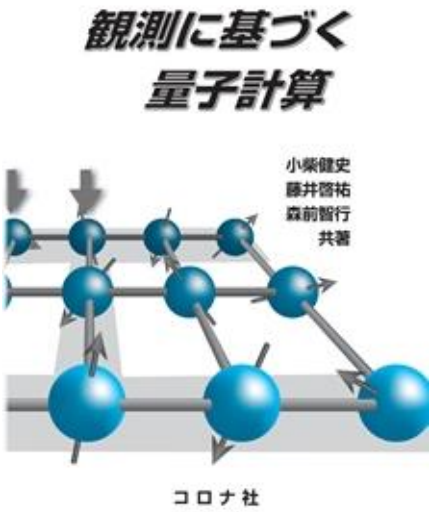
量子スプレマシーと量子計算の検証

森前智行
(京都大学基礎物理学研究所)

東北大セミナー

本日の内容

- 量子計算の基礎
- 量子スプレマシー
- セキュアクラウド量子計算、量子計算の検証

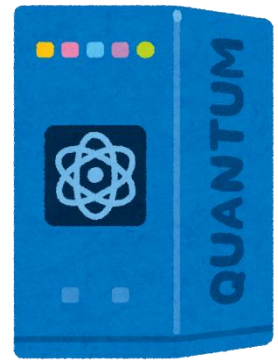


小柴、藤井、森前
コロナ社

森前
森北出版

量子計算の歴史は約３６年

おもいついた



ファインマン
１９８２年

３６年間の間に非常に多くの理論的・実験的結果が得られてきている

→現在では量子計算は古典計算よりすごいと信じられている

実際すごいのであるが、どうすごいのか正確に理解されていない。

特に、近年過剰な報道がなされ、無茶苦茶なことになっている。
→アカデミアで言われていることと全然違うことが流布されている
（大学研究者がそれに加担しているのは信じられない。）

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）古典の場合、指数爆発する組み合わせの中から解を探すの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、創薬、金融、スケジューリングといった様々な場面で役に立つ。

（２）量子コンピューターは長い間実現に苦労していたが、ゲート型とは違う量子アニー〇ングという方法を用いることにより、カナダのベンチャーがいち早く商用化に成功した。

（３）そのマシンはGoogleのチームが古典計算機より１０億倍高速であると報告し、世界を騒がせた。

（４）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。

（５）しかしながら、最近では国産マシンも実用化され、しかも電機メーカたちも量子コンピューターの商用マシンを次々だしてきており、オールジャパンのまきかえしが起こっている。

（６）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＊＊型であり組み合わせ最適化を得意とする。

全部間違い

（1）古典の場合、指数爆発する組み合わせの中から解を探すの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、創薬、金融、スケジューリングといった様々な場面で役に立つ。

→しらみつぶしにしかできないブラックボックスの場合、量子でも指数時間かかる。

→重ね合わせで並列処理しただけだと古典と同じ。

→干渉で打ち消すのは、一般にはどうやっていいか分からない。

→現実的な問題に有用な高速量子アルゴリズムはぶっちゃけ、まだなんもない。

（２）量子コンピューターは長い間実現に苦労していたが、ゲート型とは違う量子アニー〇ングという方法を用いることにより、カナダのベンチャーがいち早く商用化に成功した。

（４）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。

→それは、昔から世界中で研究されてきて、実現が目指されていたいわゆる「量子コンピューター」とは違う別のもの。特に、量子コンピューターと違い、高速であるという証拠がまだない。

（３）そのマシンはGoogleのチームが古典計算機より１０億倍高速であると報告し、世界を騒がせた。

→ある特定の古典アルゴリズムと比べたら１０億倍速いが、他のもっと速い古典アルゴリズムには負けてる。http://news.mit.edu/2015/3q-scott-aaronson-google-quantum-computing-paper-1211

（５）しかしながら、最近では国産マシンも実用化され、しかも電機メーカたちも量子コンピューターの商用マシンを次々だしてきており、オールジャパンのまきかえしが起こっている。

→それらも量子コンピューターではない。というかむしろ古典計算機。

‘６）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＊＊型であり組み合わせ最適化を得意とする。

→ゲート型、という不思議な言い方は日本でしか使われていない。海外で量子コンピューターと呼ばれているものが、なぜか日本国内ではゲート型の量子コンピューターという謎の呼ばれ方をしている。

→ゲート型の枕詞に必ず汎用の、とつくのも意味不明。汎用だから偉いわけではない。

→そもそも、もう一つの＊＊型はゲート型と違い、古典より速いという証拠が無い。並列して並べて、あたかも同じものでタイプが違うだけ、という印象を与え、速いかのようにミスリードをしている。

ここにも書いてある

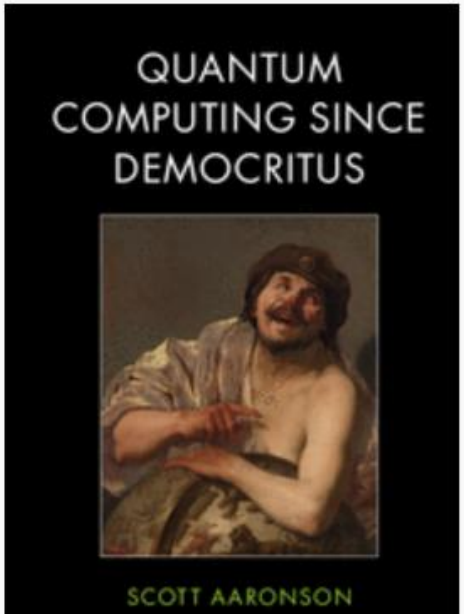
Aaronsonのブログ

My Y Combinator podcast

June 29th, 2018

Here it is, recorded last week at Y Combinator's office in San Francisco. For regular readers of this blog, there will be a few things that are new—research projects I've been working on this year—and many things that are old. Hope you enjoy it! Thanks so much to Craig Cannon of Y Combinator for inviting me.

Associated with the podcast, Hacker News will be doing



気を取り直して。。。

量子計算の基礎

量子計算と古典計算の違い

古典確率的計算：

計算機の状態は確率ベクトル (p_1,p_2,…,p_n)
計算ステップは確率行列の作用

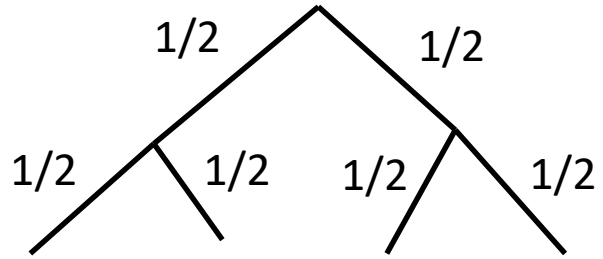
量子計算：
計算機の状態はL2ノルムが１の実数ベクトル (p_1,…,p_n)
計算ステップはL2ノルムを保存する行列の作用

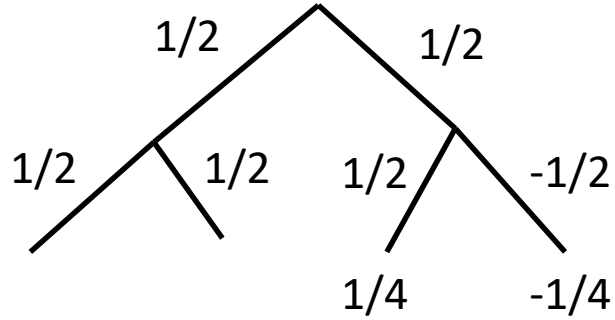
$$\sum_i |p_i|^2 = 1$$

１．複素数は２つの実数で表すことができる。

２．なぜこうなのかはこうだと自然をうまく説明できるから、としかいいようがない（例：地球がまるいこと）

３．古典にはない不思議な現象が：テレポーテーション、エンタングルメント、重ね合わせ、トンネル効果、etc.

