- ここでは、2^{53} 個の量子の全状態を、メモリー上ではなく、Summitの250ペタバイトのディスク上に置けるかどうかをチェックしてみよう。
- $2^{10} \approx 1K$ キロ とすると、
  $2^{20} \approx 1M$ メガ
  $2^{30} \approx 1G$ ギガ
  $2^{40} \approx 1T$ テラ
  $2^{50} \approx 1P$ ペタ である。
- 量子の状態は、二つの複素数の組みで表されるから、四つの実数の組みと考えていい。実数が4バイト(32ビット)で表現されるなら、量子の状態は16バイトで表現される。
- $2^{53} = 2^3 \cdot 2^{50} =$ 8ペタ個の量子の状態は、
  8ペタ x 16バイト = 64ペタバイトの容量を持つ。
- 64ビットの実数なら、128ペタバイトになる。ギリギリ、セーフ？

IBM論文に対する Aaronsonの指摘

“Quantum supremacy: the gloves are off”

Scott Aaronson **2019/10/23**

https://www.scottaaronson.com/blog/?p=4372

アーロンソン反論を開始する

- アーロンソンは、このブログ投稿で、自分がGoogleのNature論文の査読者であったことを初めて明かす。 査読者なので論文公開まで、「批判」に反論できなかったという。また、Googleのスーパー・コンピュータでのシミレーションが、自分の提案したアルゴリズムに基づいていたことを認める。（それは、Googleの論文の注を見ればわかる。）
- 彼は、このIBM論文を、Google論文の最初のリークに対するIBMのフィナンシャル・タイムズでの冷笑的なコメントよりずっとマシなものだとする。 さらに、Googleも、もっとしっかりやれば良かったのにと言う。
- ただ、アーロンソンは、次のように語る。
  「この分析は、Googleの実験では量子優越性が、達成されていないことを意味するのであろうか？　断じてそうではない。」

量子プロセッサ Sycamoreは、世界最速のスーパー・コンピュータSummitより、1,200倍早い

- Sycamoreは、500万個のデータサンプルを得るのに、約3分かかった。IBMの論文では、それは 1万年ではなく 2.5日で計算できると言う。でも、3分 vs. 2.5日は、1,200倍の違いだ。量子プロセッサ Sycamoreは、世界最速のスーパー・コンピュータSummitより、1,200倍早いのだ。
- しかし、もっと重要なのは、実験で利用された「基本的演算」の数の比較だ。量子コンピュータの場合、基本演算の数は量子ゲートの数だが、スーパーコンピュータの場合、「基本的演算」は「浮動小数点演算 FLOP」だ。
- アーロンソンの試算によれば、今回の実験での基本演算の数は、Sycamoreが $5x10^9$ 量子ゲート、Summitが 2×10^{20} FLOPs で、その比は、400億倍にもなると言う。

53qubitではなく 55qubitになれば、Summitが二台必要になる。70qubitの量子コンピュータでは？

- 全てをハードディスクに格納すると言うスタイルでは、例えば、量子プロセッサーのqubitが実験時のsycamoreの53qubitから55qubitに増えれば、明らかにSummitの250ペタバイトのハードディスクの容量を超えることになる。55qubitでは、Summitが2台必要になる。
- 5qubit増えて60qubitになれば、qubitの状態の数は $2^5=32$倍になるから、さらに32台のSummitが必要になる。70qubitになればどうだろう？ 60qubitから10qubit増えると、状態の数は、$2^{10}=1024$倍になる。だから、70qubitの量子プロセッサーをシミレートするには、3,000台以上のSummitが必要だと言うことになる。
- （Googleは 2018年には、72qubitのBristleCornを開発している。）

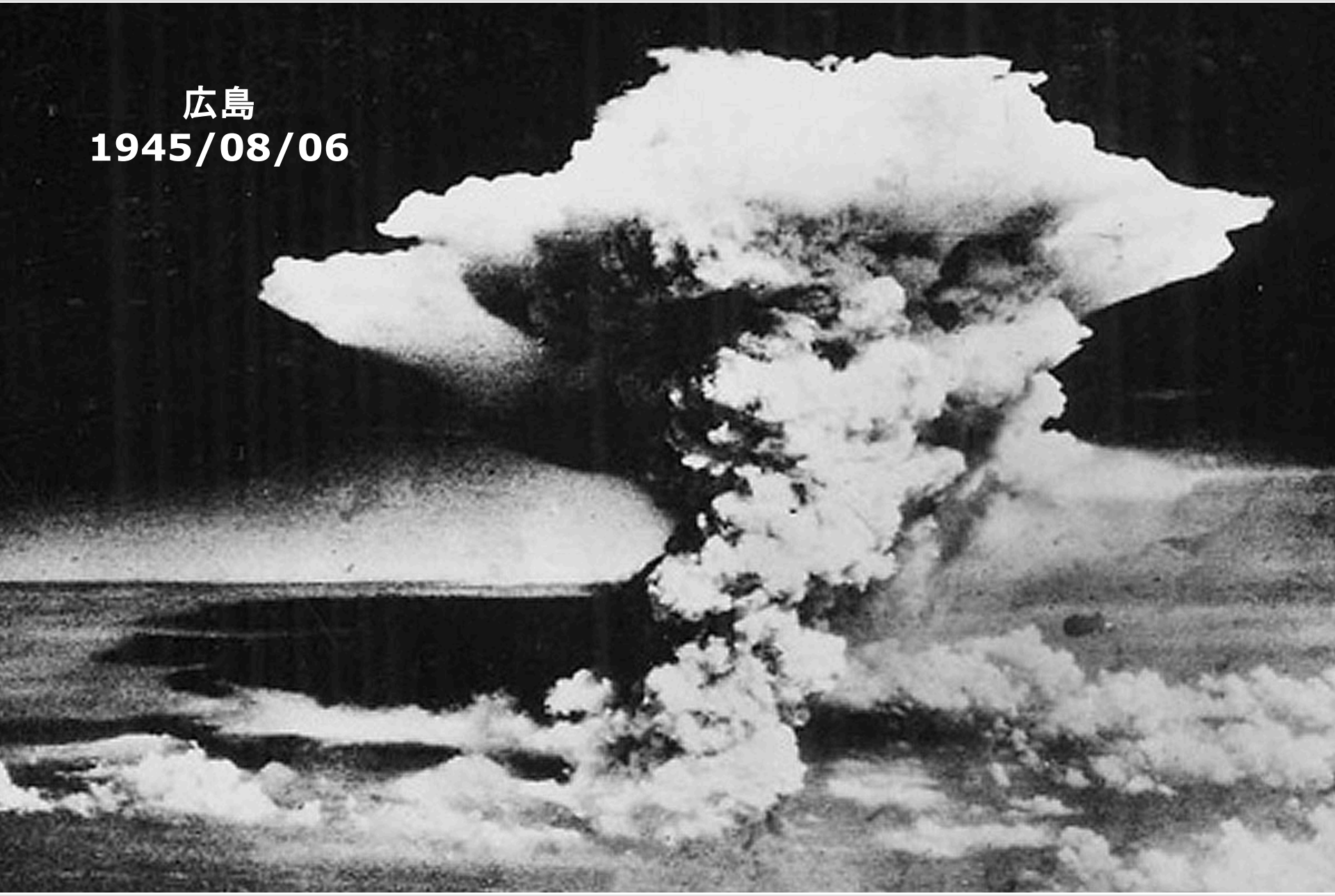
「なぜ、Googleの量子優越性のマイルストーンは重要なのか？」

- アーロンソンは、一般の読者向けに、ニューヨーク・タイムス紙に、「なぜ、Googleの量子優越性のマイルストーンは重要なのか？」という記事を投稿している。こちらの記事も参照されたい。

"Why Google's Quantum Supremacy Milestone Matters" Scott Aaaronson, **2019/10/30**

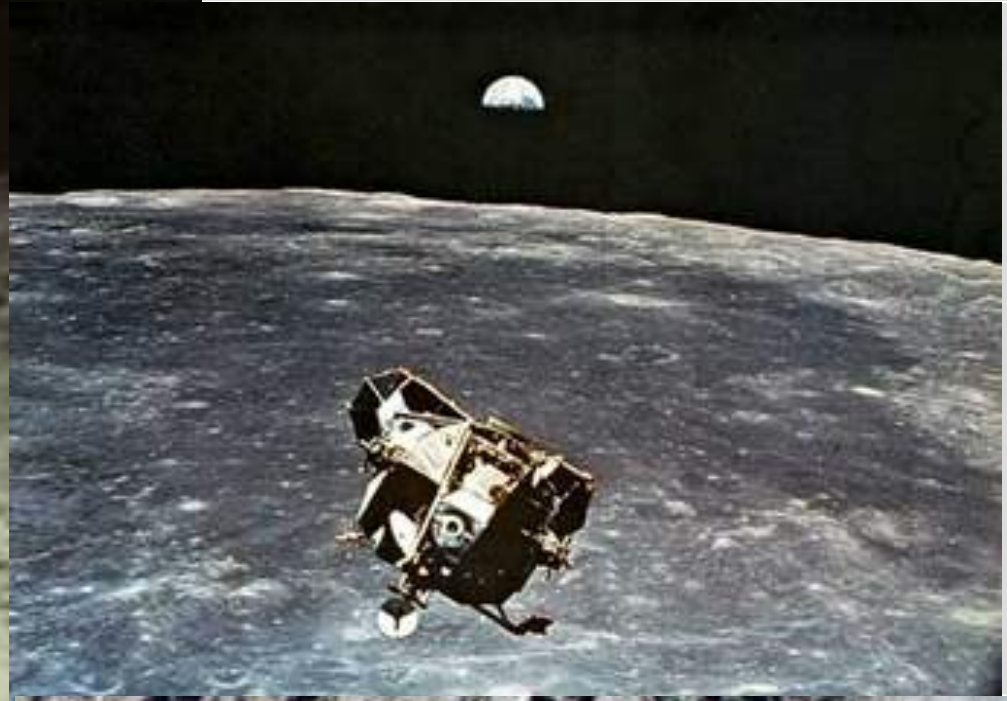
https://www.nytimes.com/2019/10/30/opinion/google-quantum-computer-sycamore.html

