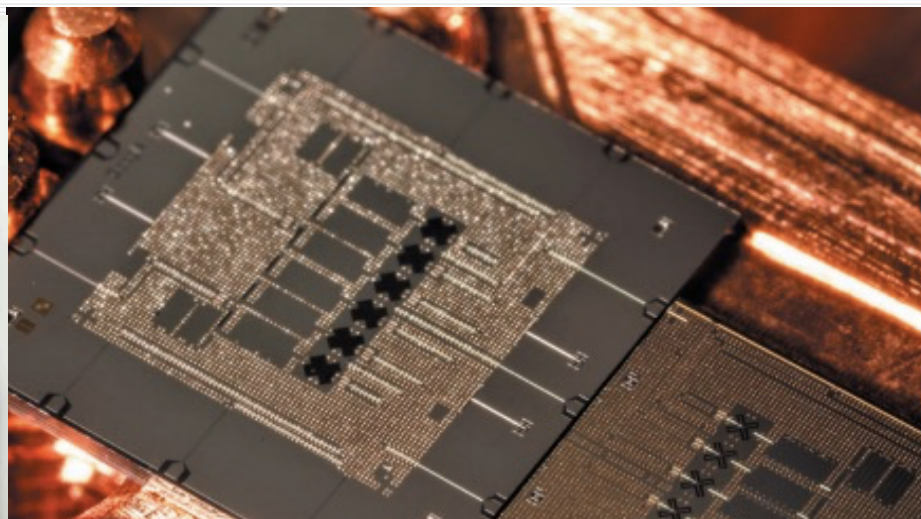
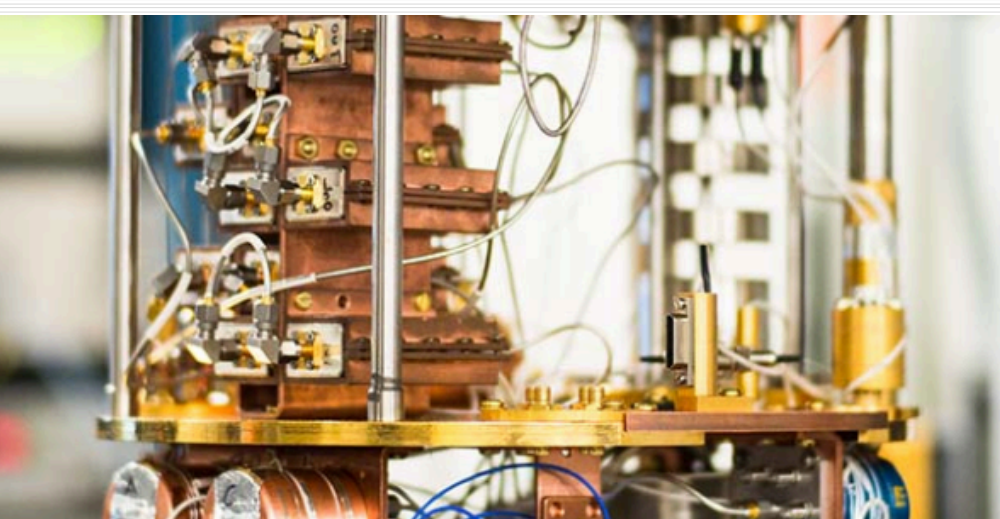
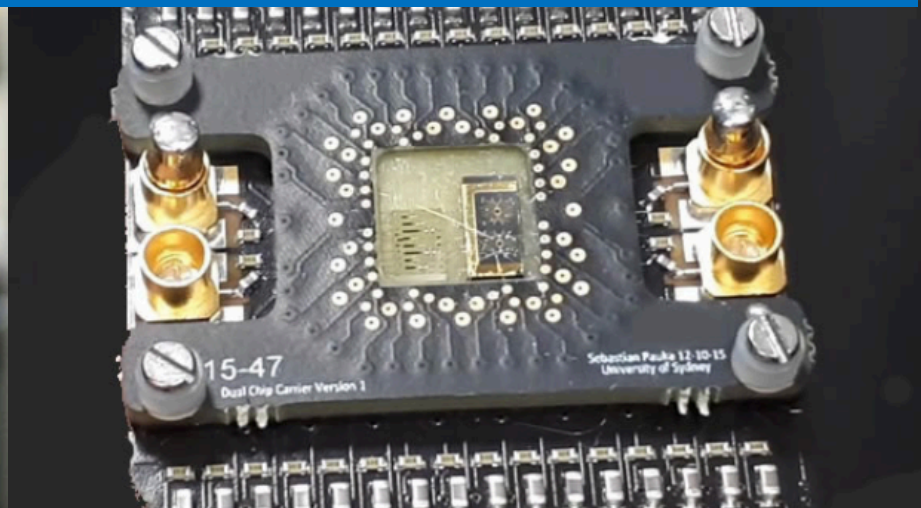
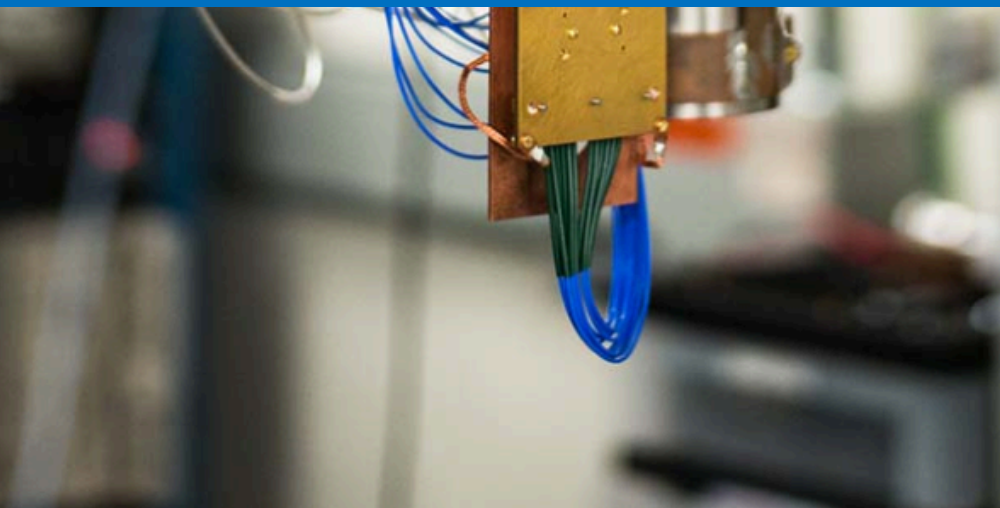




量子コンピュータとは何か？



丸山不二夫

*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.*

– Jennifer and Peter Shor

*To read our E-mail,
how mean of the spies and their quantum machine;
be comforted though, they do not yet know how to
factorize twelve or fifteen.*

– Volker Strassen

For example, factorizing a 2,000-bit number in one day, a task believed to be intractable using classical computers , would take 100 million qubits, even if individual quantum operations failed just once in every 10,000 operations. We have yet to assemble digital quantum processors with tens of qubits.

-- Google Quantum AI Team

はじめに

- 小論は、量子コンピュータとは何かについて、一般の読者を対象に、そのオーバービューを与えようとするものである。
- 量子コンピュータの世界は、今、技術的にもビジネス的にも一つの展開点を迎えようとしている。その展開点とは、技術的には、この数年以内に、50 qubit程度のシステムを安定的に構築する目処が付き始めたことであり、ビジネス的には、そうした技術的達成をきっかけに、それらを利用した量子コンピュータの具体的・現実的なビジネス利用の可能性の模索が始まっていることである。
- それらの到達点は、確かに、未だ萌芽的なものではあるのだが、こうした動きは、将来の量子コンピュータの飛躍を確実に準備していく軌道を切り開きつつある重要なものだと、僕は考えている。

はじめに

- 小論では、最初に、我々が、量子の不思議な振る舞いにどのようにして気づき、またそれをどのように理解してきたのかを紹介する。続いて、こうした量子の奇妙な性質をコンピュータに利用しようとするアイデアが、どのように発展してきたかを振り返る。
- 続く、二つの章では、「量子ゲート型」と「量子アニーリング型」という、現在の量子コンピュータの二つの基本的なアーキテクチャを取り上げる。
- 最後に、各社の現時点での取り組みの状況を紹介する。ここでは、「量子コンピュータのキラー・アプリは、素因数分解での暗号破り」というこれまでの通念が、もはや働いていないことに、留意すべきかもしれない。

はじめに

- 小論では、量子コンピュータの技術的側面を主に述べたのだが、こうした新しい技術を牽引しているのは、新しい科学的な知見である。前回のマルレクで取り上げた、「量子情報理論」は、これからますます、理論的にも実践的にも、その重要性を増していくだろう。今後も、引き続き紹介していきたいと考えている。
- 今回、マルレクでの量子コンピュータの概論と並んで、演習形式で「量子情報理論基礎演習」を開講する。こちらにも、多くの人に参加することを期待したい。
- 量子コンピュータのビジネスに参入するには、いろいろ障壁があるかもしれない。ただ、その前提として、その基礎理論を知ることには大きな障壁はない。「紙と鉛筆」があればいいだけだと思う。まず、「学ぶ」ことから、始めよう。

Agenda

□ Part I 量子の世界

- 二重スリットの実験
- Mach-Zehnder干渉計の実験
- 重ね合わせ Superposition
- もつれ合い Entanglement

□ Part II 量子コンピュータの理論的可能性

- 1943年 Church-Turing Thesis
- 1982年 Feynmannの洞察
- 1985年 Deutschの新しい原理
- 1994年 Shorの素因数分解アルゴリズム
- 計算の複雑性の理論と量子情報理論

Agenda

□ Part III 量子ゲート型量子コンピュータ

- 量子ゲート
- 量子アルゴリズム
- 量子ゲート型の問題

□ Part IV アニール型量子コンピュータ

- イジング・モデル (Ising Model)
 - 量子アニール
 - D-Wave のハードウェア
-

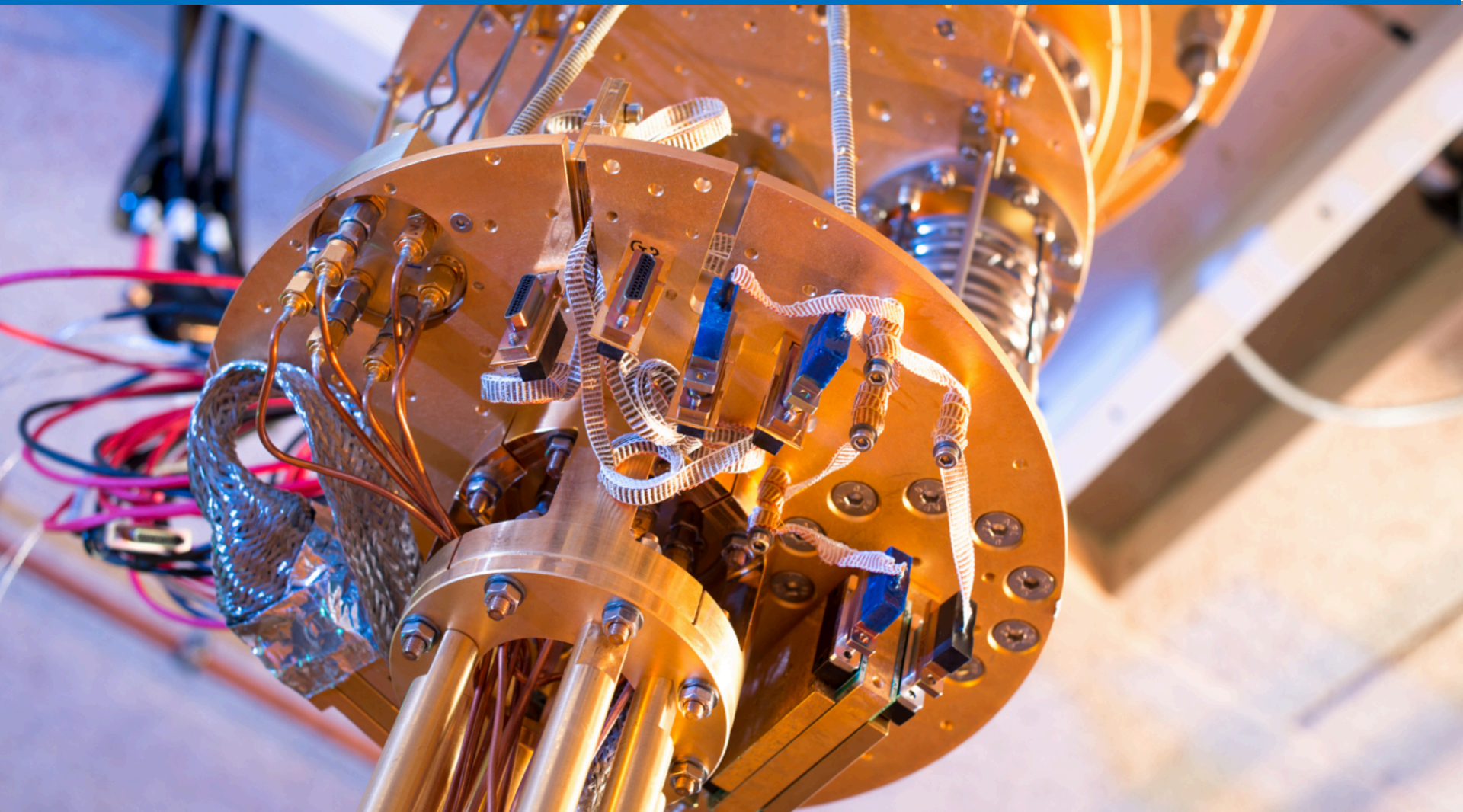
Agenda

□ Part V 量子コンピュータの動向

- Google
 - IBM
 - Microsoft
 - D-Wave
 - ImPACT(日本)
-

Part I

量子の世界



量子の世界

実験で明らかになったこと

20世紀の初め、アインシュタインは、光を金属に当てると電子が飛び出すという光電効果の現象が、光を波と考えては説明できず、光を波長に比例したエネルギーをもつ粒子だと考えると説明できることを示す。

粒子である電子も、二重スリットで干渉縞を示し、粒子性と波動性の二つの性質を持つことが明らかになる。



二重スリットの実験

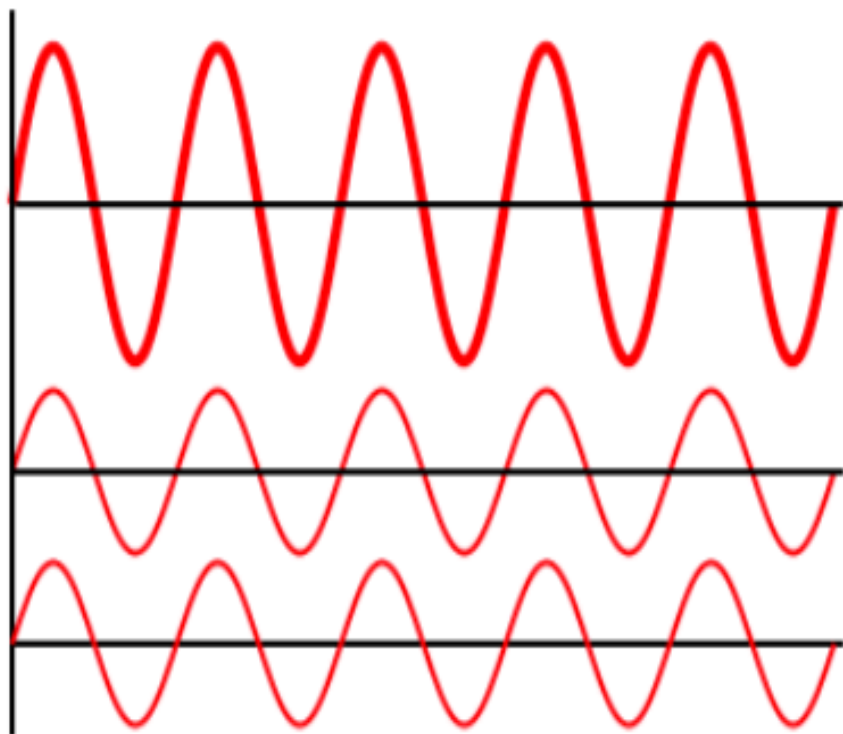
19世紀の初め、トーマス・ヤングは、二重スリットを通した光が干渉縞を示すことを示し、光が粒子なのか波なのかという古くからの問題に、**光は波であるという結論を与えた。**

波の重ね合わせ

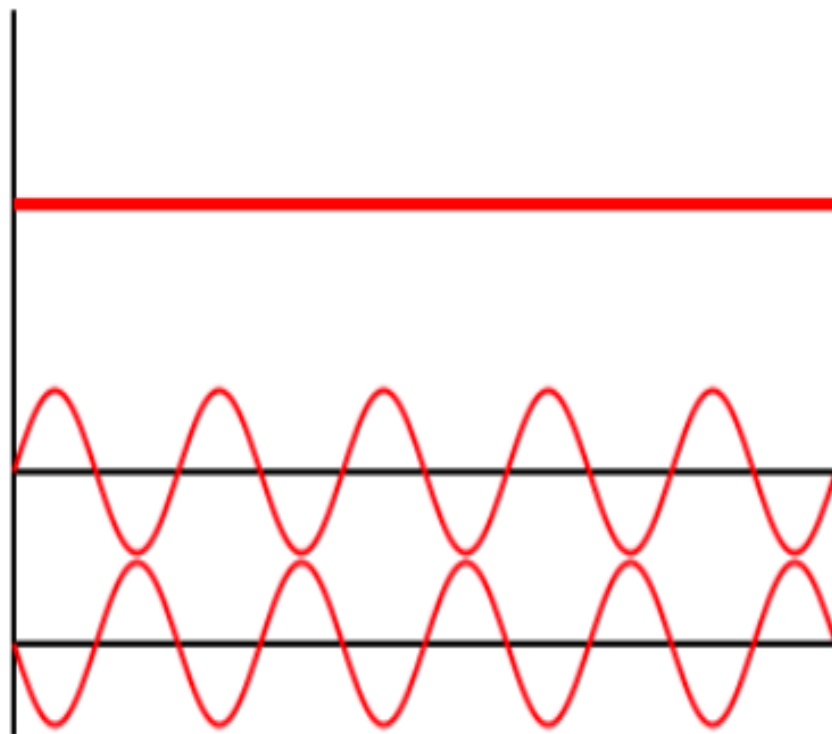


波の重ね合わせ

強めあう



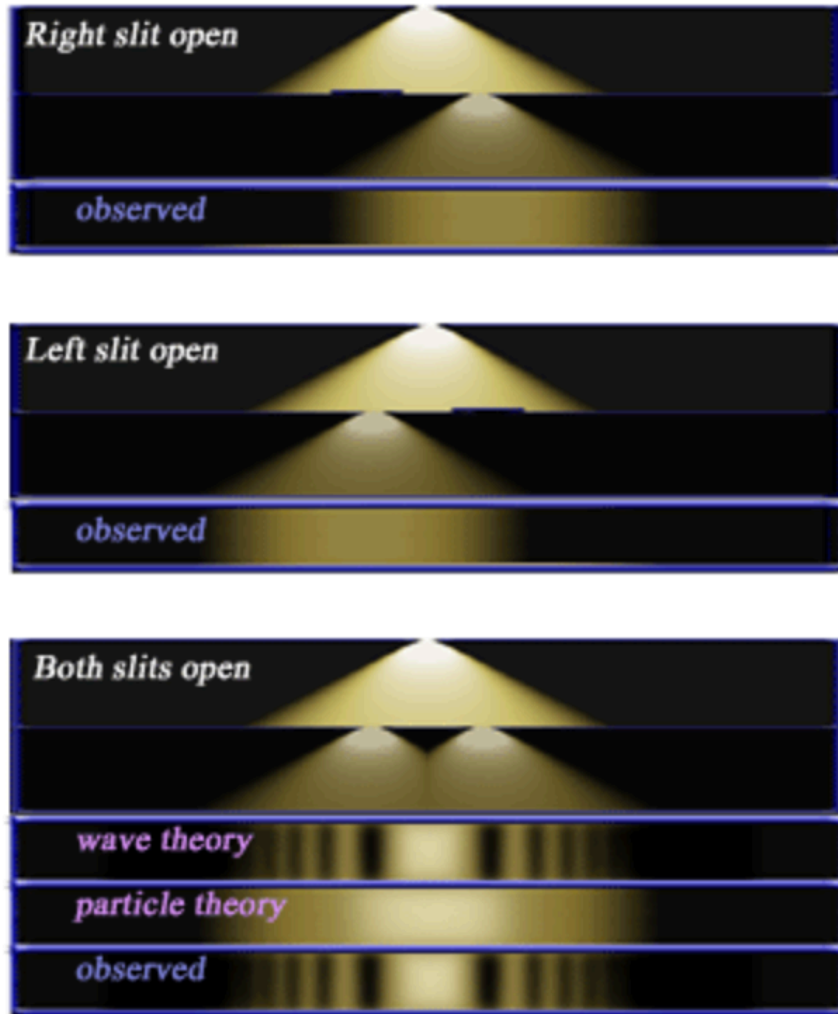
打ち消しあう





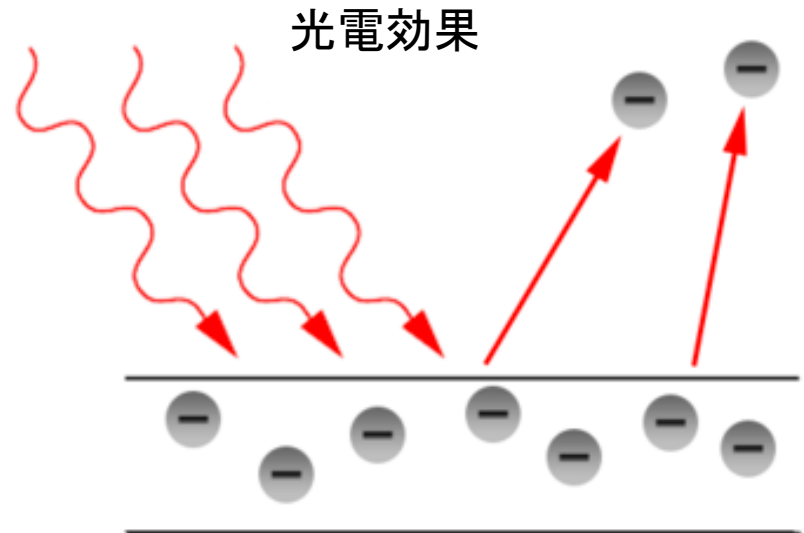
干渉縞が生まれる

光は波



1805年 ヤングの実験

光は粒子



「光子は振動数に比例する
エネルギーを持つ粒子である」

1905年 アインシュタイン 光子

Feynmann's Lectures on Physics

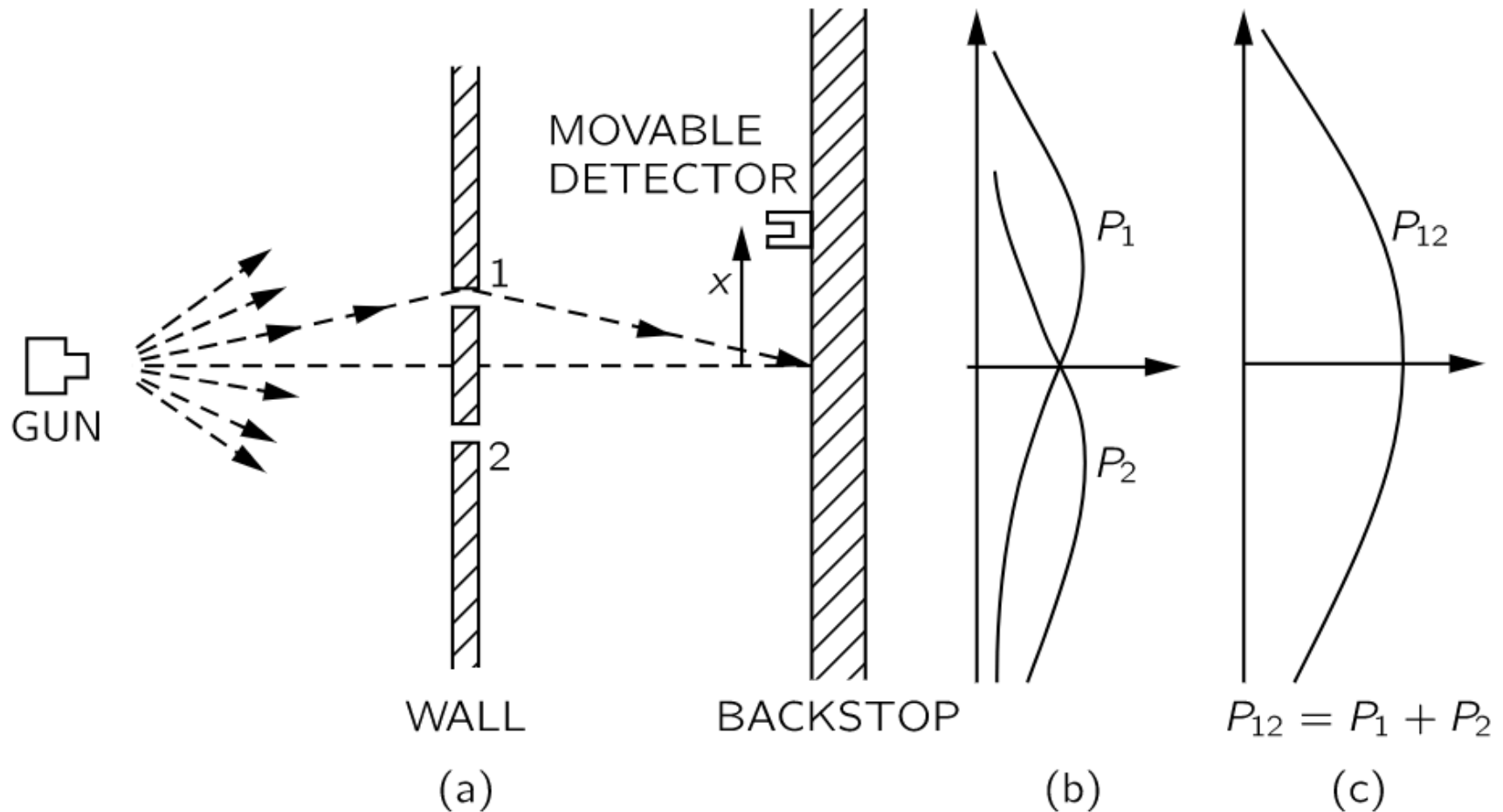


Fig. 1-1. Interference experiment with bullets.

Feynmann's Lectures on Physics

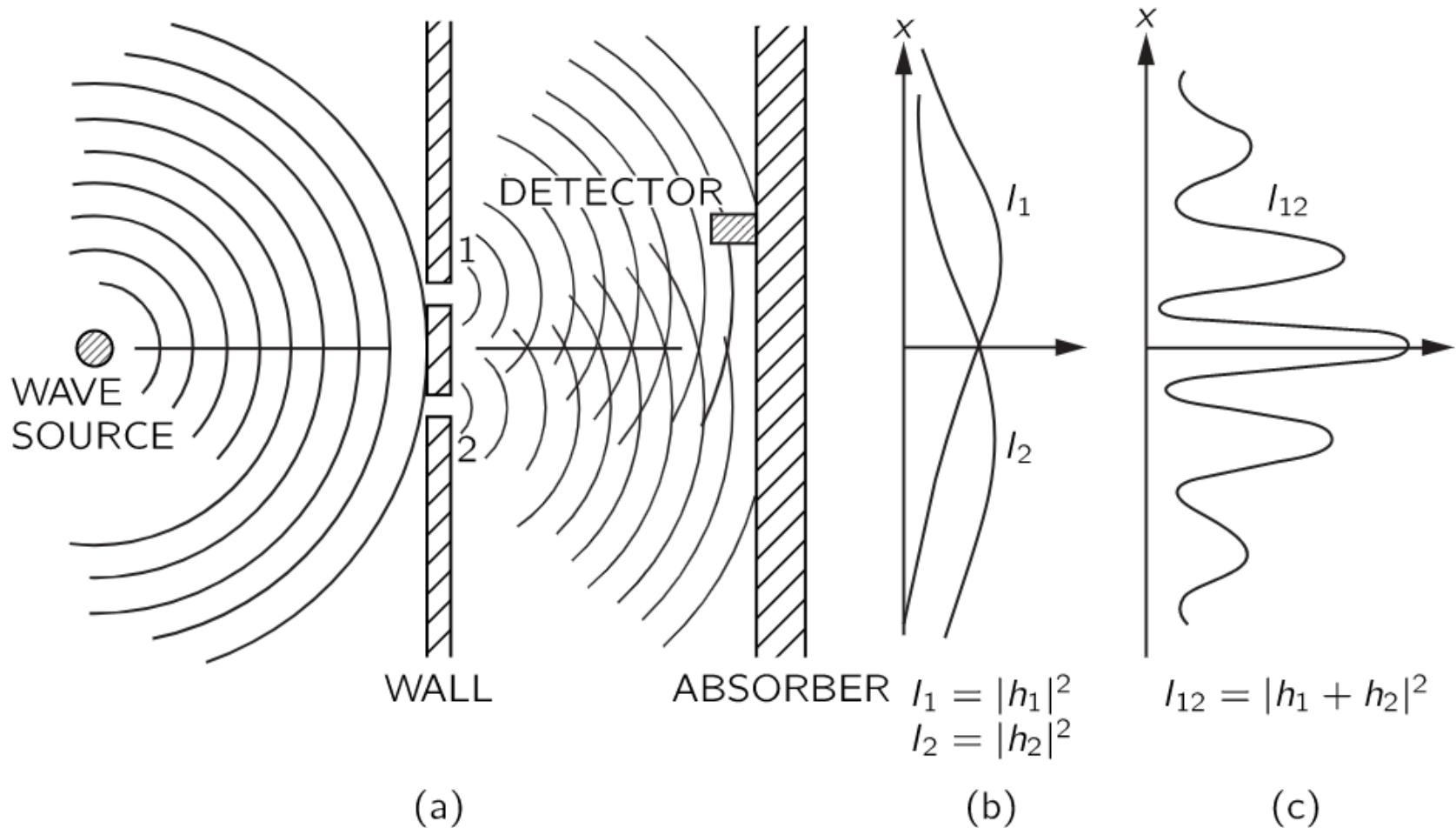


Fig. 1–2. Interference experiment with water waves.

Feynmann's Lectures on Physics

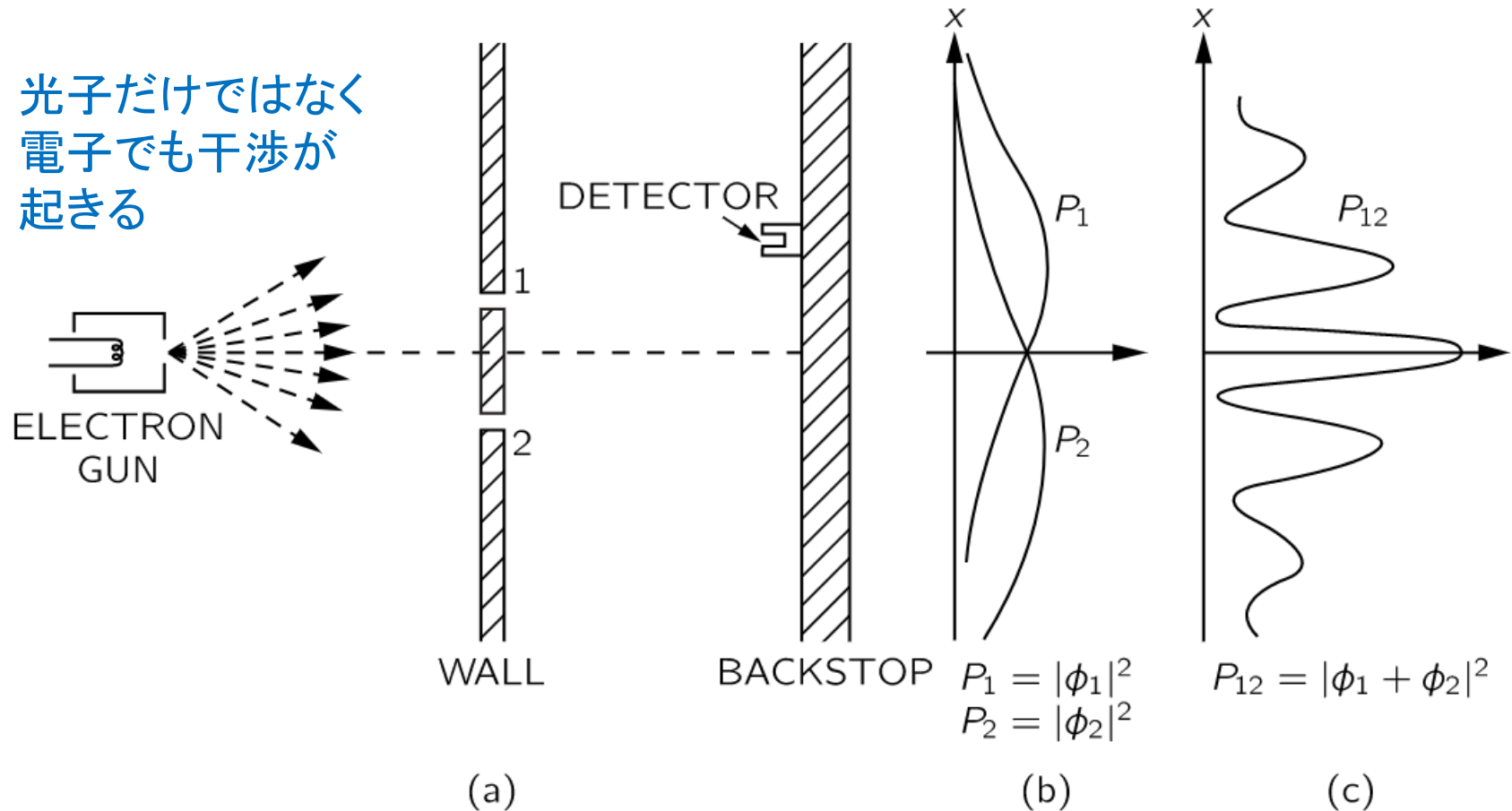


Fig. 1–3. Interference experiment with electrons.



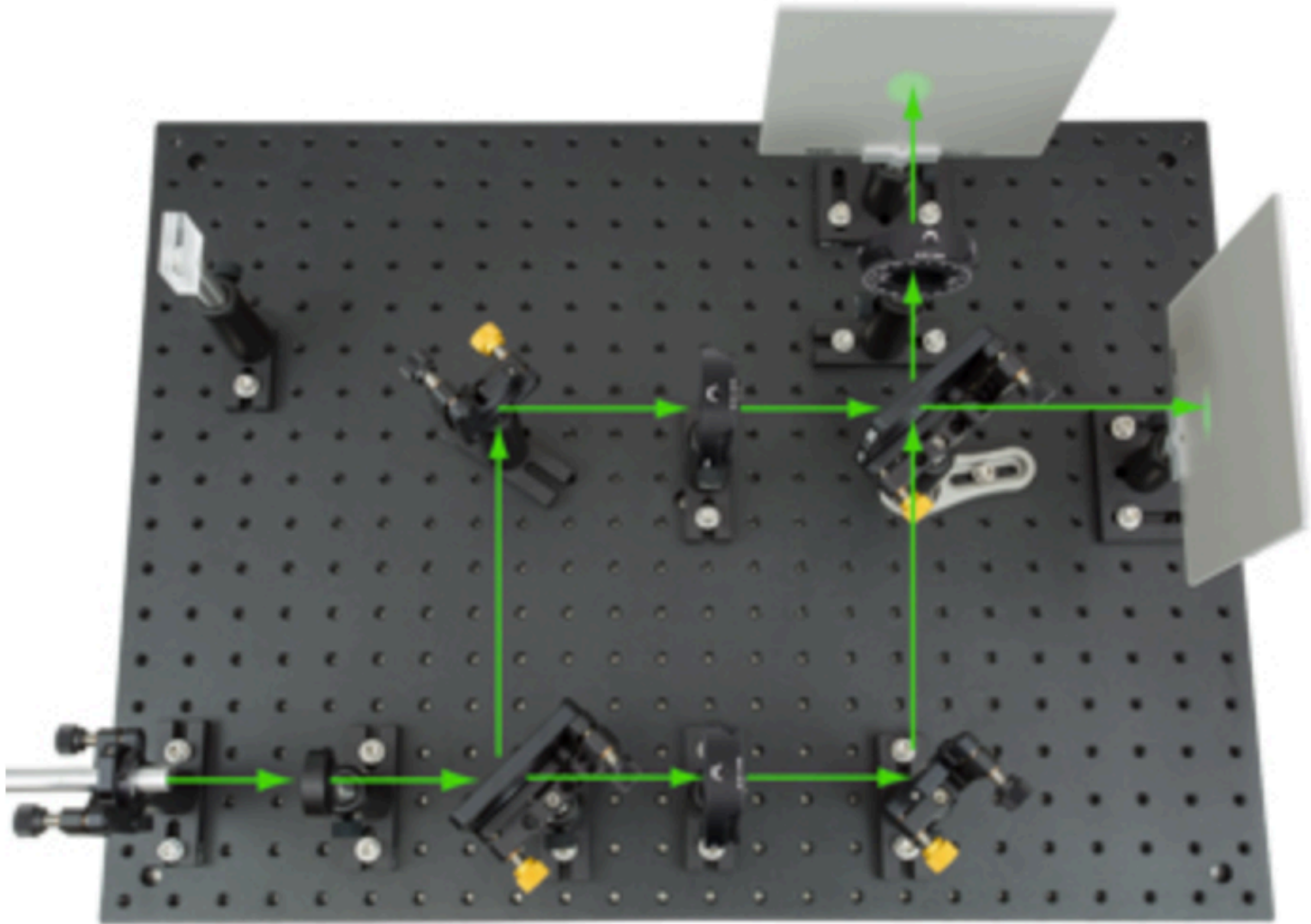
Dr. Quantum <https://goo.gl/CFJfjy>

The background of the slide is a black and white photograph of a Mach-Zehnder interferometer's output pattern. It shows a series of concentric, slightly distorted circular fringes that create a moiré-like effect, with alternating light and dark regions. The pattern is centered and fills the entire frame.

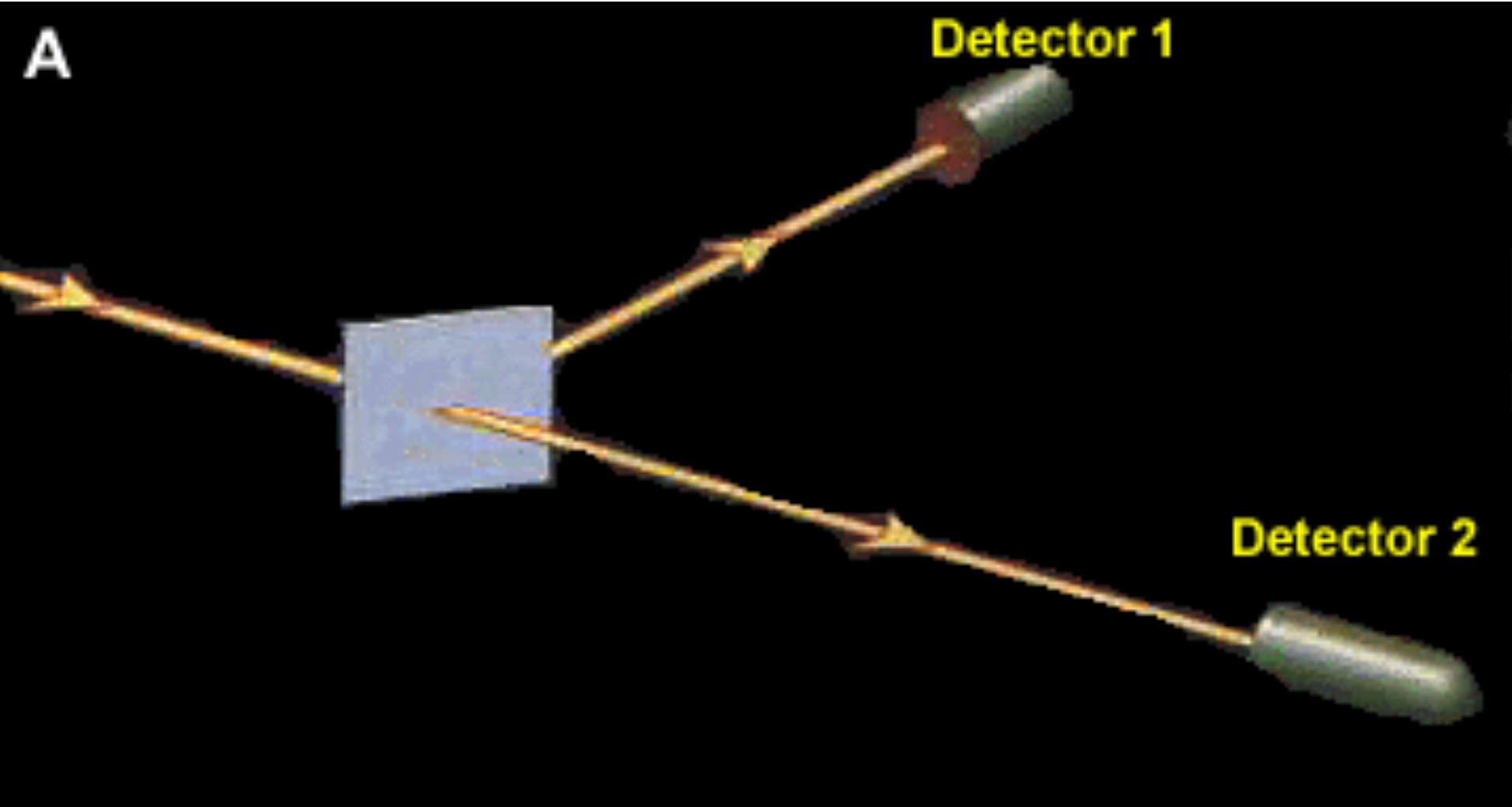
Mach Zehnder 干渉計の実験

Mach-Zehnder干渉計の実験は、一つの光子であっても、それが、「同時に」、波でもあり粒子でもあることを示す。

Mach Zehnder 干渉計

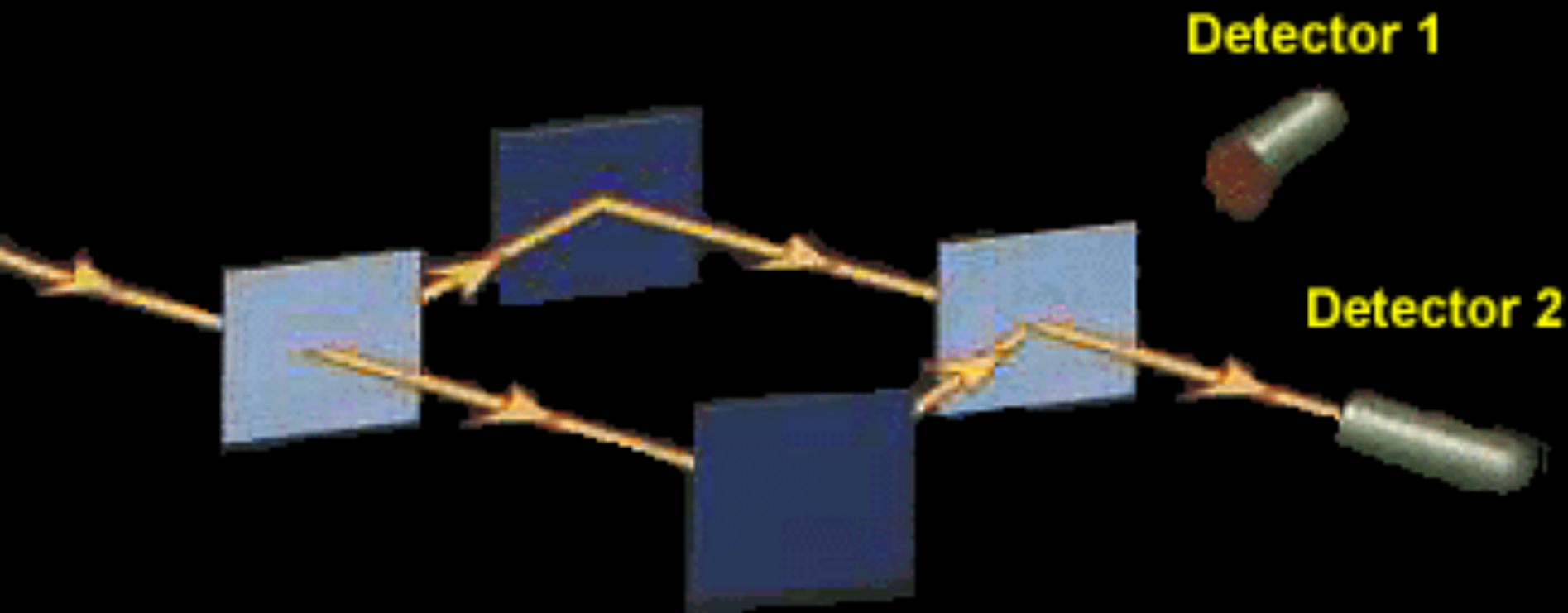


量子消しゴム(Quantum Eraser)実験キット
<https://goo.gl/BB4F5D>



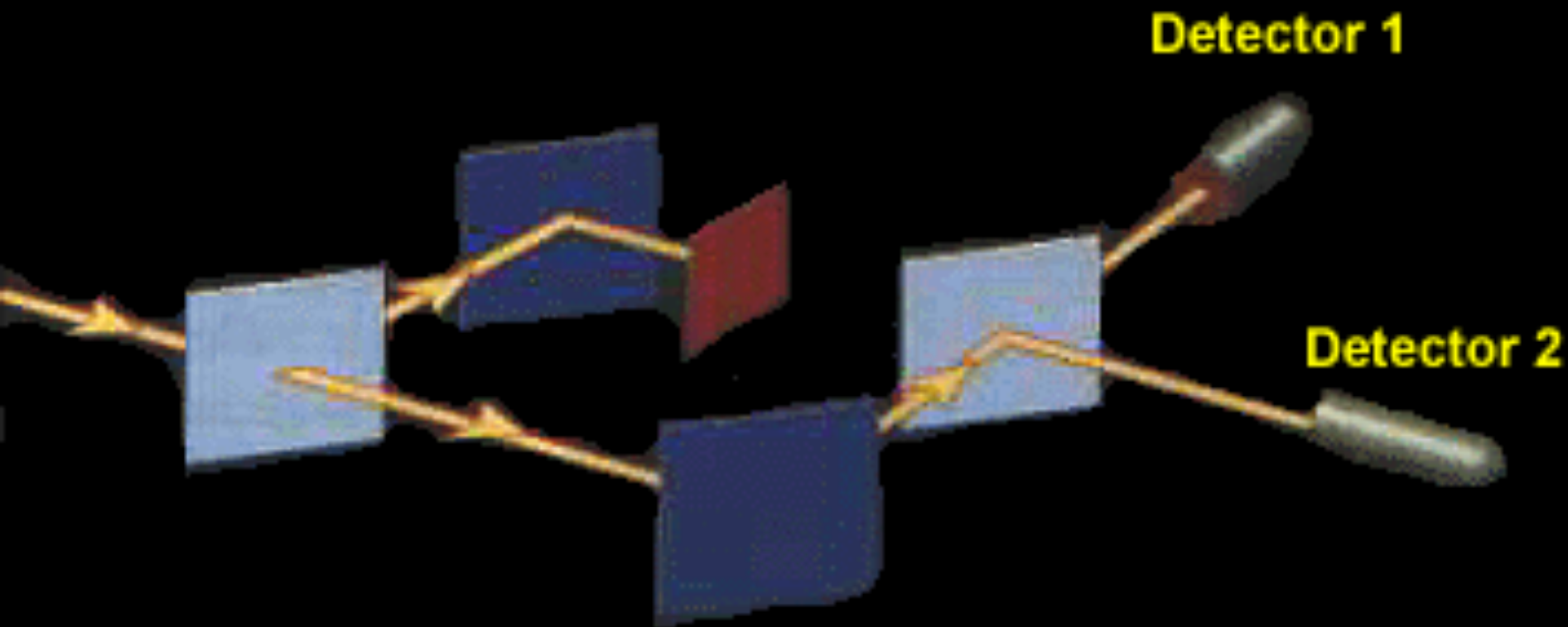
光を半分は通し半分は反射する、ハーフミラーを45度の角度で光の進路に置く。**光は、二つの検出器に届く。**光子一個で実験を繰り返すと、ある光子は検出器1に、ある光子は検出器2に届く。その確率は等しい。ここに不思議なことはない。

B



ハーフミラー二つと鏡二つを組み合わせて、上のような装置を作る。光は干渉をおこして、検出器の一方にしか届かなくなる。奇妙なことは、光子一個で実験しても、このことは変わらない。一個の光子は、二つの道を「同時」に通っている。

C



もっと奇妙なことは、**光路の一方を塞ぐと、光は両方の検出器に届くようになる。**光子一個で考えると、行く手を阻まれた光子は、そのことを、他方の光子に伝えて(どちらも自分自身なのだが)、その性質を変えているように見える。

量子論の成立

実験結果を説明する理論の登場

20世紀の20年代、シュレジンガー、ハイゼンベルグ、ディラックらが、これらの実験結果を説明できる理論を提出し、量子論が成立する。その後、フォン・ノイマンが、その数学的・形式的な定式化を完成する。

重力を一般相対性理論で時空の性質として説明することに成功したアインシュタインは、量子論に満足せず、1935年、量子の「もつれ合い」という奇妙な現象を発見する。

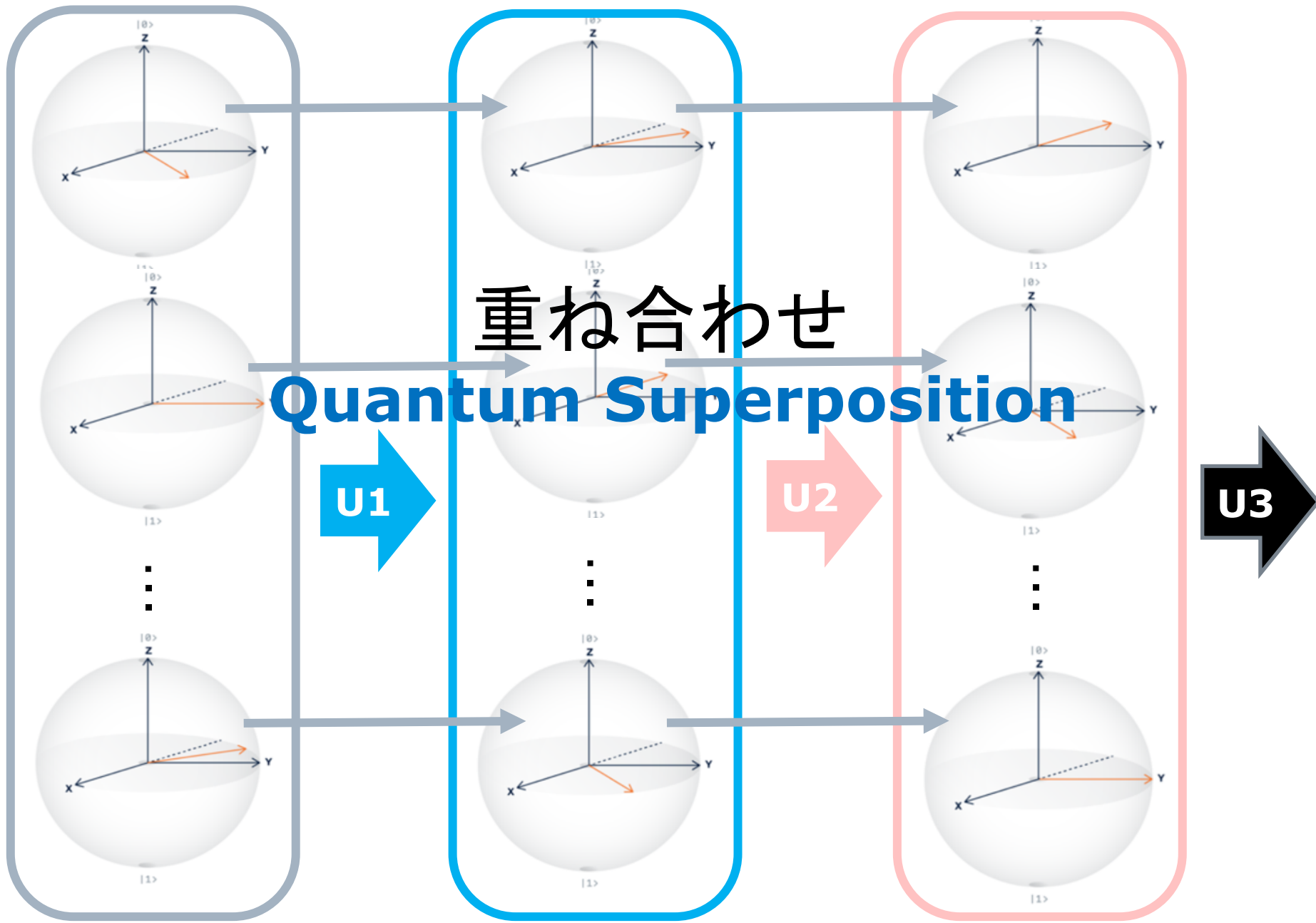
重ね合わせ

Quantum Superposition

U1

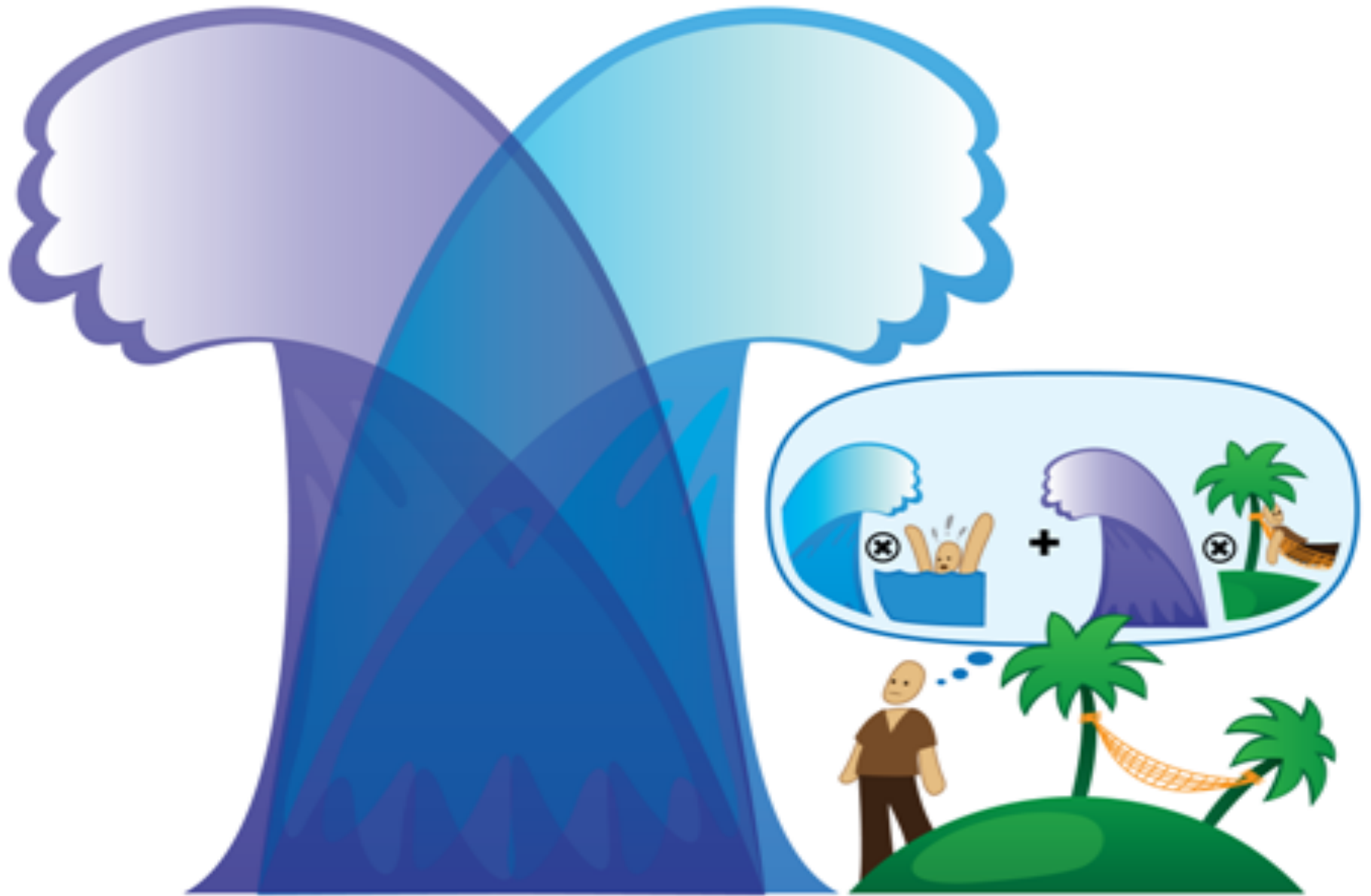
U2

U3





二つの波の重ね合わせ



古典Bit

0か1

0

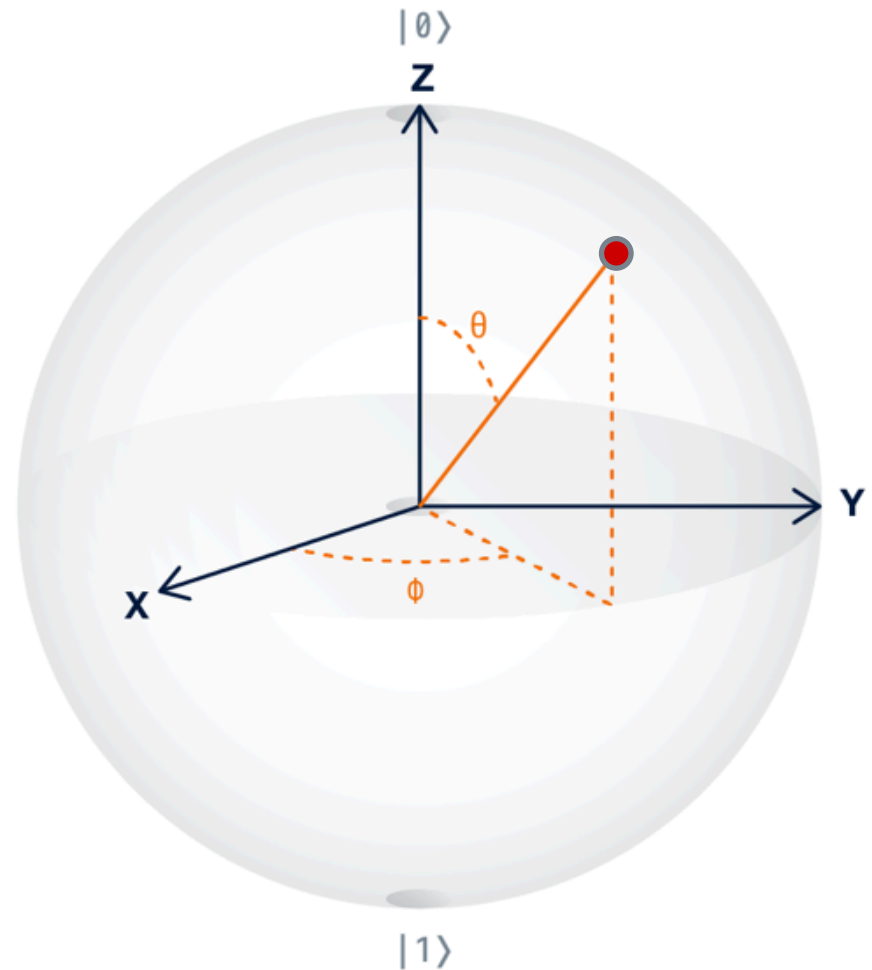


1



Bitは、0または1
どちらかの状態を取る

量子Qubit

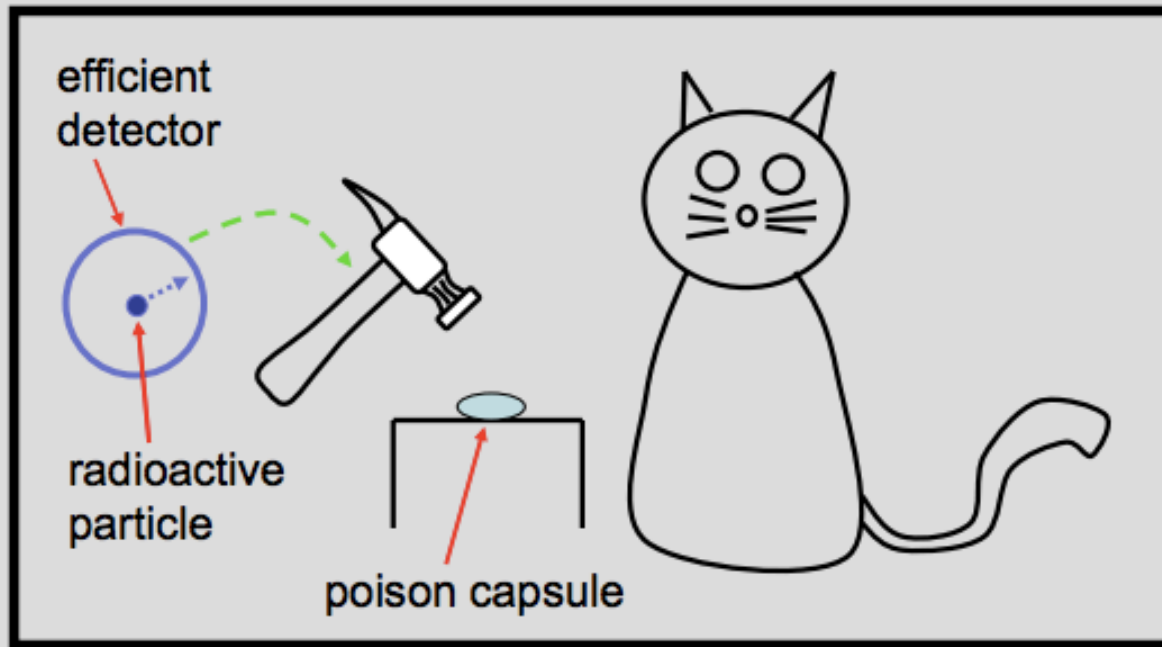


Qubitは、状態 $|0\rangle$ と
状態 $|1\rangle$ の重ね合わせ
の状態を取る

$$|\text{Qubit}\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$\alpha^2 + \beta^2 = 1 ; \alpha, \beta \in \mathbb{C}$$

Erwin Schrödinger's Cat (1935)

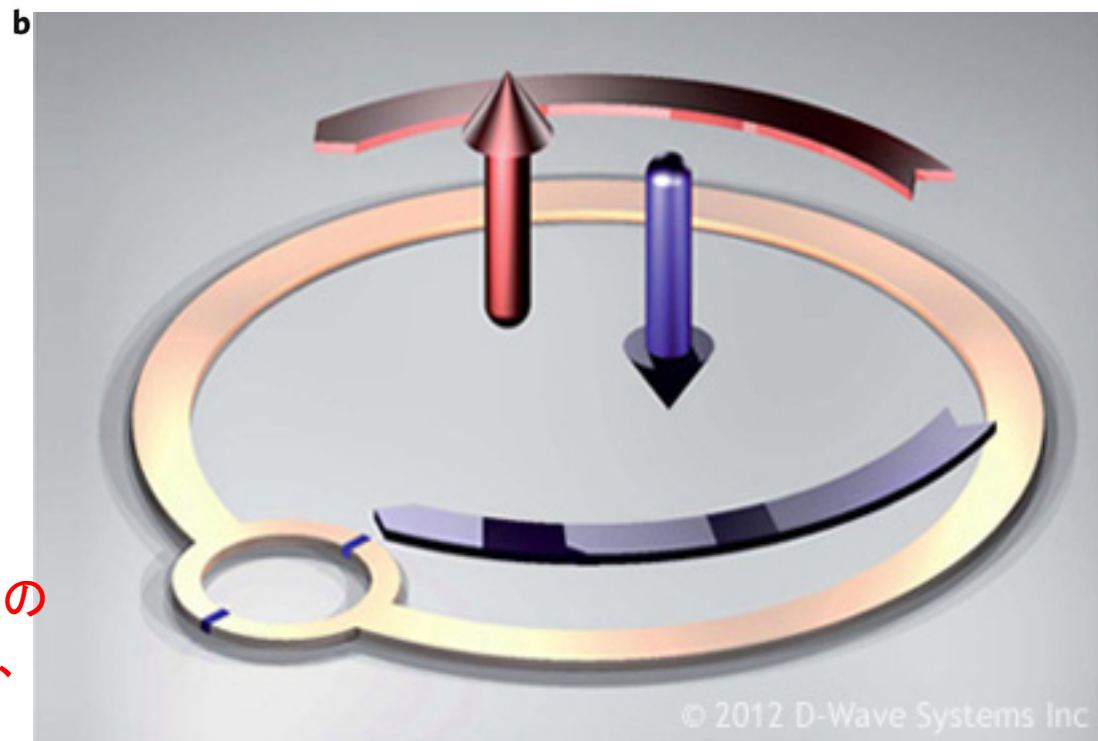
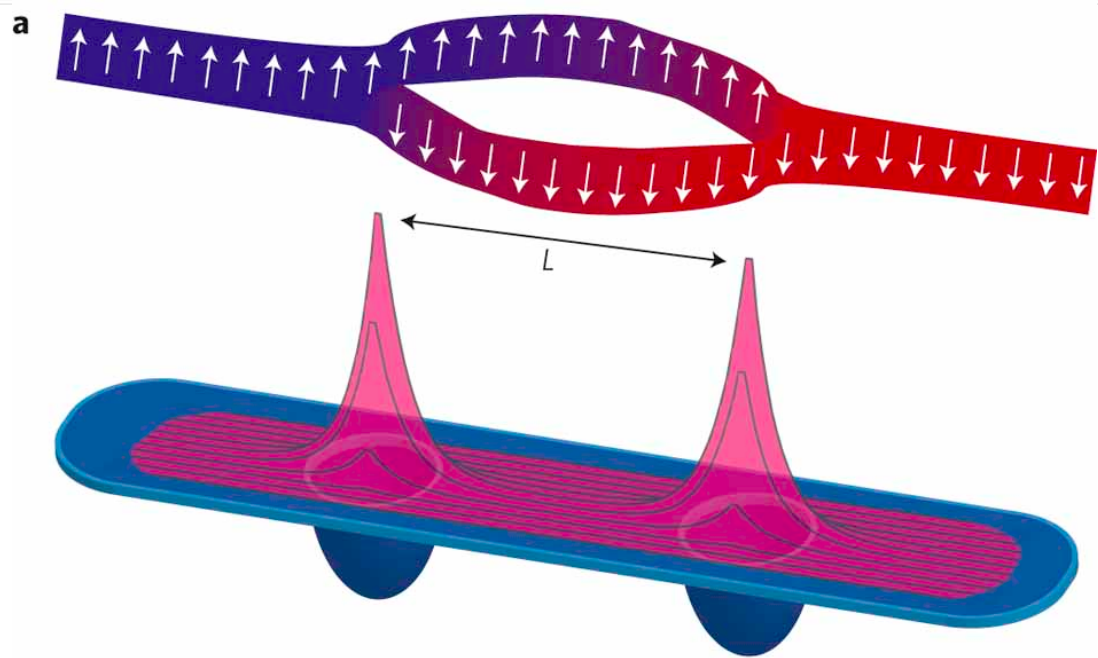
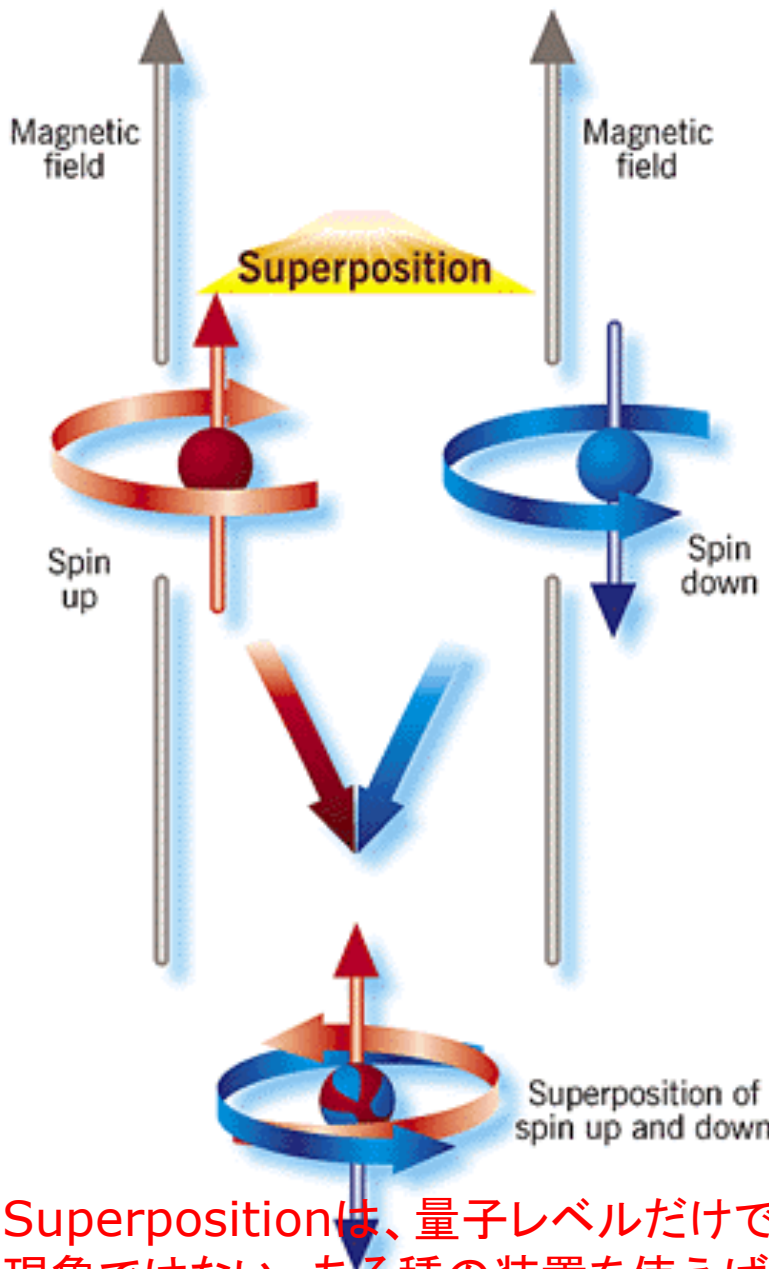


At “half-life of particle, quantum mechanics says
cat is simultaneously dead and alive!