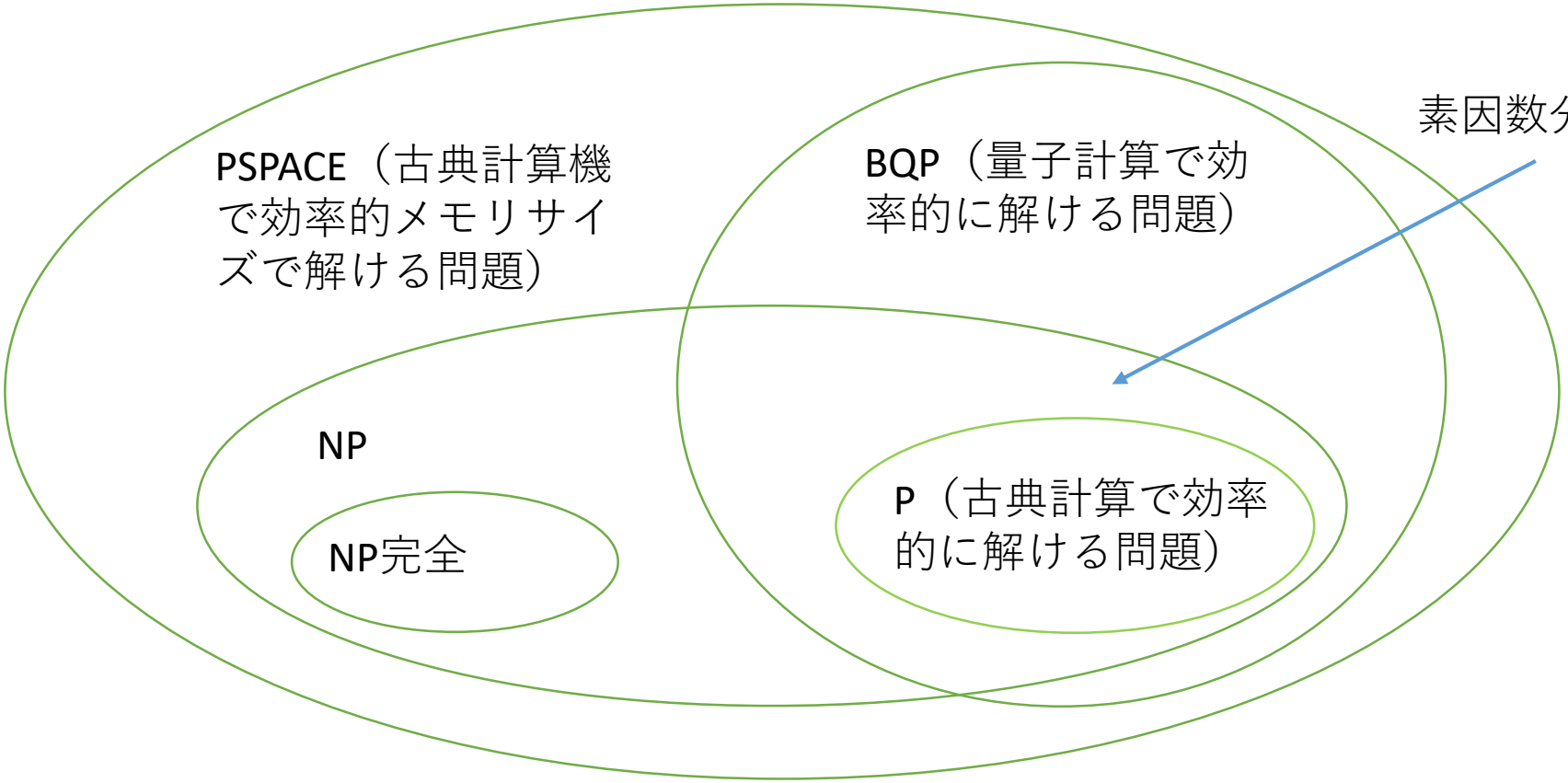




量子計算は異なる計算パスを互いに打ち消すことが可能。

→これが（おそらく唯一の）古典計算と量子計算の違い！

量子計算のできないこと

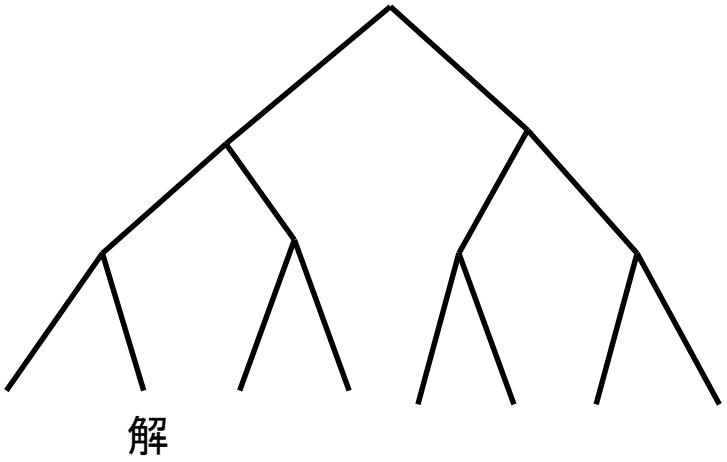


1．量子計算は、どれだけ時間をかけてもいいなら古典計算機でシミュレート可能

2．量子計算はNPが苦手

量子計算はNPが苦手

NP：指数個のパターンの中に、解があるか無いか判定せよ



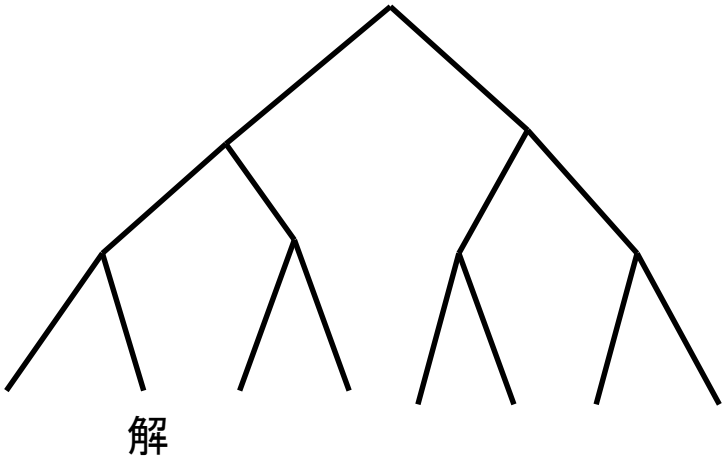
よくある間違った説明：「古典だとしらみつぶしに調べるから指数時間かかるけど、量子なら重ね合わせを使って一度に処理できるから指数倍高速！」

→大嘘。解のでる確率は指数的に小さい！

しかも、それなら乱数を使った古典確率的計算と何も変わらない。

量子計算はNPが苦手

NP：指数個のパターンの中に、解があるか無いか判定せよ



量子的干渉を使い、不必要な状態を消せばよいのでは？

→ある意味YES。しかし、問題が良い構造を持っておりそれをたまたまうまく利用できるときしかうまくいかない。

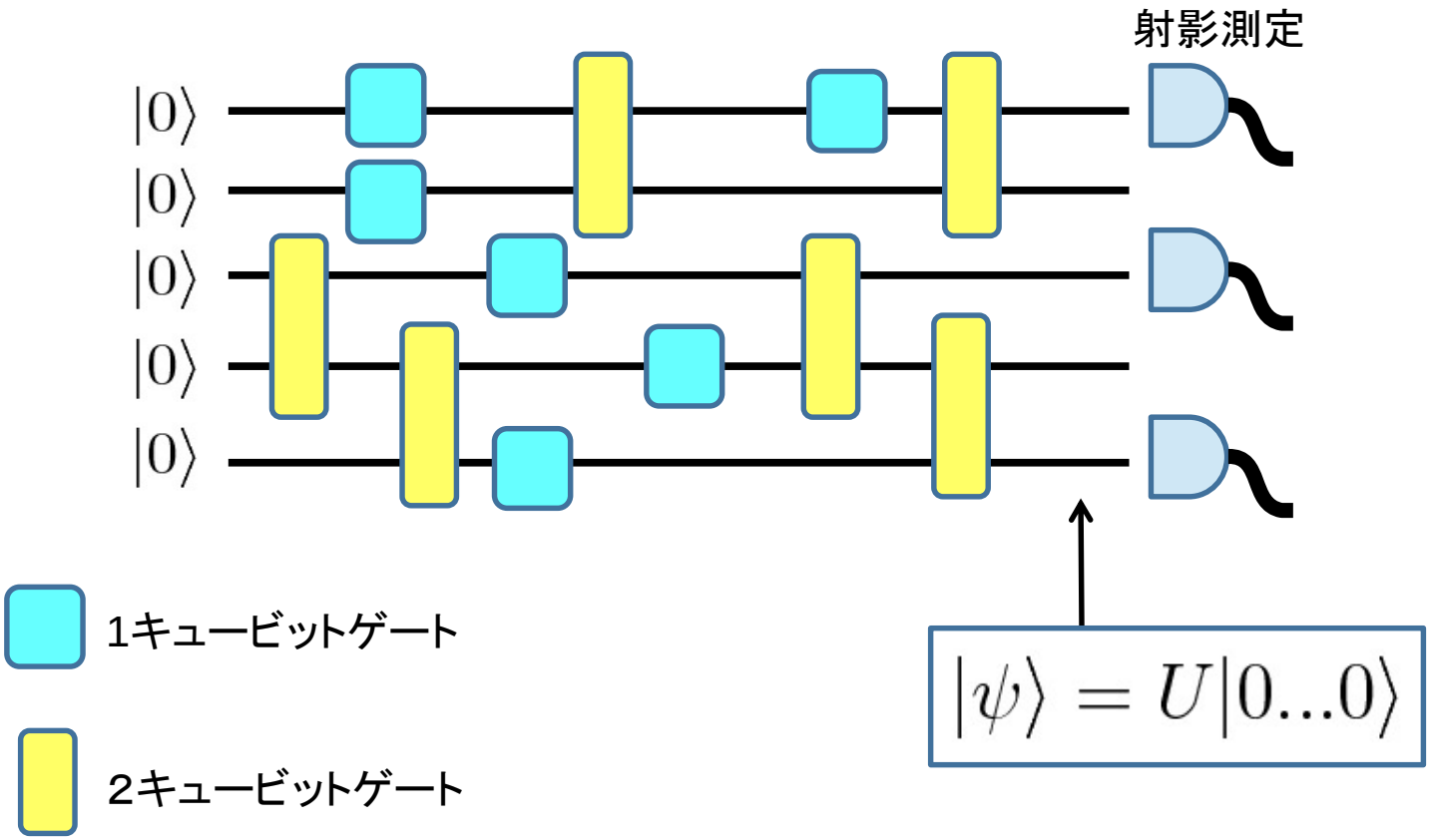
→　一般にはどうやっていいか分からない。

→特に、問題の構造を全く使えないブラックボックスの場合（つまりしらみつぶし）、量子でも指数時間かかることは２１年前にすでに証明されている！

[Beals et al. J ACM 48, 778 (2001)]

回路モデル

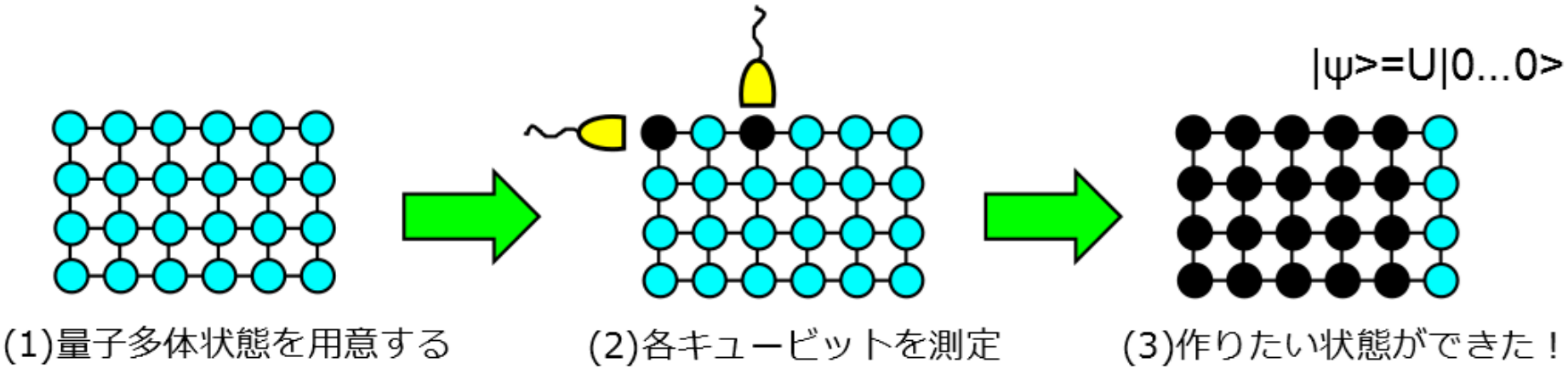
|ψ>を|0...0>からユニタリ演算子を作用させて作る。



伝統的な量子計算モデルであった

測定型量子計算

(Raussendorf and Briegel, PRL 2001)



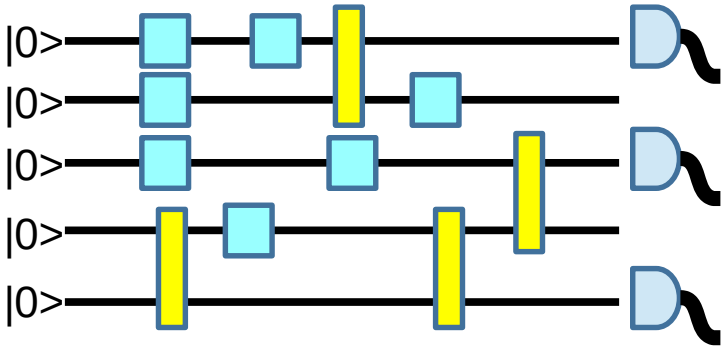
量子計算とは|ψ>を作ること。とにかくできたんだから目的は達せられた!

なぜ量子計算できるの？　→　測定による反作用を利用！！

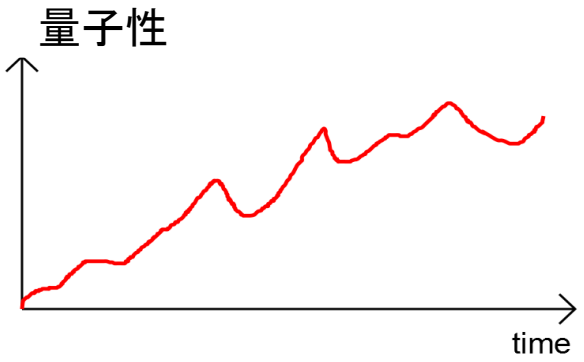
最初に用意する量子多体状態は、|ψ>に依存しない：ある一つの状態から何でも作れる！
（例：グラフ状態）

測定型量子計算のメリット

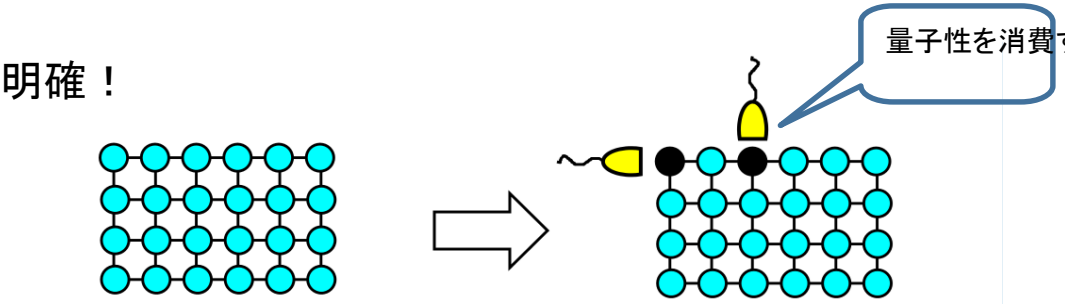
測定型量子計算は量子vs古典の境界が明確！



だらだらと量子

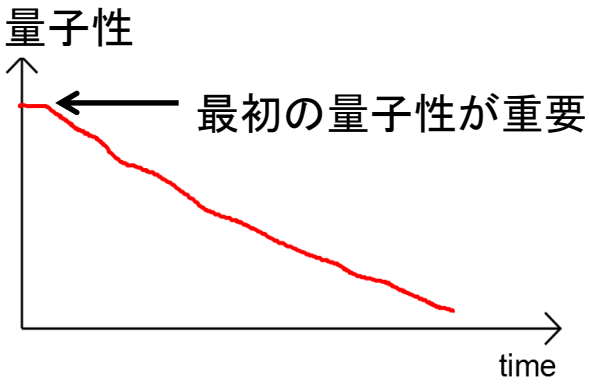


どこの量子性が重要か良く分からん。。。



量子的段階　　古典的段階

量子と古典の境界がくっきり明確

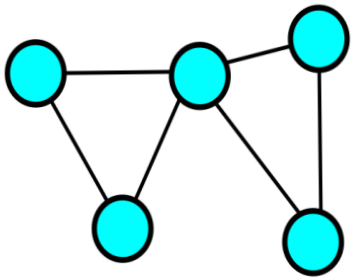


この、「量子・古典分離」が、ここ16年の多くの成功を可能にしてきた。

測定型量子計算と古典統計力学

測定型量子計算と古典イジング分配関数の間には面白い関係がある！

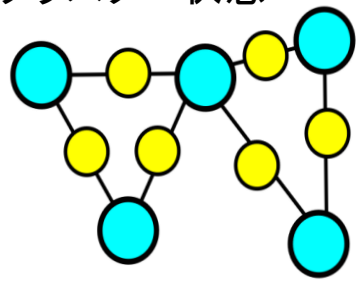
古典イジングモデル



$$H = J \sum_{<i,j>} \sigma_i^z \sigma_j^z + \sum_j h_j \sigma_j^z$$

$$Z_\beta = |\langle \phi | C \rangle|^2$$

クラスター状態



$$|\phi\rangle = \bigotimes_{j=1}^{n} |\phi_j(\beta, J, h_j)\rangle$$

古典統計物理の結果：
可解
NP-hard...

