量子計算と物理

森前智行
京都大学基礎物理学研究所

内容（５０分）

- 量子論とは（１０分）
- 量子計算の基礎（１５分）
- 量子スプレマシー（１０分）
- 量子暗号：セキュアクラウド量子計算（１５分）

量子論とは

量子論とは

古典力学

1687：ニュートン　力学

1873：マックスウェル　電磁気学

車、ロボット、ロケットなど「マクロ」な世界を記述できる

1900～：原子や分子などのミクロ世界が、古典論ではうまく説明できないことが発覚。。。

量子力学

1925：ハイゼンベルク　行列力学

1926：シュレディンガー　波動力学

原子、分子、光、電子等ミクロな世界の説明にことごとく成功

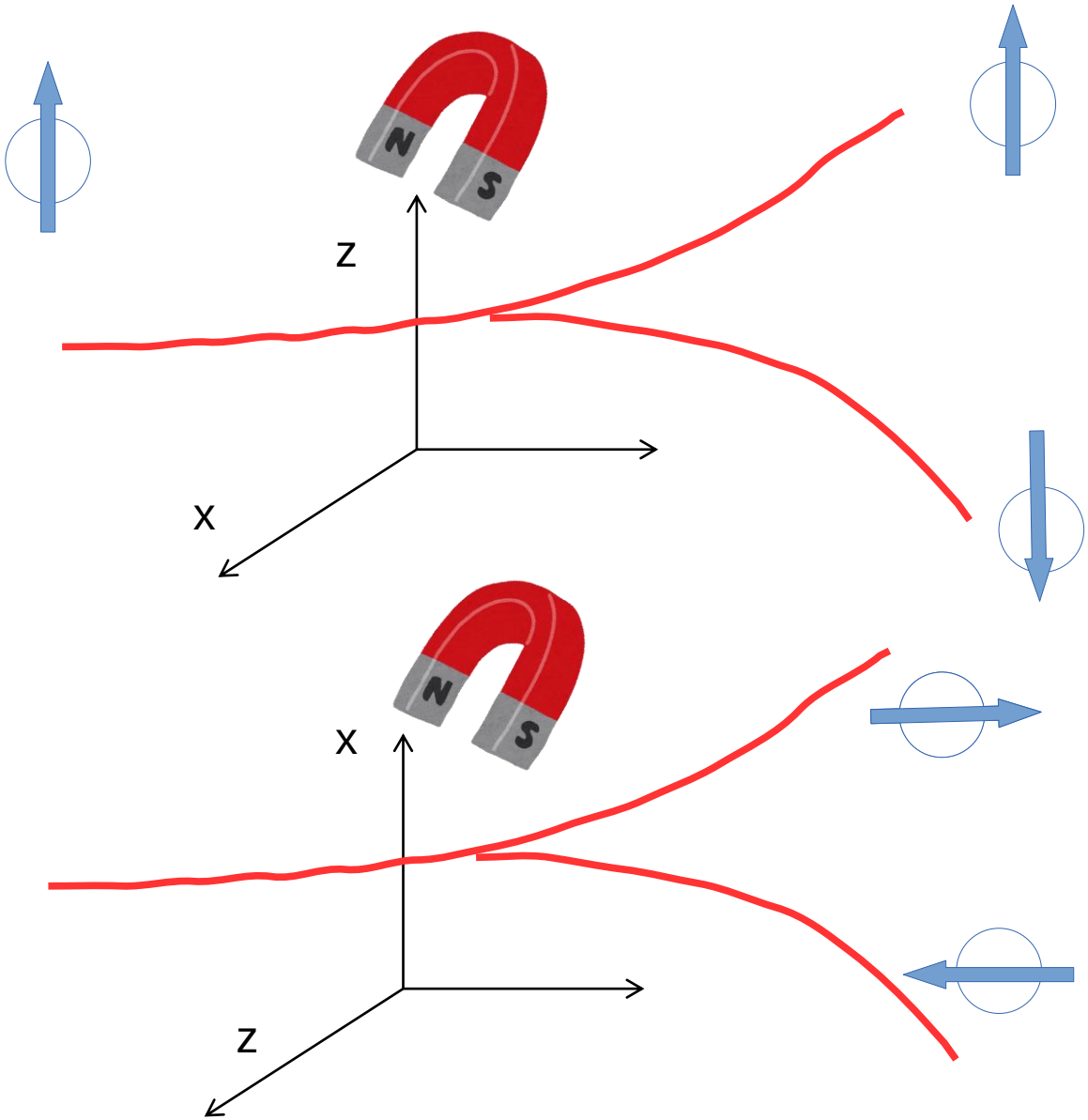
1982：ファインマン　量子コンピュータを提案
（1983年ファミコン販売）

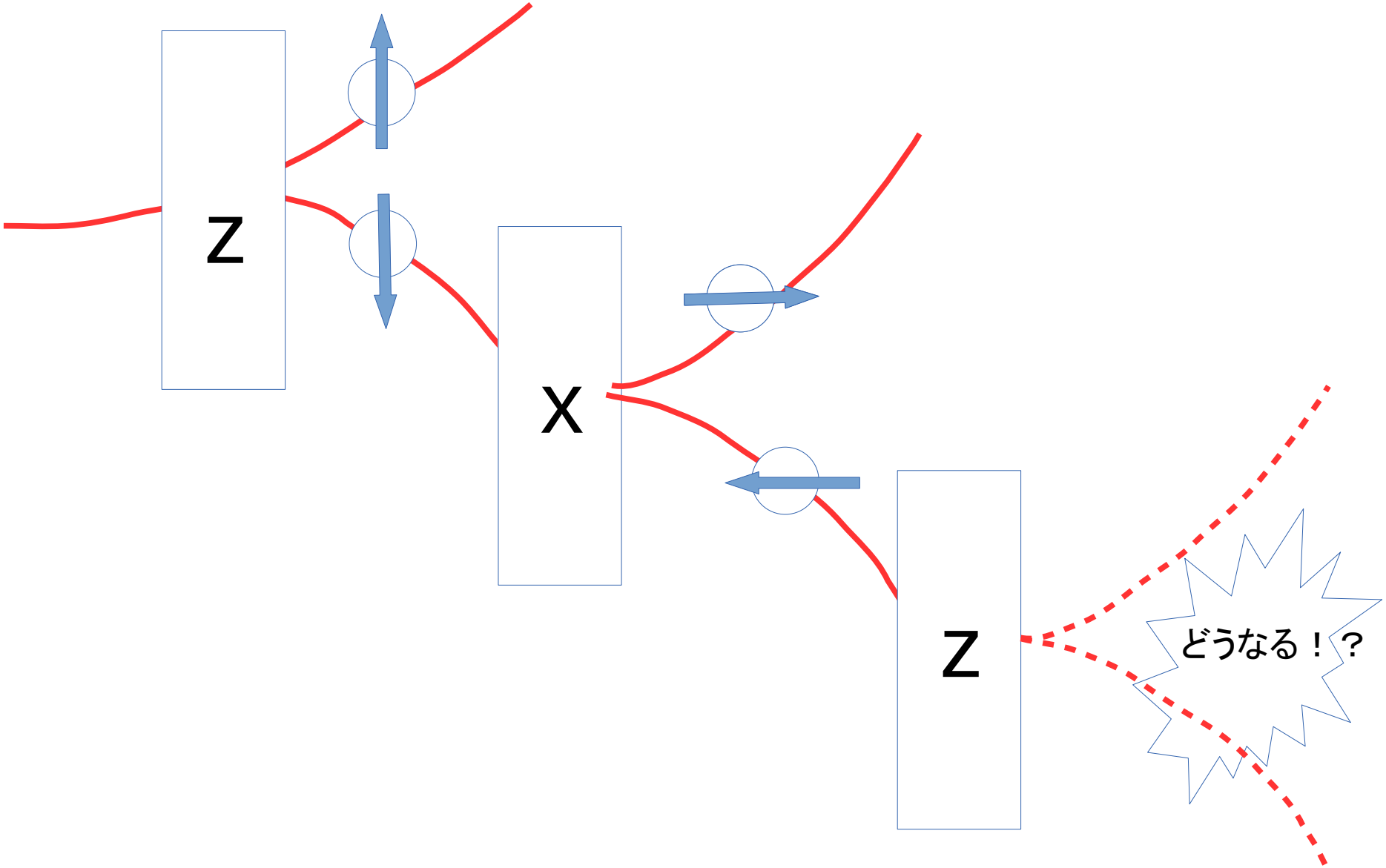
2019：Googleが量子スプレマシー？

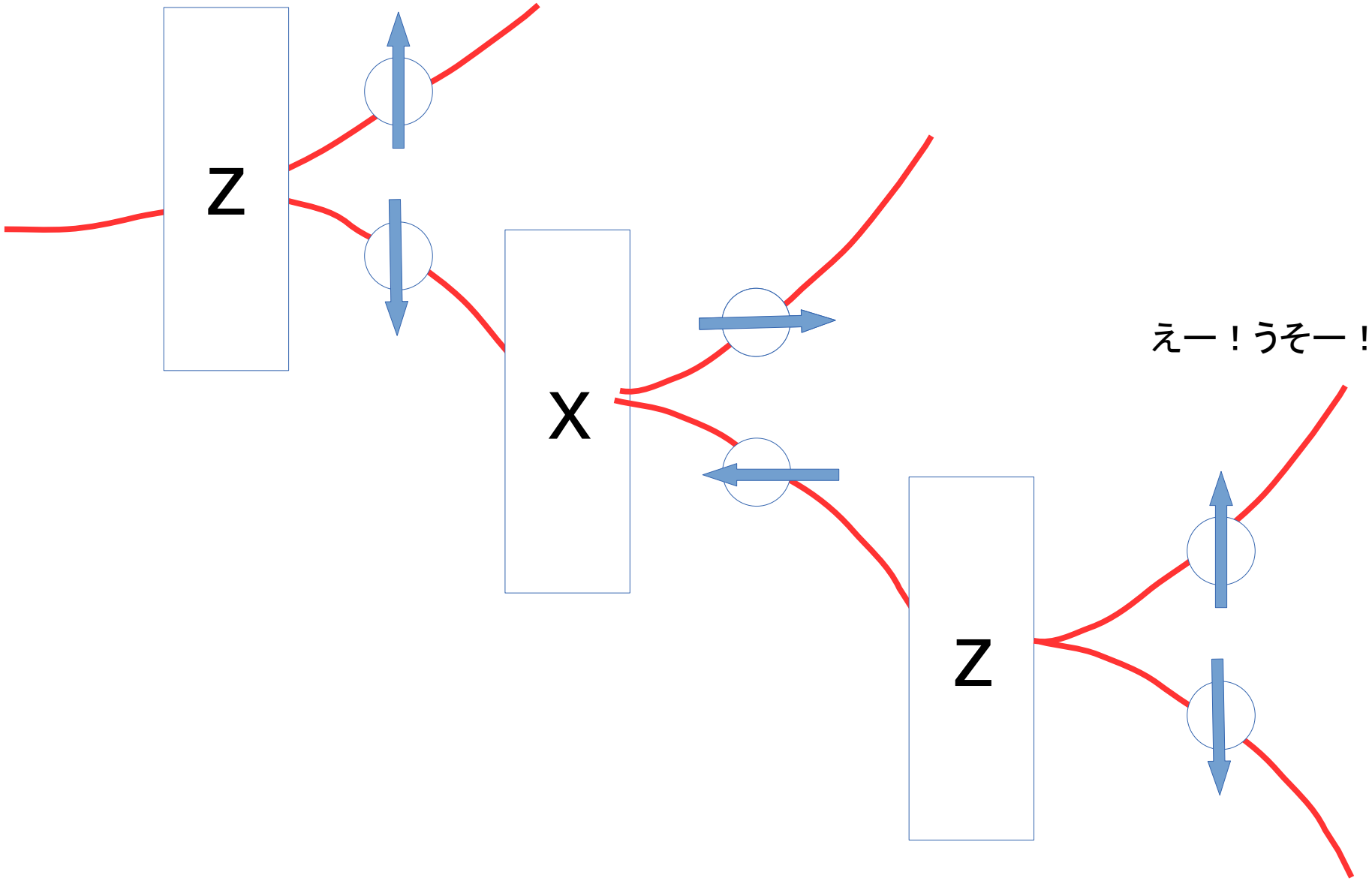
計算機というのは面白い物理系

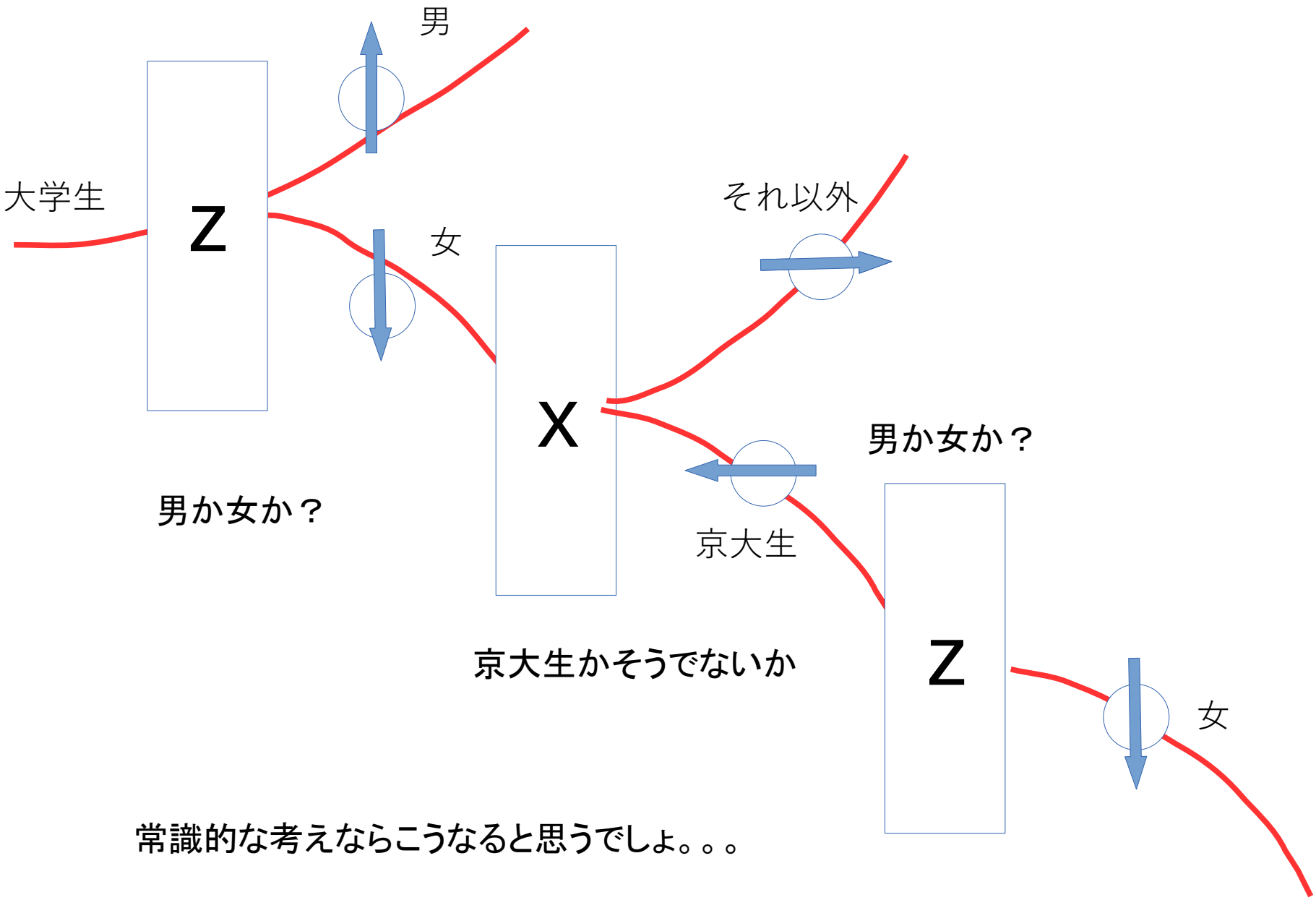
（シュテルンゲルラッハの実験：学部の量子力学で習う）

スピン：小さな磁石

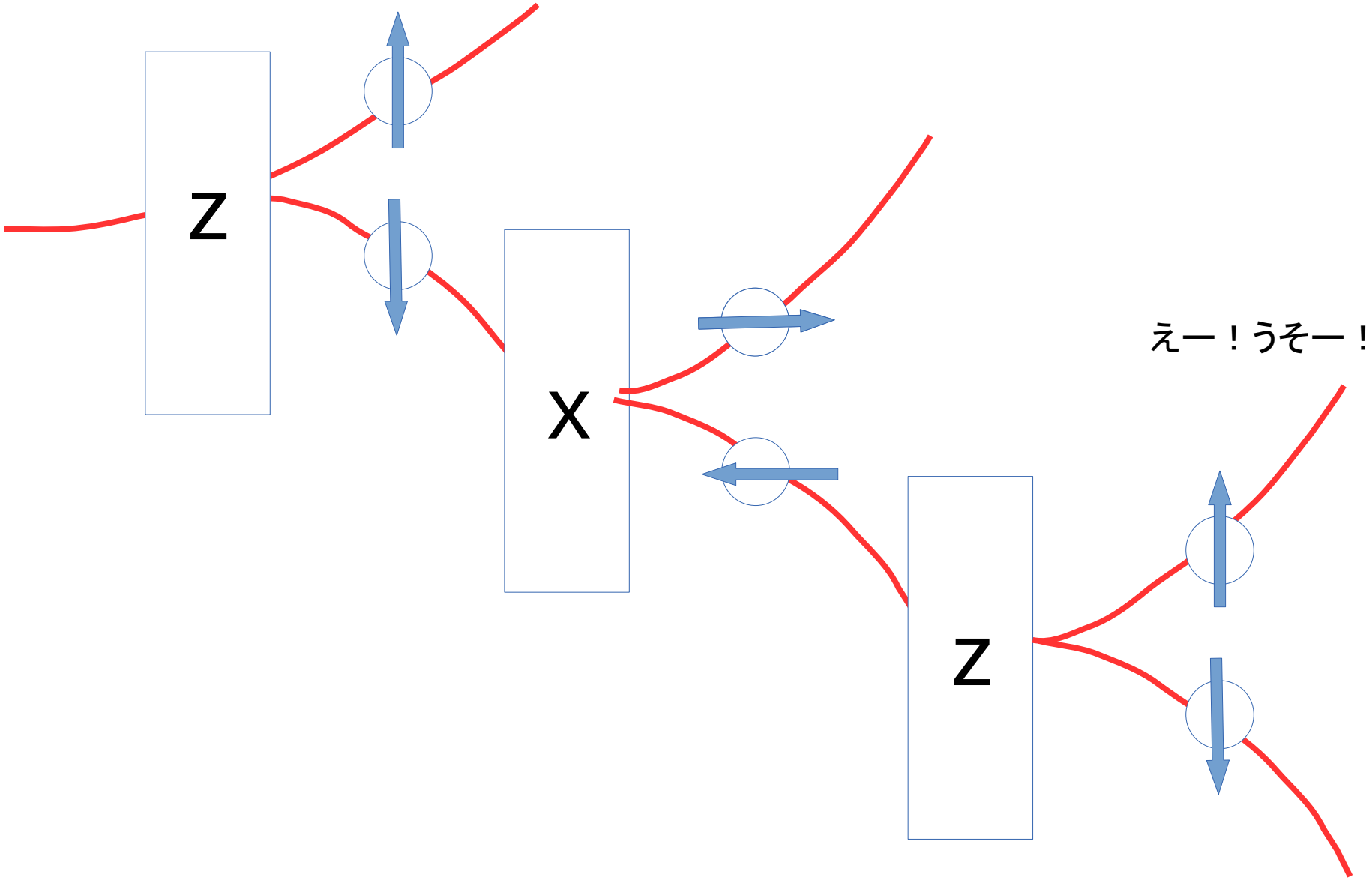



Z
X
Z
どうなる！？


Z
X
Z
えー！うそー！



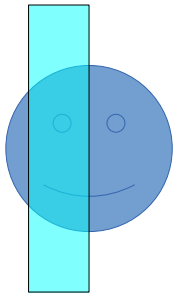
常識的な考えならこうなると思うでしょ。。。


Z
X
Z
えー！うそー！

他にも不思議な現象がいっぱい