科学・技術のマイルストーンを考える


広島
1945/08/06

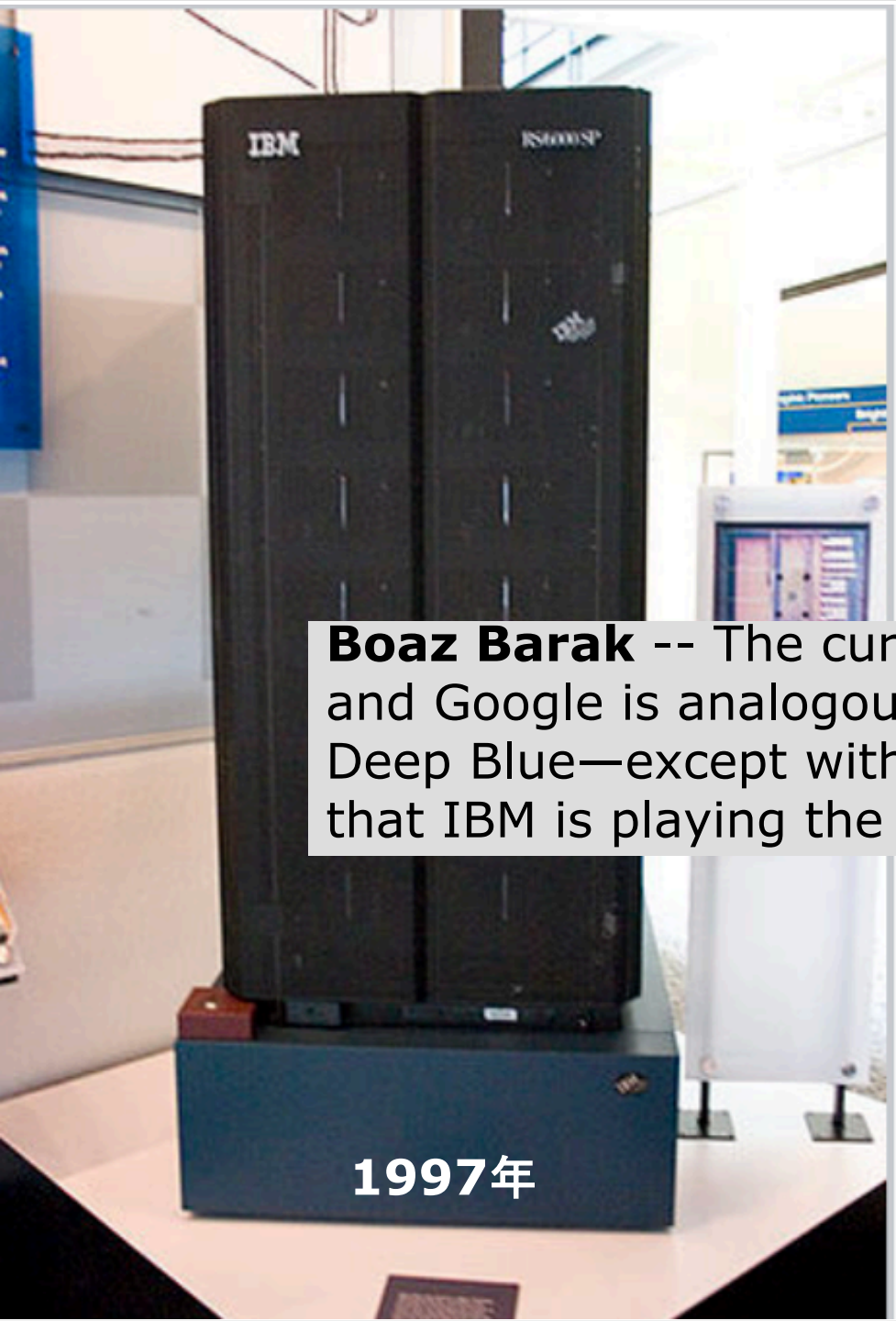

Sputnik 1
1957/10/04

Apollo 11
1969/07/20



Quantum supremacy would not be a milestone like the moon landing


IBM
RS6000 SP
1997年



1997年

Boaz Barak -- The current contest between IBM and Google is analogous to Kasparov versus Deep Blue—except with the world-historic irony that IBM is playing the role of Kasparov!