量子計算の結果：
古典シミレート可能
Universal...

(Bravyi and Raussendorf, PRA 2007)
(Nest, et. al. PRL 2007)
(Fujii and TM, NJP2016)

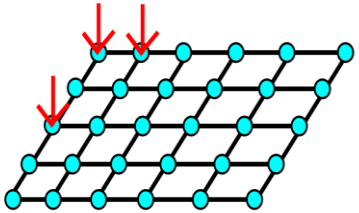
量子サブルーチン

測定型量子計算の別の解釈

Classical computer
（only XOR gate）

サブルーチン

測定



Quantum many-body system
（resource state）

Classical XOR + graph state = quantum universal

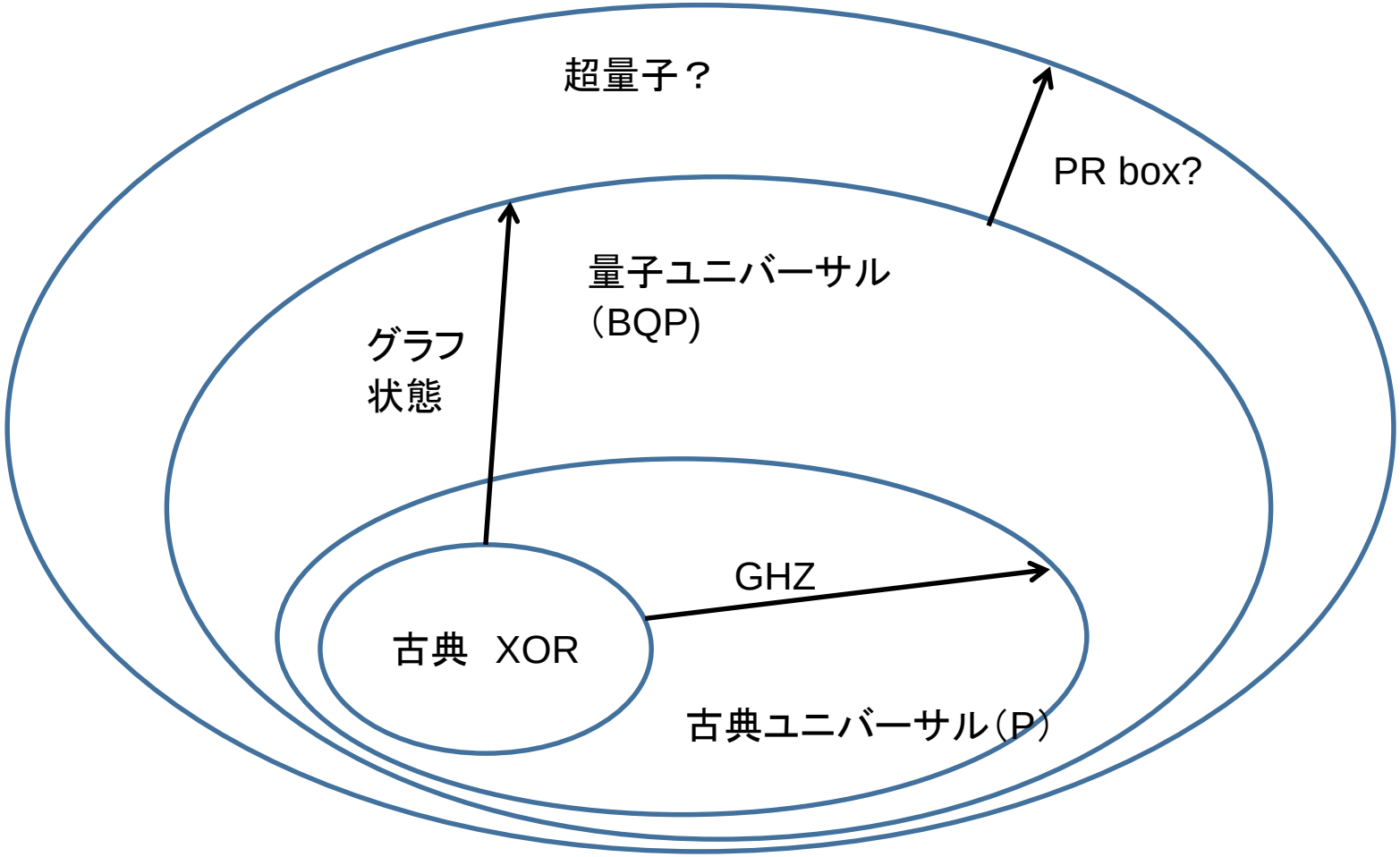
XOR＋GHZ＝classical universal [Anders and Browne, PRL2009]

$$|0^n\rangle + |1^n\rangle$$

XOR gate

0 0 → 0
0 1 → 1
1 0 → 1
1 1 → 0

リソース理論

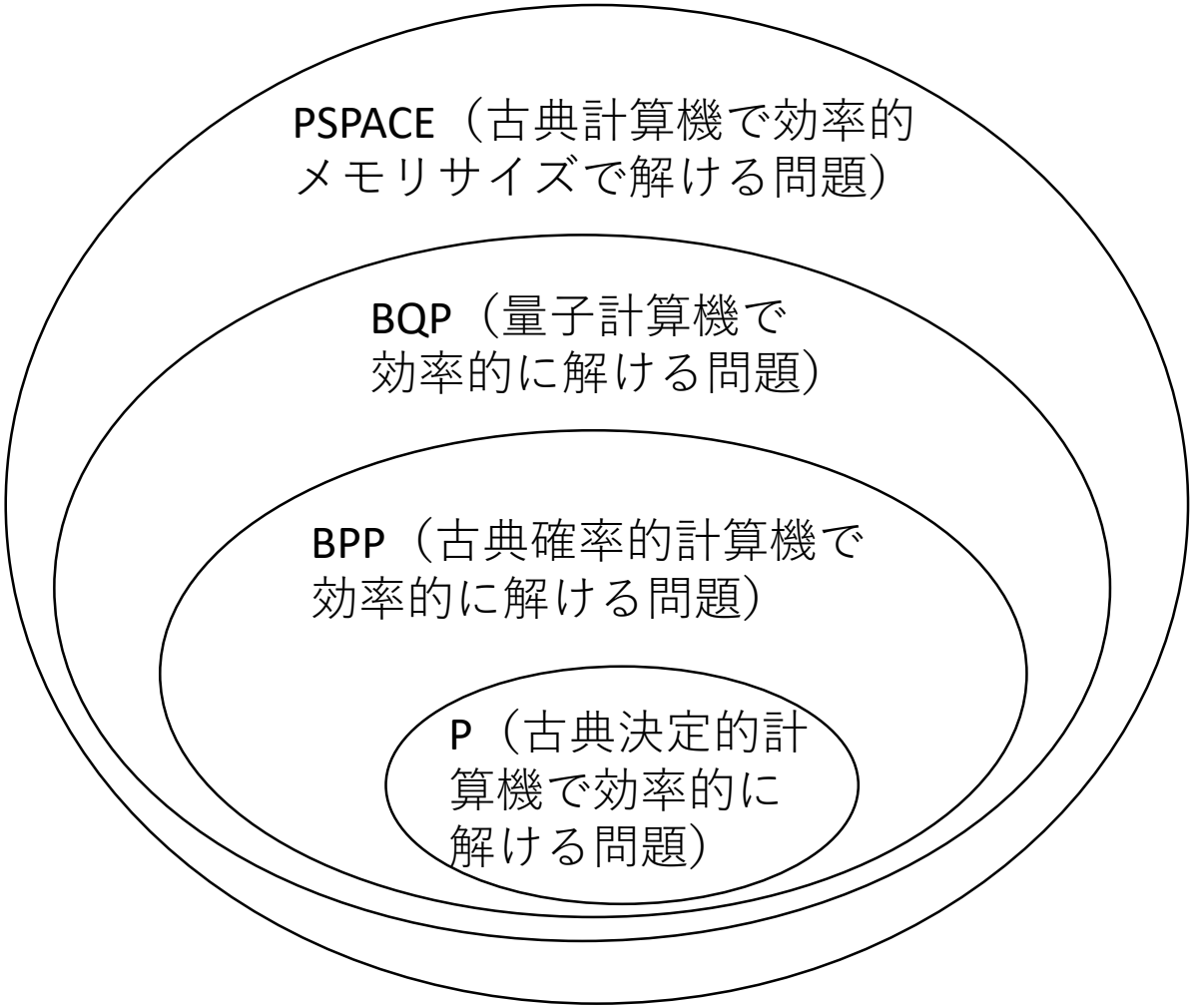


量子スプレマシー
（量子超越性）

弱い量子計算機が古典より強いことを強い基盤に基づいて証明する

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）

グローバータイプ

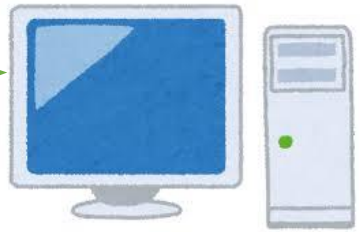
私の勝ち

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！

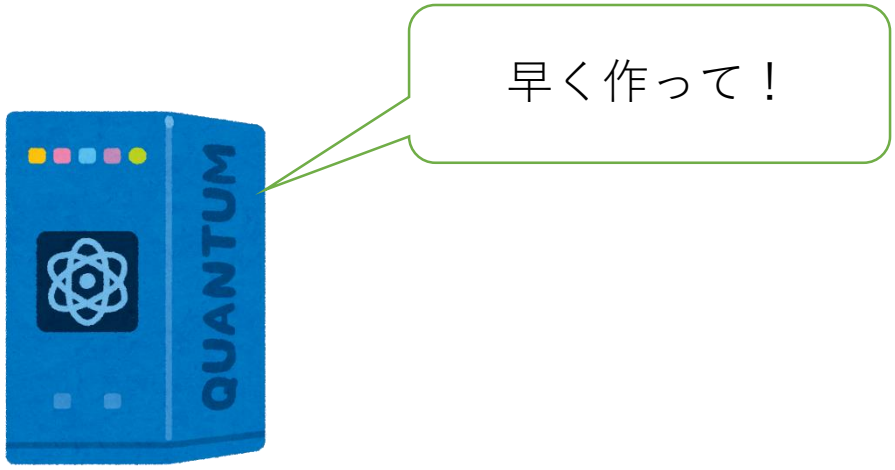
さらなる問題点

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]



