

情報処理応用B 第4回

藤田 一寿

量子計算機 概要の概要

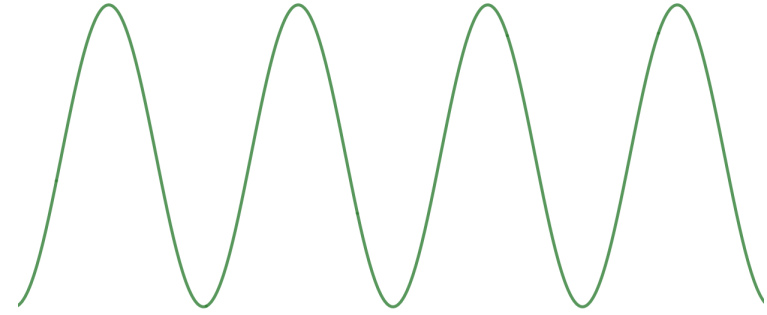
量子の世界の基礎の基礎の基礎

物質は粒か波か



粒

例えばボールは丸い物体だから粒だろう。



波

そのボールに波の性質があるのか？

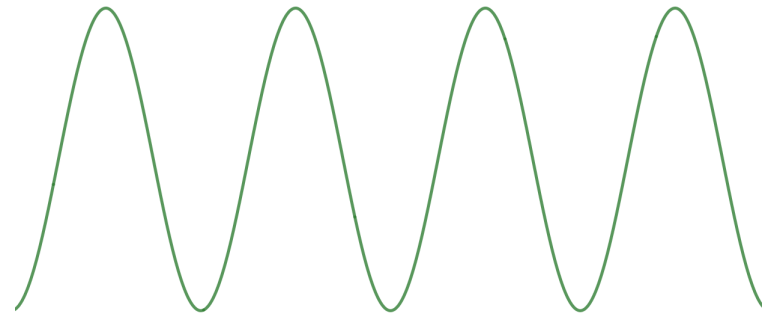
粒が波とか何言ってるんだ…



■ 量子の世界では物質は粒でもあり波でもある



粒



波

物質は粒でもあり波でもある！！



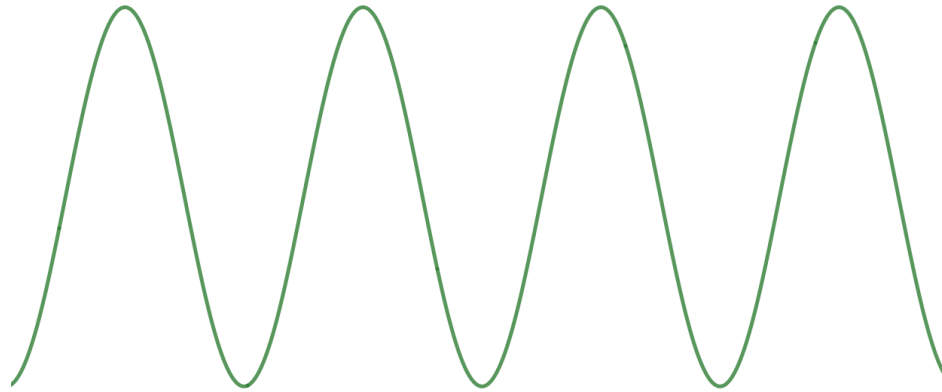
■ 粒とは

- 我々が思う粒
 - ボールのようなもの.
 - 手にとって触ることが出来る.
 - それぞれは別のもの.
 - 数えられる.
- 量子の世界の粒（量子）
 - 数えられる.



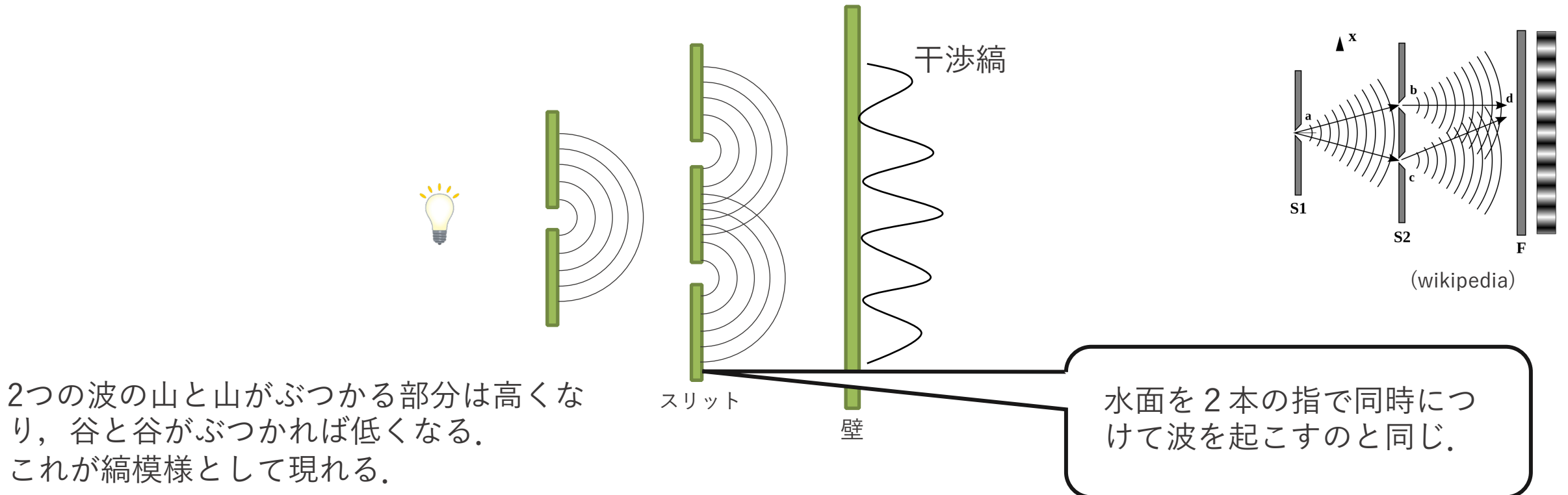
■ 波とは

- 振動している.
- 振動が周りに伝わる.

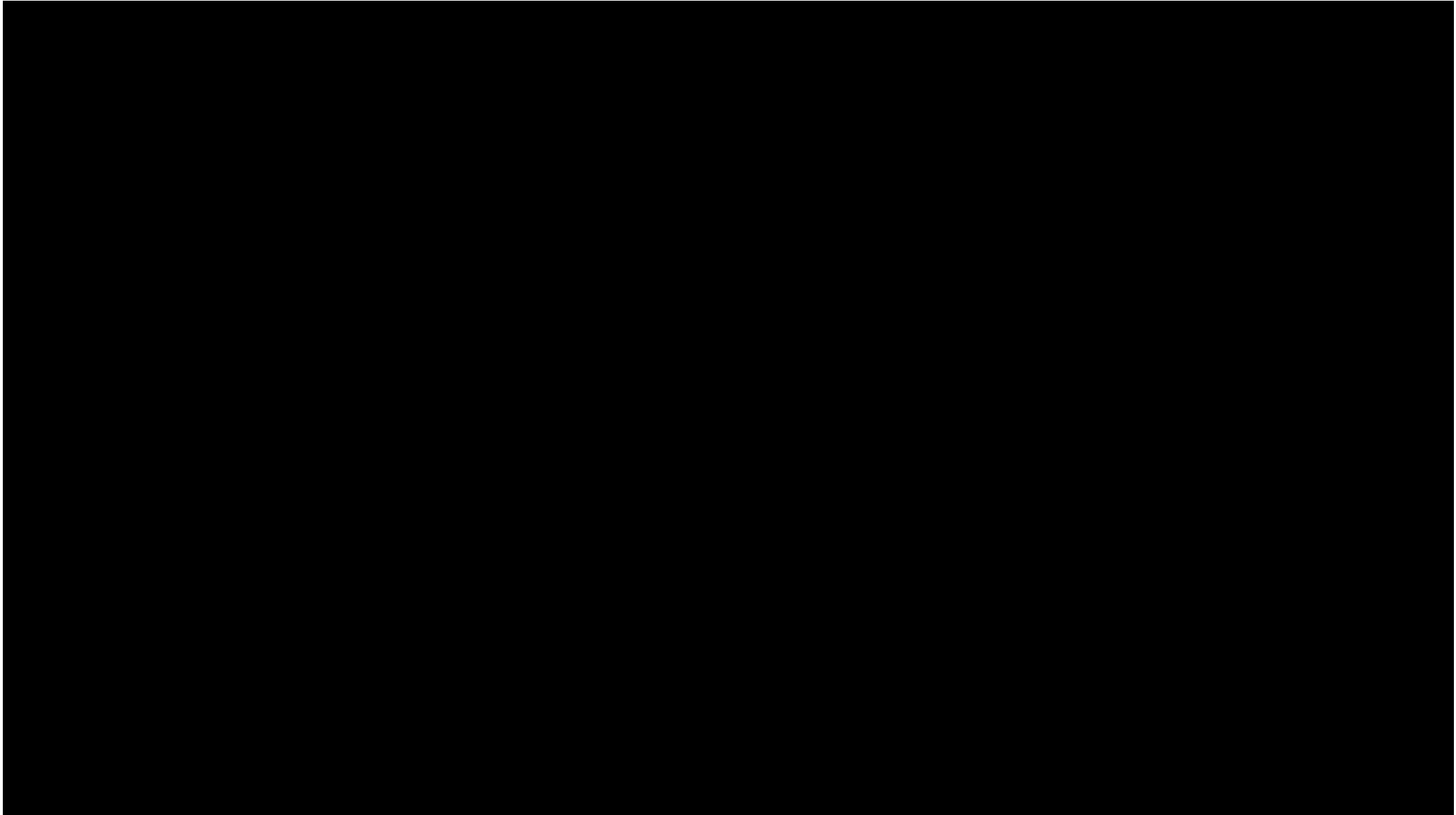


■ ヤングの2重スリット実験

- 2重スリットから出てきた波を壁で観測すると干渉縞が現れる.
- 干渉縞は波である証拠となる.
- 光も波なので同じ実験をすると干渉縞が現れる.