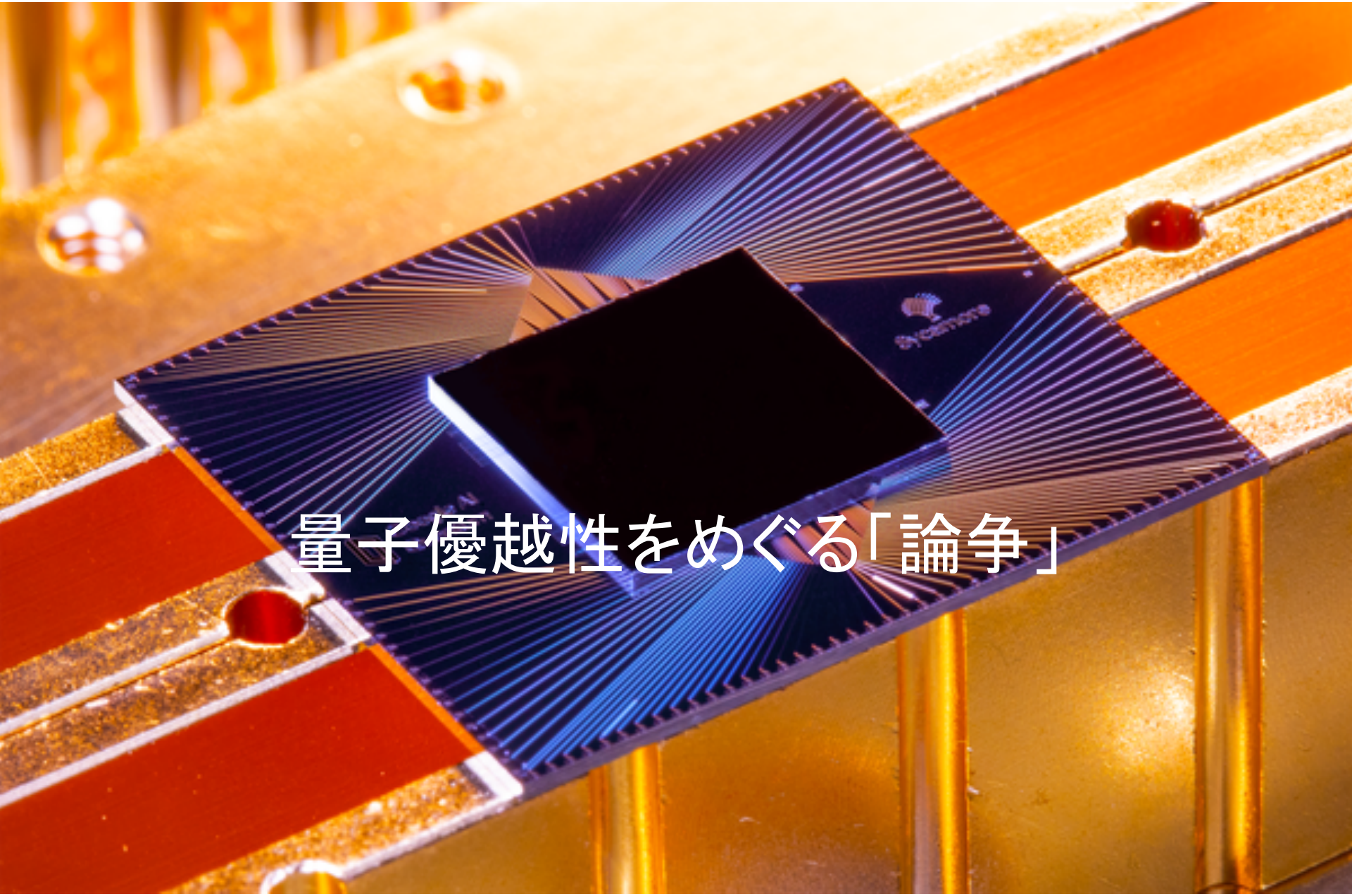
未来の量子コンピュータが
こういうイメージだとすると

今回の実験成功は
こういうイメージ

今回の実験成功は
こういうイメージ

1903年

でも、この時、人間は
初めて機械で空を飛んだ！

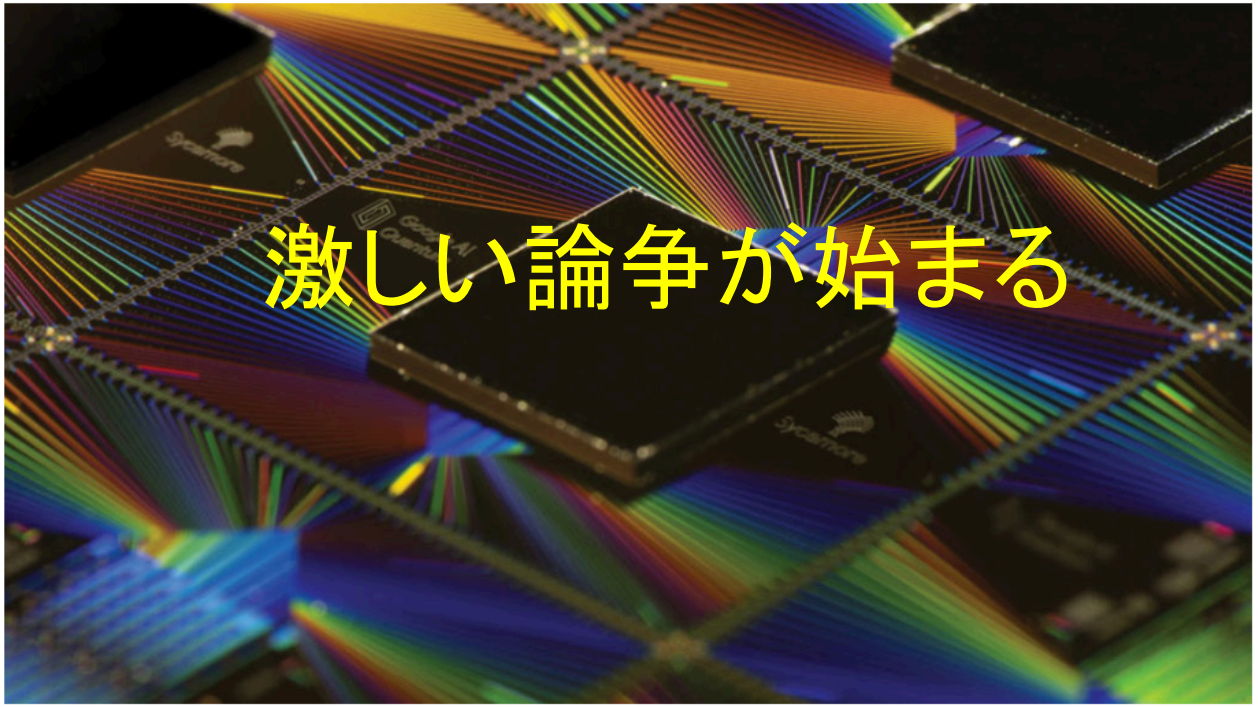

量子優越性をめぐる「論争」

ScienceNews
INDEPENDENT JOURNALISM SINCE 1921

YEAR IN REVIEW QUANTUM PHYSICS

Google claimed quantum supremacy in 2019 — and sparked controversy

Competitors questioned whether the milestone had truly been achieved



Google's quantum computer Sycamore performed a calculation that would take thousands of years with a classical supercomputer, researchers claimed in 2019. An array of quantum computer chips is shown.

GOOGLE

http://bit.ly/31MgLV6

「論争」の起点

「スーパーコンピューターを使えば、10,000万年ではなく、2.5日でシミレートできる。」（10/22 IBM論文）が、論争の起点だと考えている人は多いかもしれない。

ただ、それ以降の「論争」の進行を見れば、そうではないと僕は感じている。 10/22 IBM論文は、技術的な論文で、しかも正しい内容を含んでいたと思う。

論争をミスリードしたのは、10/22 IBM論文に、別の解釈を与えた 10/21 IBM Research Blog であると思う。

以下、10/21 IBM Research Blogの問題点を見る前に、量子優越性の提唱者であるプレスキルが、この間どのような発言をしているかを見ておこう。

私はなぜそれを
量子優越性と呼んだのか？

Why I Called It ‘Quantum Supremacy’

Preskill **2019/10/02**

https://www.quantamagazine.org/john-preskill-explains-quantum-supremacy-20191002/

なぜ、この言葉を提案したか？

- 私は、この新しい言葉で、現在が我々の惑星の歴史の中で、特別の時期だと言うことを強調したかったのだ。すなわち、現在は、量子物理学の原理に基づく情報技術が登場し隆盛になる時期なのだと。
- 他の言葉の可能性も考えたのだけど、それらは退けて、私が伝えたいポイントをもっとも捉えている言葉として、この言葉に決めた。
- この言葉の代わりの一つは、今でも広く使われている「量子アドバンテージ」なのだが、それは、私には「優越性」の持つパンチが欠けている。競馬で、鼻の差で勝っても、それはアドバンテージだ。
- それとは対照的に、ある計算について、量子コンピュータのスピードは、古典コンピュータのスピードを、遥かに超えている。少なくとも、原理的には、それが正しいのだ。

反対論と擁護論

- 「量子優越性」という言葉は、その概念が問題ではないにしても、2つの理由で議論の余地があることが明らかになった。一つは、「白人の優越性」という言葉との連想を通じて、忌まわしい政治的スタンスを呼び起こすということである。もう一つの理由は、この言葉が、量子テクノロジーの状況に関する既に誇張された報道をさらに悪化させるということである。
- 第二の反対論は、予期していたものであったが、第一の反対論は予見することができなかった。
- いずれにしろ、この言葉は人の心を捉え、GoogleのAI量子チームは、特別の熱意を持ってこの言葉を擁護してきた。

Googleの実験について

- 最近のGoogleの論文は、それが正しいものなら、それは実験物理学における驚くべき成果であり、量子コンピューティングハードウェアの急速な進歩のあかしである。関係者全員に心からのお祝いを申し上げたい。
- 実験結果自体は、意味のある情報を持たないにしても、しかしながら、このデモが示したことは、依然として重要である。量子コンピューターの出力が従来のスーパーコンピューターの出力と一致することを確認することにより（計算に数千年もかからない場合だが）、チームはデバイスを理解し、それが予想した通りに振る舞うことを確認したのだ。ハードウェアが機能していることがわかったので、さらに有用なアプリケーションの研究を開始できる。

NISQ時代の先駆けとしての Googleの実験

- Googleによって達成されたと伝えられる量子優越性のマイルストーンは、実用的な量子コンピューターの研究における極めて重要なステップである。私は、今、明けつつある時代について一つの言葉があった方がいいと 考えて、最近、NISQという言葉を作った。（riskと同じ韻を踏んでいる。）
- Googleチームは、以前は解決できなかった問題を解決する為の、十分な大きさで正確な量子マシンを構築できるようになったことを明らかにした。それは、先駆けとして、NISQ時代の始まりを告げるものだ。

IBM Research Blogの二つの問題

On “Quantum Supremacy”
IBM Research Blog, **2019/10/21**
https://www.ibm.com/blogs/research/2019/10/on-quantum-supremacy/

IBM Research Blogの二つの問題

- 10月21日に発表された IBM Research Blogは、大きく言うと二つの問題がある。
- 第一の問題は、Googleの実験は、「量子優越性を示したものではない」と断じたことである。それは、量子優越性についての初歩的な誤解によるものである。
- 第二の問題は、「量子優越性」という「言葉」を使わないようにしようとよびかけていることである。それを突き詰めれば、「言葉」だけでなく、その「概念」そのものを否定することになるだろう。

- 以下、それを見ていこう。

Googleの実験は、「量子優越性」の条件を満たさない

- IBM Research Blogは、次のように語る。
  「なぜなら、2012年にジョン・プレスキルが提案した「量子優越性」という用語の本来の意味は、量子コンピューターが古典的なコンピューターではできないことを実行できる点を説明することであったのだから、この条件は満たされていない。」

- 要するに、スーパーコンピュータSummitを使えば、Googleの実験は、2.5日でシミレートできるのだから、それは、古典コンピュータで出来ないことではない。だから、Googleの実験は、「量子優越性」の閾値を超えたとは言えないということだ。
- ただ、ここには、知ってか知らずか、量子優越性の「本来の意味」の大きなすり替えがある。原文で比較してみよう。

両者の文章を比較する

- **IBM Research Blog:**
  Because the original meaning of the term "quantum supremacy," as proposed by John Preskill in 2012, was to describe the point where quantum computers can do things that classical computers can't, this threshold has not been met.

- **Preskill:**
  Classical systems cannot in general simulate quantum systems efficiently.

両者の文章を比較する

- **IBM Research Blog:**
  Because the original meaning of the term "quantum supremacy," as proposed by John Preskill in 2012, was to describe the point where quantum computers can do things that **classical computers can't**, this threshold has not been met.

- **Preskill:**
  Classical systems **cannot** in general simulate quantum systems **efficiently**.