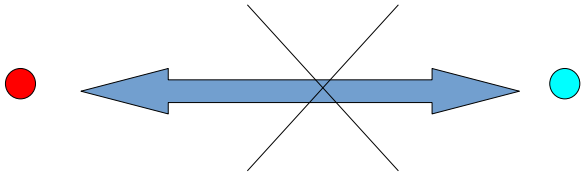
・量子的重ね合わせ

・トンネル効果



壁をとおりぬける！

・複製不可能性（No-cloning theorem）



量子マネーへの応用

そんな変な理論なんて間違っているのでは？

無数の実験的、理論的研究がこれまで行われてきているが、すべて量子論と矛盾しない。

→量子論は正しいと信じられている

例：地球はまるい

我々の常識：マクロ世界に基づいている
→ミクロ世界はマクロ世界と違っていた、というだけのこと

量子論基礎：量子論について研究する学問

量子論は本当に正しいのか？
量子論をちょっと拡張した理論を考えてみよう（一般化確率論）
なぜ量子論がこうなっているのか理解・説明しよう

じゃあ、量子論はどういう理論？

日常言語では説明できません。線形代数の知識が必要

状態：ベクトル
状態の時間発展：ユニタリ行列の作用
物理量：エルミート行列

線形代数の知識が必要。。。（大学1年教養レベル）

難しい数学を使わないで量子論を説明できないの？

→無理。日常言語はマクロ世界にもとづいて作られている。
そもそもそれで説明できないから量子論が生まれた

By definitionで量子論は日常言語で説明不可能

量子計算の基礎

量子コンピューター検定：以下の文は正しいか間違っているか？

（１）量子コンピューターには２種類ある。一つはゲート型であり汎用。もう一つはアニーリング型で組み合わせ最適化に特化。

（２）古典計算の場合、指数爆発する組み合わせの中から解を探すには、しらみつぶしにやらないといけないので指数時間かかる。一方で量子の場合、重ね合わせを使って一発で解けるため、配送、創薬、金融、スケジューリング、自動運転といった実社会の様々な場面で役に立つ。