“superposition” $\Psi = |\text{circle with dot}\rangle |\text{cat with open eyes}\rangle + |\text{circle with dot and arrow}\rangle |\text{cat with closed eyes}\rangle$

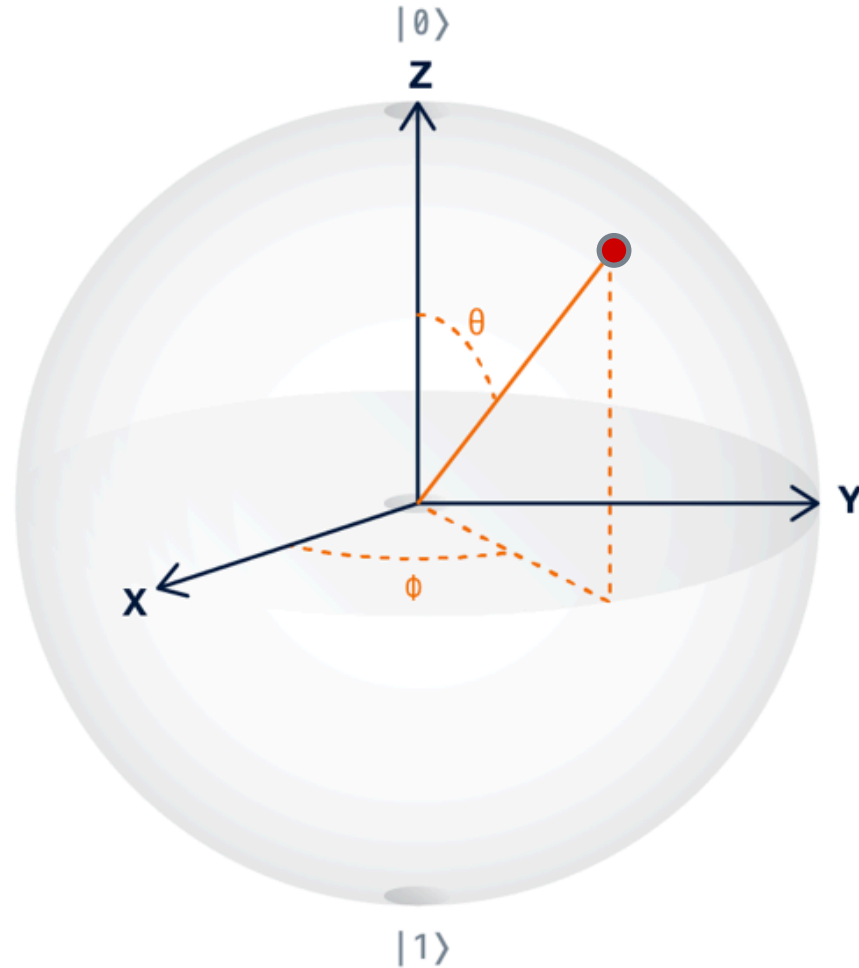
2012年 Winelandのノーベル賞記念講演から

http://www.nobelprize.org/nobel_prizes/physics/laureates/2012/wineland-lecture_slides.pdf



Superpositionは、量子レベルだけの現象ではない。ある種の装置を使えば、それはマクロな現象として現れる。

Qubit

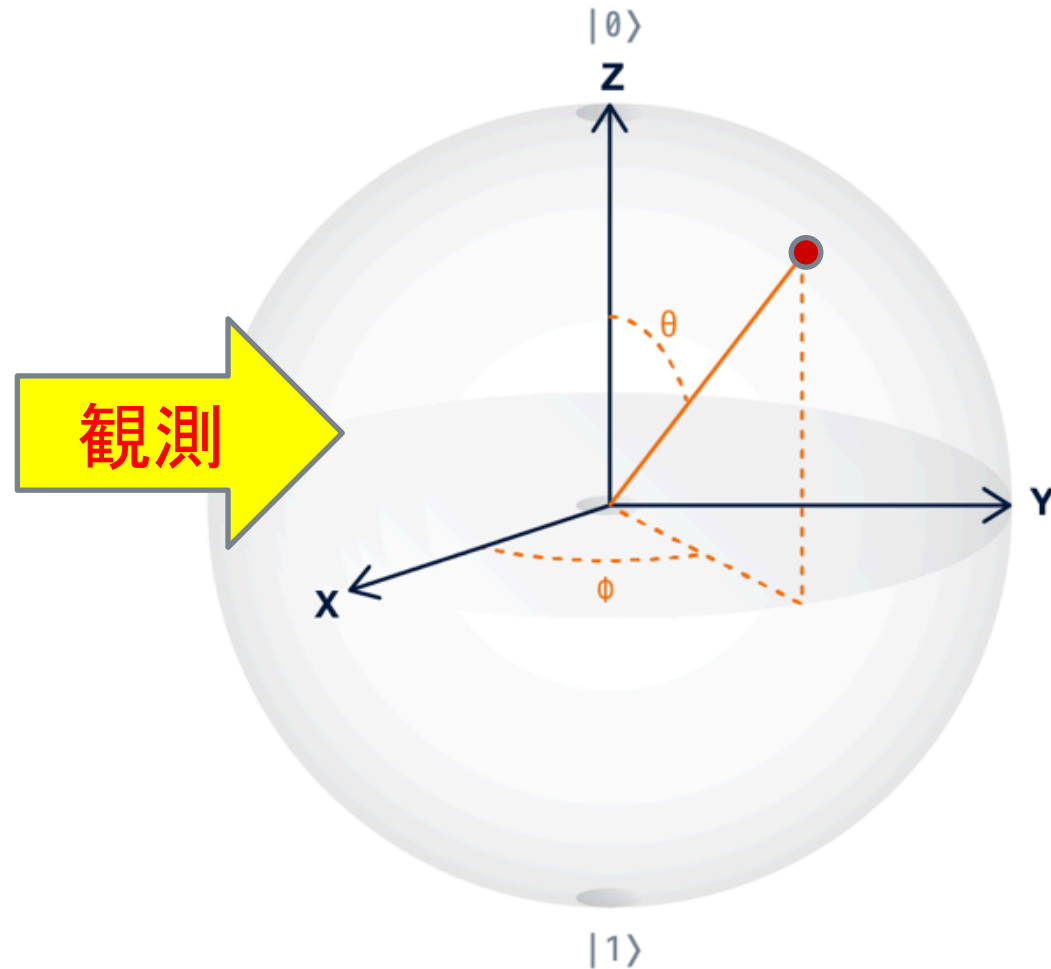


Qubitは、状態 $|0\rangle$ と
状態 $|1\rangle$ の重ね合わせ
の状態を取る

$$|\text{Qubit}\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$\alpha^2 + \beta^2 = 1 ; \quad \alpha, \beta \in \mathbb{C}$$

Qubit

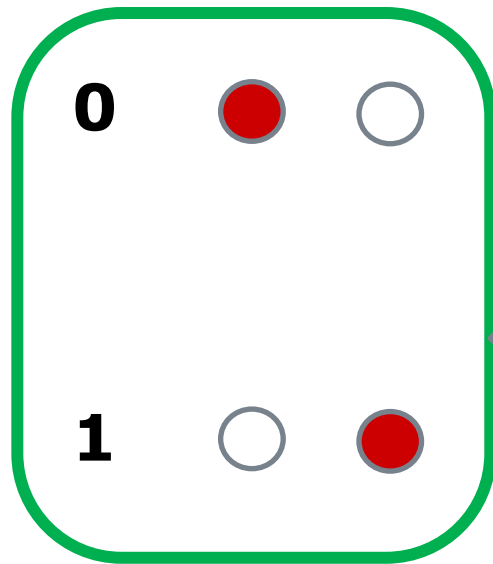


Qubitは、状態 $|0\rangle$ と
状態 $|1\rangle$ の重ね合わせ
の状態を取る

$$|\text{Qubit}\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$\alpha^2 + \beta^2 = 1 ; \alpha, \beta \in \mathbb{C}$$

観測を行うと、Qubitの
重ね合わせの状態は
失われ、0か1かの情報
が返る。



観測

観測値

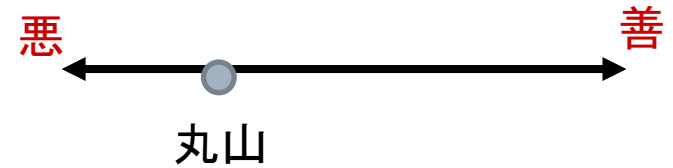
Qubit

$\alpha|0\rangle + \beta|1\rangle$
の重ね合わせの
状態は、失われる

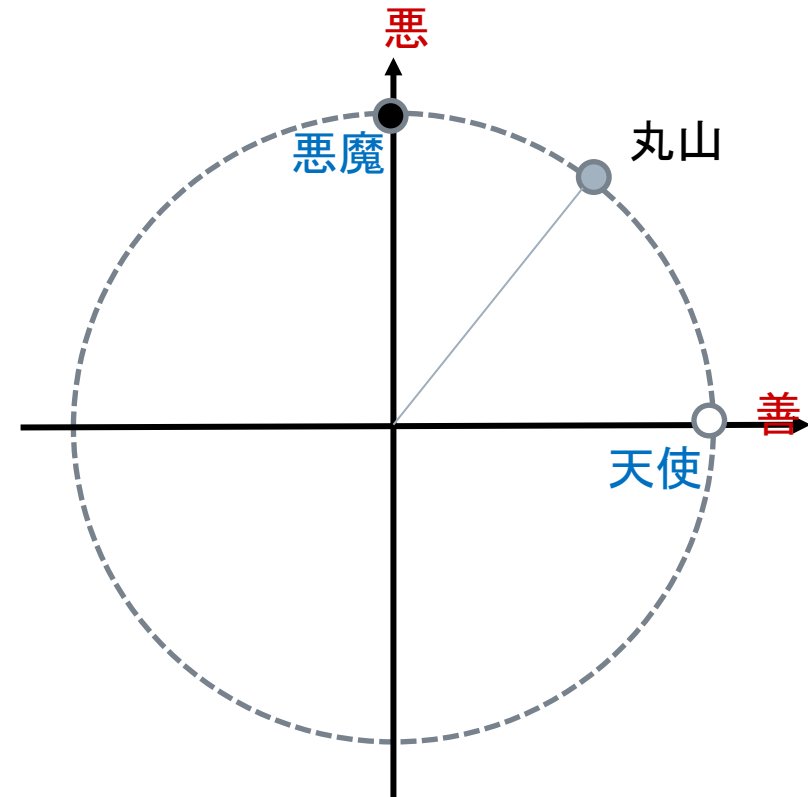
この時
0を得る確率は、 $|\alpha|^2$ で、
1を得る確率は、 $|\beta|^2$ で、
与えられる。

$$\alpha^2 + \beta^2 = 1 ; \alpha, \beta \in \mathbb{C}$$

単純な善悪観



善悪判定器



善と判定される確率は、 $|\alpha|^2$ で、
悪と判定される確率は、 $|\beta|^2$ 。

善と悪の重ね合わせ

$$|\text{丸山}\rangle = \alpha |\text{善}\rangle + \beta |\text{悪}\rangle$$

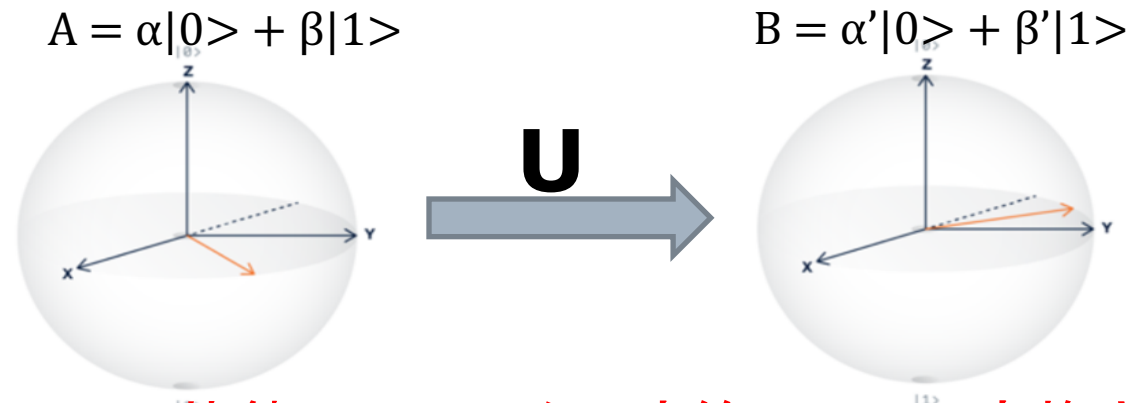
ユニタリ変換

状態 $A = \alpha|0\rangle + \beta|1\rangle$ が、 U によって状態 $B = \alpha'|0\rangle + \beta'|1\rangle$ U に変わったとしよう。

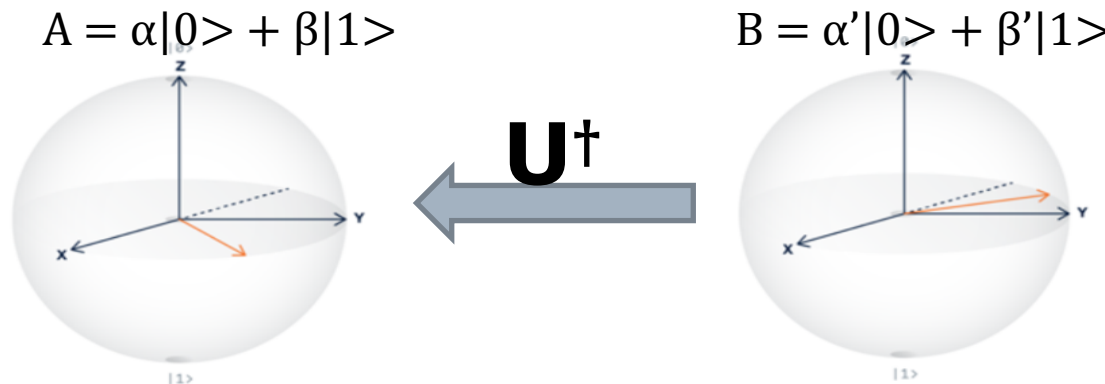
$$\mathbf{U} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ とすると、 } \mathbf{U}A=B \text{ で、 } \mathbf{U}^\dagger = \begin{pmatrix} a^* & c^* \\ b^* & d^* \end{pmatrix}$$

この時、 $\mathbf{U}^\dagger \mathbf{U} = \mathbf{U} \mathbf{U}^\dagger = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ を示すことができる。

こうした性質を持つ演算子をユニタリ演算子という



Qubitの状態は、ユニタリ演算子 U で変換される



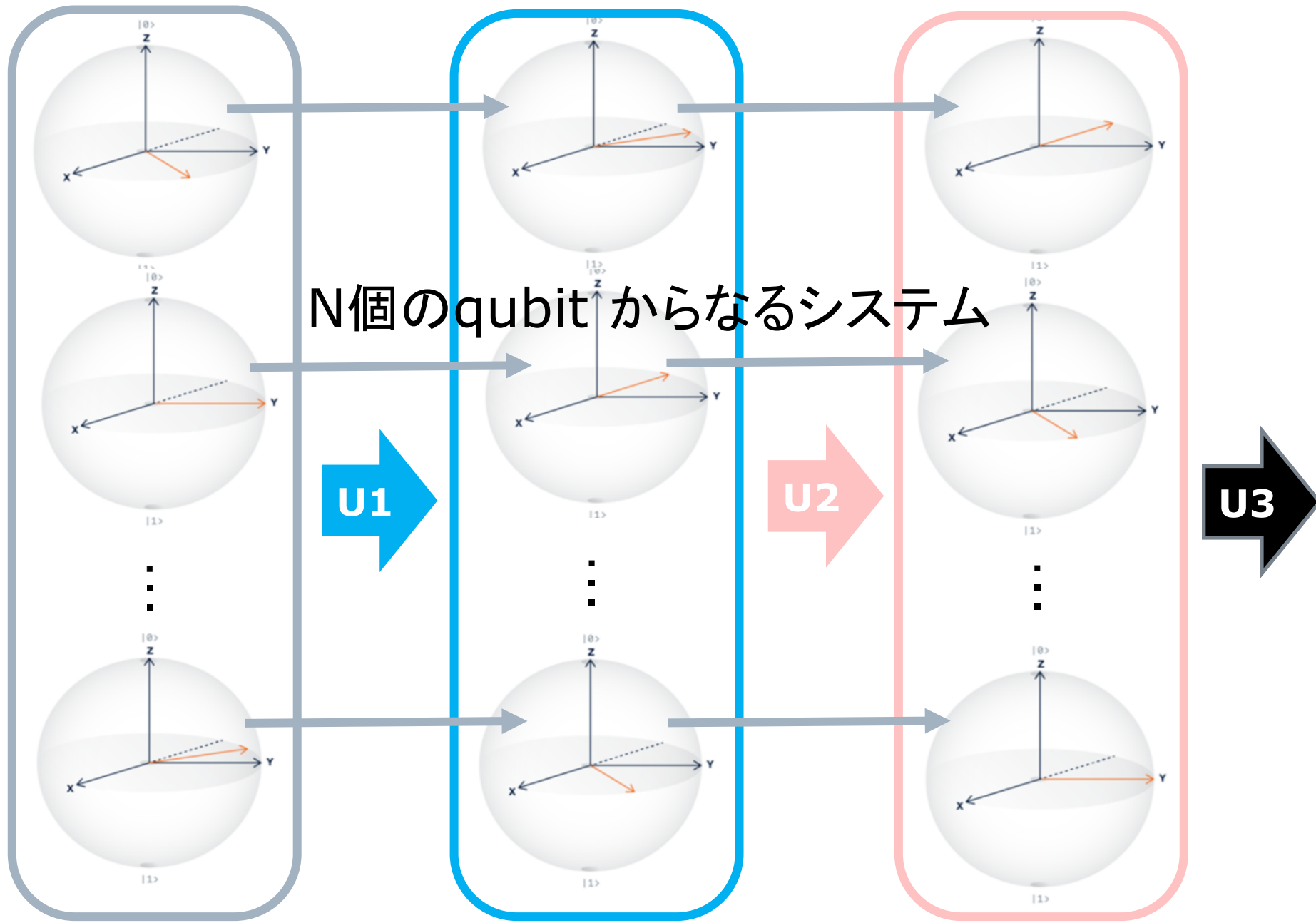
量子ビットが従う、基本的な規則 $\alpha\alpha\alpha$

1. 量子Qubitは、状態 $|0\rangle$ と状態 $|1\rangle$ の重ね合わせの状態を取る

$$|\text{Qubit}\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$\text{ただし、} |\alpha|^2 + |\beta|^2 = 1 ; \alpha, \beta \in \mathbb{C}$$

2. 観測を行うと、量子Qubitの重ね合わせの状態は失われ、0か1かの古典Bit情報が返る。
3. この時
0を得る確率は、 $|\alpha|^2$ で、
1を得る確率は、 $|\beta|^2$ で、与えられる。
4. Qubitの状態の変化は、ユニタリ演算子で与えられる。



2つのqubitからなるシステム

- qubit $a|0\rangle + b|1\rangle$ のみを含むシステムを $S1$ 、qubit $c|0\rangle + d|1\rangle$ のみを含むシステムを $S2$ がある時、この二つを一緒にしたシステム S を $S1 \otimes S2$ で表す。
- この時、次のような計算で、 S の状態を計算する。
$$S = S1 \otimes S2 = (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle)$$
$$= ac|0\rangle \otimes |0\rangle + ad|0\rangle \otimes |1\rangle + bc|1\rangle \otimes |0\rangle + bd|1\rangle \otimes |1\rangle$$
- $|i\rangle \otimes |j\rangle$ を $|ij\rangle$ と表すことにすると、
 $S = ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle$ となる。
ただし、 $(ac)^2 + (ad)^2 + (bc)^2 + (bd)^2 = 1$
- 一般に、二つのqubitからなるシステム S は、次のように、4つの状態の重ね合わせの形で表すことができる。
 $S = A|00\rangle + B|01\rangle + C|10\rangle + D|11\rangle$ ただし、 $A^2 + B^2 + C^2 + D^2 = 1$

3つのqubitからなるシステム

- 先のSに、もう一つqubit $e|0\rangle+f|1\rangle$ のみを含むシステムS3を追加して、3つのqubitからなるシステムを考えよう。改めて、これもSとすると

$$\begin{aligned} S &= S1 \otimes S2 \otimes S3 \\ &= (a|0\rangle+b|1\rangle) \otimes (c|0\rangle+d|1\rangle) \otimes (e|0\rangle+f|1\rangle) \\ &= \dots \\ &= A|000\rangle+B|001\rangle+C|010\rangle+D|011\rangle \\ &\quad + E|100\rangle+F|101\rangle+G|110\rangle+H|111\rangle \end{aligned}$$

という 8つの状態の重ね合わせの形になる。

n 個のqubitで、 2^n 個の並行計算が可能

Input register

$a_1 |000\rangle$
+
 $a_2 |001\rangle$
+
 $a_3 |010\rangle$
+
 $a_4 |011\rangle$
+
 $a_5 |100\rangle$
+
 $a_6 |101\rangle$
+
 $a_7 |110\rangle$
+
 $a_8 |111\rangle$



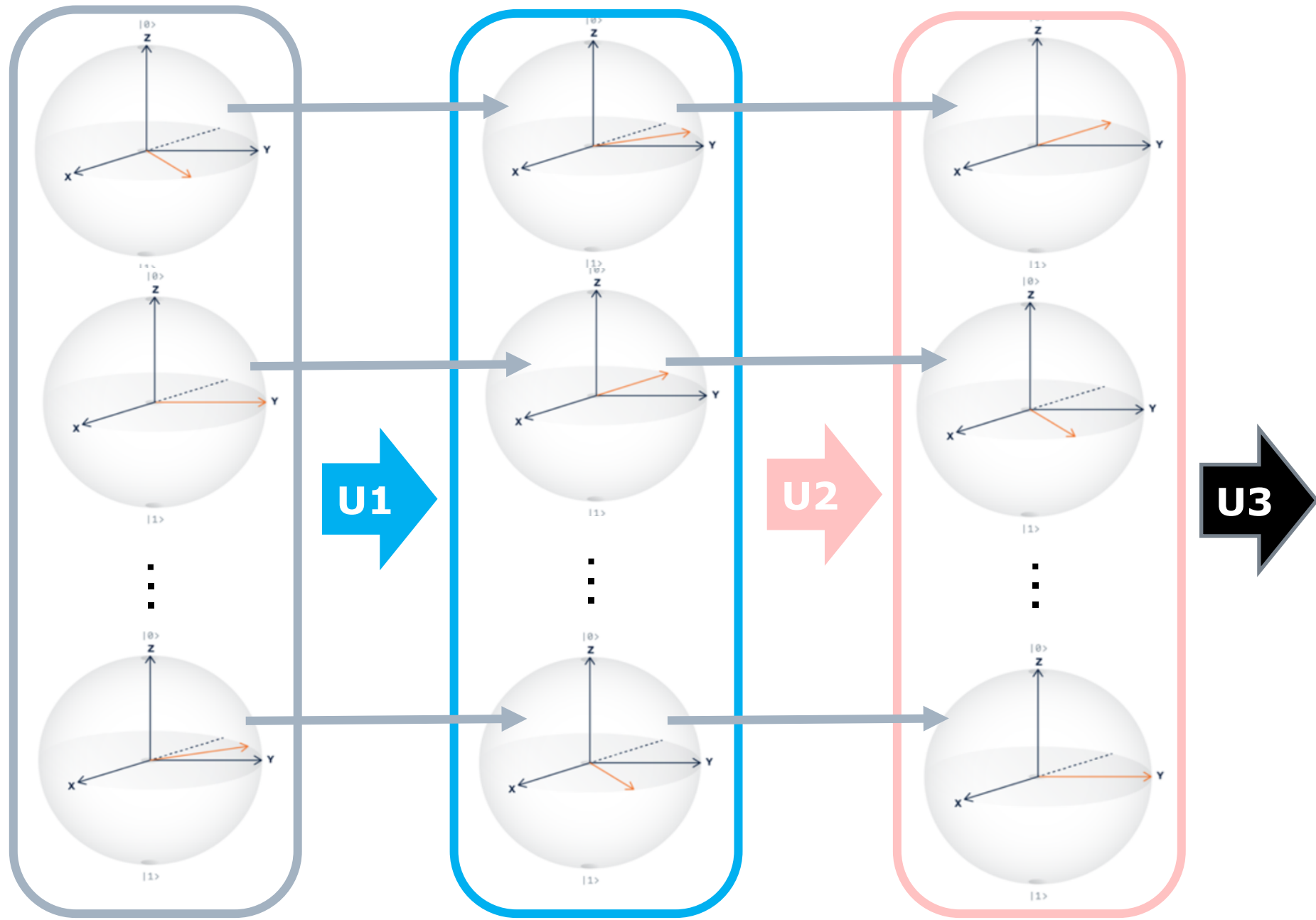
Output register

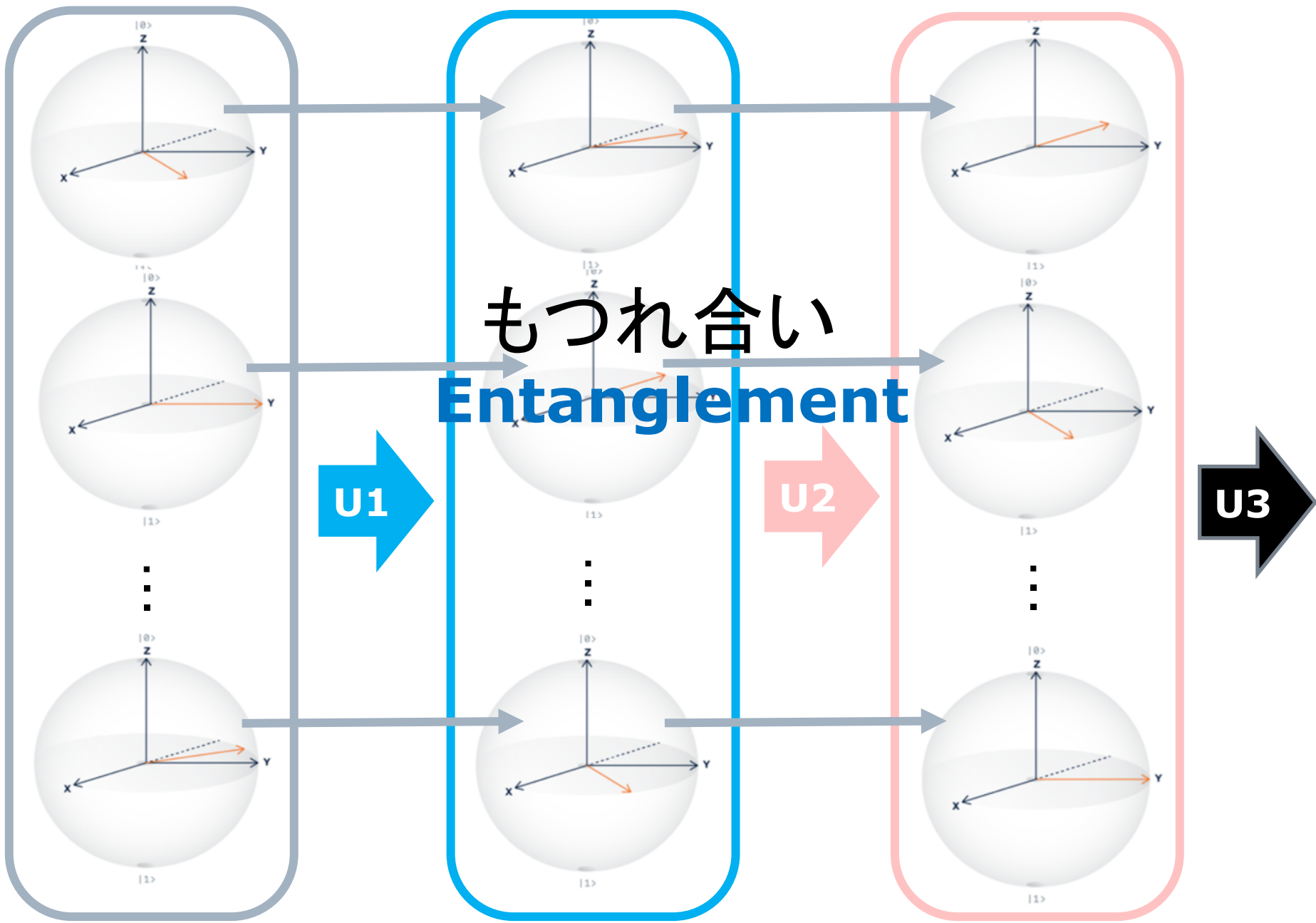
$a_1 F(|000\rangle)$
+
 $a_2 F(|001\rangle)$
+
 $a_3 F(|010\rangle)$
+
 $a_4 F(|011\rangle)$
+
 $a_5 F(|100\rangle)$
+
 $a_6 F(|101\rangle)$
+
 $a_7 F(|110\rangle)$
+
 $a_8 F(|111\rangle)$

=

$b_1 |000\rangle$
+
 $b_2 |001\rangle$
+
 $b_3 |010\rangle$
+
 $b_4 |011\rangle$
+
 $b_5 |100\rangle$
+
 $b_6 |101\rangle$
+
 $b_7 |110\rangle$
+
 $b_8 |111\rangle$

N個のqubit からのなるシステムの変化





もつれ合い – Entanglement

量子情報理論の基礎 2

「量子もつれ」は、量子のあいだに特別の相関関係が生まれる現象である。

「Superposition」が現象としては既に19世紀末に確認され、20世紀に入って量子論の成立とともに理論化が進んだのに対して「entanglement」が実験的に確証されたのは、20世紀の後半である。アインシュタインは、量子論の矛盾を示すものとして、Entanglementに注目していた。





Alice

MEASUREMENT

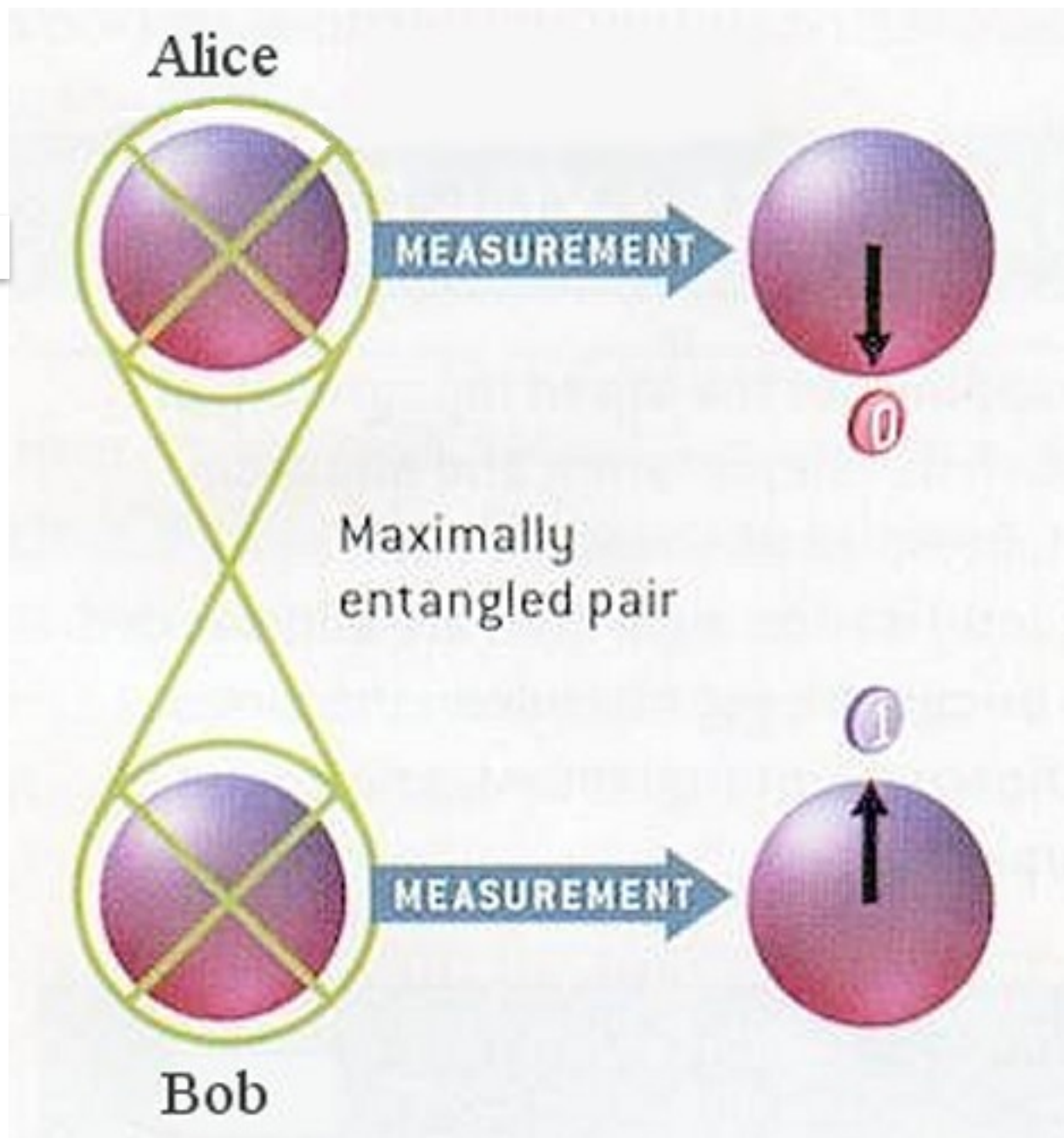
Maximally
entangled pair

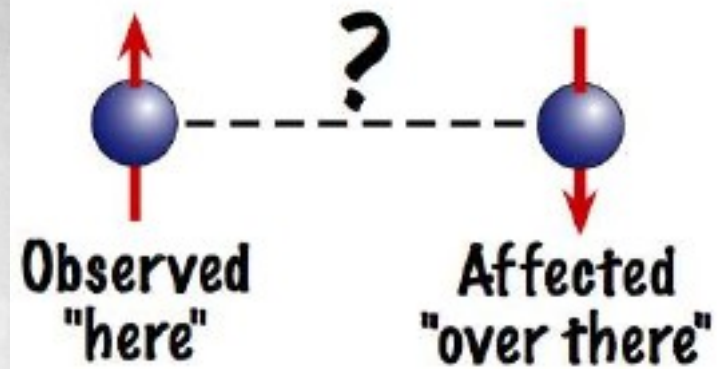
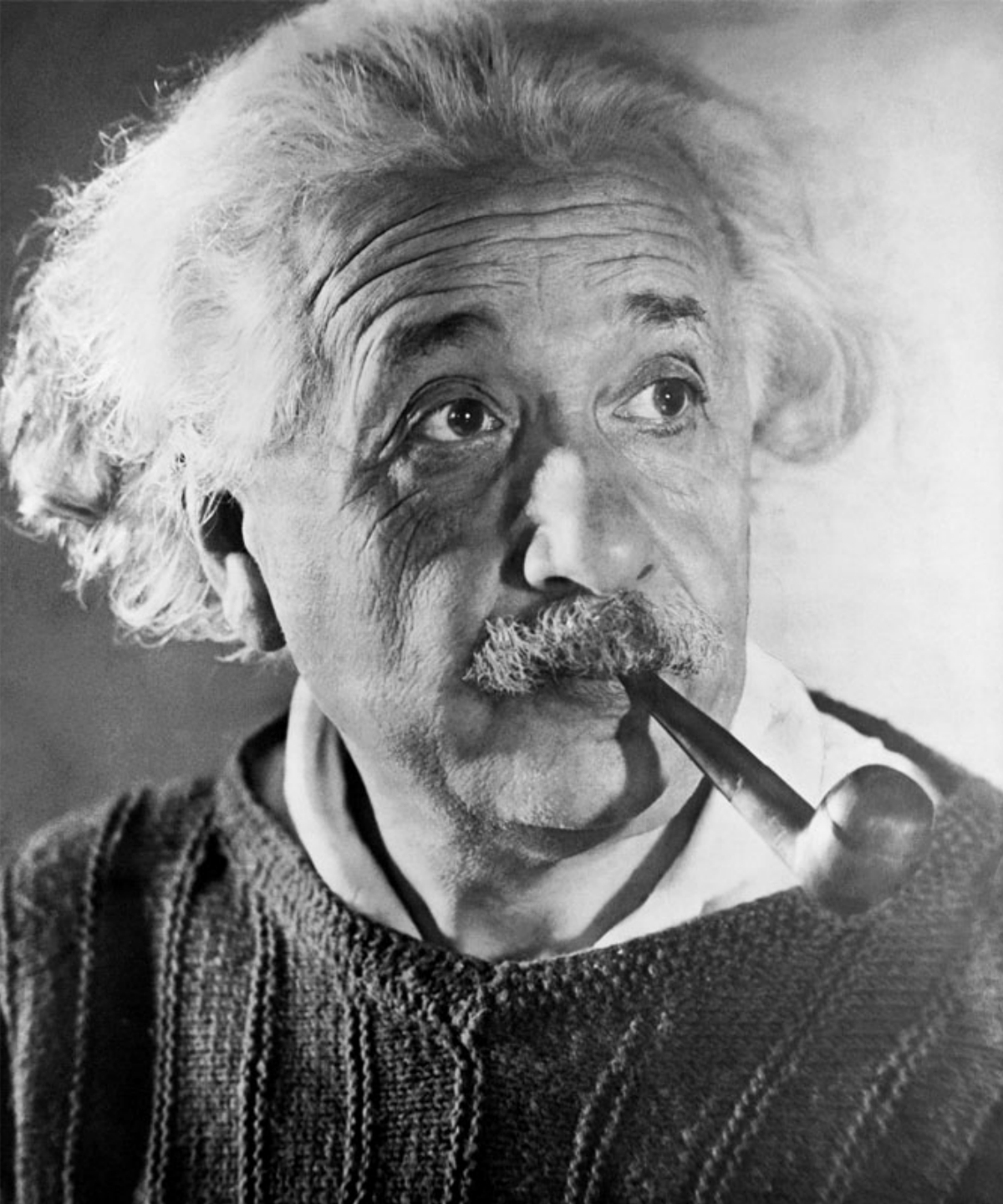
MEASUREMENT

Bob

0

1





1935年

EPRの逆理

Einstein,
Podolsky,
Rosen

1935年のアインシュタインのEPR論文 エンタングルメントの発見

□ 「神はサイコロを振らない」

アインシュタインが、量子論に懐疑的だったことは、よく知られていると思う。量子論の否定は、現在の我々の目から見れば、明らかに、アインシュタインの「誤り」と言っているものだ。

□ 1935年に、アインシュタインとポドルスキーとローゼンは、概略、次の論文を発表する。(三人の著者の頭文字をとって、EPR論文と呼ばれる。) **彼が、次の論文で量子論の中に見つけた「矛盾」は、当時の物理学者の誰も気がつかなかった深いものだった。**

□ "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete ?" 「物理的な実在の量子力学の記述は、完全なものと考えられることができるか？」 <https://goo.gl/qAWacP>

EPR論文を報ずる1935年のニューヨークタイムズ紙

EINSTEIN ATTACKS QUANTUM THEORY

Scientist and Two Colleagues
Find It Is Not 'Complete'
Even Though 'Correct.'

SEE FULLER ONE POSSIBLE

Believe a Whole Description of
'the Physical Reality' Can Be
Provided Eventually.

1935年のアインシュタインのEPR論文 エンタングルメントの発見

- アインシュタインが発見した、量子力学の「矛盾」を、「EPRパラドックス」という。これに「エンタングルメント」という名前をつけたのは、シュレディンガーらしい。
 - 今日では、エンタングルメントは、パラドックスどころか、量子論の基礎を構成するもっとも基本的な前提となっている。
 - ただ、このエンタングルメントという奇妙な現象を、誰よりも先に発見したのは、他ならぬアインシュタインであったことは、興味ふかいことである。
-

But in his final attack Einstein pointed to something so deep, so counterintuitive, so troubling, and yet so exciting, that at the beginning of the twenty-first century it has returned to fascinate theoretical physicists. Bohr's only answer to Einstein's last great discovery—the discovery of entanglement—was to ignore it.

Leonard Susskind

1964年 Bellの定理 アインシュタインの「隠れた変数」の否定

ON THE EINSTEIN PODOLSKY ROSEN PARADOX*

J. S. BELL[†]

Department of Physics, University of Wisconsin, Madison, Wisconsin

(Received 4 November 1964)

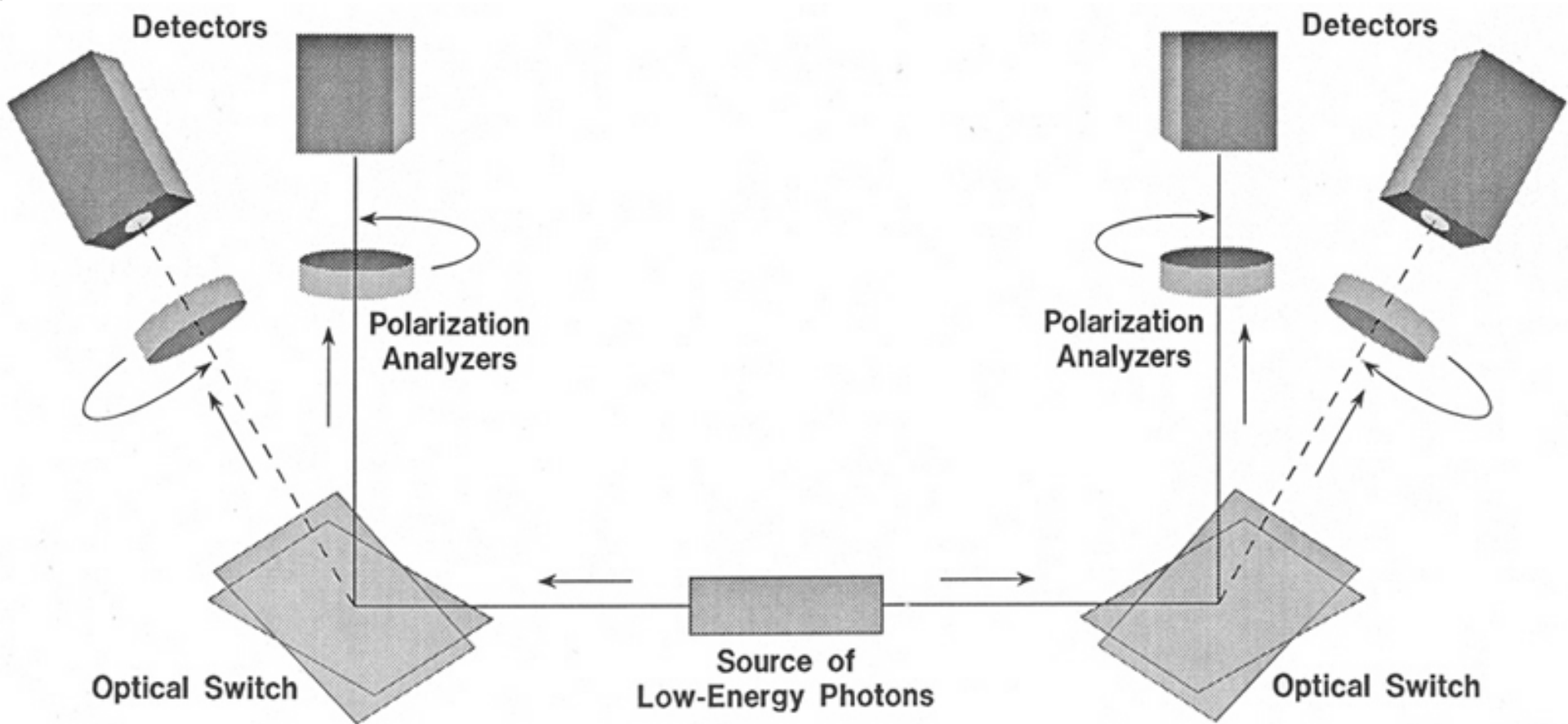
I. Introduction

THE paradox of Einstein, Podolsky and Rosen [1] was advanced as a theory which could not be a complete theory but should be supplemented by additional variables were to restore to the theory causality and locality [2]. In this paper it is mathematically and shown to be incompatible with the statistical predictions of the requirement of locality, or more precisely that the result of a measurement on a system by operations on a distant system with which it has interacted in the past is independent of the difficulty. There have been attempts [3] to show that even without such assumptions no “hidden variable” interpretation of quantum mechanics is possible. This has been examined elsewhere [4] and found wanting. Moreover, a hidden variable theory [5] has been explicitly constructed. That particular interpretation is not a local structure. This is characteristic, according to the result to be proved, that it reproduces exactly the quantum mechanical predictions.



<https://goo.gl/wyv7B>

1982年 Aspectの実験



Bellの定理が成り立っていることの実験での確認

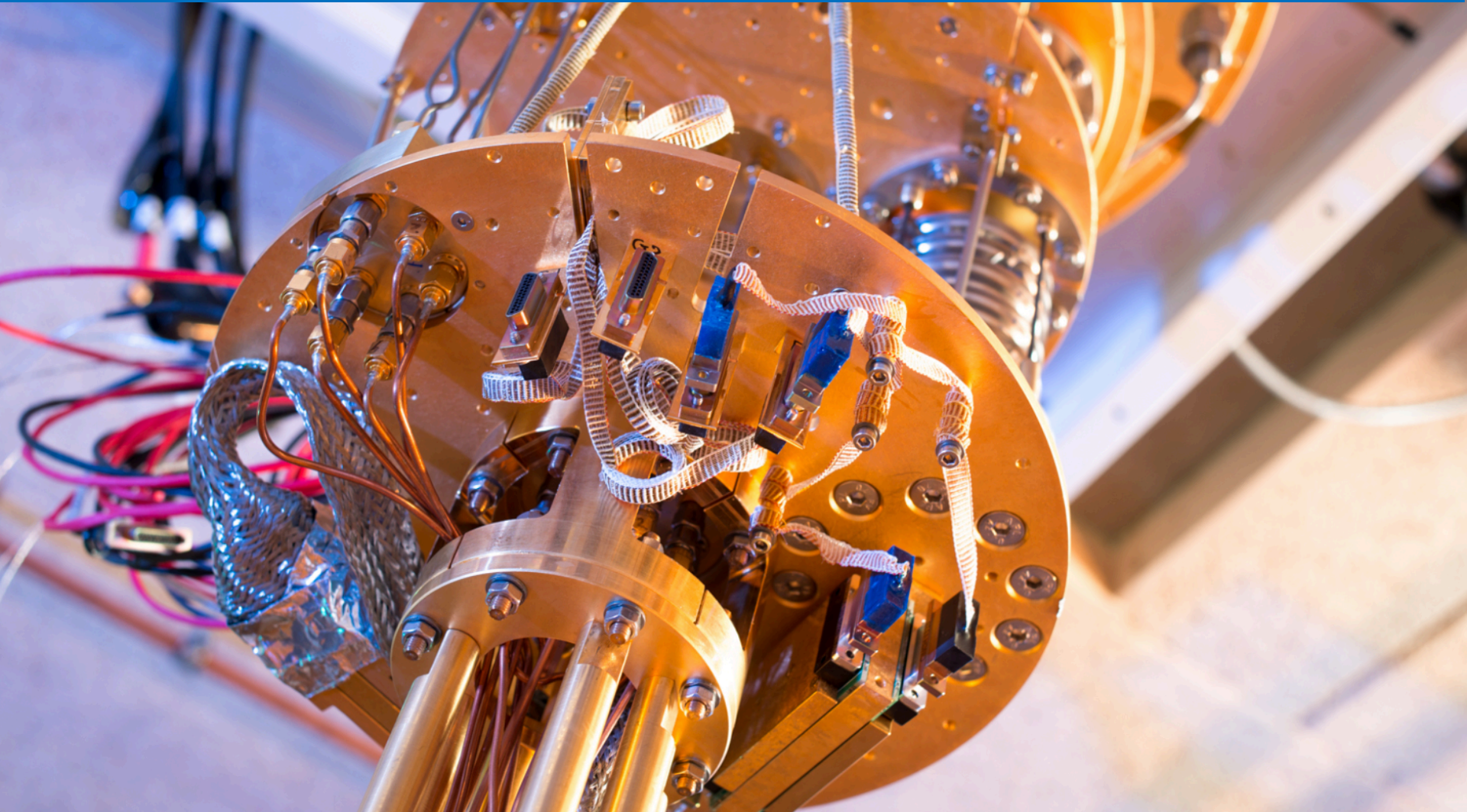
「パラドックス」から
通信の「原理」へ

量子通信
量子テレポーテーション

http://www.sciencenews.org/view/feature/id/65060/description/Everyday_Entanglement

Part II

量子コンピュータの理論的可能性



量子コンピュータの理論的可能性

「量子コンピュータ」は、今から約30年前のファインマンの洞察を発端とする。ドイッチェがそれを定式化し、それが現在のコンピュータの限界を超えうることを明確に示した。ただ、「量子コンピュータ」が広く注目され研究者が爆発的に増大したのは、Shorが、量子コンピュータによる素因数分解のアルゴリズムを発見してからであった。

計算の複雑性の議論は、現在の量子情報理論の中心問題の一つとして、活発な研究が続けられている。

計算の原理的可能性 Church-Turingの提言

計算量の大小とは独立に、どうやっても計算出来ない問題が存在する。また、計算には、いろいろなスタイルがあるのだが、それらは、共通の数学的特徴を持つことが発見された。こうした数学的な特徴を、「計算可能性」として定義しようと言うのが、「Church-Turingの提言」である。



Church–Turing thesis

Wiki

http://en.wikipedia.org/wiki/Church%E2%80%93Turing_thesis

1943年 Kleene

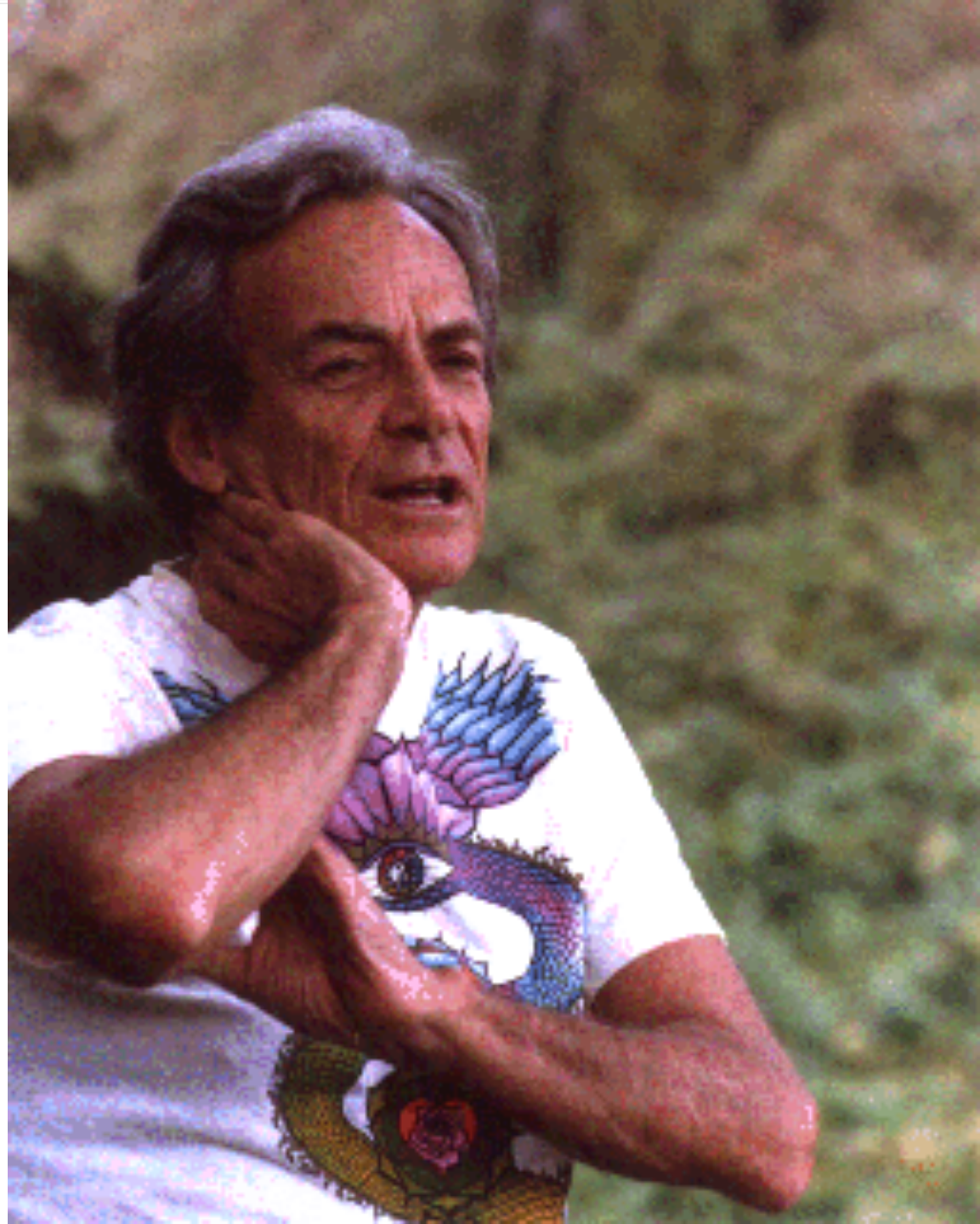
“Recursive Predicates and Quantifiers”

Kleene proposes Church's Thesis

- “一般帰納関数は、実効的に計算可能である”というこの経験的な事実は、Churchを次のようなテーゼの記述に導いた。
同じテーゼは、チューリングの計算機械の記述のうちにも、暗黙のうちに含まれている。
 - “THEESIS I. *全ての実効的に計算可能な関数(実効的に決定可能な述語)*は、一般帰納関数である。”
-

ファインマンの 洞察

1982年



Simulating Physics with Computers

1982年 Richard P. Feynman

<http://www.cs.berkeley.edu/~christos/classics/Feynman.pdf>

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。



ドイッチェ

新しい原理の
確立

1985年

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

1985年 David Deutsch

http://www.cs.berkeley.edu/~christos/classics/Deutsch_quantum_theory.pdf

Church-Turing-Deutsche Thesis

- Church-Turingの仮説の基礎には、暗黙の物理学的主張があることが考察される。
この物理学的主張は、次のような物理学の原理として、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。」
 - 古典物理学と万能チューリング・マシンは、前者は連続的で後者は離散的であるので、この原理には従っていない。
-

万能量子コンピューター

- 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が記述され、量子論と、この「万能量子コンピューター」が、先の原理と両立可能であることが示される。
 - この万能量子コンピューターをまねた計算機械は、原理的には、構築可能である。そしてそれは、いかなるチューリング・マシンによっても再生不可能な、多くの目覚ましい特徴を持つであろう。
-

Quantum Parallelism

- これらの中には、非帰納的な計算は含まれていない。しかし、「量子並行計算」が含まれる。その方法によれば、古典的な制限の下でのコンピューターよりはるかに高速に、ある種の確率論的問題を万能量子コンピューターが実行出来る。
 - こうした特質の直観的な説明は、エヴェレット以外の量子論の解釈ではすべて、堪え難い緊張をもたらす。
-

The theory of computation has traditionally been studied almost entirely in the abstract, as a topic in pure mathematics. This is to miss the point of it. Computers are physical objects, and computations are physical processes. What computers can or cannot compute is determined by the laws of physics alone, and not by pure mathematics.

-- David Deutsch

Like mathematics, computer science will be somewhat different from the other sciences, in that it deals with artificial laws that can be proved, instead of natural laws that are never known with certainty.

-- Donald Knuth

DAVID DEUTSCH'S **MULTIVERSE**

ドイッチェは、物理学者としては、エベレットとともに、量子力学の多世界解釈(「パラレル・ワールド」=並行宇宙論)の熱心な提唱者として知られていた。

現在でも、そうした立場は変わっていないようである。彼は量子コンピュータが超並行計算を可能にすることをMultiverseで説明している。

ちなみに、D-Wave社のblogページは、“Hack The Multiverse”と名付けられている。



Our Universe is just one of many. David Deutsch believes this Multiverse view of reality could hold the future of computing.

量子コンピューターは、パラレル宇宙の間の
コラボレーションに、有用な仕事を実行させる
ことを可能にする最初のテクノロジーになる
であろう。

- David Deutsch @ TED



ショア

量子コンピュータによる
素因数分解アルゴリズム
の発見

1994年



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

1995年 Peter W. Shor

<http://arxiv.org/pdf/quant-ph/9508027v2.pdf>

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 by 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 which 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.



A Venn diagram illustrating the hierarchy of complexity classes. It consists of a large outer oval labeled 'NP-hard' at the top. Inside this oval is a smaller oval labeled 'NP-complete'. Within the 'NP-complete' oval is a smaller region labeled 'NP'. At the bottom of the 'NP' region is a small wedge-shaped area labeled 'P'. The diagram shows that P is a subset of NP, which is a subset of NP-complete, which is a subset of NP-hard.