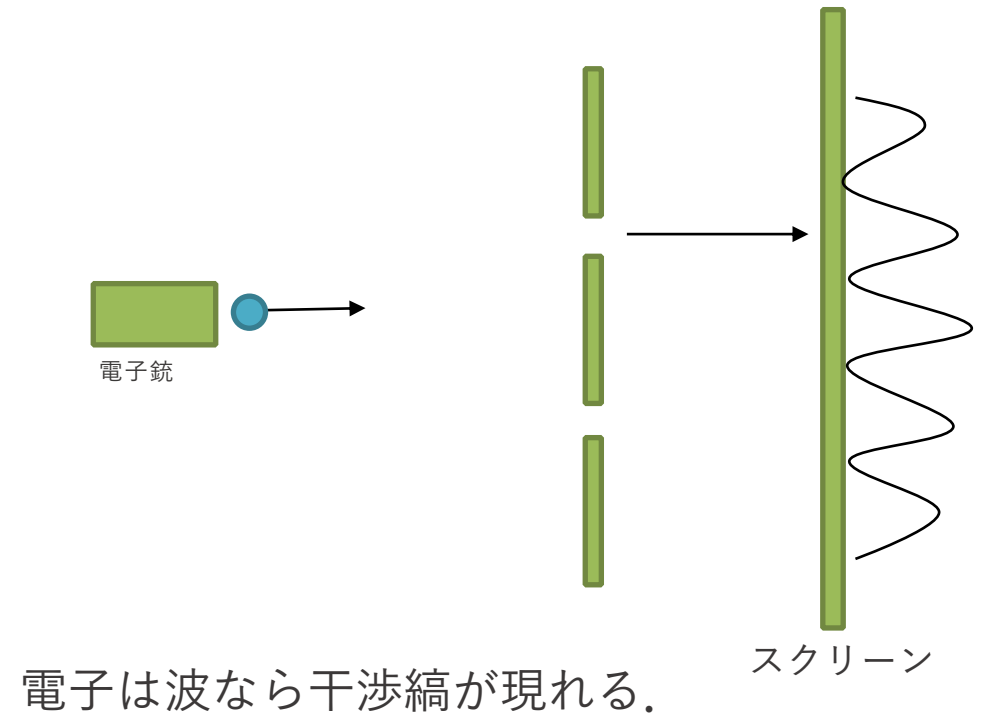
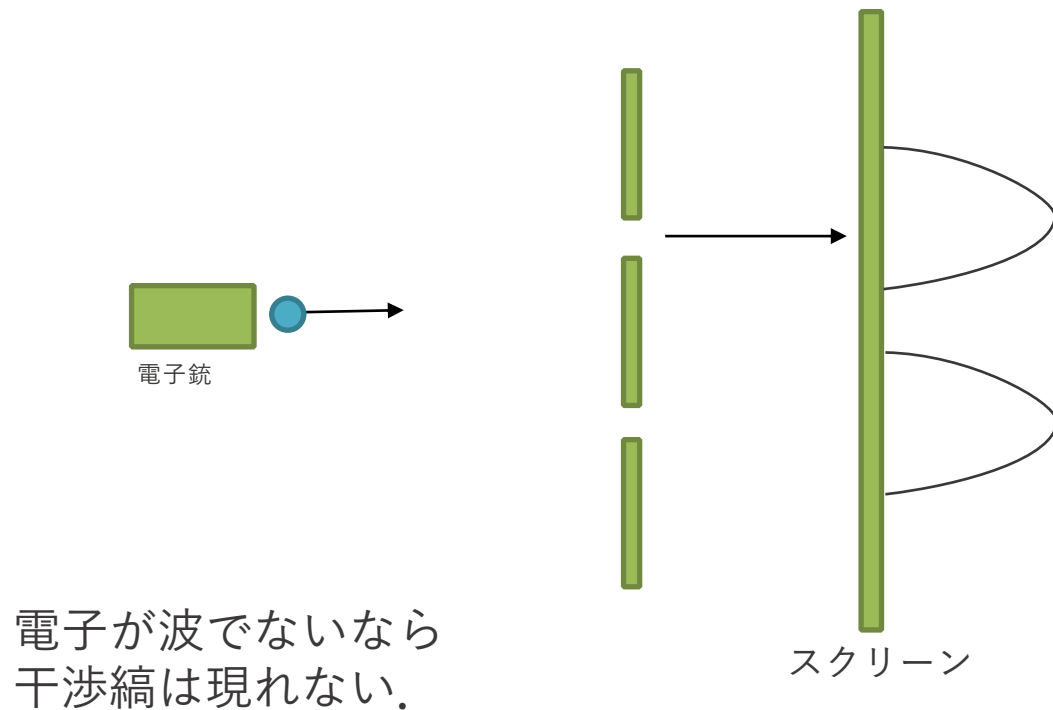
■ 干渉縞の実験



<https://www.youtube.com/watch?v=luv6hY6zsd0>

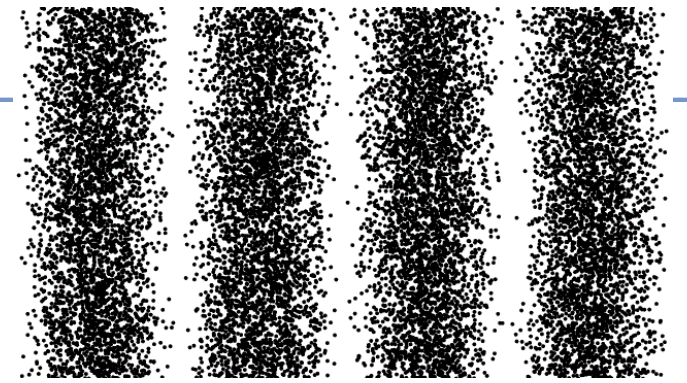
■ 電子の2重スリット実験

- ド・ブロイは粒も波として振る舞うと突拍子もない提案をする。
 - 物質は波らしい？（物質波とよぶ）
- 粒の代表として電子を2重スリットにぶつけたらどうなるか？
 - 電子の2重スリット実験

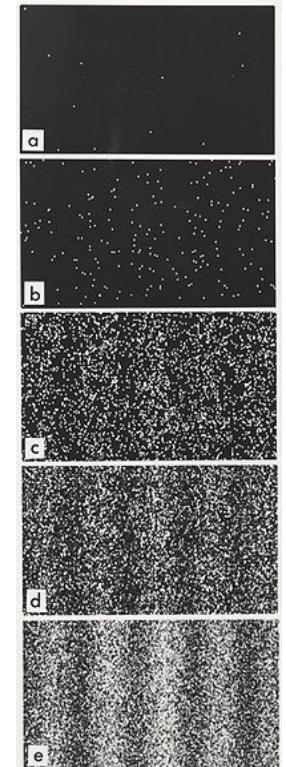
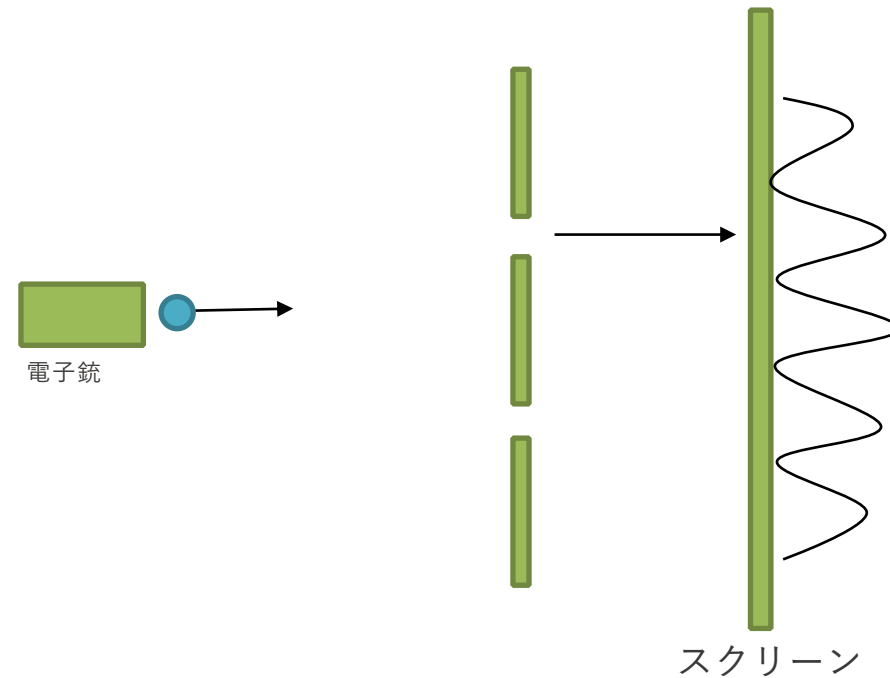


■ 電子の2重スリット実験

- 電子を2重スリット越しのスクリーンに当てる.
- スクリーンには干渉縞が現れる.
- 電子は波だった.



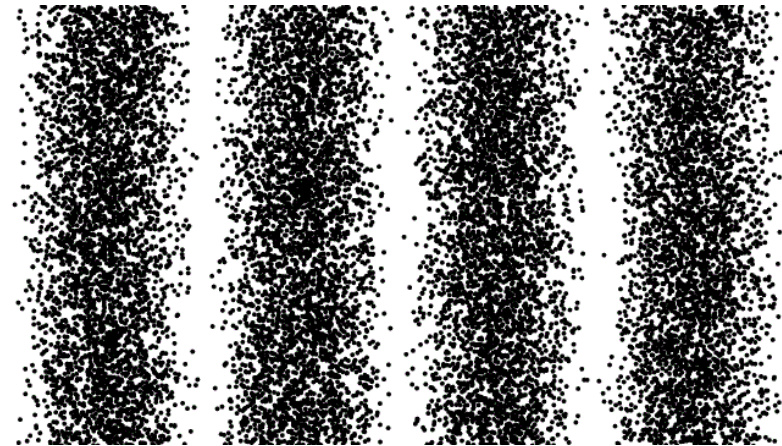
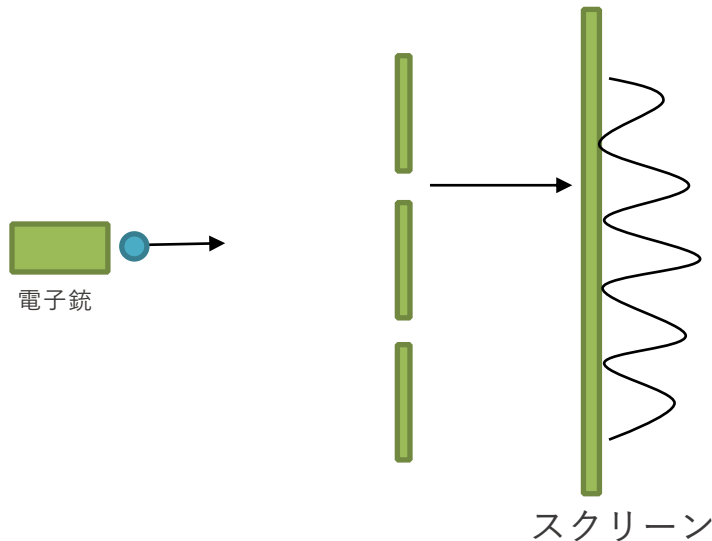
(https://en.wikipedia.org/wiki/File:Wave-particle_duality.gif)