量子スプレマシー

ショアータイプ、グローバータイプに次ぐ第三の新しいアプローチ！

２０１１頃から活発に。今ではGoogle等が実現を目指しており、一般向けのビジネス雑誌にも（用語だけは）出るように

これまでの問題を解決！

１．基盤が弱い→計算量理論の強力な基盤で量子高速性を証明

２．実現が大変→シンプルな量子計算機でもOK

注：デメリットもある
サンプリングなので応用がない
Additive errorの場合さらなる仮定が必要

サンプリング問題

$$z \in \{0,1\}^n$$

n ビット列 z を確率 p_zで出す量子マシン

確率分布 {p_z}を厳密もしくは
近似的にシミレートしろ

$$\sum_z |p_z - q_z| \leq \epsilon$$

$$|p_z - q_z| \leq \epsilon p_z$$

$$z \in \{0,1\}^n$$

「弱い」量子マシンであっても、古典でシミレートできない！

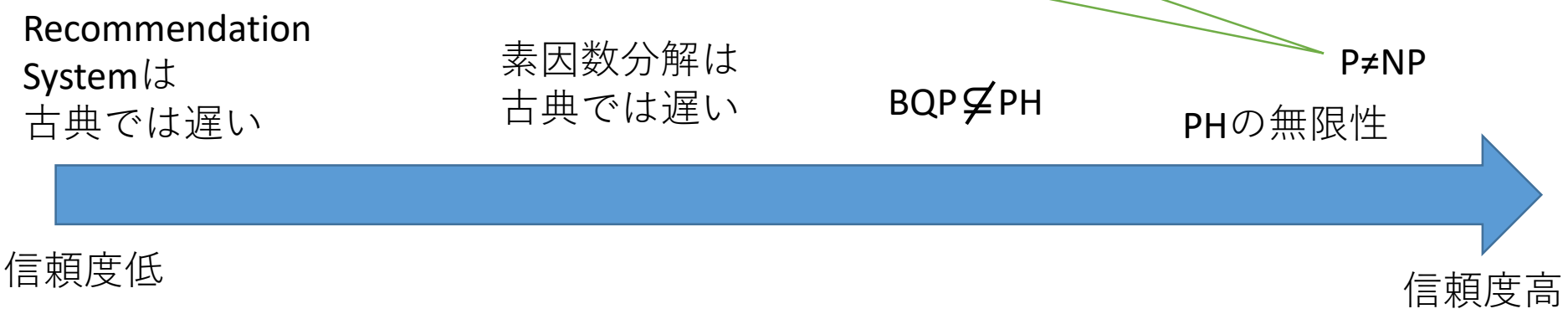
強力な基盤

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



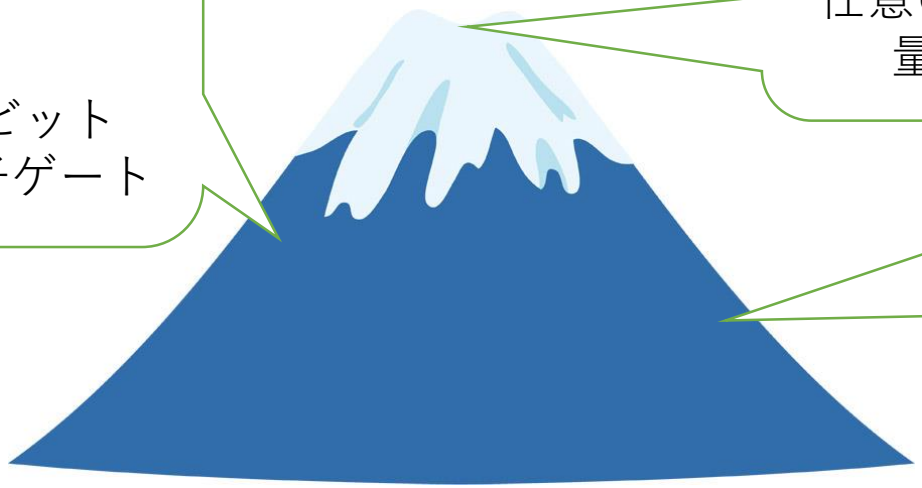
P、NPを一般化した多項式階層の無限性を使う！

シンプルでもOK

もう一つの重要なメリット：
量子スプレマシーは、ユニバーサルでなくて非常に弱い量子計算機でもOK!

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



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

弱い量子計算機でも量子優位性が強力な基盤で示せる！

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

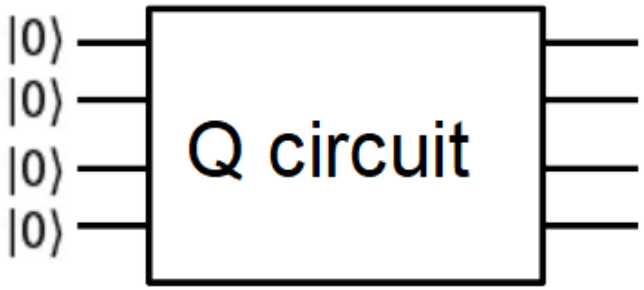
交換するゲート(IQP)
Bremner, Jozsa, and Shepherd, Proc. Roy. Soc. A 2010
（古典イジング分配関数[Fujii and TM, NJP 2015]）

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

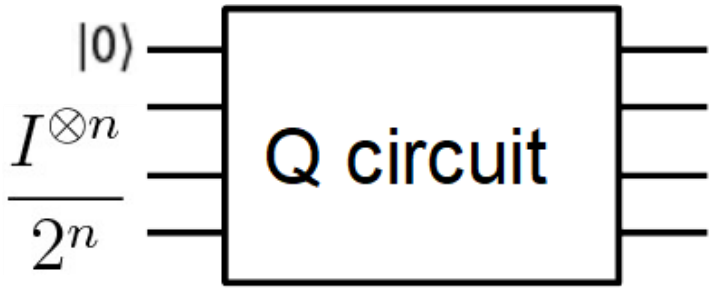
ランダム回路
Fefferman et al. arXiv:1803.04402

Googleが実現！？

One-clean qubit モデル



通常の量子計算

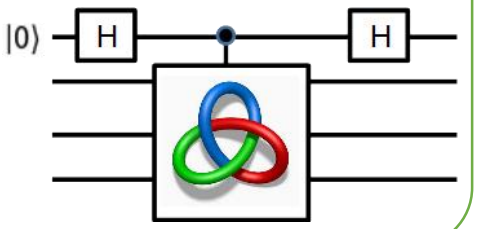


One clean qubit model

[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 QIC 2007]



ここじゃない
[Ambainis 2000]

古典 → ユニバーサル量子

明日誰かが古典の高速なアルゴリズムを発見するかも。。。

結果

One-clean qubitモデルがもし古典計算機で効率的にシミレートできたら
多項式階層が崩壊する

$$\mathrm{P} \subset \mathrm{NP} \subset \mathrm{NP}^{\mathrm{NP}} \subset \mathrm{NP}^{\mathrm{NP}^{\mathrm{NP}}} \subset \ldots$$

P=NPが信じられていないのと同様、多項式階層の崩壊は計算機科学では信じられていない
→　one-clean qubitモデルの古典シミレート不可能性

TM, Fujii, and Fitzsimons, PRL 2014
TM, PRA(R) 2017
Fujii, Kobayashi, TM, Nishimura, Tamate, and Tani, PRL 2018

長らく古典より速いだろうと信じられていたone-clean qubit modelの量子高速性を計算量理論の強固な基盤に基づいて初めて証明した！

セキュアクラウド量子計算

量子セキュリティ

「量子セキュリティ、量子暗号＝QKD」ではない！QKD以外にも様々なものがある！

・狭い意味での量子セキュリティ

→量子鍵配送、QKD　→　エンタングルメント必要ないので簡単（実現できている。）

・広い意味での量子セキュリティ

理論は昔からやられている

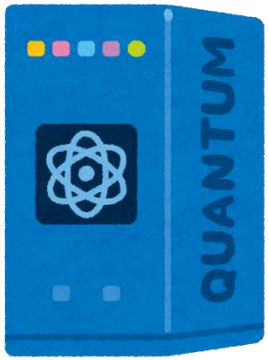
→セキュアクラウド量子計算、量子秘密分散、BC、Zero-knowledge、multi-party computing,
量子認証、量子ワンタイムパッド、etc.

エンタングルメント、量子メモリ等が必要。量子計算なみに難しい。
→計算には十分でない量子計算機でもセキュリティには有用だったりする→　今がチャンス！

SchaffnerのQIP2018トークスライド
https://qutech.nl/wp-content/uploads/2018/01/QIP18_ChristianSchaffner.pdf

Broadbent, Quantum cryptography beyond QKD
https://link.springer.com/article/10.1007/s10623-015-0157-4

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）

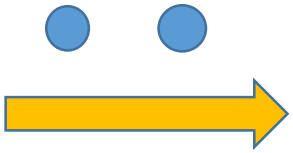
計算内容を秘密に保ったまま、量子クラウドに量子計算を委託できるか？

古典の場合でも、RSA暗号が提案されてから３０年間未解決問題であった
→２００９年にIBMのGentryがfully homomorphic encryptionを提案！

量子の場合も、可能であることが２００９年にBroadbent-Fitzsimons-Kashefiにより証明された！

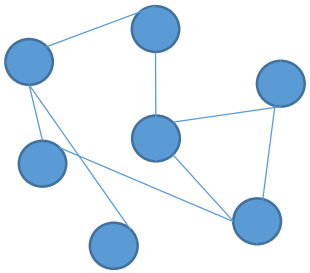
BFKプロトコル

アリス



量子ビット
（暗号鍵）

ボブ

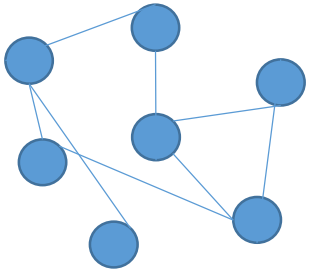


グラフ状態作る

アリス

古典通信
（暗号化）

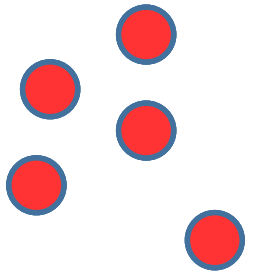
ボブ



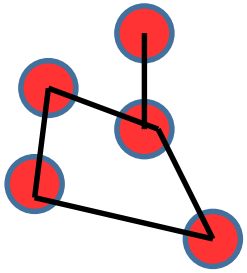
測定型量子計算実行

Broadbent, Fitzsimons, Kashefi, FOCS2009

量子論が正しいなら安全 (c.f. FHEは計算量的安全性)



ボブに送る



$\{e^{iZ\theta_j}|+\rangle\}_j$

$CZ(\otimes_{j=1}^{N} e^{iZ\theta_j}|+\rangle) = (\otimes_{j=1}^{N} e^{iZ\theta_j})|G\rangle$