NP-hard

**NP-
complete**

計算の複雑性の理論と量子情報理論

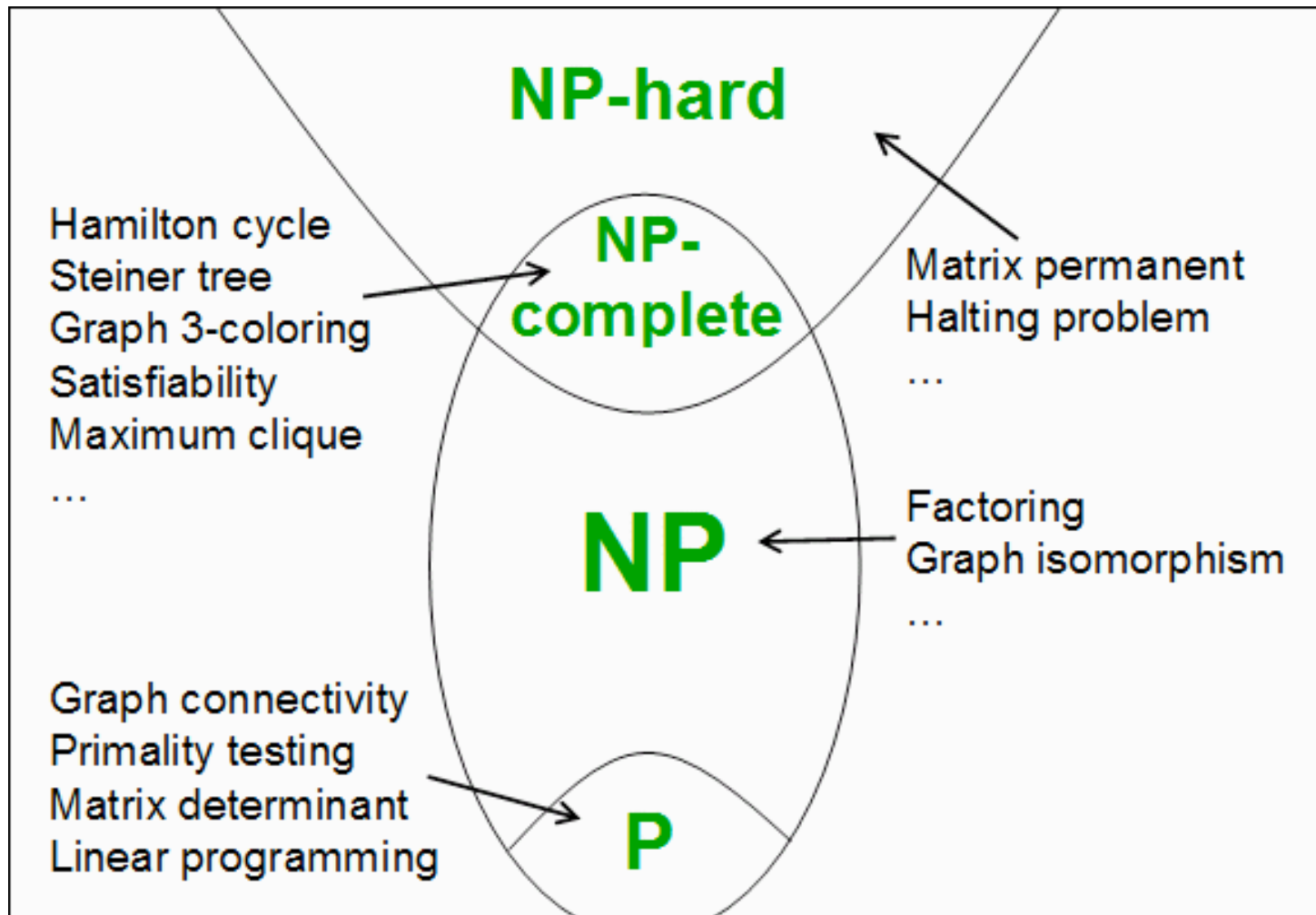
NP

P

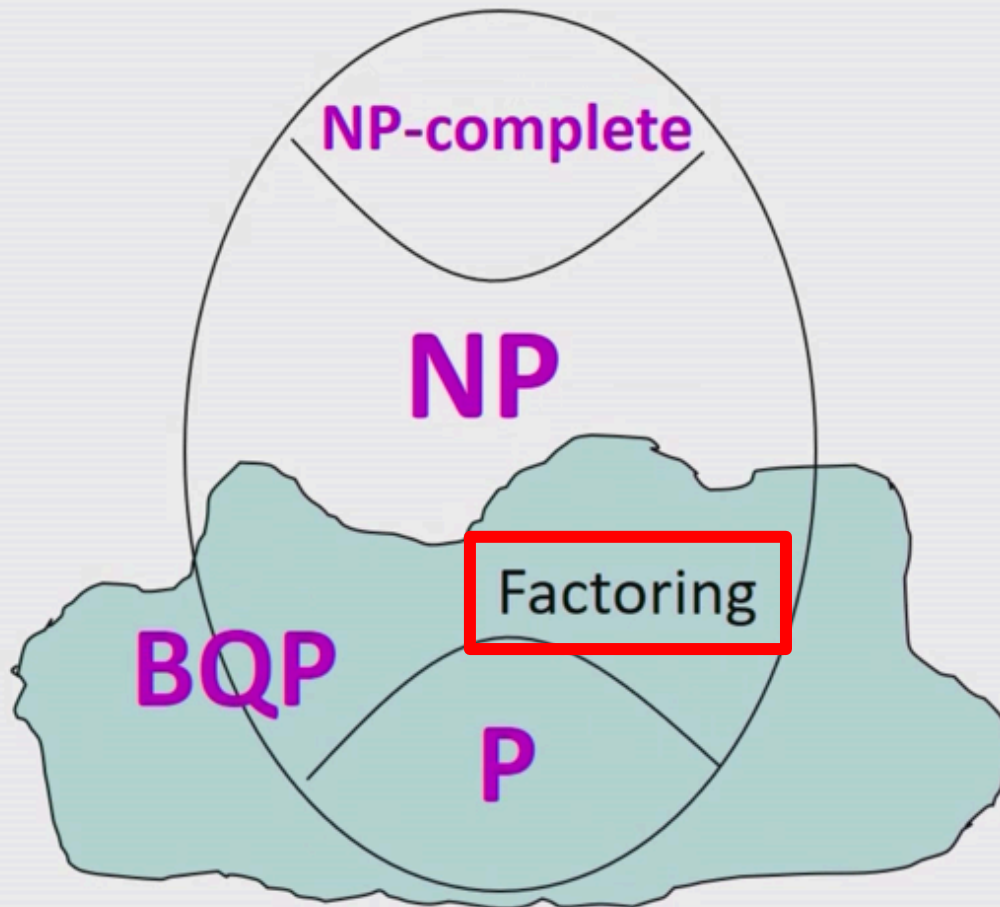
計算量の理論 $P \neq NP$ 予想

- Pは、多項式時間でTuringマシンで解ける問題。
- NP(Nondeterministic Polynomial)は、その答えがYESなら、そのチェックが多項式時間で解ける問題。
- $n=pq$ なる素数 p, q を求める問題は、NP問題である。
 n と同時に p あるいは q が与えられた時、それが条件を満たすかのチェックは、すぐに出来るから。
- 例:
 $127 \times 129 = 29083$
 ~~$? \times ? = 29083$ を満たす?を見つけよ。~~
 127×129 は、29083か? YES!

計算量の理論 $P \neq NP$ 予想

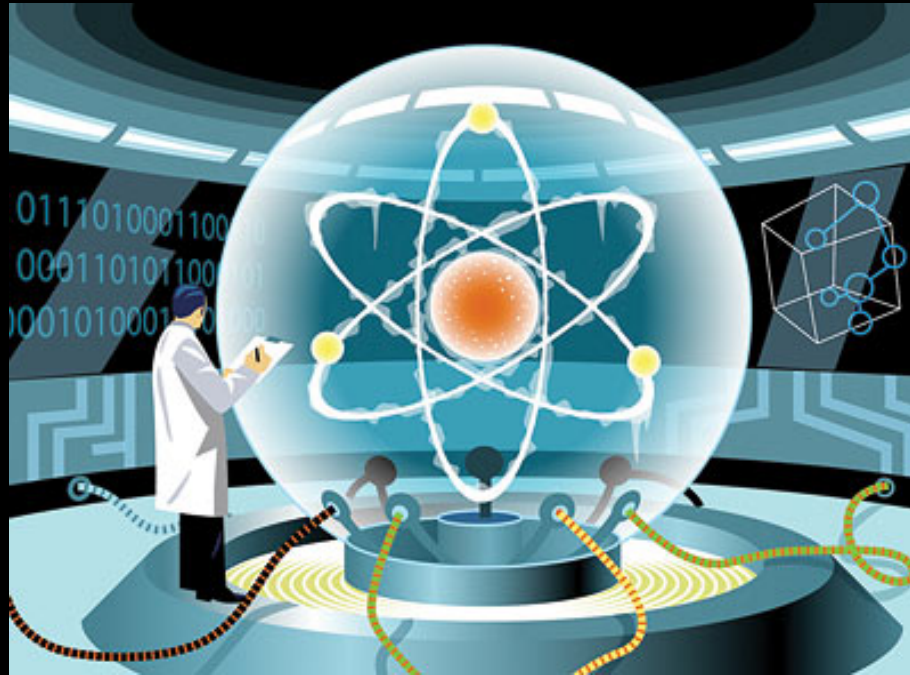


It Isn't A Magic Bullet That Solves All Problems Instantly



"What Quantum Computing Isn't" Scott Aaronson <https://goo.gl/95SpPA>

Quantum Computing and the Limits of the Efficiently Computable



Scott Aaronson

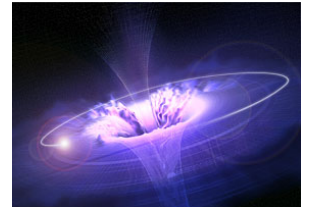
MIT

<https://goo.gl/fcRSx2>

Computational Complexity and the Black-Hole Information Loss Problem

Maybe the single most striking application so far of complexity to fundamental physics

Hawking 1970s: Black holes radiate!

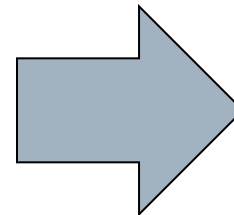
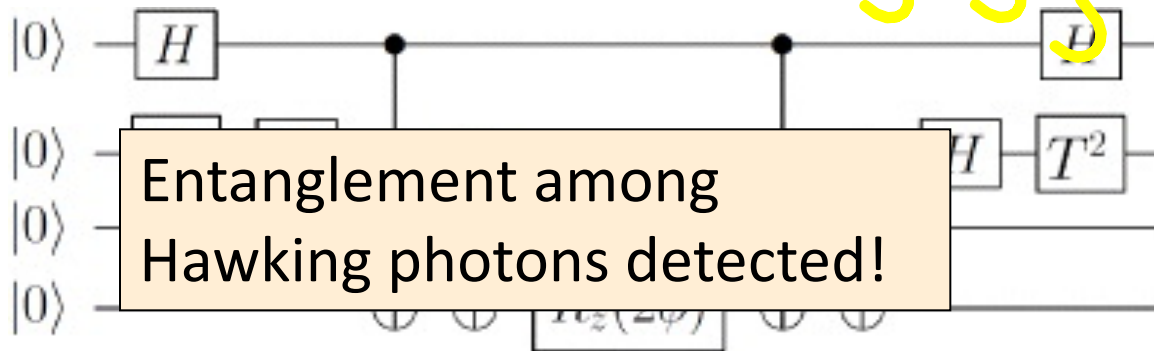


The radiation *seems* thermal (uncorrelated with whatever fell in)—but if quantum mechanics is true, then it can't be

Susskind et al. 1990s: “Black-hole complementarity.” In string theory / quantum gravity, the Hawking radiation should just be a scrambled re-encoding of the same quantum states that are also inside the black hole

The Firewall Paradox [Almheiri et al. 2012]

If the black hole interior is “built” out of the same qubits coming out as Hawking radiation, then why can’t we **do something** to those Hawking qubits (after waiting $\sim 10^{70}$ years for enough to come out), then dive into the black hole, and see that we’ve completely destroyed the spacetime geometry in the interior?



Harlow-Hayden 2013: Sure, there's *some* unitary transformation that Alice could apply to the Hawking radiation, that would generate a “firewall” inside the event horizon. But **how long** would it take her to apply it?

Plausible answer: Exponential in the number of qubits inside the black hole! Or for an astrophysical black hole,

$$\sim 2^{10^{70}} \text{ years}$$

She wouldn't have made a dent before the black hole had already evaporated anyway! So ... problem solved?

HH's argument: If Alice could achieve (a plausible formalization of) her decoding task, then she could also break collision-resistant hash functions—beyond what even QCs seem able to do

Recently, I strengthened the HH argument, to show that Alice could even invert arbitrary one-way functions

Conclusion

Any one of these would make me as happy as low-energy SUSY would make you:

Prove $P \neq NP$

Prove that not even quantum computers can solve NP-complete problems

Build a scalable quantum computer

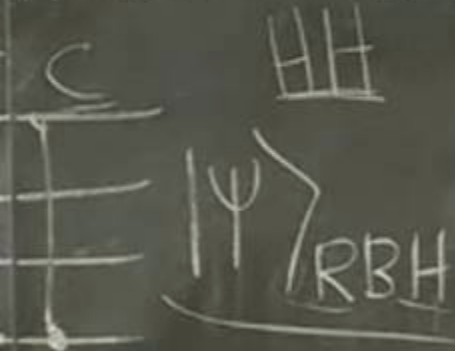
(or even more interesting, show that it's impossible)

Clarify whether all of known physics can be simulated by a quantum computer

Use No-SuperSearch or related impossibility principles to make progress in quantum gravity



HAYDEN ARGUMENT



$$\rho_{BH} = I_{BH}$$

Size (#gates)
 $\leq n^{O(1)}$

$\exists$ 1 qubit of
distillable entanglement
between R & B

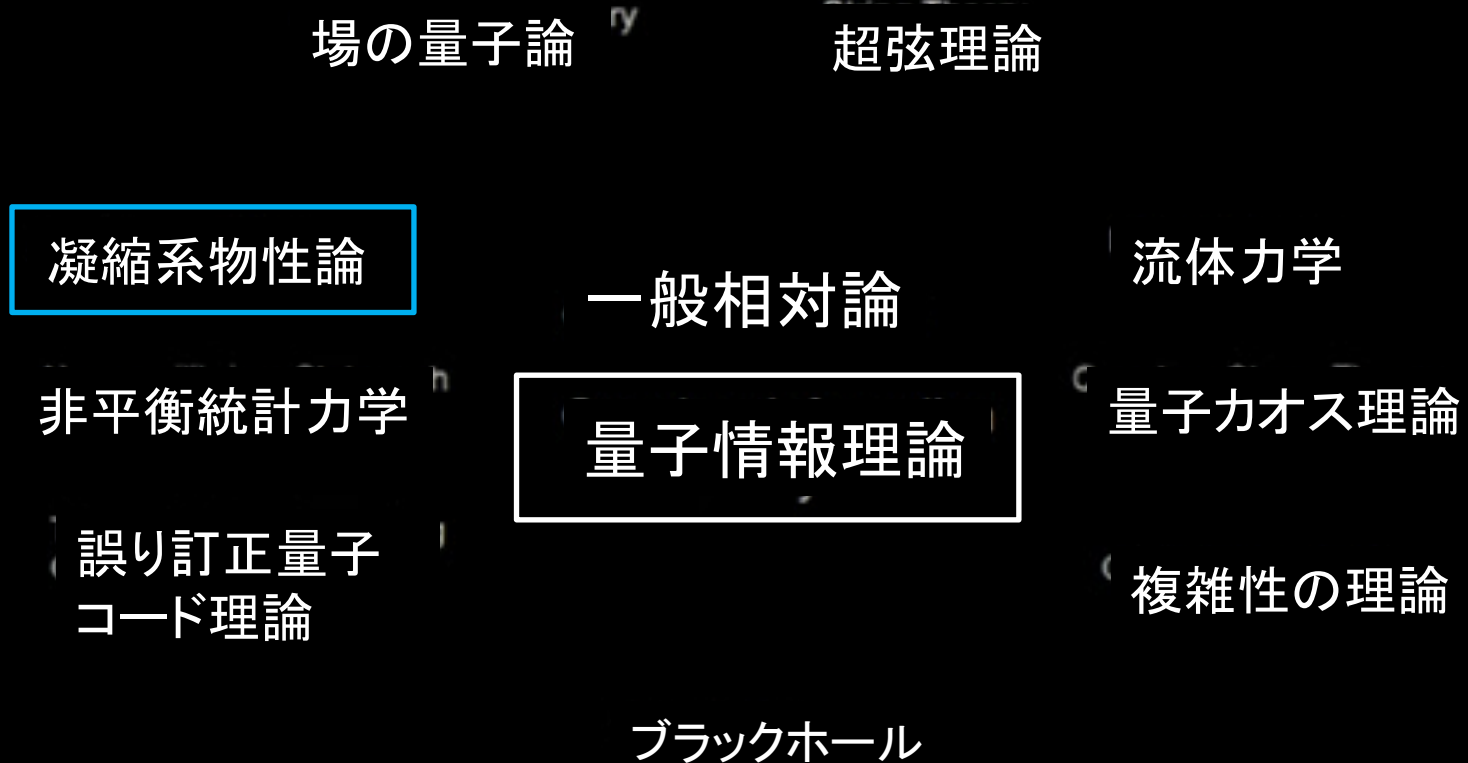
Alice's task

Apply U_R to R
so that



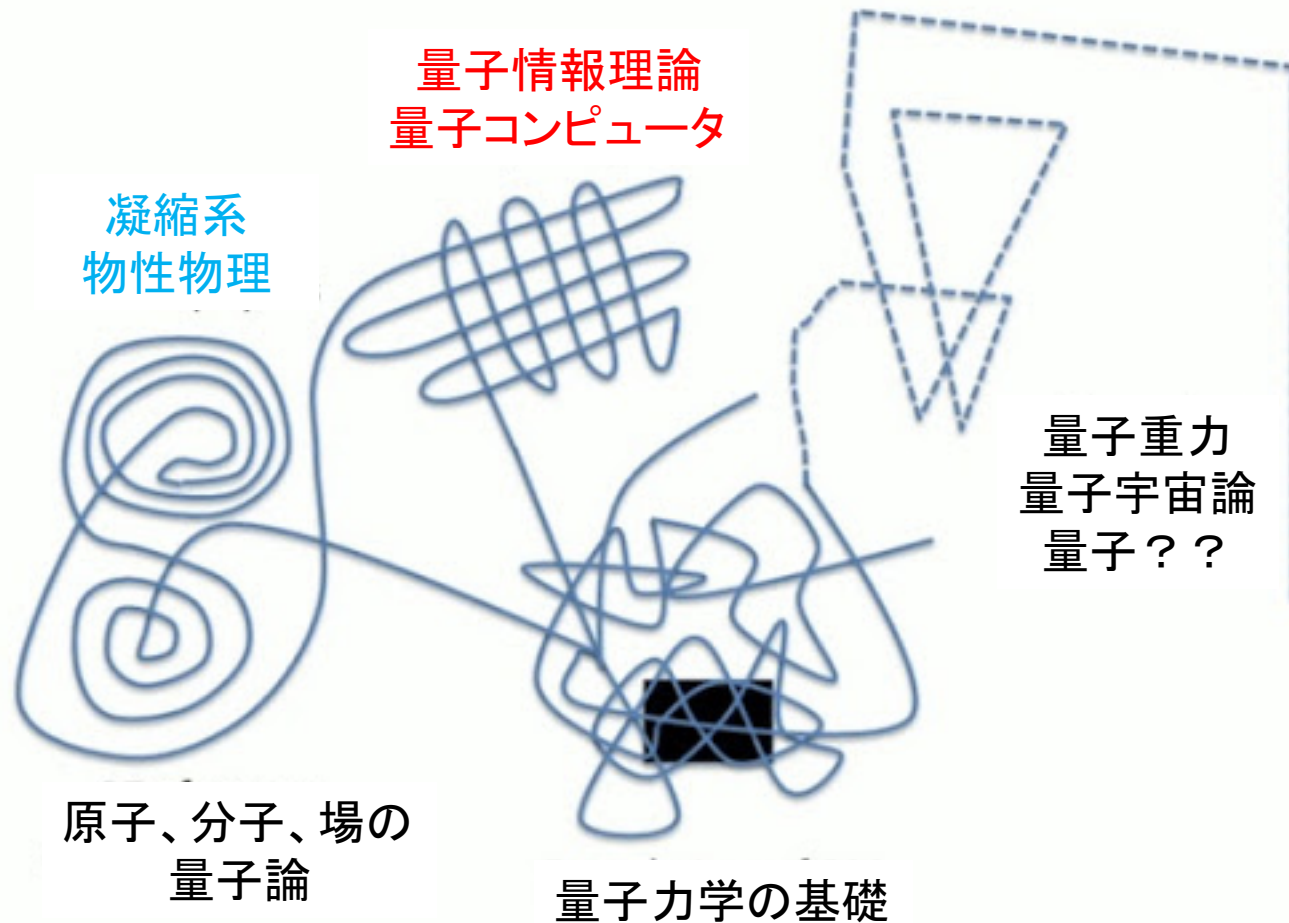
Leonard Susskind

現代物理学の俯瞰図 by Susskind



Susskind "Entanglement and Complexity: Gravity and Quantum Mechanics"
<https://goo.gl/J0wSkf>

エンタングルメントの歴史の絵解き



"Our Quantum Society: Living with Entanglement" <https://goo.gl/aWtAzi>
Cathryn Carson <https://goo.gl/j7bE57>

量子多体系の物理

(場の理論、物性理論、統計力学、可解系)

AdS/CFT
(ホログラフィー)



重力理論
(超弦理論)

量子エンタングルメント
テンソルネットワーク

量子情報理論
(情報幾何)

HEE



BH情報問題

高柳匡 「重力理論と量子エンタングルメント」

<https://goo.gl/kRPcNI>

The Computational Complexity of Linear Optics

Scott Aaronson, Alex Arkhipov

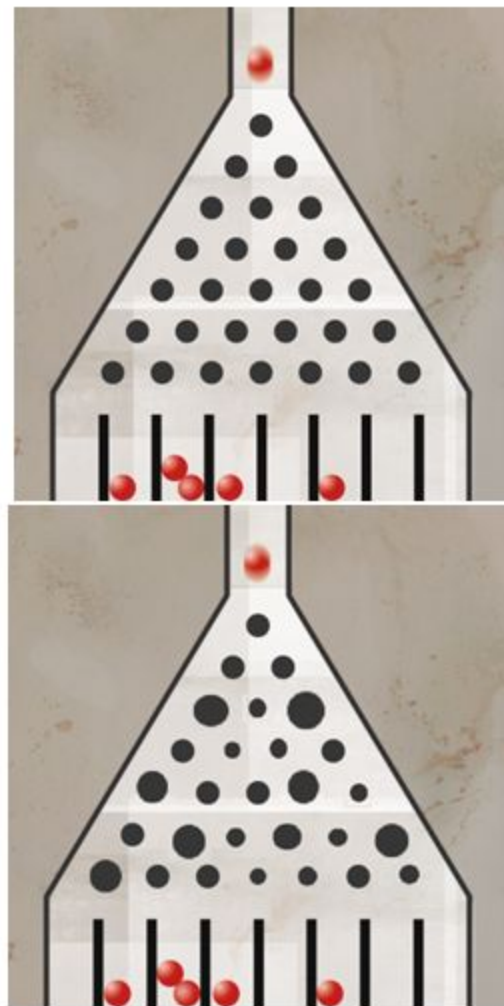
<https://goo.gl/FtXVqw>

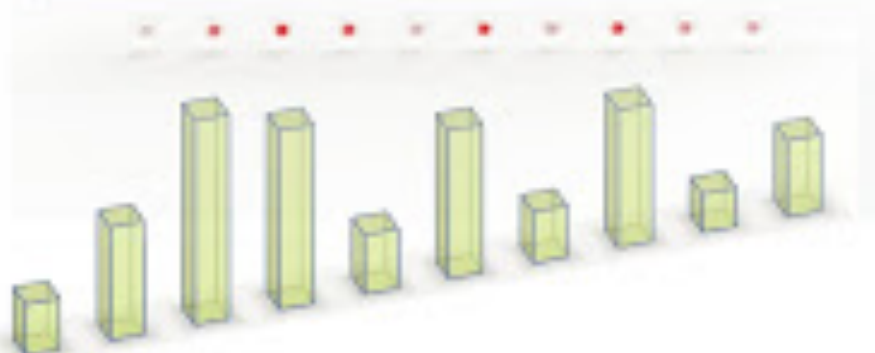
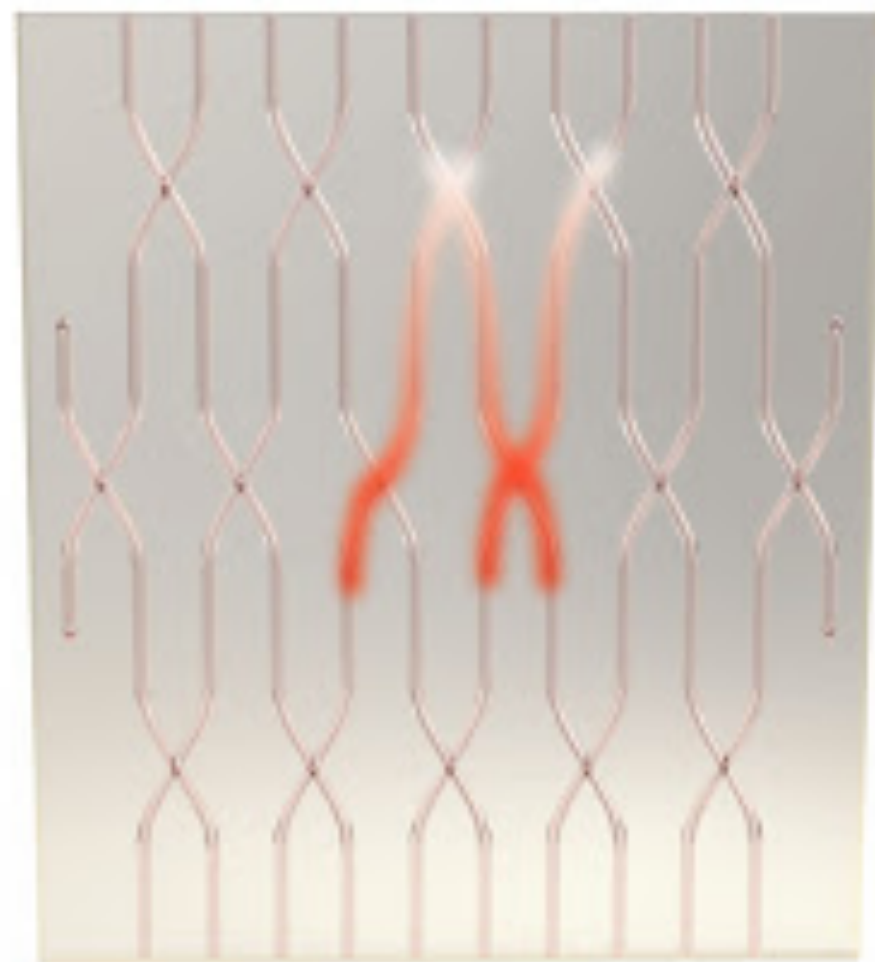
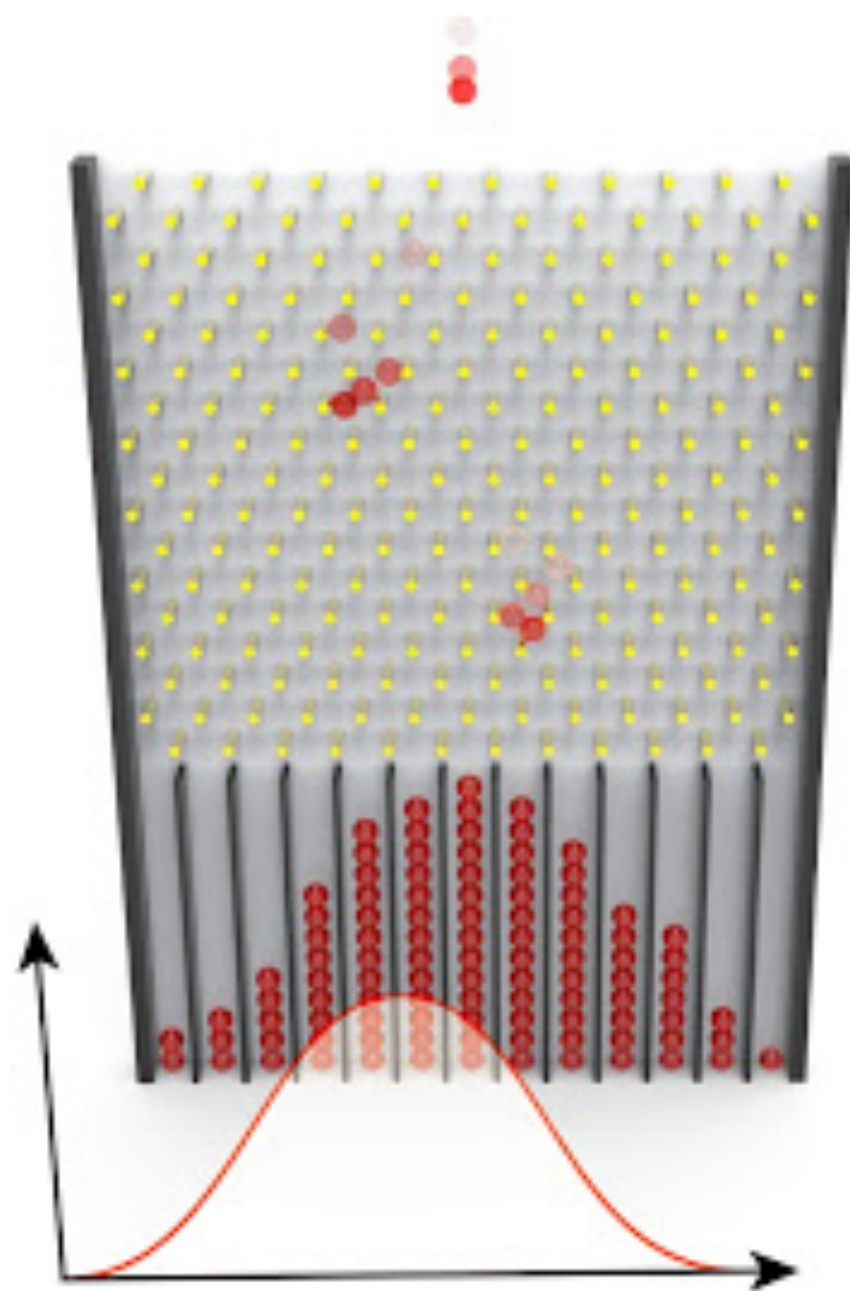
In Proceedings of the 43rd annual ACM symposium on Theory of computing (STOC '11). ACM

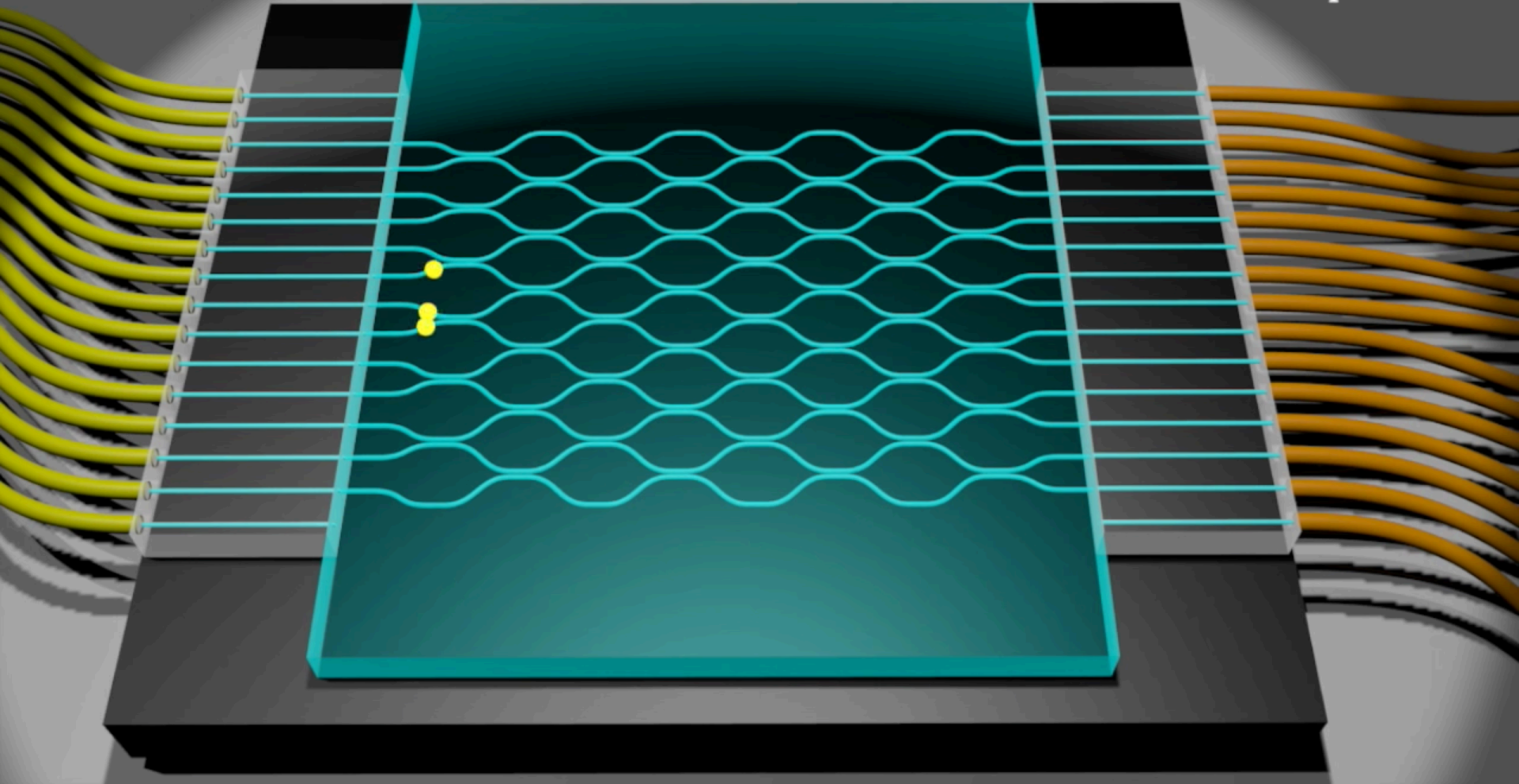
Boson Sampling

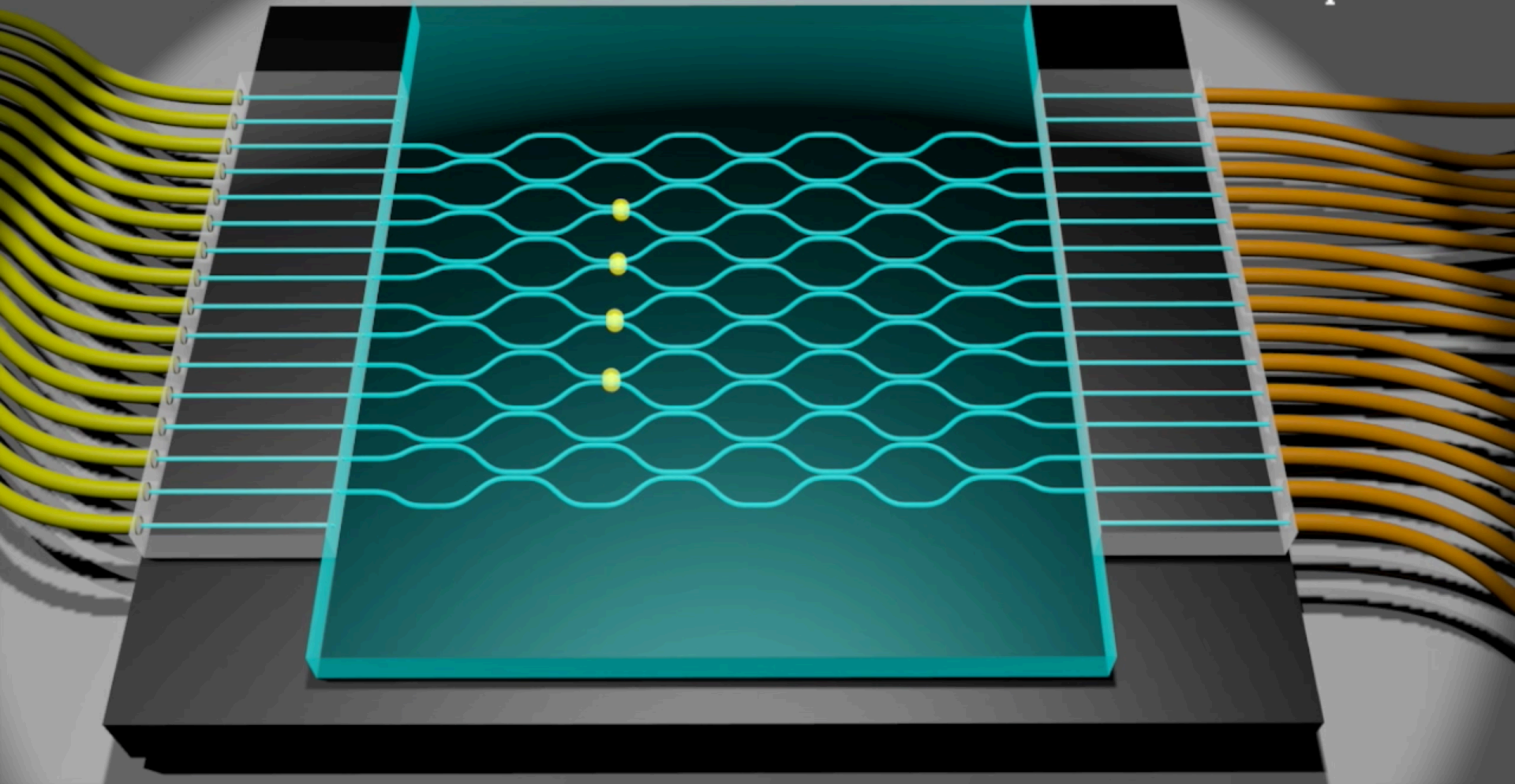
General Idea of Boson Sampling

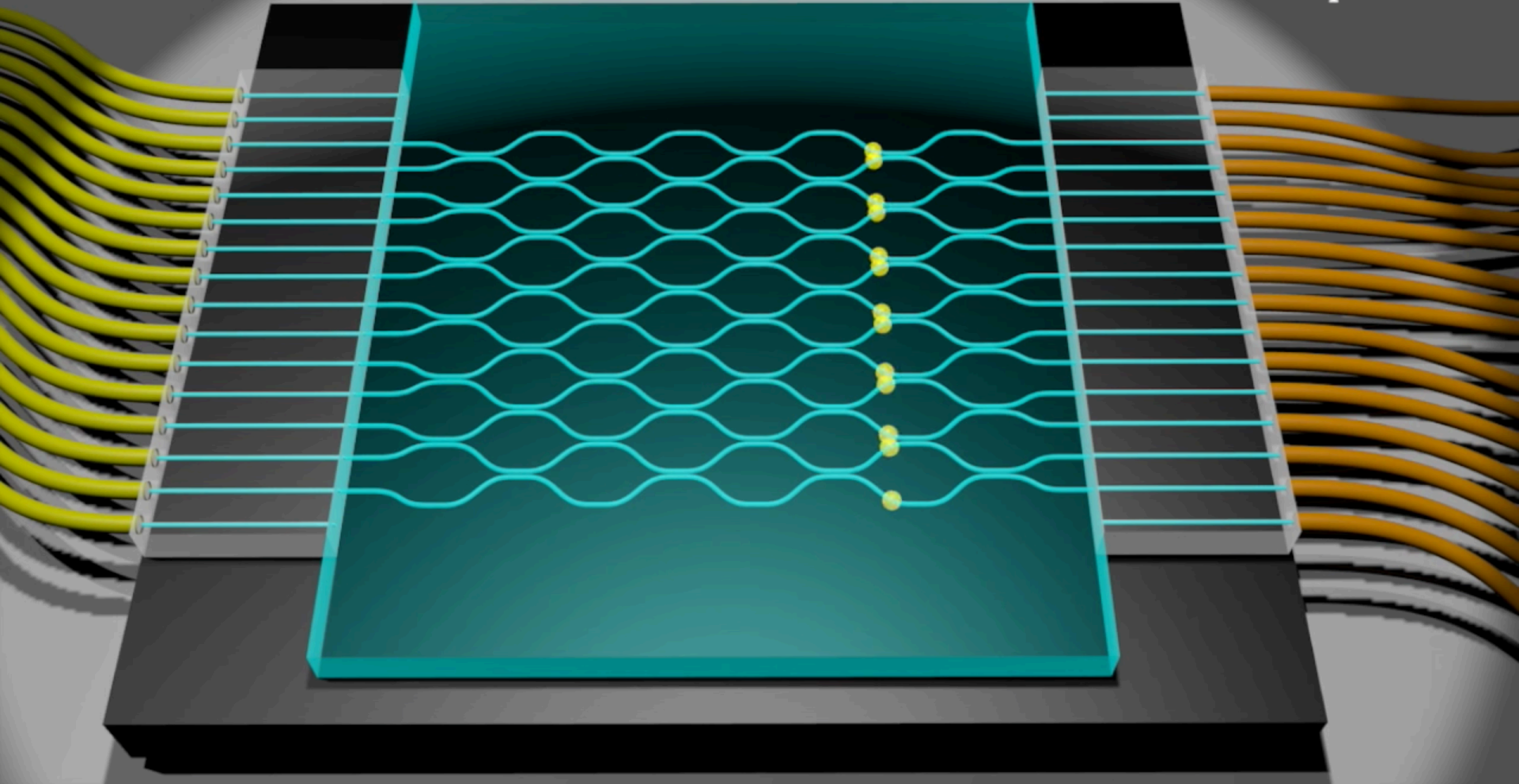
- The idea of boson sampling was proposed in 2011 [1].
 - Uses photons
- Similar to a Galton board, which samples from the binomial distribution.
- By engineering the peg sizes and locations a desired system can be modeled.
- The response is governed by quantum photon statistics.

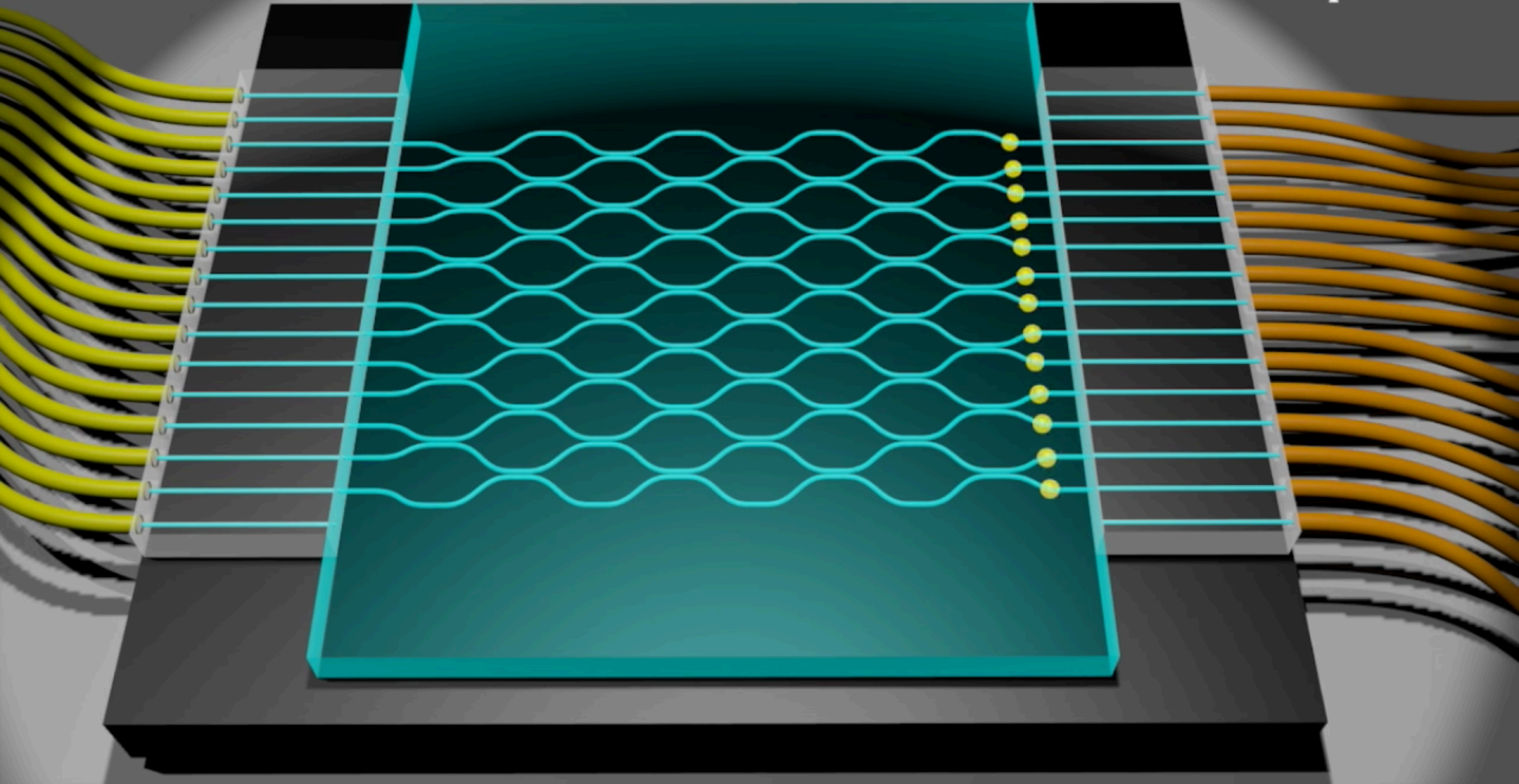






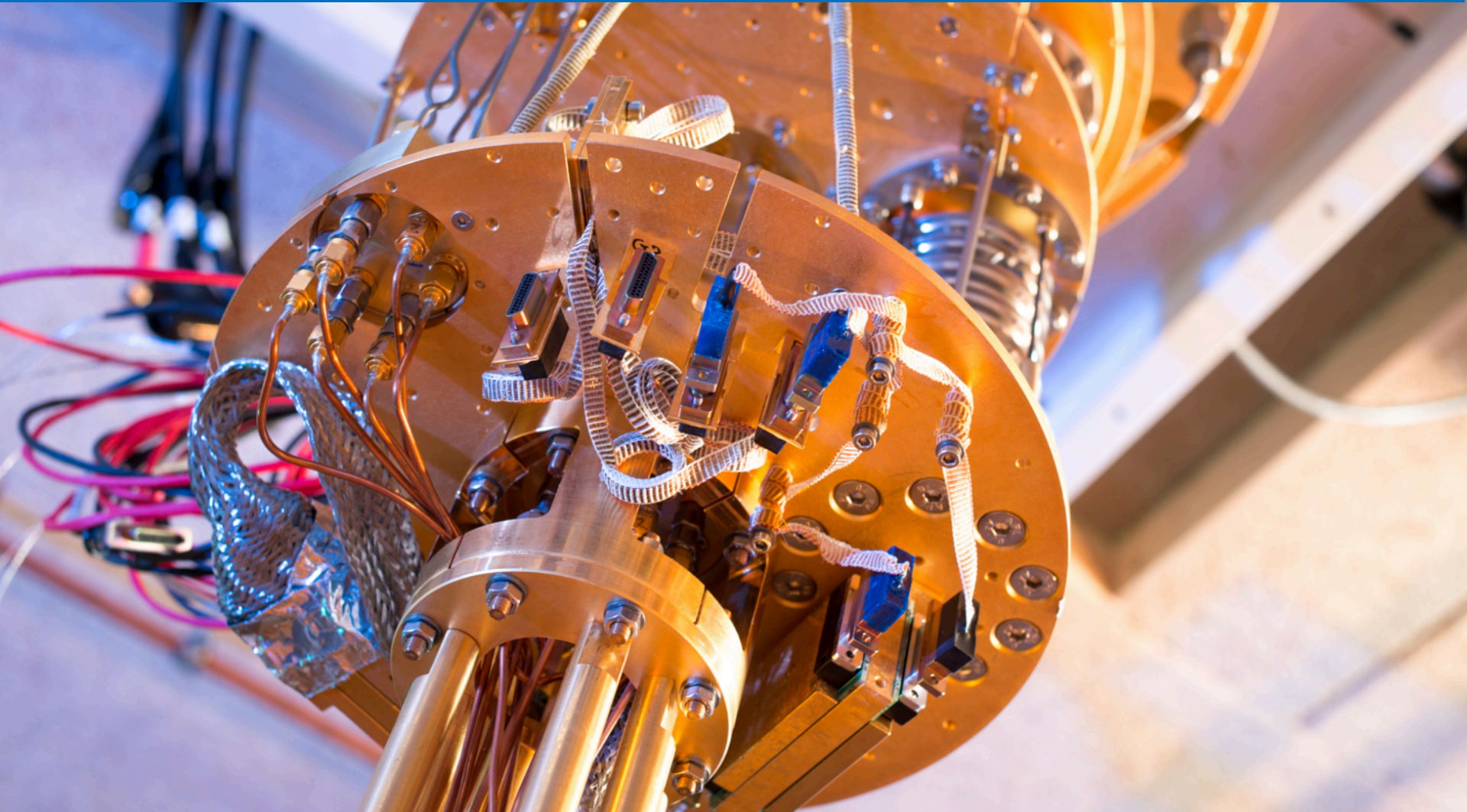






Part III

量子ゲート型量子コンピュータ

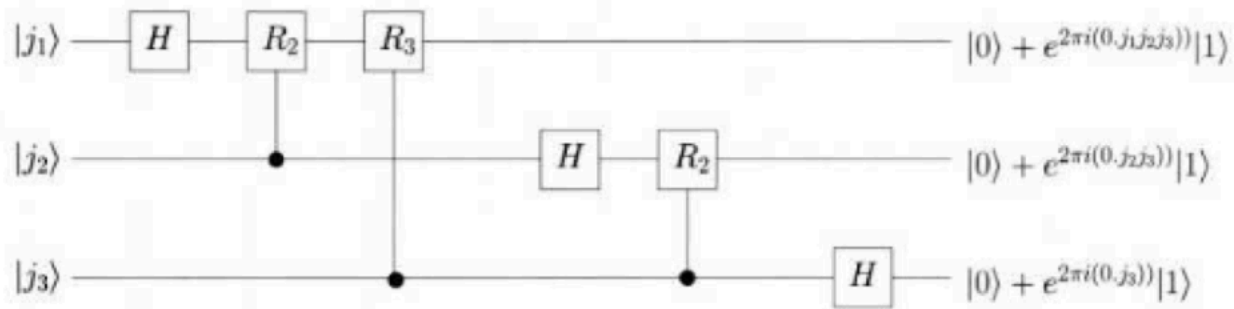


量子ゲート型量子コンピュータ

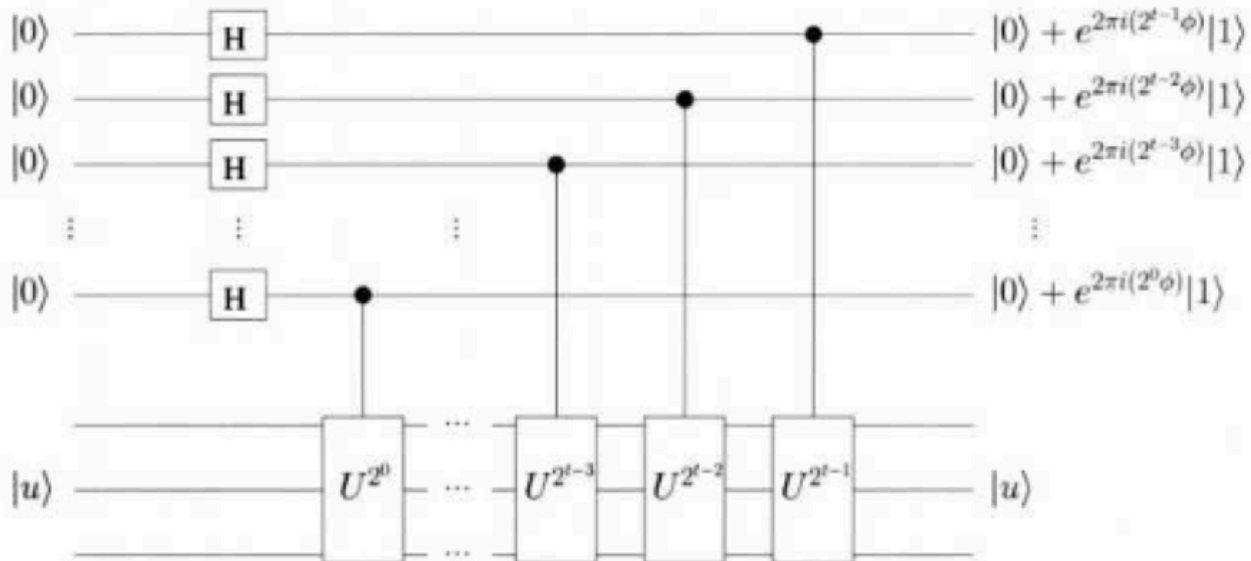
0と1との二つの状態の重ね合わせとしてのqubitの状態の変化は、「ユニタリ」という性質を満たす演算の適用として表現される。

量子ゲート型量子コンピュータは、ユニタリ演算子を一つの量子論理回路(これを「量子ゲート」という)として、コンピュータを構成する。

このアプローチは自然なものだが、実際にそうした回路を構成するのには、難しい。



量子ゲート



量子コンピューターと量子ゲート

これまで、量子コンピュータの実現を目指す研究の主流は、汎用の量子論理回路、量子ゲートの実装とそれを組み合わせたシステムの構築に向けられてきた。

1-qubitの回路



Bit Flipper

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



Phase Flipper

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

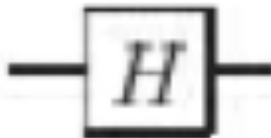
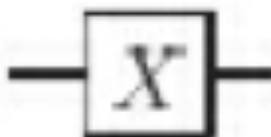
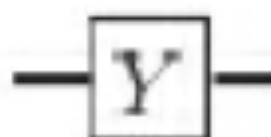
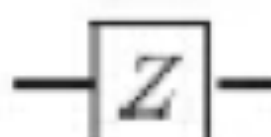
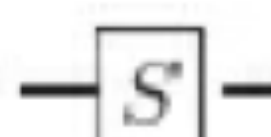
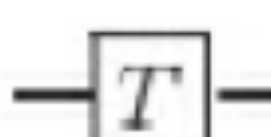


Hadamard

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

Summary of quantum gates

Table of Quantum Gates and what they do				
State	Gate sequence to prepare the state	Transformation on Bloch sphere	Gates to measure in the respective basis	Name of measurement basis
$ 0\rangle$	(none, ground state)	None		Z, "standard"
$ 1\rangle$		π rotation around X		Z, "standard"
$ +\rangle$		π rotation around X + Z	 	X
$ -\rangle$	 	π rotation around X + π rotation around X + Z	 	X

Hadamard		$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Pauli- X		$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli- Y		$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli- Z		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Phase		$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$		$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$

1-qubitの回路に対応する行列

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ とすると、}$$

$$X \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} b \\ a \end{pmatrix}$$

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ とすると、}$$

$$Z \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a \\ -b \end{pmatrix}$$

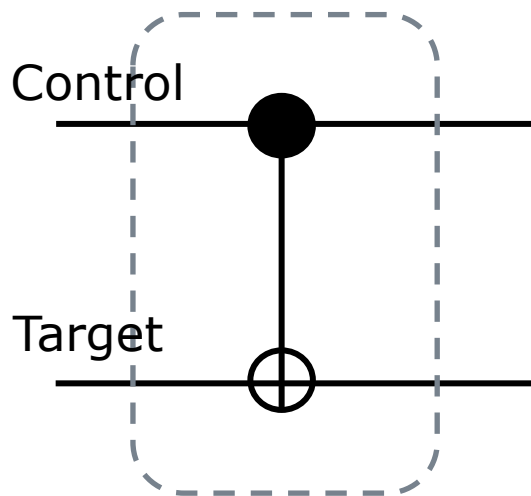
$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \text{ とすると、}$$

$$H \begin{pmatrix} a \\ b \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} a + b \\ a - b \end{pmatrix}$$

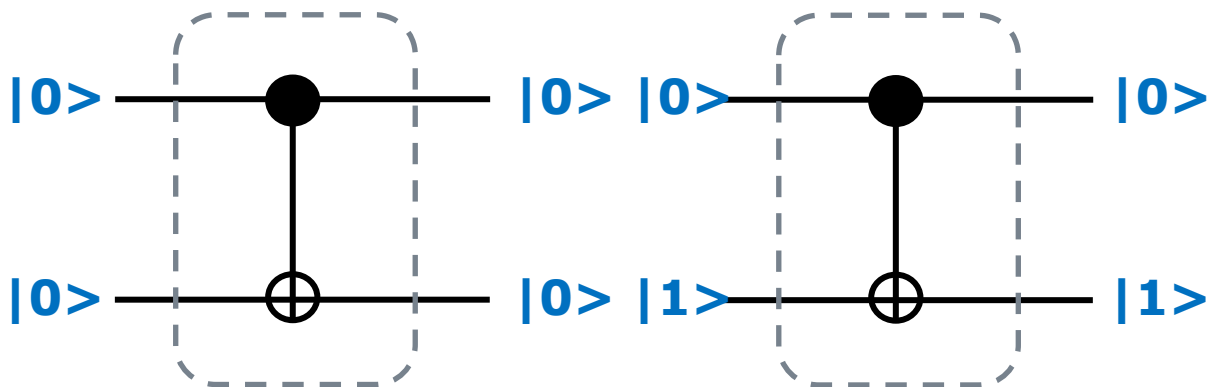
2-qubitの回路

CNOT (Control-NOT)

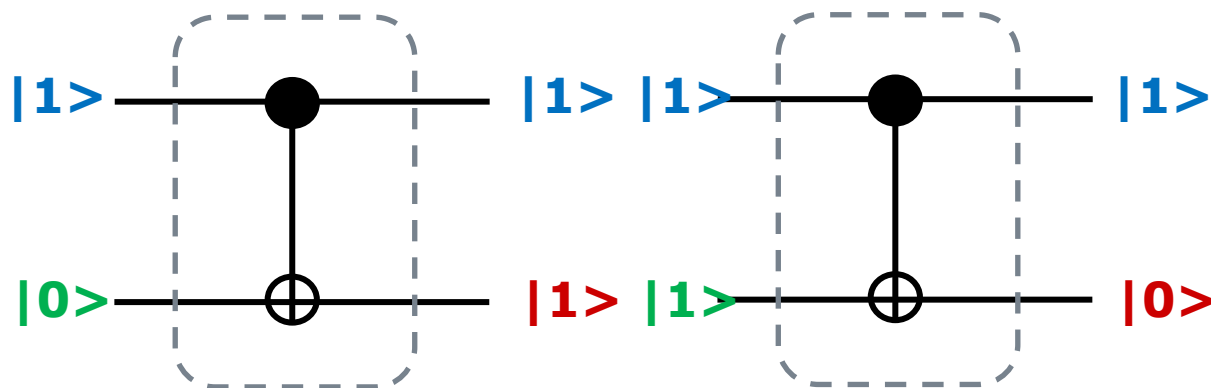
Control が $|1\rangle$ の時
Target のNOTをとる



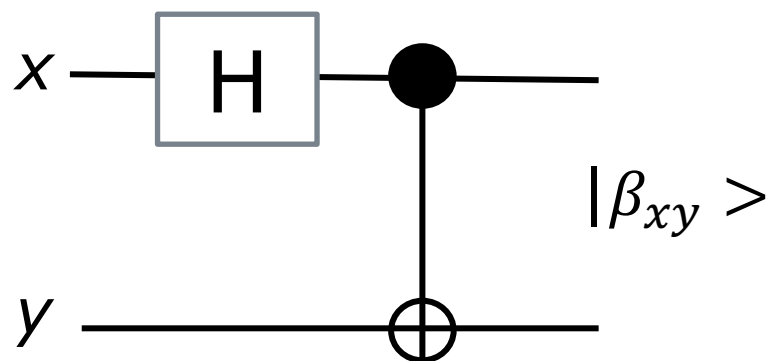
Controlが $|0\rangle$ なら何もしない



Controlが $|1\rangle$ ならNOT操作



2-qubitの回路の例



この回路は、xとyの
Entangle状態を作る！

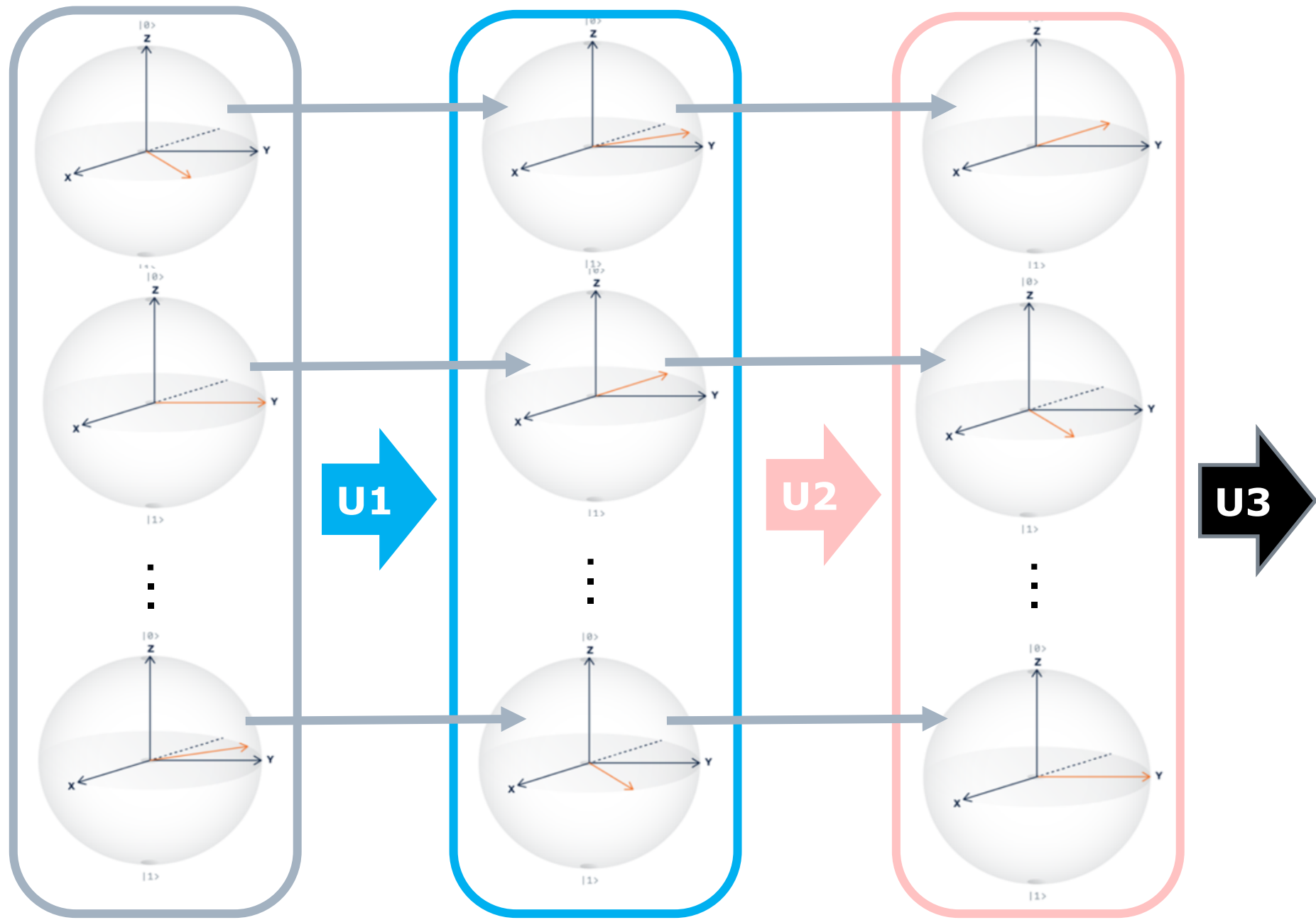
$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}};$$