原康夫 現代物理学

■ 電子の2重スリット実験

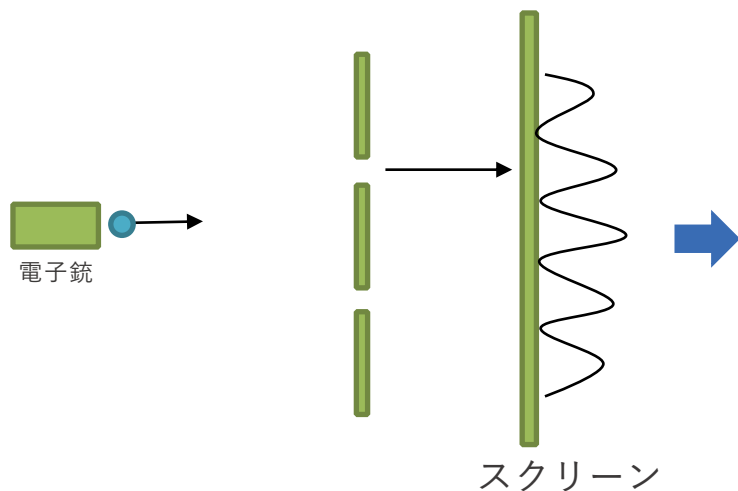
- 電子一つを飛ばして、それがスクリーンのどの場所にぶつかるか分からない。
- しかし、ぶつかりやすい場所は分かっている。
 - 干渉縞の濃い部分にぶつかりやすい。



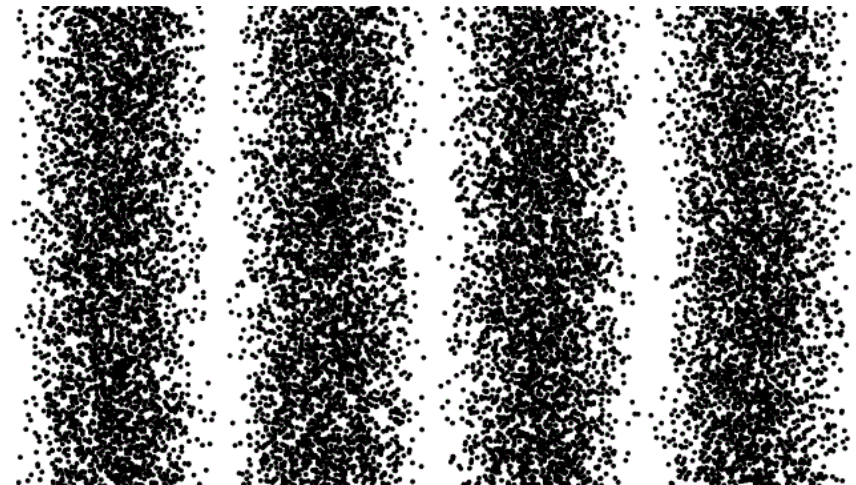
(https://en.wikipedia.org/wiki/File:Wave-particle_duality.gif)

■ 電子の2重スリット実験

- ぶつかりやすさを確率だと思えば、干渉縞の濃淡は電子がぶつかる場所の確率分布になっている。
- 電子の場所は確率で決まる。



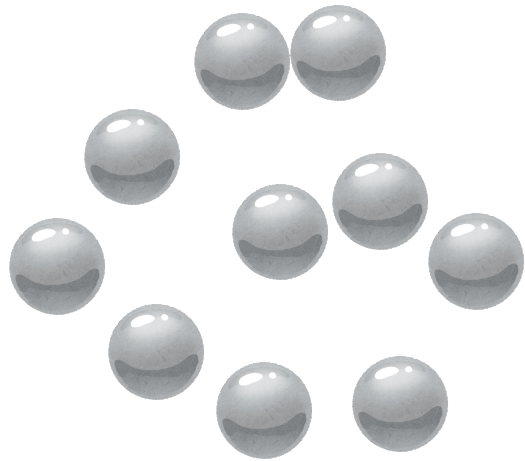
縞模様（濃淡）が、ある場所で電子が検出される確率密度関数（確率分布）になっている。



(https://en.wikipedia.org/wiki/File:Wave-particle_duality.gif)

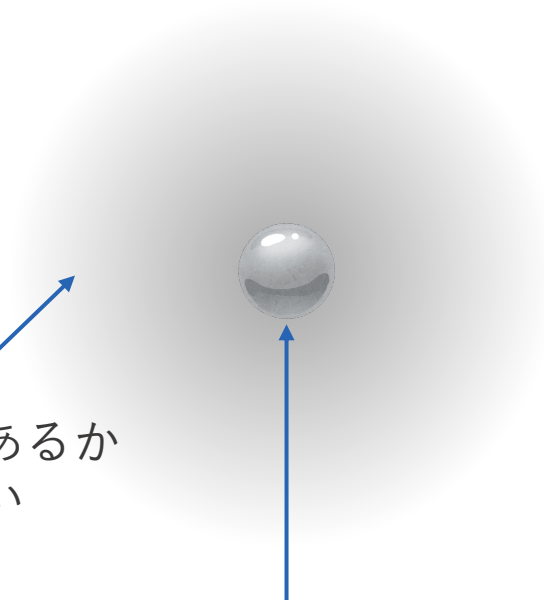
覚えておきたい量子の性質

- 電子などの小さな粒子（量子）は数えられる.
- 電子などの小さな粒子（量子）の状態は確率で決まる.
- 電子などの小さな粒子（量子）の状態は飛び飛び（離散的）である.



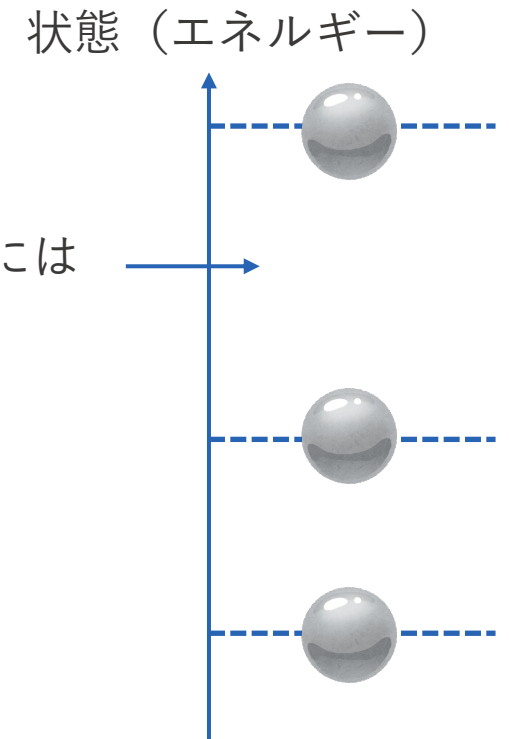
数えられる

この辺にあるか
もしれない



おおよそこの辺にある

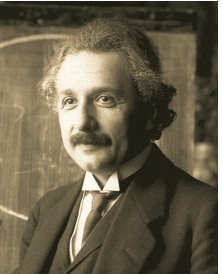
この状態には
なれない



状態は飛び飛び

■ 歴史

- 1920年 イジングモデル (Ising and Lenz)
- 1924年 物質波 (de Broglie)
 - 物質は波である.
- 1926年 シュレディンガー方程式
 - 量子の世界の基礎方程式.
- 1935年 EPR パラドックス (Einstein, Podolsky, Rosen)
 - 量子もつれ (量子エンタングルメント) 現象を指摘.
 - もつれ状態にある量子の片方を観測すれば, もう片方の状態が決まる.
 - 量子力学がこの奇妙な現象を予言している.



■ 歴史

- 1935年 シュレディンガーの猫
 - シュレディンガーが量子力学の奇妙さを猫の思考実験で表現.
- 1939年 ブラケット記法 (Dirac)
 - エレガントな記法
- 1969年 ベルの不等式
 - ベルの不等式が破られると量子もつれが実在する.



2022年のノーベル賞はベルの不等式が破られることを実験で確認したことに対して授与された。



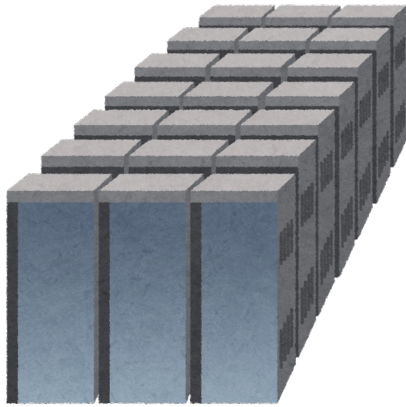
Dirac Heisenberg Schrodinger

量子計算の基礎の基礎の基礎

量子計算機と量子計算

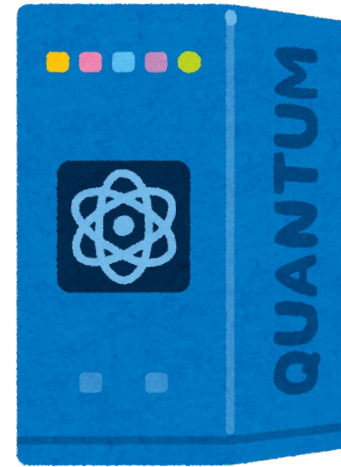
- 量子計算機（量子コンピュータ）は量子計算を行っている。
- 量子計算機以外を古典計算機と呼ぶ。

古典計算機



論理計算が行われている。

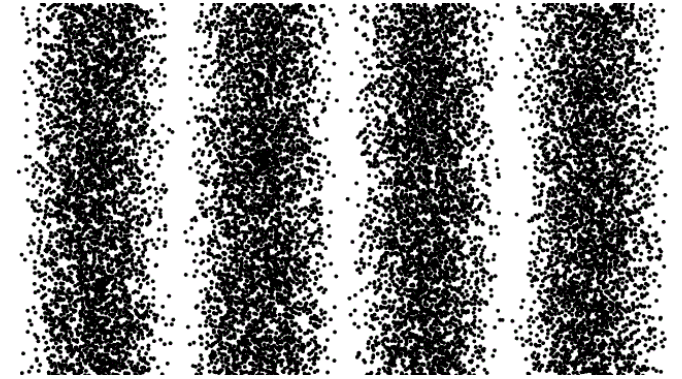
量子計算機



量子計算が行われている。

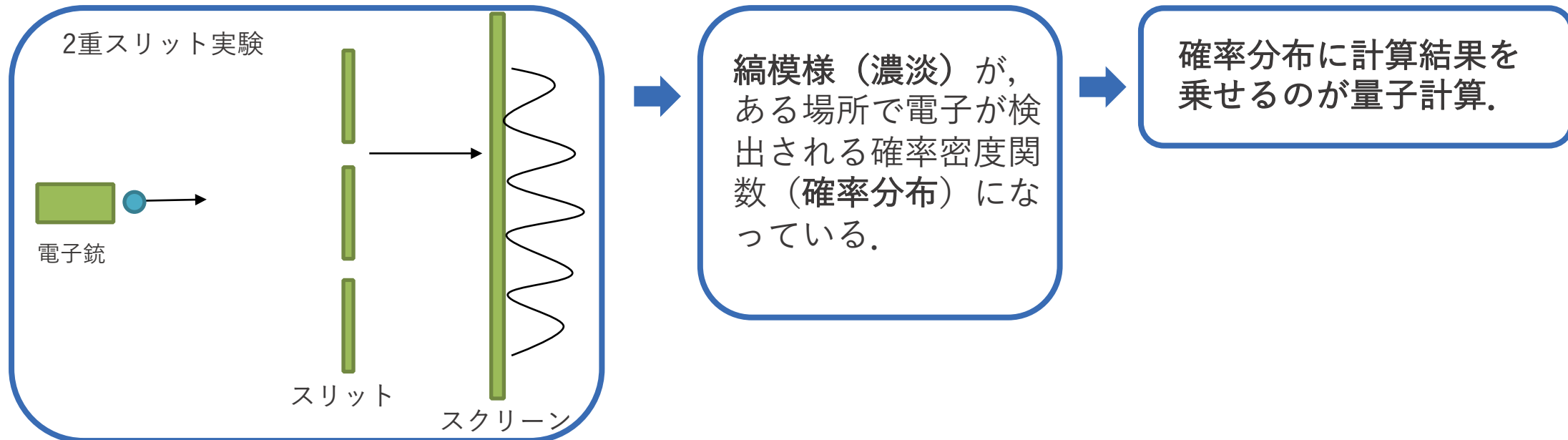
■ 電子の2重スリット実験を使った量子計算の直感的理解

- 電子の2重スリット実験
 - 電子を2重スリット越しのスクリーンに当てる.
 - スクリーンに干渉縞が現れる.
- 量子計算では確率分布が計算結果となる.