‘efficiently’ は、重要な概念である

- 量子優越性の概念は、IBM Research Blogが言うように「古典コンピュータで出来ないこと」と「量子コンピュータで出来ること」を対比したものではない。
- 量子優越性の概念は、「古典コンピュータでは、効率的には(‘efficiently’)出来ないこと」と「量子コンピュータで出来ること」を比較したものである。
- 「古典コンピュータで2.5日で計算できた」としても、その同じ計算が「量子コンピュータで3分で計算できる」なら、古典コンピュータは、量子コンピュータより、効率的に計算できないとみなすことができるのである。
- 量子複雑性の概念で、計算の効率性は、とても重要な概念なのである。’efficiently ‘を、量子優越性の定義から取り去ってしまえば、「古典コンピュータで不可能なこと」を証明しない限り、どうやっても、量子優越性の概念は成立しないことになる。

量子優越性概念が含意するもの

- 計算複雑性の議論では、理論的には、計算が「効率的か否か」の境界は、その計算が「多項式時間」で計算可能か、それとも「指数関数的時間」を要するかで判断される。'efficiently'には明確な理論的意味があるのだ。
- だから、量子優越性と言う概念は、'efficiently' を考慮に入れれば、「古典コンピュータでは多項式時間では計算できず指数関数的時間を要するが、量子コンピュータでは多項式時間で解ける問題がある」ということと等しいことになる。これは、今回の実験のとても重要な含意である。

- このBlogの作者は、優越性の概念について、基本的なところで、大きな誤解をしている。

量子優越性という言葉を使わないように呼びかける

- このBlogのもう一つの問題は、量子優越性という言葉を使わないように呼びかけていることである。なぜか？
- Blogは、先に紹介したプレスキルの「私はなぜそれを量子優越性と呼んだのか？」の投稿を、あたかも、プレスキル自身が、この用語に対する反対論を支持しているかのように引用する。「この言葉が、量子テクノロジーの状況に関する既に誇張された報道をさらに悪化させる」「「白人の優越性」という言葉との連想を通じて、忌まわしい政治的スタンスを呼び起こす」
- プレスキルが、こうした意見について語っているのは、「第一の反対論は、予期していたものであったが、第二の反対論は予見することができなかった。」ということだけである。（引用の順序が、Blogではなぜか前後している）

プレスキルを引用し、プレスキルと反対のことを主張する

- プレスキルの投稿は、量子優越性という言葉に反対する主張があることを認め、それを紹介しつつも、自分が作り出したこの言葉が不適切であるということなど、少しも認めてはいない。
- それどころか、プレスキルは、量子優越性という言葉を熱心に擁護したGoogleのグループが、この概念を実証したことを、新しい時代の先駆けとして高く評価しているのである。
- このBlogの立場は、Googleの実験の意義を認めず、量子優越性という言葉にも反対するものである。それはそれでいい。それなら、プレスキルの引用で、量子優越性への批判を「権威づける」必要は全くないはずである。プレスキルを引用し、プレスキルと反対のことを主張するより、プレスキルの投稿を批判するほうが、よほど筋が通っている。

量子優越性という言葉を使わない、第三の理由

- Blogは、プレスキルも認めているかのように装って導入された先の二つの理由に加えて、量子優越性という言葉を使わない第三の理由をあげる。それは次のような驚くべき理由だ。
- 「優越性という言葉は、ほとんどすべての人に誤解されている（その言葉を、適切なコンテキストのもとで使用できる、量子コンピューティングの専門家の高尚な世界の外側では）」
- まず指摘したいのは、先に見たように、このBlogの作者自身が、量子優越性について基本的なところで大きな誤解をしていることである。これは深刻な問題かもしれない。IBMのようなところで、なぜ、こんなことが起きるのか、僕には理解できない。
- 専門家の外部で、ほとんどすべての人が誤解しているのなら、必要なことは、誤解を解くことだ。名前を変えたからといって、誤解がなくなるわけではない。それは誤解から目を逸らすだけだ。

原文を引用しておこう。黄色の部分は、科学者の文章ではないと思う。

- Both are sensible objections. And we would further add that the "supremacy" term is being misunderstood by nearly all (outside of the rarified world of quantum computing experts that can put it in the appropriate context). A headline that includes some variation of "Quantum Supremacy Achieved" is almost irresistible to print, but it will inevitably mislead the general public. First because, as we argue above, by its strictest definition the goal has not been met. But more fundamentally, because quantum computers will never reign "supreme" over classical computers, but will rather work in concert with them, since each have their unique strengths.

- For the reasons stated above, and since we already have ample evidence that the term “quantum supremacy” is being broadly misinterpreted and causing ever growing amounts of confusion, we urge the community to treat claims that, for the first time, a quantum computer did something that a classical computer cannot with a large dose of skepticism due to the complicated nature of benchmarking an appropriate metric.

優越性は人種差別主義者のもの
量子アドバンテージを使おう

Supremacy is for racists—use ‘quantum advantage’’

Natureへの投稿, **2019/12/10**

https://www.nature.com/articles/d41586-019-03781-0

- 2019年12月10日付のNature誌に、” Supremacy is for racists—use ‘quantum advantage’ “という論文が投稿された。一週間後に、論文のタイトルは、” Instead of ‘supremacy’ use ‘quantum advantage’”に変更された。内容は、次のようなものである。

- コミュニティは、量子優位性は特定の意味を持つ専門用語であると主張しています。ただし、この記述の技術的な正当性は、過去数か月間のメディアの激しい報道の後、公共の場に入ると圧倒される可能性があります。

- 私たちの見解では、「優越性」という言葉は、「白人至上主義」との連想を通じて、暴力、新植民地主義、人種差別と響き合うところがあります。本質的に暴力的な言葉が、他の科学分野にも浸透しています。たとえば、人間やロボットの宇宙飛行の分野では、「征服」、「植民地化」、「開拓」などの用語は、入植者の植民地主義的な「無主の地」の主張を呼び起こします。それらの言葉は、進行中の新植民地主義の問題に対抗して文脈化する必要があります。

- **Carmen Palacios-Berraquero,** Nu Quantum, Cavendish Laboratory, Cambridge, UK.
- **Leonie Mueck** Riverlane, Cambridge, UK.
- **Divya M. Persaud** University College London, UK.

- Syed Mustafa Ali Open University, Milton Keynes, UK.
- Steve Brierley Riverlane, Cambridge, UK.
- Hope Bretscher Cavendish Laboratory, University of Cambridge, UK.
- Juani Bermejo-Vega University of Granada, Spain.
- Helmut G. Katzgraber Microsoft, Redmond, Washington, USA.
- Chris Granade Microsoft, Redmond, Washington, USA.
- Alan Aspuru-Guzik University of Toronto, Canada.
- Sabine Wollmann University of Bristol, UK.
- Dominic Horsman Université Grenoble Alpes, France.
- Anne Broadbent University of Ottawa, Canada.
- Ariel Bendersky University of Buenos Aires, Argentina.
- Cecilia Cormick National University of Córdoba, Argentina.
- Shazeaa Nisa Ishmael University of Oxford, UK.

ダボス会議でのIBM 量子パネル

From shtetl to Forum

Scott Aaronson, **2020/01/23**

https://www.scottaaronson.com/blog/?p=4536

1月23日にダボス会議の中で行われたIBM主催の量子コンピューティングのパネル・ディスカッションの様子を、聴衆として参加したスコット・アーロンソンが、ブログで書いている.

パネル冒頭、IBM CEOのジニ・ロメッティの発言
“things you can do in two seconds that are not commercially valid”

- 「量子技術は、サプライ・チェインやその他の最適化問題の高速化で世界を変えるでしょう。IBMは、顧客にその価値を伝えることにコミットしています。それは、商業的には妥当な意味のない、2秒かそこらでできるようなものではありません。」

- 前半の発言は、量子技術が世界に与えるインパクトについて、適切なものだとは、僕は思わなかった。後半の発言は、明らかに、「量子優越性を実験的に明らかにした」という昨年のGoogleの発表を、「そんな役に立たないものに意味があるの？」とあてこすったものだ。（もっとも、Googleの実験は、2秒じゃなく200秒かかったのだけど）

「量子コンピューティングの科学的背景については、全く何も知らないという人、手をあげて。」

- 彼女は100人近くの聴衆に問う。「この中で、量子コンピューティングの科学的背景については、全く何も知らないという人、手をあげて。」ほとんどの人が手を挙げたようだ。そして、「みなさん、全員そうですよね！」と冗談を言う。

- 「優越性という言葉は、ほとんどすべての人に誤解されている（その言葉を、適切なコンテキストのもとで使用できる、量子コンピューティングの専門家の高尚な世界の外側では）」と、IBM Research Blogは言うのだが、それでいいのかと僕は思う。

IBMのSenior Vice President Arvind Krishnaの発言

- 「我々は、量子優越性と言う概念を、全面的に拒否する。なぜなら、それは的外れの興味本位のものだからである。サプライ・チェーンの最適化のような市場の顧客にとっての価値を創造することこそが、この問題にとって重要な唯一のテストなのである。」

  IBM rejects the entire concept of “quantum supremacy”: because it’s an irrelevant curiosity. and creating value for customers in the marketplace (for example by solving their supply-chain optimization problems) is the only test that matters.

IBMのSenior Vice President Arvind Krishnaの発言

- Later, Krishna explained why quantum computers will never replace classical computers: because if you stored your bank balance on a quantum computer, one day you'd have $1, the next day $1000, the day after that $1 again, and so forth! He explained how, where current supercomputers use the same amount of energy needed to power all of Davos to train machine learning models, quantum computers would use less than the energy needed to power a single house. New algorithms do need to be designed to run neural networks quantumly, but fortunately that's all being done as we speak.