（３）みんななかなか実現できなくて苦労しているところ、海外のベンチャーがいち早く商用化し、世界を騒がせた。

（４）そのマシンは古典計算機より１０億倍高速であるというGoogleチームの報告が世界に衝撃を与えた。

（５）量子コンピューターは日本人がアイデアを生み出したにも関わらず海外に先に実用化されてこれだから日本の科学政策はけしからん。

（６）しかしながら、最近では国産マシンも実用化され、しかも電機メーカーも「量子コンピューターの原理を利用した量子コンピューターより高速な古典マシン」を開発し、オールジャパンのまきかえしが起こっている。

量子コンピューター検定：以下の文は正しいか間違っているか？

（１）量子コンピューターには２種類ある。一つはゲート型であり汎用。もう一つはアニーリング型で組み合わせ最適化に特化。

（２）古典計算の場合、指数爆発する組み合わせの中から解を探すには、しらみつぶしにやらないといけないので指数時間かかる。一方で量子の場合、重ね合わせを使って一発で解けるため、配送、創薬、金融、スケジューリング、自動運転といった実社会の様々な場面で役に立つ。

（３）みんななかなか実現できなくて苦労しているところ、海外のベンチャーがいち早く商用化し、世界を騒がせた。

（４）そのマシンは古典計算機より１０億倍高速であるというGoogleチームの報告が世界に衝撃を与えた。

（５）量子コンピューターは日本人がアイデアを生み出したにも関わらず海外に先に実用化されてこれだから日本の科学政策はけしからん。

（６）しかしながら、最近では国産マシンも実用化され、しかも電機メーカーも「量子コンピューターの原理を利用した量子コンピューターより高速な古典マシン」を開発し、オールジャパンのまきかえしが起こっている。

量子計算の基礎

古典計算機：古典論に基づく計算機。要するに今我々が使っているもの。

量子計算機：量子論の不思議な現象をうまく使って古典計算より高性能な計算を行うコンピューターのこと

高性能の意味

古典計算より高速
古典計算より省メモリ
古典計算より安全
古典計算にない機能がつく

量子ビット

量子ビット：０と１の量子的重ね合わせ

→確率1/2 で０と１が出るという意味ではない！！！

量子的重ね合わせ　|0> と |1> の線形結合

→どういう意味？それ以上は説明不可。

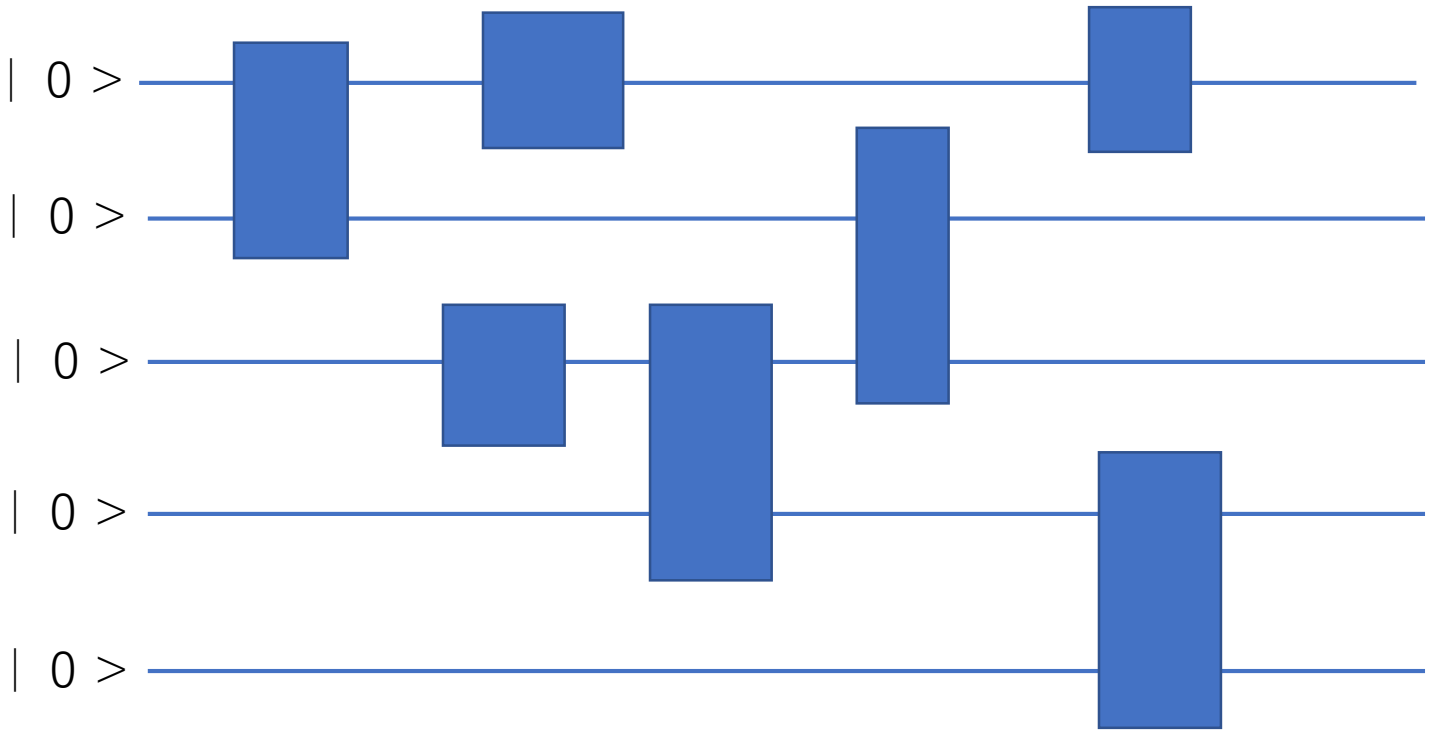
量子計算機ではこのような状態を作ることができる

$$\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

ルート２分の１の確率？？
負の確率？？

日常言語では説明不可能。

量子回路、量子ゲート



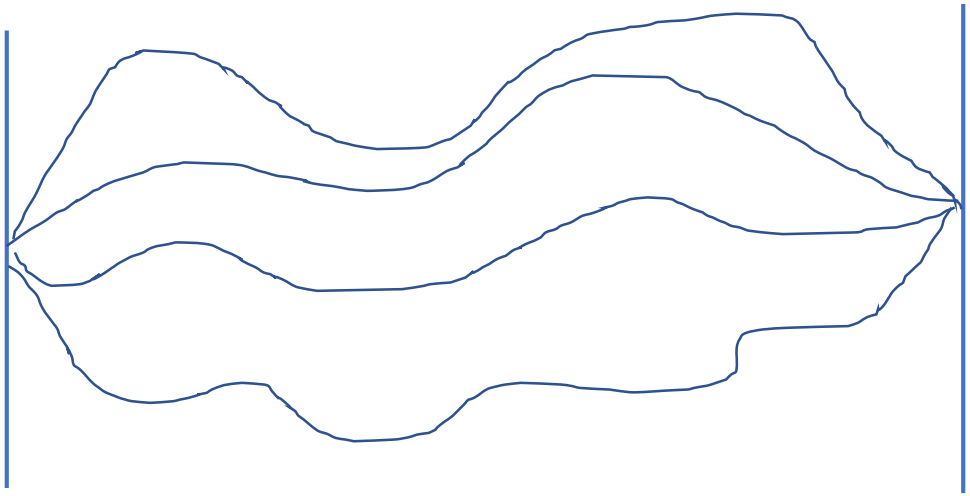
最後に測定する。

１量子ビットゲート：１つの量子ビットを回す
２量子ビットゲート：２つの量子ビットの間にエンタングルメントをつくる

時間さえかければ古典でも代用可

量子計算機はすごいといっても、なんでもできるわけではない。

量子計算機は、指数時間かけてよいなら古典計算機でシミレート可能。



経路積分：各パスの計算は多項式時間で可能。パスの数が指数個あるからそれを足すのに指数時間必要。

高速な量子アルゴリズムの例

（１）Shorの素因数分解アルゴリズム（１９９４）

素因数分解を高速に行うことができる　→　今の公開鍵暗号が危険に

（２）Groverの検索アルゴリズム（１９９６）

データーベースの検索が高速に（ただし指数）できる

Quantum algorithm zooというウェブページに量子アルゴリズムの一覧がある

高速かつ役に立つ量子アルゴリズムを見つけるのはものすごく難しい。

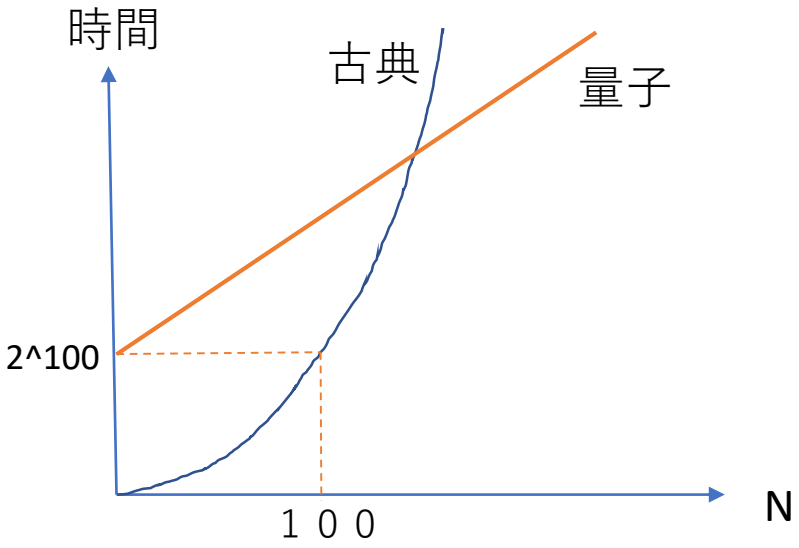
→量子計算機用に焼き直しただけでは量子アルゴリズムと呼ばない（古典より速いことのなんらかの証明が必要）