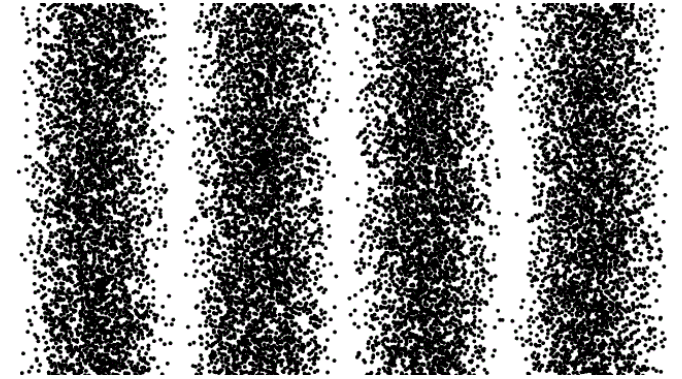
(https://en.wikipedia.org/wiki/File:Wave-particle_duality.gif)

注：あくまでも量子計算の雰囲気伝えるための例え話。実際の量子計算とは異なる



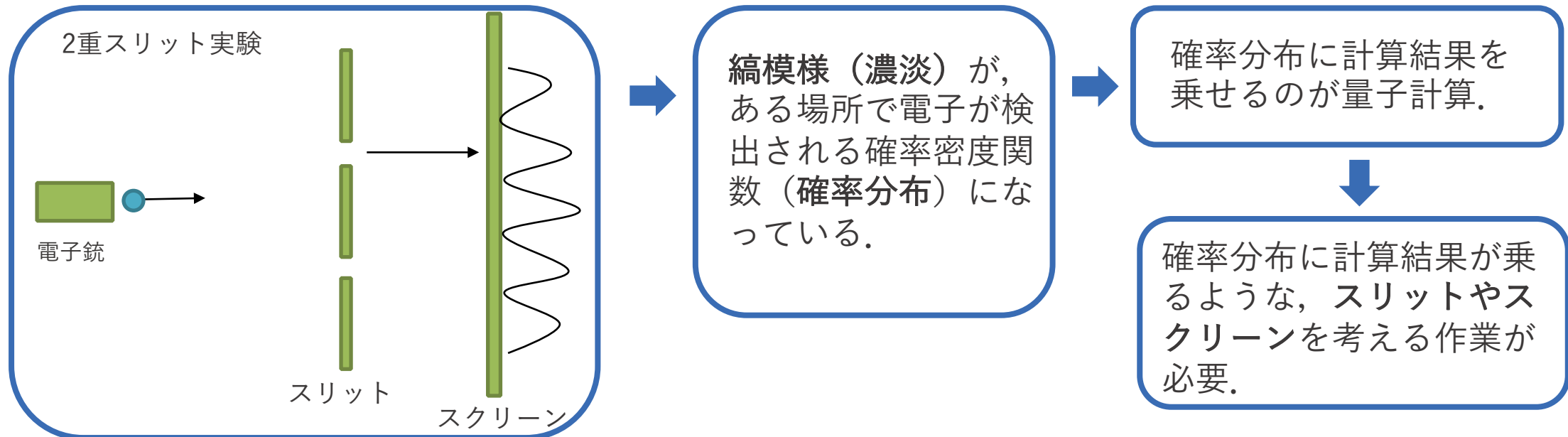
■ 電子の2重スリット実験を使った量子計算の直感的理解

- 干渉縞に計算結果が現れるようなスリットやスクリーンを考えると量子計算では必要である.
- 量子計算では確率分布を変えるスリットやスクリーンにあたるものを量子ゲートと呼ぶ.



(https://en.wikipedia.org/wiki/File:Wave-particle_duality.gif)

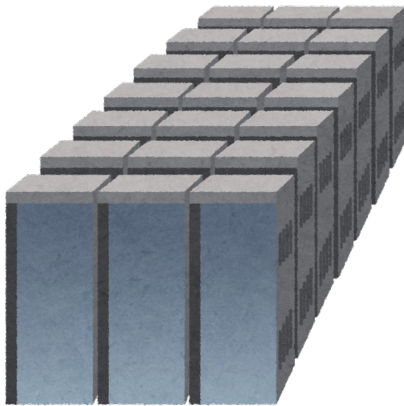
注：あくまでも量子計算の雰囲気伝えるための例え話。実際の量子計算とは異なる



■ ビットと量子ビット

- 古典計算機ではビットを使い情報を表現する.
- 量子計算機では量子ビットを使い情報を表現する.

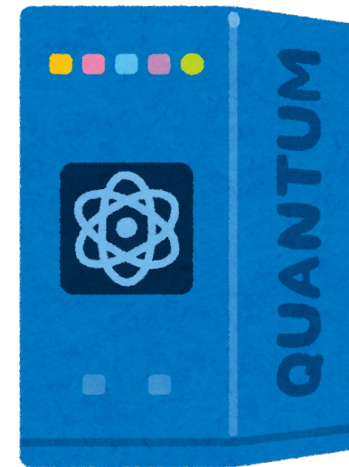
古典計算機



ビットは0か1の値

ビットの値は0か1のどちらかの値に必ず決まっている.

量子計算機



量子ビットは0か1の状態

量子ビットの状態は確率的に決まる.

■ 重ね合わせ状態

- 古典ではビットは 0 か 1 の値しか取れない.
- 量子では量子ビットは 0 と 1 の状態が確率的に決まる.
 - 重ね合わせた状態という.

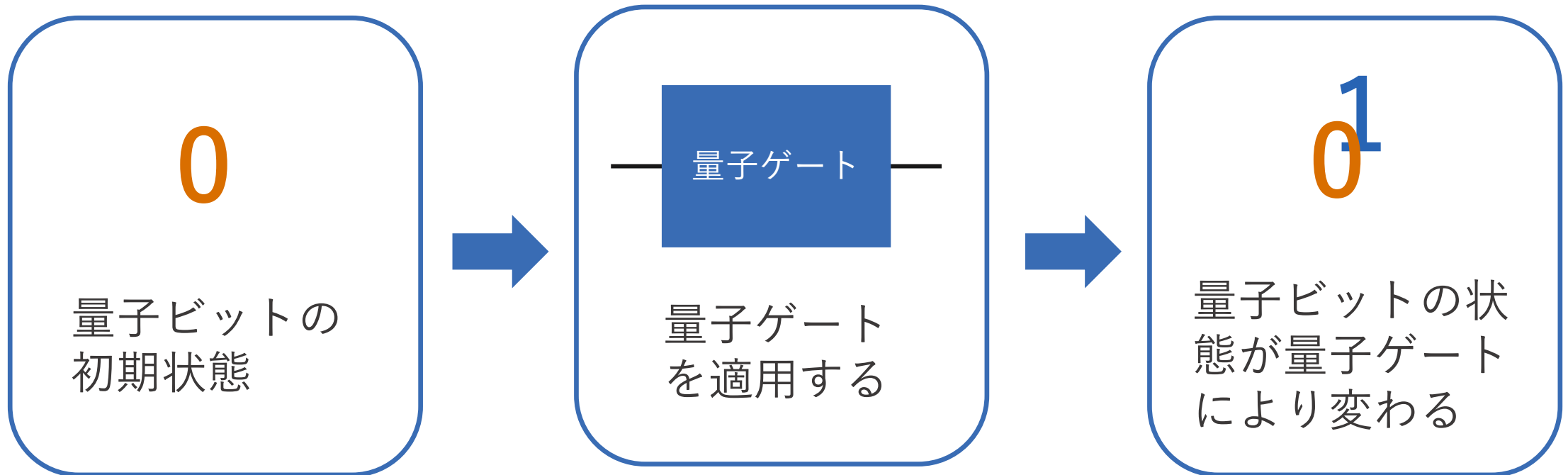
0
1

量子ビットの状態は 0 かもしれないし 1 かもしれない.
0 か 1 かは確率で決まる.



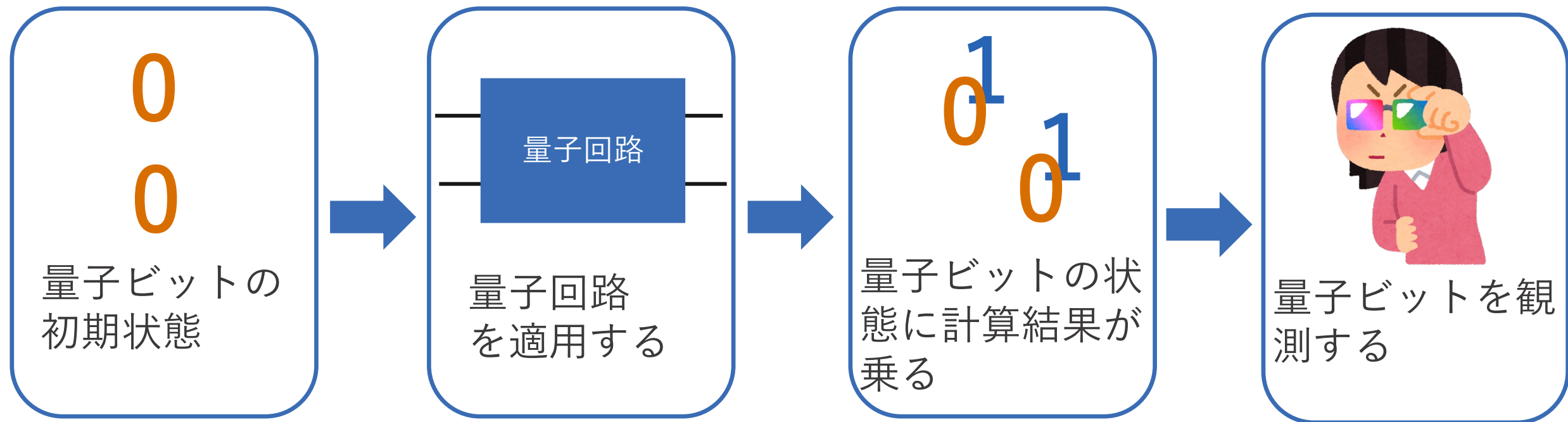
■ 量子ゲート

- 量子ビットの状態は量子ゲートにより変化する.
- 量子ビットに作用させる量子ゲートを組み合わせて, やりたい計算を実現する.
- 量子ゲートの組み合わせを量子回路という.
- 目的の計算結果を得られるように量子回路を組む.