- こうしたIBM経営幹部の見通しは、先に見たプレスキルのNISQ論文での見通しとは、大きく異なるものである。
  あらためて、それを確認しておこう。

量子技術の商業的可能性について

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。

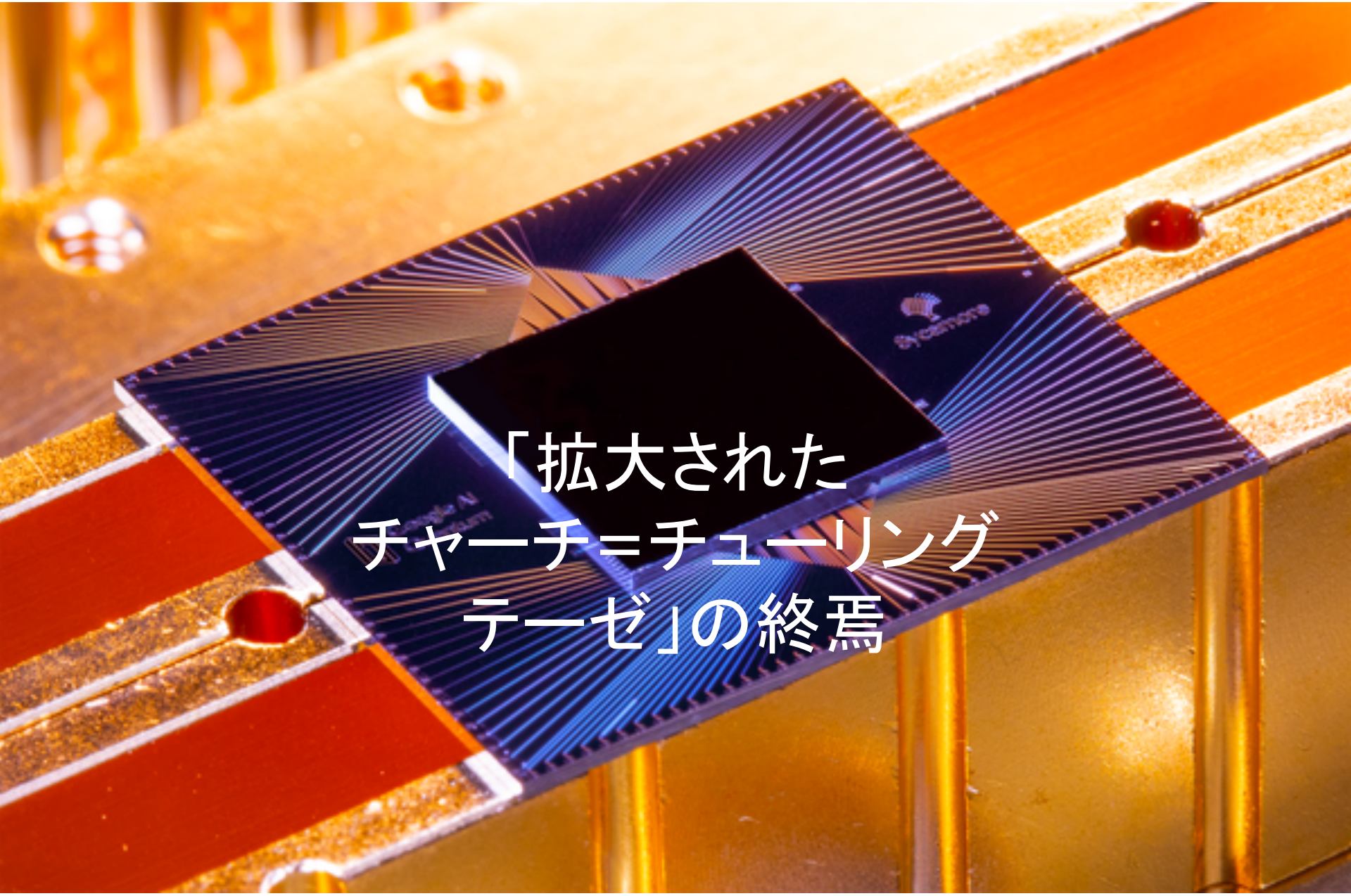
我々の到達点

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ィジタル・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。

現在のコンピュータでは
自然のシミュレートはできない

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。


「拡大された
チャーチ＝チューリング
テーゼ」の終焉

「計算可能性理論」が、大きな転機を迎えるのは、1980年代に入ってからだ。

ファインマンが、コンピュータでは量子力学の法則に従う自然のシミュレートができないことに気づく。彼は、自然のシミュレートが可能なコンピュータは、量子力学の法則に従ったコンピュータでなければならないと主張する。

この指摘が、「量子コンピュータ」研究の始まりである。

数学的体系と同様に、自然もまた、我々の認識の対象である。数学だけでなく、物理学もまた、我々の認識の可能性と限界について、強い関心を持っているのだ。

ドイッチェは、ファインマンの考えを受けて、チューリングマシンの量子版を構成し、こうした量子チューリング・マシンで計算可能なものが計算可能であるとする。これを、計算可能性についての「チャーチ＝チューリング＝ドイッチェのテーゼ」という。

一見すると、同じような定式化に思えるのだが、本質的な違いがあるのだ。

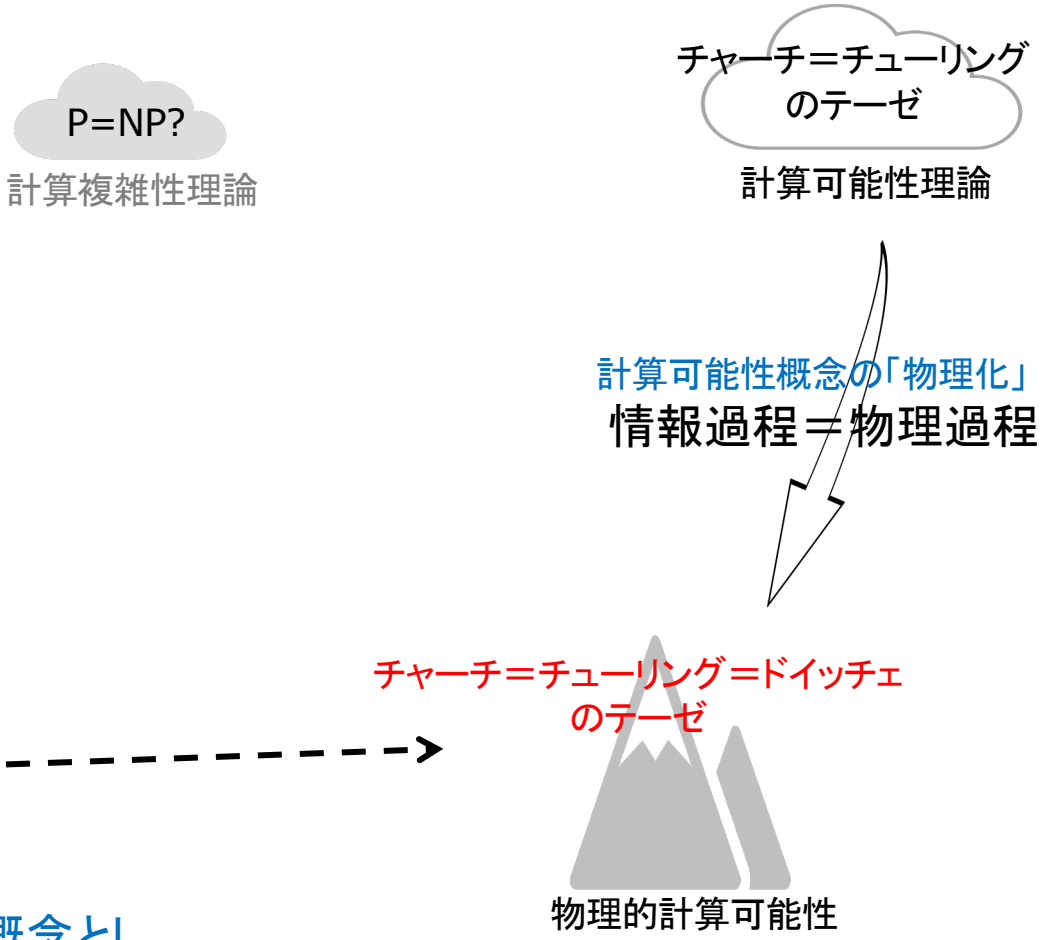
「チャーチ＝チューリングのテーゼ」は、抽象的・形式的・数学的な「計算可能性」の定義についての提言なのだが、「チャーチ＝チューリング＝ドイッチェのテーゼ」は、「計算可能性」が、実在的・物理的に定義されねばならないと主張しているのだ。

「チャーチ＝チューリングのテーゼ」は、いわば、遠くの雲の上に抽象的に存在する原理だったのだが、「チャーチ＝チューリング＝ドイッチェのテーゼ」は、地上に降りた現実の物理的原理だ。

重要なことは、こうした「計算可能性」概念の「物理化」の背景にある思想である。それは、情報過程が、けっして抽象的なものではなく、物理的なものに支えられた物理過程に他ならないという考えである。

ただ、80年代は、まだ、量子コンピュータは概念としてしか存在していなかった。「計算可能性」の物理化という画期的な変化も、まだまだ、抽象的な議論だった。

80年代



80年代は、まだ、量子コンピュータは概念としてしか存在していなかった。「計算可能性」の物理化という画期的な変化も、まだまだ、抽象的な議論だった。

Feynman

"Simulating Physics with Computers”
1982年

https://goo.gl/ueVbdp

「計算可能性」の理論として出発した「複雑性理論」が、質的な深化を果たすのは、1980年代になってからである。

大きな転回点になったのは、1982年のファインマンの論文 "Simulating Physics with Computers" https://goo.gl/ueVbdp である。

この論文は、複雑性理論の進化の重要な画期を与えるとともに、現在の量子コンピュータのアイデアの出発点ともなる重要な論文である。（同時に、現在の量子コンピュータ技術の到達点は、ある意味、この論文への「回帰」として特徴付けられるのは、興味ふかいことである。

ファインマンは、次のように述べる。

「コンピューターが、正確に自然と同じように振る舞う、正確なシミュレーションが存在する可能性について話そうと思う。」

「それが証明されて、そのコンピュータのタイプが先に説明したようなものであるなら、必然的に、有限の大きさの時空の中で起きる全てのものは、有限な数の論理的な操作で正確に分析可能でなければならないことになるだろう。」

「量子論的なシステムは、古典的な万能計算機で、確率論的にシミュレートされるだろうか？」

「 別の言い方をすれば、コンピューターは、量子論的なシステムが行うのと、同じ確率を与えるだろうか？　コンピューターを今まで述べてきたような古典的なものだとすれば（前節で述べたような量子論的なものではないとすれば）、また法則はすべて変更されないままで、ごまかしもないとすれば、答えは明らかにノーである。」