量子ソフトウェア（笑）、量子キラーアプリ（笑）

量子計算が速いの意味

漸近的な意味であることに注意！

例：
古典計算だと2^N時間かかる
量子計算だとN+2^100時間で解ける



100量子ビット以下だと古典のほうが速い

→量子が古典に負けていることを意味しない！

十分大きな量子ビットでは量子が勝つようになる

チャーチチューリングのテーゼ

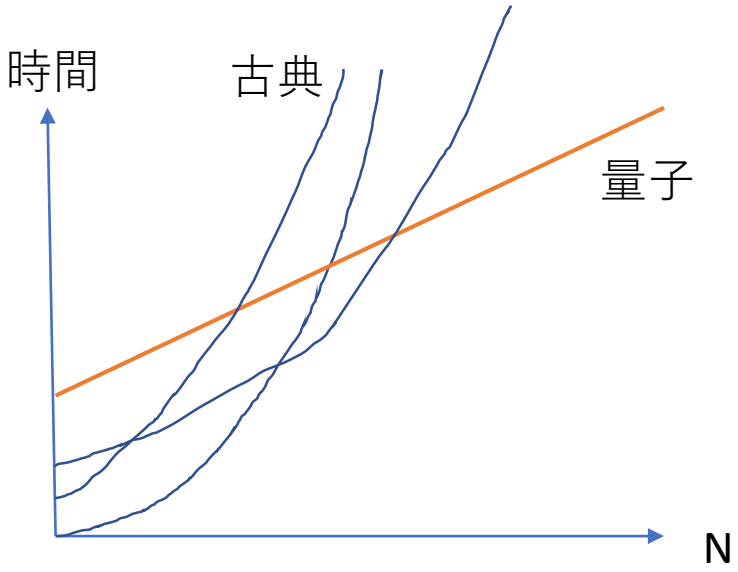
どんな古典計算機も漸近的には同じ速度

→メーカー等が出しているいろいろな「量子コンピューターの原理にインスパイアーされて作った量子コンピューターより速い古典マシン」はあくまで古典マシンなのですべて漸近的には普通の古典計算機と等価。

→今後どんな古典マシンがでてきてもそれは漸近的には全て等価。

量子計算機はその全ての古典計算機
に漸近的に勝つことが理論的に示されている

（注意：ゲート型の話。量子アニーリング
はそうなっているかどうか不明。）



つまり、実測値でみるのか漸近でみるのかを区別しないといけない

意味があるのは

（１）量子的性質を使うことにより全ての古典マシンより漸近的に速いことが理論的に示されている

→ゲート型はこれ。

（２）量子か古典かとか高速証明とかおいといて、なぜかわからないけど使ってみるととにかくやたら実測値で爆速

→それはそれであり。ただし、（２）が達成できていないから（１）であるかのように錯覚させてごまかすのは詐欺。

なぜ量子計算機は速いの？

答え：負の「確率」のおかげ

$$\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

負の確率以外古典計算機と同じなので。

古典計算機：マルコフ連鎖
量子計算機：負の確率を使ったマルコフ連鎖

ただし、「じゃあ負の確率をどう使って高速化を実現しているの？」と聞かれたら、答えは「まだわかりません」。

→現在研究中の最先端の研究テーマ

量子計算機は常に古典より高速というわけではない

量子計算機は古典計算機の上位互換なので
（1）量子計算機＞古典計算機
（2）量子計算機＝古典計算機
のどちらか

（1）の場合、（2）の場合ともに事例が知られている。

どういう時に（1）になり、どういう時に（2）になるのかという一般的な理解はまだ全然できていない
→まさに最先端の研究テーマ

量子性があるなら速いとは限らない

計算機が量子系なら常に自動的に速くなるというわけではない。

例：クリフォード回路

→エンタングル状態を作るけど、古典でシミレート可能

「量子性がでている」だけでは駄目で、「量子性が高速化にきいている」ことを示さないといけない！

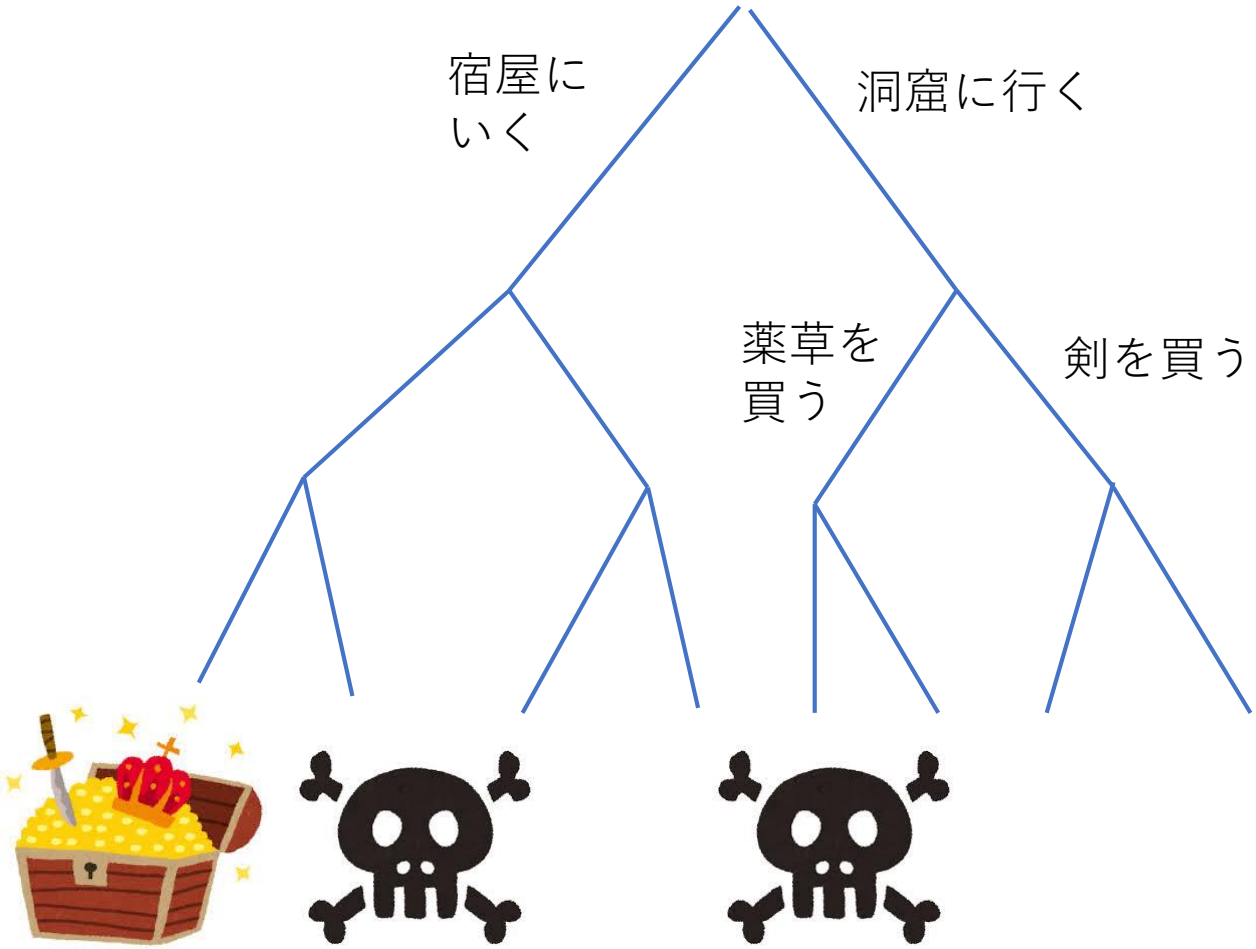
そろばんにレーザーポインターくっつけたら量子コンピューターになるんか

よくあるまちがった説明

全ての組み合わせパターンをしらみつぶしに調べると計算時間が指数的に爆発するような問題は社会に多い。

スケジューリング、配送、金融、創薬、自動運転。。。

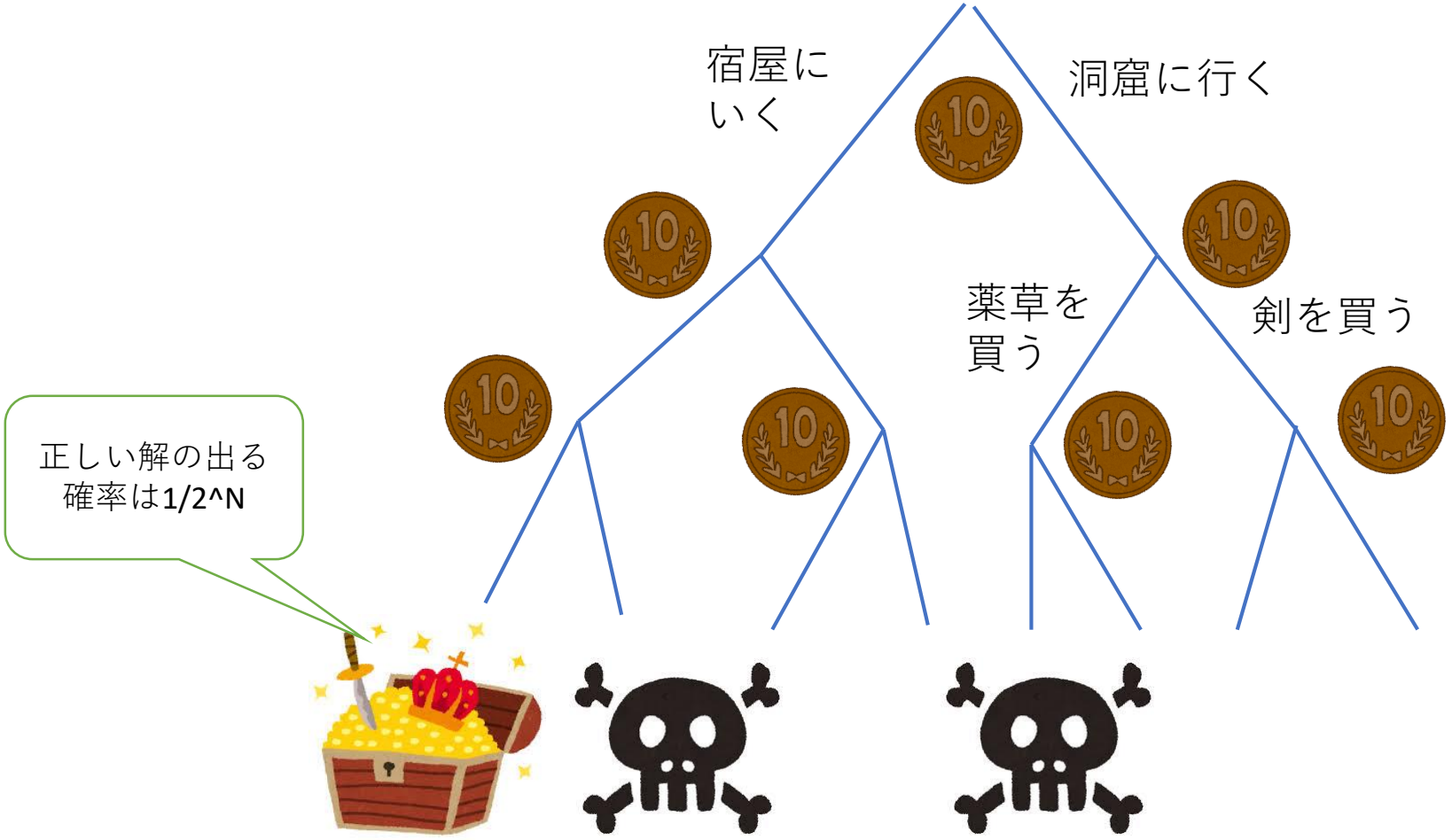
量子計算機を使えば、全てのパターンの量子的重ね合わせで並列処理できるので一発で解ける。