測定角度の指示

$e^{iZ\delta_j}|\pm\rangle$ 基底で測定

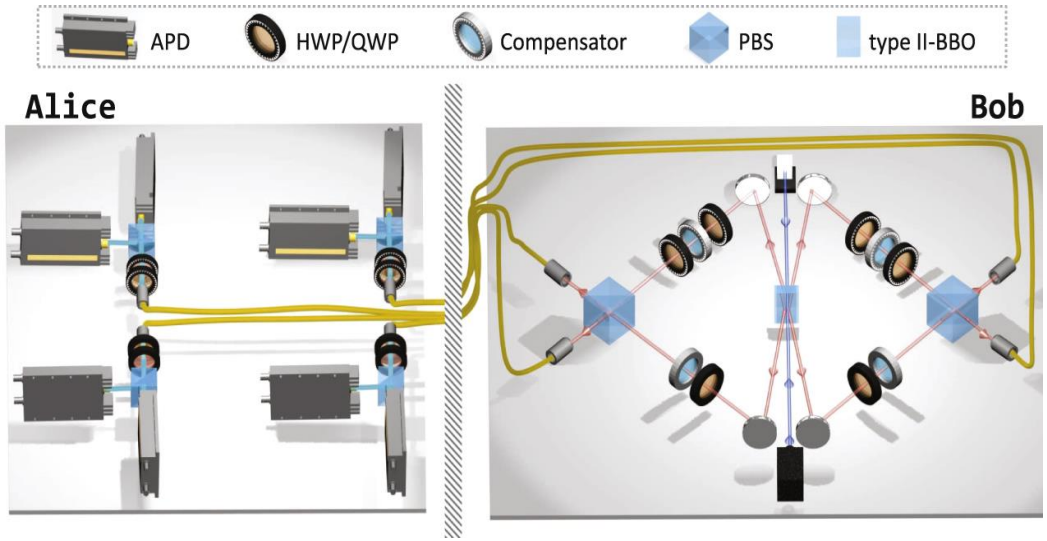
$\delta_j = \phi_j - \theta_j$

測定結果もらう

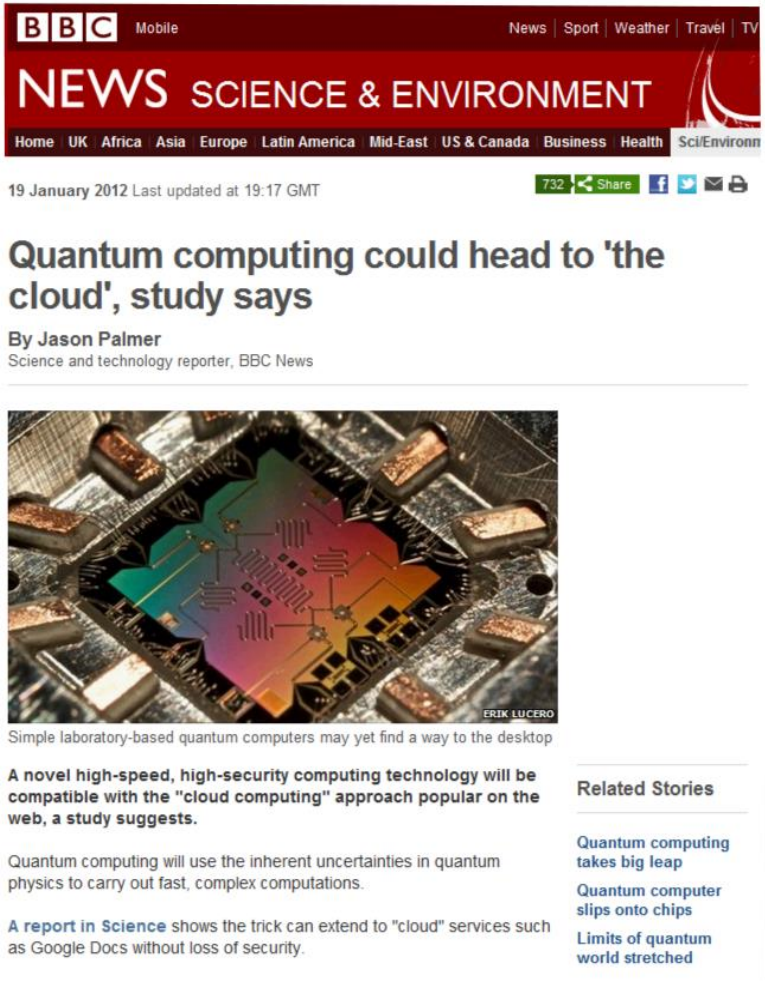
ボブは $\{\phi_j\}_j$ を知ることができない！！

もっとちゃんとした厳密な証明が知りたい方は[Dunjko et al. ASIACRYPTO2014]を参照。

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



BBC Mobile | News | Sport | Weather | Travel | TV

NEWS SCIENCE & ENVIRONMENT

Home | UK | Africa | Asia | Europe | Latin America | Mid-East | US & Canada | Business | Health | Sci/Environn

19 January 2012 Last updated at 19:17 GMT

732 Share

Quantum computing could head to 'the cloud', study says

By Jason Palmer
Science and technology reporter, BBC News

ERIK LUCERO

Simple laboratory-based quantum computers may yet find a way to the desktop

A novel high-speed, high-security computing technology will be compatible with the "cloud computing" approach popular on the web, a study suggests.

Quantum computing will use the inherent uncertainties in quantum physics to carry out fast, complex computations.

A report in Science shows the trick can extend to "cloud" services such as Google Docs without loss of security.

Related Stories

Quantum computing takes big leap
Quantum computer slips onto chips
Limits of quantum world stretched

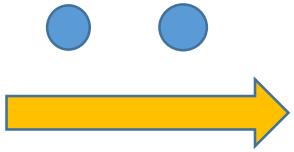
BFKプロトコルの問題点

1．Fault-tolerantなのか？

2．証明が複雑

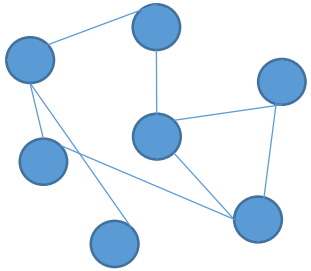
3．アリスが量子ビットを生成する必要がある

アリス



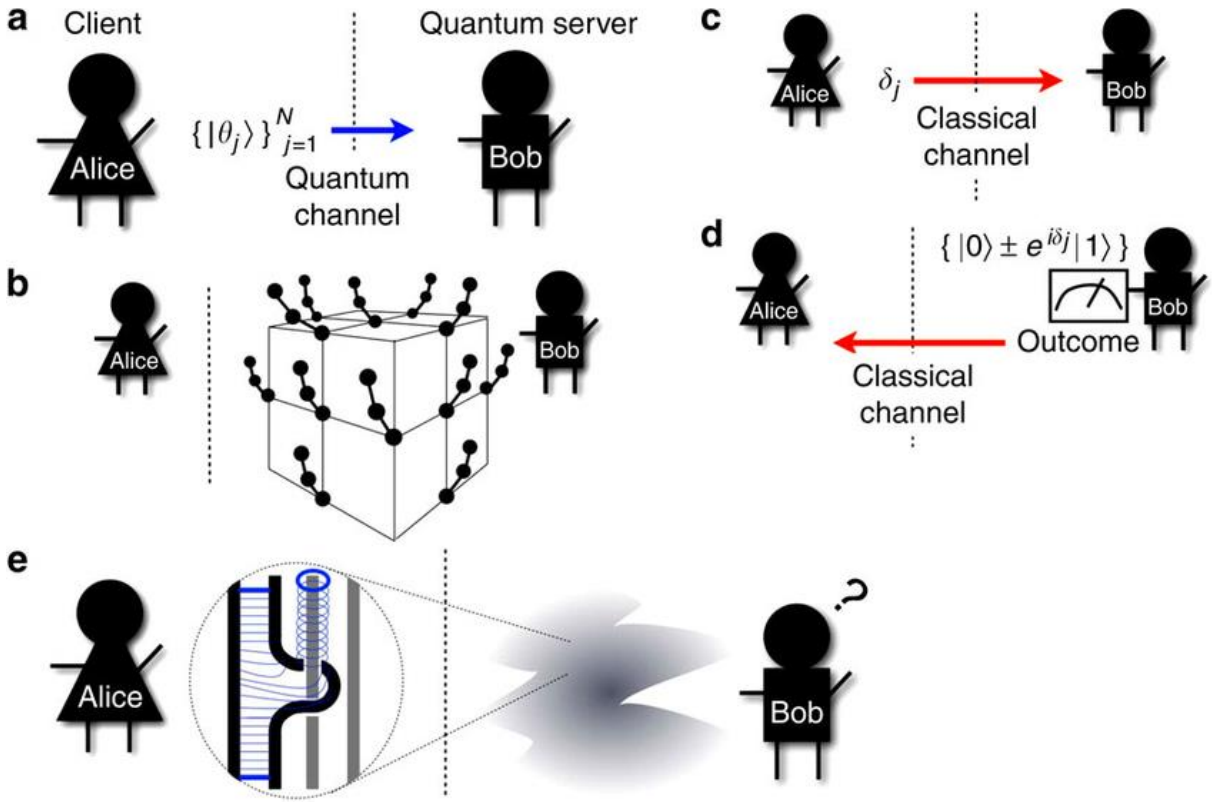
量子ビット送る

ボブ



グラフ状態作る

トポロジカルプロトコル



TM and Fujii, Nature Communications 2012

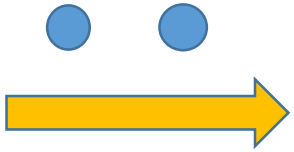
BFKプロトコルの問題点

1．Fault-tolerantなのか？

2．証明が複雑

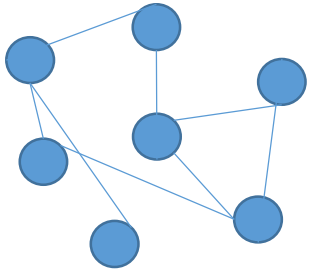
3．アリスが量子ビットを生成する必要がある

アリス



量子ビット送る

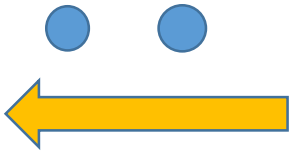
ボブ



グラフ状態作る

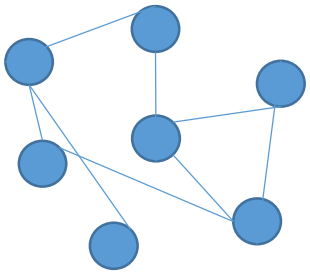
Measurement-only プロトコル

アリス
測定する

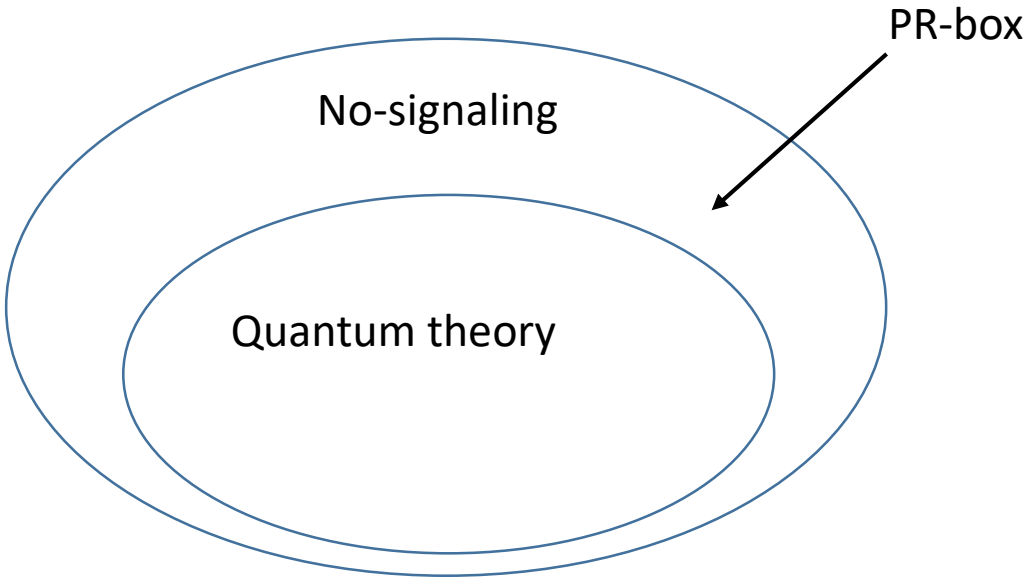


量子ビット送る

ボブ



グラフ状態作る



メリット：

測定は簡単な場合が多い
量子論より強い安全性
証明がシンプル（安全性を無視できる）
Device-independent

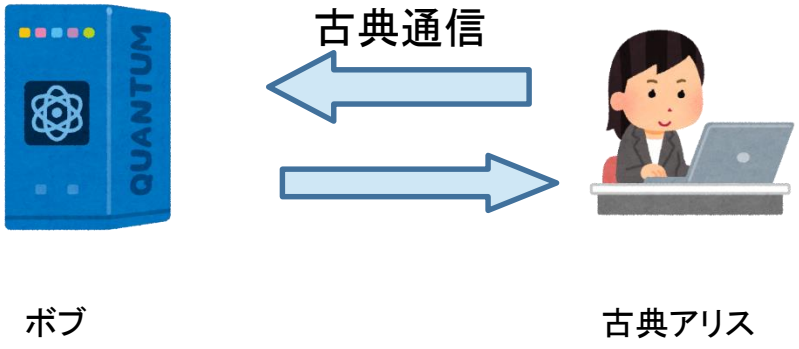
TM and Fujii, PRA(R) 2013

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、

その他の結果

通信量の効率化 [Giovanetti, Maccone, TM, and Rudolph, PRL 2013]

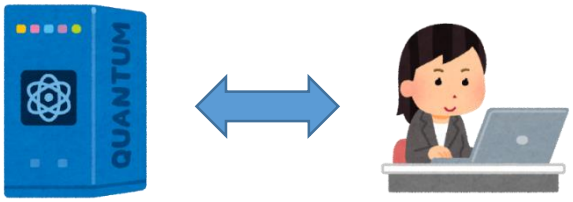
エンタングルメント蒸留 [TM and Fujii, PRL 2013]

アンシラ駆動型 [Sueki, Koshiba, and TM, PRA(R) 2013]

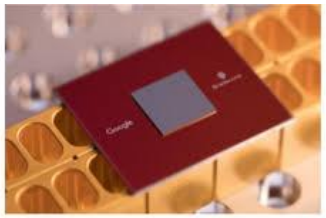
連続変数 [TM, PRL 2012]