「それは、新しいタイプのコンピューター、量子コンピューターで可能になるだろう。」

「 私が理解する限りでは、それは量子論的なシステムによって、量子コンピューターの要素によって、シミュレート出来るようになることは、いまや、明らかになった。それはチューリング・マシンではない。別のタイプのマシンである。」

Deutsch

"Quantum theory, the Church-Turing principle and the universal quantum computer"

1985年

https://goo.gl/PVHGKa

ファインマンの「量子コンピュータによる自然のシミュレーション」という刺激的な問題提起を受け、それを「計算可能性理論」の中心的な原理である「チャーチ＝チューリングのテーゼ」との関連で整理しなおして「計算可能性」を再定式化したのは、ドイッチェである。

1985年の論文 "Quantum theory, the Church-Turing principle and the universal quantum computer" https://goo.gl/PVHGKa で、ドイッチェは、「チューリング・マシンのクラスの量子論的一般化である計算機械のクラス」＝「万能量子コンピュータ」を構成して見せる。

彼は、「チャーチ＝チューリングのテーゼ」を次のように捉える。

『「計算可能と自然に見なされる関数」は、全て、万能テューリング・マシンで計算可能である。.』

ただ、彼は、この「チャーチ＝チューリングのテーゼ」の基礎には、暗黙の物理学的主張がある」という。これが、この論文の眼目である。

彼は、彼が構成して見せた「万能量子チューリング・マシン」＝「万能計算機械」を用いて、「チャーチ＝チューリングのテーゼ」を書き換える。

チャーチ＝チューリング＝ドイッチェのテーゼ

「この物理学的主張は、次のような物理学的原理として、明確に表現することが出来る。」

『有限な方法で実現可能な物理システムは、有限な手段によって操作される万能計算機械のモデルで完全にシミュレート可能である。』

これを、「チャーチ＝チューリング＝ドイッチェのテーゼ」という。

ドイッチェは、論文で、これらの原理が、次の熱力学の第三法則に似ていること注意を向けているのは、興味ふかい。

『どのような有限のプロセスも、有限な手段実現可能な物理システムのエントロピーあるいは温度をゼロにはできない。』

形式的・数学的で抽象的な「計算可能性」の原理だった「チャーチ＝チューリングのテーゼ」は、ここに「チャーチ＝チューリング＝ドイッチェのテーゼ」として、実在的な過程としての「計算」の原理として「物理化」されることになる。

「計算可能性」の原理の「物理化」は、関連する諸科学に、一つのインパクトをもたらすことになる。なぜなら、それは、それまで別々の学問の対象だった「計算過程」「物理過程」「情報過程」（それぞれ、数学・物理学・コンピュータ科学が扱っていた）に対して、「計算過程」＝「物理過程」＝「情報過程」という、強力な三位一体の図式が、しかも、物理学の優位の元に生まれたことを意味することになるからである。

こうした動きのすぐれた解説は、彼の死後に発刊されたファインマンの最後の著作である "Feynman Lectures on Computation" https://goo.gl/PyqgyT の第5章 "Reversible Computation and the Thermodynamics of Computing" と第6章 "Quantum Mechanical Computers" をみるのがいい。30年前のものだが、少しも古くない。

ただ、「チャーチ＝チューリング＝ドイッチェのテーゼ」は、その認識論的意味を考えると、本当は、なかなか手強いものだ。その辺の議論は、あとで振り返ることがあると思うが、ニールセンの次の投稿を見て欲しい。"Interesting problems: The Church-Turing-Deutsch Principle" https://goo.gl/Q6EiYi

BQP
Bernstein と Vazirani

“Quantum Complexity Theory”
1993年

https://goo.gl/3y4RSf

Just as the theory of computability had its foundations in the Church-Turing thesis, computational complexity theory rests upon a modern strengthening of this thesis, which asserts that, any "reasonable" model of computation can be efficiently simulated on a probabilistic Turing Machine (an efficient, simulation is one whose running time is bounded by some polynomial in the running time of the simulated machine). For example, computers that can operate on arbitrary length words in unit, time, or that can exactly compute with infinite precision real numbers are unreasonable models - since it seems clear that they cannot be physically implemented. It had been argued that the Turing Machine model (or the polynomial time equivalent cellular automaton model) is the inevitable choice once we assume that we can implement only finite precision computational primitives. Given the widespread belief that NP ≠ BPP, this would seem to put a wide range of important, computational problems (the NP-hard problems) well beyond the capability of computers.

However, the Turing Machine is an inadequate model for all physically realizable computing devices for a. fundamental reason: the Turing Machine is based on a classical physics model of the Universe. whereas current physical theory asserts that, the Universe is quantum physical. Can we get inherently new kinds of (discrete) computing devices based on quantum physics?

The first indication that such a. device might potentially be more powerful than a probabilistic Turing Machine appeared in a paper by Feymnan [Fe82] about a decade ago. In that paper, Feynman pointed out a very curious problem: it, appears to be impossible to simulate a general quantum physical system on a probabilistic TM without an exponential slowdown. The difficulty with the simulation has nothing to do with the problem of simulating a continuous system with a. discrete one - we may assume that, the quantum physical system to be simulated is discrete, some kind of a quantum cellular automaton. In view of Feynman's observation, we must reexamine the foundations of computational complexity theory, and the complexity-theoretic form of the Church-Turing thesis, and study the computational power of computing devices based on quantum physics.

In this paper, we prove the existence of a universal quatum Turing Machine whose simulation overhead is polynomially bounded. In full generality, on any given input a quantum TM produces a random sample from a probability distribution. We say that quantum TM T' simulates T with accuracy c, if on every input z, T' outputs a sample from a distribution which is within total variation distance c of the corresponding distribution for T. We prove that there is a universal quantum TM, which takes as input the description of a quantum TM T. time t, and input, z, and simulates T(x) for time t with accuracy ϵ. The slowdown is polynomial in t and $1/\epsilon$.

In this paper, we present, the first evidence that, quantum TMs might, be more powerful than classical probabilistic TMs. We prove that there is an oracle relative to which there is a language that can be accepted in polynomial time by a quantum TM but cannot be accepted in $n^{O(\log n)}$ time by a bounded-error classical probabilistic TM. A more careful construction exhibits an oracle relative to which quantum polynomial time is not even contained in the class Arthur-Merlin where the verifier has $n^{O(\log n)}$ time (see [BMW] for a definition of this class).

BQP

Let BQP (bounded-error quantum polynomial time) be the class of languages that are accepted by a polynomial time quantum TM with error probability at most 1/3. It is not hard to show that, BQP $\subseteq$ PSPAC'E. Therefore, we cannot, hope to prove that BPP $\subset$ BQP without resolving the longstanding open question BPP $\neq$? PSPACE. In fact, Valiant [Va92] recently pointedout to us that, the above result can be strengthened to say that BQP $\subseteq$ #P.

Controlling Error

- In the early days of quantum computing (the ’80s, say), skeptics said quantum computation was ‘just’ another form of analog computation (a machine manipulating real-valued quantities), and subject to the same limitation: perturbative noise that could erase information and throw off a computation by successively accumulating errors.
- This criticism ignored or glossed over an important insight (explained in Bernstein-Vazirani ’93): unlike other types of transformations used in classical analog computers, quantum operations cannot amplify error except by directly introducing more of it!

- Bernstein and Vazirani observe that the total error is (in an appropriate sense) at most the ‘sum’ of the errors in all preparation and gate components. Thus, if engineers can produce circuit elements with error 1/t we expect to be able to faithfully execute computations on quantum circuits with size on the order of t.

Threshold Theorem

- This idea was improved upon substantially. In a sequence of papers, work by Aharanov, Ben-Or, Knill, Laflange, Zurek and others culminated in the 1996 'Threshold Theorem', which showed how to use 'hierarchical coding' ideas to build quantum circuits for arbitrary BQP computations, which would remain reliable even if each gate was subjected to a sufficiently small (but constant) rate of error. This result was analogous to (but more complicated than) earlier work by Von Neumann on fault-tolerant classical computation.

Quantum Complexity Theory

"Quantum Complexity Theory"
Bernstein & Vazirani
1997年

https://goo.gl/jdSS91

Abstract

In this paper we study quantum computation from a complexity theoretic view point. Our first result is the existence of an efficient universal quantum Turing Machine in Deutsch's model of a quantum Turing Machine. This construction is substantially more complicated than the corresponding construction for classical Turing Machines - in fact even simple primitives such as looping, branching and comp osition are not straightforward in the context of quantum Turing Machines. We establish how these familiar primitives can be implemented and also intro duce some new purely quantum mechanical primitives such as changing the computational basis and carrying out an arbitrary unitary transformation of polynomially bounded dimension.

We also consider the precision to which the transition amplitudes of a quantum Turing Machine need to be specified. We prove that O(log T) bits of precision suffce to support a T step computation. This justifes the claim that that the quantum Turing Machine model should be regarded as a discrete model of computation and not an analog one.

We give the first formal evidence that quantum Turing Machines violate the modern complexity theoretic formulation of the Church-Turing thesis.

We show the existence of a problem relative to an oracle, that can be solved in polynomial time on a quantum Turing Machine, but requires super polynomial time on a bounded error probabilistic Turing Machine and thus not in the class **BPP** .

- The class **BQP**, of languages that are efficiently decidable with small error probability on a quantum Turing Machine, satisfies: $\mathbf{BPP} \subseteq \mathbf{BQP} \subseteq \mathbf{P}^{\#\mathbf{P}}$.