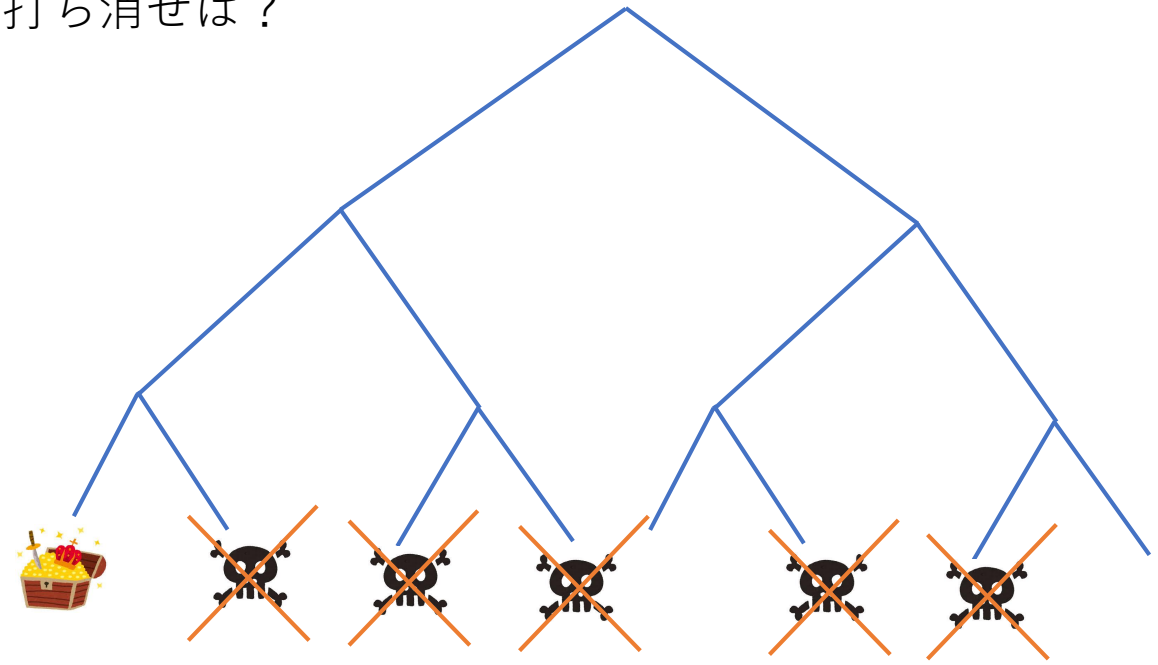
選択肢の数がN個あると、全てのパターンは２のN乗個になる。。。

量子的重ね合わせを使えば一発で並列処理できるのでは！？

重ね合わせを作って測定するだけなら古典の確率的計算（各分岐でコインを振る）と同じ



量子的干渉効果を使い、打ち消せば？



→しかし、打ち消してうまくいくのは特定のうまい構造がある場合のみしか知られていない。（素因数分解とか）。一般にはどうやって打ち消していいか分からない。

→まったく構造を使えない場合（＝しらみつぶし）は、量子計算機でも指数時間必要であることが数学的に証明されている！

[Bernstein et al. 1997]　　ショアーのアルゴリズムは１９９４年！

つまり、研究者の間では、量子計算のかなり初期のころから知られている常識。

古典計算の場合、指数爆発する組み合わせの中から解を探すには、しらみつぶしにやらないといけないので指数時間かかる。一方で量子の場合、重ね合わせを使って一発で解けるため、配送、創薬、金融、スケジューリング、自動運転といった実社会の様々な場面で役に立つ。

問題点１：古典でしらみつぶしにやるような場合、量子でも指数時間かかる。古典だけしらみつぶしで比較するのはアンフェア。古典でもしらみつぶしより速い方法がいろいろある。ちゃんと古典のベスト（ベストアルゴリズム＋専用機）と比較しているのか？

問題点２：「重ね合わせで意味のある問題がいろいろ高速に解ける」という超驚きなことをくちばしっちゃっている。はやく証拠プリーズ。

まとめ

（1）量子計算機とは、量子的な不思議な性質をうまくつかうことにより、古典計算機よりも高性能な計算を行うコンピューターのこと

（2）量子計算機はものすごく時間をかけていいなら古典計算機で代用可能

（3）いくつかの問題については高速に解けると理論的に示されている

（4）量子計算機が速いというのは漸近的な意味

（5）量子計算機がなぜ速いのか、どういう時に速いのか、についての一般的な理論はまだよく分かっていない最先端の研究テーマ

（6）量子的重ね合わせを利用して指数的並列処理で一発。というのはまちがい

（7）実社会の問題を高速に解くすぐに役に立つアルゴリズムはまだない。

量子スプレマシー
（量子超越性）

有料会員限定 記事 今月の閲覧本数： 3 本 登録会員の方は月 10 本まで閲覧できます。

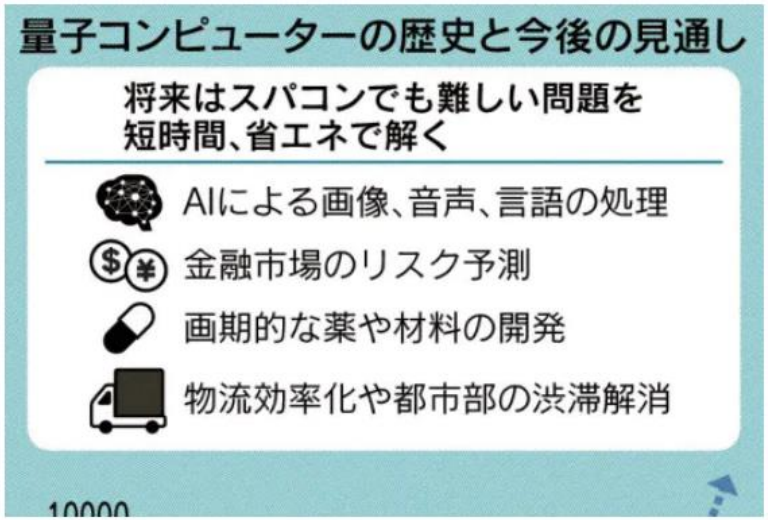
量子コンピューターで「超計算」人類の手中に

スパコン1万年分、3分で　グーグル実証か

2019/10/19付

保存 共有 印刷 その他

人工知能（AI）などに続く革新的技術として期待される**量子コンピューター（総合2面きょうのことば）**が「スーパーコンピューターを超える日」が近づいてきた。米グーグルは、理論上の概念だった性能を実証し、最先端のスパコンで1万年かかる問題を瞬時に解く実験に成功したもようだ。米IBMなども研究に力を入れる。急速な進歩はいずれ人類にこれまでにない計算パワーをもたらす。AIの活用や金融市場のリスク予測などを通じ、社会にディスラプション（創造的破壊）を起こす可能性を秘める。



アクセスランキング

1. （チャートは語る）決戦は年金支給日
2. 英首相、EUに離脱延期申請　「10月末」諦めぬ書簡も
3. ソフトバンクGの節税策、財務省が抜け穴封じへ

日経からのお知らせ

台風19号 救援募金受け付け

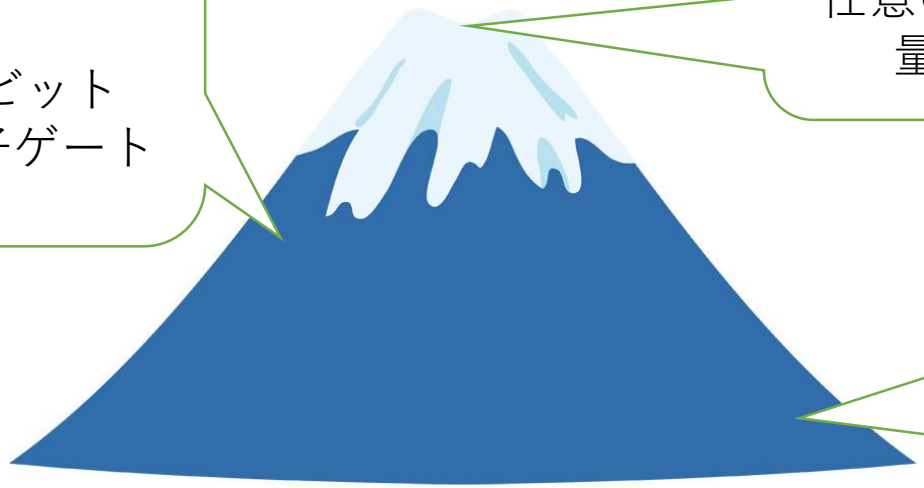
キャリア採用、通年で募集

nikkei.jpg

量子スプレマシー

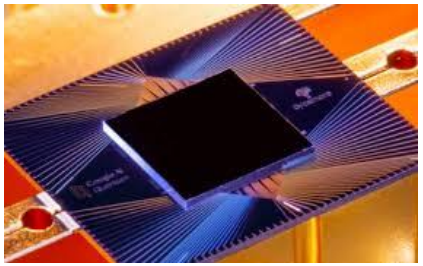
１０２４ビットの素因数分解

２０００量子ビット
10^11 個の量子ゲートが必要



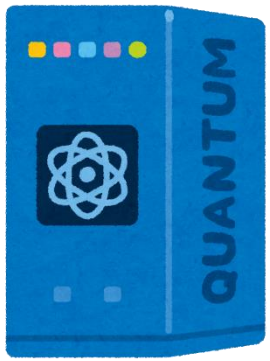
究極のゴール：
量子ビット使い放題
任意の量子アルゴリズム
量子誤り訂正完璧

近い将来に実現できそうな弱い量子計算機でとにかく古典に対する優位性を示す



Googleの５３量子ビットマシン

サンプリング



01011100....