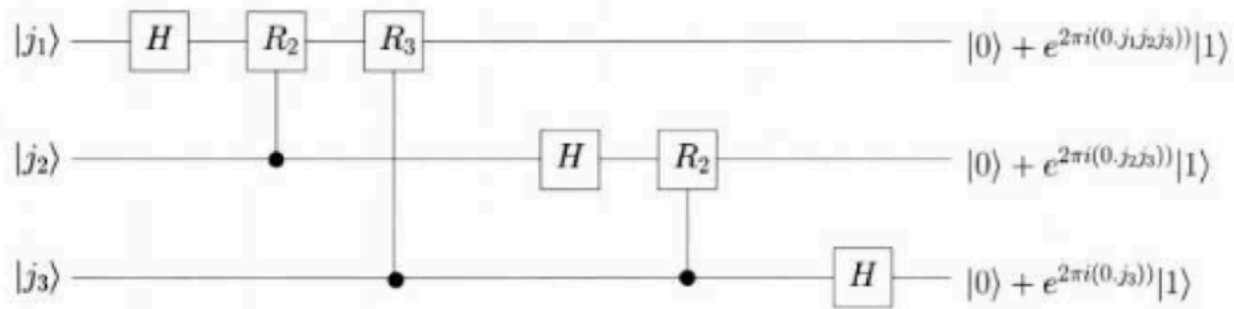
$$|\beta_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}};$$

$$|\beta_{10}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}};$$

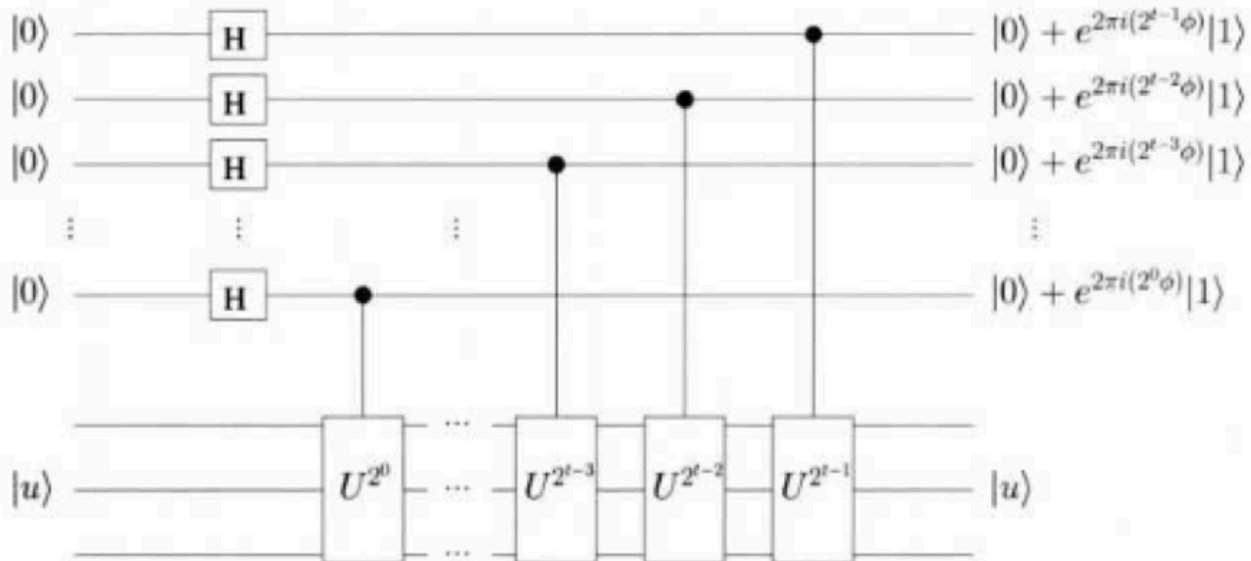
$$|\beta_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}};$$

n-qubit システム





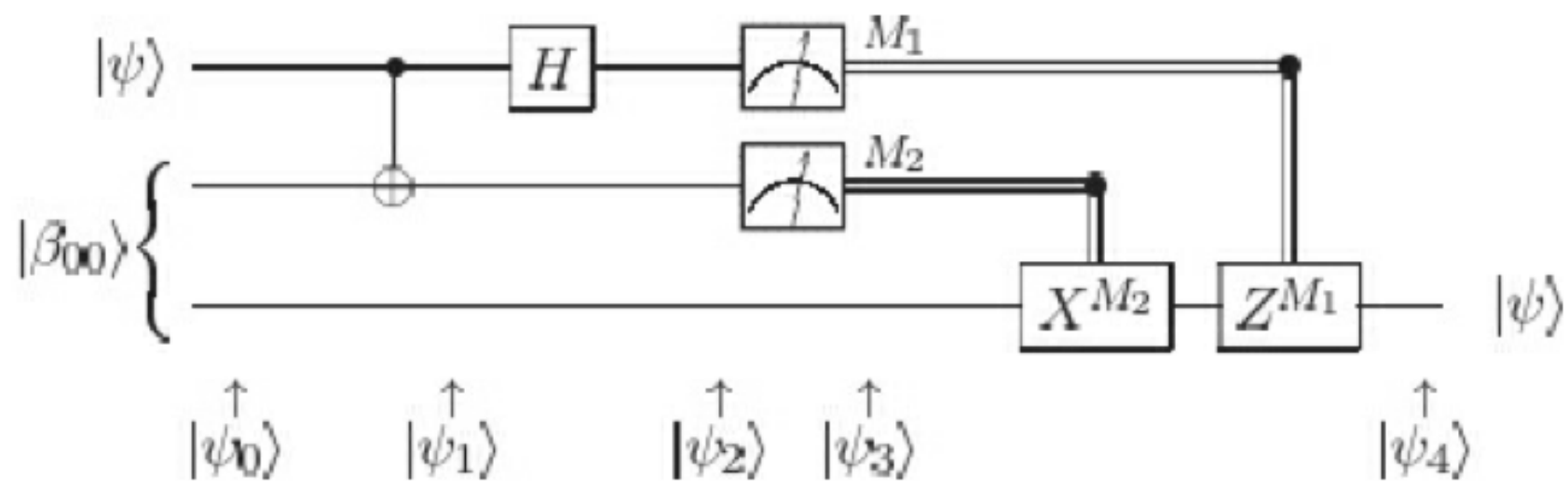
量子アルゴリズム



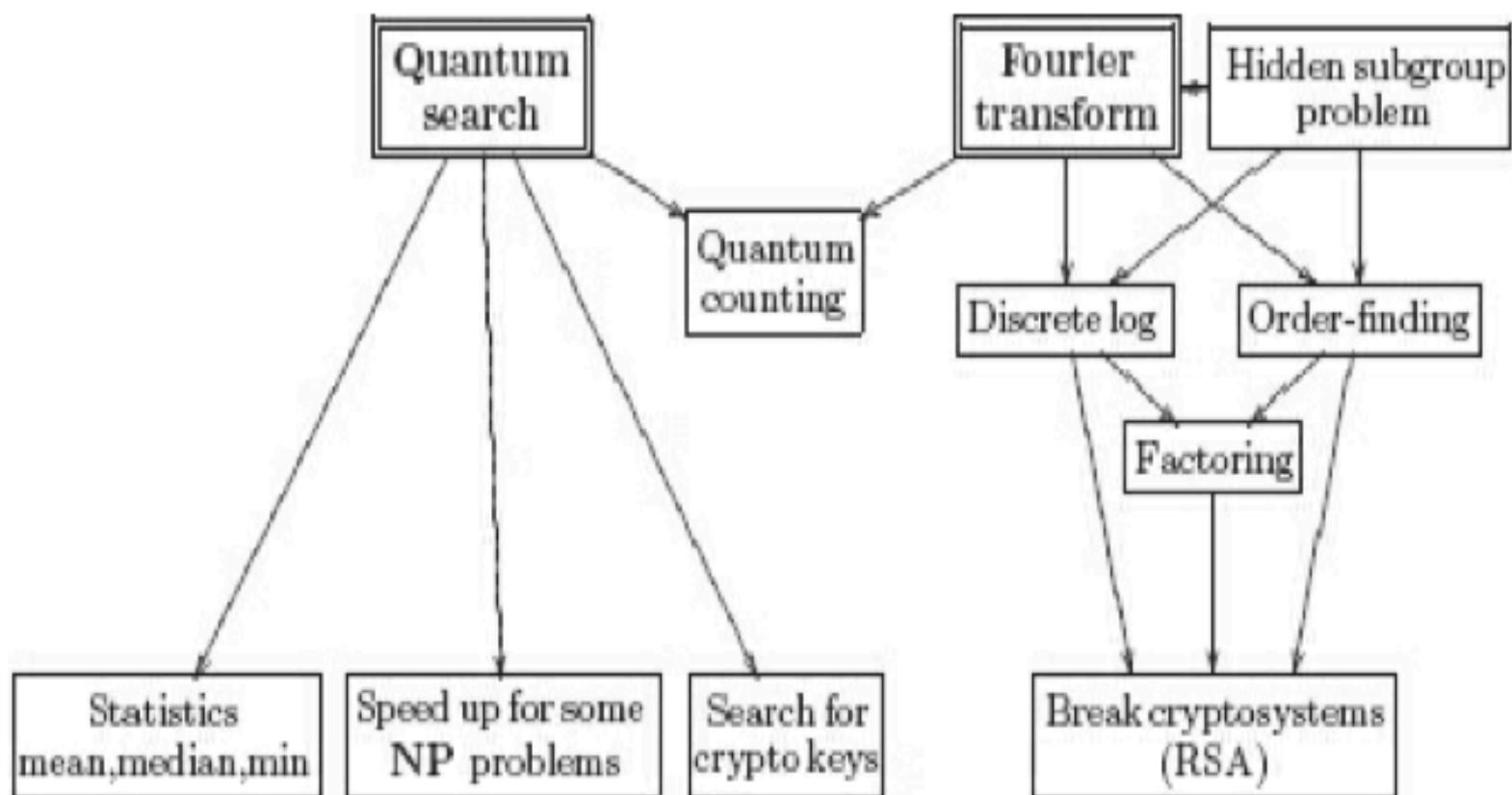
主要な量子アルゴリズム

- Quantum Teleportation
 - Grover's Quantum Search Algorithm
 - Quantum Fourier Transformation
 - Shor's Quantum Factorization
 - Quantum Error Correction
-

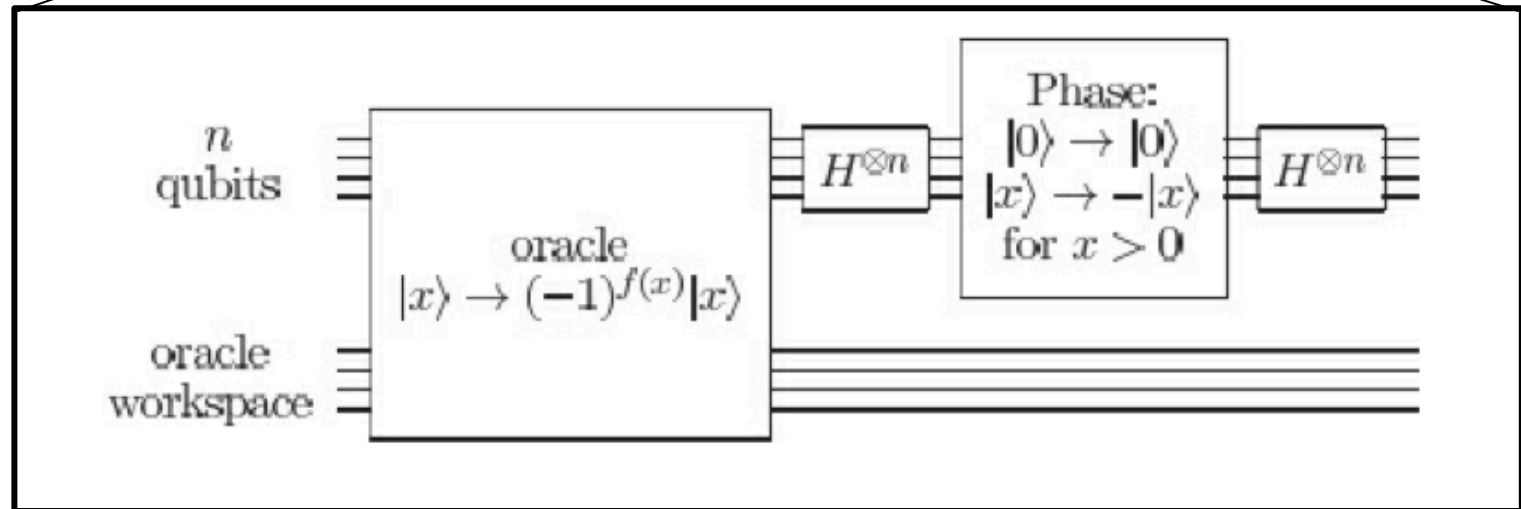
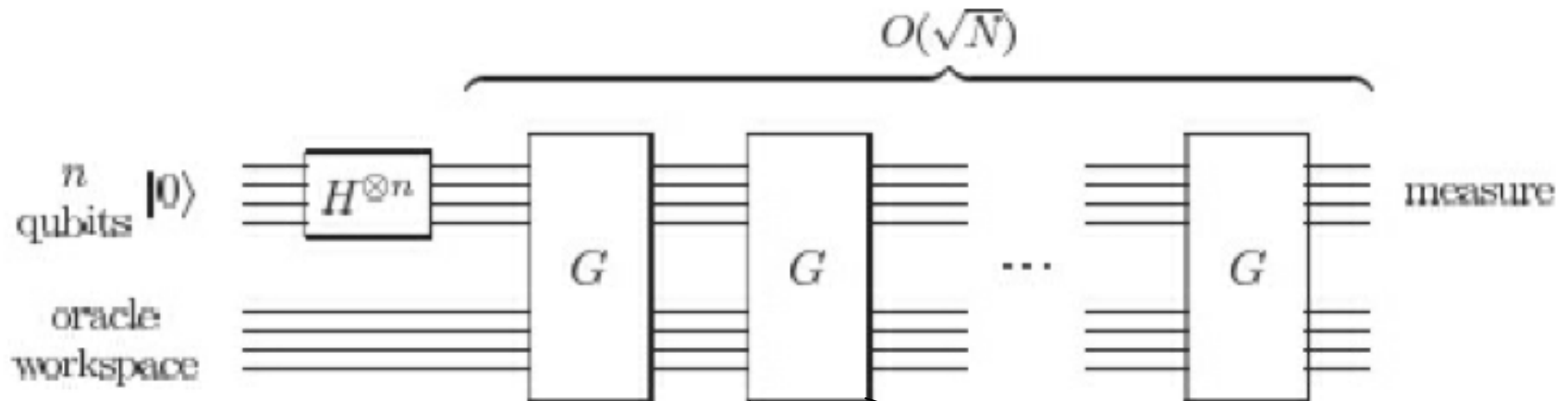
Quantum Teleportation



主要な量子アルゴリズムの関係と応用



Grover's Search Algorithm



Grover's Search Algorithm

$$1. |0\rangle^{\otimes n} |0\rangle$$

initial state

$$2. \rightarrow \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$$

apply $H^{\otimes n}$ to the first n qubits,
and HX to the last qubit

$$3. \rightarrow \left[(2|\psi\rangle\langle\psi| - I)O \right]^R \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$$

apply the Grover iteration $R \approx$
 $\lceil \pi\sqrt{2^n}/4 \rceil$ times.

$$\approx |x_0\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$$

$$4. \rightarrow x_0$$

measure the first n qubits

Shorのアルゴリズムの中心部分 量子フーリエ変換を実現する量子回路

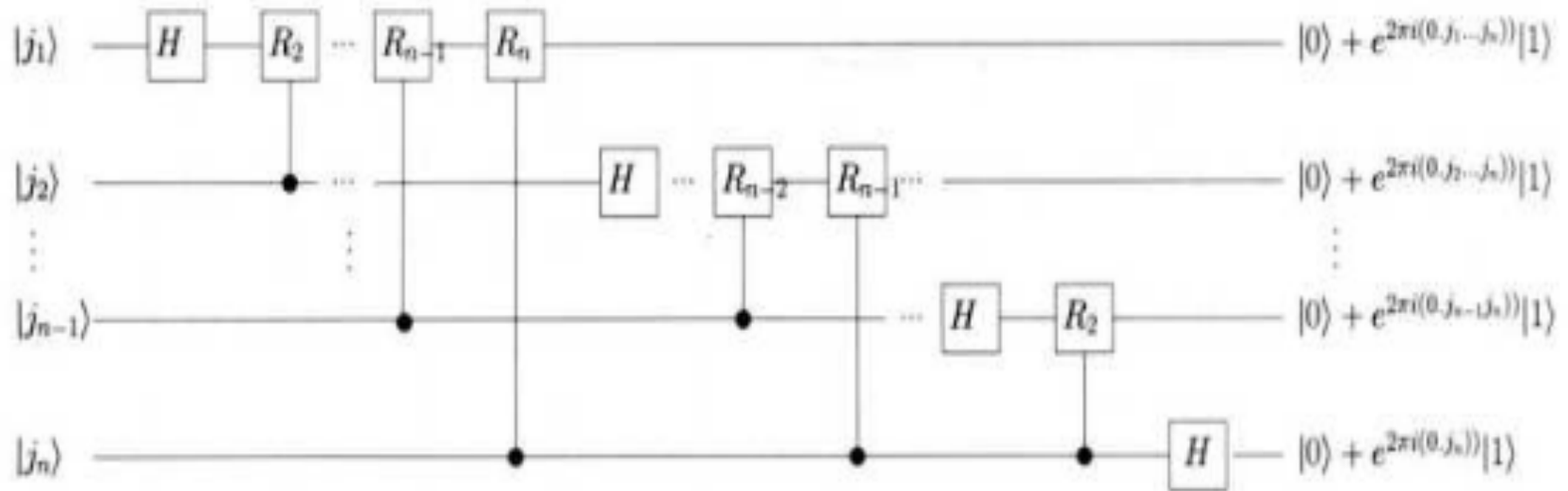


Fig. 11.6 The quantum Fourier transform on n qubits. A black dot together with R_k denotes the control bit of CR_k . The breakdown of the quantum Fourier transform into elementary unitary gates shows that the quantum Fourier transform is unitary itself.

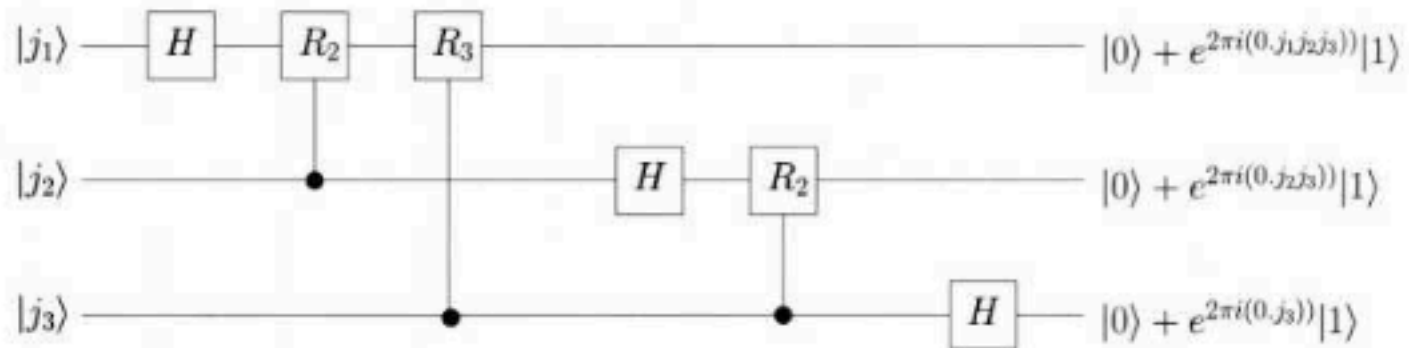


Fig. 11.7 The quantum Fourier transform on three qubits.

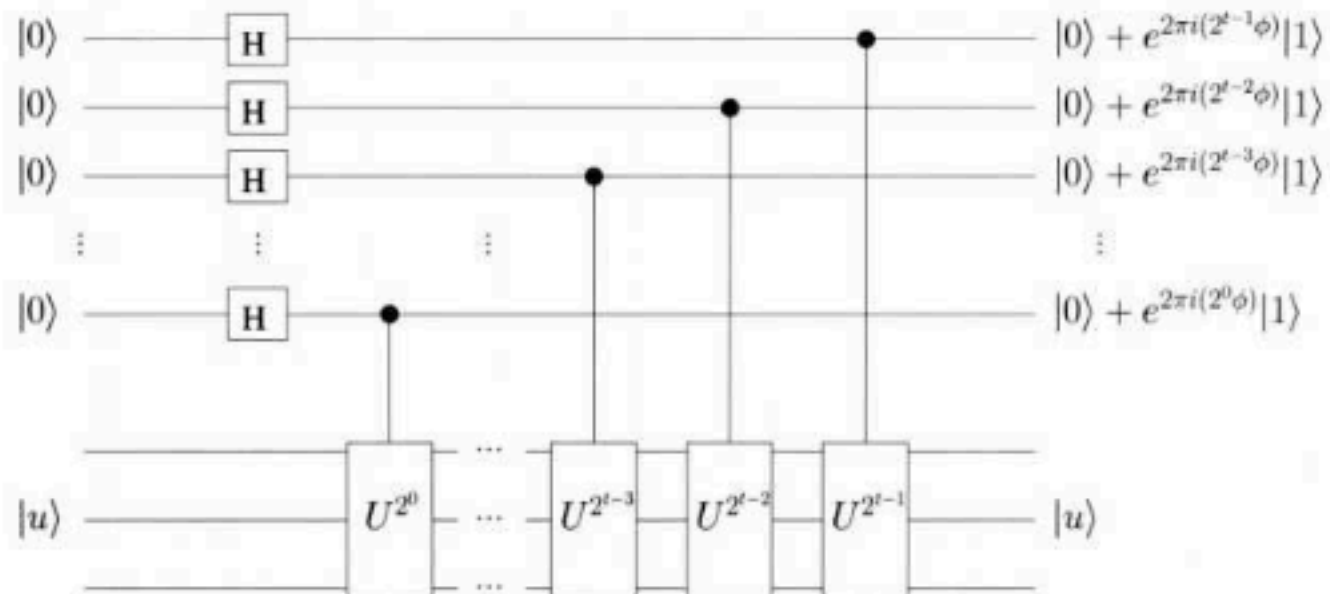
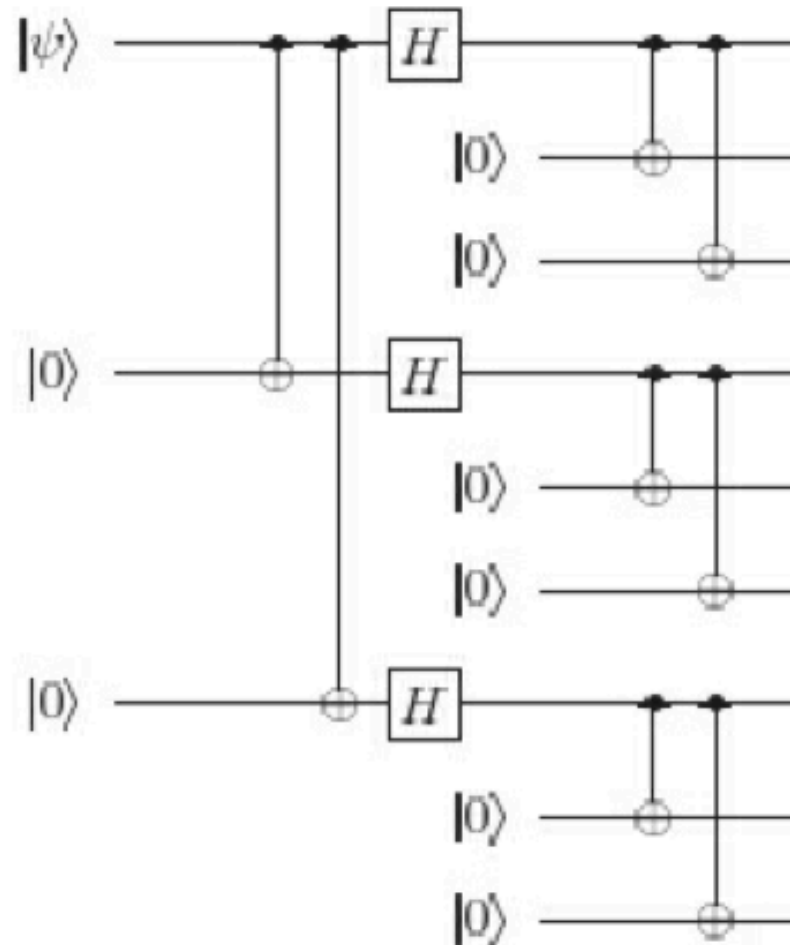


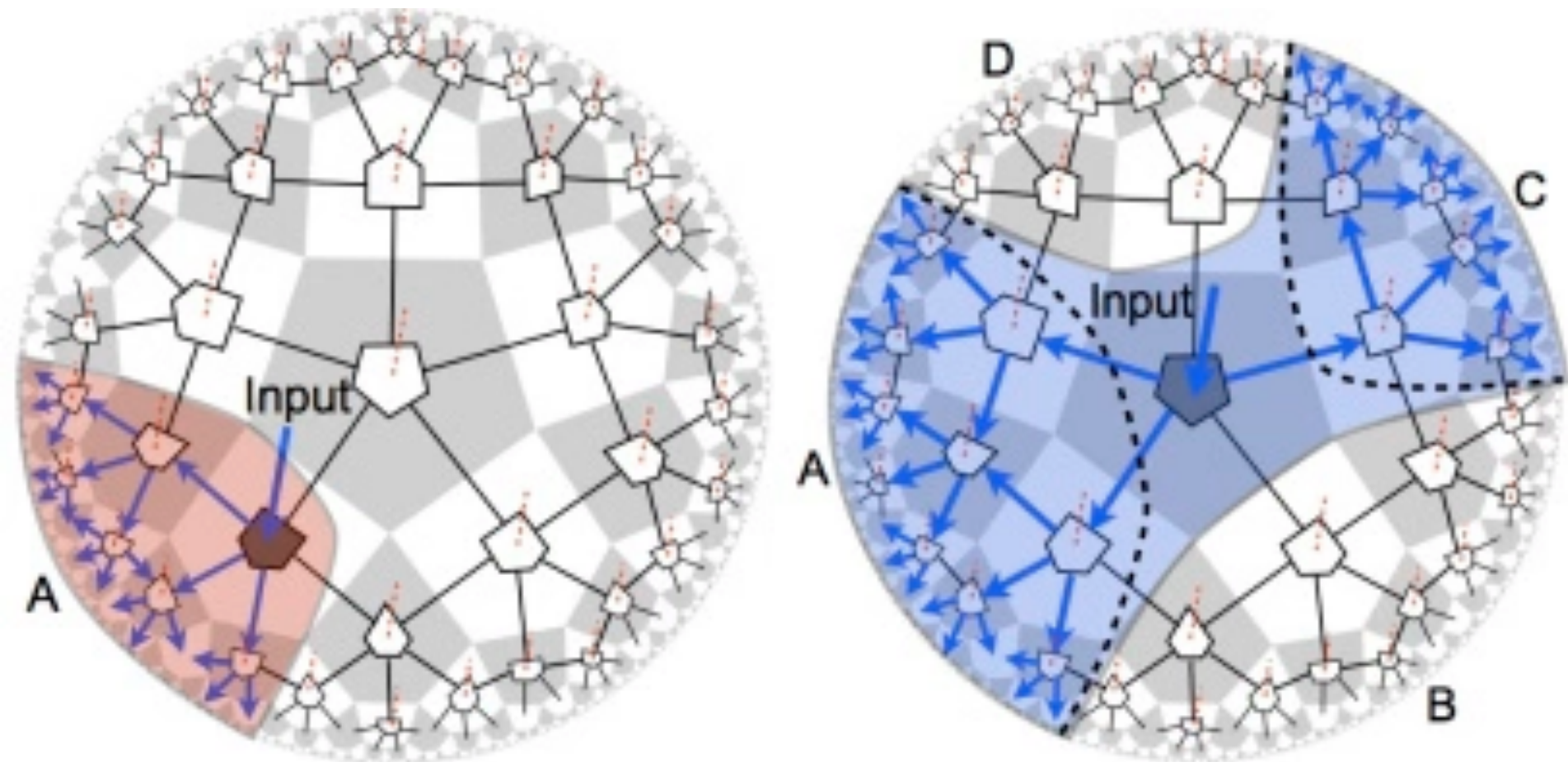
Fig. 11.8 The first part of the phase estimation algorithm. The algorithm is finished by applying the inverse of the quantum Fourier transform to the first registers.

Quantum Error Correction

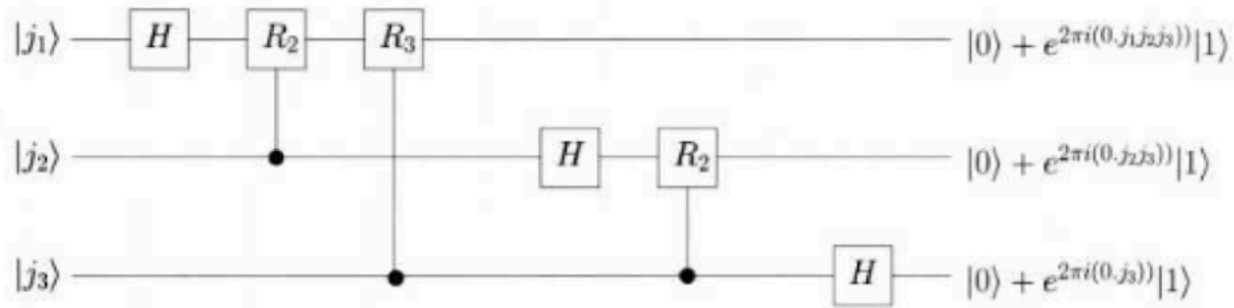
Encoding circuit for the Shor nine qubit code.



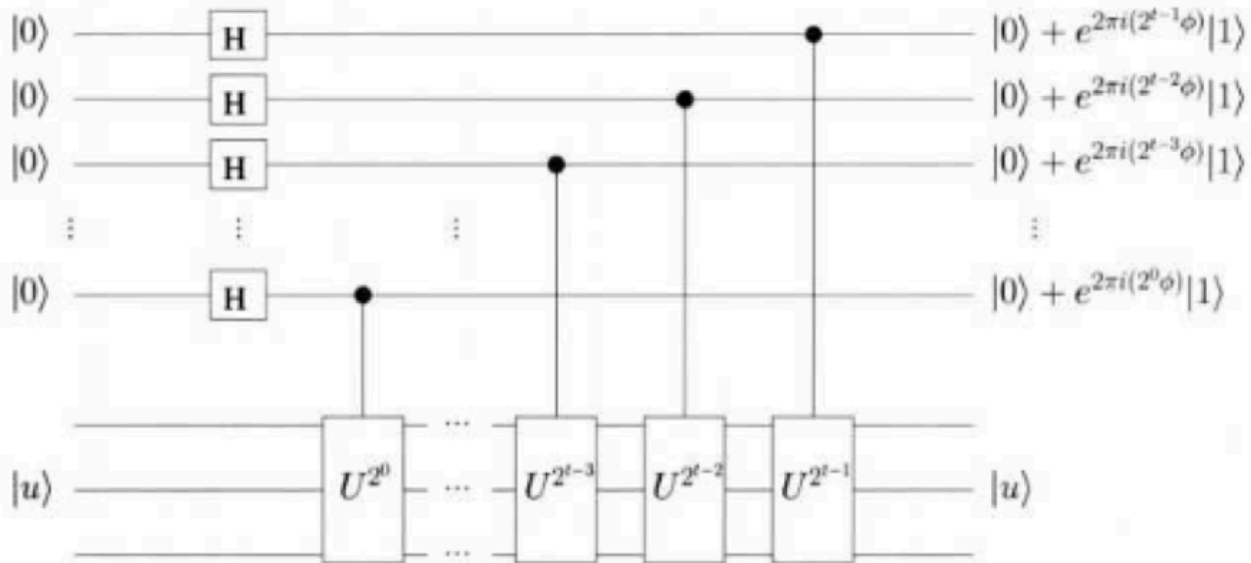
AdS/CFT対応とTensor Network(MERA)



<https://goo.gl/GUCedR>



量子ゲートの問題



「量子ゲート」によるアプローチの問題

「回路図」と「回路」

- ある問題を解く為の、量子ゲートの「回路図」を作ることと、その「量子回路」を現実につくることは、別の問題である。そして前者より後者の方が、はるかに難しい。
 - 現状は、「回路図」が出来ていても、その「回路」の実現のところで足踏みをしている。
いつの日か、現在のLSI製造システムのように、回路図を作れば回路が出来ようになるのかもしれないのだが。
-

「量子ゲート」によるアプローチの問題

量子コンピュータのアーキテクチャ

- 「量子ゲート」のアプローチでは、「アルゴリズム」は、直接、「ハードウェア」のワイアリングで表現されることになる。
- このこと自体は問題ではなく当然のことなのだが、明らかに、「ソフトウェア」という抽象のレベルには向いていない。それは、シリコン上で半導体を設計している人のコンピュータとの関係と同じである。
- 別の言い方をすれば、「量子ゲート」の研究は、おそらくは「ハードとソフト」から構成されるであろう「万能量子コンピュータ」のアーキテクチャの研究には届いていない。

Experimental Quantum Computation with Nuclear Spins in Liquid Solution

量子コンピュータは、何ができるか？
Shorアルゴリズム実装の成功例

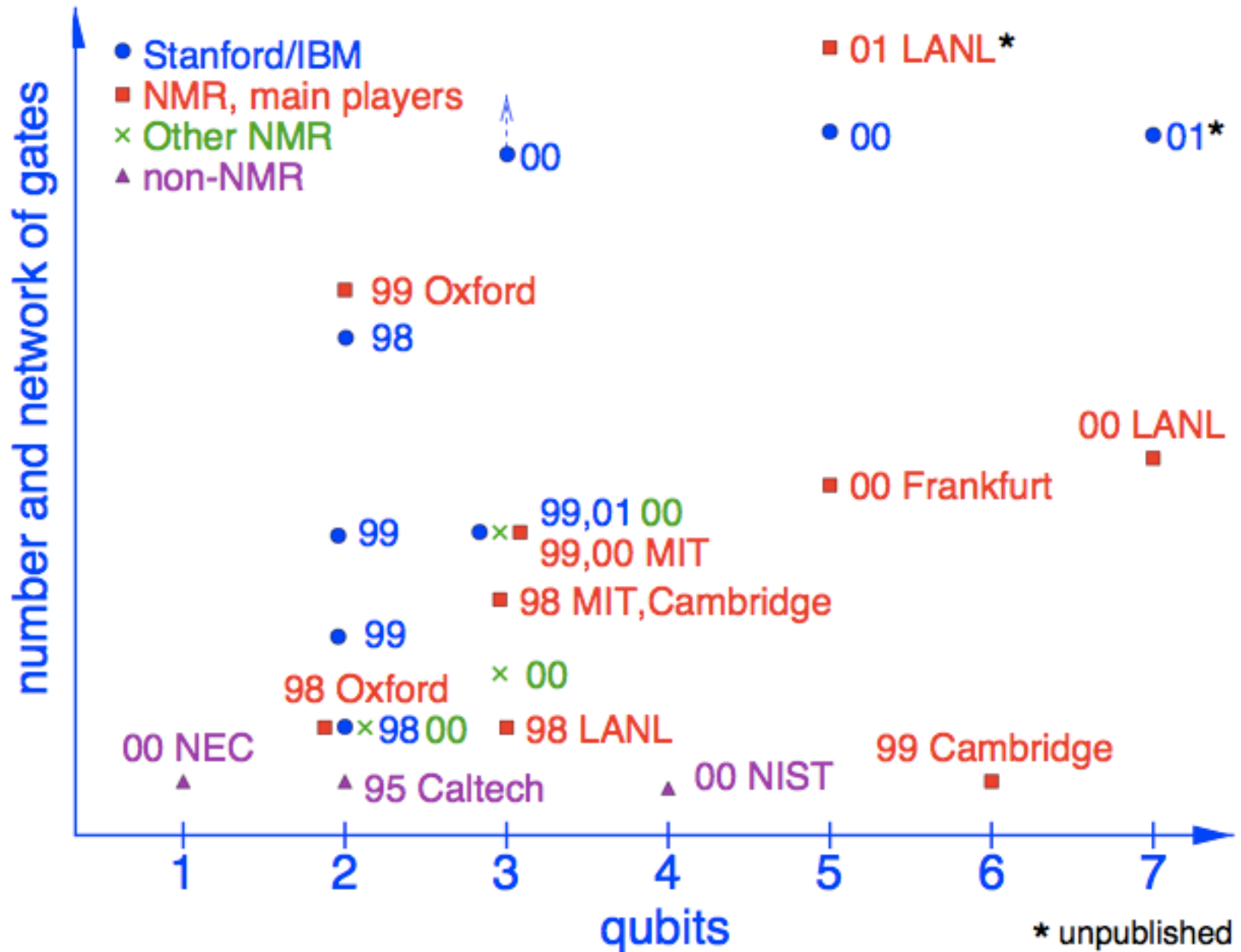
Lieven M. K. Vandersypen

July 2001

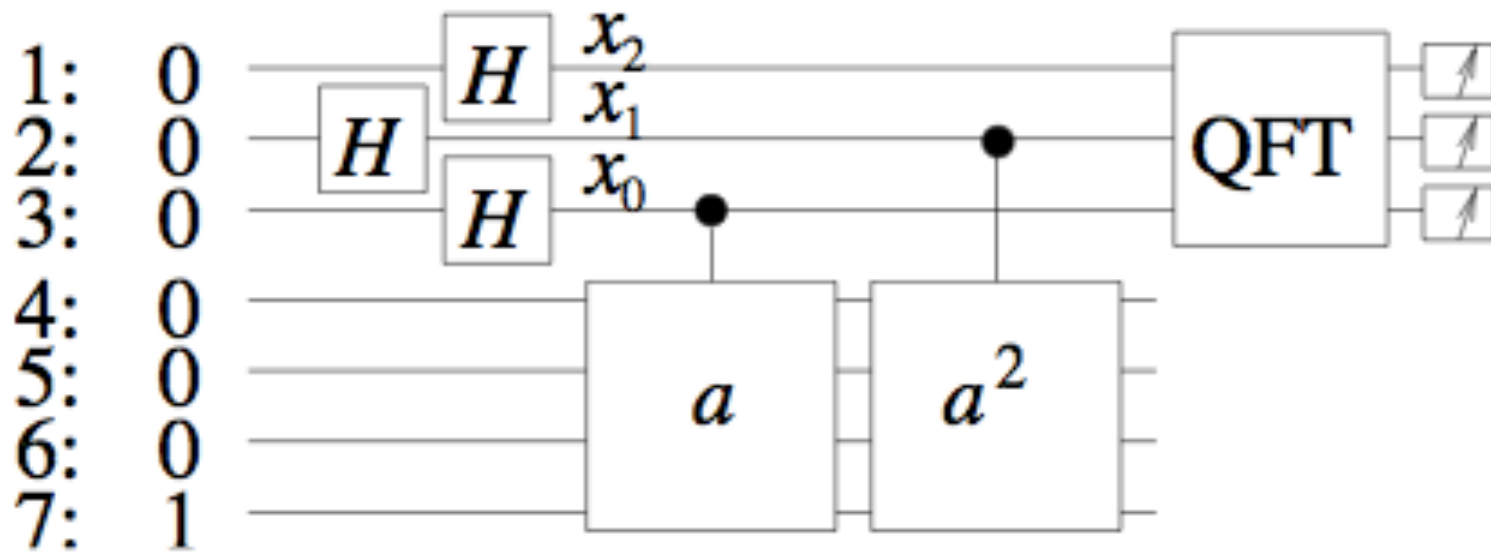
<http://arxiv.org/pdf/quant-ph/0205193v1.pdf>

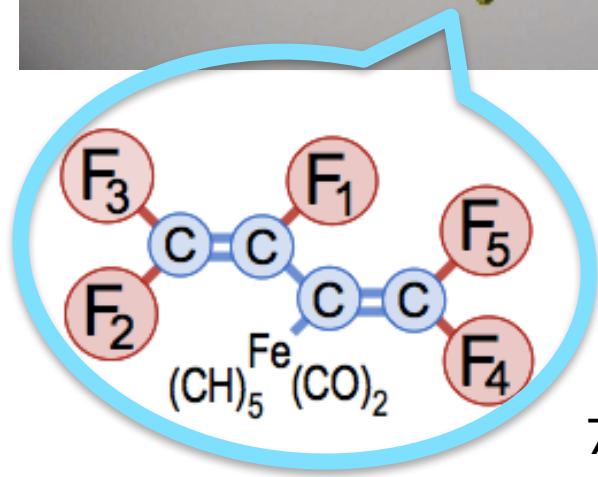
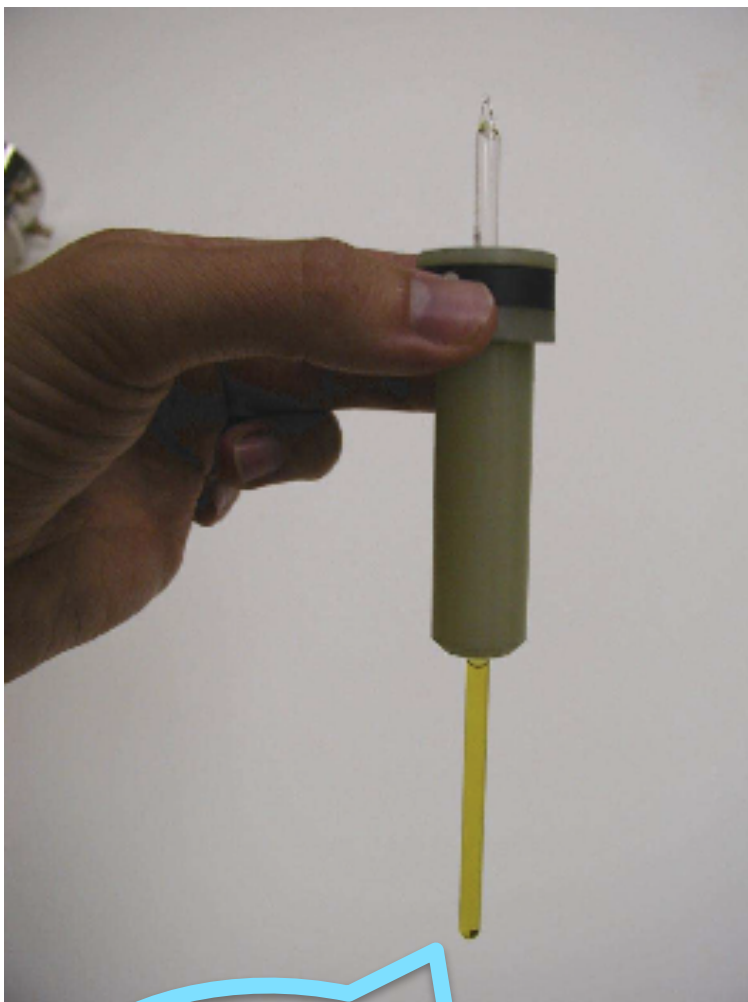


Overview of quantum computing experiments.



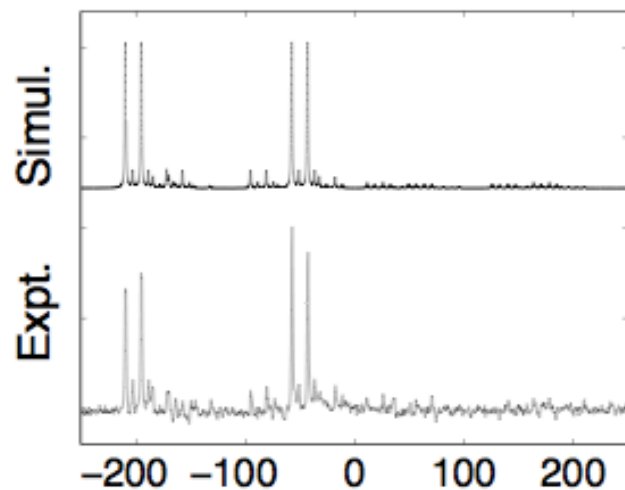
15の素因数分解の為に、 単純化された量子回路



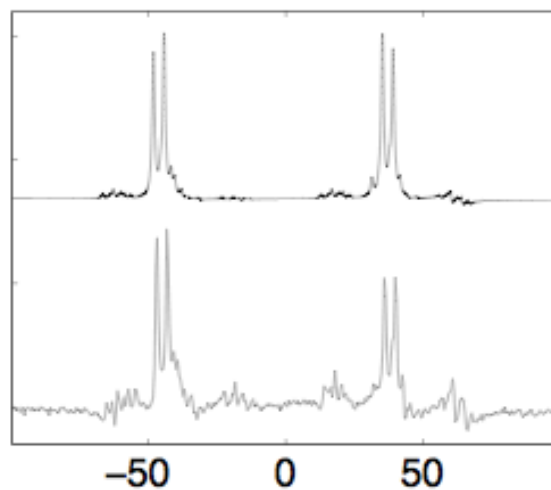


7つのスピンを持つ物質

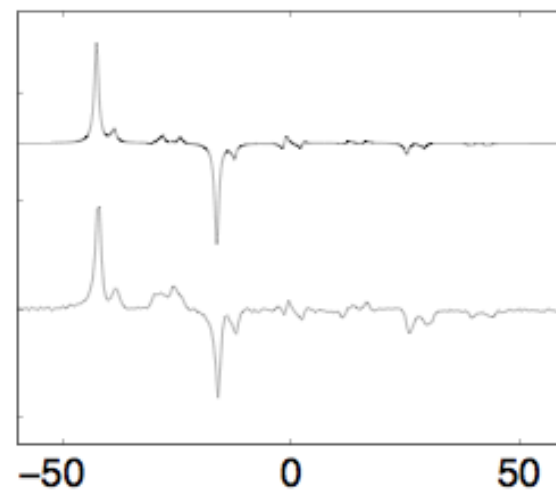
Spin 1



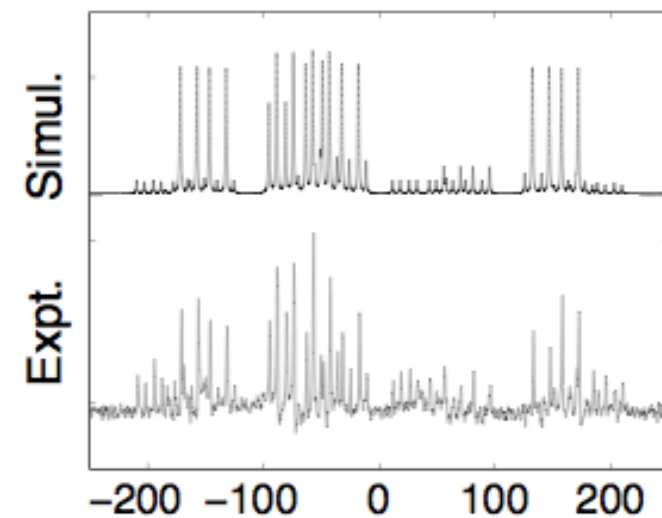
Spin 2



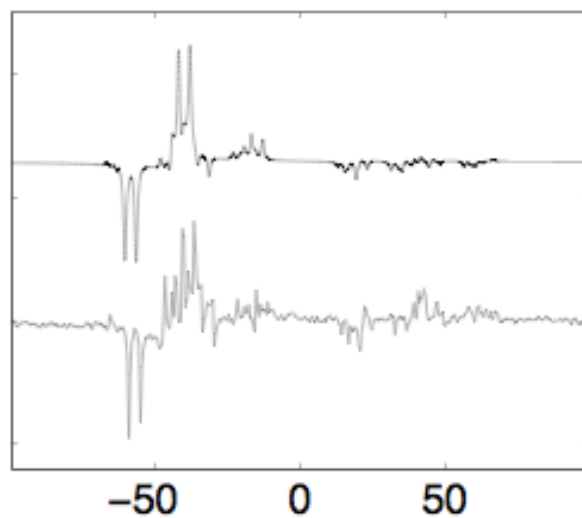
Spin 3



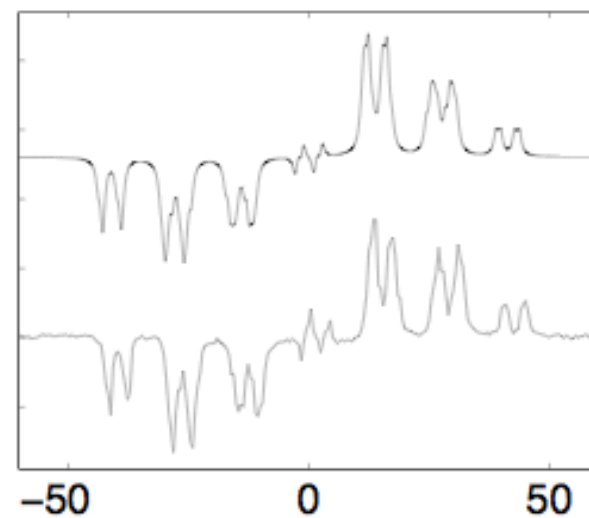
Spin 1



Spin 2



Spin 3



15は、3と5に素因数分解された！（らしい）

プログラミング+

<http://ascii.jp/programming/>

講師 丸山不二夫氏

会場 角川第3本社ビル (東京・飯田橋)

日時 2017年12月9日(土)

紙と鉛筆で学ぶ 量子情報理論 基礎演習

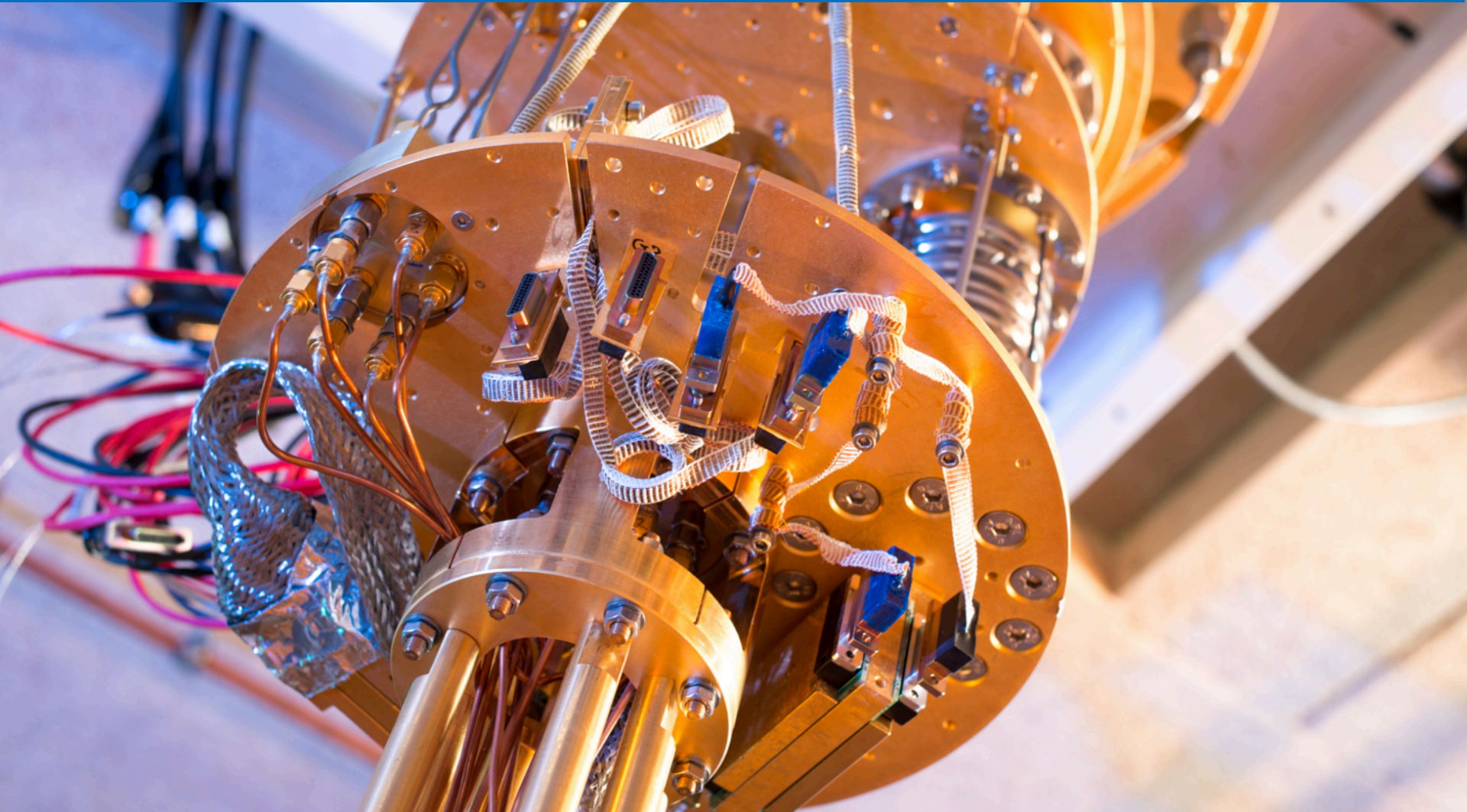
6時間集中講座



<http://lab-kadokawa38.peatix.com/>

Part IV

アニーリング型量子コンピュータ



アニーリング型量子コンピュータ

量子ゲートをコヒーレントな状態(量子重ね合わせの状態)に維持しておくのは、なかなか難しい。アニーリング型では、コヒーレントが破れて、系がエネルギーの最小状態に遷移することを利用する。

「汎用ゲートモデル」の問題点

by Geordie Rose

- ❑ エネルギーの固有状態のsuperpositionを維持して利用する必要がある。その状態は全く「不自然」なもので、極めて破れやすい。
- ❑ 「量子エラー訂正」のオーバーヘッドが大きく、高速で高いクォリティのフィードバックを必要とする。
- ❑ 必要とされる高速のコントロールは、スケールするのが難しい。
- ❑ プロセッサのアーキテクチャーについての研究は、全く進んでいない。

Roseの述懐

- ゲート・モデルが、どうしたら動くようになるのか、全く見えなかった。2003年には、決断をしなければと思うようになった。選択肢は二つあった。一つは、研究をあきらめること。もう一つの選択は、何か他のものを作ることだった。
- この時、1999年の4月にScience誌に掲載された、Brookeらの“Quantum Annealing of a disordered magnet”という論文に注目した。彼らは、計算を古典的なスピン問題に変換して、それを量子アニーリング効果を使って解くことを提案していた。

Roseの述懐

- 二つの重要なアイデアが生まれた。
 - 一つは、古典的なスピン問題を攻略する超伝導プロセッサーを作ること。
 - あと一つは、プロセッサーが有用な解を高速で返すように、量子効果を利用することである。
-

D-Waveマシンの動作のモデル イジング・モデル(Ising Model)

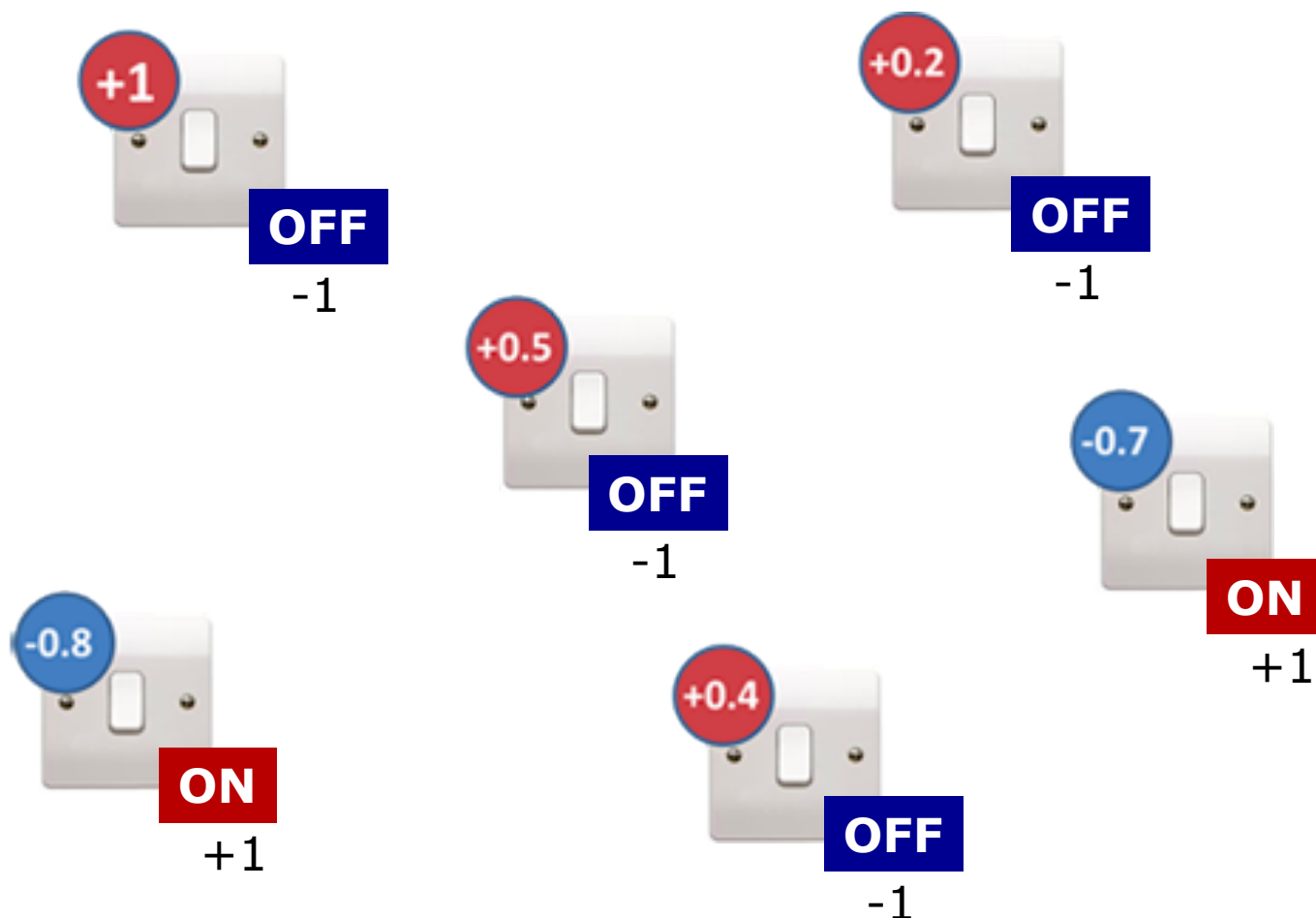
ここでは、D-Wave社のチュートリアル “Quantum Computing Primer”にしたがって、D-Waveマシンの動作のモデルを紹介する。それは、「古典的スピン問題」のイジング・モデル(Ising Model)のいい説明にもなっている。

<http://www.dwavesys.com/en/dev-tutorial-intro.html> (このURLは、現在利用できない)

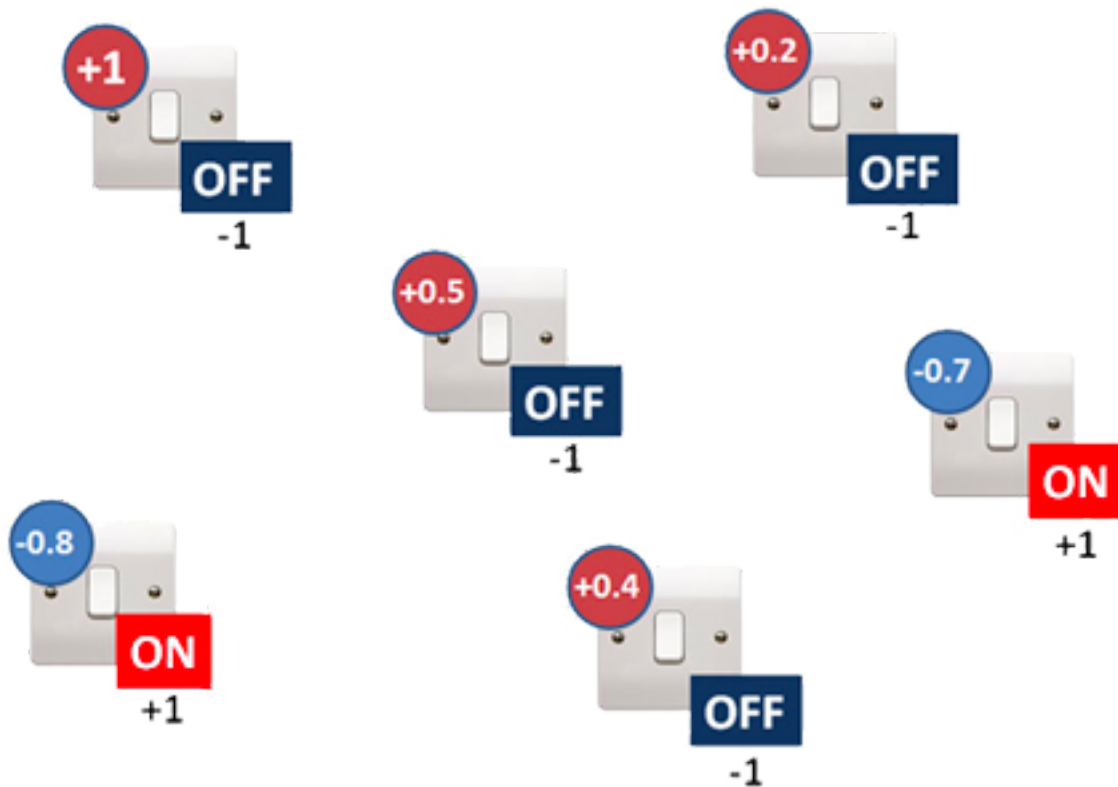
いくつかのスイッチがあったとしよう。この例では、5つのスイッチがある。それぞれのスイッチには、数字が割り当てられている。 $+1, +0.2, +0.5, -0.7, -0.8, +0.4$ のように。これを bias と呼ぼう。



スイッチは、ONまたはOFFの状態を取るものとしてよう。
この例では、3つのスイッチがOFFで、2つのスイッチがONの
状態になっている。スイッチがONの時には+1を、スイッチが
OFFの時には-1を割り当てよう。



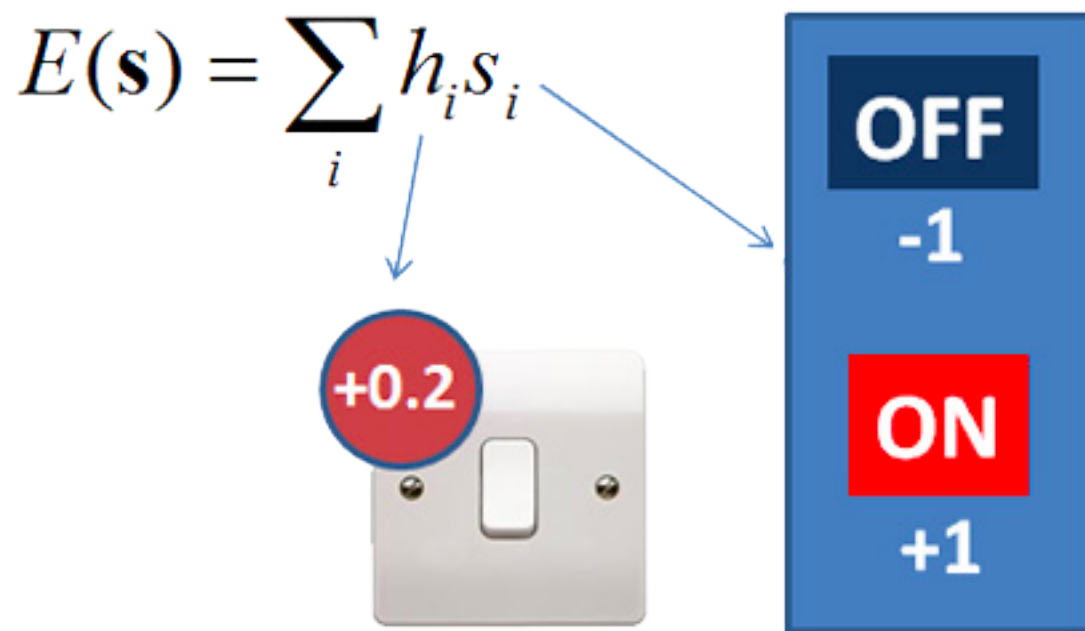
それぞれのスイッチに割り当てられたbiasの値と、スイッチのON,OFFの状態を表す+1,-1を掛けた数字を、全部足しあわせた量を考えてみよう。この例の場合には、その量は、-3.6になる。



$$\begin{array}{rclcl} +1 & \times & -1 & = & -1 \\ +0.2 & \times & -1 & = & -0.2 \\ +0.5 & \times & -1 & = & -0.5 \\ -0.8 & \times & +1 & = & -0.8 \\ +0.4 & \times & -1 & = & -0.4 \\ -0.7 & \times & +1 & = & -0.7 \end{array}$$

Total: -3.6

式で書くと次のようになる。

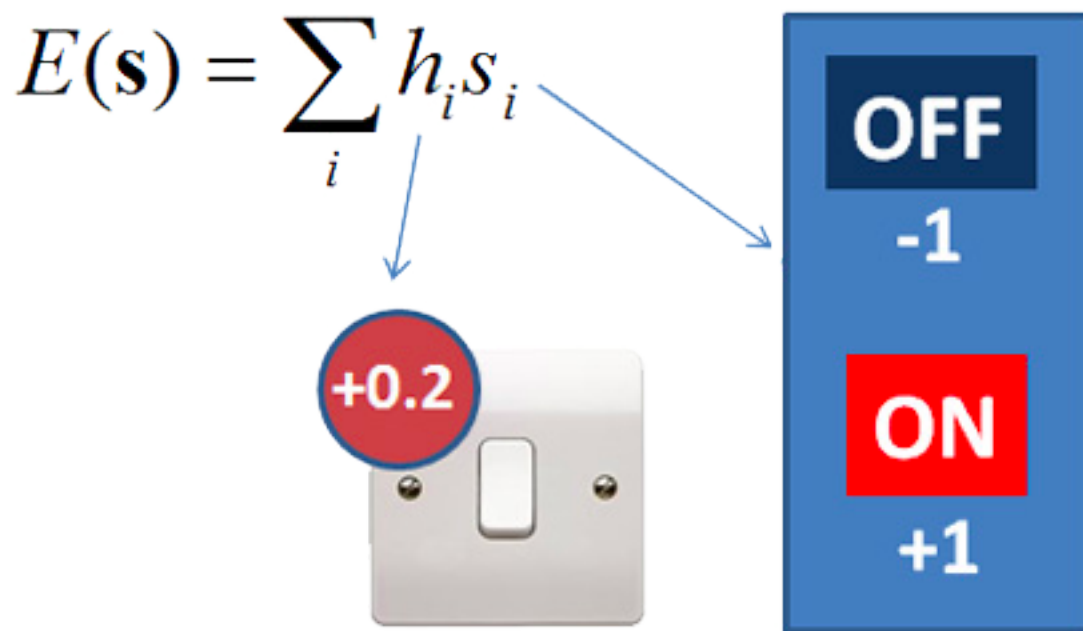


h は、それぞれの
スイッチに割り当てら
れたbiasの値

s は、それぞれの
スイッチのON,OFFの
状態に対応した、
+1,-1の値

次のような問題を考える。

「biasが与えられた時、この $E(s)$ を最小にするスイッチの状態を求めよ。」

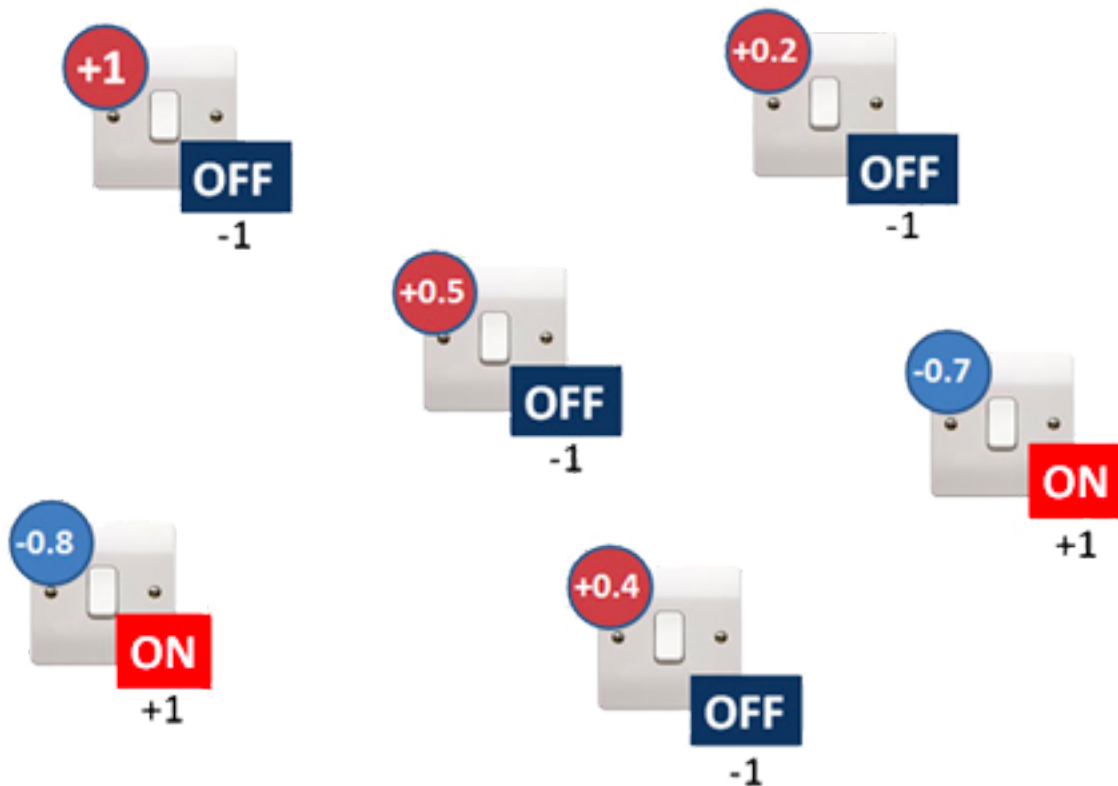


h は、それぞれの
スイッチに割り当てら
れたbiasの値

s は、それぞれの
スイッチのON,OFFの
状態に対応した、
 $+1, -1$ の値

この問題を解くのは、簡単である。

biasがマイナスの時にはスイッチをONにし、biasがプラスの時にはスイッチをOFFにすれば、全ての項がマイナスになり最小値を与える。先の例が、答えになっている。



$$\begin{array}{rclcl} +1 & \times & -1 & = & -1 \\ +0.2 & \times & -1 & = & -0.2 \\ +0.5 & \times & -1 & = & -0.5 \\ -0.8 & \times & +1 & = & -0.8 \\ +0.4 & \times & -1 & = & -0.4 \\ -0.7 & \times & +1 & = & -0.7 \end{array}$$