Definition of BQP

- **Definition. BQP** is the class of languages L $\subset \{0,1\}^*$ for which there exists a uniform family of polynomial-size quantum circuits $\{C_n\}$ over some basis of universal gates and a polynomial q so that for all n and inputs x $\in \{0,1\}^n$
  - if x $\in$ L then $C_n(|x> |0>^{\otimes q(n)})$ accepts with probability > 2/3
  - if x $\notin$ L then $C_n(|x> |0>^{\otimes q(n)})$ accepts with probability < 1/3

Since circuits have to pre-specify the input size, so we need a circuit for each input size n. By uniform, we mean that there is a classically ecient algorithm to produce C_n given n.

- We define the class **EQP**, exact or error free quantum polynomial time, as the set of languages which are exactly accepted by some polynomial time QTM. More generally we define the class **EQTime** (T(n)) as the set of languages which are exactly accepted by some QTM whose running time on any input of length n is bounded by T(n).
- More generally, we defune the class **BQTime** (T(n)) as the set of languages which are accepted with probability 2/3 by some QTM whose running time on any input of length n is bounded by T(n).

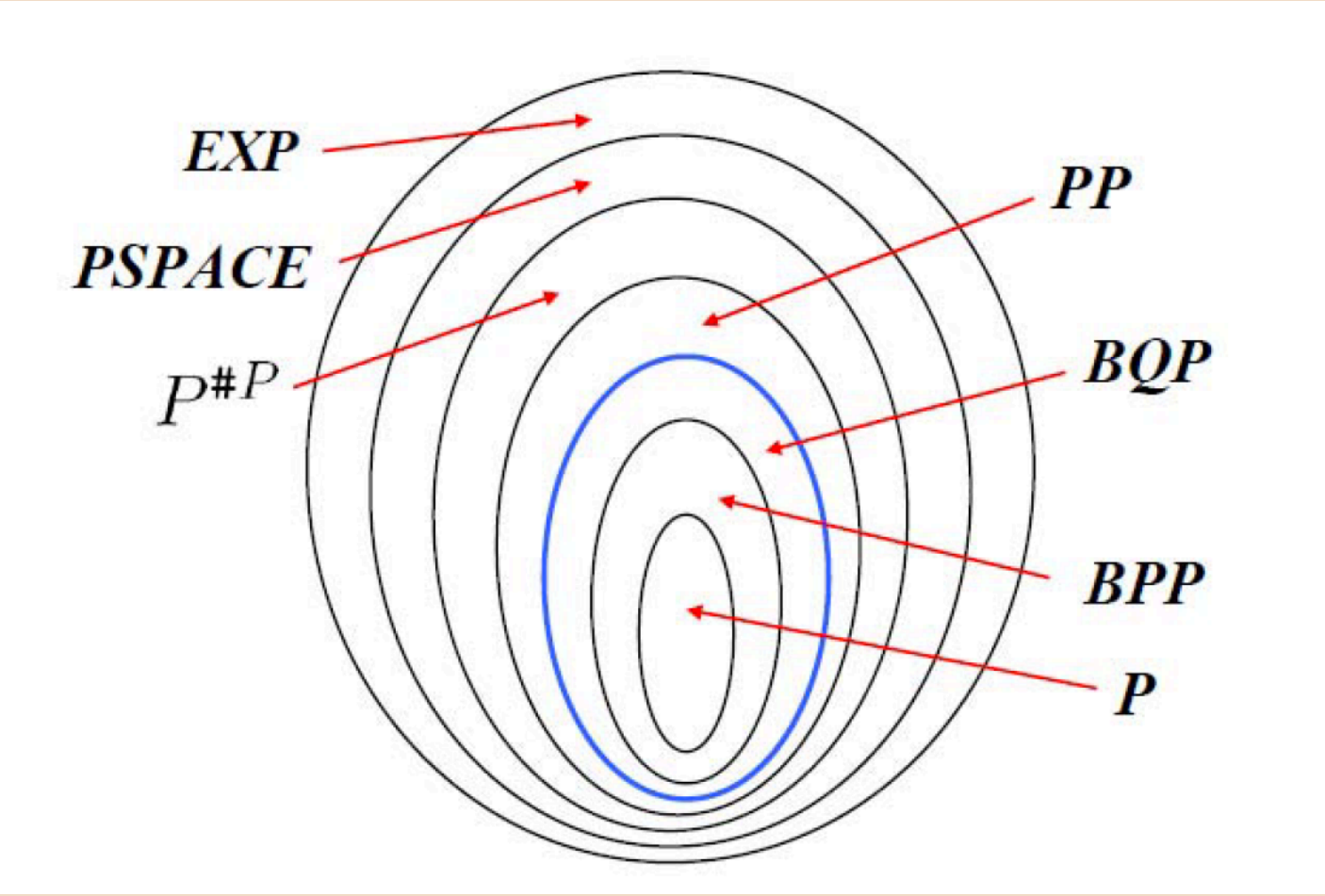
Upper and lower bounds on the power of QTMs

- Theorem 1 **P ⊆ EQP**
- Theorem 2 **BPP ⊆ BQP**
- Theorem 3 **BQP ⊆ PSPACE**
- Theorem 5 **BQP ⊆ $P^{\#P}$**

- **Fourier Sampling and the power of QTMs**

  In this section we give evidence that QTMs are more powerful than bounded error probabilistic TMs. We define the recursive Fourier sampling problem which on input the program for a boolean function takes on value 0 or 1. We show that the recursive Fourier sampling problem is in BQP.

Basic properties of BQP



Shor

“Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer”

1997年

https://goo.gl/kf4ScC

Abstract

A digital computer is generally believed to be an efficient universal computing device; that is, it is believed able to simulate any physical computing device with an increase in computation time of at most a polynomial factor. This may not be true when quantum mechanics is taken into consideration. This paper considers factoring integers and finding discrete logarithms, two problems which are generally thought to be hard on a classical computer and have been used as the basis of several proposed cryptosystems. Efficient randomized algorithms are given for these two problems on a hypothetical quantum computer. These algorithms take a number of steps polynomial in the input size, e.g., the number of digits of the integer to be factored.

1994年、ショアは驚くべき発見をする。（論文は、1997年）

量子コンピュータでは、古典的なコンピュータでは指数関数的時間を要する素因数分解が、多項式時間で解けるという発見である。

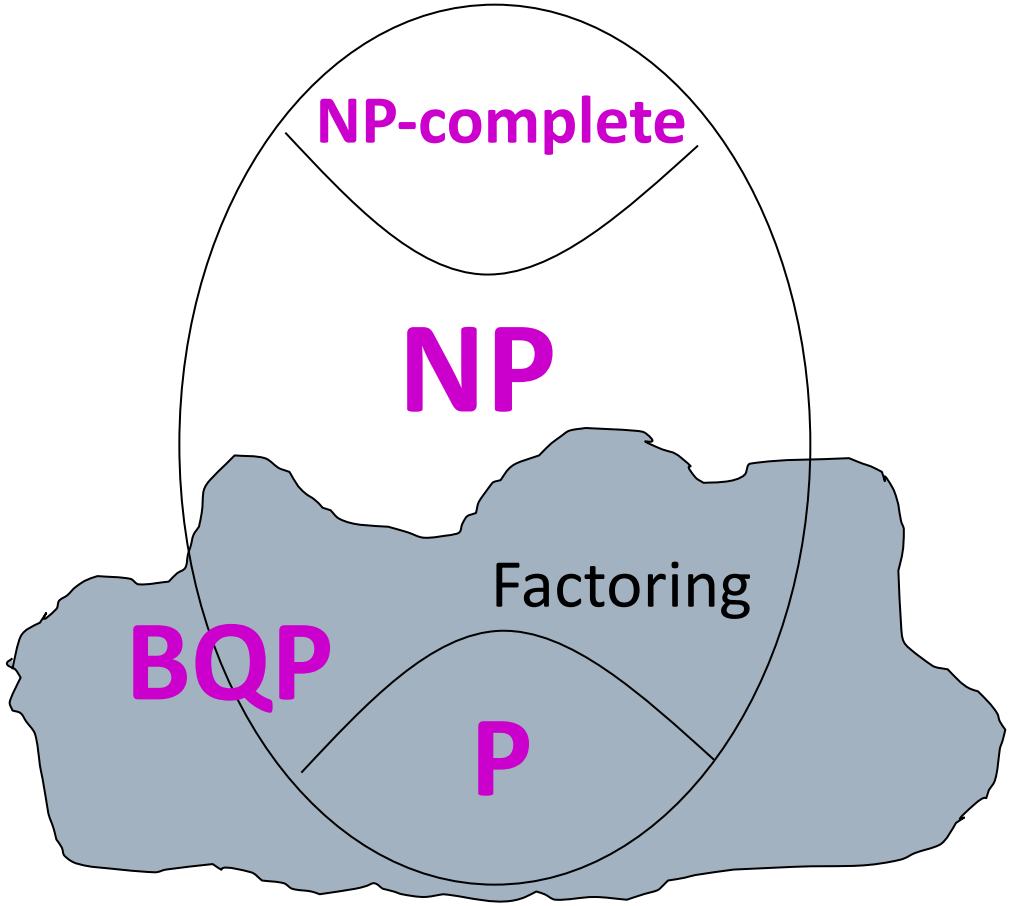
現代のセキュリティ技術の根幹部分が、RSA暗号のように素因数分解の困難性に基礎を置いている事情から、この「ショアのアルゴリズム」の発見は、コンピュータ・サイエンスの枠を超えた、社会的と言っていい大きな反響を呼び起こした。

If computers that you build are quantum,
Then spies everywhere will all want 'em.
Our codes will all fail,
And they'll read our email,
Till we get crypto that's quantum, and daunt 'em.