確率的にビット列を吐き出す量子計算機を作る。

→古典計算機で同じ確率分布をシミレートせよ。

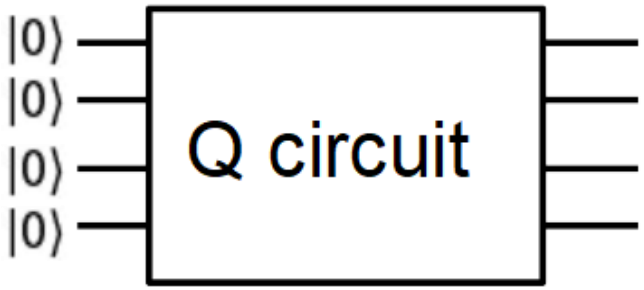
→常識的な時間では不可能です。

メリット：
量子優位性が強力な理論的基盤で保証されている
実現するのが比較的簡単

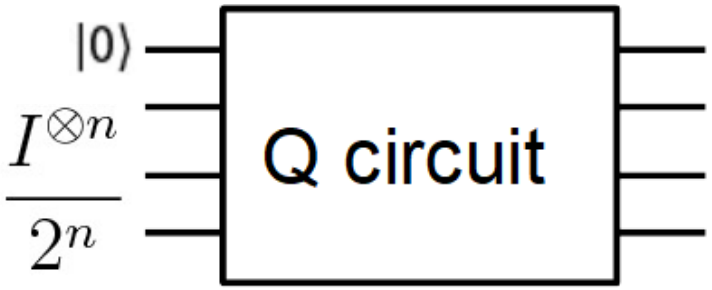
デメリット：
役に立つ応用が不明
（量子優位性の証明を最優先。応用は二の次。）

こんな「しょうもない」レベルでもものすごく大変
→逆に言うと、社会にすぐに役に立つ応用なんてのはまだまだぜんぜん先の話。

One-clean qubit モデル



通常の量子計算



One clean qubit model

[Knill and Laflamme, PRL 1998]

古典よりはちょっと強いだろう

例：Jones多項式の計算
[Shor and Jordan 2007]

古典 → ユニバーサル量子

計算量理論の強力な基盤にもとづいて量子優位性を証明！
[TM, Fujii, and Fitzsimons, PRL 2014]

量子スプレマシーの歴史

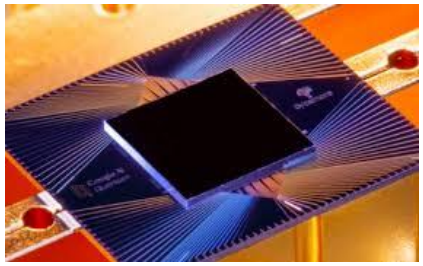
深さ４の回路
Terhal and DiVincenzo, QIC 2004

相互作用無し光子(Boson Sampling)
Aaronson and Arkhipov, STOC 2011

交換するゲート(IQP)
Bremner, Jozsa, and Shepherd, Proc. Roy. Soc. A 2010
（古典イジング分配関数[Fujii and TM, NJP 2015]）

One-clean qubit model
TM, Fujii, and Fitzsimons, PRL 2014

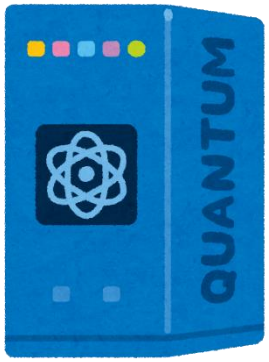
ランダム回路
Bouland et al. Nature Phys. 2018



2019 Googleがついに実現！？

Fine-grained量子スプレマシー　（理論はどんどん先へ！）
[Dalzell et al. 2018, TM and Tamaki 2019]

Fine-grained量子スプレマシー



01011100….

古典計算機で同じ確率分布を
シミレートせよ。

従来の量子スプレマシー：多項式時間では不可能です。

→ $n^{\log\log\log\log(n)}$ なら可能かも。スパコンで頑張ればできるかも。。

Fine-grained量子スプレマシー：指数時間でも不可能です。

[Dalzell et al. arXiv:1805.05224]
[TM and Tamaki, QIC 2019]