Total: -3.6



$$E(\mathbf{s}) = \sum_i h_i s_i + \sum_{i,j} J_{i,j} s_i s_j$$

問題を少し難しくしよう。今までは、一つのスイッチにbiasが割り当てられていただけだったが、今度は、二つのスイッチのあいだに、weight J を割り当てよう。

この例では、それぞれのスイッチに、bias $+1$ と -0.8 が、二つのスイッチのあいだに、weight -1 が割り当てられている。



$$E(\mathbf{s}) = \sum_i h_i s_i + \sum_{i,j} J_{i,j} s_i s_j$$

$E(s)$ の値は、二つのスイッチのON,OFFに応じて、次のように計算される。OFF,OFFの時、最小値を取る。

ON,ON
= -0.8

ON,OFF
= +1.2

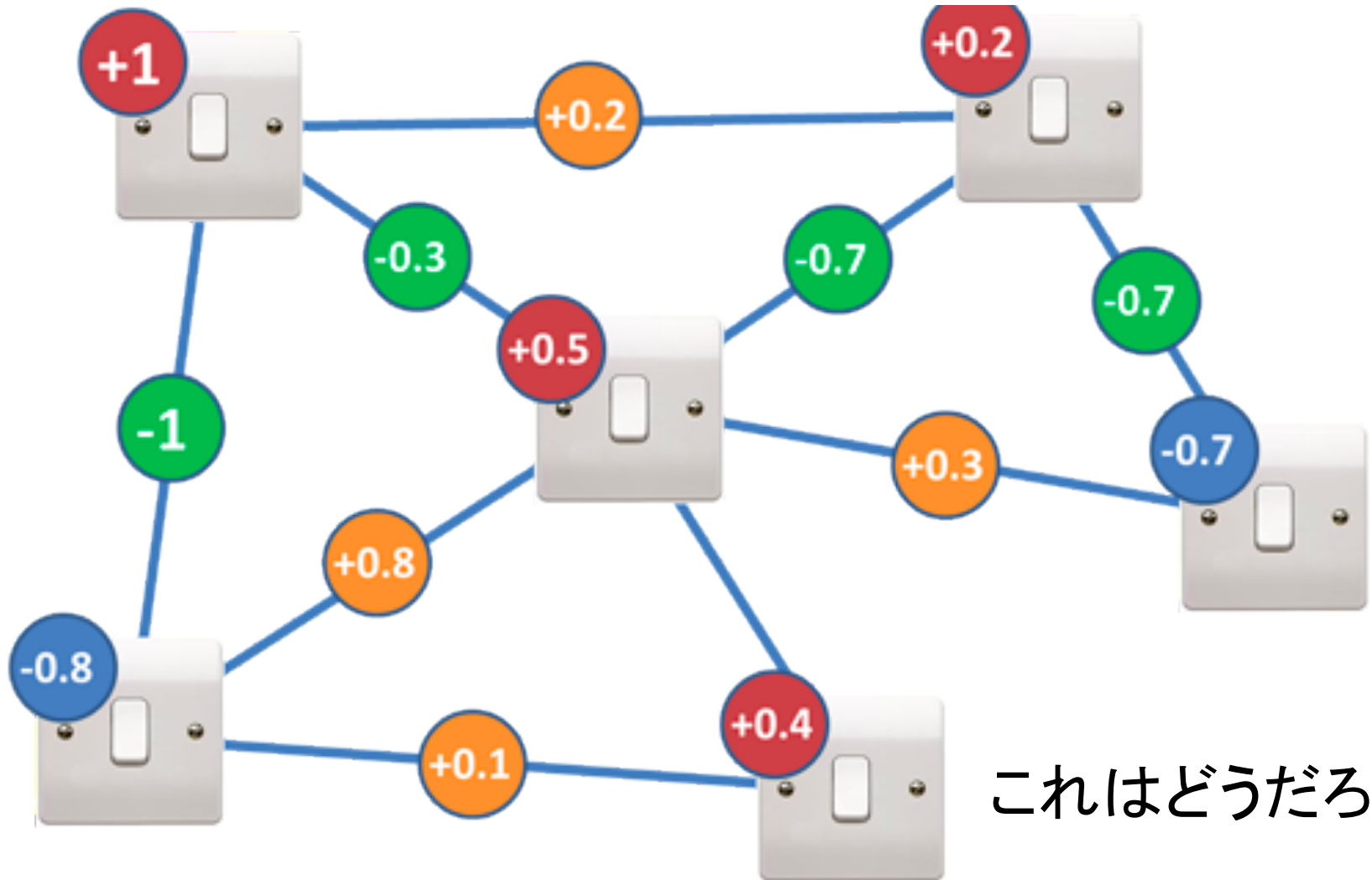
OFF,ON
= -0.8

OFF,OFF
= -2.8

+1 x +1
-0.8 x +1
+1 x +1
-0.8 x -1
+1 x -1
-0.8 x +1
+1 x -1
-0.8 x -1

-1 x +1 x +1
-1 x +1 x -1
-1 x -1 x +1
-1 x -1 x -1

スイッチが5個だから、スイッチのON,OFFの組み合わせは、 $2^5=32$ 通り。その全てについて $E(s)$ を計算して、最小のものを選べばいい。ただ、スイッチの数が増えると、場合の数が増えて、急に難しくなる。



これはどうだろう？

この式を最小に出来るか？

$$E(\mathbf{s}) = \sum_i h_i s_i + \sum_{i,j} J_{i,j} s_i s_j$$



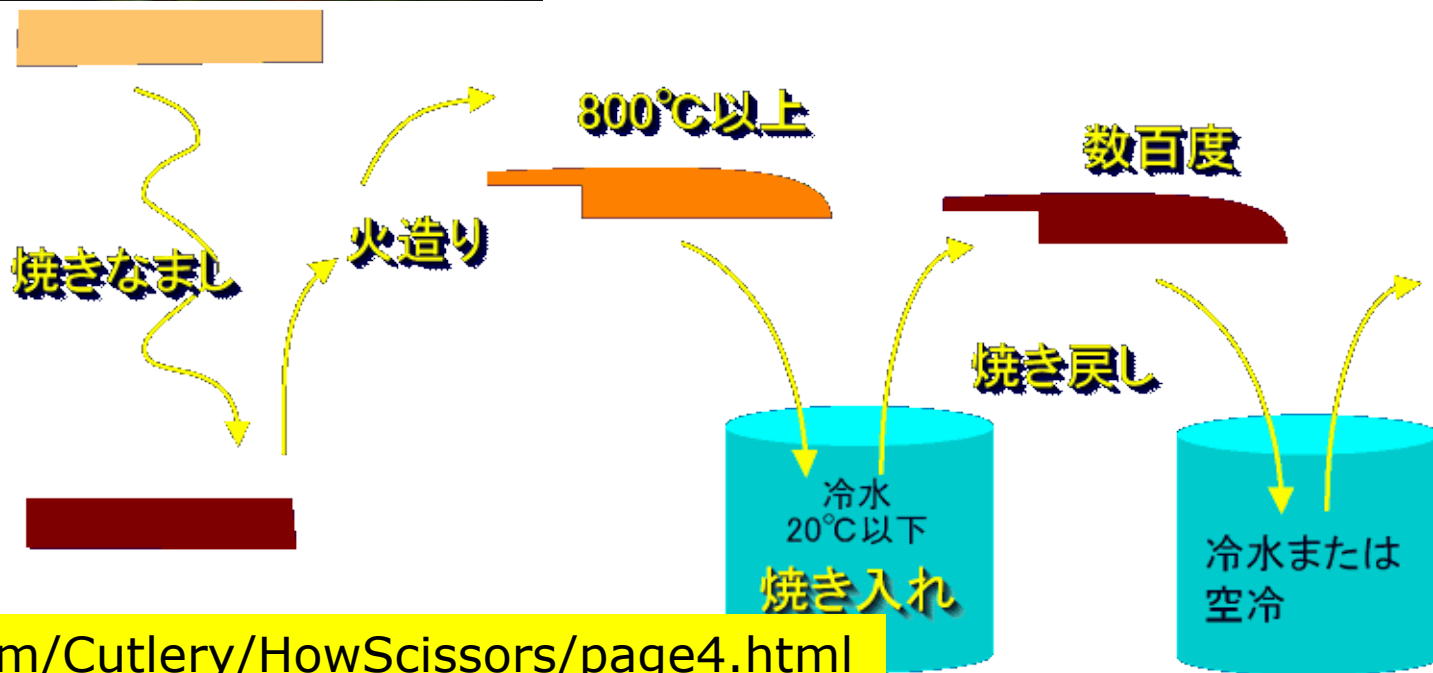
これは、Ising Modelの問題だ。

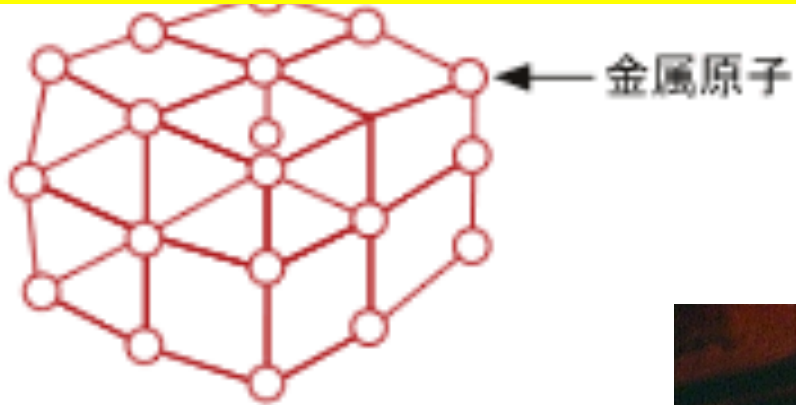
量子アニーリング



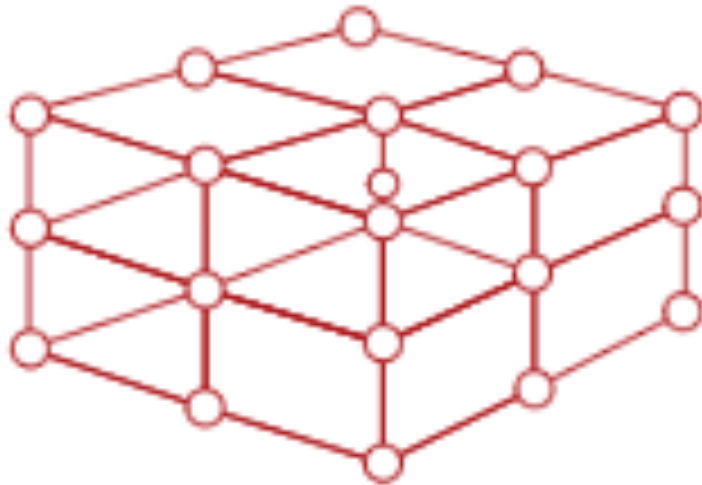


焼きなまし
焼き入れ
焼き戻し





加工により歪んだ金属組織



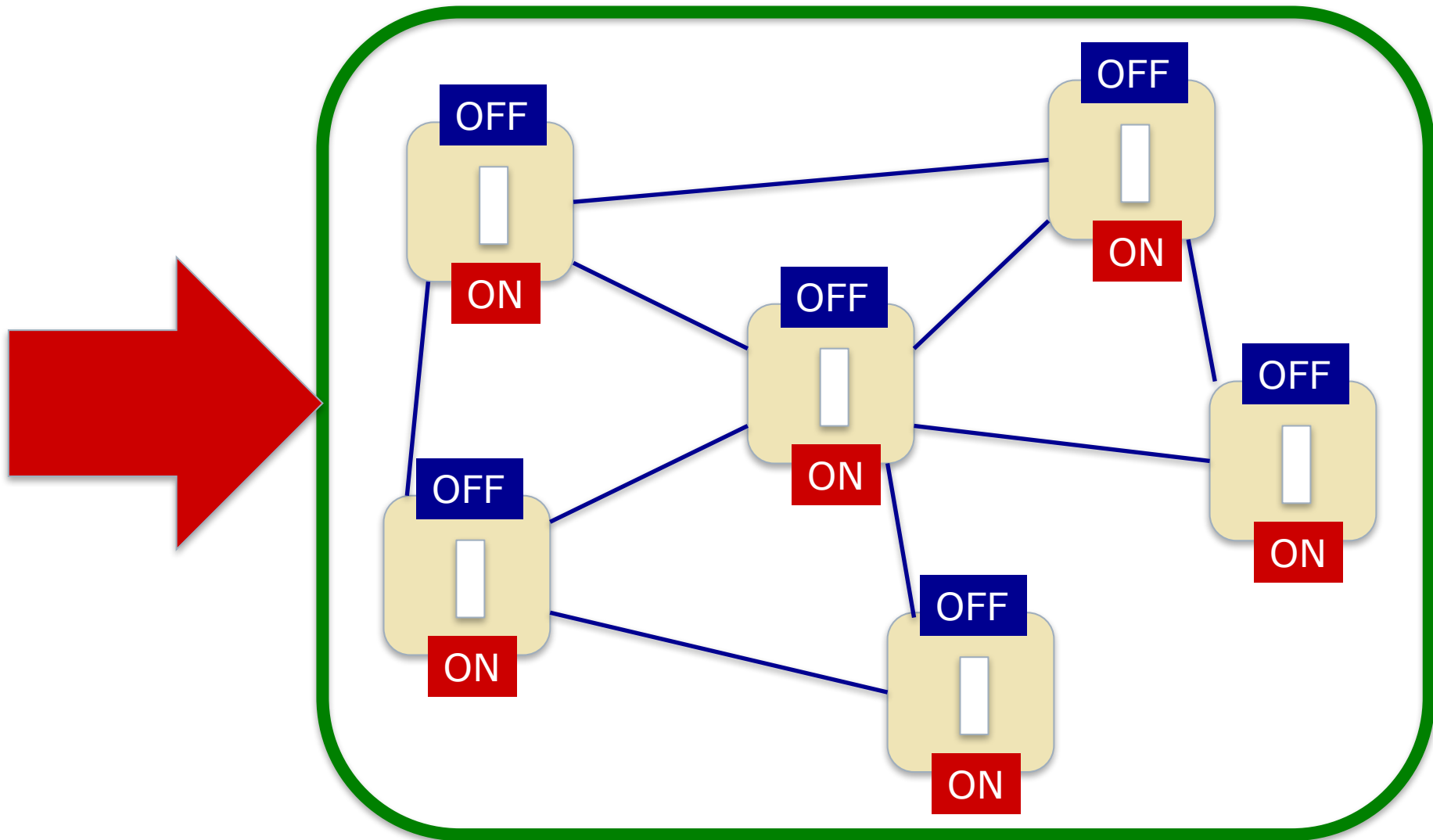
再結晶化により均質化

焼なまし

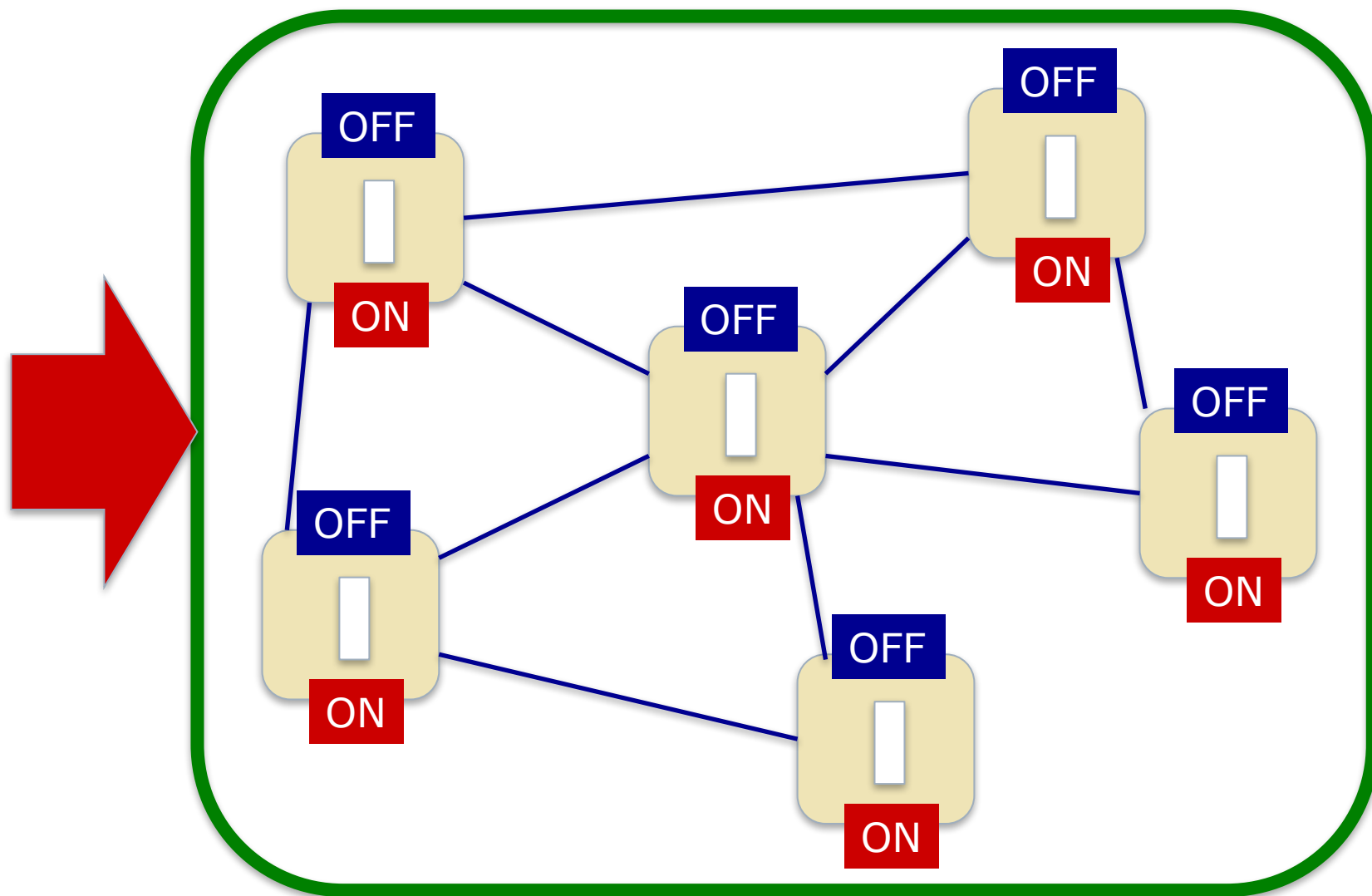


金属やガラスの熱処理操作の一。
金属・ガラスをある温度に加熱したのち、
ゆっくりと冷却すること

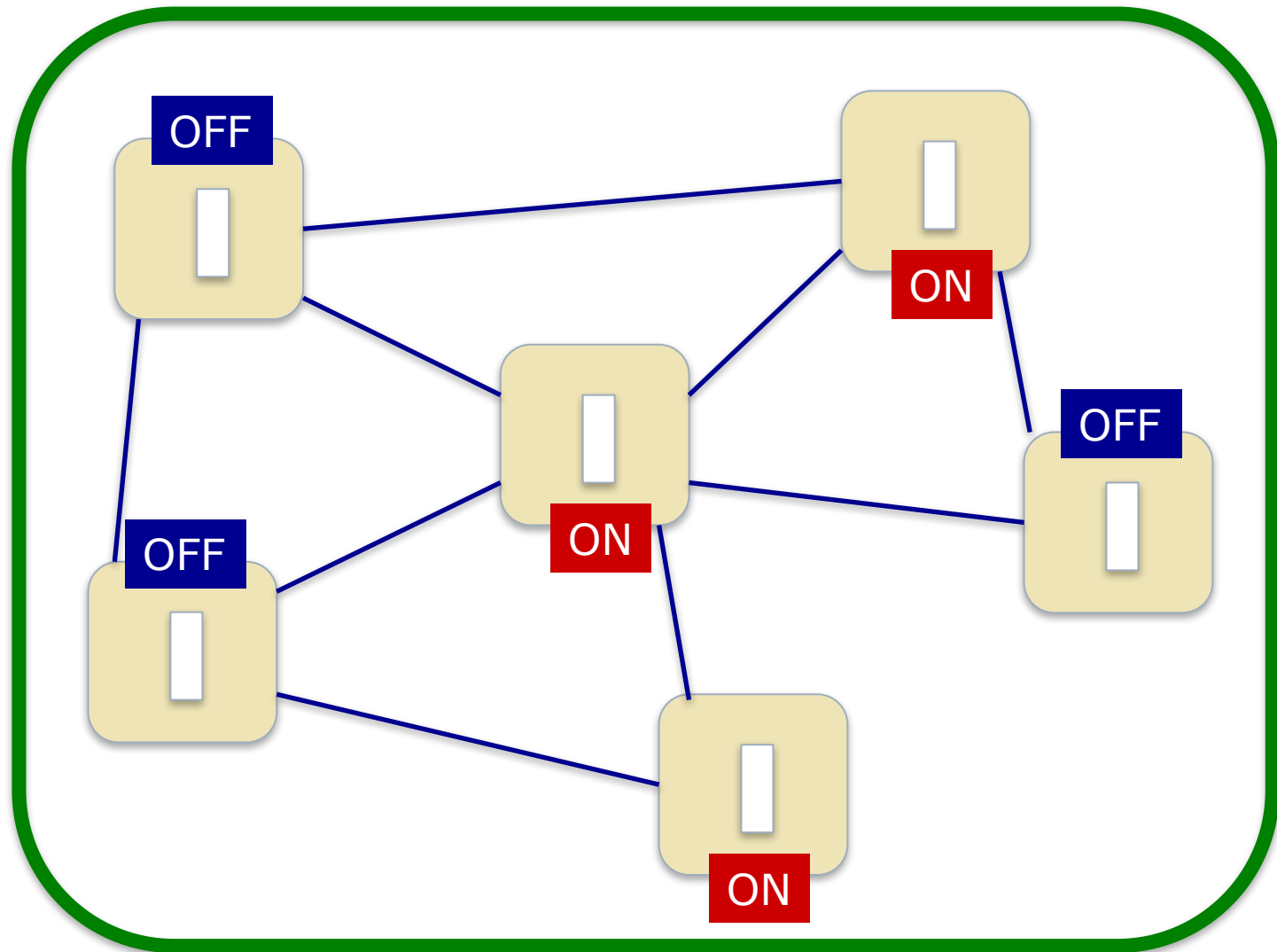
スイッチが、ON,OFF両方の状態をとるSuperpositionの状態
で、高いエネルギーを加える。

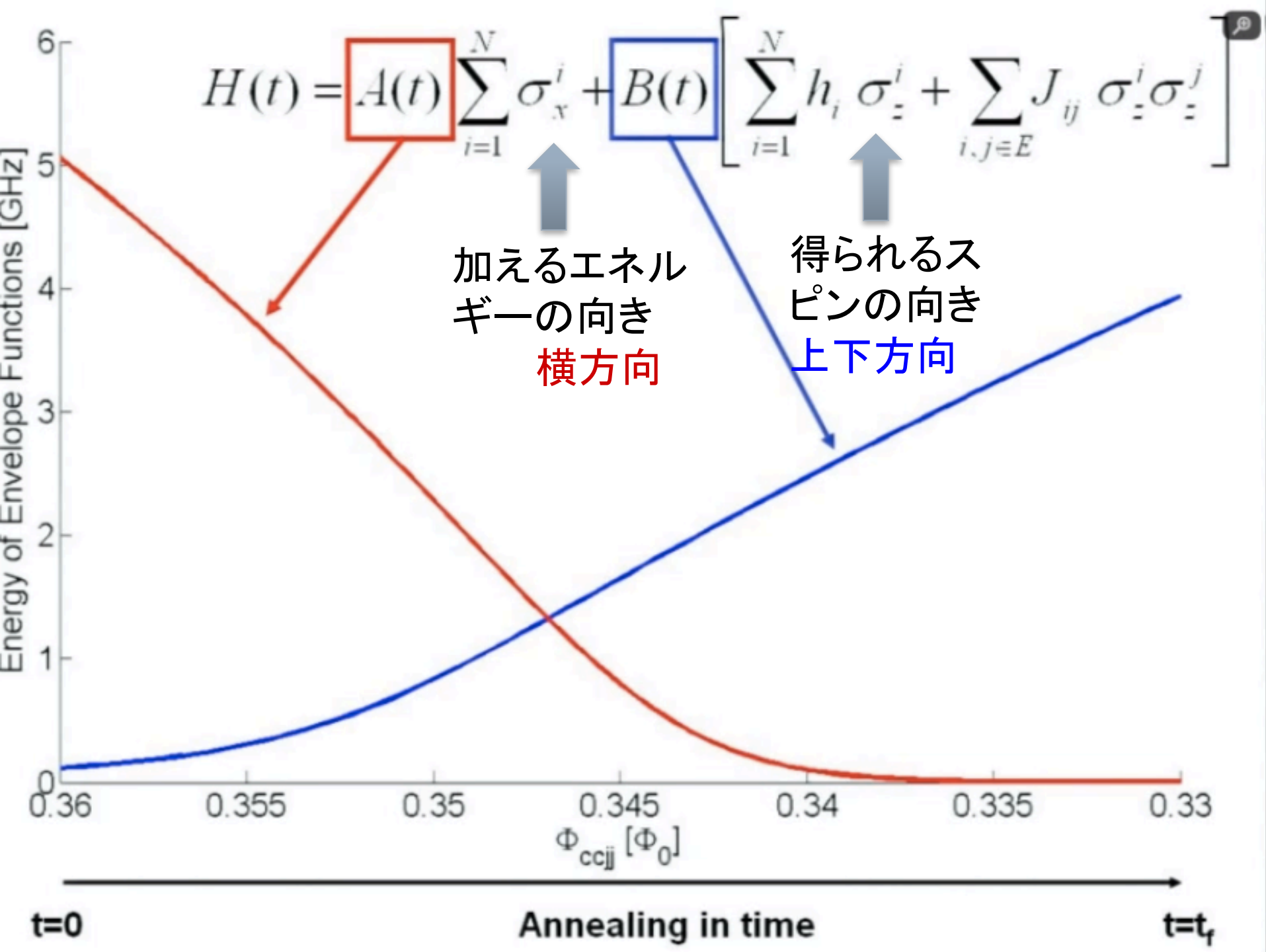


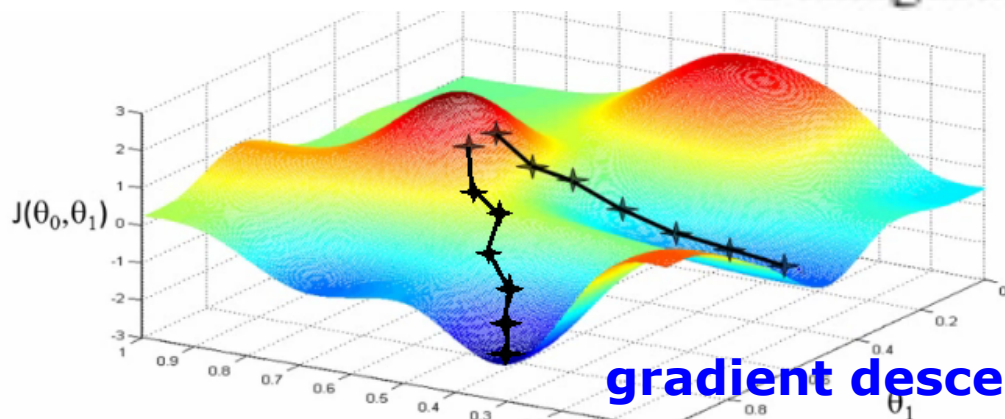
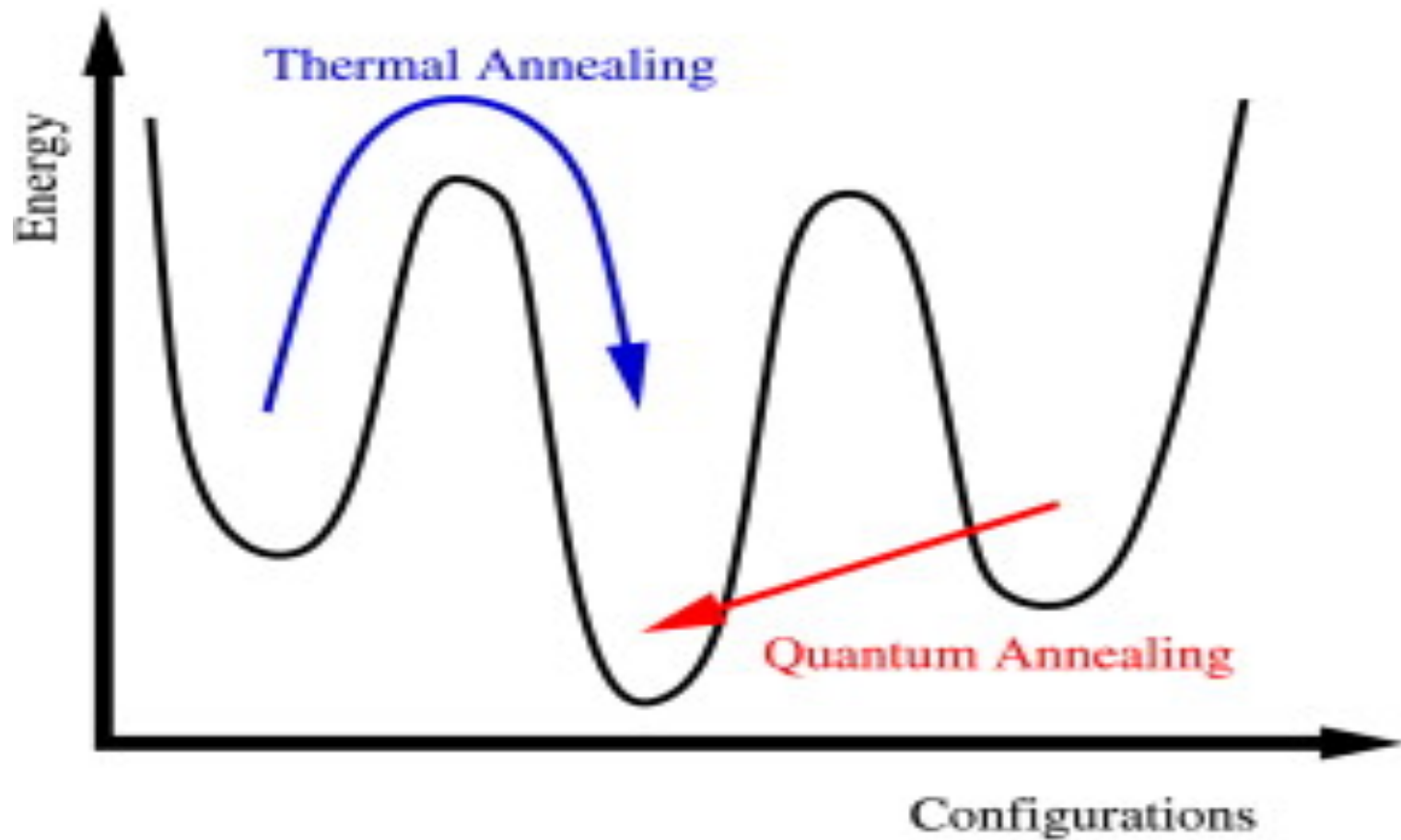
加えるエネルギーを、少しずつ下げていく。



加えるエネルギーがゼロになると、 $E(s)$ が最小になるような状態に落ち着く。この時のスイッチの状態を読み出せば、 $E(s)$ を最小にする問題の解が得られる。







gradient descent method

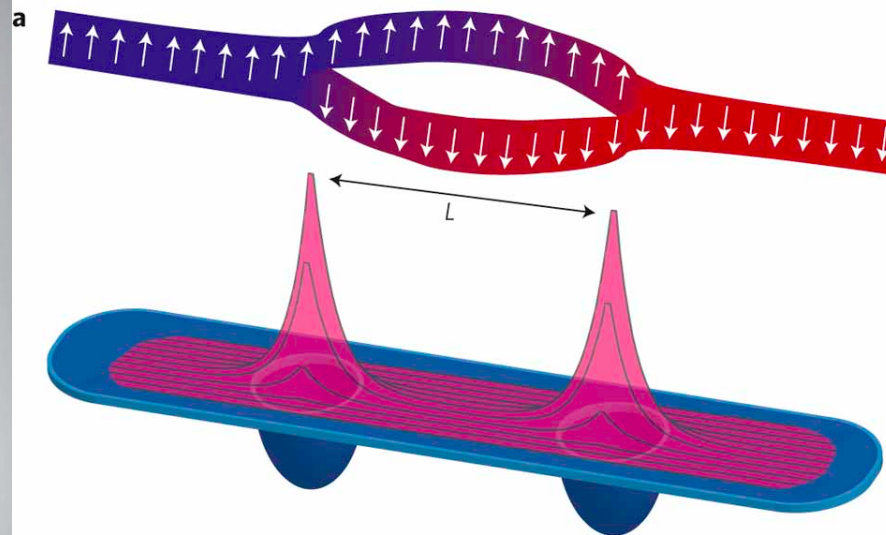
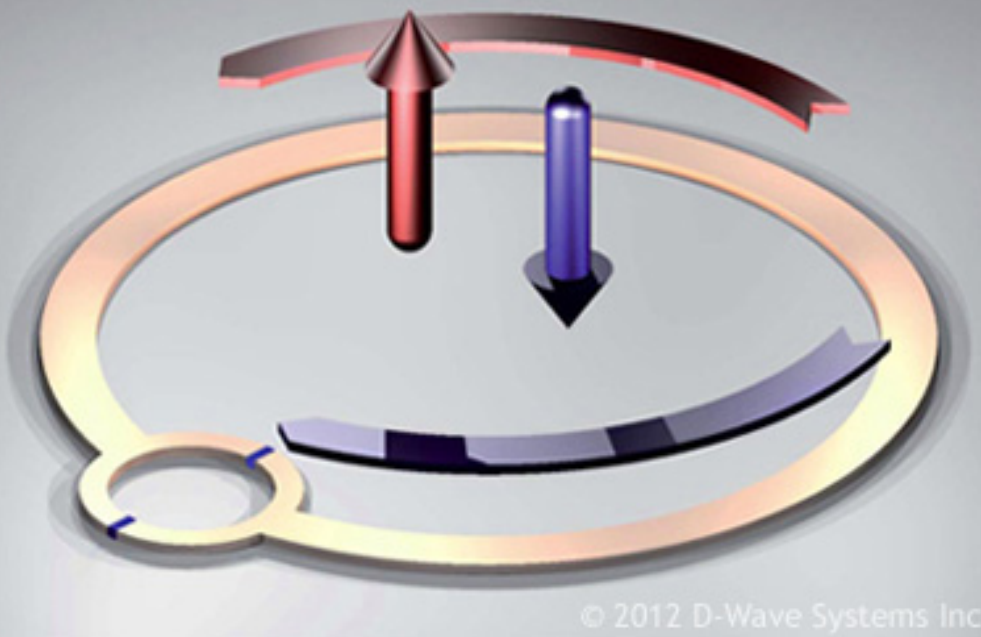
Summary of observations: accuracy

- Solved > 12,000,000 Ising problem instances on 8-, 52- and 72-qubit Rainier chips over past 12 months
- 99.5% gave ground state as **most likely** result
- 99.9995% returned ground state at least once
- Distributions generally Boltzmann-like (but not exactly... QM!)
- Output probability distributions match open quantum systems model with no free parameters



that you've defined. So, just to give you an idea about how well this works, the thing

D-Waveのハードウェアと 機械語レベルのプログラミング

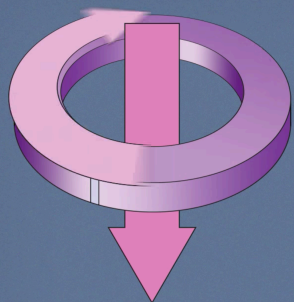


SQUID

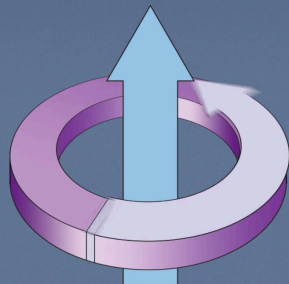
superconducting
quantum
interference
device

D-Waveマシンの
qubitを構成して
いるのは、SQUID
である



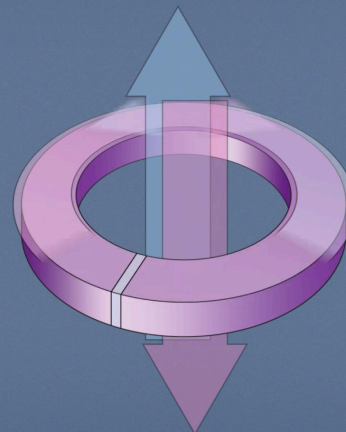


0

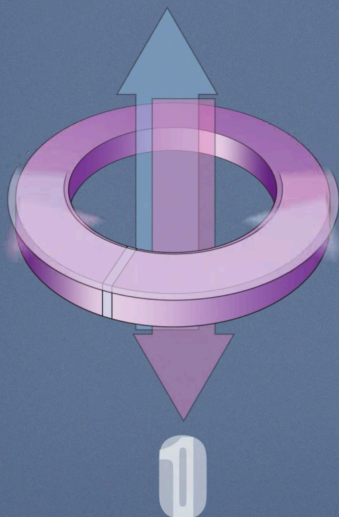


1

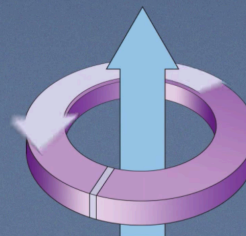
superposition



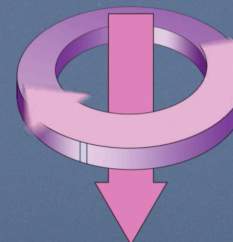
superposition



quantum
annealing

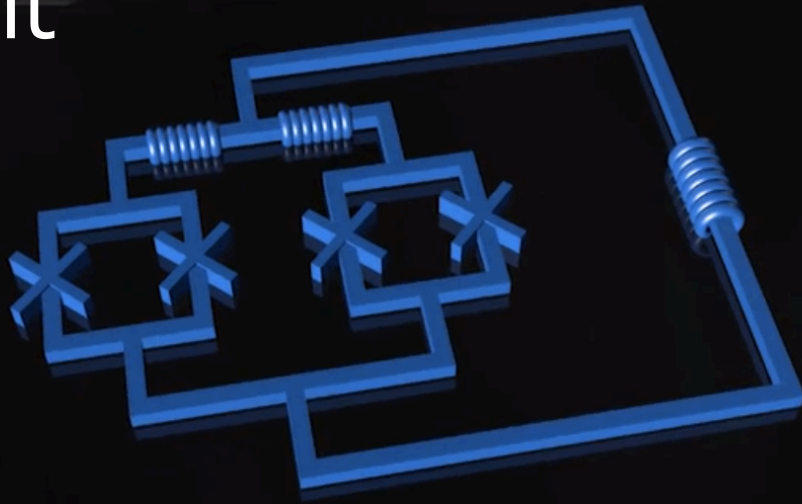


1



0

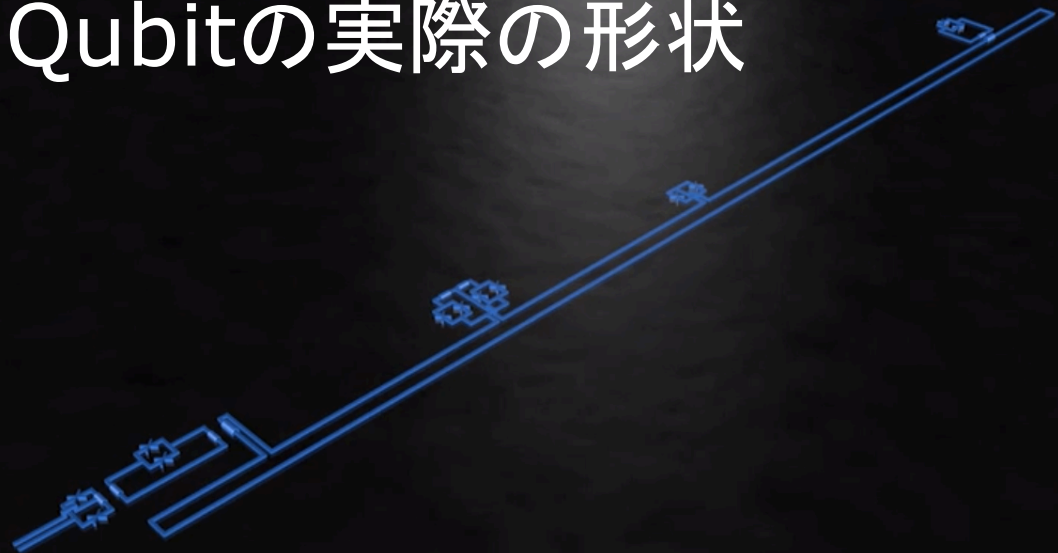
Qubit

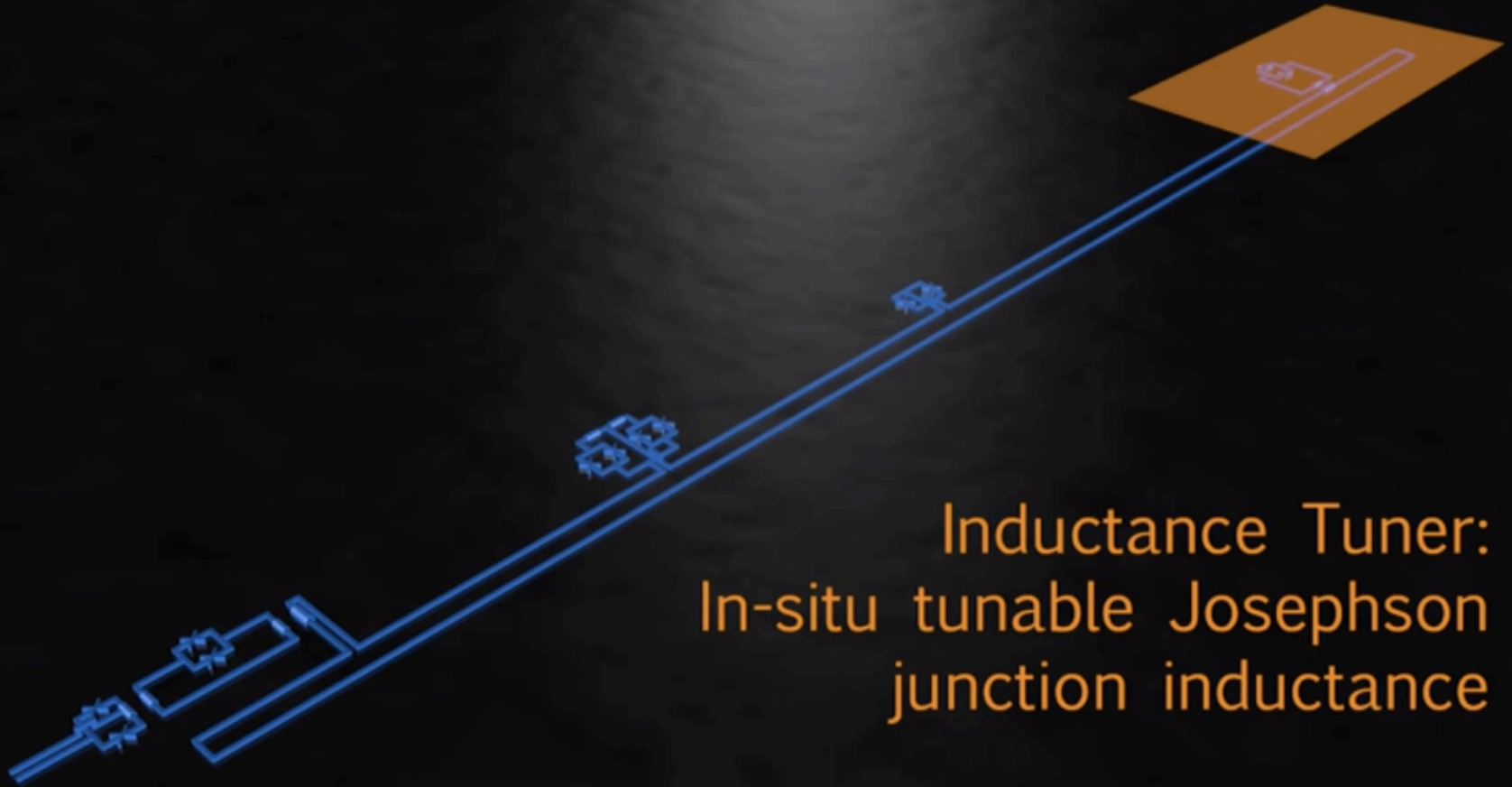


いくつかの技術的な理由から、複数のSQUIDが組み合わされて、一つのqubitを構成している。

チップ上のQubitは、長い矩形状に引き延ばされて、その周囲にいくつかの周辺素子が配列されている。

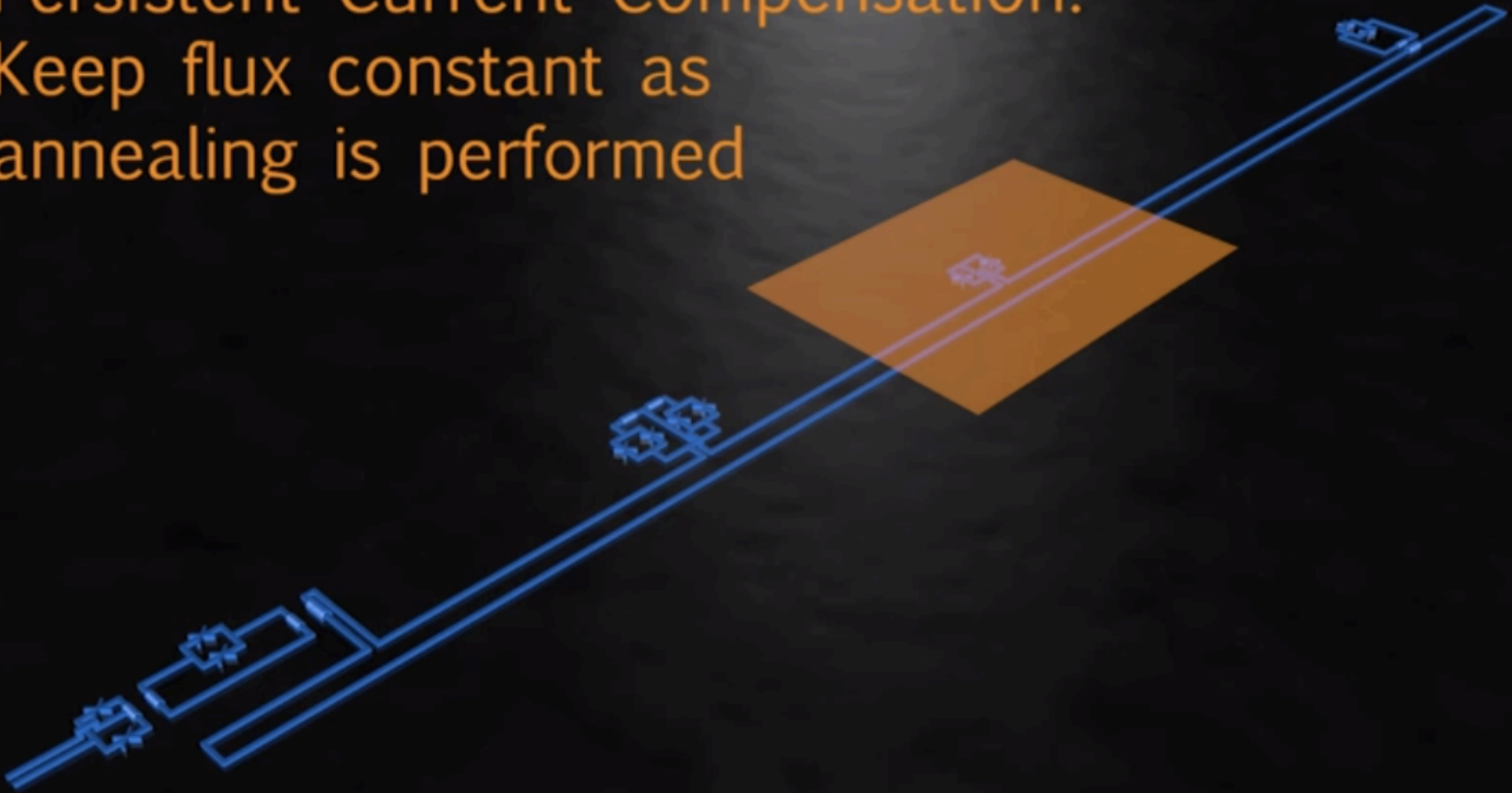
Qubitの実際の形状

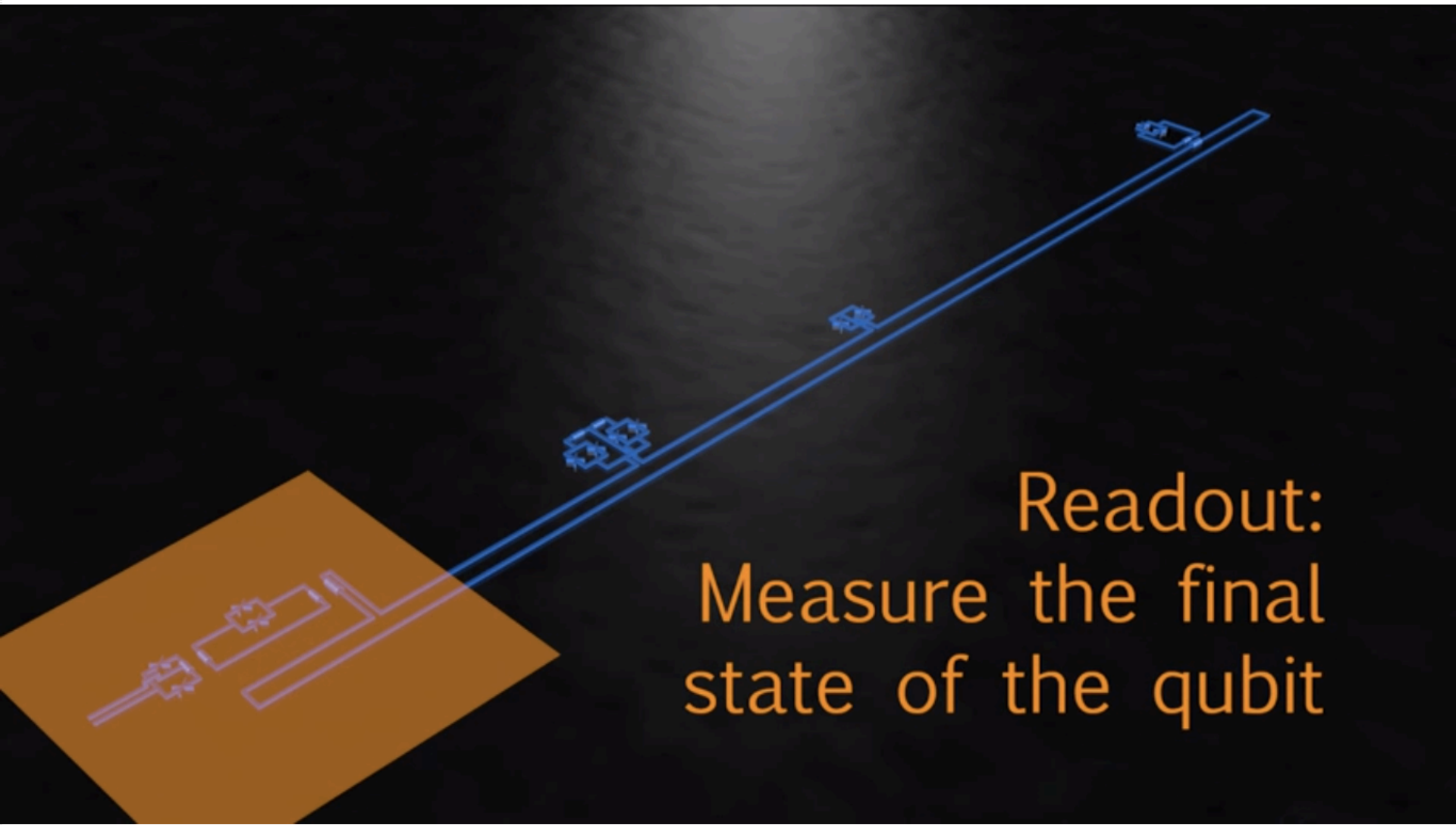




Inductance Tuner:
In-situ tunable Josephson
junction inductance

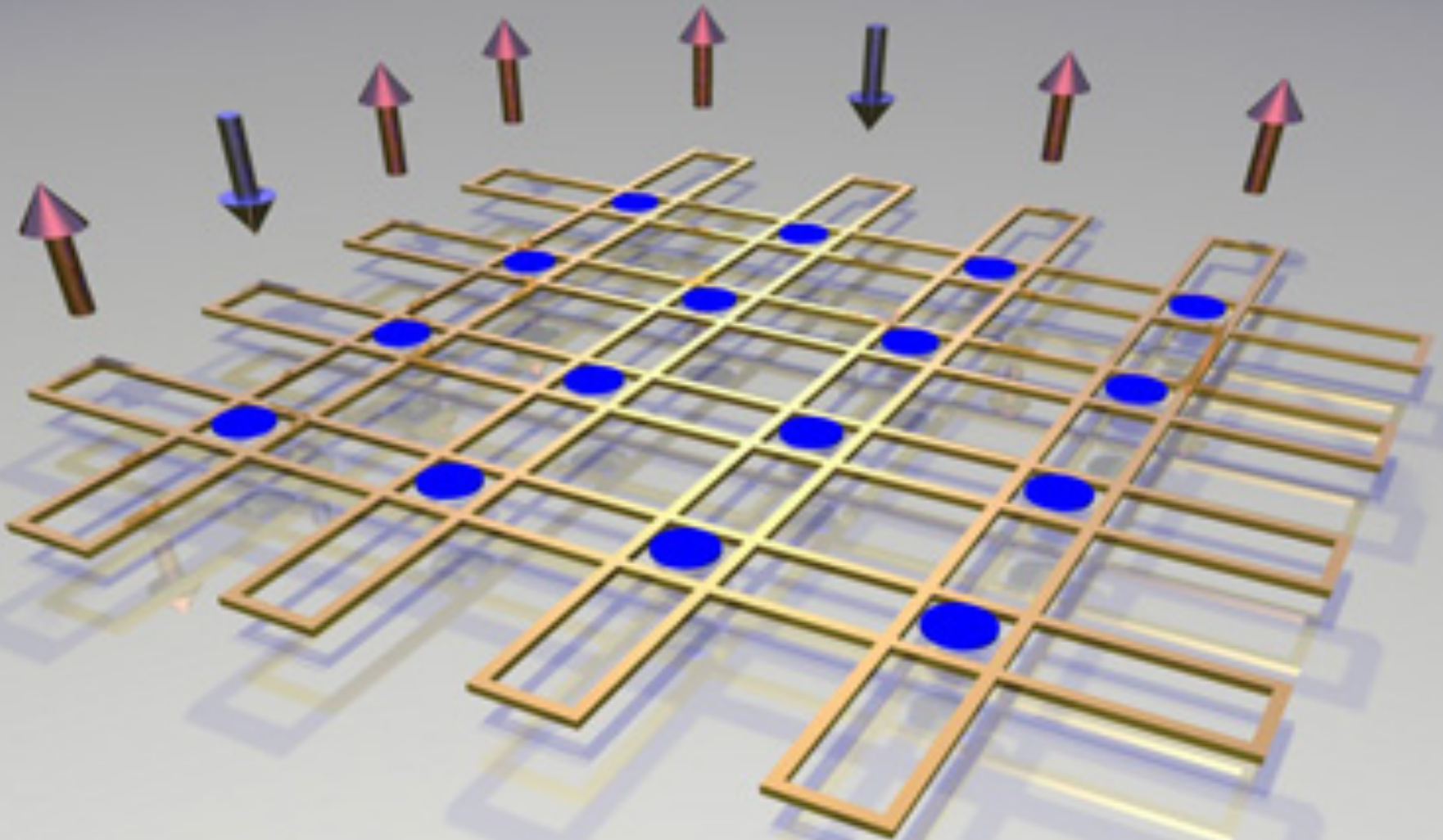
Persistent Current Compensation:
Keep flux constant as
annealing is performed



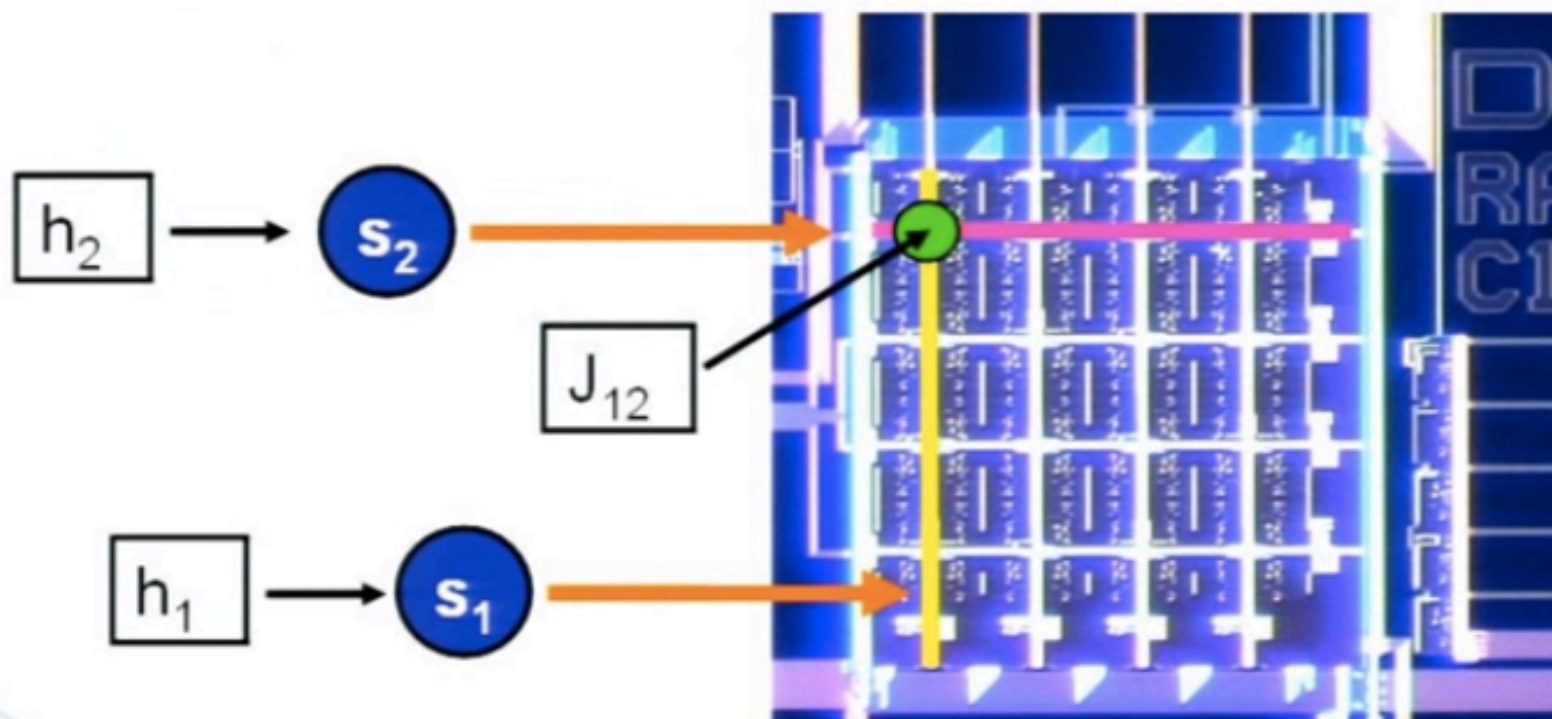


Readout:
Measure the final
state of the qubit

縦四列、横四列に配置された8個の**qubit**の模式図
青色の部分は、**coupler**と呼ばれ、交差するqubit
同士を結合する。

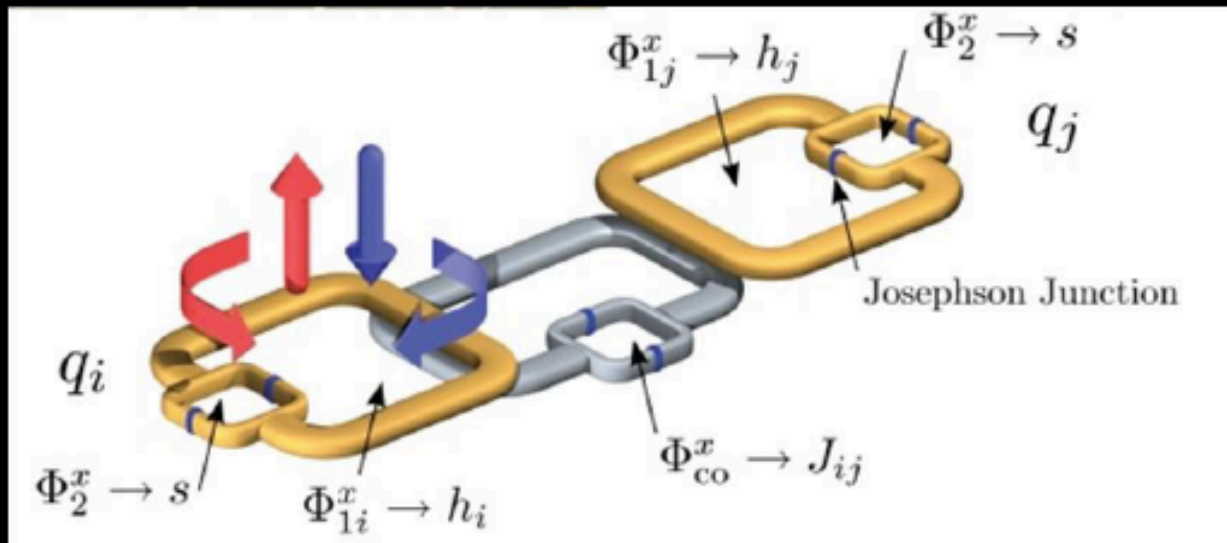


プログラム可能なプロセッサの 二つのタイプ **qubit**と**coupler**



プログラム可能なプロセッサ・デバイス

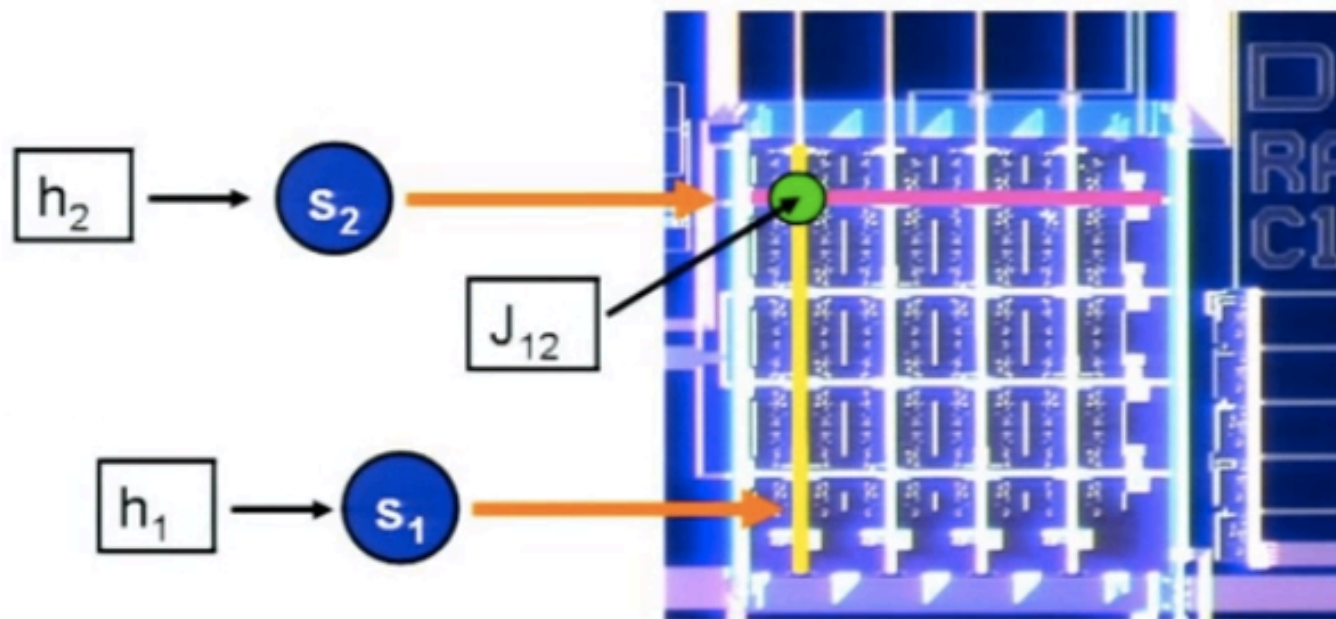
Two types: qubits and couplers



問題をハードウェアで解く

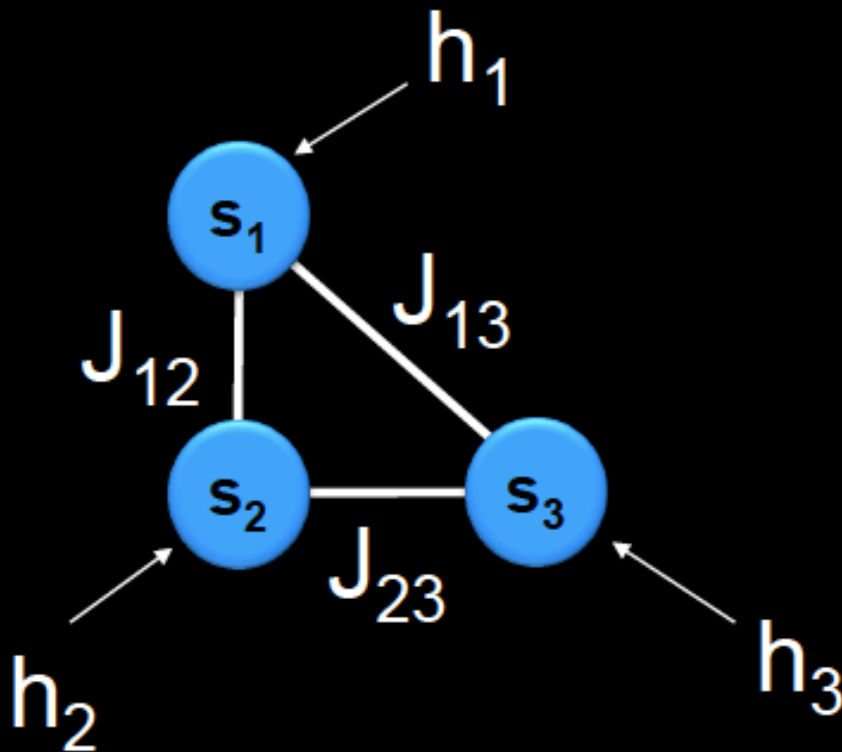
例： 2変数の場合

$$\xi(s_1, s_2) = h_1 s_1 + h_2 s_2 + J_{12} s_1 s_2$$



3変数の場合

$$\xi(s_1, s_2, s_3) = \sum_{j=1}^3 h_j s_j + \sum_{i < j} J_{ij} s_i s_j$$



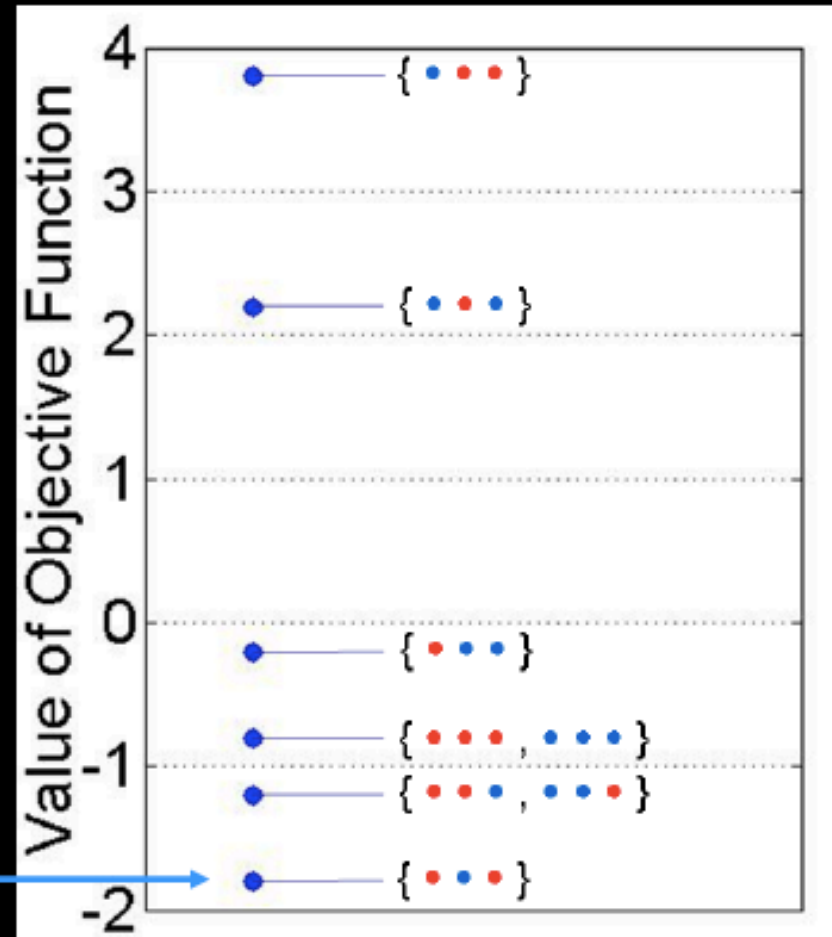
h	J
$h_1 = +1.0$	$J_{12} = -1.0$
$h_2 = -1.0$	$J_{13} = -0.5$
$h_3 = 0$	$J_{23} = +0.3$

$$\xi(s_1, s_2, s_3) = \sum_{j=1}^3 h_j s_j + \sum_{i < j} J_{ij} s_i s_j$$

3変数の場合

s_1	s_2	s_3	ξ
-1	-1	-1	-1.2
-1	-1	+1	-0.8
-1	+1	-1	-1.8
-1	+1	+1	-0.2
+1	-1	-1	3.8
+1	-1	+1	2.2
+1	+1	-1	-0.8
+1	+1	+1	-1.2