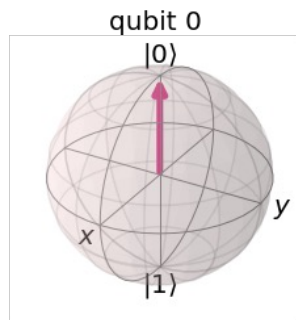
■ 量子回路と計算結果

- 量子ビットに量子回路を作用させることで、量子ビットに計算結果が乗っかる。
- その量子ビットの状態を観測する。
- ただし、量子ビットの状態は確率的に決まるため、何度も観測する。

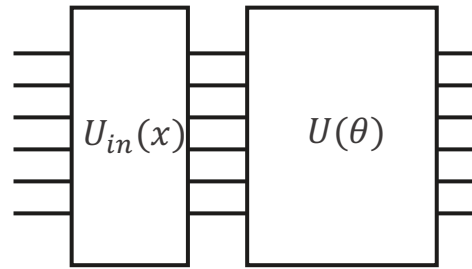


量子計算まとめ

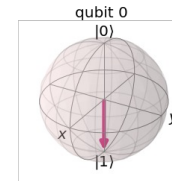
- 量子計算では、量子ビットの状態が現れる確率を観測し、その観測結果を計算結果とする。
- 観測結果に計算結果が現れるように量子回路をつくる。



量子ビット



量子回路



量子ビットの状態を観測

量子ビットが量子回路で状態が変わり、その状態を観測する。
観測結果に計算結果が乗っかる。

■ 量子アルゴリズム

- 量子計算を使い目的の計算を行う手順を量子アルゴリズムという.
- 歴史
- 1992年 Duetch Jozsaアルゴリズム
 - 量子並列化アルゴリズムの有効性を示す.
- 1994年 Shorアルゴリズム
 - 因数分解アルゴリズム, 古典暗号が実用的な時間で解ける可能性
- 1996年 Groverアルゴリズム
 - 探索問題を解くアルゴリズム

量子計算機

■ 量子計算機のきっかけ

1981年「量子のシミュレーションは指数関数的に計算コストが増えるから量子的なコンピュータのほうが良くない？」

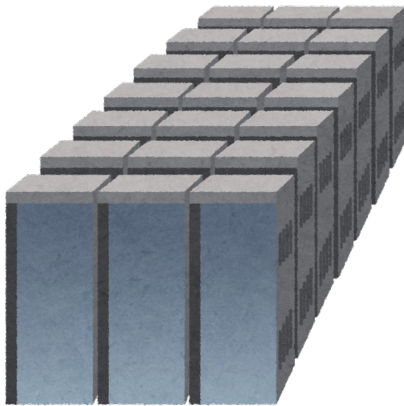


ボンゴで有名なFeynman

■ ビットと量子ビット

- 古典計算機ではビットを使い情報を表現する.
- 量子計算機では量子ビットを使い情報を表現する.

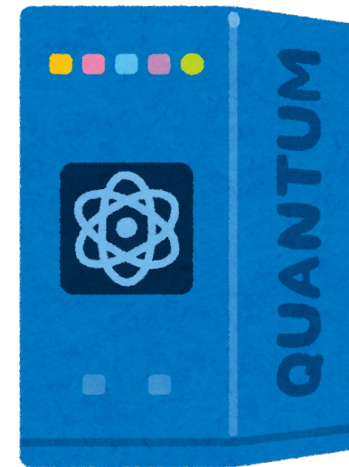
古典計算機



ビットは0か1の値

ビットの値は0か1のどちらかに決まっている.

量子計算機



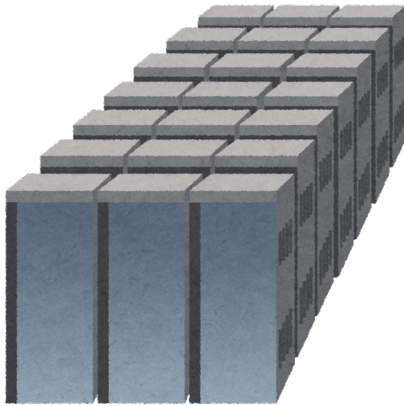
量子ビットは0か1の状態

量子ビットの状態は確率的に決まる.

■ 論理演算と量子計算

- 古典計算機では論理演算を用いる.
- 量子計算機では量子計算を用いる.

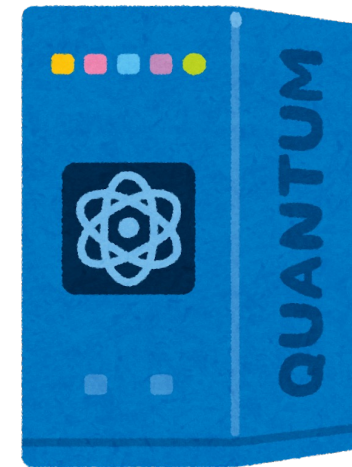
古典計算機



論理演算

かつ, または, など論理ゲートを用いる.

量子計算機



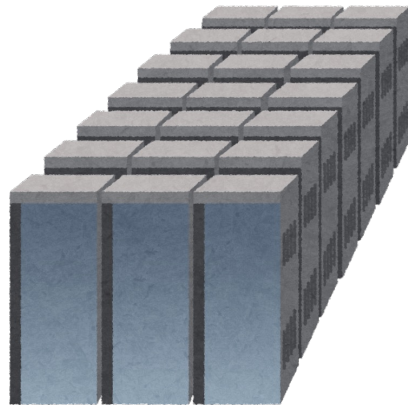
量子計算

量子ゲートを用いる.

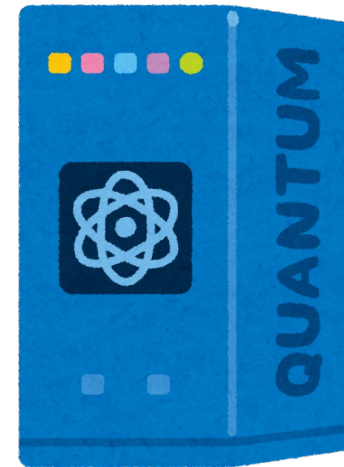
■ 量子計算機と古典計算機は同じ計算が出来る

- 量子計算機は万能計算機械であらゆる計算が出来る.
- 古典計算機も万能計算機械であらゆる計算が出来る.

古典計算機



量子計算機

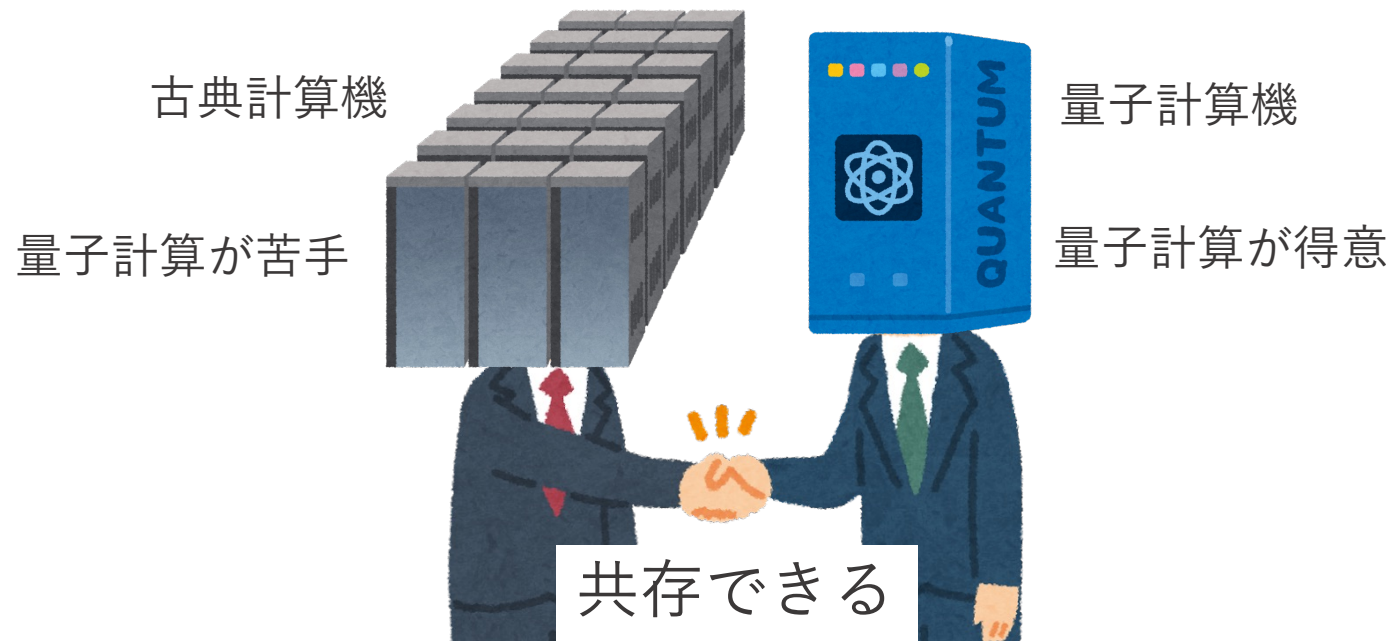


=

同じ計算が出来るという観点で言えば、古典計算機も量子計算機も同じである.