はたして量子スプレマシーはでたのか！？

Googleの論文を待ちましょう。。。

量子暗号

暗号

もともとは敵に秘密にメッセージを送る手段だった　（限られた場所、限られた人のみ）

今では一般の人が日常的に使用している

量子暗号

量子暗号：量子を使って暗号タスクを実現する研究

注１：量子鍵配送とは限らない
注２：古典暗号の量子攻撃に対する安全性を研究するものもある（格子暗号等）

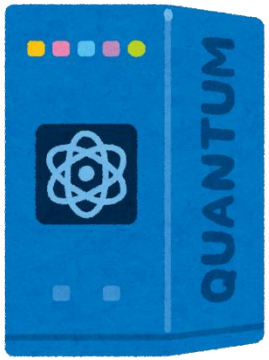
計算量的安全性：ある問題が難しいことを仮定（例：素因数分解）

情報理論的安全性：そういう仮定なし。

量子暗号は情報理論的安全性が達成できる場合が多い！
例：量子鍵配送、セキュアクラウド量子計算

→暗号でも量子の優位性がある！！

セキュアクラウド量子計算



量子計算機
（クラウド）

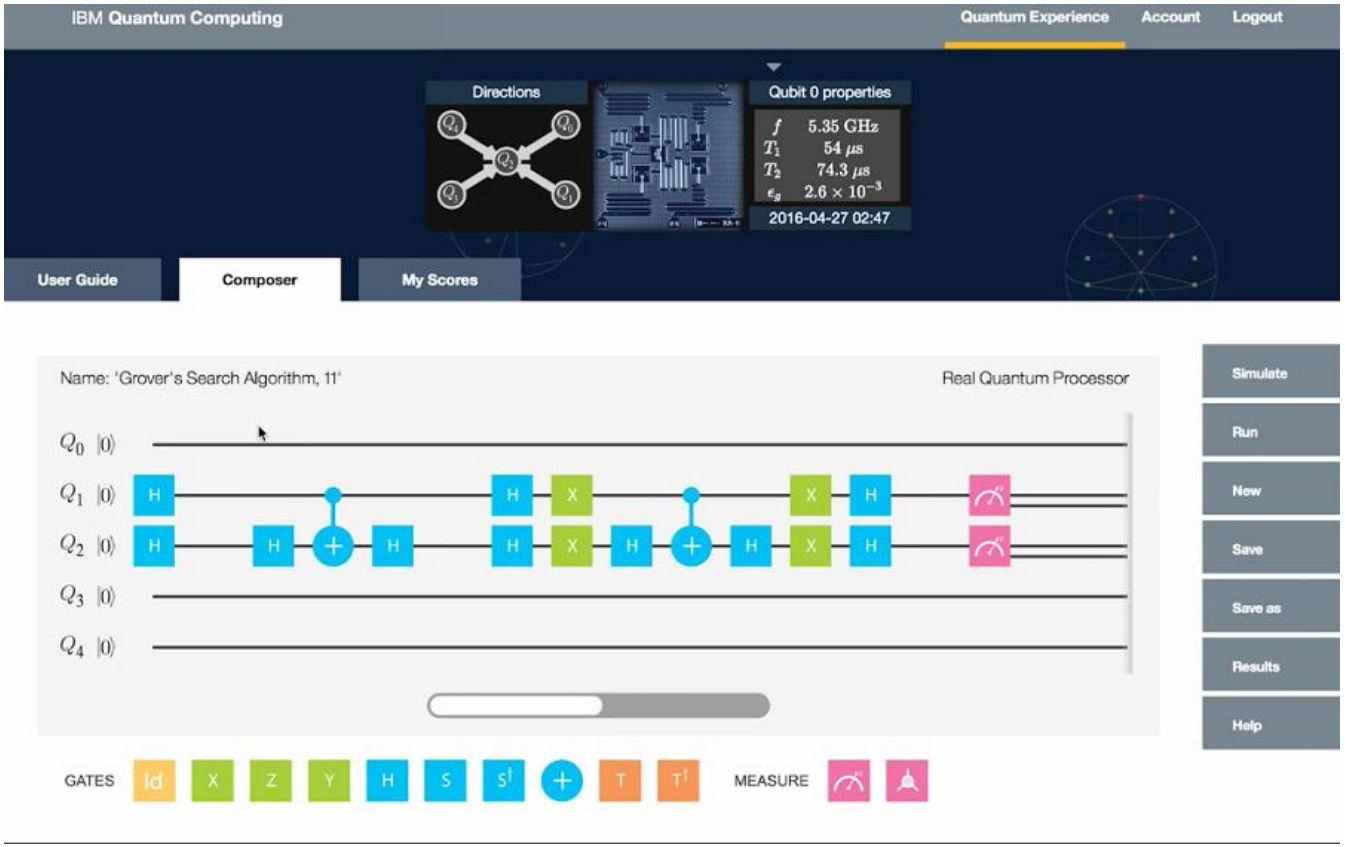
通信路（古典）

利用者（古典計算のみ）

計算内容を秘密に保ったまま、量子クラウドに量子計算を委託できるか？

古典計算の分野でも「委託計算」などと呼ばれ古くから研究されている

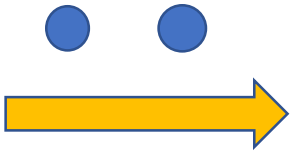
クラウド量子計算　（IBM）



今は研究者が使用。今後一般に普及するためにはセキュリティが大切に

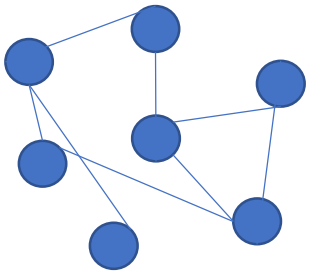
BFKプロトコル

アリス



量子ビット
（暗号鍵）

ボブ

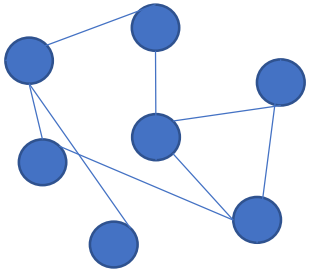


グラフ状態作る

アリス

古典通信
（暗号化）

ボブ

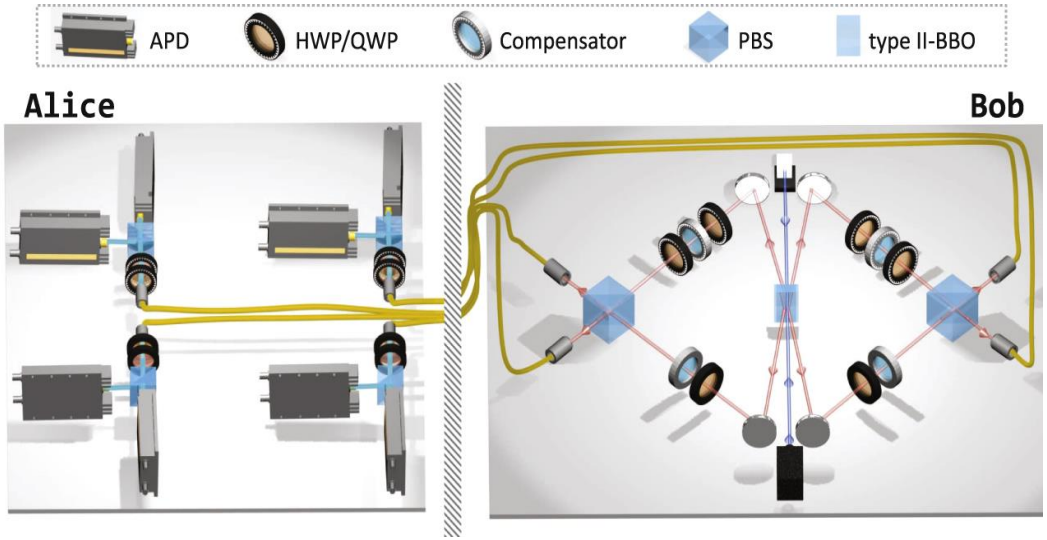


測定型量子計算実行

Broadbent, Fitzsimons, Kashefi, FOCS2009

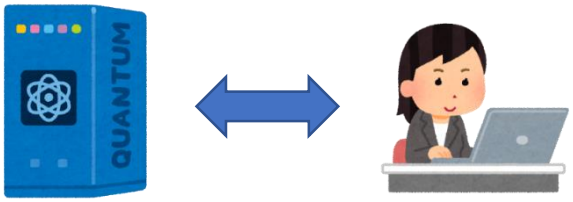
情報理論的安全性（量子論が正しいなら安全)

実験

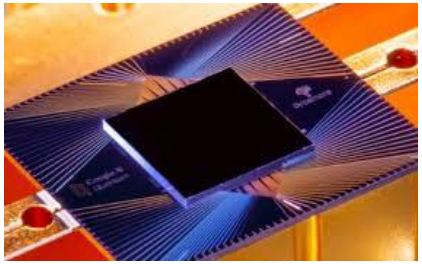


光キュービットによる実験(ウィーン大学)
Barz et al., Science 2012

量子計算の検証



量子クラウドが正しい量子計算をしているのかどうか、量子計算機を持たない利用者は検証できるか？



Google等は量子スプレマシーの領域に達する→どうやって検証するのか？

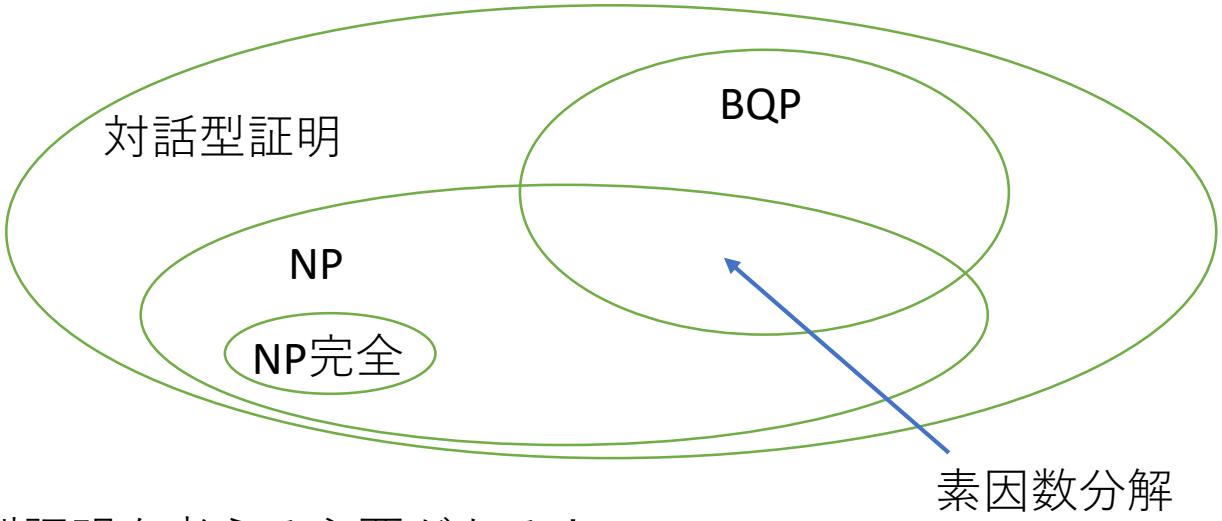
量子計算機は古典計算機ではシミレートできない
→　古典計算機では検証ができないという皮肉なジレンマ

→非常に重要な問題であり、世界中で研究がなされている

NPなら検証可能

NP＝答えをもらえば、チェックは簡単にできる問題
素因数分解、巡回セールスマン等

しかし、NPは量子計算と相性が悪い！



対話型証明を考える必要がある！

対話型証明系

通信路（古典）

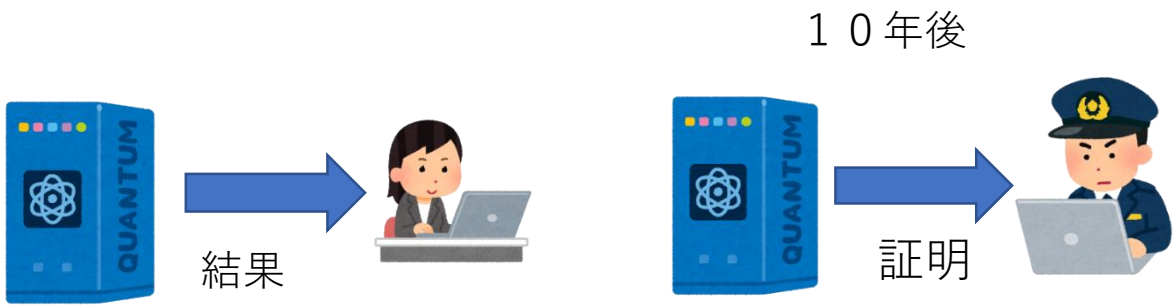
Merlin（なんでも解ける）

Arthur（古典計算のみ）

NPの拡張。計算量理論におけるもっとも重要な概念の一つであり、暗号や近似アルゴリズム等においても重要！

例：ペプシとコーラ

Post hoc 検証



Fitzsimons, Hajdusek, and TM, PRL 2018

QUANTUM COMPUTING

Graduate Student Solves Quantum Verification Problem

72

Urmila Mahadev spent eight years in graduate school solving one of the most basic questions in quantum computation: How do you know whether a quantum computer has done anything quantum at all?

13:36
2019/02/04

耐量子暗号の利用

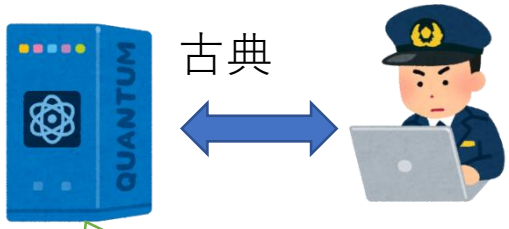
LWE（耐量子暗号）が量子計算では難しいと仮定するなら、量子計算の検証は可能！[Mahadev, arXiv:1804.01082]

→post hocプロトコルを利用！

Morimae-Fitzsimons

$$|\Psi\rangle = \sum_{t=0}^{T} U_t ... U_1 |0^n\rangle \otimes |t\rangle$$

Mahadev



$$|\Psi\rangle = \sum_{t=0}^{T} U_t ... U_1 |0^n\rangle \otimes |t\rangle$$

まとめ

（1）量子スプレマシー

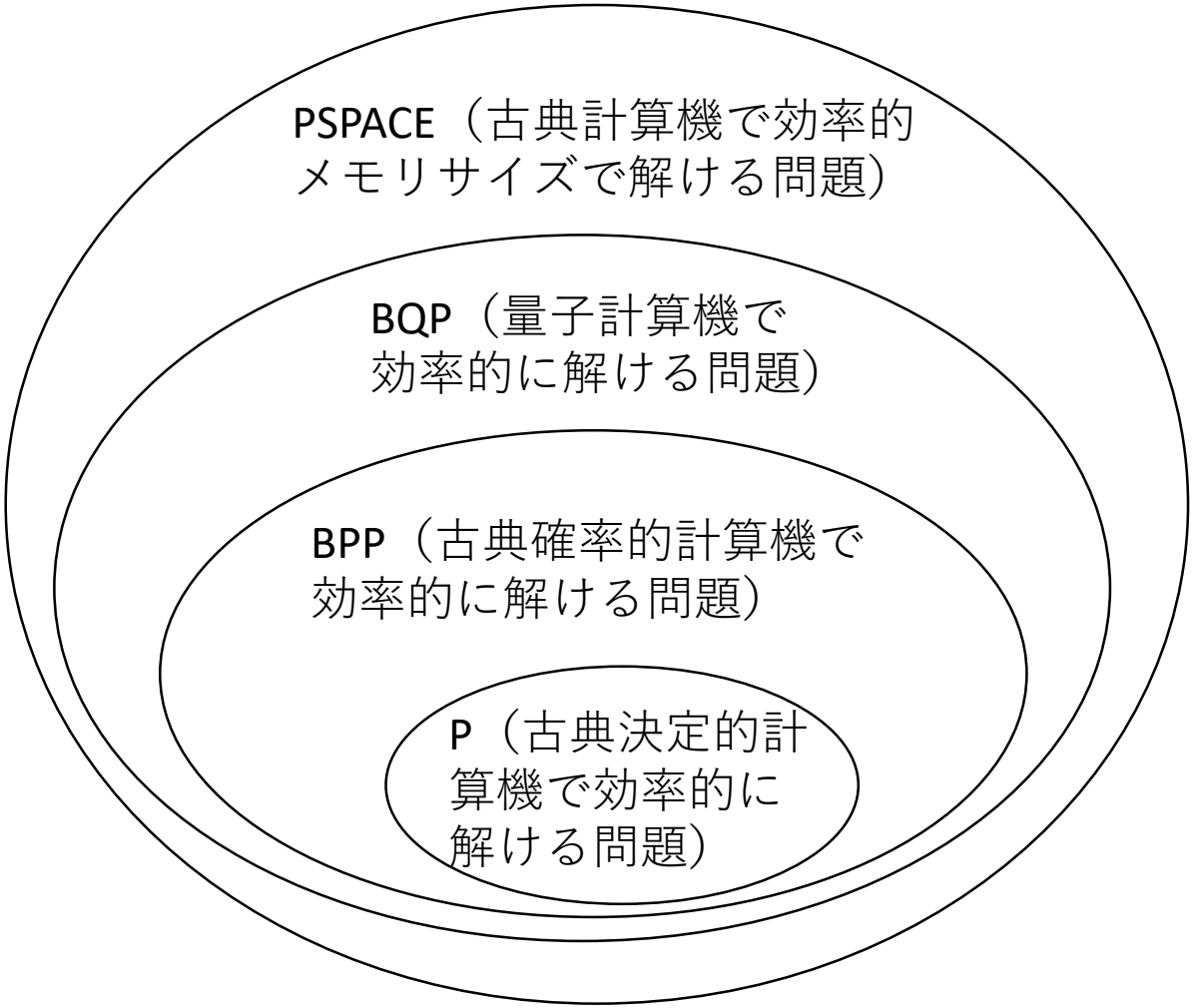
近い将来にできそうな「弱い」量子計算機で量子優位性を示す
→Googleがついに実現！？