量子計算の検証

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？

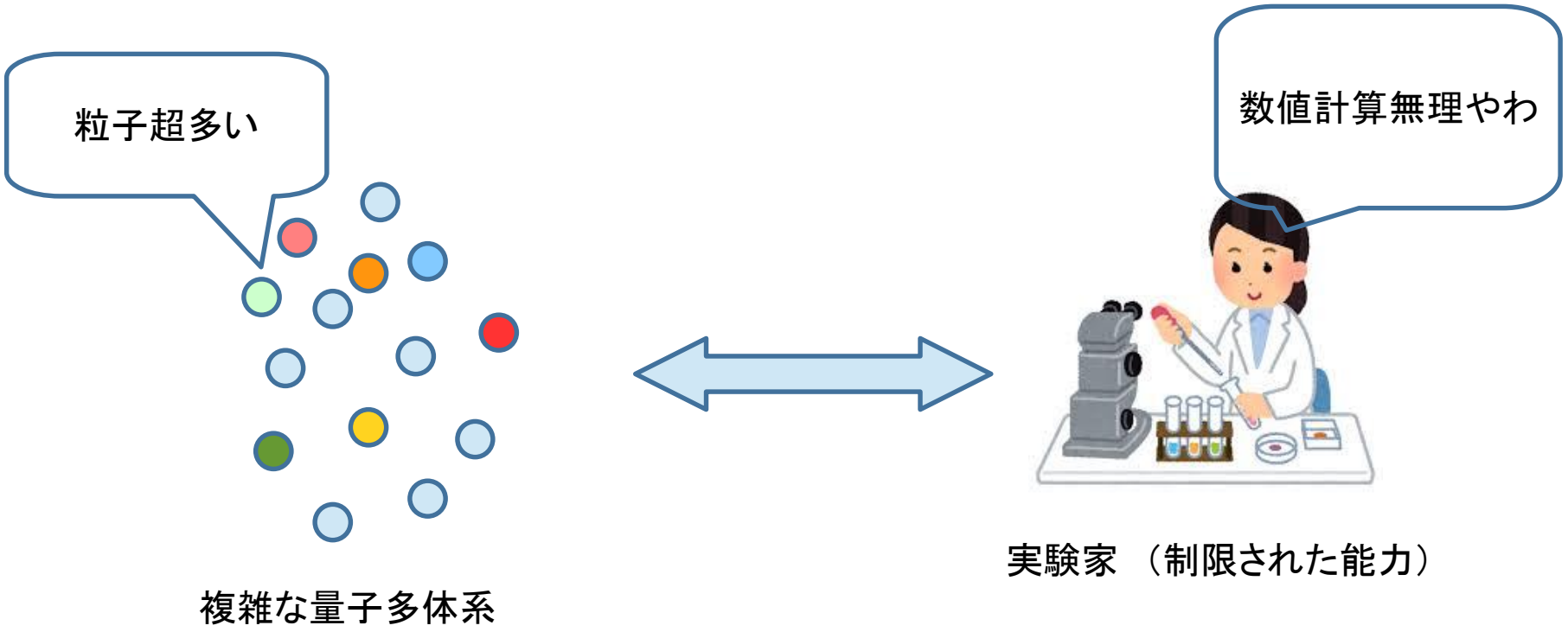


Google等は量子スプレマシーの領域に達する→どうやって検証するのか？

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

量子論基礎への応用



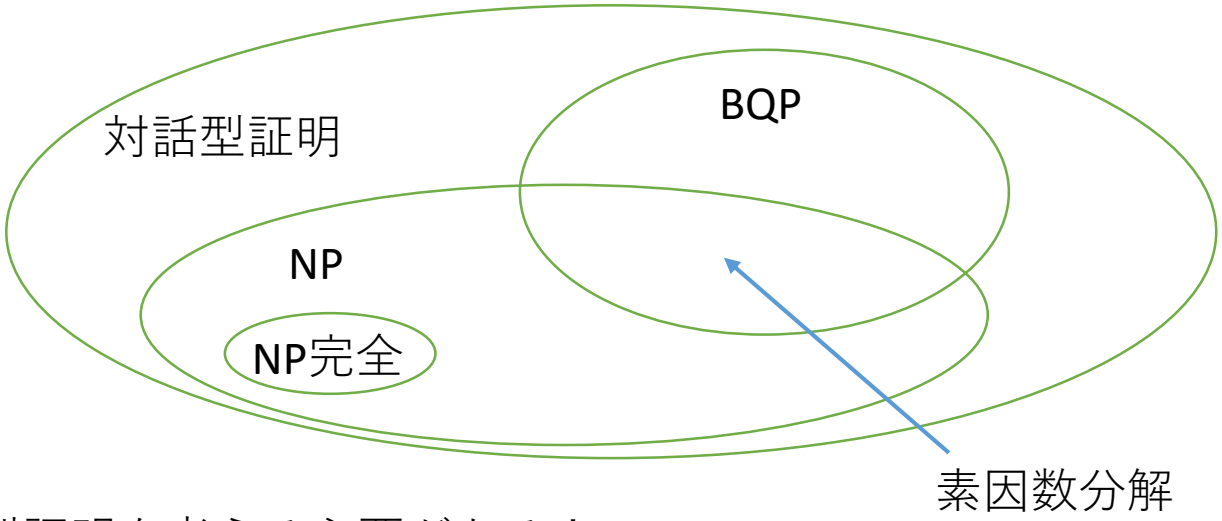
実験家は、量子多体物理理論が本当に正しいのか検証できるのか！？

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！

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

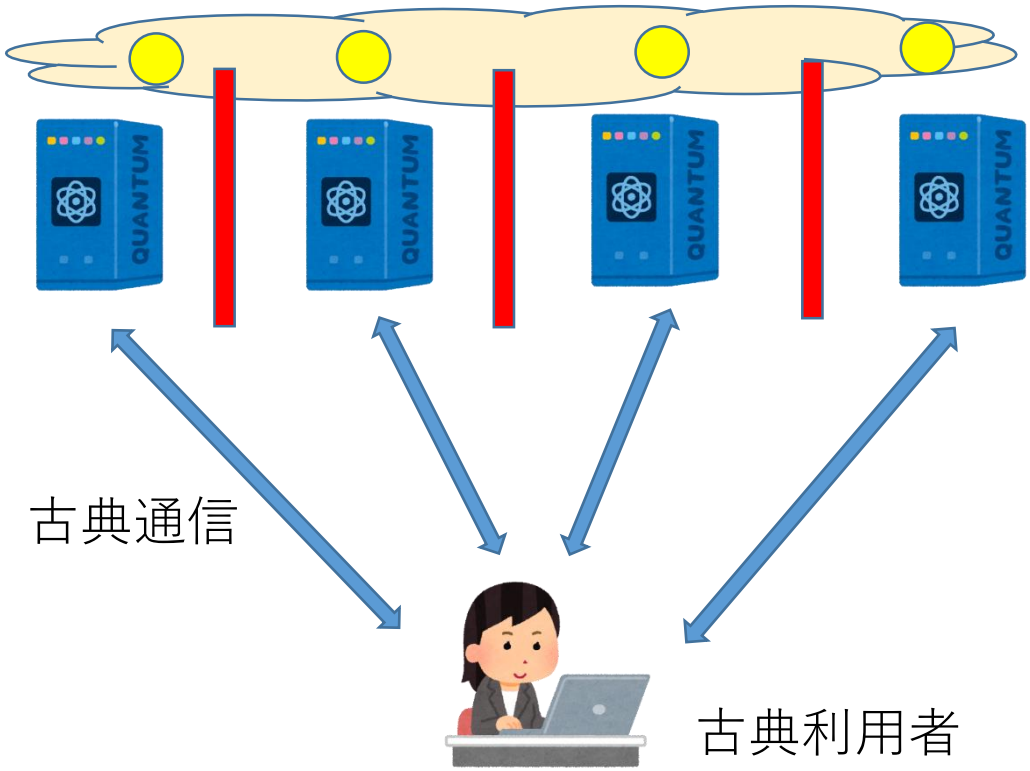
通信路（古典）

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！

サーバーが複数



サーバー同士はエンタングルメントをシェアしてる。
通信はできない。

Reichardt, Unger, Vazirani, Nature 2013
McKague Theory of Computing 2016
Zi, STOC16

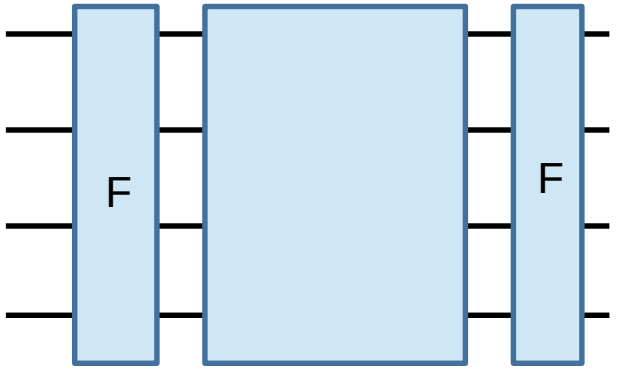
Experiment: Jian-Wei Pan, PRL2017

サーバー間で通信ができないというのは不自然

特定の問題なら検証可能

FH_2に注目

理由:
Simon, Shor, IQPなど、重要なクラス。
FH_1は古典なので、最弱の量子？
FH_2の出力確率はBPPで計算可能。



→ zの生成はサーバーがやる
　p_zの値の検証はユーザーがやる

$$p_z = \frac{1}{2^N} \sum_x f(x)$$

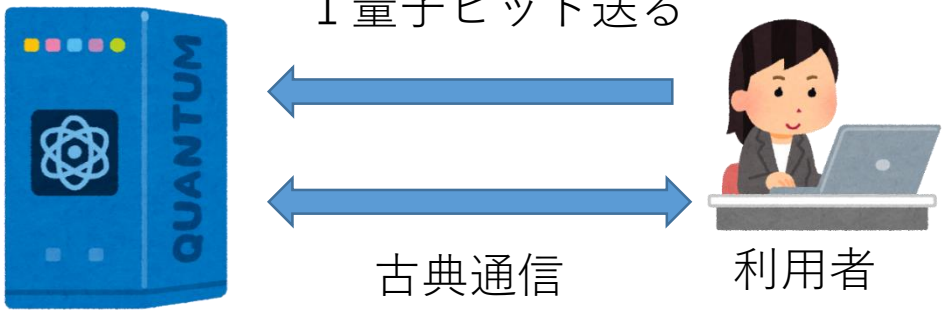
$$Pr\left[\left|\frac{1}{T}\sum_{j=1}^{T} f_j - E[f_j]\right| \leq \epsilon\right] \geq 1 - 2e^{-\frac{T\epsilon^2}{2}}$$

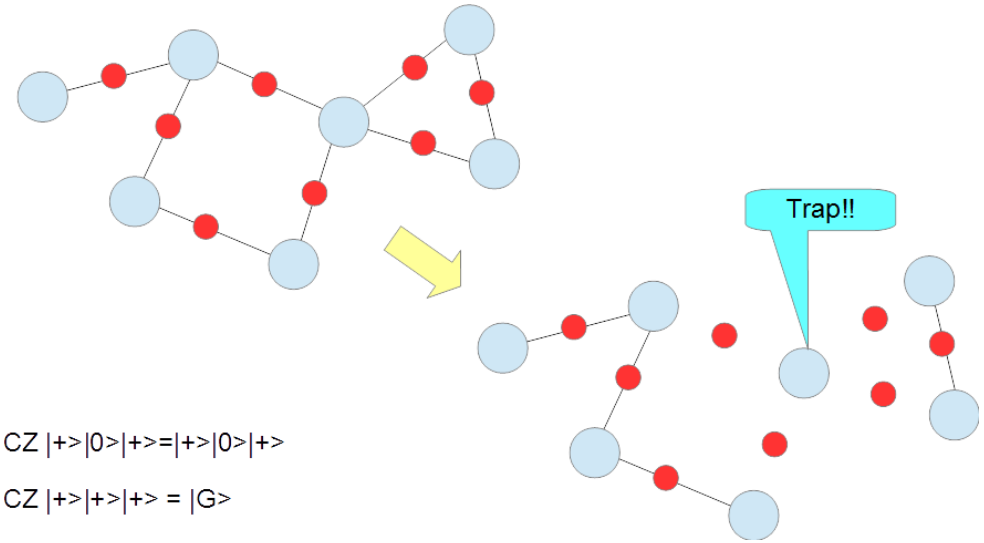
以下のようなプロミス問題は

1.任意の回路ならBQP完全
2. FH_2ならMA with BQP Merlinに入る [TM, Takeuchi, Nishimura, 2017]