エネルギーの最小値は、
量子アニーリングで自動的に
見つかる



Notation: +1 = ●, -1 = ●

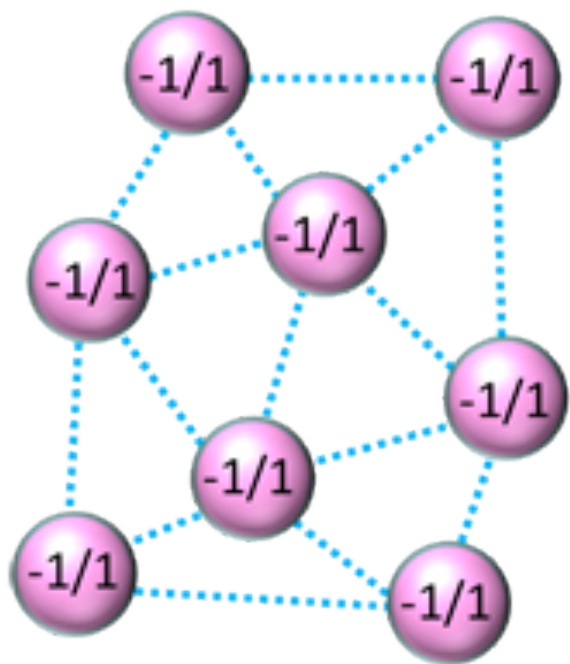
機械語レベルのプログラミング

$$\xi(s_1, \dots, s_N) = \sum_{j=1}^N h_j s_j + \sum_{i,j \in E} J_{ij} s_i s_j \longleftrightarrow H_P = \sum_{j=1}^N h_j \sigma_j^z + \sum_{i,j \in E} J_{ij} \sigma_i^z \sigma_j^z$$

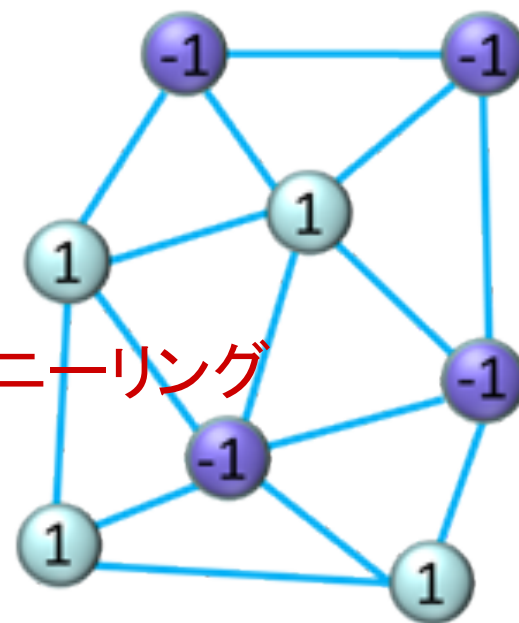
Optimization	Hardware
Variables s_j	Qubits σ_j^z
Linear terms h_j	Qubit biases h_j
Quadratic terms J_{ij}	Coupler biases J_{ij}
Allowed edge set E	Locations of couplers between qubits
Objective function values $\xi(s_1, \dots, s_N)$	Allowed energy eigenvalues E

D-Waveのマシン語レベルのプログラムとは、
 h_j と J_{ij} を与えること。

Superposition状態の
量子ビットが入力

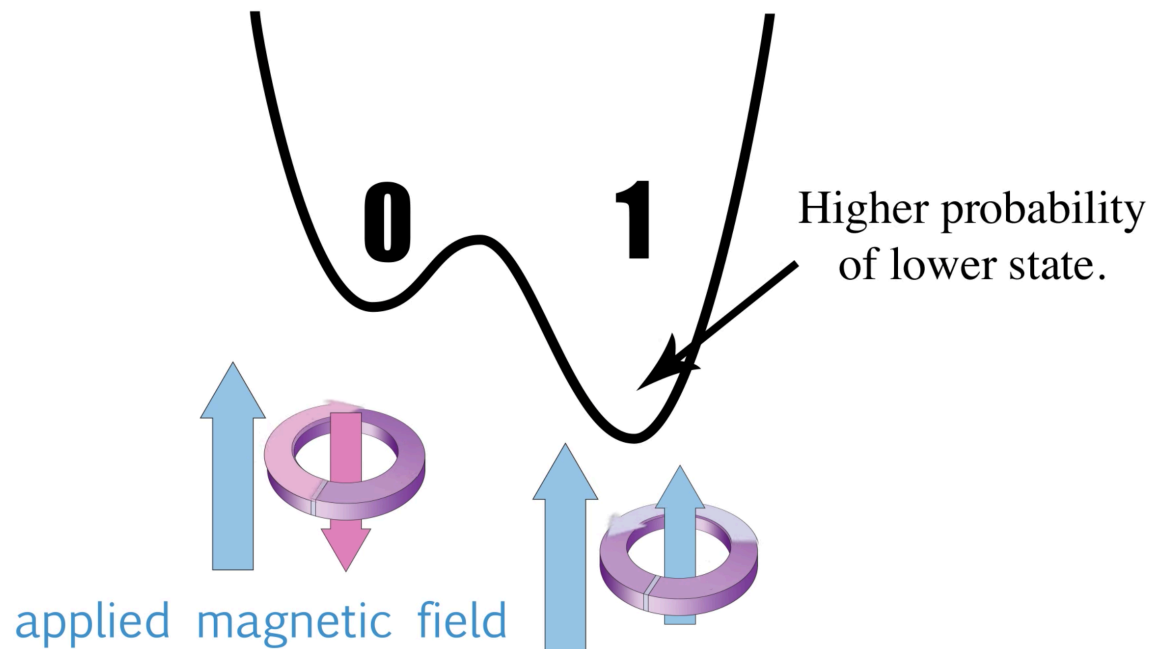
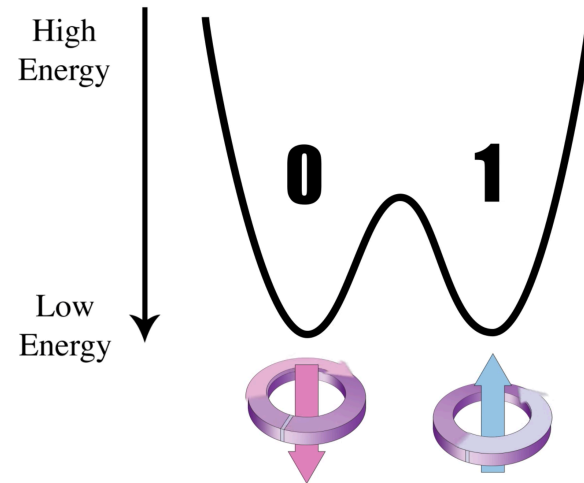
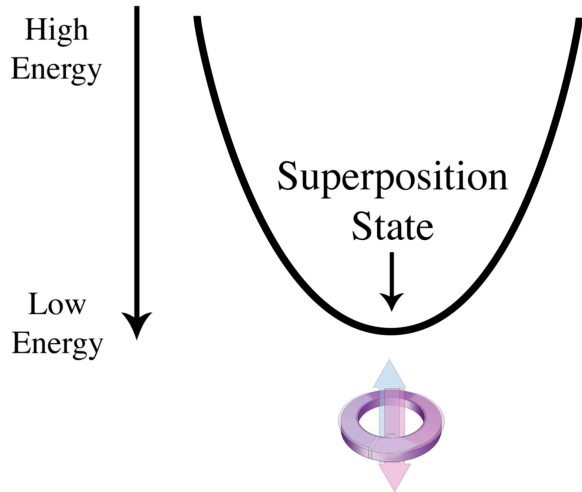


量子アニーリング



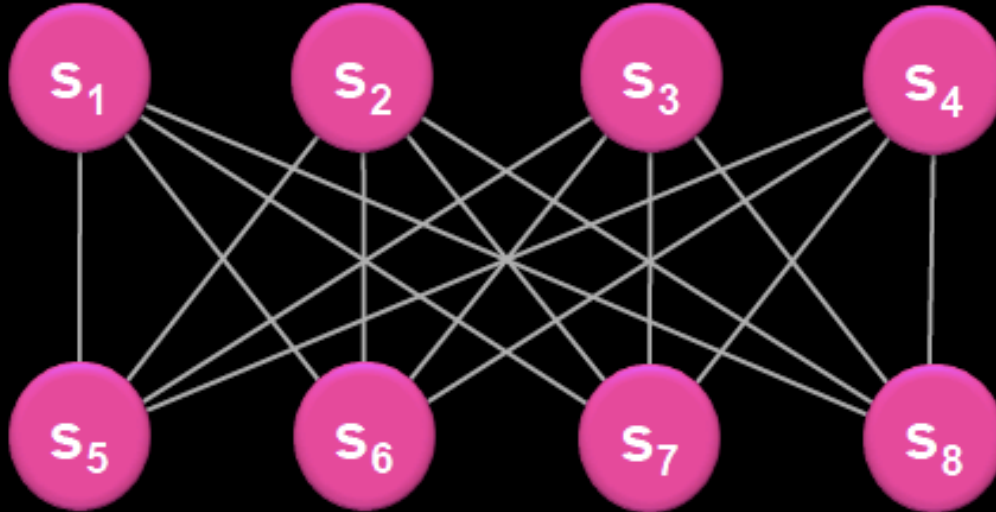
最良のビットの配置が
出力される

エネルギーを最小にする問題と
して、プログラムを与える



量子アニーリング

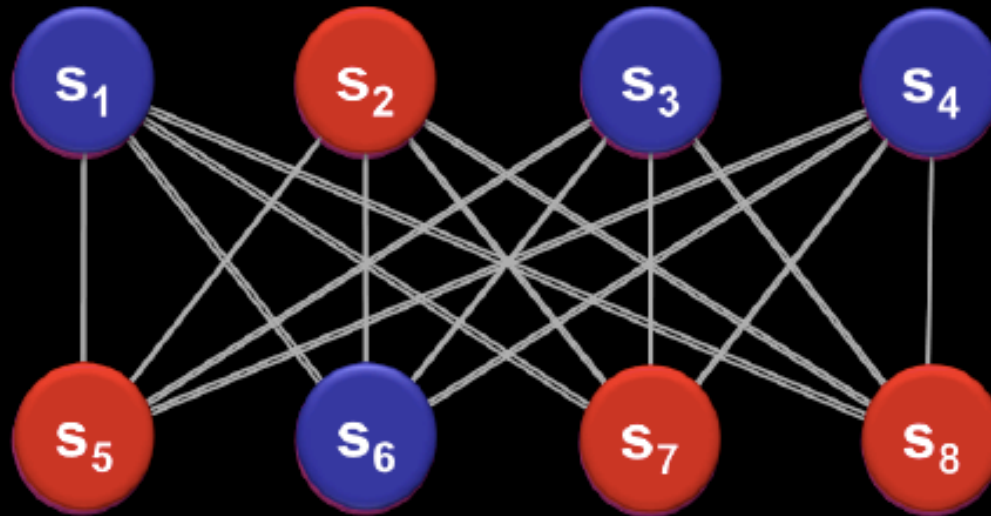
すべてのqubitが superpositionにある状態から始める



8個のqubitなら、可能な 2^8 の状態が同時に存在することになる

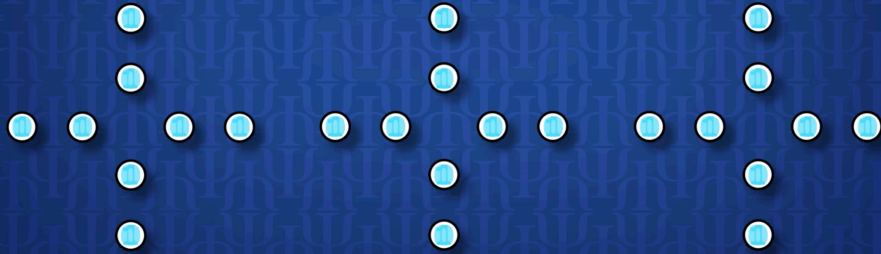
量子アニーリング

superposition状態が破れると、 h , J の設定に応じて、それぞれのノードは、エネルギーが最小になるような、 $+1$ または -1 の値に落ち着く。

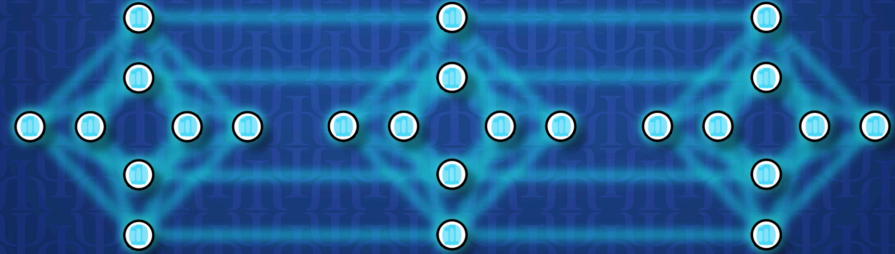


Initial states is quantum

$$\text{Energy } \mathcal{H}_S(s) = \text{Initial Hamiltonian} - \frac{1}{2} \sum_i \Delta(s) \sigma_i^x$$



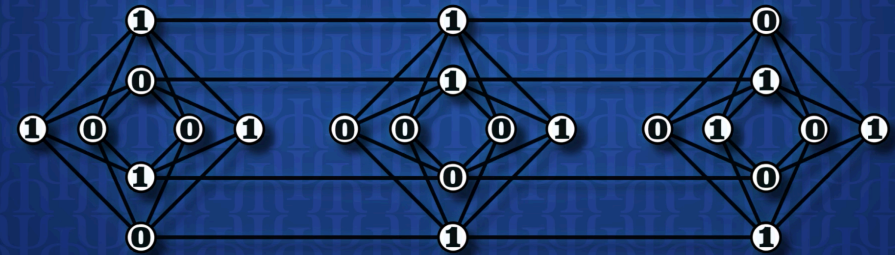
$$\text{Energy } \mathcal{H}_S(s) = \text{Initial Hamiltonian} - \frac{1}{2} \sum_i \Delta(s) \sigma_i^x + \text{Final Hamiltonian } \mathcal{E}(s) \left(-\sum_i h_i \sigma_i^z + \sum_{i < j} J_{ij} \sigma_i^z \sigma_j^z \right)$$



$$\text{Energy } \mathcal{H}_S(s) = \text{Initial Hamiltonian} - \frac{1}{2} \sum_i \Delta(s) \sigma_i^x + \text{Final Hamiltonian } \mathcal{E}(s) \left(-\sum_i h_i \sigma_i^z + \sum_{i < j} J_{ij} \sigma_i^z \sigma_j^z \right)$$



$$\text{Energy } \mathcal{H}_S(s) = \text{Final Hamiltonian } \mathcal{E}(s) \left(-\sum_i h_i \sigma_i^z + \sum_{i < j} J_{ij} \sigma_i^z \sigma_j^z \right)$$

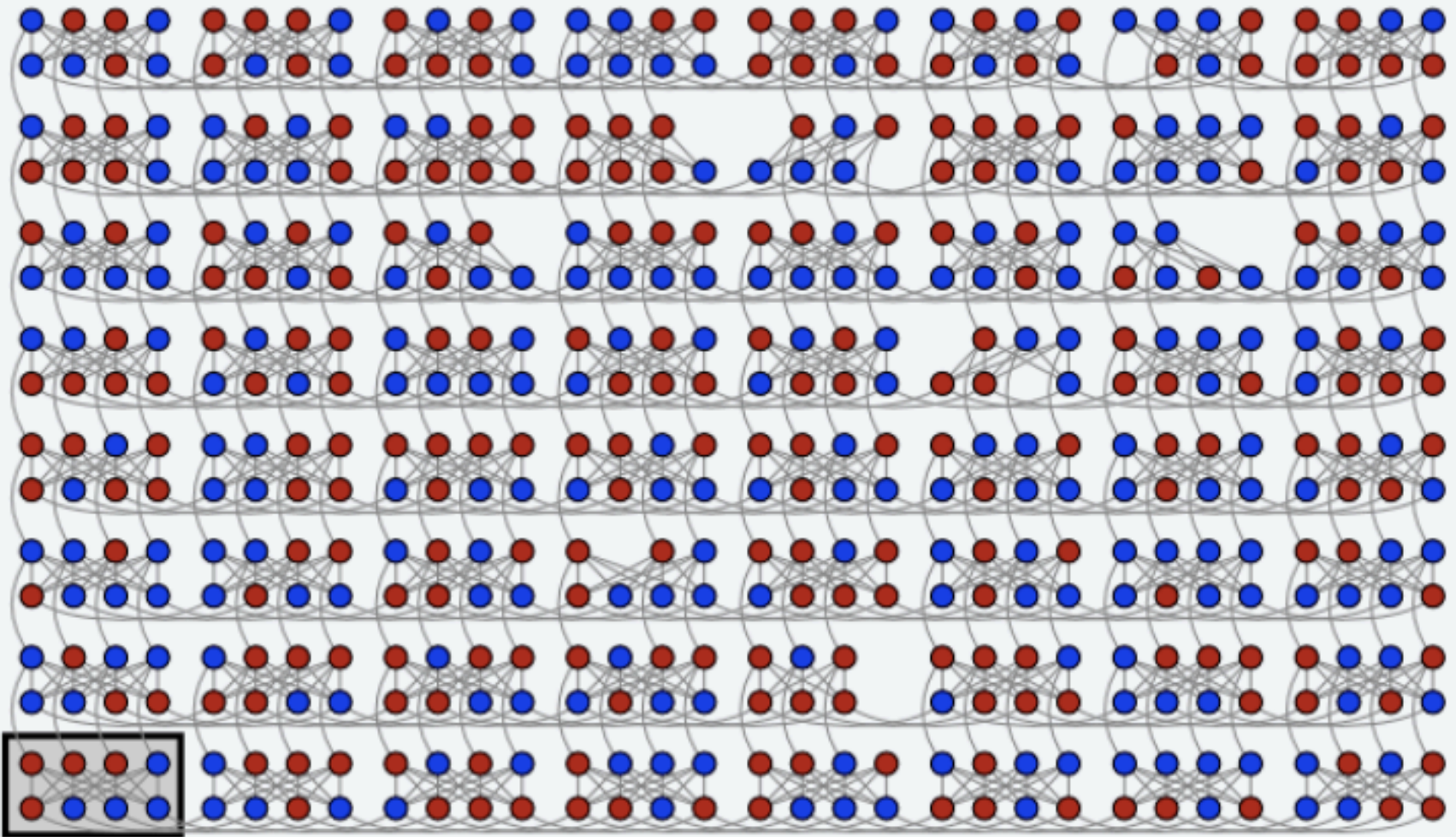


Final states is classic

Vesuvius SR10-V6

500 qubits, 1,472 couplers

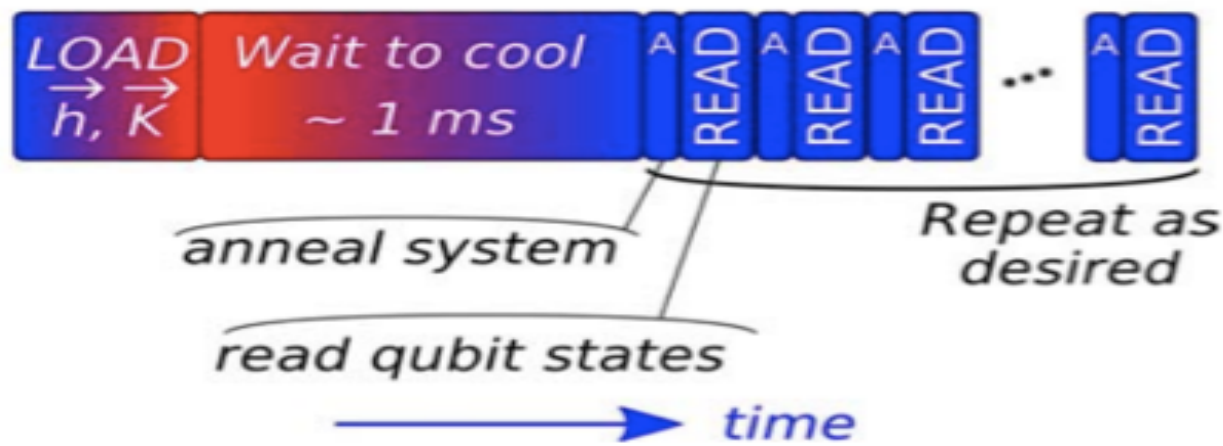
技術的なことになるが、この図は、external couplerがqubit間をどのように結合しているかを示していて、興味深いものだ。



プロセッサの処理

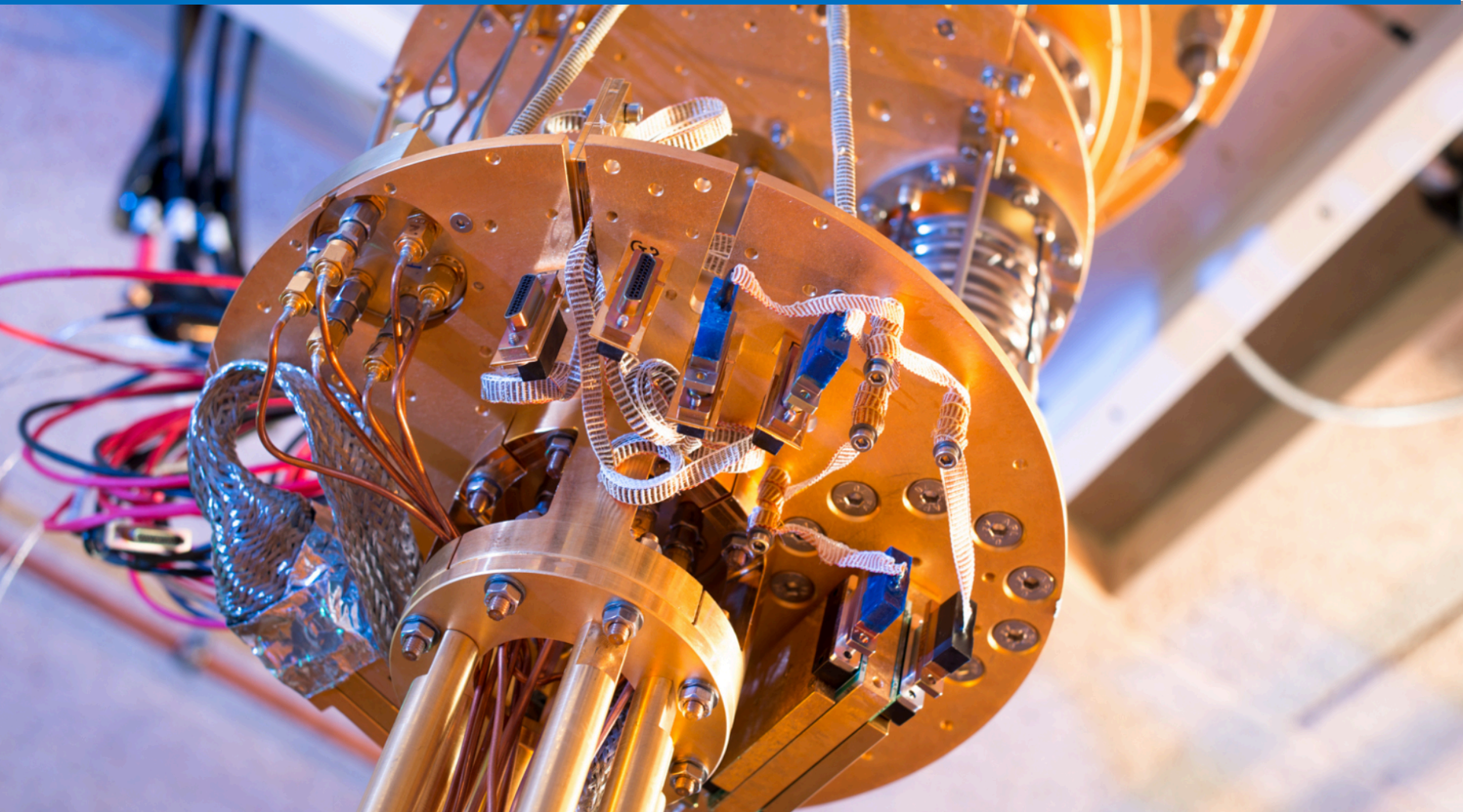
1. (h, J) の値を、サブシステムを利用してセットする。
2. チップが操作可能な温度にまで下がるのを待つ。
3. QA(Quantum Annealing)アルゴリズムを実行する。
4. Readoutサブシステムを利用して、全てのqubitの値を読み出す。
5. 2-4のプロセスを、ユーザーがセットした回数繰り返す。

Chip Level Timing Diagram



Part V

量子コンピュータの動向



量子コンピュータの動向

ここでは、量子コンピュータをめぐる最近の動向をまとめた。

この数年以内に、50 qubit程度のシステムを安定的に構築する技術的目処が付き始めたことをきっかけに、ビジネス利用の可能性の模索が始まっている。それは、将来の飛躍を準備していこう。



Quantum Computing for Business

NASA-AMES RESEARCH CENTER, BUILDING 152 | MOUNTAIN VIEW, CALIFORNIA

DECEMBER 4 - 6, 2017

<https://www.q2b.us/>

Guest Speakers



John Preskill

Keynote Speaker,
California Institute
of Technology



John Martinis

Google



Jerry Chow

IBM



Bo Ewald

D-Wave



Martin Hofmann

VW



Thierry Botter

Airbus



Paul Burchard

Goldman Sachs



Shaun Maguire

GV

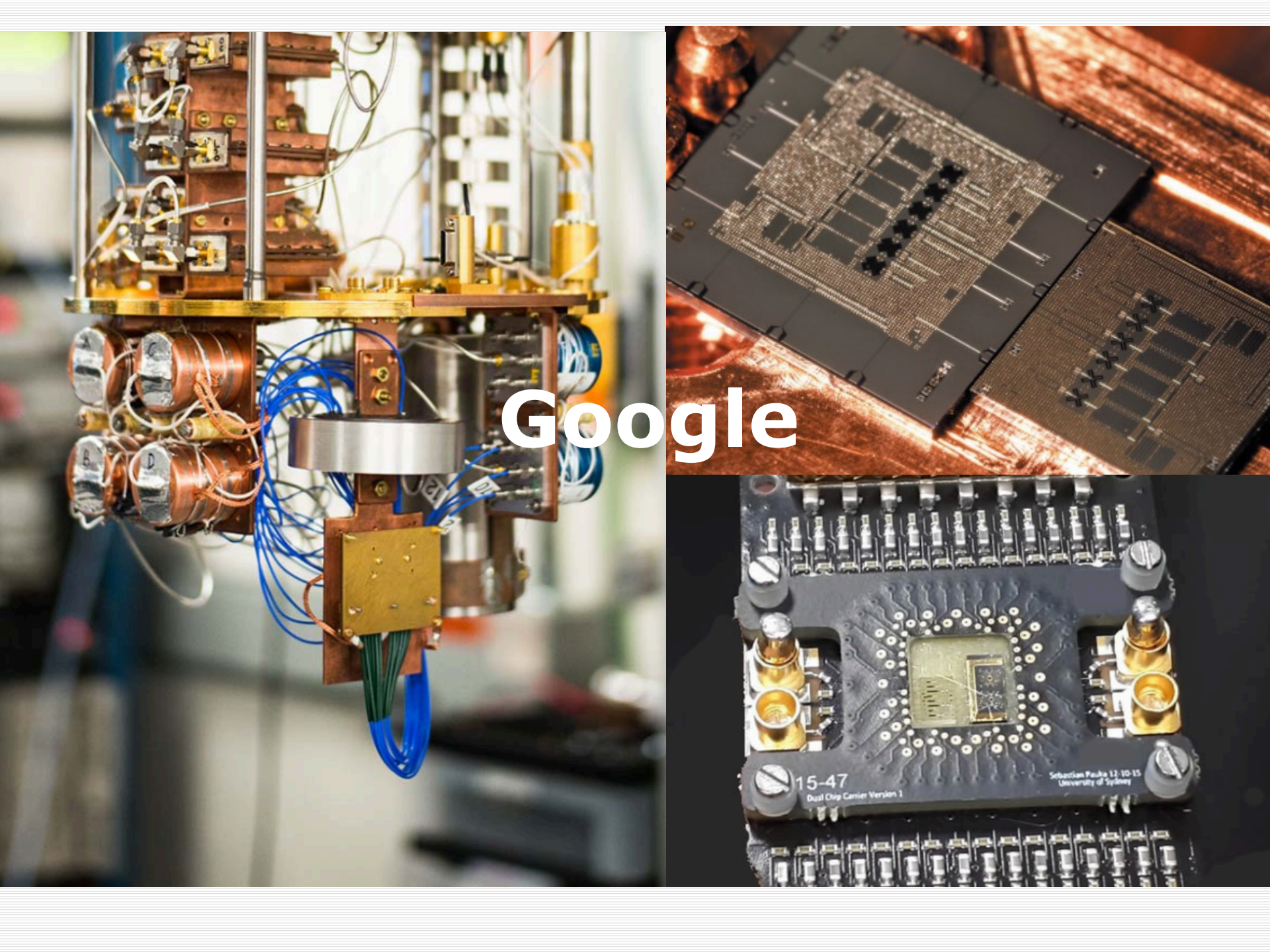
7:30 - 8:30 AM	<i>Breakfast</i>
8:30	Master of Ceremonies: <u>Matt Johnson</u>, CEO, QC Ware
8:30 - 9:15 AM	Keynote: <u>John Preskill</u>, Caltech
9:15 - 10:00 AM	Digital Quantum Computing: John Martinis, Google
10:00 - 10:30 AM	Analog Quantum Computing: <u>Bo Ewald</u>, President, D-Wave International

10:30 - 10:45 AM	<i>Networking Break</i>
10:45 - 11:15 AM	Quantum Chemistry Applications: Bert de Jong, LBL
11:15 - 11:45 AM	Prospects for Quantum Machine Learning: The Promise and the Caveats: <u>Peter McMahon</u> , Postdoctoral Researcher, Stanford University & QC Ware
11:45 - 12:15 AM	Optimization Applications: Masoud Mohseni, Google

12:15 - 1:30 PM	<i>Networking Lunch</i>
1:30 - 2:00 PM	QC for the Automotive Industry: Martin Hoffman, VW
2:00 - 2:30 PM	QC Application for Finance: Paul Burkhard, Goldman Sachs
2:30 - 3:00 PM	QC Applications in Aerospace: Thierry Botter, Airbus
3:00 - 3:30 PM	QC Applications in Transport/Logistics and Manufacturing: Yianni Gamvros, IBM
3:30 - 4:00 PM	<i>Networking Break</i>
4:00 - 4:30 PM	US Public-Sector QC Funding: Carl Williams, NIST
4:30 - 5:00 PM	European Public-Sector QC Funding: Juergen Mlynek, EU Flagship Program
5:00 - 5:30 PM	Chinese QC Funding: Xiaobo Zhu, USTC

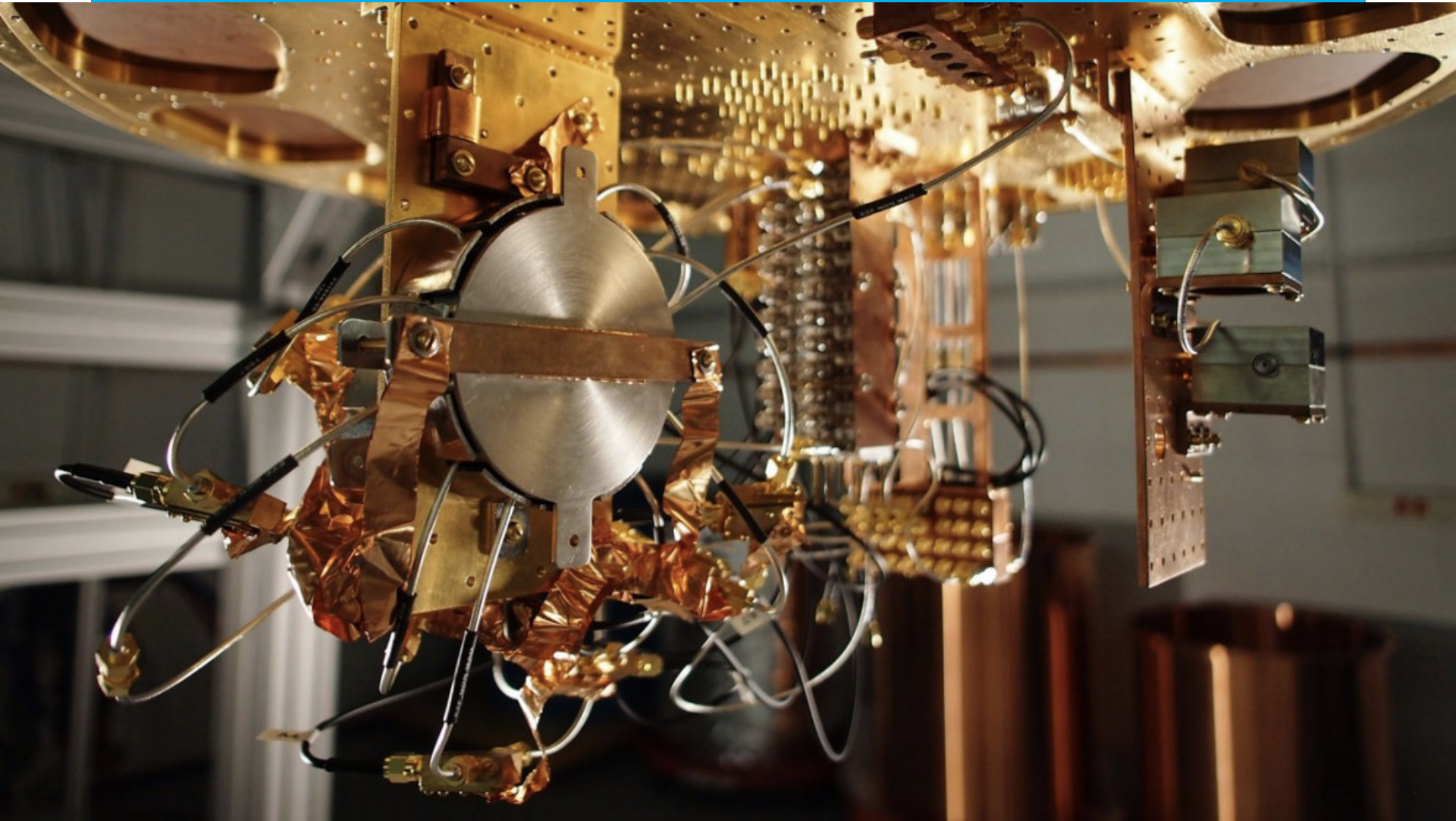
7:30 - 8:30 AM	<i>Breakfast</i>
8:30	Master of Ceremonies: Matt Johnson , CEO, QC Ware
8:30 - 9:15 AM	Keynote: Rupak Biswas, NASA Hardware
9:15 AM - 10:00 AM	ATOS - QC Simulation Products: Jerome Sandrini, ATOS
10:00 - 10:30 AM	IBM - QC Hardware/Software Programs: Jerry Chow, IBM
10:30 - 10:45 AM	<i>Break</i>
10:45 - 11:15 AM	Microsoft - QC Hardware/Software Programs: Julie Love , Microsoft
11:15 - 11:45 AM	IonQ - Ion Trap QC Program: Dave Moehring, CEO, IonQ
11:45 AM - 12:15 PM	Hardware Panel: John Martinis, Google; Jerry Chow, IBM; Bob Willett, Nokia; Bo Ewald, D-Wave; Dave Moehring, IonQ, Xiaobo Zhu, USTC

12:15 - 1:30 PM	<i>Networking Lunch</i>
1:30 - 2:00 PM	VC Perspective on QC Investment Opportunities: <u>Shaun Maguire</u> , GV
2:00 - 2:30 PM	VC Panel: <u>Shaun Maguire</u> , GV; Maryanna Saenko, DFJ; Luka Tomljenovic, Airbus; Aaron VanDevender, Founders Fund; Joe Raffa, IBM Ventures; Aaron Sisto, IQT
2:30 - 3:00 PM	VCの投資 Software Panel: <u>Matt Johnson</u> , QC Ware; Chris Savoie, Zapata; Andrew Fursman, 1QBit; Michael Brett, QxBranch
3:00 - 3:30 PM	Closing Remarks



Google

Google's Quantum Dream Machine



<https://goo.gl/Y9zvV5>

Google's Quantum Dream Machine

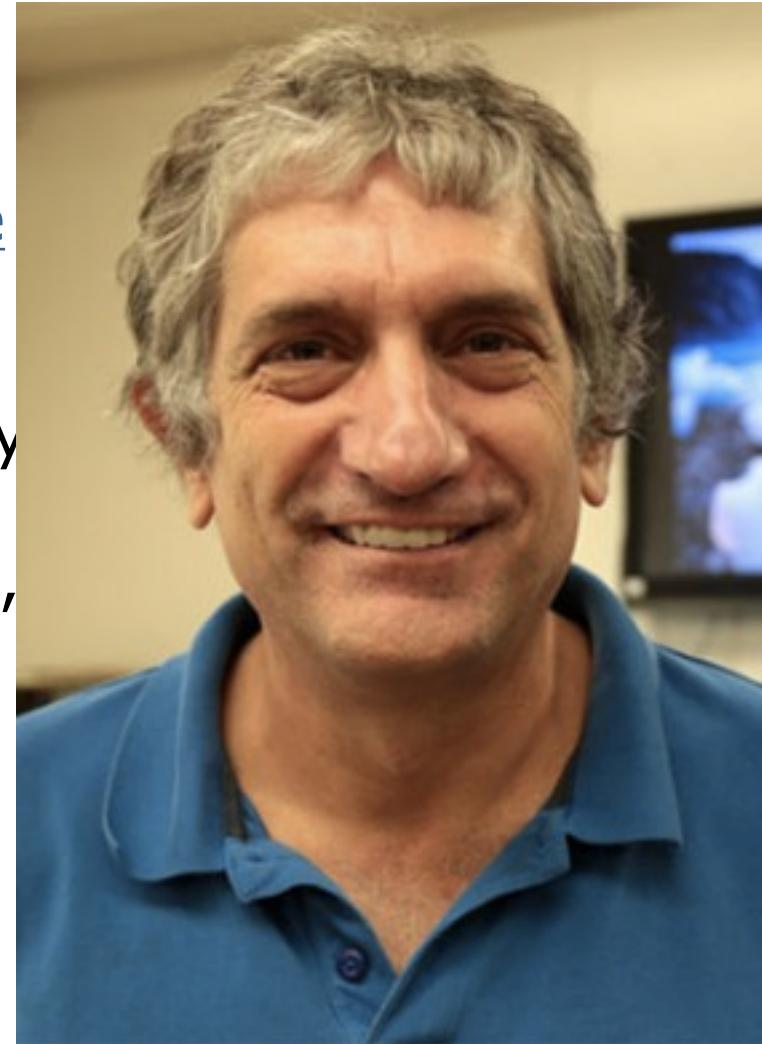
John Martinis

- The theoretical underpinnings of quantum computing are well established. And physicists can build the basic units, known as qubits, out of which a quantum computer would be made. They can even operate qubits together in small groups. But they have not made a fully working, practical quantum computer.
- Martinis is a towering figure in the field: his research group at the University of California, Santa Barbara, has demonstrated some of the most reliable qubits around and gotten them running some of the code a quantum computer would need to function.

<https://goo.gl/MTrLFX>

John Martinis

- He was [hired by Google in June 2014](#) after persuading the company that his team's technology could mature rapidly with the right support. With his new Google lab up and running, Martinis guesses that he can demonstrate a small but useful quantum computer in two or three years. "We often say to each other that we're in the process of giving birth to the quantum computer industry," he says.



<https://goo.gl/MTrLFX>

“Commercialize early quantum technologies”

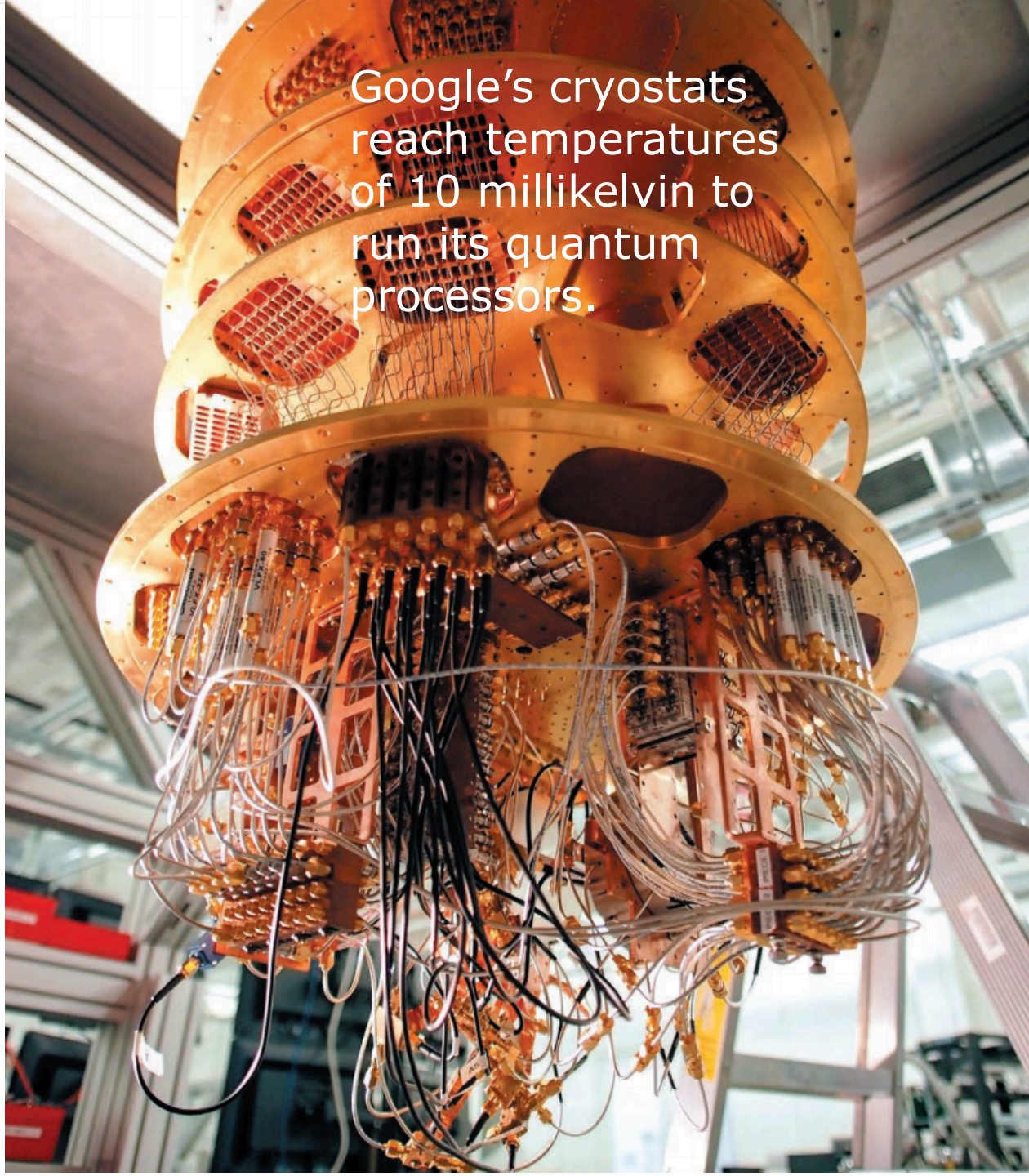
Masoud Moand hseni, Peter Read, Hartmut Neven et al. (Google Quantum AI Laboratory)

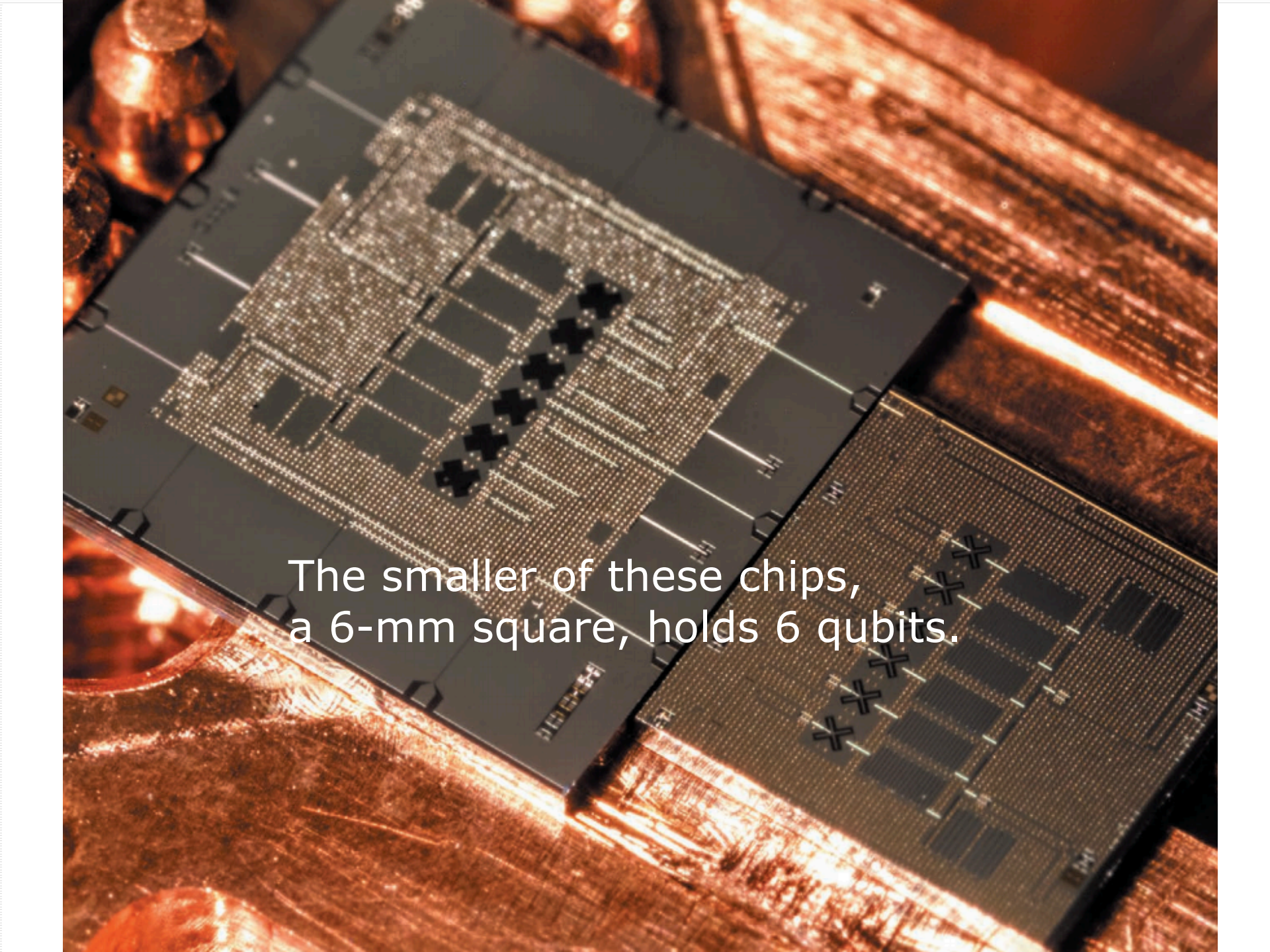
NATURE誌 VOL 543

<https://goo.gl/4qee3o>

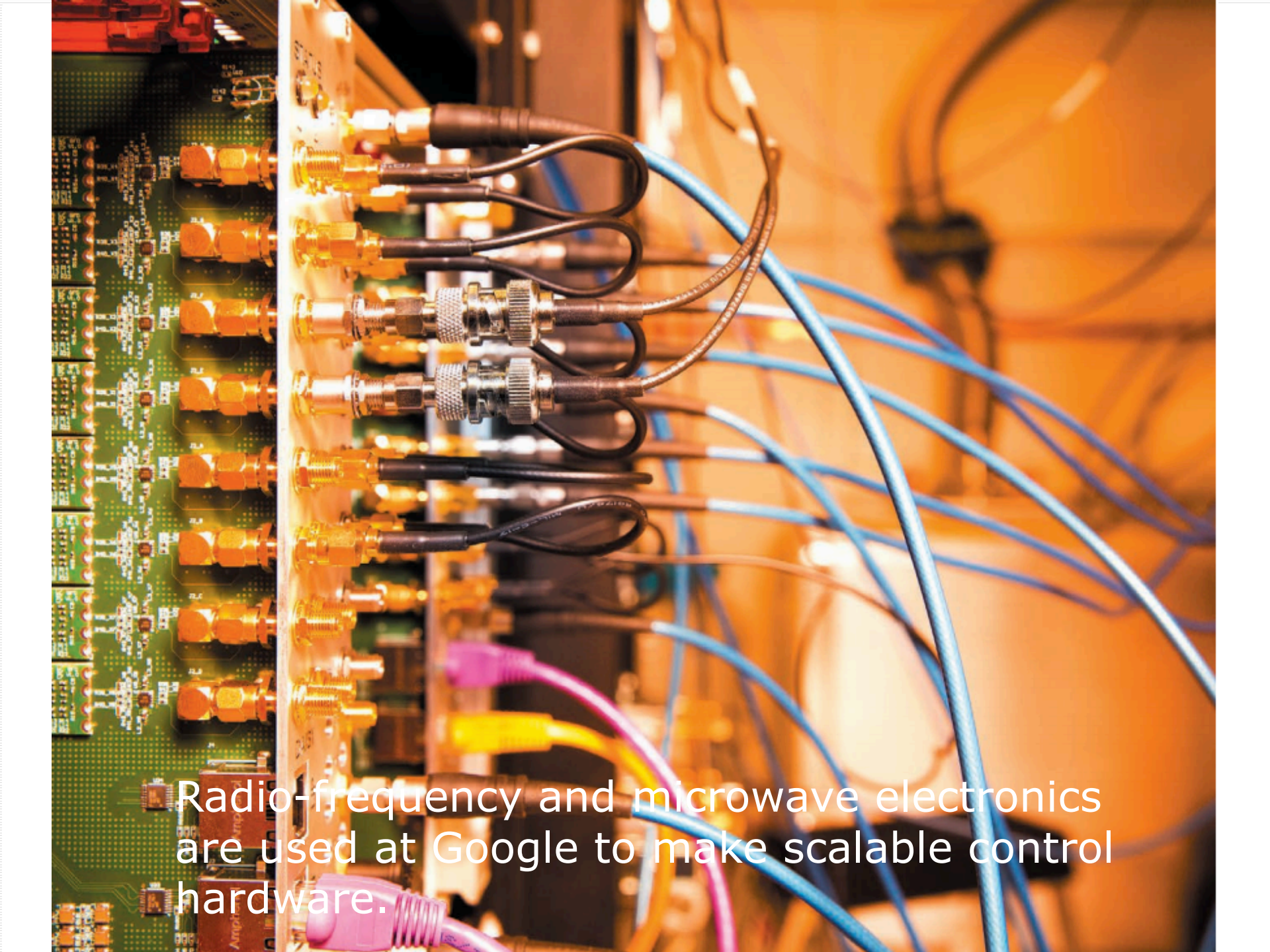
2017年3月9日

Google's cryostats reach temperatures of 10 millikelvin to run its quantum processors.



A close-up photograph of two superconducting qubit chips mounted on a copper substrate. The chips are dark, rectangular, and feature a grid of small, dark, cross-shaped structures. The copper substrate is highly reflective and shows some wear. The lighting is warm, highlighting the metallic surfaces.

The smaller of these chips,
a 6-mm square, holds 6 qubits.



Radio-frequency and microwave electronics are used at Google to make scalable control hardware.

-
- ❑ 量子コンピューティングについてのこの保守的な見方は、投資家が長期的にのみ利益を得るという印象を与える。我々は、今後5年以内に出現する小型デバイスでは、完全な誤り訂正の能力が欠けているにもかかわらず、短期間でのリターンが可能であると主張している。
 - ❑ 理論的保証が欠けていることは、必ずしも成功を排除するものではない。量子論的と古典的なアプローチを融合したヒューリスティックな「ハイブリッド」手法は、将来の強力なアプリケーションの基盤となる可能性がある。
-

THREE PRIORITIES

1. Quantum simulation

- **化学反応とマテリアルのモデリング**は、量子コンピューティングの最も期待される応用の1つである。何年もかけて、何百万ドルも費やして、ほんの一握りの材料を作って、その特徴を知るかかわりに、研究者は何百万もの候補を、コンピュータ上で研究することができるだろう。
- **航空機用のポリマー、車用のより効果的な触媒コンバータ、太陽電池用のより効率的な材料、より優れた医薬品、より通気性の高い繊維**など、目的が何であれ、より高速な発見のパイプラインは、莫大な価値をもたらすだろう。
- 様々なビジネスモデルが量子シミュレータを提供することができる。研究所はアクセスのためにサブスクリプションを支払うかもしれない。コンピューティング企業はコンサルタントとして働くことができる。いくつかの企業は、革新的なマテリアル開発に結びつく量子に支えられたブレークスルーのために資本を交換するかもしれない。

THREE PRIORITIES

2. Quantum-assisted optimization

- 物理学や社会科学といった、量を対象とするすべての学問分野でも、産業の分野でも、計算で、一番中心的で難しい作業は、最適化である。この最適化問題は、従来のコンピュータでは解くのが難しい。従来のアルゴリズムでは、数学的に可能と思われる見通しがある解の中を、ゆっくりと移動することしかできないからである。乗り越えるのが難しく見える高い障壁の背後に、良い最適解が隠されているかもしれないのだ。
-

THREE PRIORITIES

2. Quantum-assisted optimization

- たとえば、**広告のオンライン・リコメンデーションと入札**の戦略では、消費者のニーズと市場の変化に最も効果的な方法で対応する最適化アルゴリズムが使用される。量子的と古典的の両方の解決法を組み合わせたより強力なプロトコルは、多くの業界で製品とサービスの品質を向上させることができる。**ロジスティクス企業は毎日スケジューリング、プランニング、製品配給を最適化**する必要がある。量子的に強化されたアルゴリズムは、**ヘルスケアでの患者の診断を改善**することができる。Google、マイクロソフト、Amazon、Facebookなどの大規模な情報技術企業の検索や製品のリコメンデーションの質を高めることができる。
-

THREE PRIORITIES

3. Quantum sampling

- 確率分布からのサンプリングは、統計や機械学習で広く使用されている。理論的には、理想的な量子回路は、古典的回路よりも大きな確率分布の集合から、同時にサンプリングすることができる。我々の計算では、信頼性の高い量子ゲートを含む比較的小さな回路の場合、約25の深さの層に 7×7 qubit程度の回路を使用して、古典的にはアクセスできない確率分布からサンプリングすることが可能であることが示されている。
 - 実際、そのような浅い量子回路を用いた、分布からのサンプリングが、「量子優位性」の最初の例を構成する可能性が高い。我々は、数年後に量子優位性を達成する実験が行われると予測している。
-

THREE PRIORITIES

3. Quantum sampling

- 量子サンプリングの有望な応用の中には、機械学習における推論およびパターン認識がある。学界と産業界の間での実験を容易にするために、私たちはクラウドコンピューティングインターフェースを通じて量子ハードウェアへのアクセスを提供する予定である。
-

TECHNICAL HURDLES

- 量子ハードウェアは、何十年も指数関数的に向上してきた従来のハードウェアと競合するために、スケールアップする必要がある。
 - Qubitは、量子もつれ合いをもたらす量子コヒーレンスを必要とする。それは、古典的回路のトランジスタにとって、利得を得ることが必要なのと同じである。
 - スケーリングとコヒーレンスを組み合わせることは、量子システム工学の大きな課題である。量子情報はコピーすることができず、また、サブシステムがもつれあうので、本質的にグローバルな設計上のトレードオフにつながり、基本的に困難である。
-

TECHNICAL HURDLES

- 我々は、超伝導qubitが量子コンピュータの最も有望なハードウェアプラットフォームの1つであると考えている。それらは、標準的な集積回路技術と超伝導技術に基づいて、構築および制御が比較的容易である。
 - また、デジタルとアナログの量子プロセッサのさまざまな要件に適合する可能性のある、多くのデザインがある。10qubit程度の高い信頼性を持つシステムが実証され、エンジニアリングの概念レベルでは実現可能性が示されている。
-

BUSINESS OPPORTUNITIES

- 新しい技術は、収益を増やすこと、コストを削減すること、インフラへの投資を減らすことの3つの方法でビジネスを改善することができる。
 - デジタル時代では、新しい技術を導入することは、指数関数的な影響がある。1%の製品品質でさえ、企業がユーザー数や収益面で圧倒的な成長を達成するのに役立つ。これは、密接な競争、透明性、効率的な市場を前提とした「スーパースター効果」である。
-

BUSINESS OPPORTUNITIES

- 例えば、デジタル量子コンピュータのための「キラーアプリ」としてメディアでよく描かれる暗号化の崩壊は、市場の適合性の点では高く評価されない。ある日、量子攻撃の影響を受けない暗号システムに取って代わられるだろう。また、ほとんどの民間企業は暗号化システムを破ることに無関心である。
 - 対照的に、**ポートフォリオの最適化とリスク管理**には即時のデータのフィードバックが必要であり、量子強化モデルの恩恵を受けることができる。より効率的な**量子化学計算は、医薬品、触媒コンバータ、太陽電池および肥料の開発に革命をもたらす。**
-

BUSINESS OPPORTUNITIES

- 量子を用いた最適化および推論技術は、新しい機械学習および人工知能システムに力を与えることができる。これらは、再生可能な発電機の管理、およびリモートセンシングおよび早期警戒システムの管理を改善する可能性がある。この技術は、オンライン貨物やサービス、倉庫の自動化や自家用車の動的価格設定にも役立つ。
-

WHAT NOW?