BQP (Bounded-Error Quantum Polynomial-Time): The class of problems solvable efficiently by [illegible] defined by Bernstein and Vazirani in 1993

Interesting

Shor 1994: Factoring integers is in **BQP**



Extended Church-Turing Thesis

“P ?= NP”

Scott Aaronson

2011年

https://goo.gl/bGwYJG

Extended Church-Turing Thesis

The time it takes to compute something on any one machine is polynomial in the time it takes on any other machine

Even before quantum computing, there were indications that the Extended Church-Turing Thesis might be on shakier ground than the original Church-Turing Thesis. For example, randomized algorithms are sometimes faster than deterministic algorithms, leading to a class called BPP(Bounded-Error Probabilistic Polynomial-Time). Obviously$P \subseteq BPP$. (Today we believe that BPP =P,but we can't prove it.)

https://goo.gl/b2Z1M9

More precisely, the Church-Turing Thesis holds that virtually any model of computation one can define will be equivalent to Turing machines, in the sense that Turing machines can simulate that model and vice versa. A modern refinement, the Extended Church-Turing Thesis, says that moreover, these simulations will incur at most a polynomial overhead in time and memory. Nowadays, most computer scientists and physicists conjecture that quantum computation provides a counterexample to the Extended Church-Turing Thesis—possibly the only counterexample that can be physically realized.

It’s also conceivable that access to a true random-number generator would let us violate the Extended Church-Turing Thesis, although most computer scientists conjecture that it doesn’t, for reasons that I’ll explain in Section 5.4.1. On the other hand, as long as we’re talking only about classical, digital, deterministic computation, the Extended Church-Turing Thesis remains on extremely solid ground.

Conjecture P = BPP

Of course, if P = BPP, then the question of whether randomized algorithms can efficiently solve NP-complete problems is just the original P ?= NP question in a different guise. Ironically, however, the "obvious" approach to proving P = BPP is to prove a strong circuit lower bound—and if we knew how to do that, perhaps we could prove P ≠ NP as well!

Conjecture $NP \not\subseteq BQP$

Naturally, there's little hope of proving Conjecture 34 at present, since any proof would imply P /= NP! We don't even know today how to prove conditional statements (analogous to what we have for BPP and P/poly): for example, that if $NP \subseteq BQP$ then PH collapses.

On the other hand, it is known that, if a fast quantum algorithm for NP-complete problems exists, then in some sense it will have to be extremely different from Shor's or any other known quantum algorithm.

Example Problems

Harder

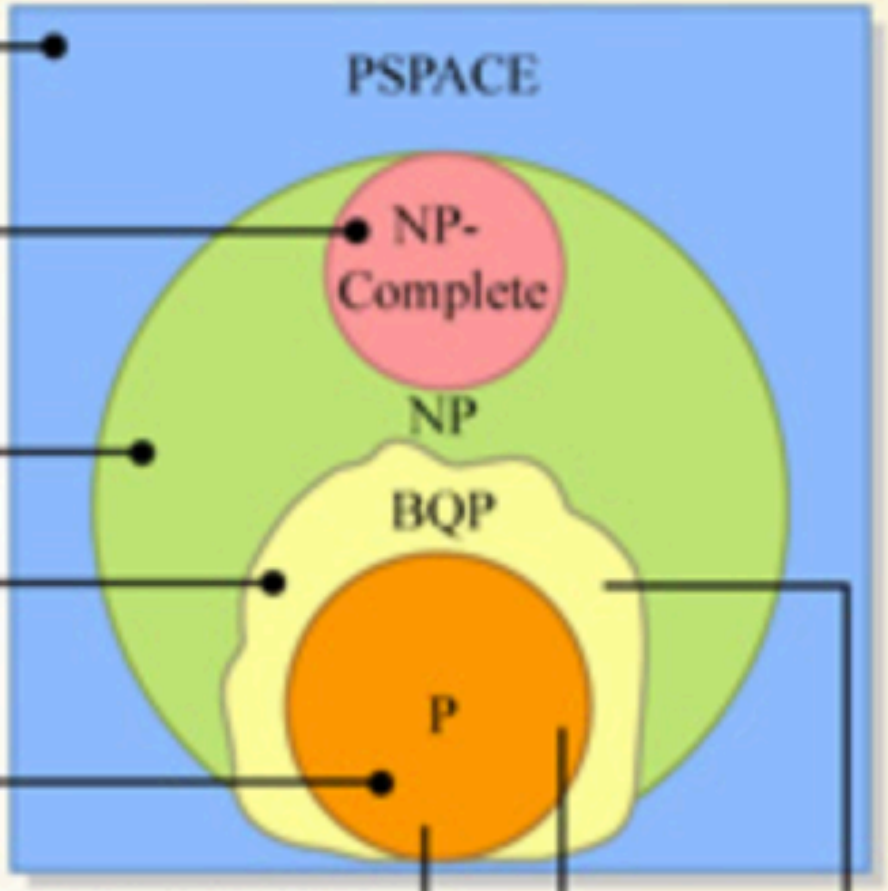
$n \times n$ chess
$n \times n$ Go

Box packing
Map coloring
Traveling salesman
$n \times n$ Sudoku

Graph isomorphism

Factoring
Discrete logarithm

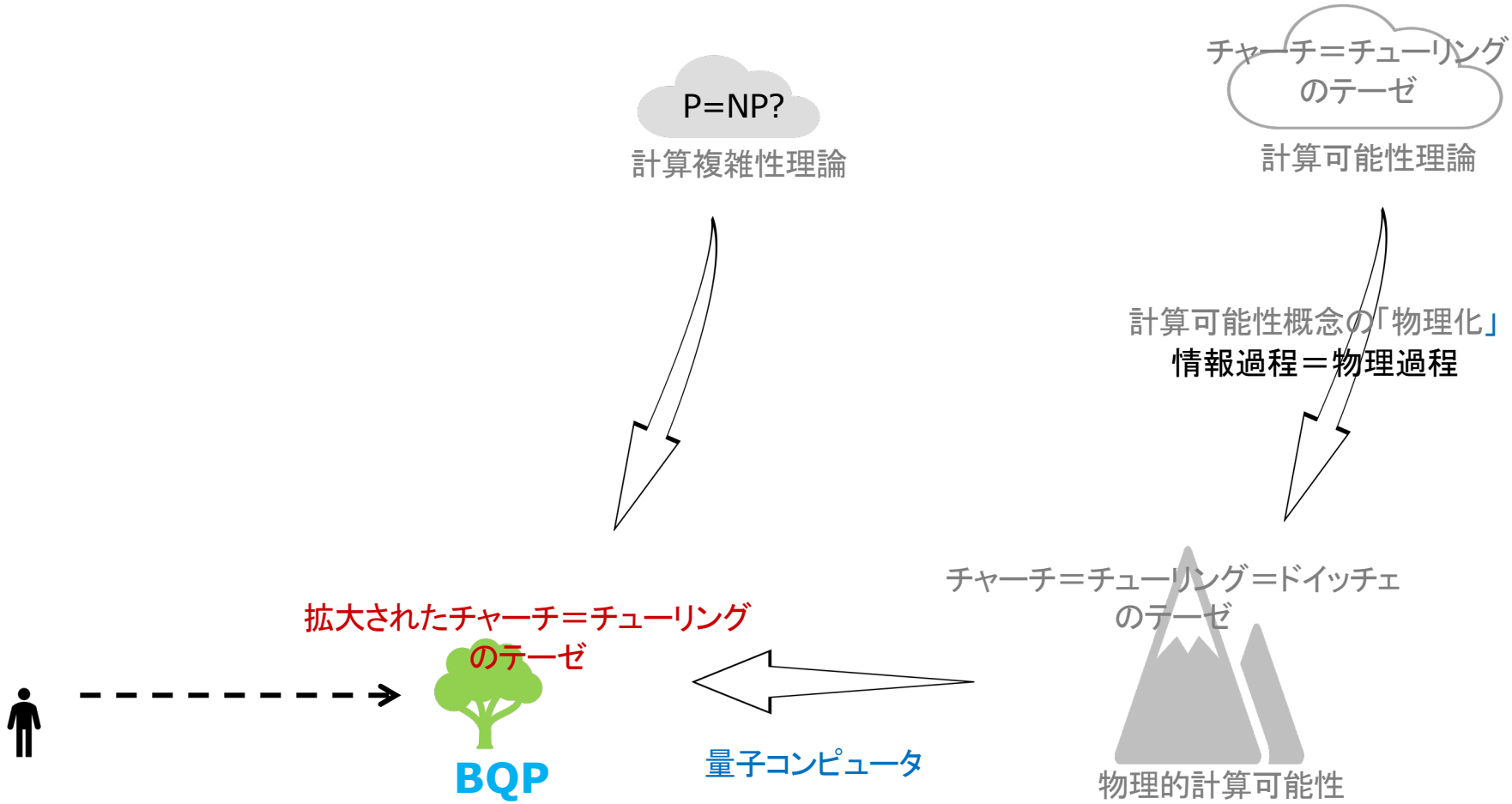
Graph connectivity
Testing if a number is a prime
Matchmaking



Efficiently solved by classical computer

Efficiently solved by quantum computer

90年代



量子複雑性の理論が登場し、BQPという新しい複雑性の概念が確立する。ショアのアルゴリズムは、広い関心をあつめた。