YES: there exists z such that |p_z-q_z|>a
NO: for any z, |p_z-q_z|<b

利用者が少し量子なら可能





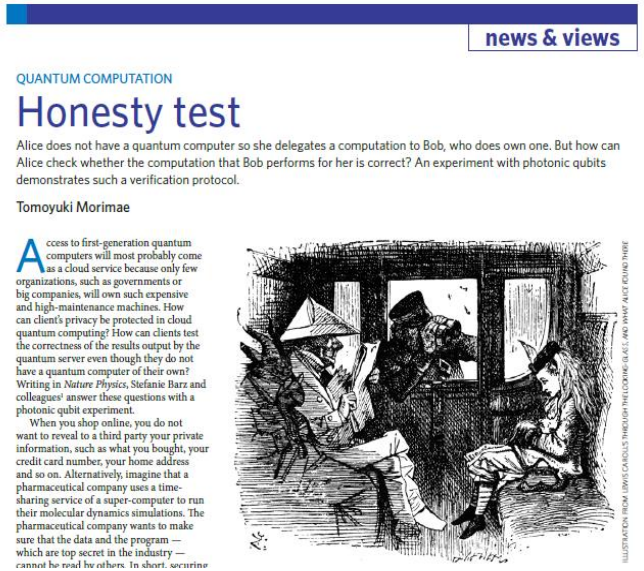
CZ CZ |+>|0>|+>=|+>|0>|+>

CZ CZ |+>|+>|+> = |G>

理論:

Fitzsimons and Kashefi, PRA 2017

TM, Phys. Rev. A (R) 2014



news & views

QUANTUM COMPUTATION

Honesty test

Alice does not have a quantum computer so she delegates a computation to Bob, who does own one. But how can Alice check whether the computation that Bob performs for her is correct? An experiment with photonic qubits demonstrates such a verification protocol.

Tomoyuki Morimae

Access to first-generation quantum computers will most probably come as a cloud service because only few organizations, such as governments or big companies, will own such expensive and high-maintenance machines. How can client's privacy be protected in cloud quantum computing? How can clients test the correctness of the results output by the quantum server even though they do not have a quantum computer of their own? Writing in *Nature Physics*, Stefanie Barz and colleagues[1] answer these questions with a photonic qubit experiment.

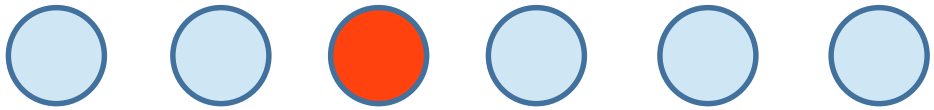
When you shop online, you do not want to reveal to a third party your private information, such as what you bought, your credit card number, your home address and so on. Alternatively, imagine that a pharmaceutical company uses a time-sharing service of a super-computer to run their molecular dynamics simulations. The pharmaceutical company wants to make sure that the data and the program — which are top secret in the industry — cannot be read by others. In short, securing

実験:

Barz et al. Nature Phys. 2013

TM, Nature Phys. N&V 2013

量子誤り訂正符号を使う



トラップに触れる確率＝1/N

量子誤り訂正符号をかませる

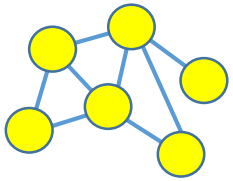
少数キュービットだけ触ってもただのエラーとして訂正(無視）される

内容を変えるにはd個以上のキュービットに触れる必要がある

→ トラップに触れないでロジカルビットを変えれる確率=2^{-d}

１量子ビット
づつ送る

１量子ビットづつ測定
（スタビライザーテスト）



$|G\rangle$

ρ

スタビライザーテストにパス
したら高い確率で

$$\langle G|\rho|G\rangle \simeq 1$$

（i.i.d.でなくてもquantum de Finetti定理使えばよい）

$$g_i|G\rangle = |G\rangle$$

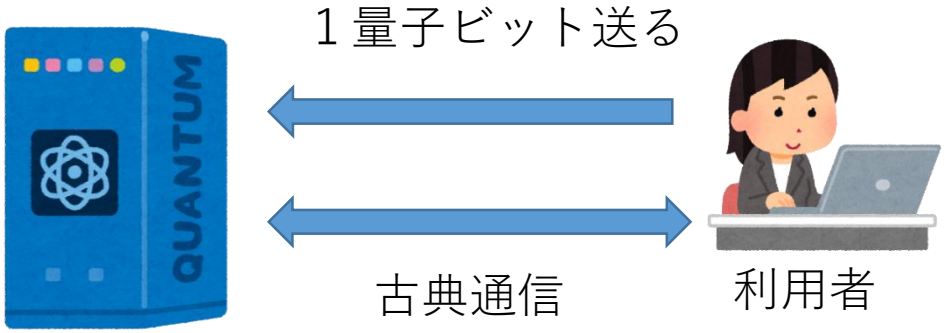
$$|G\rangle\langle G| = \prod_i \frac{I+g_i}{2}$$

$$= \frac{1}{2^n}\sum_k s_k$$

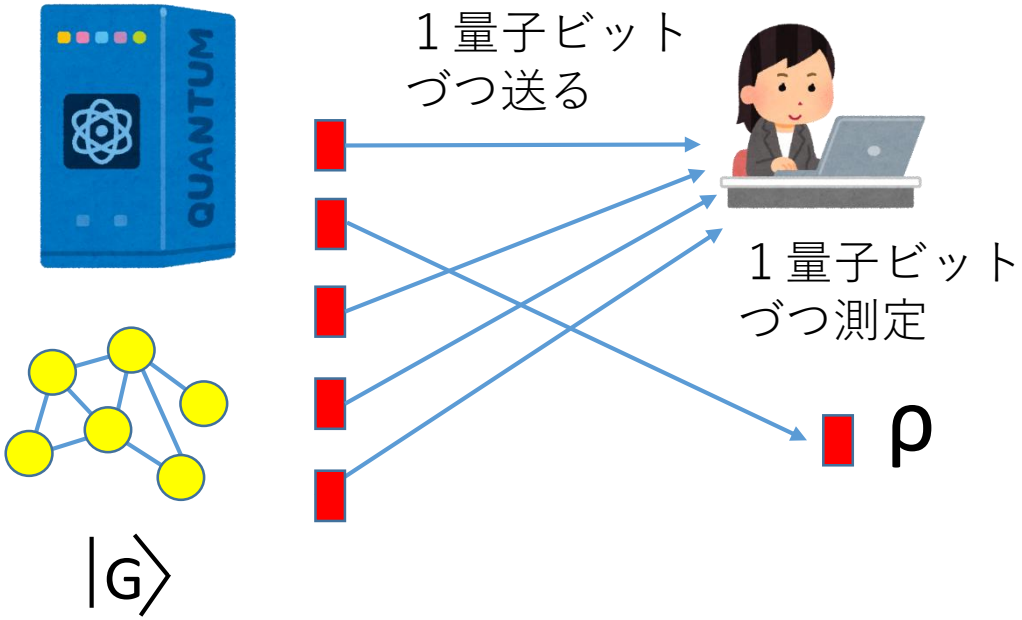
理論:
Hayashi and TM, PRL 2015
Takeuchi and TM, PRX 2018

実験:
Greganti, Roehsner, Barz, TM, and Walther, NJP 2016

計算と検証を分離できるか？

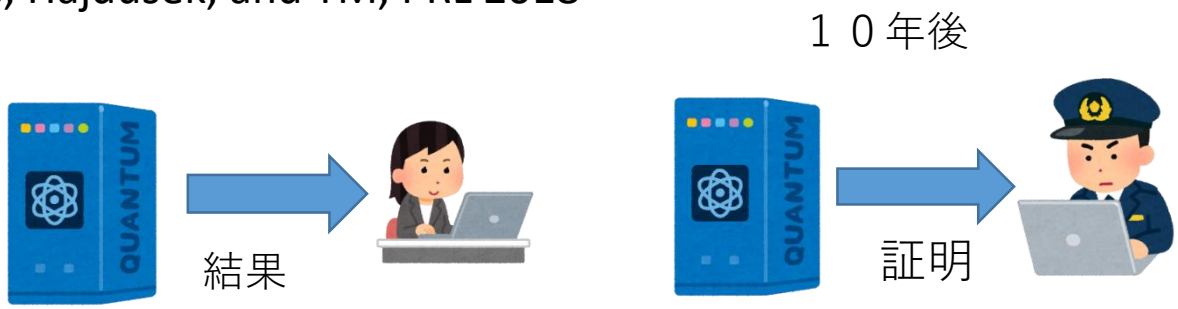


検証は検証で、計算は計算で切り離してできるのか？



Post hoc 検証

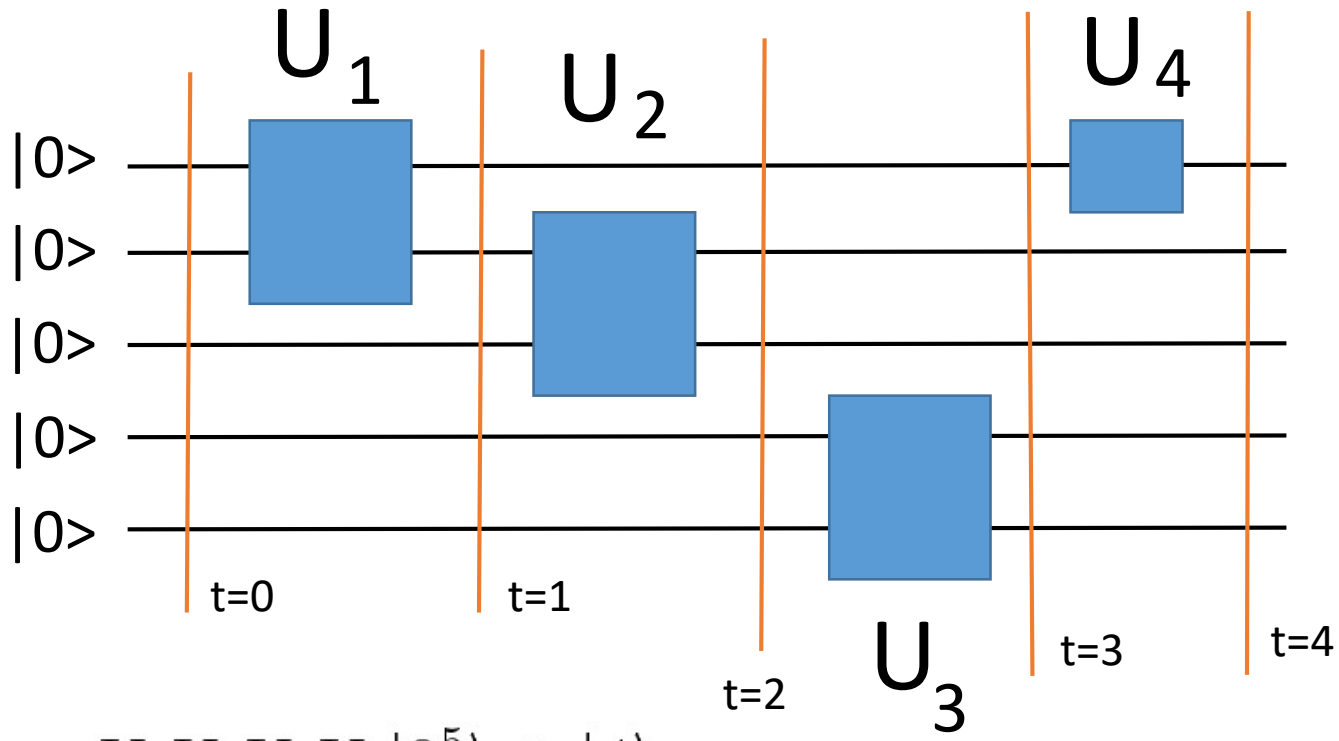
Fitzsimons, Hajdusek, and TM, PRL 2018



量子計算の正しさが事後的にチェックできる！

計算本体と検証を分離できる！
→量子計算そのものにはオーバーヘッドがない！

量子計算を状態にマップ



$$
\begin{aligned}
|\Psi\rangle \quad = \quad & U_4U_3U_2U_1|0^5\rangle \otimes |4\rangle \\
& + U_3U_2U_1|0^5\rangle \otimes |3\rangle \\
& + U_2U_1|0^5\rangle \otimes |2\rangle \\
& + U_1|0^5\rangle \otimes |1\rangle \\
& + |0^5\rangle \otimes |0\rangle
\end{aligned}
$$

history stateと呼ばれている
[Feynmann and Kitaev]