- 量子コンピューティングの分野は、すぐに歴史的なマイルストーン、すなわち量子優位性を達成するだろう。まもなく利用可能となるプロセッサを使用して、アプリケーション関連のアルゴリズムが大きな速度向上を実現できるかどうかはまだ分からない。しかし、量子ハードウェアが十分に強力になると、これをテストして新しいタイプのアルゴリズムを開発することが可能になる。
- 今後10年間で、学界、産業界、国立研究所は、量子シミュレーションと量子機械学習アルゴリズムの開発に協力しなければならない。私たちは、必要な資本、専門知識、インフラストラクチャーが不足している他の人たちに、クラウドサービスを通じてGoogleの量子プロセッサへのアクセスを提供することで、そのような研究を支援する予定である。

Characterizing Quantum Supremacy in Near-Term Devices

Sergio Boixo, Sergei V. Isakov, Vadim N. Smelyanskiy, Ryan Babbush, Nan Ding, Zhang Jiang, Michael J. Bremner, John M. Martinis and Hartmut Neven

<https://arxiv.org/pdf/1608.00263.pdf>

2017年 4月5日

Random Quantum Circuit

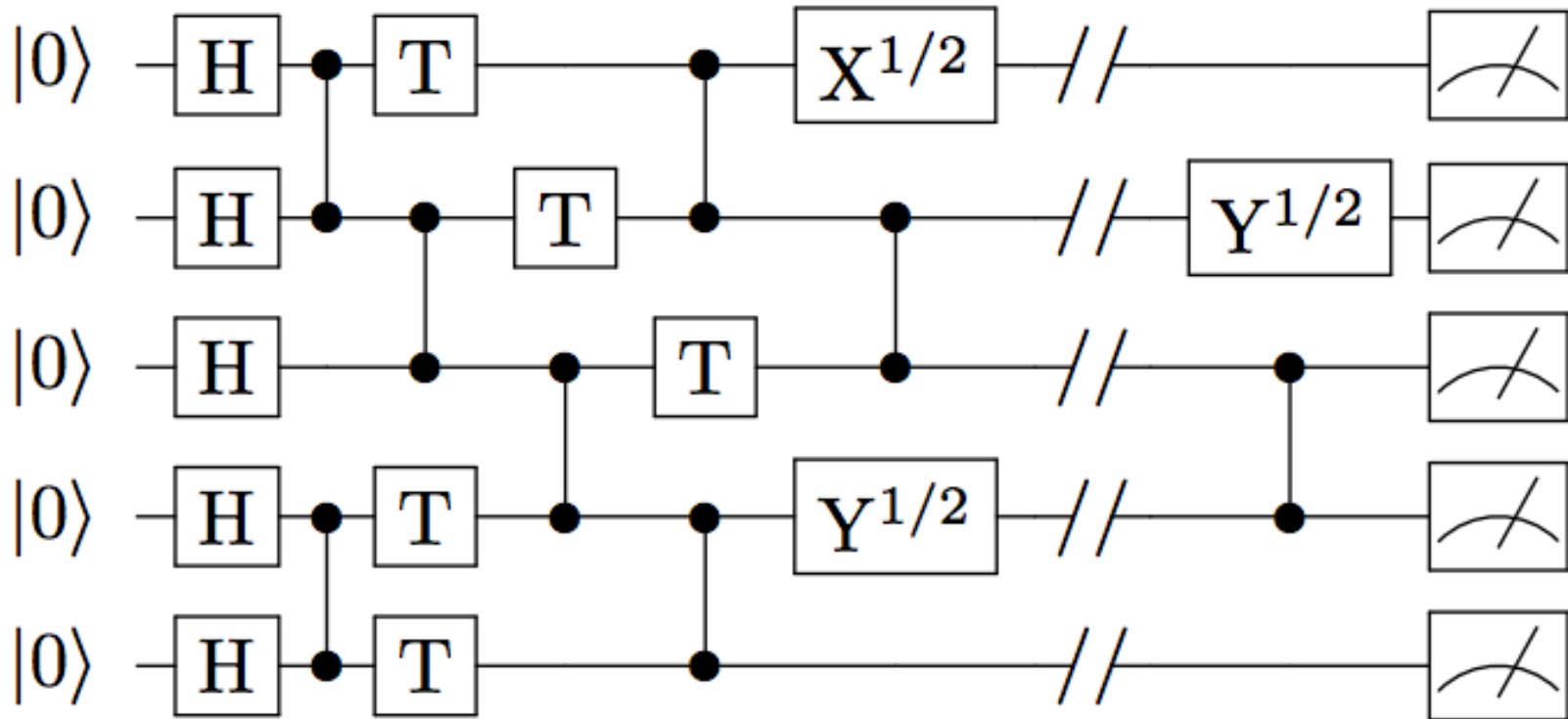


FIG. 1. Example of a random quantum circuit in a 1D array of qubits. Vertical lines correspond to controlled-phase (CZ) gates (see Sec. IV).

I. INTRODUCTION

- Despite a century of research, there is no known method for efficiently simulating arbitrary quantum dynamics using classical computation. In practice, we are unable to directly simulate even modest depth quantum circuits acting on approximately fifty qubits. This strongly suggests that the controlled evolution of ideal quantum systems offers computational resources more powerful than classical computers [1, 2]. In this paper we build on existing results in quantum chaos [3–19] and computational complexity theory [20–30] to propose an experiment for characterizing “quantum supremacy” [31] in the presence of errors.

-
- We study the computational task of sampling from the output distribution of random quantum circuits composed from a universal gate set, a natural task for benchmarking quantum computers. We propose the cross entropy difference as a measure of correspondence between experimentally obtained samples and the output distribution of the ideal circuit. Finally, we discuss a robust set of conditions which should be met in order to be sufficiently confident that an experimental demonstration has actually achieved quantum supremacy.
-

-
- ❑ Quantum supremacy is achieved when a formal computational task is performed with an existing quantum device which cannot be performed using any known algorithm running on an existing classical super computer in a reasonable amount of time.
 - ❑ 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 numerically the convergence of the output distribution to the Porter-Thomas distribution, characteristic of quantum chaos.

-
- We find a good convergence for the first ten moments and the entropy at depth 25 with circuits of up to 7×6 qubits in a 2D lattice. Using chaos theory, the properties of the Porter-Thomas distribution, and numerical simulations, we argue that the cross entropy is closely related to the circuit fidelity. State-of-the-art supercomputers cannot simulate universal random circuits of sufficient depth in a 2D lattice of approximately 7×7 qubits with any known algorithm and significant fidelity.
-

Robots & Machines

Google Just Revealed How They'll Build Quantum Computers

<https://goo.gl/kqG4Z4>

UCSB

$\langle \text{Google} \rangle$

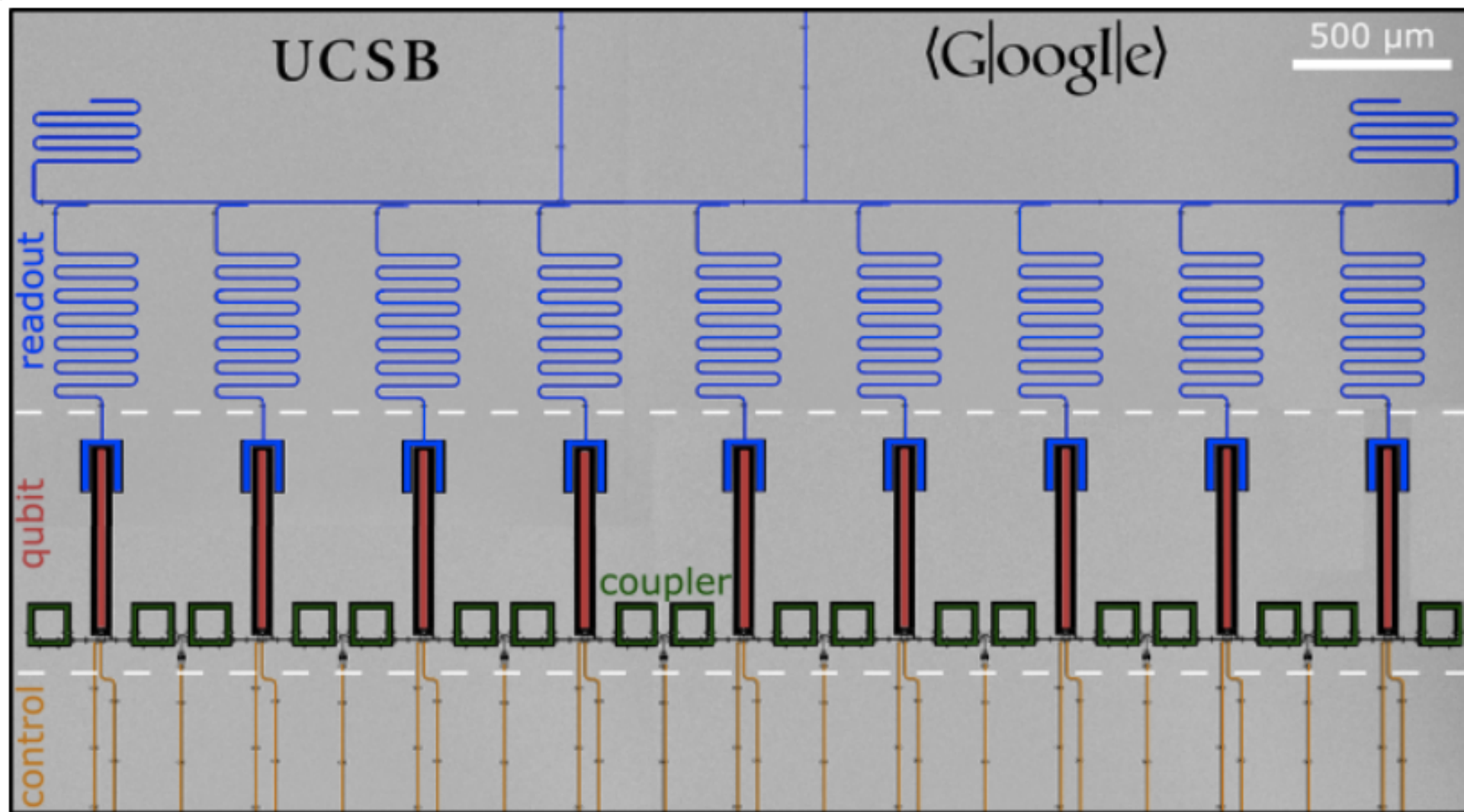
500 μm

readout

qubit

control

coupler



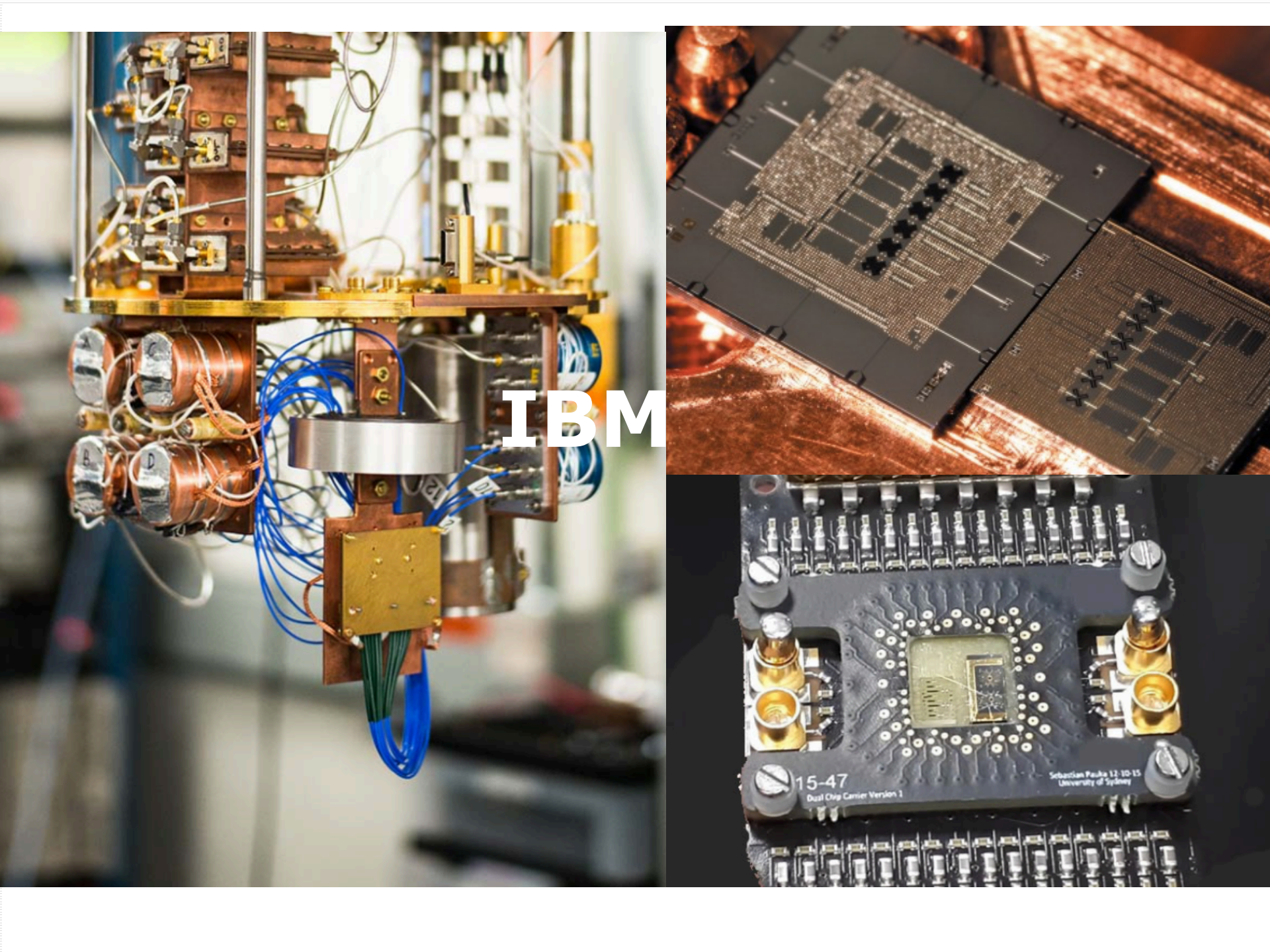
-
- Their system is a series of nine superconducting qubits, consisting of nine metal loops cooled to a low temperature with current flowing through them in both directions simultaneously. They were able to show that the supported qubits represented 512 numbers at once, and that the results were reliable, without an accompanying exponential increase in errors.
 - If the team is right, they may achieve quantum supremacy in a [matter of months](#). If they do, the applications will be staggering. We can expect to see machine learning take place [exponentially faster](#), and artificial intelligence progress much more rapidly. If it does, [we may see the singularity](#) approaching long before most predicted

A blueprint for demonstrating quantum supremacy with superconducting qubits

<https://arxiv.org/abs/1709.06678>

-
- Fundamental questions in chemistry and physics may never be answered due to the exponential complexity of the underlying quantum phenomena. A desire to overcome this challenge has sparked a new industry of quantum technologies with the promise that engineered quantum systems can address these hard problems. A key step towards demonstrating such a system will be performing a computation beyond the capabilities of any classical computer, achieving so-called quantum supremacy. Here, using 9 superconducting qubits, we demonstrate an immediate path towards quantum supremacy.
-

- By individually tuning the qubit parameters, we are able to generate thousands of unique Hamiltonian evolutions and probe the output probabilities. The measured probabilities obey a universal distribution, consistent with uniformly sampling the full Hilbert-space. As the number of qubits in the algorithm is varied, the system continues to explore the exponentially growing number of states. Combining these large datasets with techniques from machine learning allows us to construct a model which accurately predicts the measured probabilities. We demonstrate an application of these algorithms by systematically increasing the disorder and observing a transition from delocalized states to localized states. 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.



IBM

November 10, 2017

Posted in: [Quantum Computing](#)

The future is quantum

Some of the most important technical advances of the 20th century were enabled by decades of fundamental scientific exploration, whose initial purpose was simply to extend human understanding. When Einstein discovered relativity, he had no idea that one day it would be an important part of modern navigation systems. Such is the story of quantum science.

We have come a long way since the earliest days of quantum information theory, when IBM Fellow [Charlie Bennett](#) and the other quantum information science pioneers created the foundations that have given rise to a thriving scientific community. Today, this same community has made enough progress that the earliest real systems, which are able to implement theoretical predictions, are being built before our eyes.



Dario Gil

Vice President of AI and IBM Q

Share

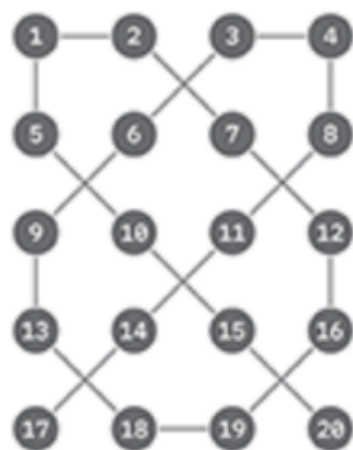


<https://www.ibm.com/blogs/research/2017/11/the-future-is-quantum/>

IBM 50Q System: An IBM
cryostat wired for a 50 qubit
system







October 17, 2017

Posted in: Quantum Computing

Quantum Computing: Breaking Through the 49 Qubit Simulation Barrier

Quantum computing is at the threshold of tackling important problems that cannot be efficiently or practically computed by other, more classical means. Getting past this threshold will require us to build, test and operate reliable quantum computers with 50 or more qubits.

Achieving this potential will require major leaps forward in both science and engineering. To help make those leaps, methods are needed to test quantum devices and to compare observed behaviors with desired behaviors so that the design, manufacturing, and operation of these devices can be improved over time. In particular, to test whether the



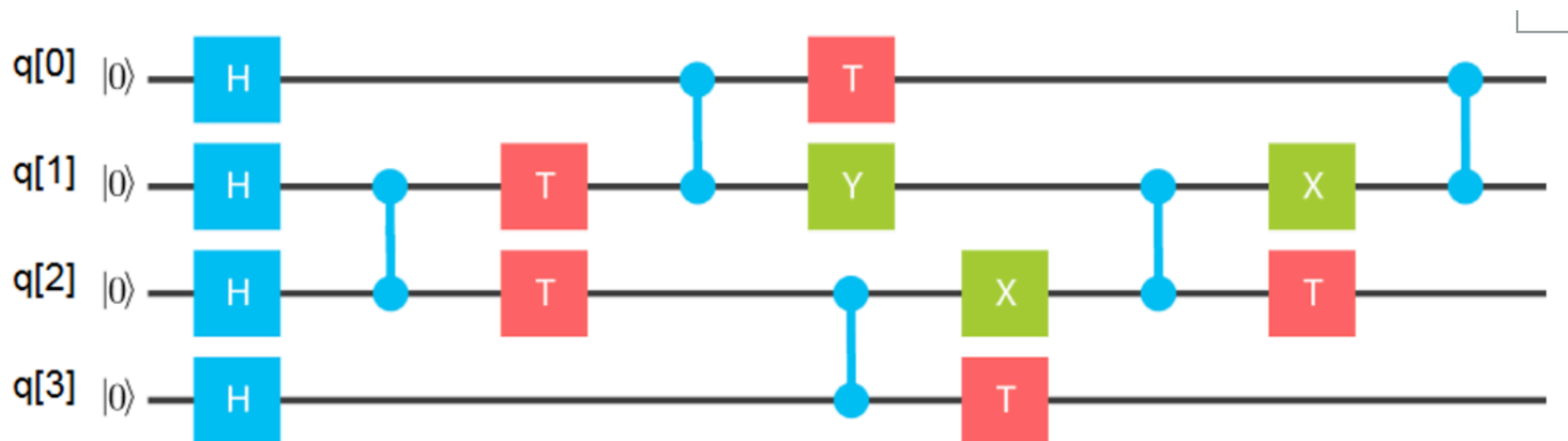
Edwin Pednault

Distinguished Research Staff Member,
IBM Research

Share



<https://www.ibm.com/blogs/research/2017/10/quantum-computing-barrier/>



(a) A 4x1 universal random quantum circuit



(b) The "bristle-brush" pattern formed by the gates applied to qubit $q[1]$

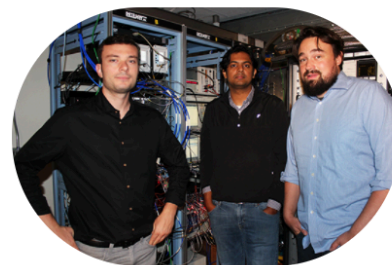
September 13, 2017

Posted in: Chemistry, Publications, Quantum Computing

How to measure a molecule's energy using a quantum computer

Editor's note: This article is by Abhinav Kandala, Antonio Mezzacapo, and Kristan Temme, IBM Research

Simulating molecules on quantum computers just got much easier with IBM's superconducting quantum hardware. In a recent research article published in *Nature*, [Hardware-efficient Variational Quantum Eigensolver for Small Molecules and Quantum Magnets](#), we implement a new quantum algorithm capable of efficiently computing the lowest energy state of small molecules. By mapping the electronic structure of molecular orbitals onto a subset of our purpose-built seven qubit quantum processor, we studied



L-R: Antonio Mezzacapo, Abhinav Kandala, Kristan Temme

Share



Related articles

<https://www.ibm.com/blogs/research/2017/09/quantum-molecule/>

March 13, 2017

Posted in: IBM Research-Africa, Quantum Computing

Quantum Algorithm Classifies 9,500 Handwritten Numbers

While still in their infancy, as quantum computers edge closer to surpassing classical computers, a new discipline is emerging called quantum machine learning. Its goal is to apply quantum information processing to pattern recognition tasks such as classification, regression and clustering. By using quantum bits (qubits) instead of normal binary bits scientists expect to achieve results on highly complex data sets, such as those found in Nature, in seconds, instead of years, rapidly accelerating the discovery of new drugs and medicines.

The underlying question whether quantum computation can help to efficiently solve hard machine learning problems has only recently gained significant interest by the machine



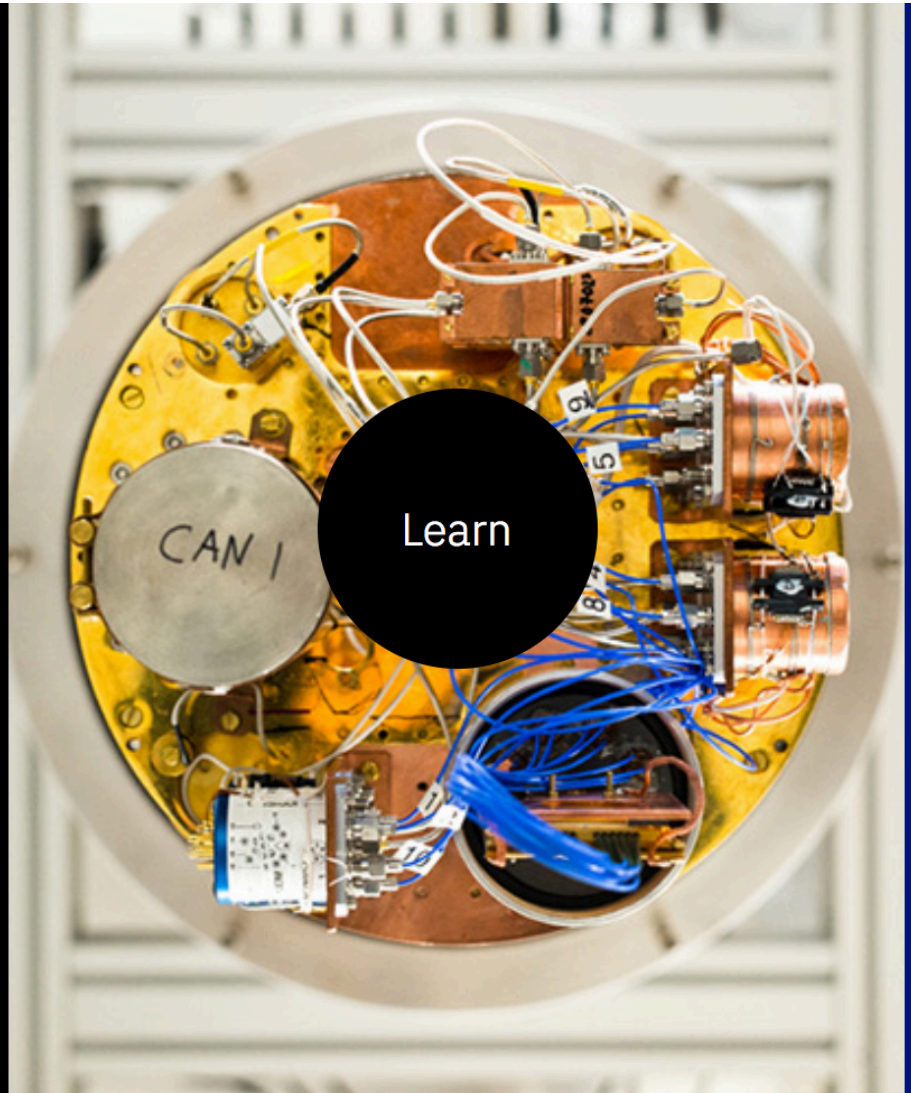
Waheeda Saib

"The [BBC] documentary also introduced me to advances in quantum computing and its potential to crack problems that are considered unsolvable, which could have significant impact in the medical, business and security domain."

<https://goo.gl/queFK8>

IBM-Q

Quantum
Computing



<https://www.research.ibm.com/ibm-q/>

Meet IBM-Q

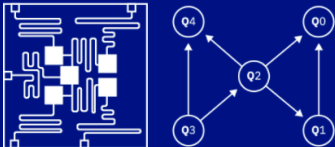
- IBM Q is an industry-first initiative to build commercially available universal quantum computers for business and science. While technologies like AI can find patterns buried in vast amounts of existing data, quantum computers will deliver solutions to important problems where patterns cannot be found and the number of possibilities that you need to explore to get to the answer are too enormous ever to be processed by classical computers. We invite you join us in exploring what might be possible with this new and vastly different approach to computing.
-

What is quantum computing?

- ❑ Quantum computers are incredibly powerful machines that take a new approach to processing information. Built on the principles of quantum mechanics, they exploit complex and fascinating laws of nature that are always there, but usually remain hidden from view. By harnessing such natural behavior, quantum computing can run new types of algorithms to process information more holistically. They may one day lead to revolutionary breakthroughs in materials and drug discovery, the optimization of complex manmade systems, and artificial intelligence. We expect them to open doors that we once thought would remain locked indefinitely. Acquaint yourself with the strange and exciting world of quantum computing.

▼ Backend: ibmqx4 (5 Qubits)

MAINTENANCE



Gate Error (10^{-3})
Readout Error (10^{-2})

Q0	Q1	Q2	Q3	Q4
0.60	0.52	1.29	1.63	8.34
6.40	4.80	3.00	6.60	14.40

MultiQubit Gate
Error (10^{-2})

CX1_0	CX2_0	CX3_2
1.74	1.89	2.14
CX2_1	CX3_4	
2.60	7.95	
CX2_4		
9.38		

Date Calibration: 2017-11-08 21:21:19 Fridge Temperature: 0.021 K

More details

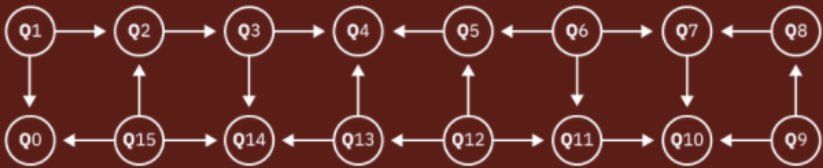
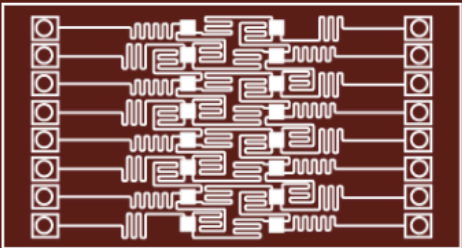
> Backend: ibmqx5 (16 Qubits)

BETA ACTIVE

> Backend: ibmqx2 (5 Qubits)

MAINTENANCE

▼ Backend: ibmqx5 (16 Qubits)



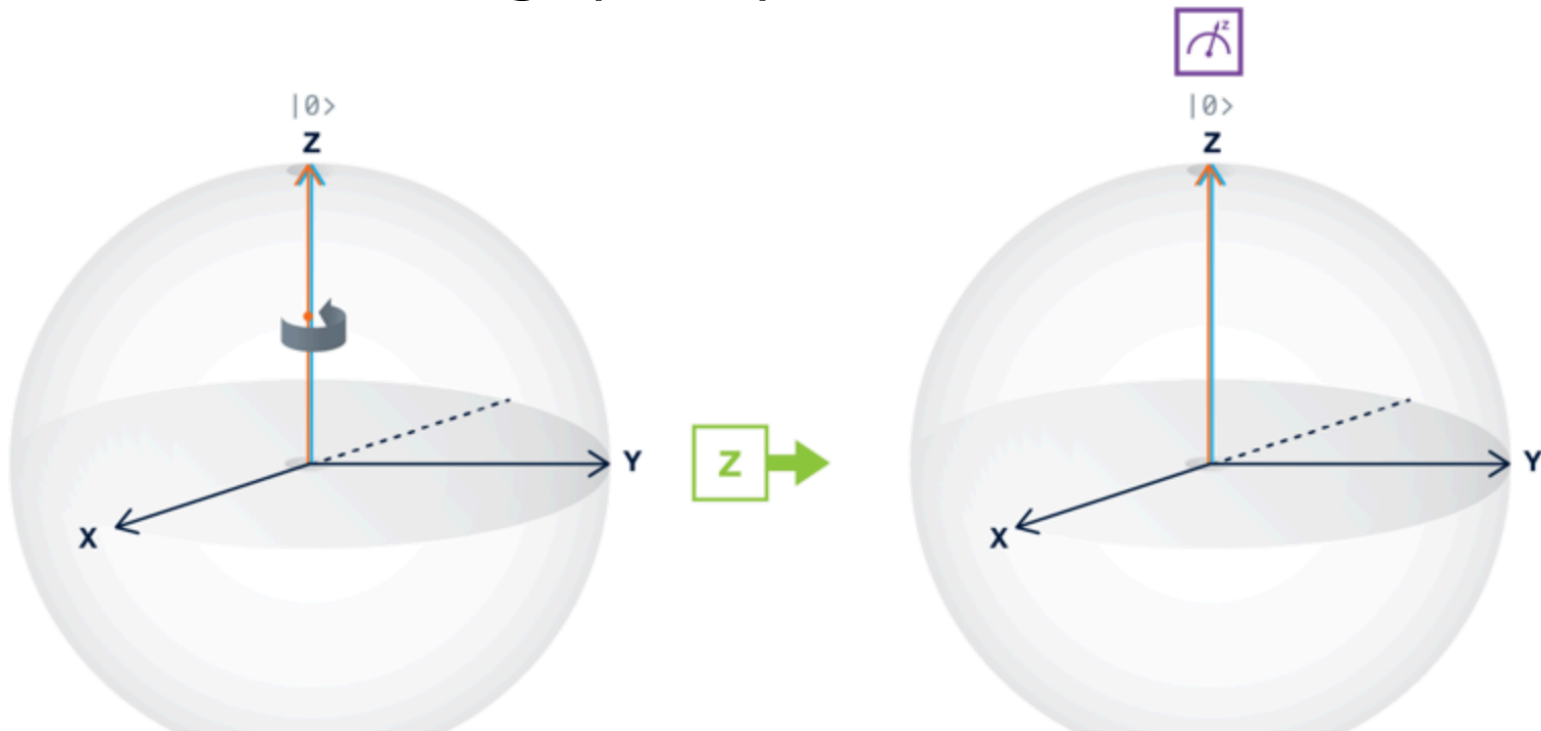
Date Calibration: 2017-11-26 12:35:09 Fridge Temperature: 0.0134909 K

New experiment

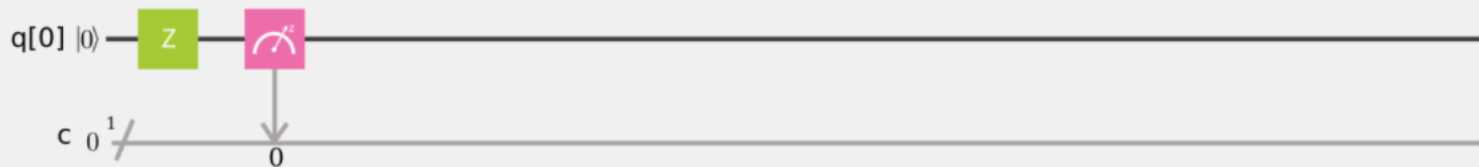
Save

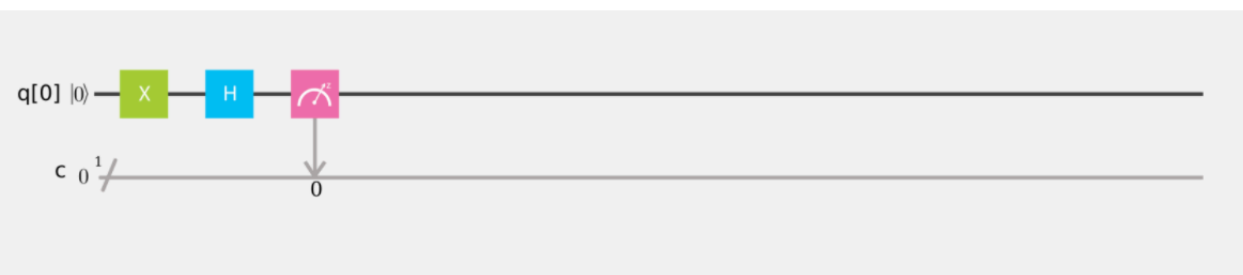
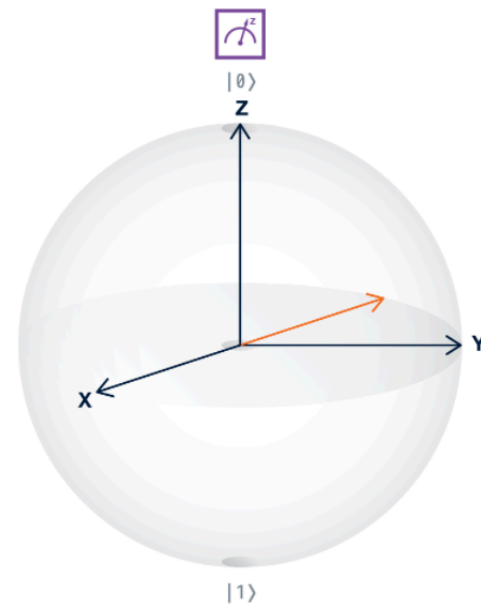
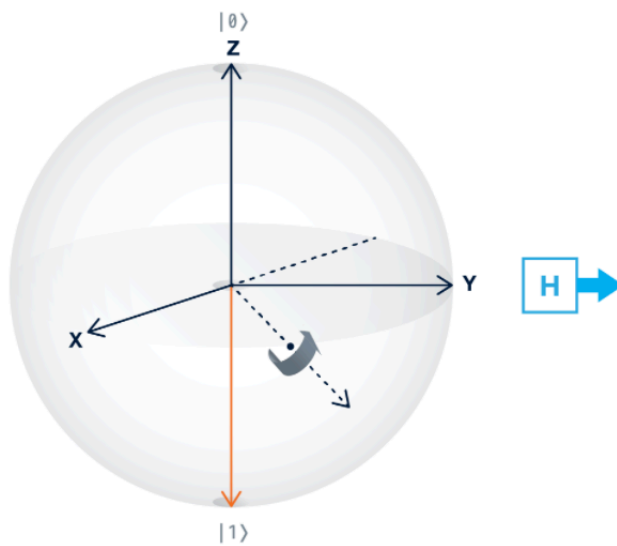
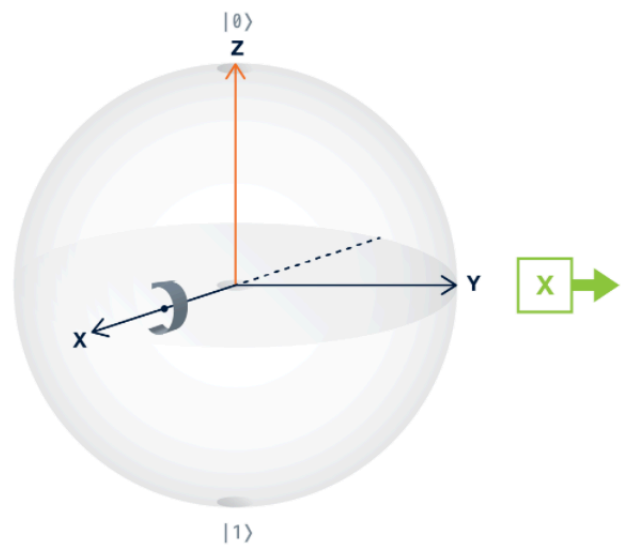
Save

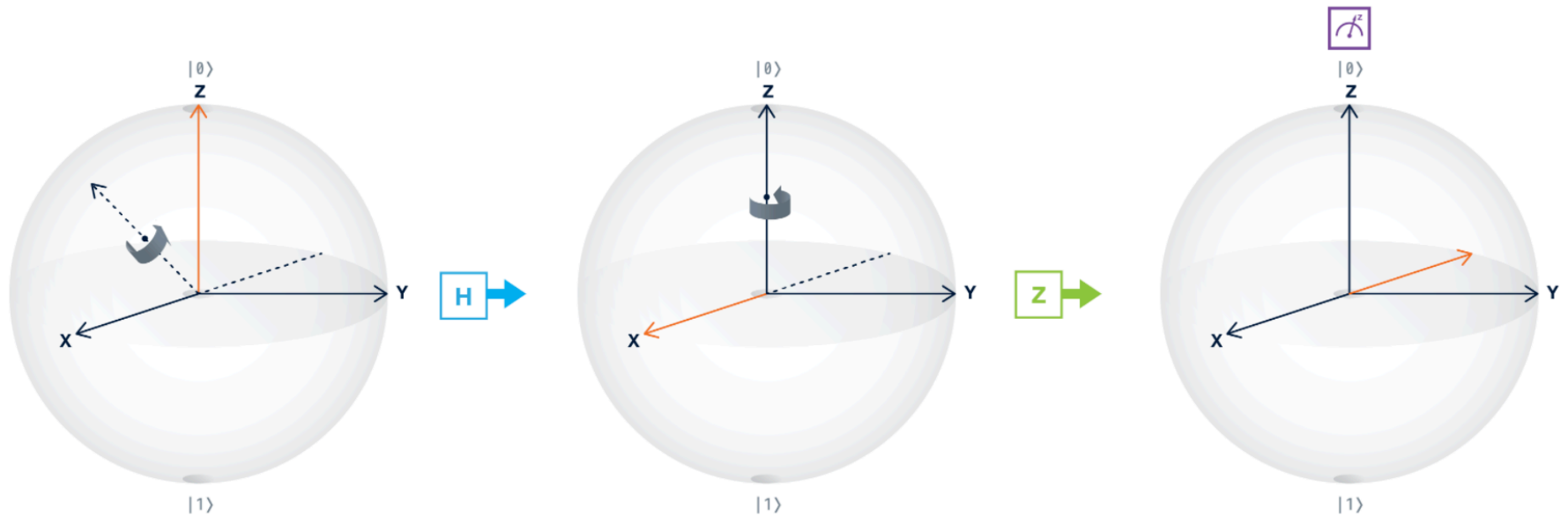
Introducing qubit phase



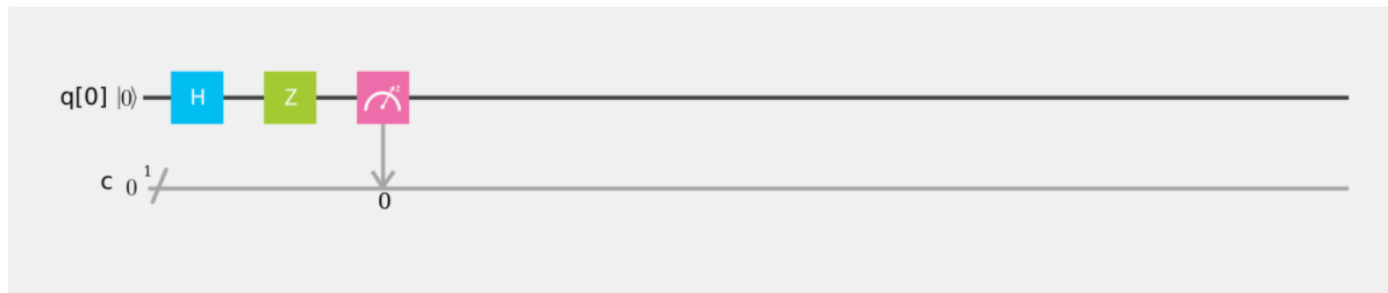
Z gate: when qubit is in the $|0\rangle$ state







Z gate: when the qubit is in the $|+\rangle$ state



Gate sequence					Rotation around Z	Probability of 0	Probability of 1
H			H		0	1.0	0
H	T		H		$\pi/4$	0.85	0.15
H	S		H		$\pi/2$	0.50	0.50
H	S	T	H		$3\pi/4$	0.15	0.85
H	Z		H		π	0	1



Create +X state



Change qubit phase



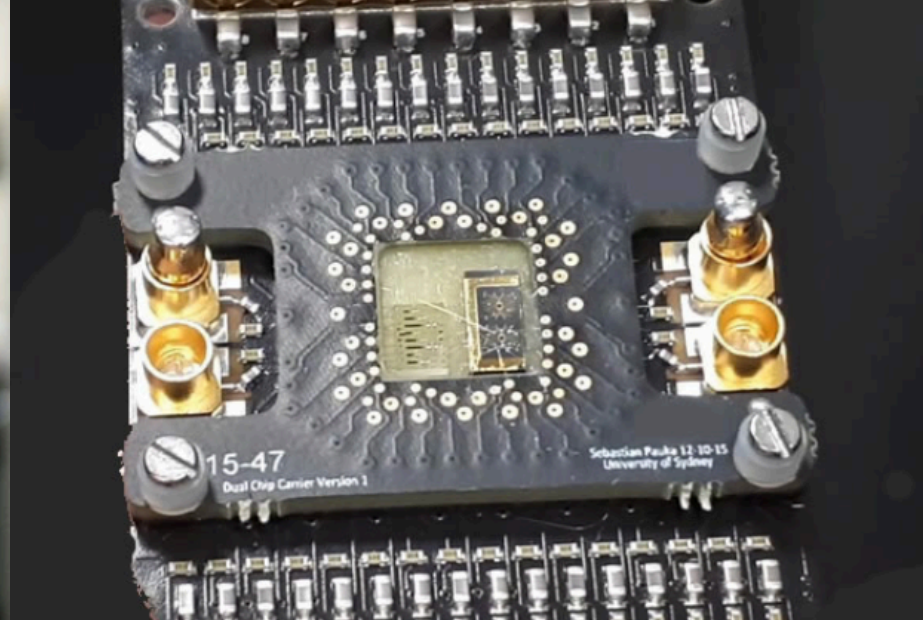
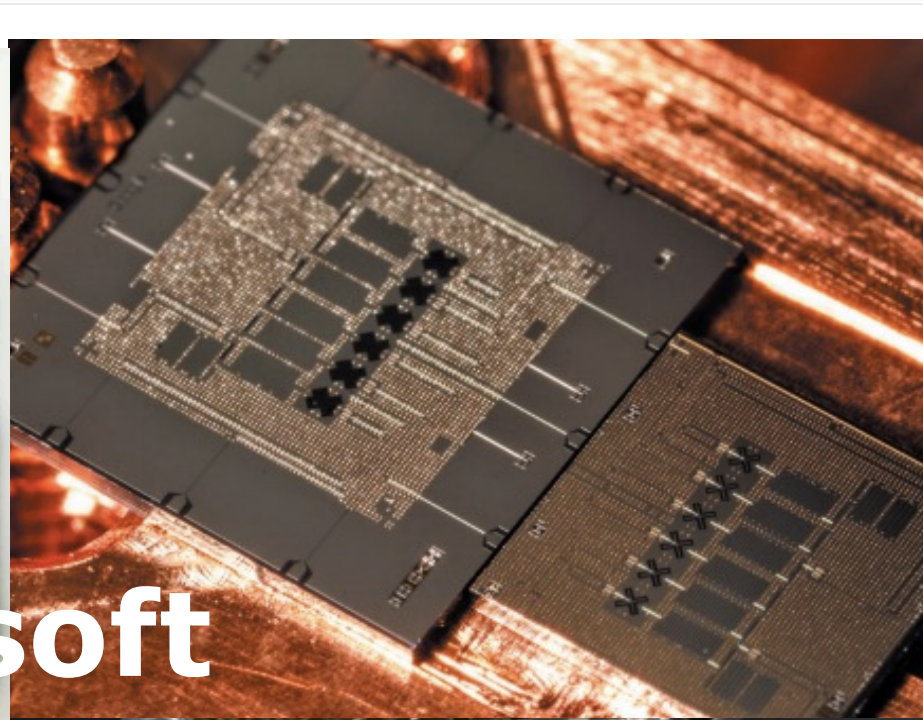
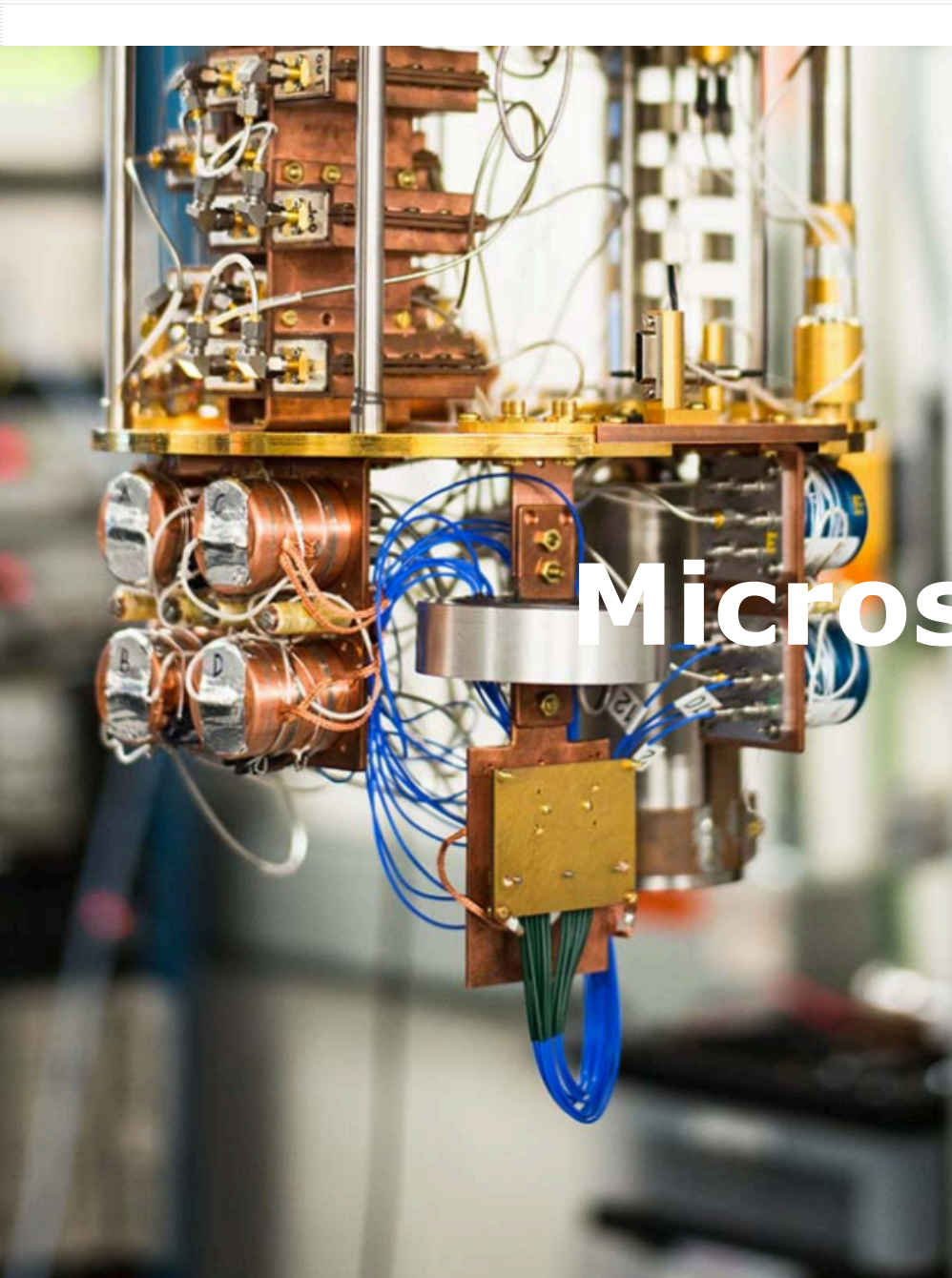
Measure in superposition basis

Summary of quantum gates

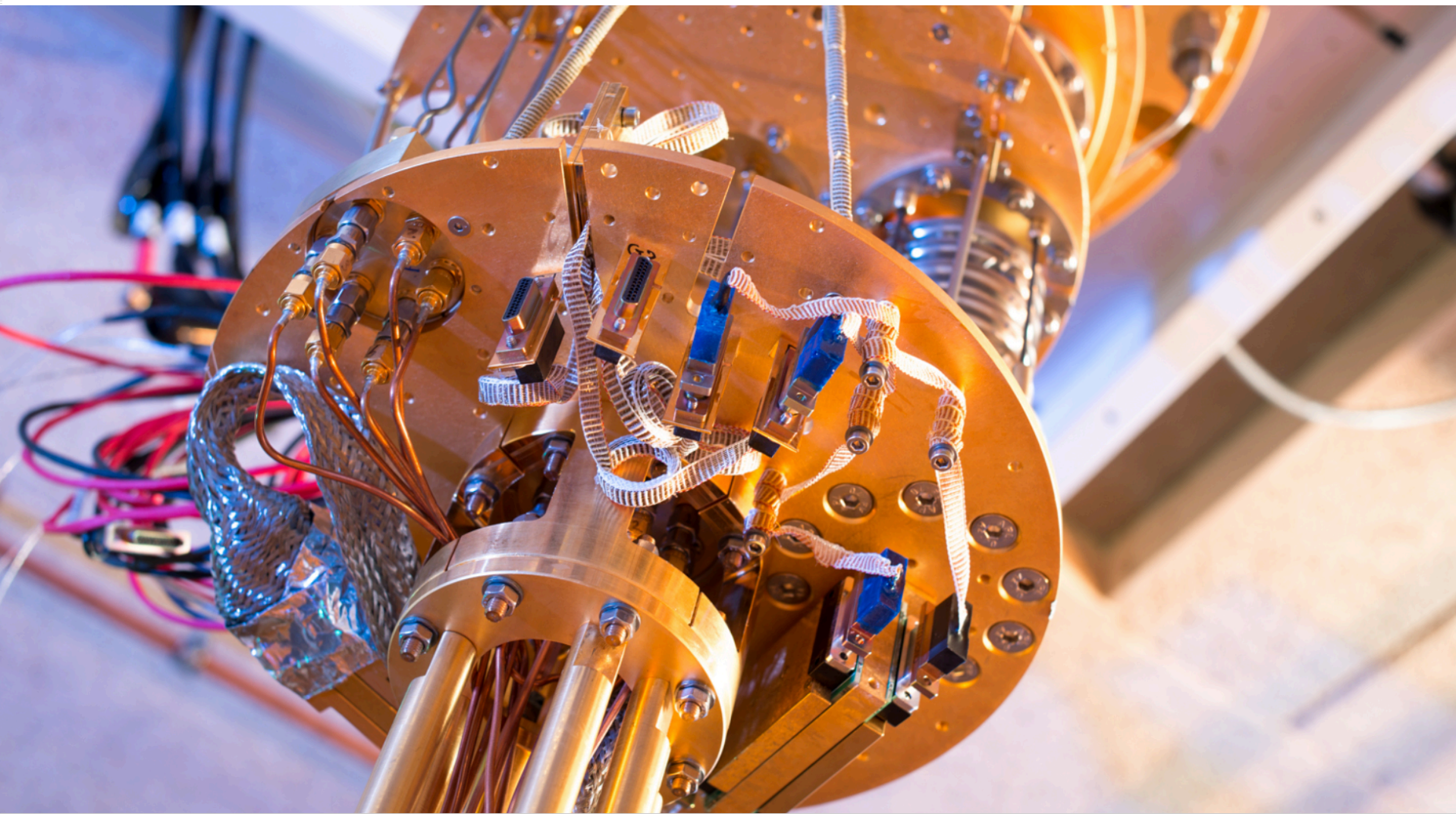
Table of Quantum Gates and what they do				
State	Gate sequence to prepare the state	Transformation on Bloch sphere	Gates to measure in the respective basis	Name of measurement basis
$ 0\rangle$	(none, ground state)	None		Z, "standard"
$ 1\rangle$		π rotation around X		Z, "standard"
$ +\rangle$		π rotation around X + Z	 	X
$ -\rangle$	 	π rotation around X + π rotation around X + Z	 	X

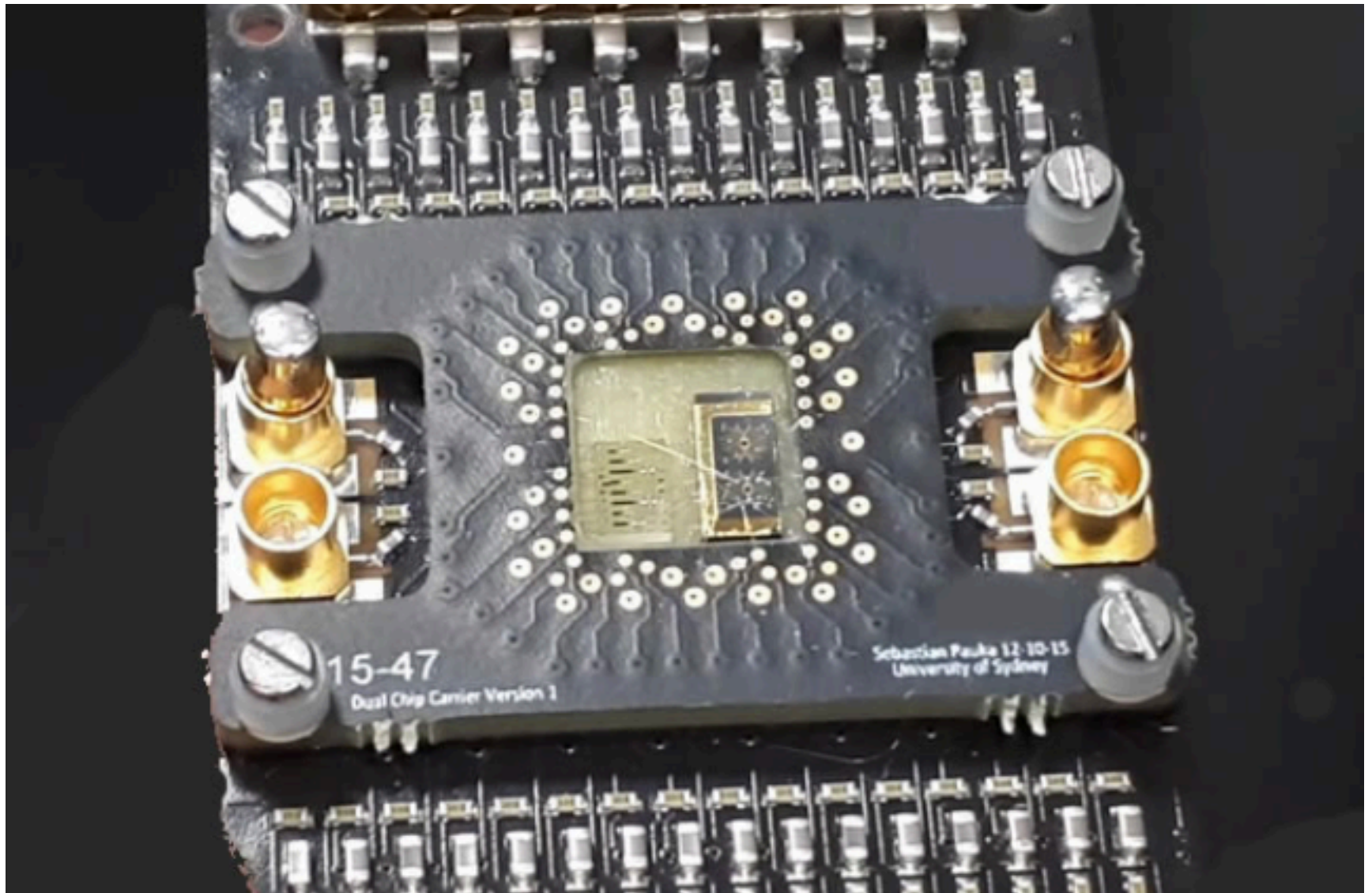
Summary of quantum gates

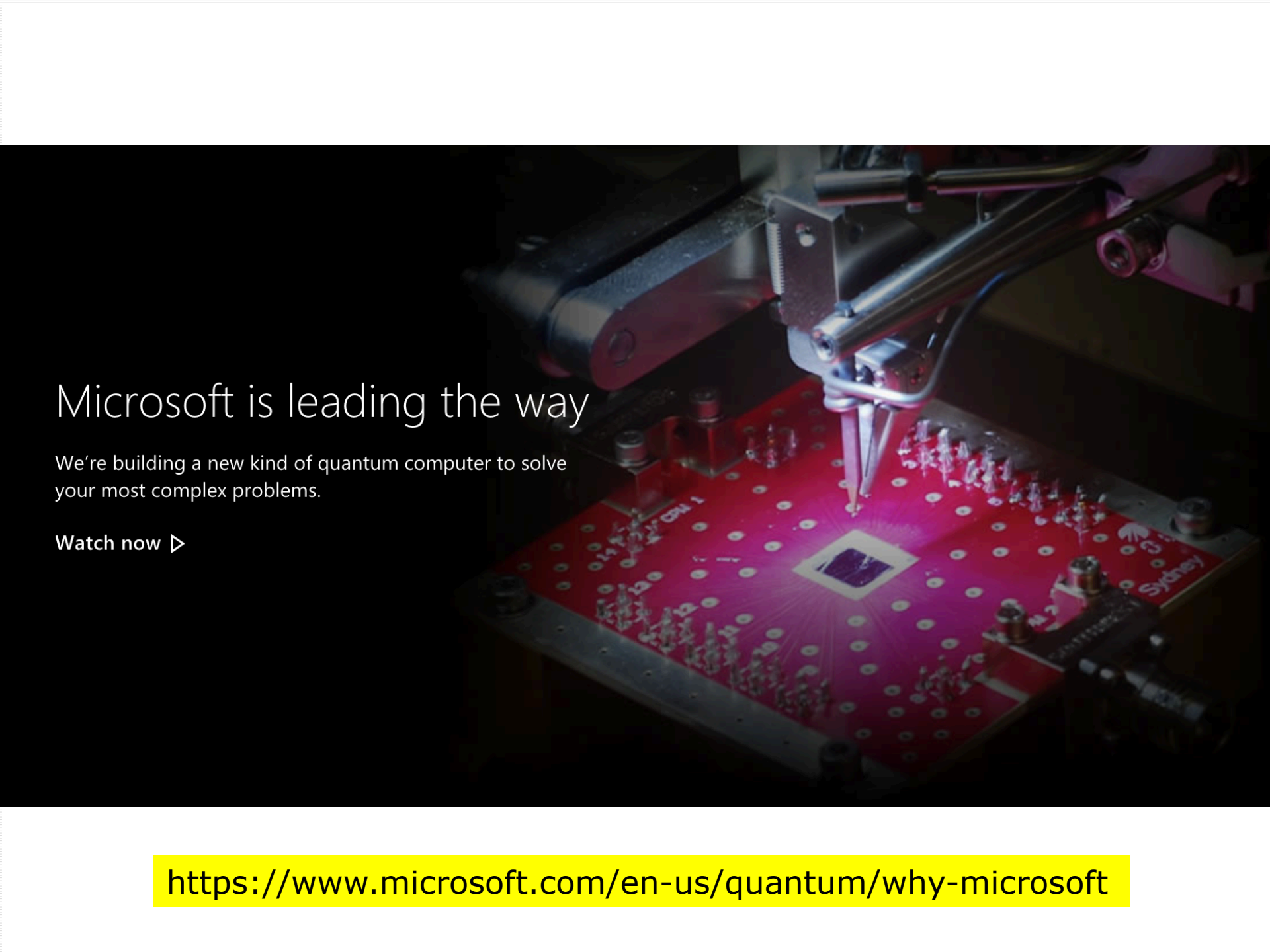
Gate	Transformation on Bloch sphere (defined for single qubit)
X	π -rotation around the X axis, $Z \rightarrow -Z$. Also referred to as a bit-flip.
Z	π -rotation around the Z axis, $X \rightarrow -X$. Also referred to as a phase-flip.
H	maps $X \rightarrow Z$, and $Z \rightarrow X$. This gate is required to make superpositions.
S	maps $X \rightarrow Y$. This gate extends H to make complex superpositions. ($\pi/2$ rotation around Z axis).
$S^\dagger$	inverse of S. maps $X \rightarrow -Y$. ($-\pi/2$ rotation around Z axis).
T	$\pi/4$ rotation around Z axis.
$T^\dagger$	$-\pi/4$ rotation around Z axis.



Microsoft







Microsoft is leading the way

We're building a new kind of quantum computer to solve your most complex problems.

Watch now ►

<https://www.microsoft.com/en-us/quantum/why-microsoft>

We've taken a revolutionary topological approach

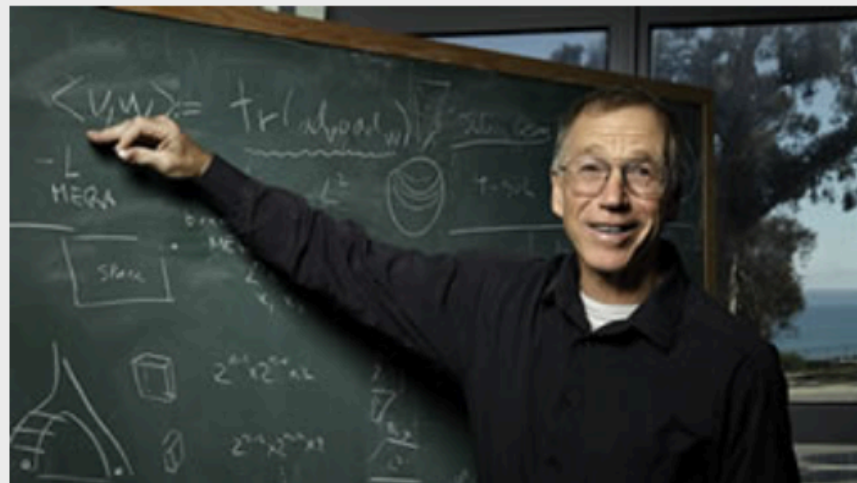
- Microsoft has pushed the limits of what's possible with topological quantum computing, and we're seeing significant benefits so far. Topological qubits can perform computations longer and more consistently, with significantly lower error rates compared to other quantum methods. Our approach also makes key advancements in cryogenics and quantum hardware that give us the unique ability to scale.
-

Michael Freedman



Krysta Svore, Ph.D.

Krysta, a Kavli Fellow of the National Academy of Science, designed one of the earliest software stacks for quantum computing and developed the first thresholds for local quantum error correction.



Michael Freedman, Ph.D.

Michael is a Fields medalist who pioneered topological quantum computation. He founded Station Q, the Microsoft-led global research consortium that got us where we are today.

Inside Microsoft's quest for a topological quantum computer

"Alex Bocharov explains why the company is hoping to build qubits out of particles that some scientists think might not even exist."