（2）量子暗号
→量子を使って高性能の暗号技術が実現可能

例：セキュアクラウド量子計算
計算内容を秘密に保ったまま量子計算を委託できる
計算の正しさもチェックできる

計算量理論

計算機科学の一分野
計算にどのくらいのリソース（時間、メモリ）が必要かを調べる学問



PSPACE≠Pは
大未解決問題！

BQP≠BPPを示すのは
恐ろしく難しいだろう

量子高速性証明のこれまでのアプローチ

しかしながら、量子＞古典であることを示唆する結果は大量にある
(quantum algorithm zoo)

二つのタイプに分類される

１．グローバータイプ　（Grover、Simon、Bernstein-Vazirani）

２．ショアータイプ　（素因数分解、Jones多項式、量子シミレーション）

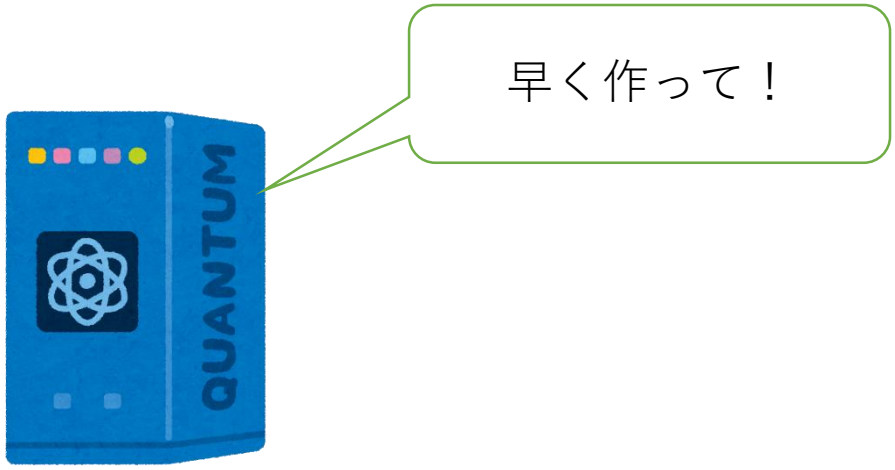
さらなる問題点

複雑なアルゴリズムばかりで、実現が難しい

１０２４ビットの素因数分解をするのに

２０００個の量子ビット、10^11個の量子ゲートが必要

[Roetteler et al., arXiv:1706.06752]



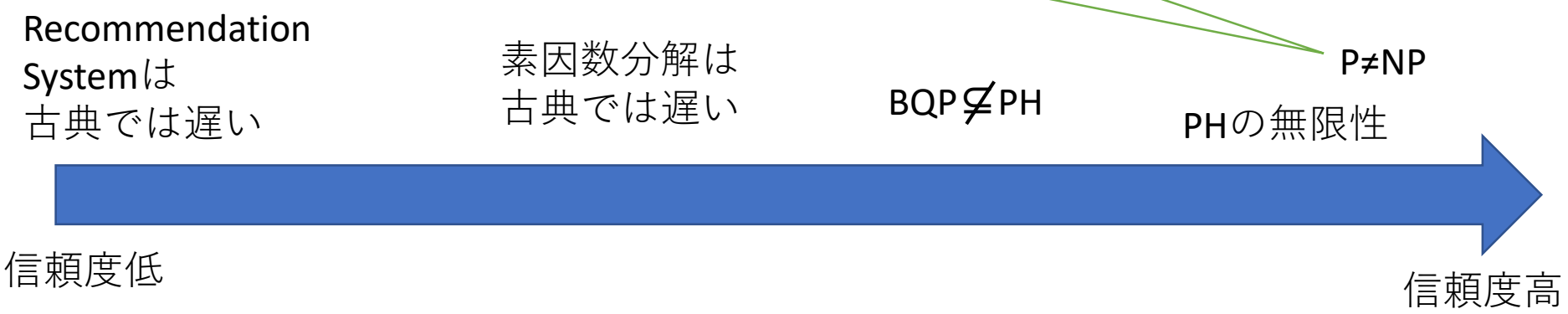
強力な基盤

計算量理論の意味で量子＞古典を完全に証明するのはほぼ不可能

量子＞古典である確率を最大化する（メタ議論）

量子計算が古典計算でシミレートできたらP＝NPになる

→P≠NPなので、量子は古典ではシミレートできない

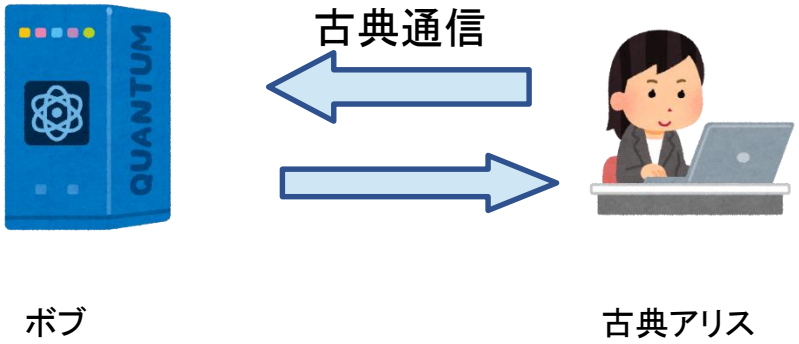


P、NPを一般化した多項式階層の無限性を使う！

完全古典アリスは可能？

ある特別な場合は不可能　　1ラウンド＋Perfectly secureで可能ならBQPがNPに入る。

（BQPがNPに入るとは信じられていない。）



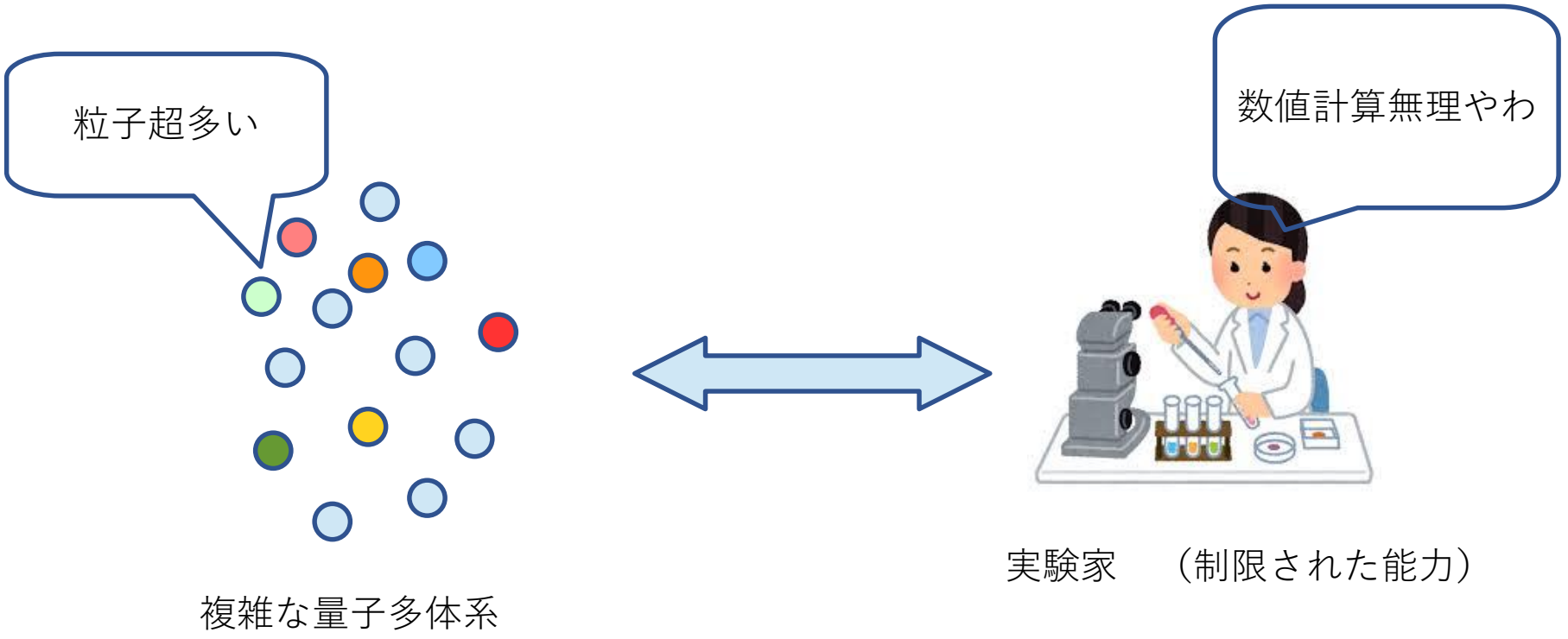
TM and Koshiba, arXiv:1407.1636

最近拡張された[Aaronson et al., arXiv:1704.08482]

　→通信回数poly, インプットのサイズは漏れてもいい、

ボソンサンプリングできたらPH4崩壊、

量子論基礎への応用



実験家は、量子多体物理理論が本当に正しいのか検証できるのか！？

少数粒子系は、解析、数値計算と実験が一致することが検証されている。
量子多体系は解析、数値計算が無理！

グローバータイプ

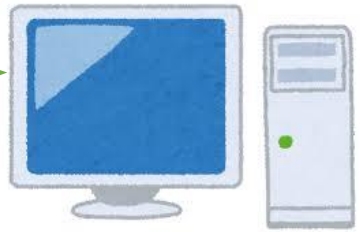
私の勝ち

量子計算機

回数少ない

サブルーチン

くやしい



古典計算機

回数多い

サブルーチン

サブルーチンを呼ぶ回数だけ見ている。
→計算量理論におけるスタンダードなアプローチ（query complexity）
→古典の限界の証明がしやすい。（多くの結果が得られている。）
→実時間でどうなるか不明。

ショアータイプ

こちらは実時間を見る(time complexity)

古典のベストより高速であることを示す

素因数分解：古典では遅いが量子では速い

→古典では遅いという数学的証明があるわけではない

将来古典の高速アルゴリズムが見つかるかも！

例：recommendation system
客の購買データーからおすすめ商品を見つける量子機械学習アルゴリズム

→米国の１８歳の学部生が高速古典アルゴリズムを見つけてしまった！

古典のベストと比較して速い、というのは危険！