得意分野が違う

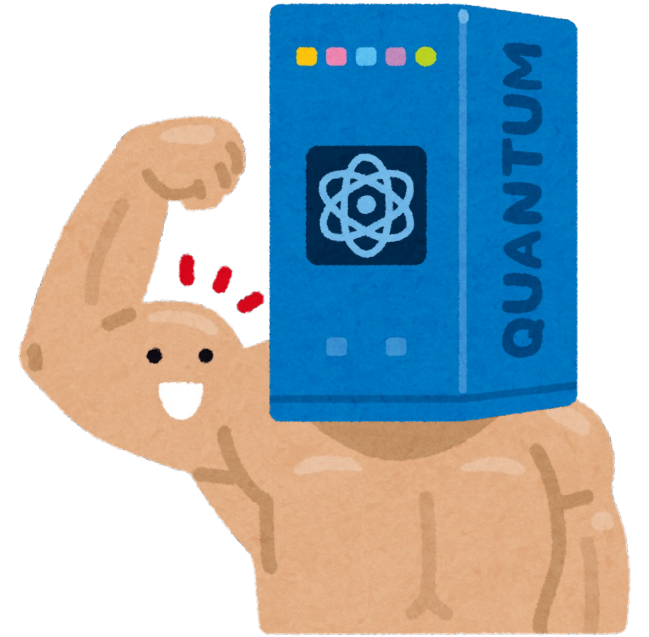
- 古典計算機で量子計算をすることは出来る。
 - しかし、必要とする計算資源が莫大で実行することが難しい。
- 量子計算機で古典計算機と同じ計算が出来る。
 - しかし、古典計算を速く計算できるわけではない。
- 量子計算機は量子計算が得意である。



■ 量子計算機の何が良い？

- 量子計算機は量子計算が得意である.
- 量子計算が有効な分野
 - 量子力学が関連する科学技術計算
 - 量子計算を活用したアルゴリズム
- 量子計算が有効なアルゴリズム
 - Shorのアルゴリズム（1994年）
 - 因数分解アルゴリズム，古典暗号が実用的な時間で解ける可能性
 - Groverアルゴリズム（1996年）
 - 探索，最適化に利用可能

量子計算機



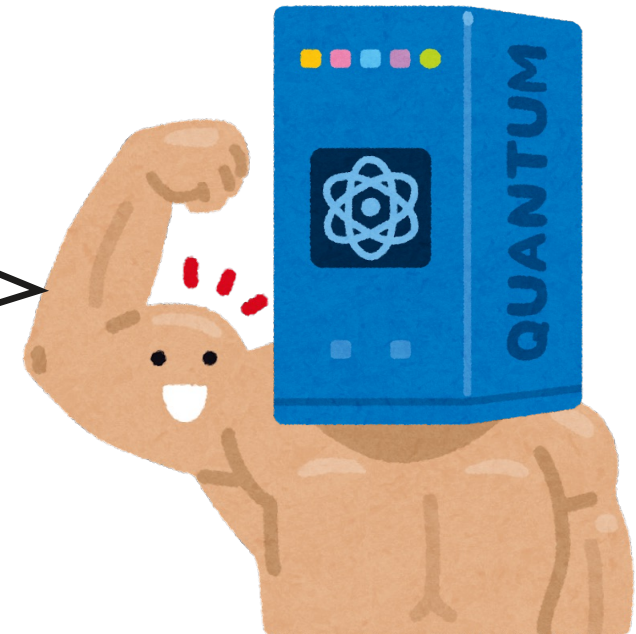
量子計算が得意

■ 量子計算機は速い？

- 量子計算機で速くなるアルゴリズムは限られる。
 - 例：Shorのアルゴリズム，Groverアルゴリズムなど
- 1990年代から量子アルゴリズムの開発が盛んに行われるようになったが，未だに古典アルゴリズムより有効なアルゴリズムは限られる。

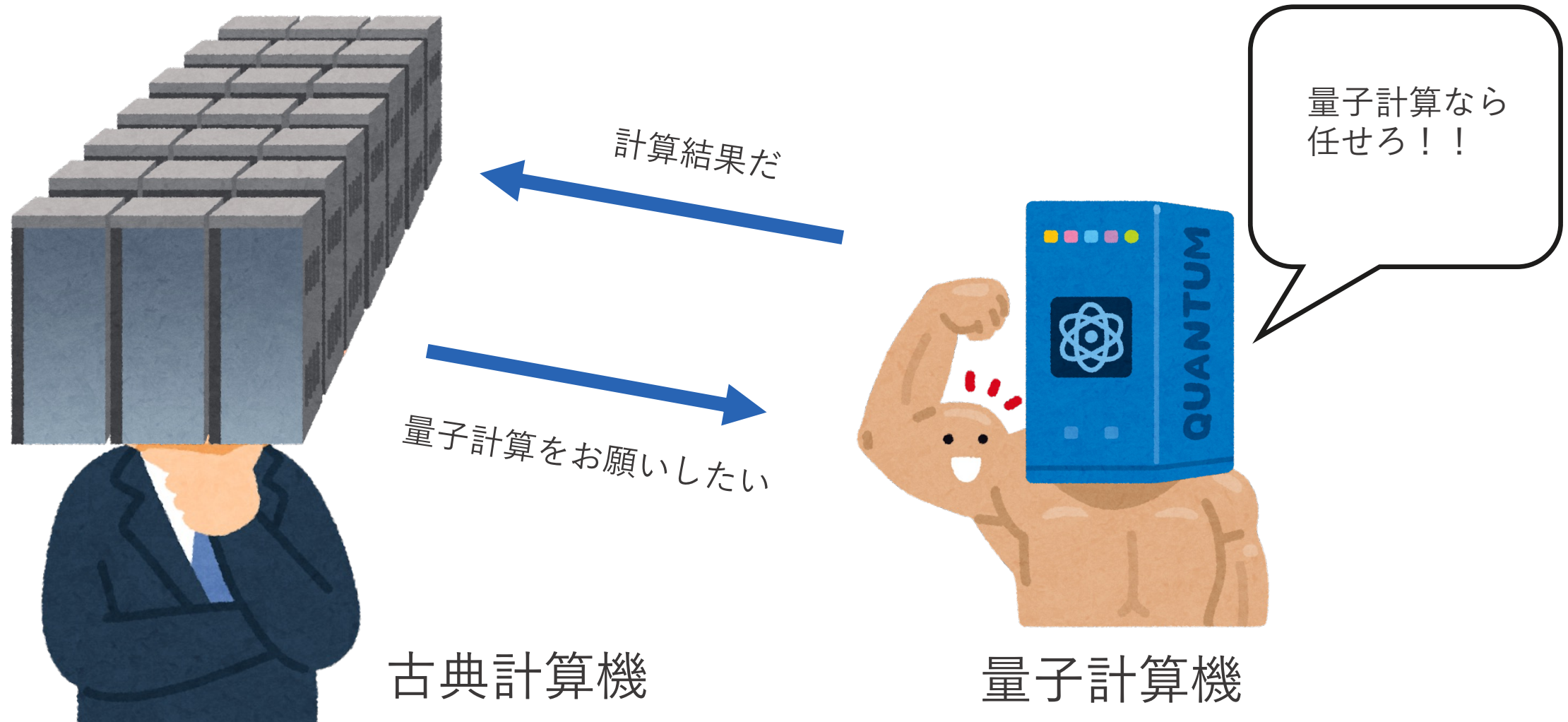
量子計算機

使えるアルゴリズムはないのか？



量子計算機の将来

量子計算機はGPUのように古典計算機に追加する計算ユニット（アクセラレータ）になるだろう。



■ 量子古典ハイブリッドアルゴリズム

- 量子計算のみ使うのではなく，古典計算も使うアルゴリズム.
- 代表的なアルゴリズム
 - 変分量子固有値ソルバ $\lambda_{min} = \langle \psi_{min} | H | \psi_{min} \rangle$.
 - 古典計算機で λ を最小になるように ψ を変更する.

量子計算機の進化 ビット数

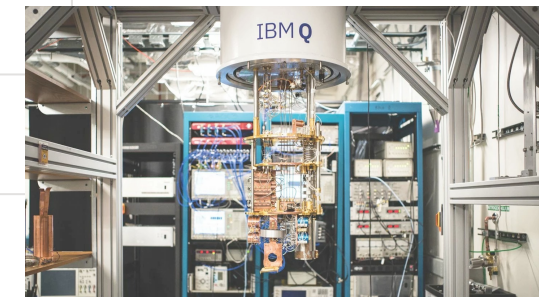
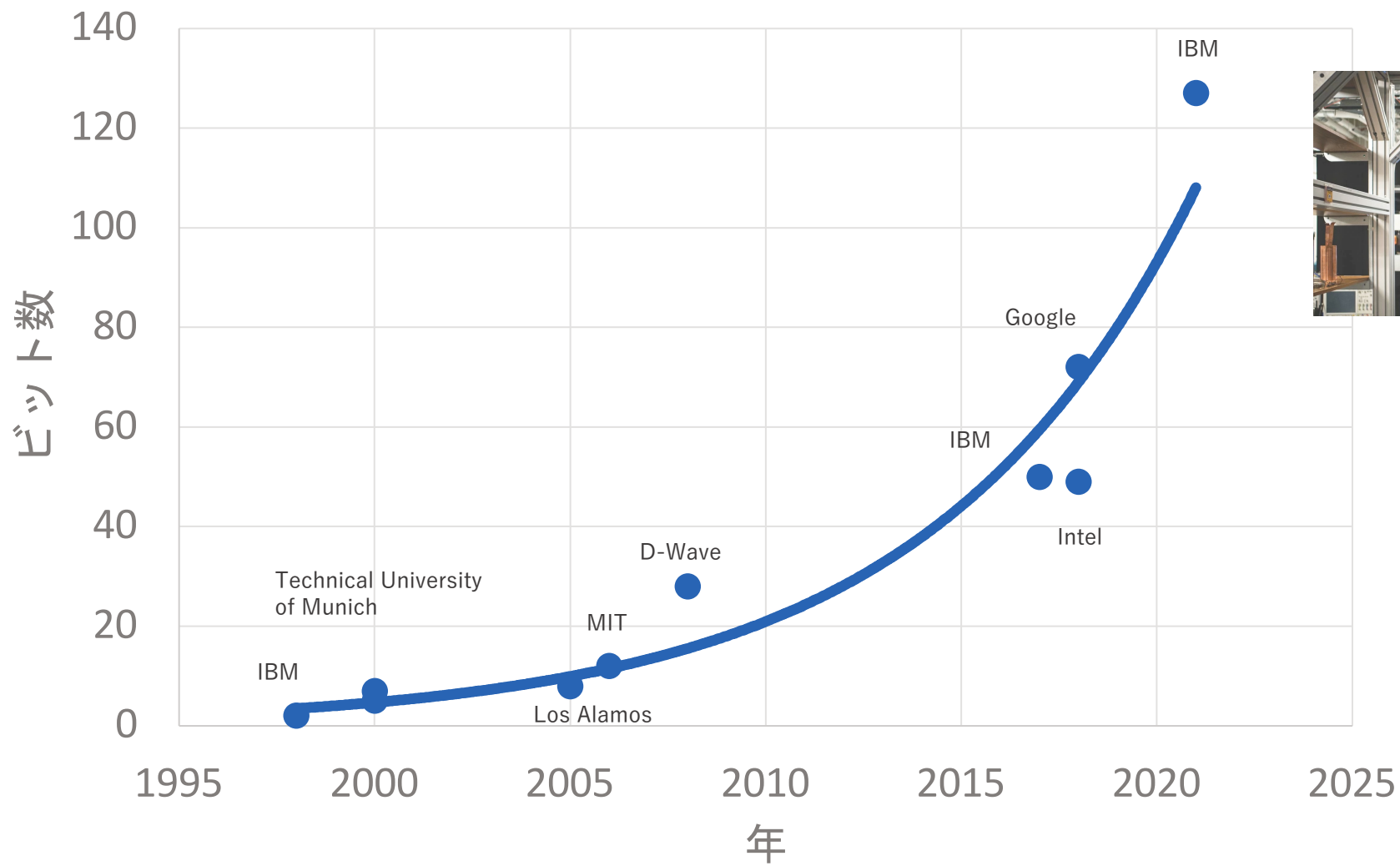
■ ビットの数

- 古典計算機では、1つの数を32個や64個のビットで表現している。
 - GPUで高速計算する場合、8個や16個のビットを使うこともある。
- もちろん、それらを複数保存しなければ計算できない。
 - パソコンのメモリ16GBは約 10^{11} 個のビットがある。
- 量子計算機も同じように多数のビット数を使いたいが、技術的に今のところ数十ビット程度しか実装できていない。

■ なぜ量子計算機の量子ビットを増やさねばならないか

- ビット数が増えないと実用的ではない.
 - 量子ビットが増えると表現力が増す.
 - 古典と同じ
 - 量子計算機はノイズに弱いため、誤り訂正のための量子ビットを搭載する必要がある.
 - 誤り訂正をしなければ動かないアルゴリズムがある.
- 技術競争のお陰でビット数が増えつつある.
 - ICのムーアの法則のようにビット数が増えていくかどうかは分からない.