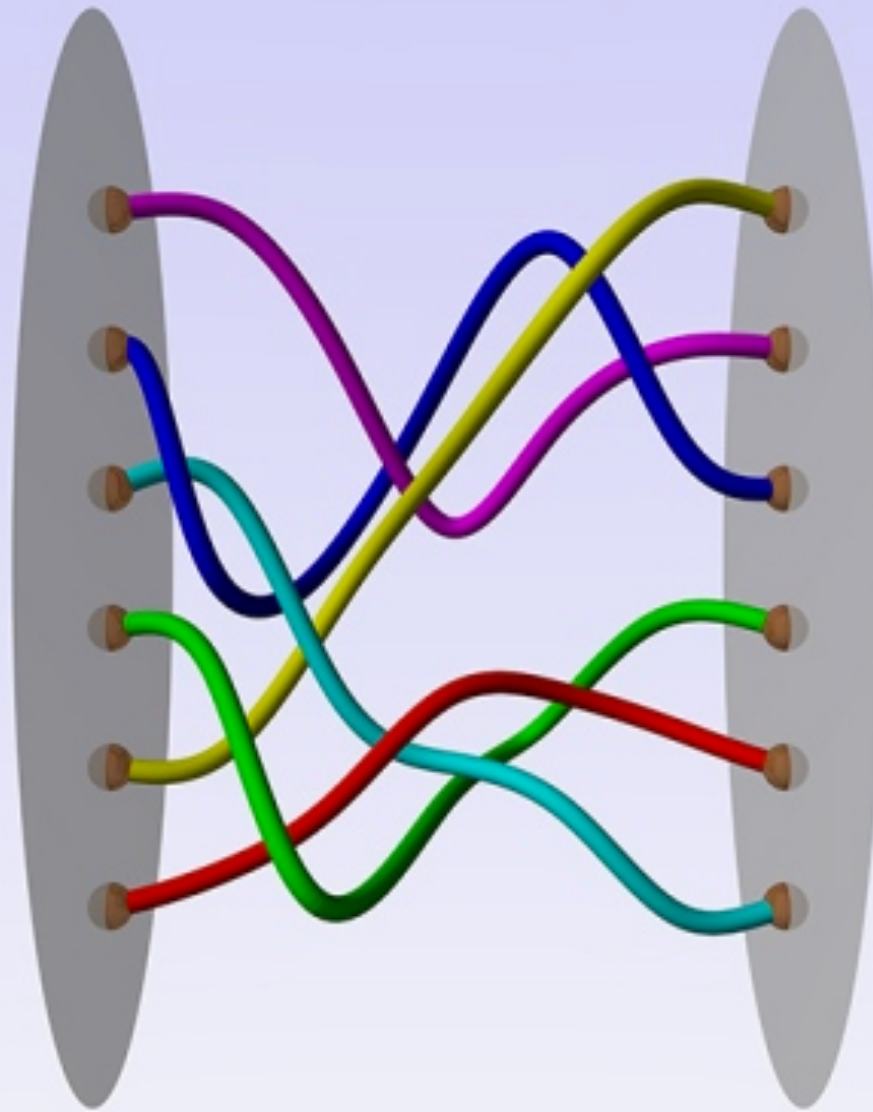
Elizabeth Gibney

Nature 21 October 2016

<https://goo.gl/f7NRXh>

- ❑ The race is on build a ['universal' quantum computer](#). Such a device could be programmed to speedily solve problems that classical computers cannot crack, potentially revolutionizing fields from pharmaceuticals to cryptography. Many of the world's major technology firms are taking on the challenge, but Microsoft has opted for a more tortuous route than its rivals.
 - ❑ IBM, Google and a number of academic labs have chosen relatively [mature hardware](#), such as loops of superconducting wire, to make quantum bits (qubits). These are the building blocks of a quantum computer: they power its speedy calculations thanks to their ability to be in a mixture (or superposition) of 'on' and 'off' states at the same time.
-

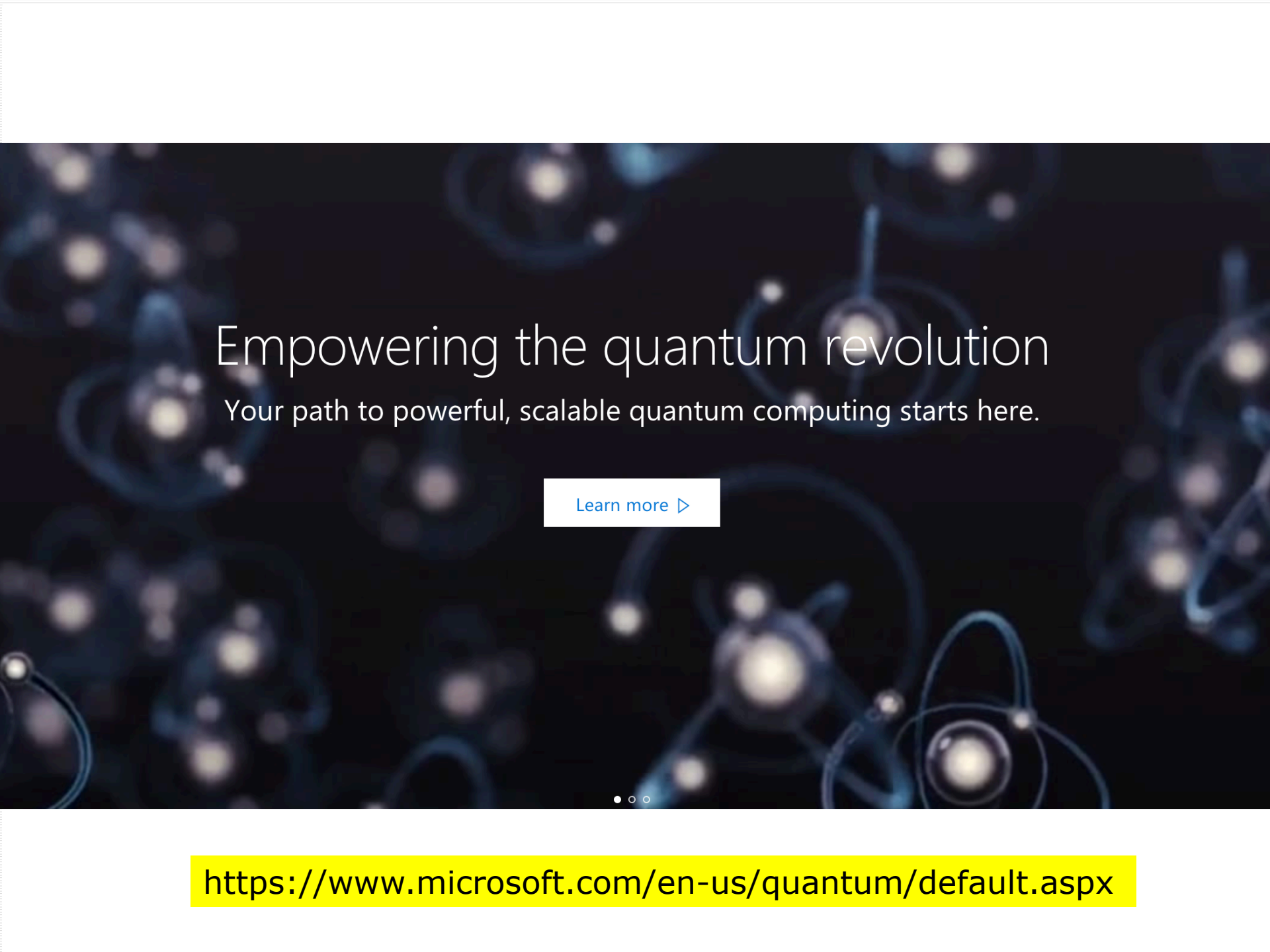
-
- Microsoft, however, is hoping to encode its qubits in a kind of quasiparticle: a particle-like object that emerges from the interactions inside matter. Some physicists are not even sure that the particular quasiparticles Microsoft are working with — called [non-abelian anyons](#) — actually exist. But the firm hopes to exploit their topological properties, which make quantum states extremely robust to outside interference, to build what are called [topological quantum computers](#). Early theoretical work on topological states of matter won [three physicists the Nobel Prize in Physics on 4 October](#).
-



The mathematical theory of braids could serve as the foundation for future topological quantum computers.

Both IBM and Google use superconducting loops as their qubits. What are the qubits you are trying to harness?

- Our qubits are not even material things. But then again, the elementary particles that physicists run in their colliders are not really solid material objects. Here we have non-abelian anyons, which are even fuzzier than normal particles. They are quasiparticles. The most studied kinds of anyon emerge from chains of very cold electrons that are confined at the edge of a 2D surface. These anyons act like both an electron and its antimatter counterpart at the same time, and appear as dense peaks of conductance at each end of the chain. You can measure them with high-precision devices, but not see them under any microscope.
-

The background of the slide is a dark blue field filled with numerous stylized atomic models. Each atom consists of a bright yellow or white central nucleus and several concentric, glowing blue elliptical orbits. The atoms are scattered across the frame, creating a sense of depth and complexity.

Empowering the quantum revolution

Your path to powerful, scalable quantum computing starts here.

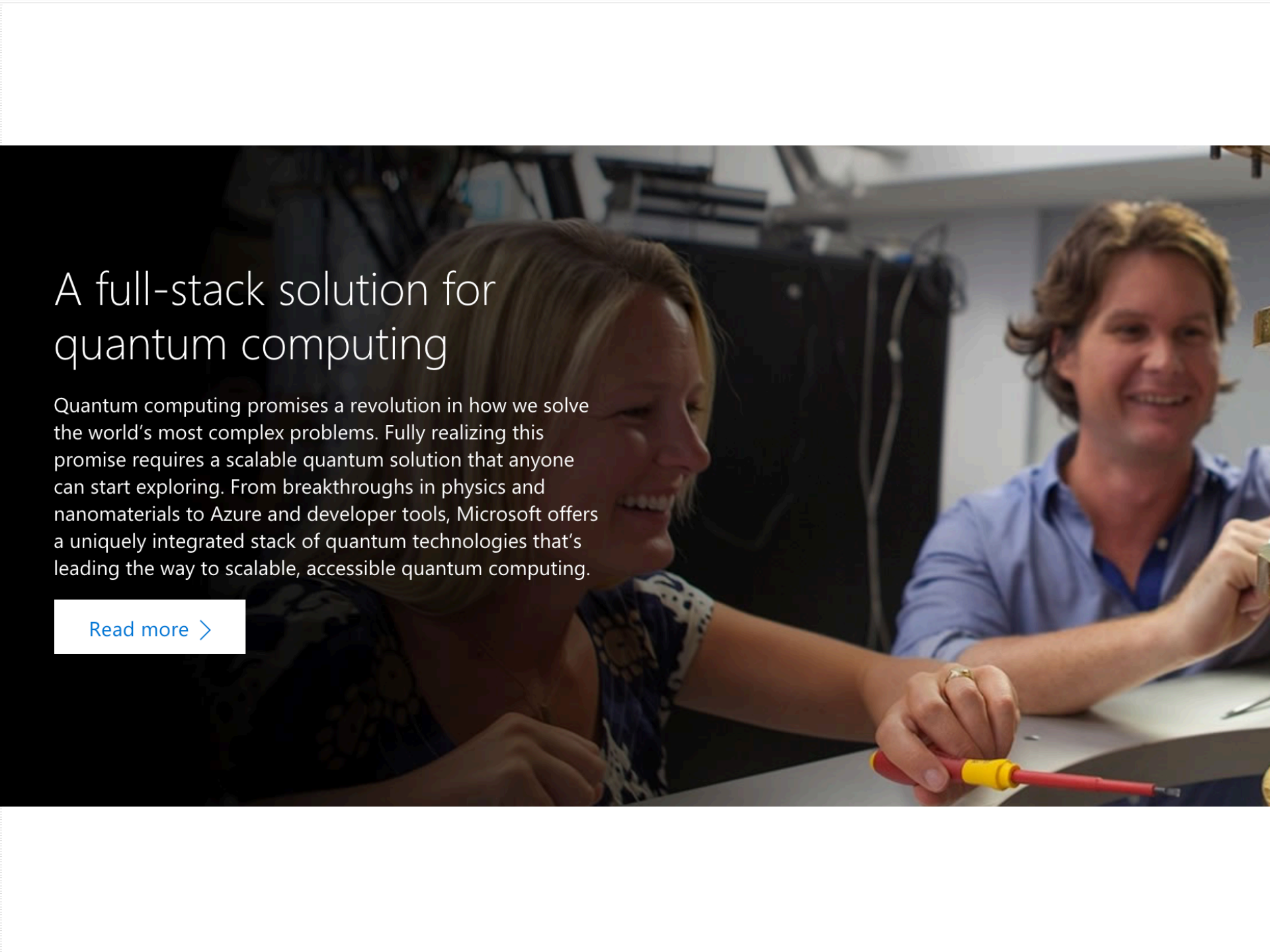
[Learn more ▶](#)



<https://www.microsoft.com/en-us/quantum/default.aspx>

Join us at the leading edge of opportunity

- ❑ Quantum computing takes a giant leap forward from today's technology—one that will forever alter our economic, industrial, academic, and societal landscape. In just hours or days, a quantum computer can solve complex problems that would otherwise take billions of years for classical computing to solve. This has massive implications for research in healthcare, energy, environmental systems, smart materials, and more. The quantum economy is coming. And Microsoft envisions a future where customers use Azure for both classical and quantum computing.
-

A woman with blonde hair and a man with brown hair are working in a laboratory. The woman is in the foreground, smiling and looking down at a piece of equipment. The man is in the background, also smiling and looking at the same equipment. They are both wearing blue shirts. The background is filled with various pieces of laboratory equipment, including cables and a large black box.

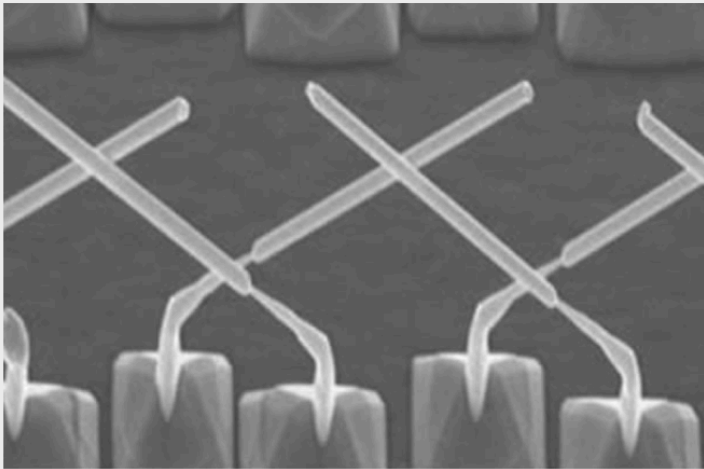
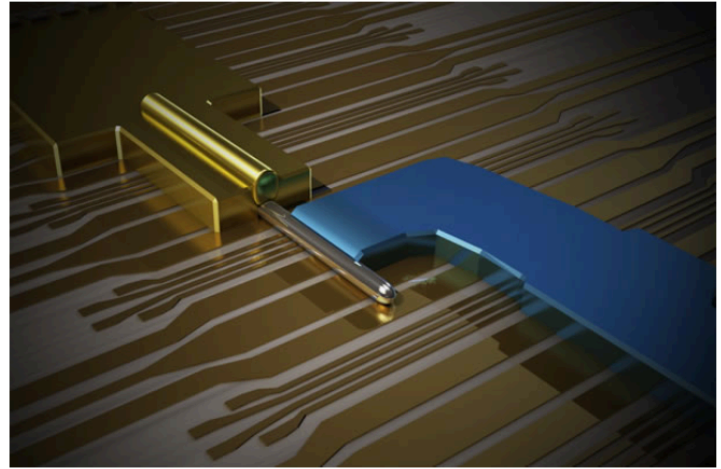
A full-stack solution for quantum computing

Quantum computing promises a revolution in how we solve the world's most complex problems. Fully realizing this promise requires a scalable quantum solution that anyone can start exploring. From breakthroughs in physics and nanomaterials to Azure and developer tools, Microsoft offers a uniquely integrated stack of quantum technologies that's leading the way to scalable, accessible quantum computing.

[Read more >](#)

Physics

Microsoft has sponsored and participated in fundamental quantum physics research for more than a decade with the goal of empowering a quantum-computing revolution. Breakthroughs in theory have led to breakthroughs in experimental physics and the reality of a path forward for scalable quantum computing. Our approach focuses on topological quantum computing through Majorana fermions, which promise to yield fast, stable quantum bits, also known as qubits.

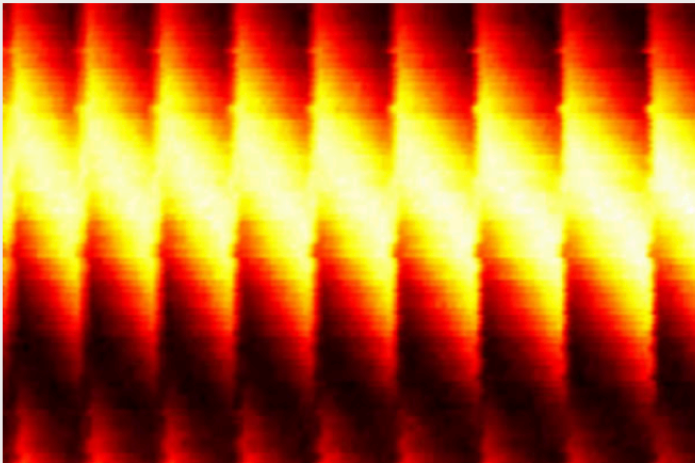
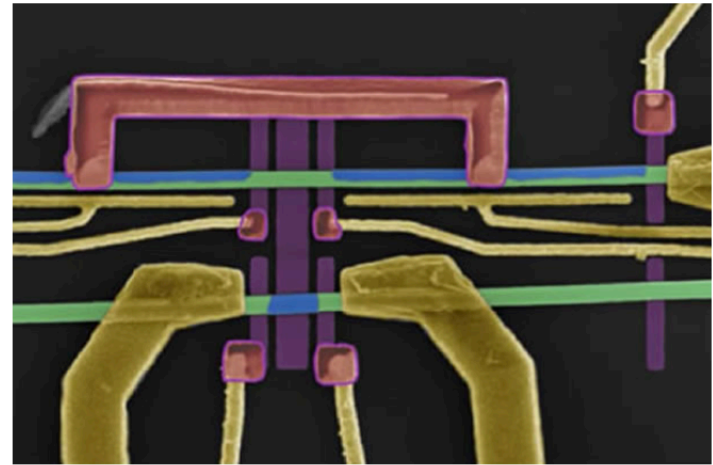


Materials

To achieve our goal, we started by creating the raw materials necessary to make topological quantum devices. We grew specialized nanowires that can be used to make qubits. We also created atomically thin conducting layers with exotic topological properties using integrated-circuit manufacturing techniques to realize a fully scalable quantum computer.

Devices

Taking the materials and turning them into working devices is no small task. Microsoft runs several labs around the world that specialize in the fabrication of quantum devices. The infrastructure we've built allows for the efficient mounting, wiring, and cooling of these devices, which in turn supports rapid prototyping, characterization, and exploration. These devices operate at temperatures almost 200 times colder than the farthest reaches of outer space.



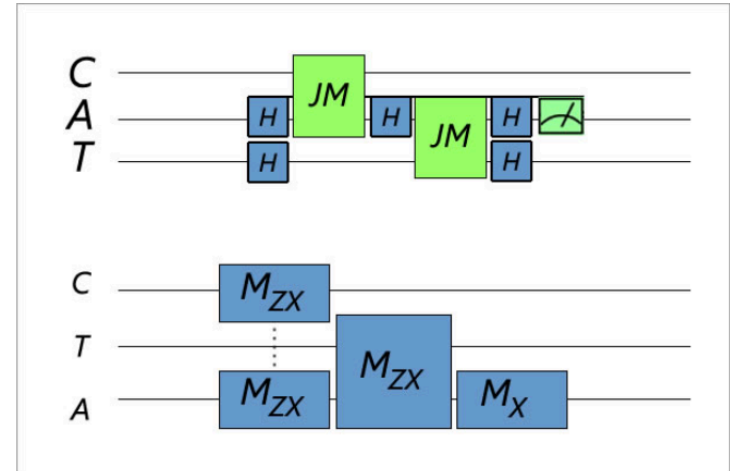
Control

Sending and receiving signals to nanoscale devices is also a daunting task. A scalable quantum computer requires many fast and reliable signals. We've designed classical integrated-circuits that run at cryogenic temperatures where standard chips will not operate. We even changed the wiring to handle signals that are in the super-conducting regime. The entire infrastructure is integrated to allow for scalability, including the cooling system itself.



Runtime

To solve problems on a quantum computer, you need a runtime that executes a quantum algorithm while maintaining the state of the machine, operating the control system in a parallel real-time environment, and communicating from the device to the outside world. The runtime layer is the firmware and operating system of the quantum computer.



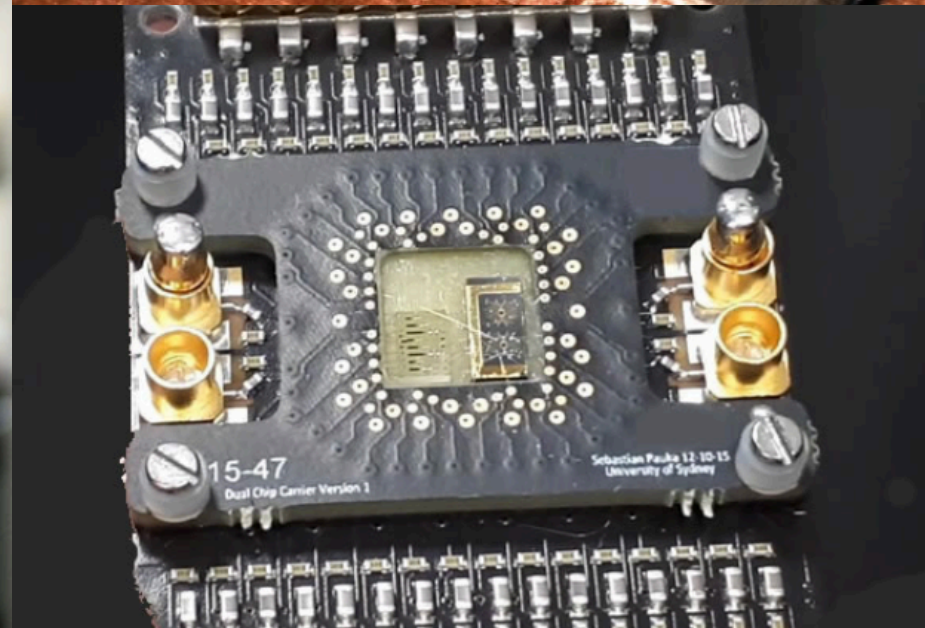
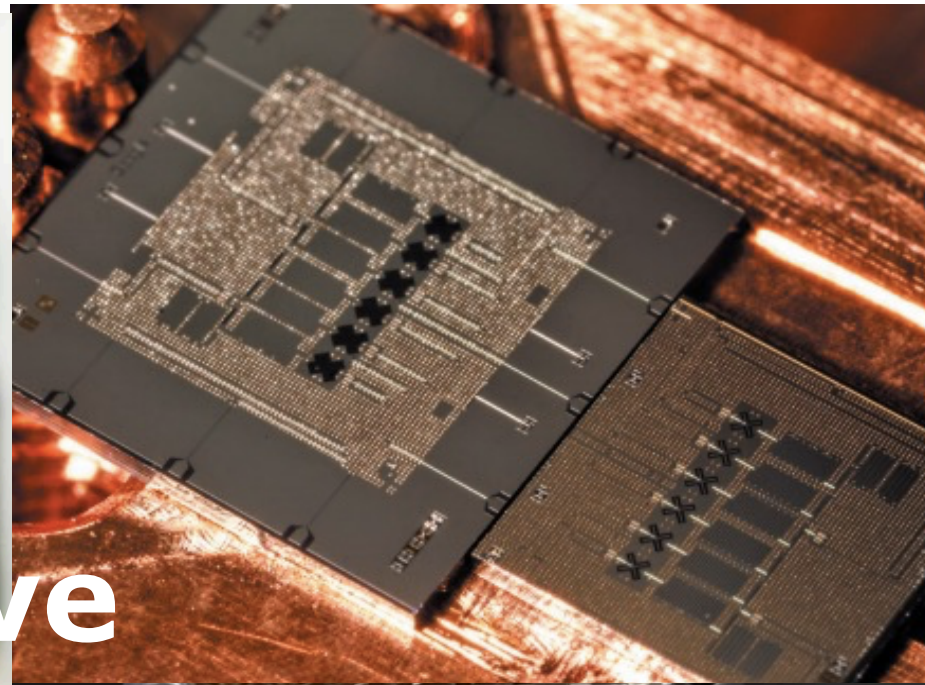
```
1 operation () EPR (Qubit q1, Qubit q2) {
2   Body {
3     H (q1)
4     CNOT (q1,q2)
5   }
6 }
7
8 operation () Teleport (Qubit msg, Qubit here, Qubit there) {
9   Body {
10    EPR (here, there)
11    CNOT (msg, here)
12    H (msg)
13
14    let m_here = M (here)
15    if (m_here == One) {
16      X (there)
17    }
18
19    let m_msg = M (msg)
20    if (m_msg == One) {
21      Z (there)
22    }
23  }
```

Applications

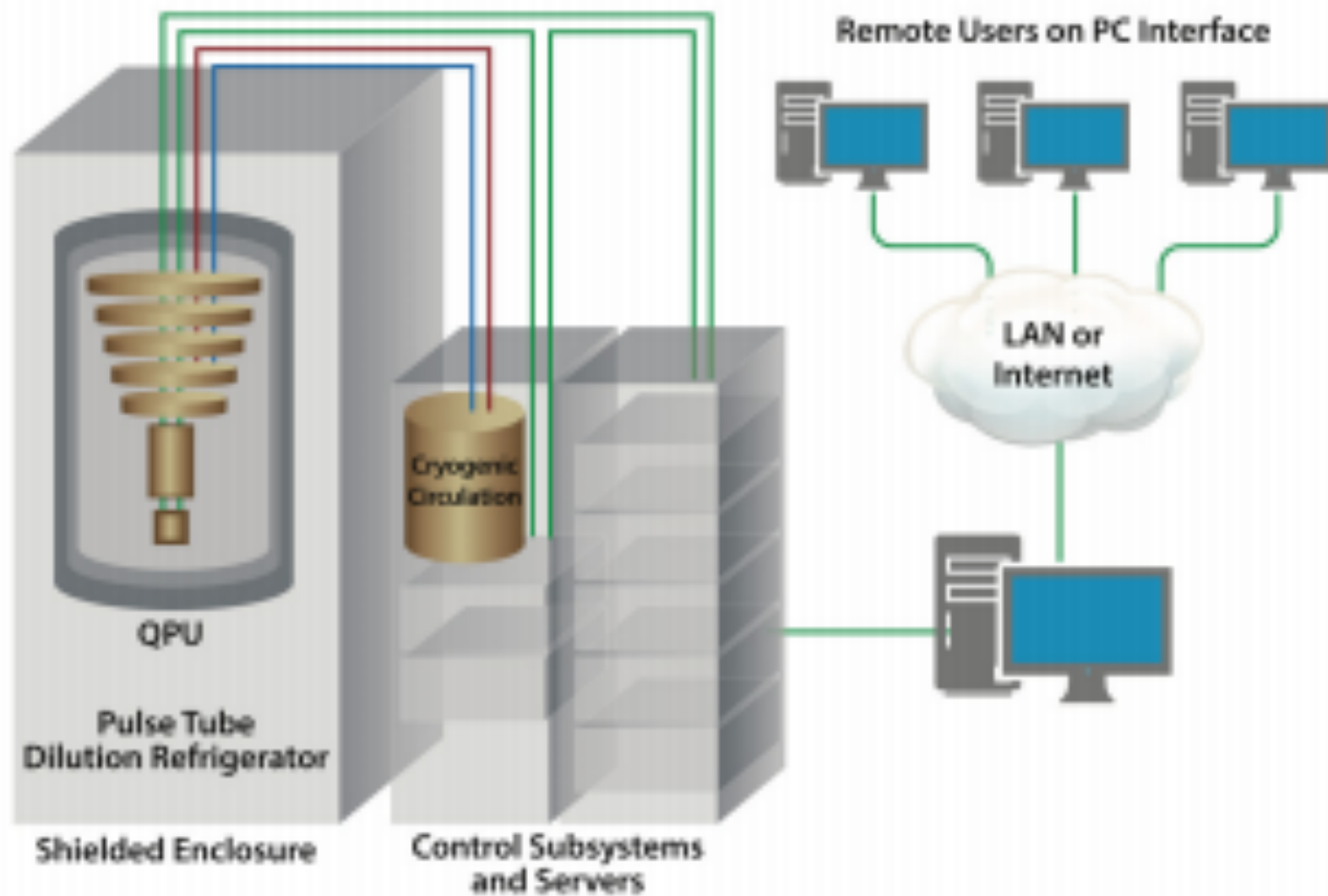
To deploy a quantum application, we've designed an environment to compile and implement quantum algorithms. Microsoft has been working on these software requirements for as long as we've been working on the hardware itself. The quantum computer will be integrated with Azure, giving the computer the necessary support of large amounts of classical computation that go hand in hand with quantum computation.



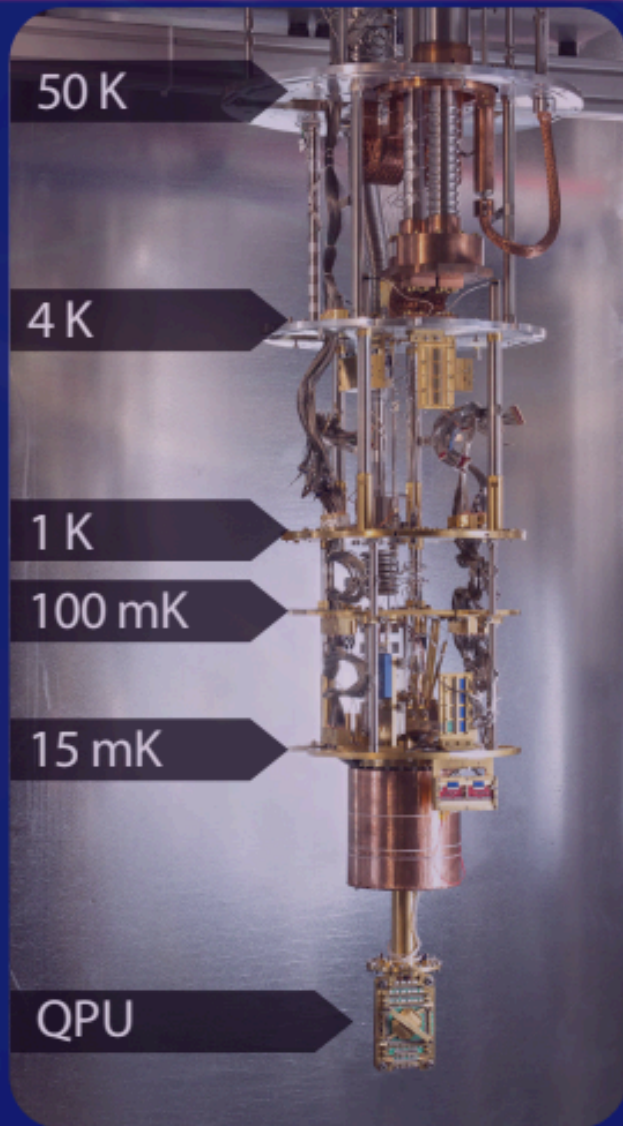
D-Wave



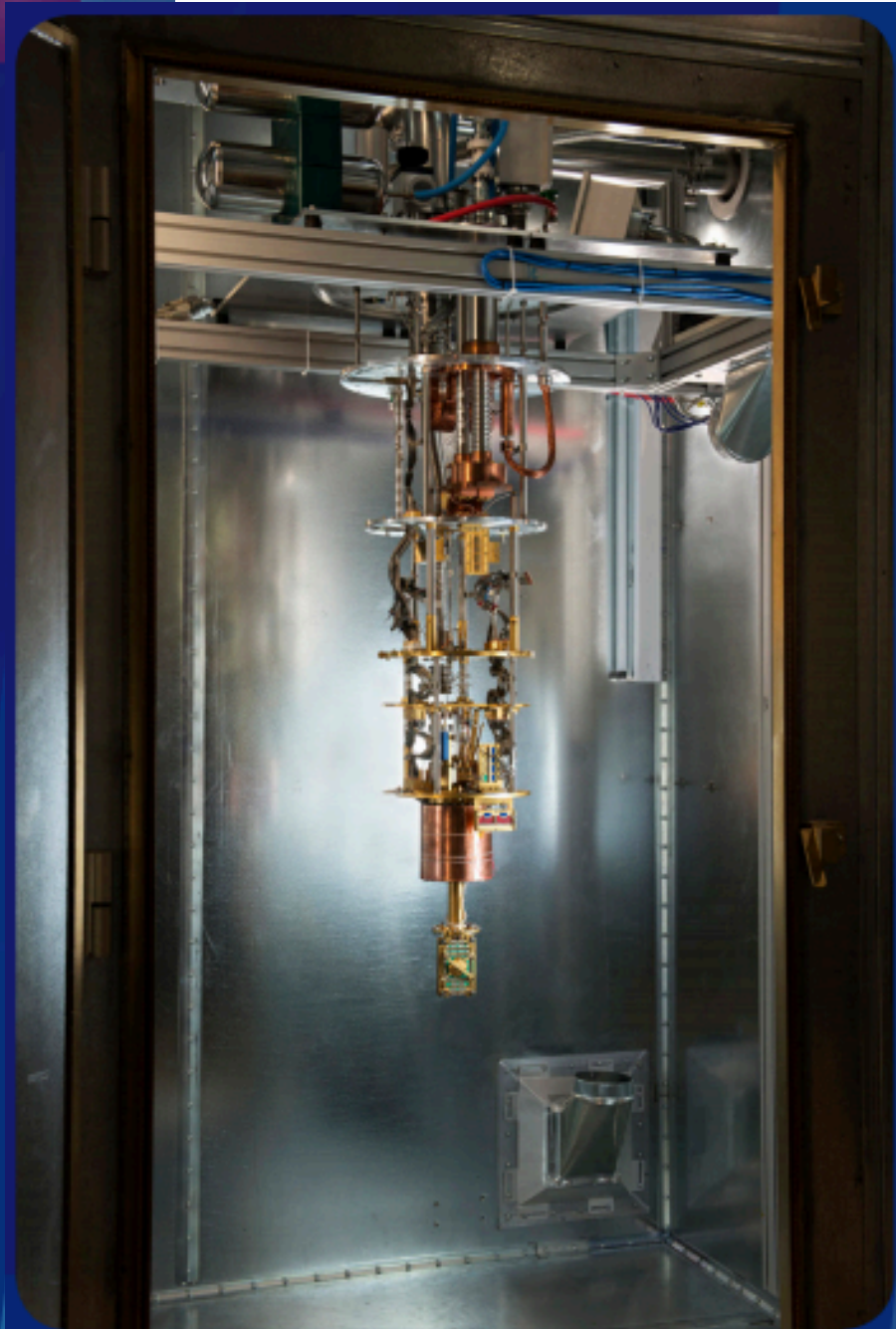


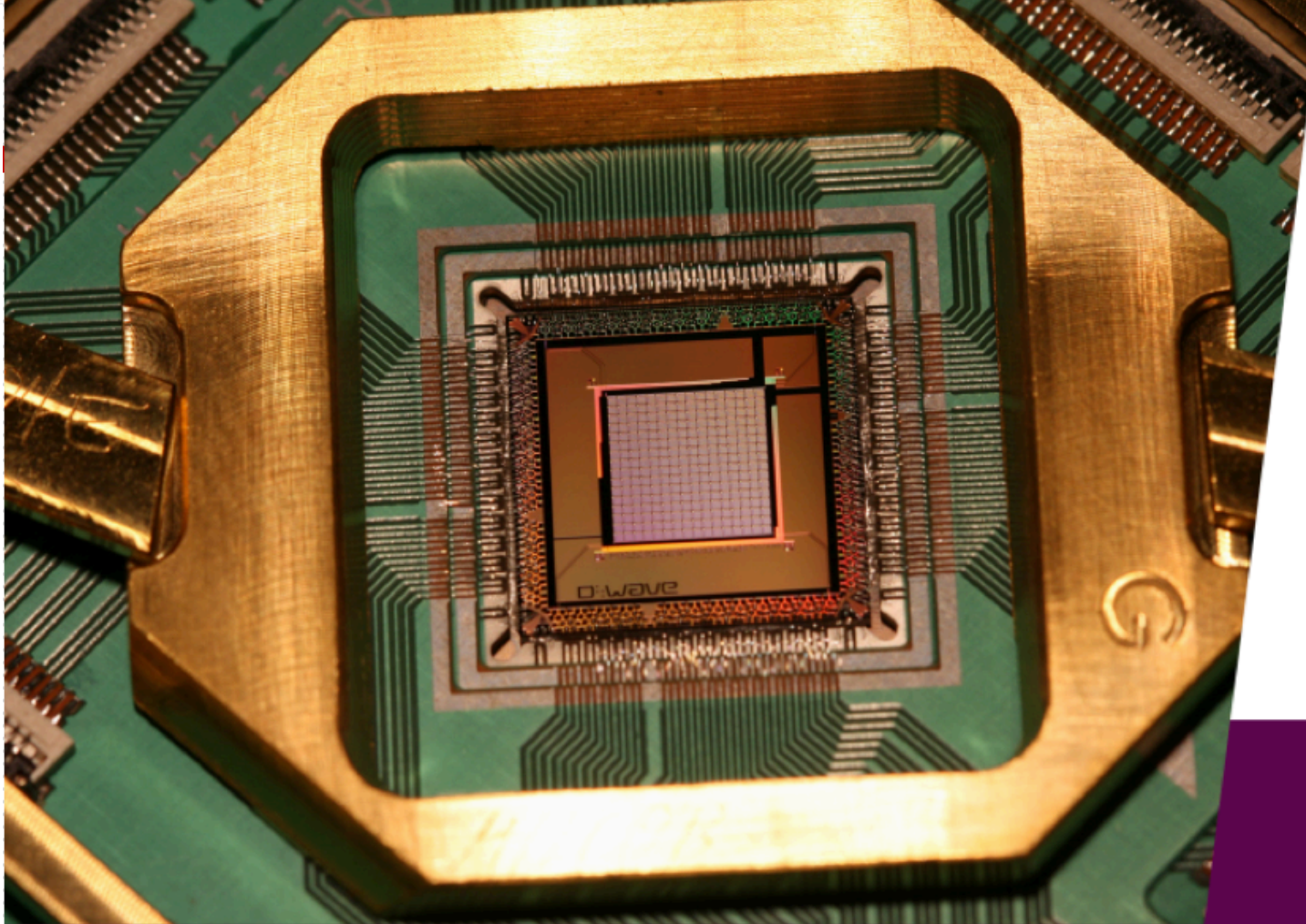


Temperature in kelvin



Starting at room temperature at the top, the temperature decreases at each level until it is close to absolute zero where the QPU itself is located.

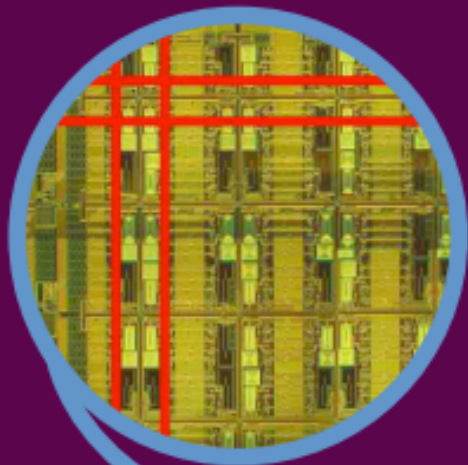




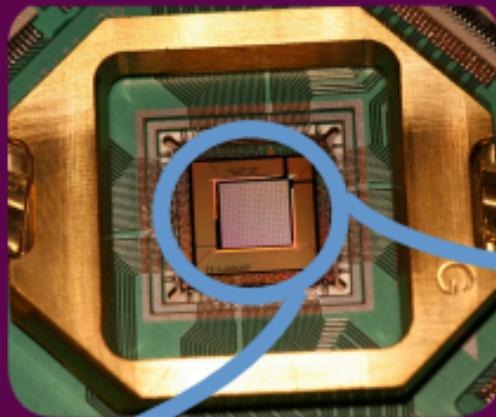
The D-Wave QPU is built from a lattice of tiny loops of the metal niobium, each of which is one qubit (shown on the next page, in red). Below temperatures of 9.2 kelvin, niobium becomes a superconductor and exhibits quantum mechanical effects.

When in a quantum state, current flows in both directions simultaneously, which means that the qubit is in superposition—that is, in both a 0 and a 1 state at the same time. At the end of the problem-solving process, this superposition collapses into one of the two classical states, 0 or 1.

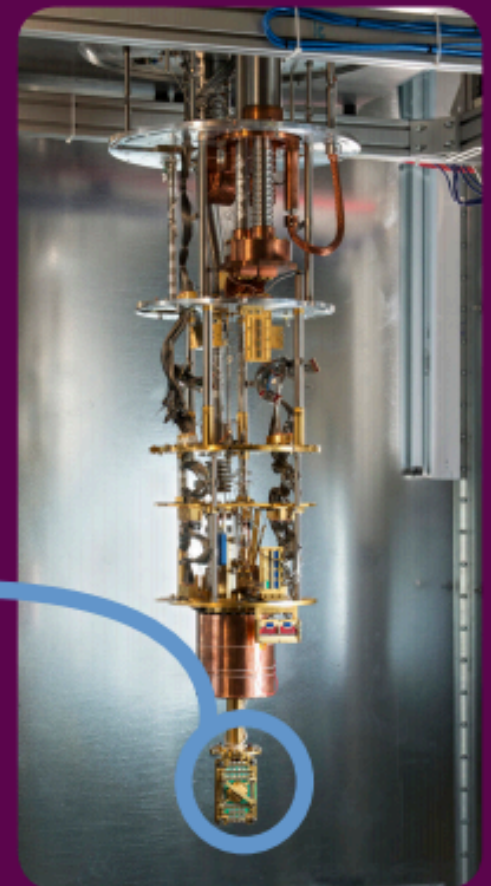
Qubits in red



Quantum processing unit



Inside the D-Wave enclosure



D-Wave Announces D-Wave 2000Q Quantum Computer and First System Order

<https://goo.gl/zhKUUo>

2017/01/24

D-Wave Announces D-Wave 2000Q

- D-Wave Systems Inc., the leader in quantum computing systems and software, today announced general commercial availability of the D-Wave 2000Q™ quantum computer. D-Wave also [announced the first customer](#) for the new system, [Temporal Defense Systems Inc.](#) (TDS), a cutting-edge cyber security firm. With 2000 qubits and new control features, the new system can solve larger problems than was previously possible, with faster performance, providing a big step toward production applications in optimization, cybersecurity, machine learning, and sampling.

-
- "D-Wave's leap from 1000 qubits to 2000 qubits is a major technical achievement and an important advance for the emerging field of quantum computing," said Earl Joseph, IDC program vice president for high performance computing. "D-Wave is the only company with a product designed to run quantum computing problems, and the new D-Wave 2000Q system should be even more interesting to researchers and application developers who want to explore this revolutionary new approach to computing."



-
- ❑ In benchmark tests, D-Wave QPUs outperformed competitive classical algorithms by 1000 to 10000 times in pure computation time. For these tests, D-Wave developed efficient CPU- and GPU-based implementations of highly specialized algorithms that are recognized as the stiffest competition to D-Wave QPUs, and ran them on the latest-generation classical computer servers. These benchmark problems in sampling and optimization were created to represent the structure of common real-world problems, while maximizing the size of the problem that could fit on the 2000-qubit QPU. The benchmark comparisons were relative to single CPU cores and 2500-core GPUs at the largest problem size. [Link to technical white paper.](#)

Aaronson D-Wave 訪問

- D-Wave批判の急先鋒だった Scott Aaronsonが、"D-Wave Open Thread"というblogを公開している。
<https://goo.gl/6kZ1dT>
- 僕が、D-Waveのアニーリング量子コンピューターに興味を持った頃、もっとも辛辣にその批判を展開していた、彼に、僕は興味を持った。すぐに、ユーモアと皮肉のセンスがあって、哲学好きの彼のファンになった。

August 26th, 2015

<https://goo.gl/Gm6XDy>



Aaronson D-Wave 訪問

- 今回のblogは、新しいD-Waveマシンに噛み付くものではなかった。もちろん、それを全面的に肯定するものではない。どちらかといえば、「生暖かく」見守ってもいいという立場だと思う。
- 国際線で、二本の子供向け映画「シンデレラ」と「トゥマローランド」を見た彼は、ふと思う。未来について、子供のような夢や希望があってもいいのだと。「スケーラブルな量子コンピュータを作るために、たくさんのアイデアの花を咲かせよう。もちろん、D-Waveのアイデアも含んで！ 勇気を持って、人に優しくなろう！」その「善意」のあかしとして、かれは、blogを、彼がD-Waveを訪問した時の写真で締めくくっている。
- 内容的に興味深いのは、Googleに入った John Martinis が取り組んでいる量子アニーリングコンピュータへの期待が大きいことだった。いずれ、何かが出てくるだろう。

<https://goo.gl/Gm6XDy>

The D-Wave 2000Q™ Quantum Computer Technology Overview



<https://goo.gl/A5W62F>

Applications

□ Machine Learning & Computer Science

- Detecting statistical anomalies
- Finding compressed models
- Recognizing images and patterns
- Training neural networks
- Verifying and validating software
- Classifying unstructured data
- Diagnosing circuit faults

□ Financial Modeling

- Detecting market instabilities
- Developing trading strategies
- Optimizing trading trajectories
- Optimizing asset pricing and hedging
- Optimizing portfolios

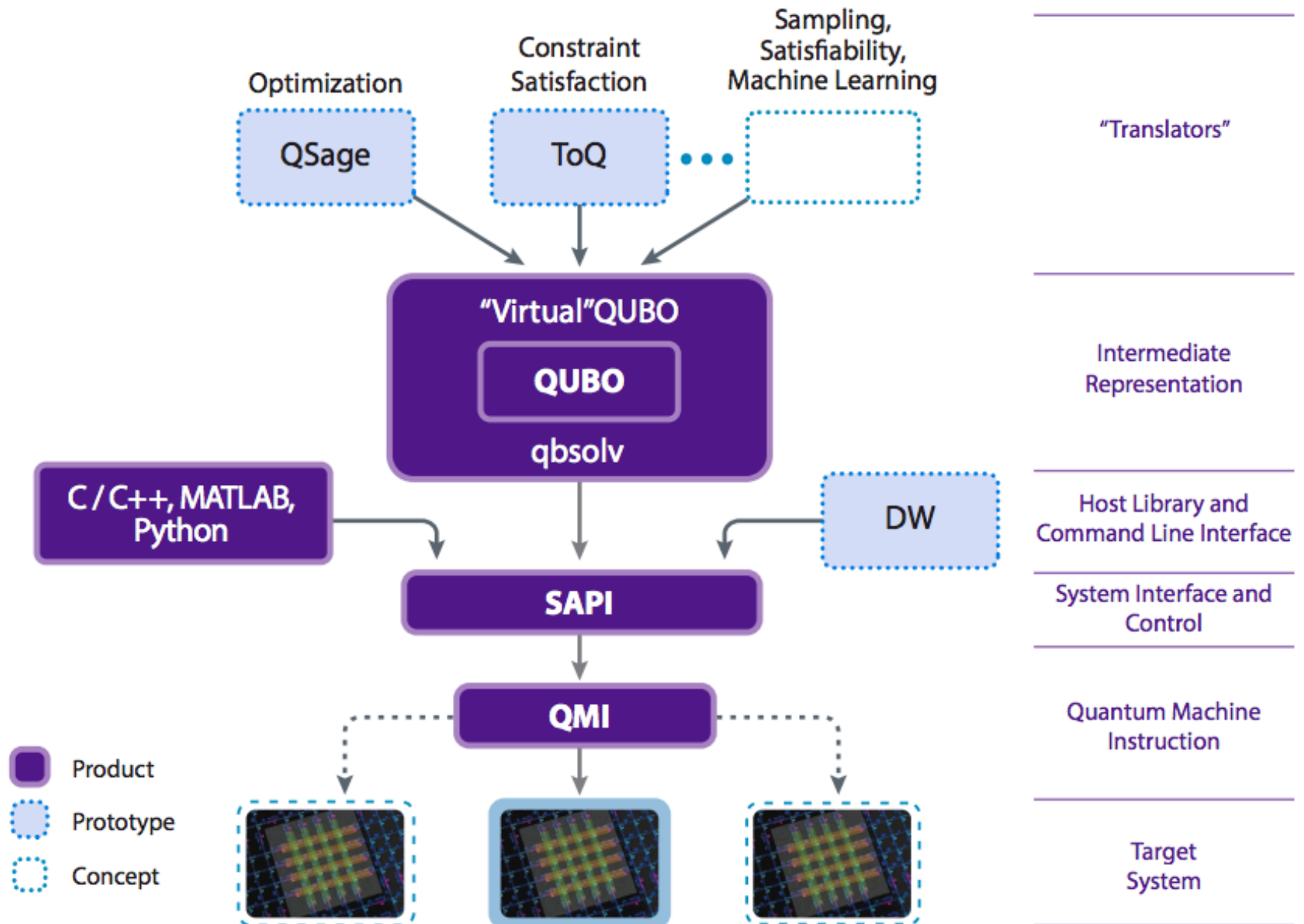
□ Security & Mission Planning

- Detecting computer viruses & network intrusion
- Scheduling resources and optimal paths
- Determining set membership
- Analyzing graph properties
- Factoring integers

□ Healthcare & Medicine

- Detecting fraud
 - Generating targeted cancer drug therapies
 - Optimizing radiotherapy treatments
 - Creating protein models
-

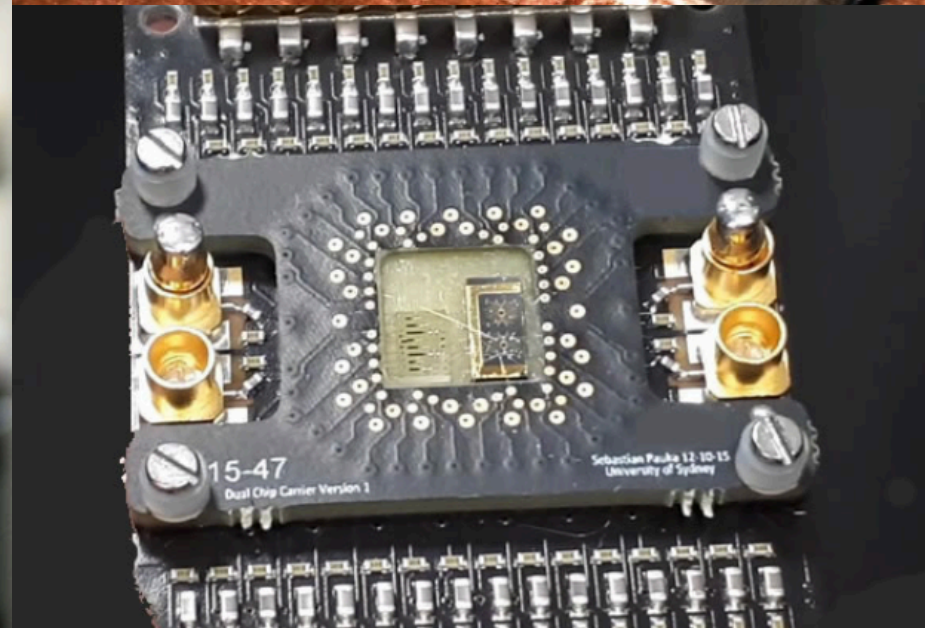
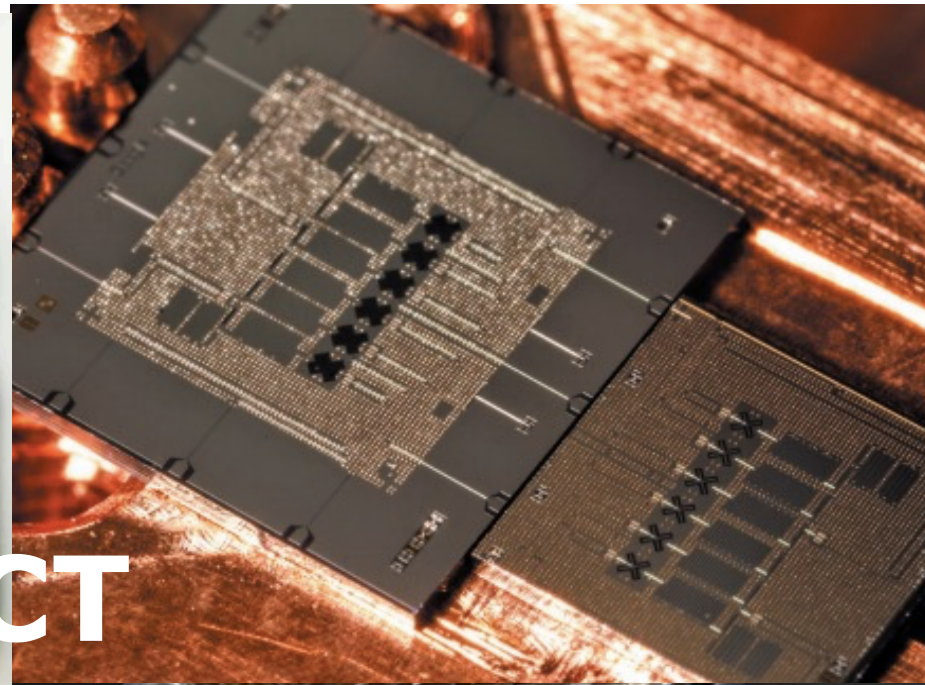
D-Wave Software Environment



What's Next

- While the D-Wave quantum computer is the most advanced in the world, the quantum computing revolution has only begun. Our vision is of a future where quantum computers will be accessible and of value to all, solving the world's most complex computing problems. This will require advances in many dimensions and contributions from experts in diverse domains. It is exciting to see increasing investment worldwide, advances in research and technology, and a growing ecosystem of developers, users, and applications needed to deliver on that vision. To learn more, contact us or check out our videos, white papers, scientific papers, and other content at www.dwavesys.com/resources

ImPACT



光を使って難問を解く新しい量子計算原理を実現 ～量子ニューラルネットワークの開発～

- 内閣府 総合科学技術・イノベーション会議が主導する革新的研究開発推進プログラム(ImPACT)の山本 喜久 プログラム・マネージャーの研究開発プログラムの一環として、日本電信電話株式会社(東京都千代田区、代表取締役社長 鵜浦 博夫 以下、NTT) NTT物性科学基礎研究所 量子光制御研究グループの武居 弘樹 主幹研究員、稲垣 卓弘 研究員らのグループと、情報・システム研究機構 国立情報学研究所(東京都千代田区、所長 喜連川 優 以下、NII)情報学プリンシプル研究系の宇都宮 聖子 准教授、Peter McMahon 研究員らのグループは、現代コンピュータでは効率よく解くことが困難とされている組合せ最適化問題の解を高速に求める「量子ニューラルネットワーク」を実現しました。

-
- インターネット、電力ネット、センサネットなど、社会を構成する様々なネットワークが大規模化・複雑化する現在、リソースの最適化が重要な課題となっています。これらの課題の多くは組合せ最適化問題と呼ばれる、現代コンピュータが苦手とする数学的問題に帰着することが知られています。量子ニューラルネットワークは、光パラメトリック発振器と呼ばれる新型レーザの発振振幅を用いてスピン^{注2)}を表した時、相互作用する多数のスピンが全体のエネルギーを最低とするようなスピン配列で発振する現象を利用して、組合せ最適化問題の解を探索するものです。
-

□ 今回、各光パラメトリック発振器の振幅を光ホモダイン検波器で測定し、得た情報を帰還する「量子測定フィードバック」を実装することで、全ての光パラメトリック発振器間の結合が可能な量子ニューラルネットワークを実現しました。これにより、最大2,000ノード・200万結合の大規模組合せ最適化問題の解探索に成功し、現代コンピュータ上で動作する既存アルゴリズムを凌駕する性能を示しました。今後、創薬、無線通信、圧縮センシング、深層学習といった実社会の様々な組合せ最適化問題への本成果の適用が期待されます。

□ 本研究は、NIIの河原林 健一 教授、東京大学の合原 一幸 教授、大阪大学の井上 恭 教授、スタンフォード大学のMartin Fejer 教授の研究グループと共同で行ったものです。本研究成果を記述した2編の論文は、2016年10月20日13時（米国東部標準時）発行の米国の科学誌「Science」のオンライン速報版で同時に公開されます。

“A coherent Ising machine”

タイトル
(和訳)

“A coherent Ising machine for 2000-node optimization problems”
(2000ノードの最適化問題を解くコヒーレントイジングマシン)

doi

[10.1126/science.aah4243](https://doi.org/10.1126/science.aah4243)

タイトル
(和訳)

“A fully-programmable 100-spin coherent Ising machine with all-to-all connections”
(全結合を有する完全にプログラム可能な100スピンのコヒーレントイジングマシン)

doi

[10.1126/science.aah5178](https://doi.org/10.1126/science.aah5178)

表1 3つの量子計算原理の比較

	量子コンピュータ	量子アニーラ	量子ニューラルネットワーク	
計算原理	状態ベクトルのユニタリ回転 (閉鎖系)	ハミルトニアン の断熱変化 (閉鎖系)	測定フィードバック系の 量子相転移 (開放系)	
開発機関	IBM/Google	D-WAVE	NII-Stanford	NTT
ビット数	5~9ビット	1,152ビット	100ビット	2,048ビット
結線数	≤10	3,300	1万	400万
動作温度	極低温 (10mK)	極低温 (10mK)	室温 (300 K)	
物理系	超伝導量子回路	超伝導量子回路	光パラメトリック発振器 ネットワーク	
適用先	問題に隠れた 周期性がある場合 (暗号解読など)	NP困難・NP完全問題 (組合せ最適化など)	NP困難・NP完全問題 (組合せ最適化など)	
有効ビットの割合	—	95%	100%	
解ける問題サイズ	—	$N \leq 15 \sim 17$	$N \leq 2,048$	

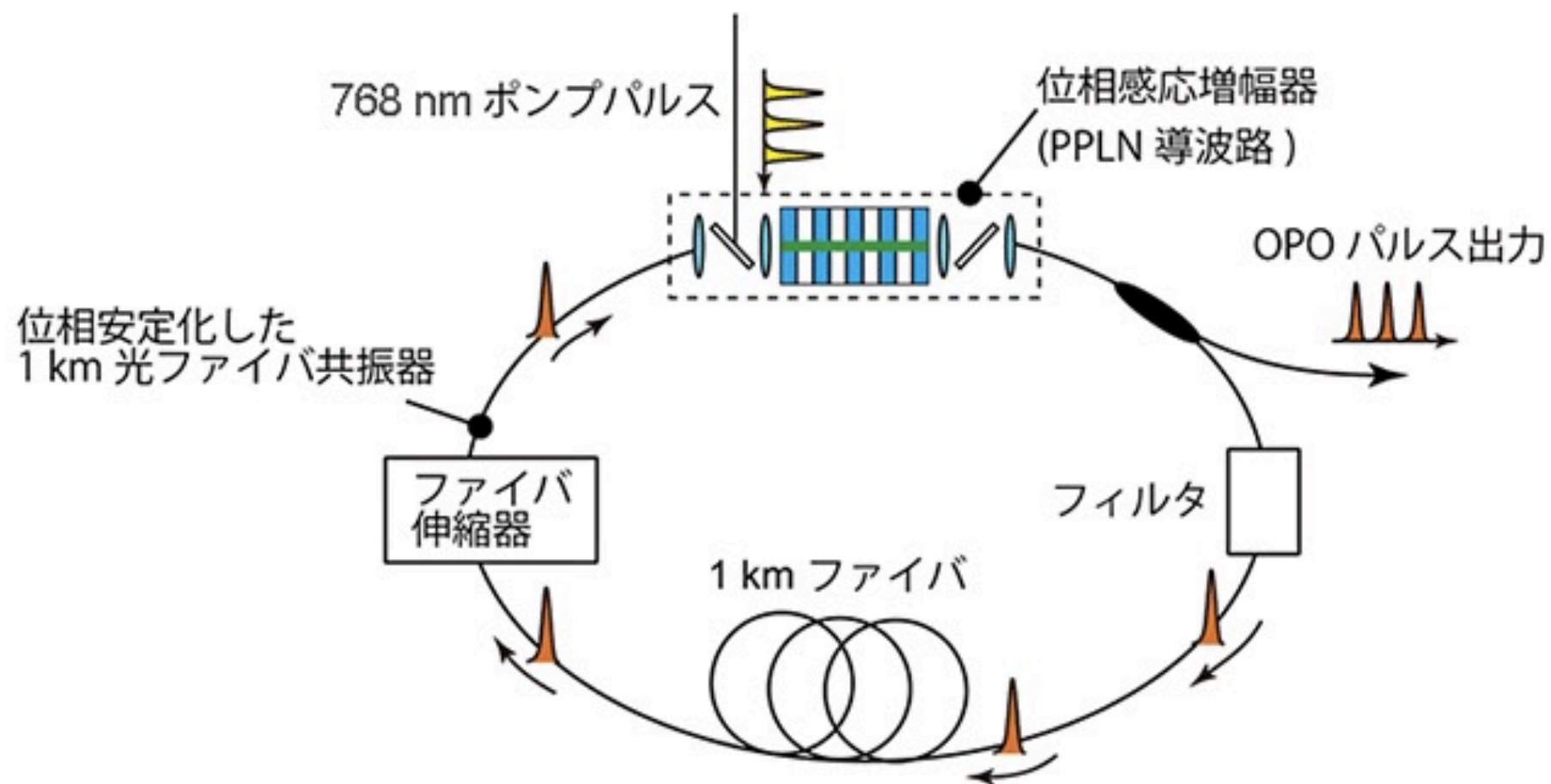


図5 長距離光ファイバ共振器による多数のOPOの一括発生

<技術のポイント>

(1) 長距離光ファイバ共振器を用いた多数のOPOの一括発生

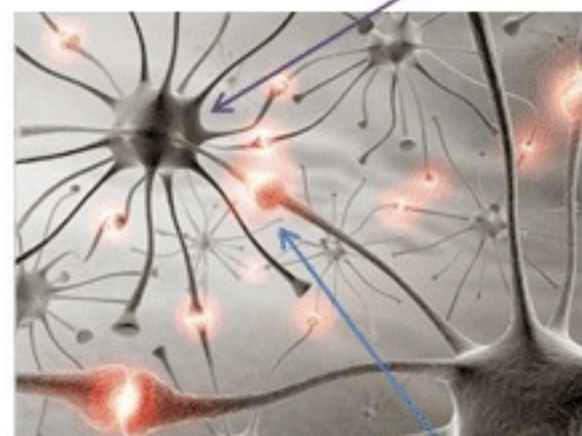
- 実験系を図5に示します。フィードバック制御により位相を安定化した長さ1kmの光ファイバ共振器中に、周期分極反転ニオブ酸リチウム (Periodically Poled Lithium Niobate: PPLN) 導波路^{注5)}を挿入します。PPLN導波路に、波長768nm、繰り返し周波数1GHzのポンプパルス列を入力します。PPLN導波路においては、ポンプ波長の2倍にあたる1536nmの波長において、ポンプ光の位相に対して0または π の位相成分だけが増幅される位相感応増幅と呼ばれる現象が得られます。ポンプ光入力直後に位相感応増幅により発生した雑音が種光となり、光ファイバ共振器中の波長フィルタの透過波長を1536nmとすることで、位相が0または π のみの光が発振するOPOを実現できます。光ファイバ共振器の一周時間が約5 μ s、ポンプパルスの時間間隔が1nsなので、本実験系を用いて時間的に多重された約5,000個のOPOを一括して発生することができます。

(2) 量子測定フィードバックによるOPO間の結合

- [図1](#)に構成を示します。OPOパルスの発生過程において、光ファイバ共振器中を周回するOPOパルス列のエネルギーを一部とりだし、各OPOパルスの位相、振幅を測定します。測定結果はFPGAに入力します。FPGAには、どのOPO間を結合するかという情報をあらかじめ入力しておきます。FPGAは、これらの情報をもとに、次のステップで各OPOに入力するフィードバック信号を計算します。このフィードバック信号を、OPOと同一の波長と位相をもつ光パルスに重畳し、該当するOPOに同期して注入することで、OPO間の結合を実現します。これにより、全ての組合せのOPO間結合を実装することが可能となります。今回の実験では、最大2, 048のOPOに対し本手法を実装することで、2百万通り以上のスピン間結合(無向グラフの場合)を実現しました。



人間の脳は、1,000億個のニューロンがそれぞれ数万個のシナプス結合で相互に結ばれた巨大な神経細胞ネットワーク



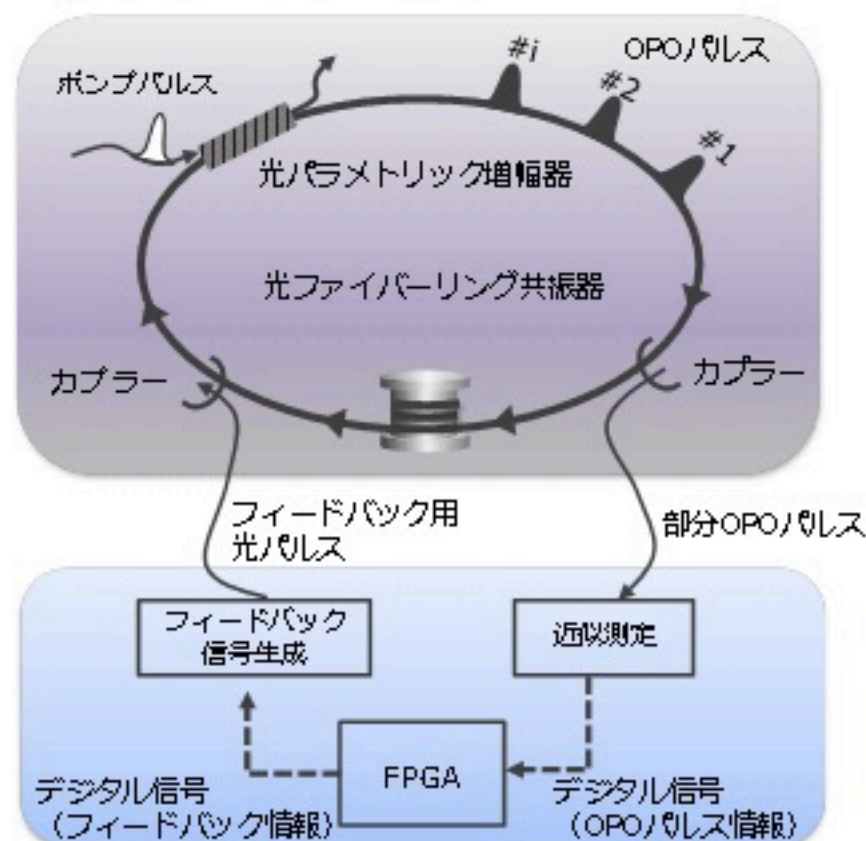
<http://www.wisc.edu/neuro/ep-neuro-communications-pov-01.html>

ニューロン

シナプス

光パラメトリック発振器(OPO)パルス
(量子アナログデバイス)

⇒ 情報処理



FPGA測定フィードバック回路
(古典デジタルデバイス)

⇒ 通信

図1 光パラメトリック発振器と量子測定フィードバックから構成される量子ニューラルネットワーク

<研究の背景と経緯>

- 現代社会の様々な分野、例えば創薬のための化合物探索、無線通信ネットワークにおけるリソース最適化、不完全な観測データから元情報をできるだけ忠実に再現する圧縮センシングなどでは、大規模な組合せ最適化問題を高速で解く計算手法が必要とされています。組合せ最適化問題とは、様々な条件の下で、多数ある選択肢の中から最適なものを選び出す問題で、問題サイズが大きくなると選択肢が爆発的に増えるために、現代コンピュータでは解くことが困難になることが知られています。組合せ最適化問題の多くは相互作用するスピン群のモデルである「イジングモデル」のエネルギー最低状態を求める問題に変換可能であることが知られています。そのために、様々な物理系を用いて人工スピン群を作製し、イジングモデルを通して組合せ最適化問題を高速に解く試みが世界の有力企業を中心に精力的に進められています。