量子計算機の量子ビット数の伸び



■ NISQの時代

- NISQとはNoisy Intermediate-Scale Quantum machineの略 (Preskill,2018)
- 現在作られる量子計算機は、そこそこの量子ビット数 (intermediate-scale) である.
 - 50から数100量子ビット (Preskill,2018)
- しかし、ノイズにまみれている (Noisy) .
 - 多くの量子アルゴリズムはノイズに弱い.
 - ノイズがあっても問題ないアルゴリズムのみ動かすことができる.

■ NISQを超える必要あり

- 量子計算機が実用的になるにはNISQを超える必要がある。
 - 量子計算はノイズに弱い.
- 誤り訂正あり量子計算機でなければ使えないアルゴリズムがある.
- しかし, 誤り訂正あり量子計算機に必要なビット数は多く, まだまだ登場しない.

■ 古典計算機を用いた量子計算シミュレーションには限界がある

- 量子計算機を古典計算機でシミュレートすることができる.
- 古典計算機で量子計算をしても良い.
- しかし、量子計算をするには莫大なメモリが必要である.
古典計算機でビットの状態を表すために必要なメモリの
ビット数（データ量）

	1ビットの状態	50ビットの状態
古典ビット	1ビット	50ビット
量子ビット	128ビット	約144ペタビット (約18ペタバイト)

と言われていたが、テンソルネットワークを使えば少なくとも数百ビットまでやれるらしい (Darmawan and Poulin, 2022). 2021年清華大学がテンソルネットワークを用いてスパコンで量子回路をシミュレーションし、Googleの量子計算機の計算時間に近い値を出した.

■ 詳細：古典計算機を用いた量子計算シミュレーションには限界がある

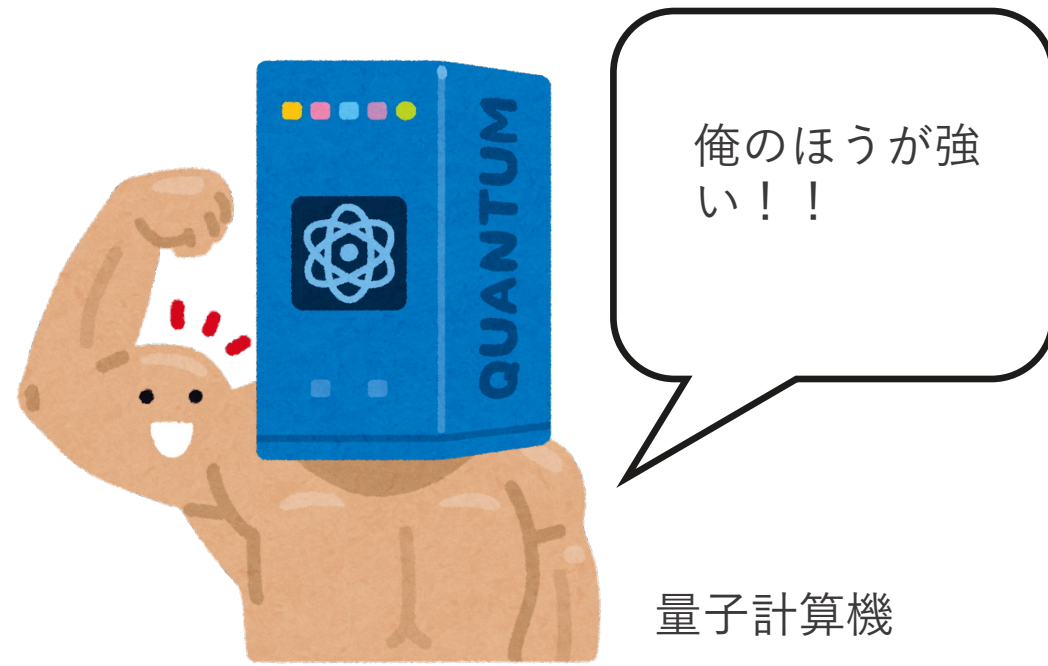
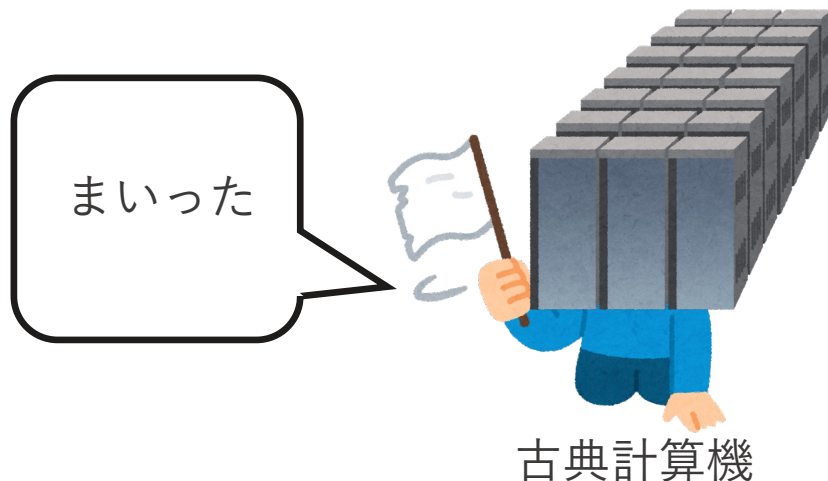
- 量子ビットは情報を0と1で表現している点で古典と同じではある。
- しかし、量子ビットの状態は複素ベクトルで表現される。
- 1つの量子ビットの状態は2つの倍精度浮動小数点数で表せるとすると、1量子ビットは128ビット（16バイト）必要である。
- 例えば、50量子ビットある量子計算機を古典計算機でシミュレーションするとする。
 - 量子ビットが50個あるので、その状態の組み合わせは 2^{50} 個ある。
 - 1つの状態に対し、複素数（浮動小数点数2個）を割り当てる必要がある。
 - 1量子ビット16バイトなので、50量子ビットを表すには約18ペタバイト必要である。
- つまり、小規模な量子計算機を古典計算機でシミュレーションすることすら難しい。
- と思われていたがテンソルネットワークでできるそうだ。

量子計算機の進化

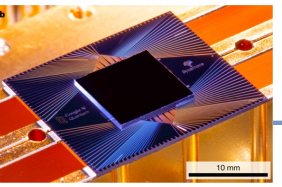
量子超越

量子超越性

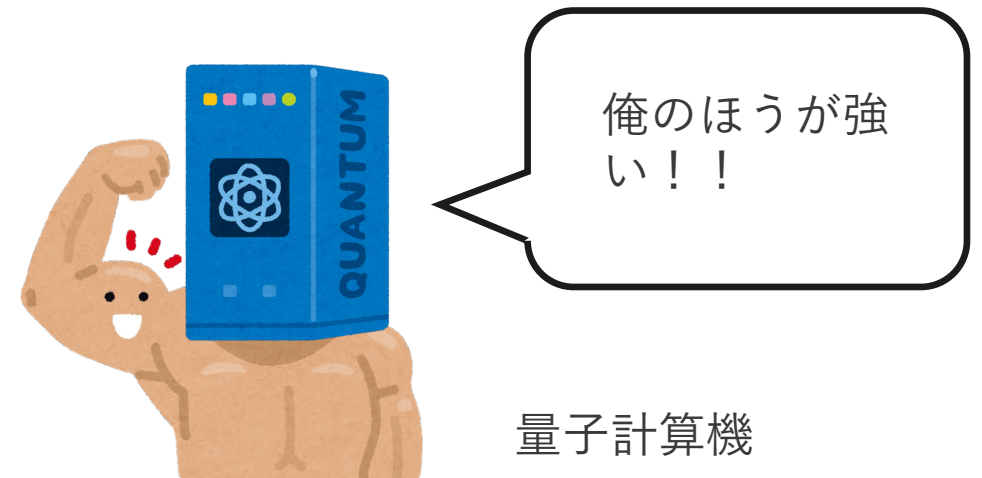
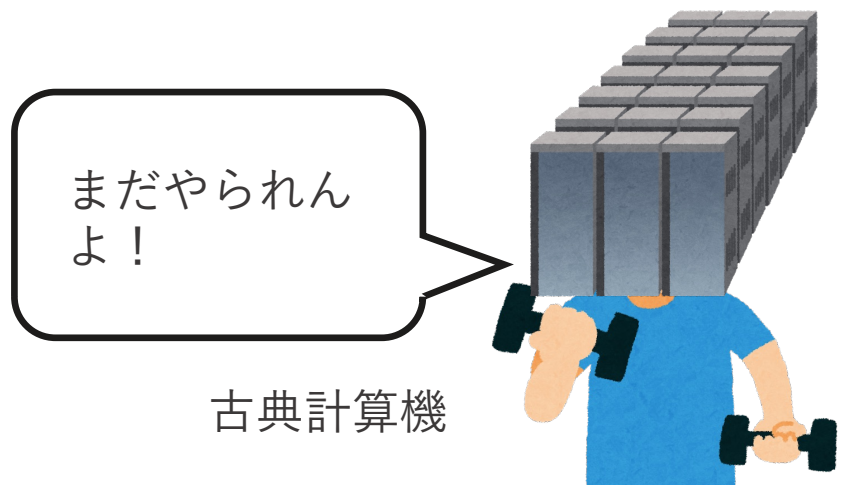
- プログラム可能な量子デバイスが、どのような古典コンピュータでも実用的な時間では解決できない問題を解決できることを（問題の有用性に関係なく）証明することである（wikipedia）
- 量子計算機が古典計算機より速いことを確認できれば、量子計算機が量子超越したと言える。



量子超越の話題



- 2019年 Googleが53量子ビットの量子計算機を開発し、量子超越した（スパコンより速い）と報告。
- 2021年 清華大学がGoogleと同じタスクをスーパーコンピュータで300秒で行い量子超越を否定。2021年ゴードン・ベル賞
- 2022年量子計算機が量子超越してるかどうかは分からない。
 - 古典計算機も古典アルゴリズムも進化し続けている。



開発環境

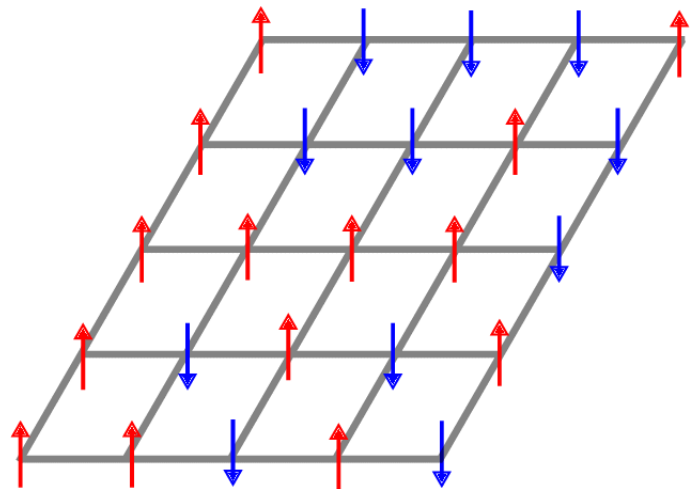
■ 開発環境

- 近年量子計算のライブラリが開発が盛んになり、様々な量子計算ライブラリが無料で公開されている.
- 量子計算ライブラリを使うことで、簡単に量子計算を使うことができる.
 - アルゴリズムの開発が容易になる.
- ライブラリ, 開発環境
 - Qiskit(IBM)
 - Cirq(Google)
 - Blueqat(blueqat)
 - Q#(Microsoft)

量子アニーリング

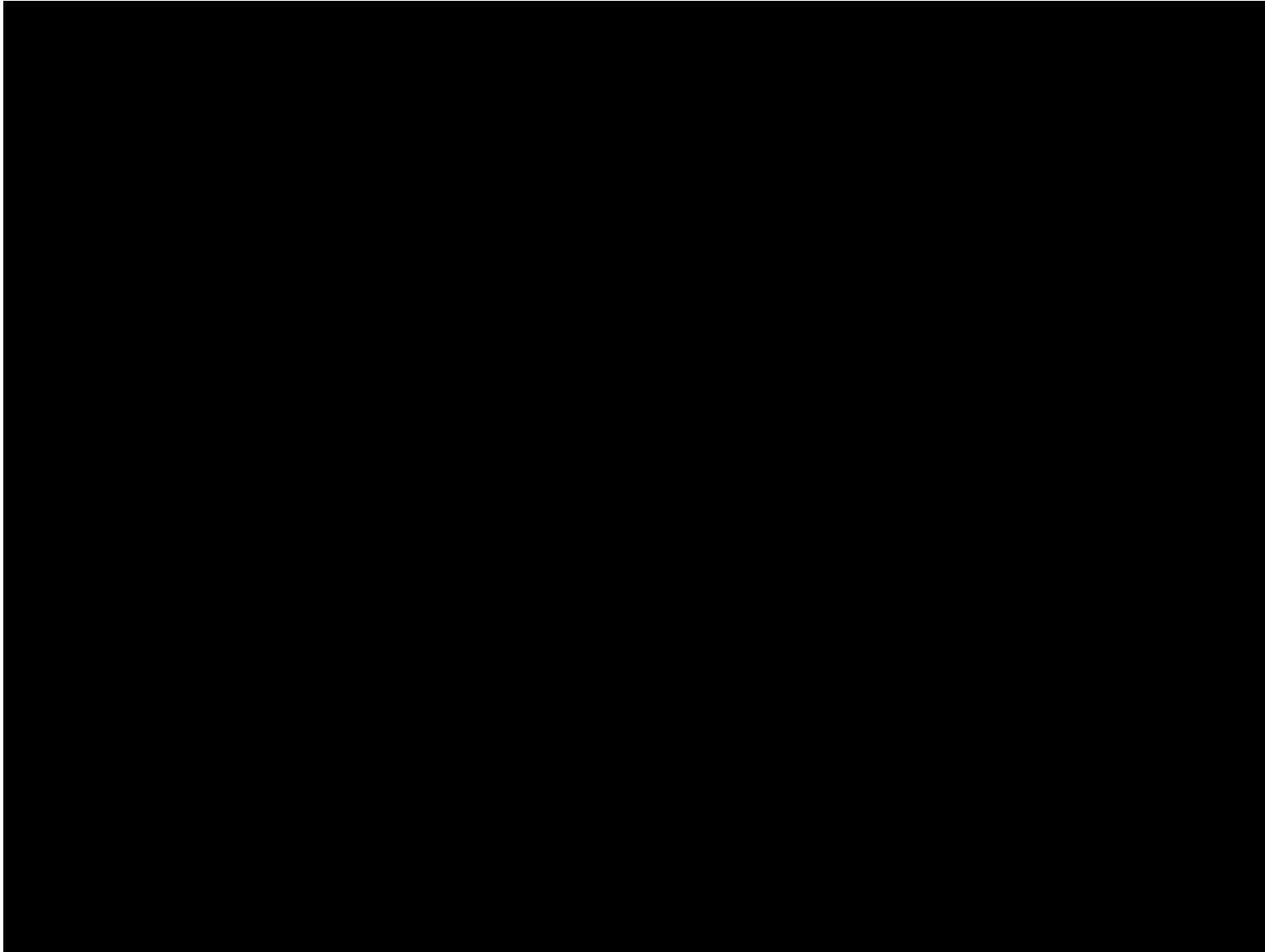
■ 量子アニーリング

- 量子ビットを使ったイジングモデル
- 量子アニーリング（量子焼きなまし法）により最適解を求める。



イジングモデル

- 格子の頂点は向きを持っている。
 - 向きは確率的に決まる。
 - 頂点は相互作用している。
 - 隣の向きに合わせようとする。
 - 頂点の向きの模様が答えになる。
-
- 磁石のモデルによく使われる。
 - ある種の最適化問題に対しヒューリックな（それっぽい）解を出せる。



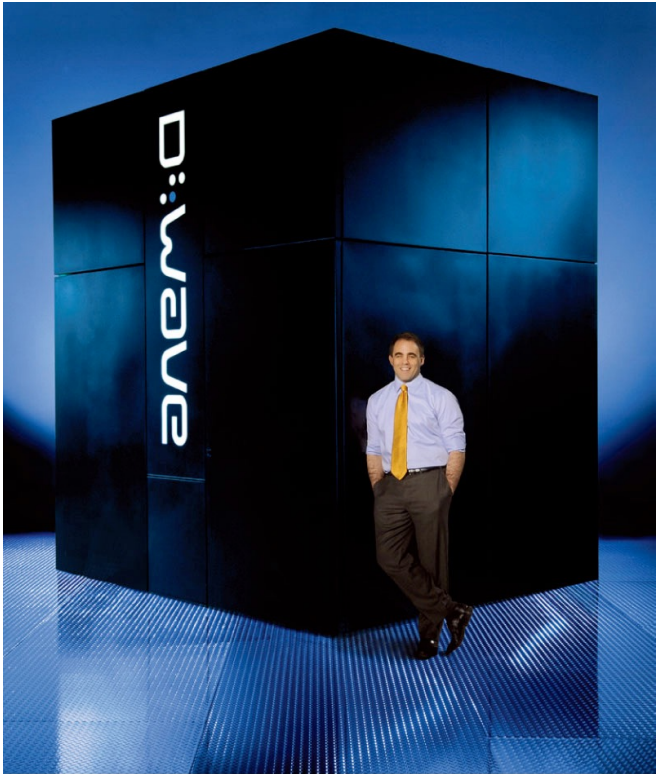
<https://www.youtube.com/watch?v=PWUTBnvGegg>

量子アニーリングの歴史

- 1998年 Kadowaki and Nisimoriが量子アニーリングを発表
- 2010年 D-wave one 発表（量子アニーラ）
- 日本は量子じゃないアニーラで参入

開発元	D-Wave Systems	富士通	日立製作所		東芝	NEC	
マシン名	Advantage	デジタルアニーラ (DA)	CMOSアニーリング (CA)		シミュレーテッド分岐マシン (SBM)	なし	超電導量子アニーリングマシン
プロセッサー	専用IC	専用IC+汎用機	専用IC、FPGA	GPU	FPGA、GPU	汎用ベクトルプロセッサー	専用IC（開発中）
求解方式	QA	一部並列化したSA	SA	MA	SB	独自SA*2	QA
最大ビット数	約5000 (ハイブリッドモードでは100万)	8192 (ハイブリッドモードでは約100万*1)	14.4万	10万	100万以上	10万*3	4
パラメーターの階調	アナログ (5ビット程度)	64ビット	3ビット		2～32ビット	未公表	未定
スピン間結合	疎結合 (キメラ、ヘガサス)	全結合 (100万ビットの場合を含む)	疎結合 (キング)	全結合	全結合	全結合	疎結合 (埋め込みで全結合化)

(<https://xtech.nikkei.com/atcl/nxt/column/18/01755/00002/>)



<https://www.natureasia.com/ja-jp/ndigest/v8/n9/%E9%87%8F%E5%AD%90%E3%82%B3%E3%83%B3%E3%83%94%E3%83%A5%E3%83%BC%E3%82%BF%E3%83%BC%E3%81%AB%E3%80%81%E6%9C%80%E5%88%9D%E3%81%AE%E8%B2%B7%E3%81%84%E6%89%8B%E3%81%8C%E3%81%A4%E3%81%84%E3%81%9F/36604>

■ 量子アニーラに対する注意

- 量子アニーラはいわゆる計算機ではない.
 - 量子アニーラはイジングモデル実行マシン.
- 古典より速いかどうか分からない.
- イジングモデルで解けないものは解けない.
- 厳密解を求める方法ではない.
 - アニーリングはヒューリスティクス.
- 勉強課題としては良い.
 - 使われている知識は比較的汎用的（量子計算機はそれに特化した知識が必要）
 - 量子力学に興味があれば挑戦しても良いのでは.

まとめ

■ 量子と古典まとめ

- 量子を使うもの以外は古典という。
- 量子計算機は古典計算機と同じ計算ができる。
 - だからといって、古典で動くプログラムが簡単に動くわけではないし、それを目指していない。
- 量子計算機で古典アルゴリズムを動かしても意味がない。
 - 量子計算の特性を生かした量子アルゴリズムを考える必要がある。
- **量子計算機がスーパーコンピュータに取って代わることはない。**
 - スーパーコンピュータの価値は失われないし、これからも開発される。
- 量子計算は古典計算機でも出来る。
 - 古典計算機で動かすには限界がある。

量子計算：量子の性質を使った計算

量子計算機：量子計算で使う量子ビットと量子ゲートを物理的に実装した計算機

量子計算 ≠ 量子計算機

■ 現状まとめ

- 量子計算機の研究は日々進んでいる.
- しかし現状の量子計算機はノイズありで中規模のサイズ
 - ノイズありだと使えないアルゴリズムがある.
 - 誤り訂正あり量子計算機が必要だが, 実現は当分先.
- 量子計算の開発ライブラリが充実している.
 - ライブラリは無料で誰でも使えるので, 誰でも簡単に量子計算を使うことができる.

出席確認