History stateは基底状態！

$$
\begin{aligned}
|\Psi\rangle \quad = \quad & U_4U_3U_2U_1|0^5\rangle \otimes |4\rangle \\
& + U_3U_2U_1|0^5\rangle \otimes |3\rangle \\
& + U_2U_1|0^5\rangle \otimes |2\rangle \\
& + U_1|0^5\rangle \otimes |1\rangle \\
& + |0^5\rangle \otimes |0\rangle
\end{aligned}
$$

$$H_0 = (I - |0^5\rangle\langle 0^5|) \otimes |0\rangle\langle 0|$$

$$H_0|\Psi\rangle = 0$$

初期状態の正しさをチェック

$$H^1_{prop} = I \otimes |1\rangle\langle 1| + I \otimes |2\rangle\langle 2| - U_2 \otimes |2\rangle\langle 1| - U_2^\dagger \otimes |1\rangle\langle 2|$$

$H^1_{prop}|\Psi\rangle = 0$　プロパゲーションのチェック

$$H = H_0 + \sum_{t=0}^{4} H^t_{prop}$$

$$H = H_0 + H_{prop}$$

$$H_0 = |0^n\rangle\langle 0^n| \otimes |t=0\rangle\langle t=0| \qquad H_{prop} = \sum_{t=0}^{T-1} H_{prop}^t$$

時間をエンコードするのにlogT量子ビット必要

摂動法により、最終的に２体のXZハミルトニアンにできる！

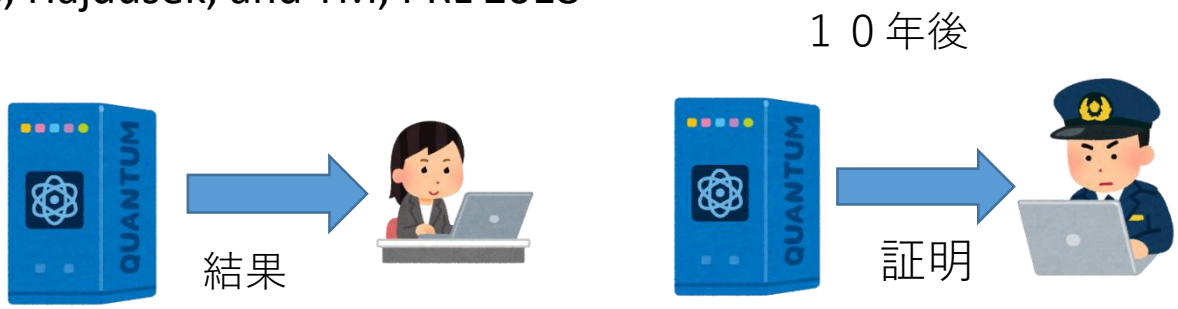
$$H = \sum_i (\alpha X_i X_{i+1} + \beta Z_i Z_{i+1} + \gamma X_i + \delta Z_i)$$

つまり、２体XZハミルトニアンの基底状態は、量子計算をエンコードしている！

（例：断熱量子計算）

Post hoc 検証

Fitzsimons, Hajdusek, and TM, PRL 2018

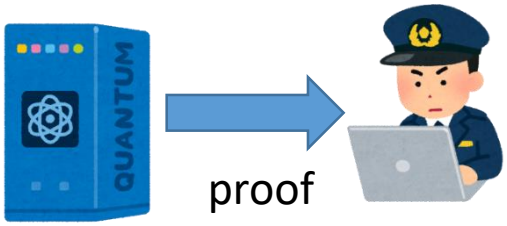


History stateを送ればよい

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

エネルギーの測定は１量子ビットでできる！
[TM, Nagaj, Schuch, PRA2016]

Fault-toleranceが簡単



CSSコードはXとZのロジカル測定が簡単！
（transversalにできる。）

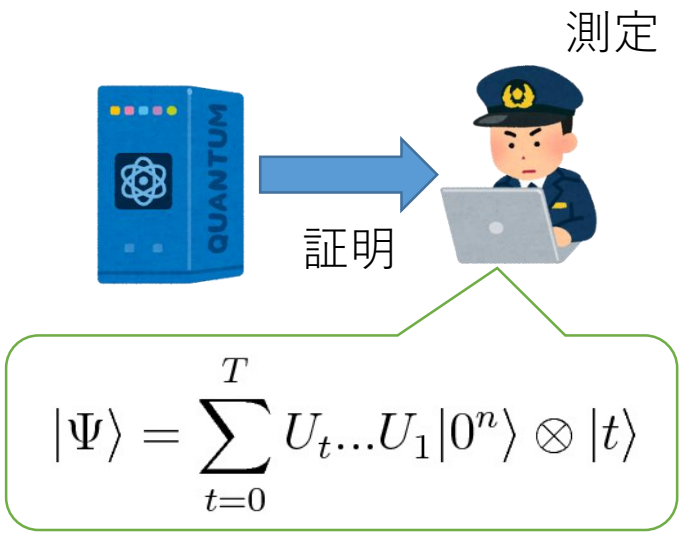
$$|\Psi\rangle = \sum_{t=0}^{T} U_t ... U_1 |0^n\rangle \otimes |t\rangle$$

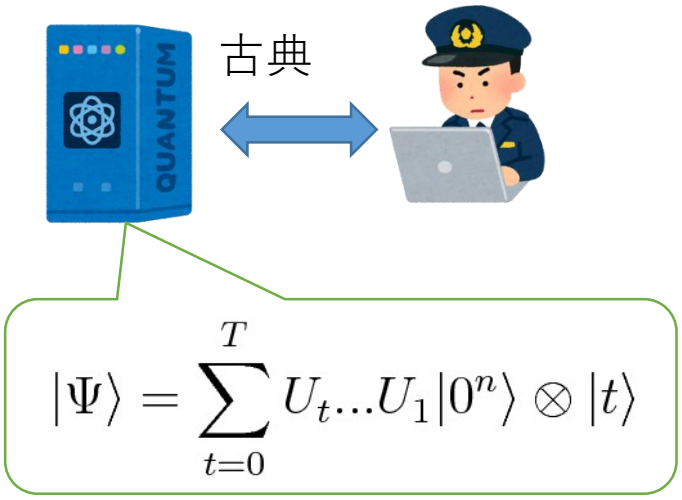
$$H = \sum_i (\alpha X_i X_{i+1} + \beta Z_i Z_{i+1} + \gamma X_i + \delta Z_i)$$

Post hocプロトコルが利用された

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！





Rational proof system

サーバーは邪悪ではなく、自己の利益を最大化するように行動する

[Azar and Micali, STOC 2012]

If $x \in L$ then b=1

If $x \notin L$ then b=0

BQP server

b

$ (b)

BPP verifier

$$\langle \$ \rangle_b = b p_{acc} + (1-b)(1-p_{acc})$$

If $x \in L$ then p_acc > 2/3

If $x \notin L$ then p_acc < 1/3

平均利益を最大化するには、サーバーは正しいbを送る必要がある!
→ もしサーバーが欲張りなら、答えの正しさは常に保証される！

TM and Nishimura, arXiv:1804.08868

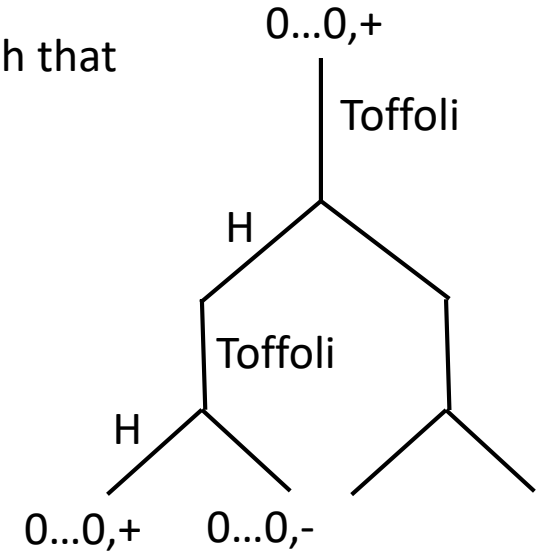
Assume L is in BQP. Then there exists poly-time quantum circuits W such that

$$p_{acc} = \langle 0^n | W | 0^n \rangle$$

We assume that W consists of only Hadamard and Toffoli

From W, we construct a non-deterministic algorithm such that

$$\langle 0^n | W | 0^n \rangle = \frac{A - R}{\sqrt{2^h}}$$



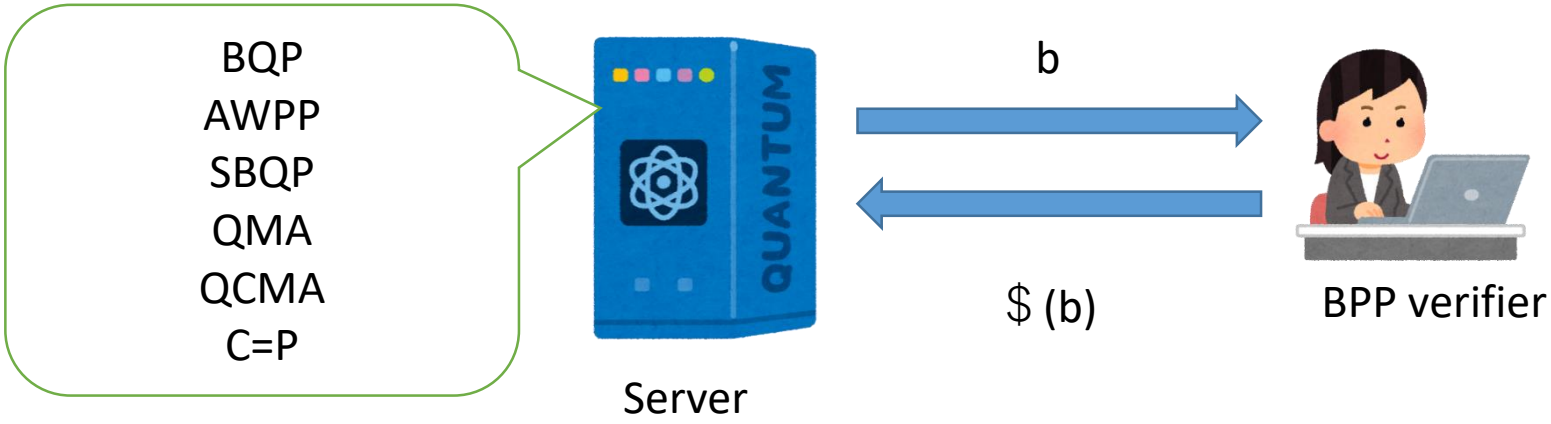
A: number of accepting paths
R: number of rejecting paths
h: number of Hadamard gates in W

Probabilistically simulate the non-deterministic machine

$$q_A = \frac{A}{2^h}, \quad q_R = \frac{R}{2^h}$$

$$\langle 0^n | W | 0^n \rangle = \frac{A - R}{\sqrt{2^h}} = \sqrt{2^h}(q_A - q_R)$$

他の計算量クラスへの拡張



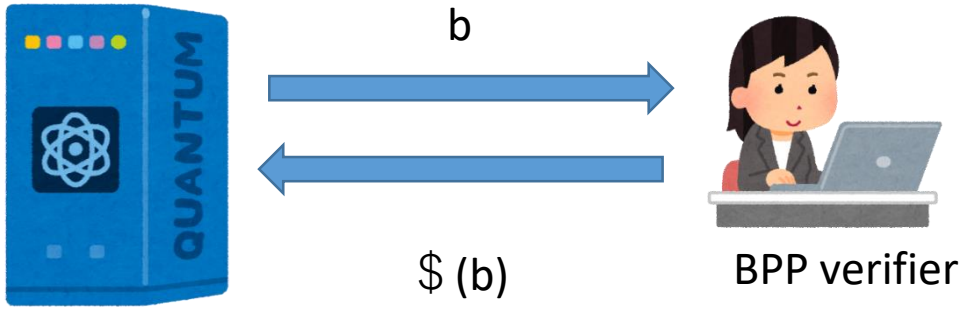
Simulate NDTM of GapP function probabilistically

Extra factors are renormalized into the reward.

To maximize the profit, the server has to send the correct b!

TM and Nishimura, arXiv:1804.08868

報酬は指数的に増加してしまう



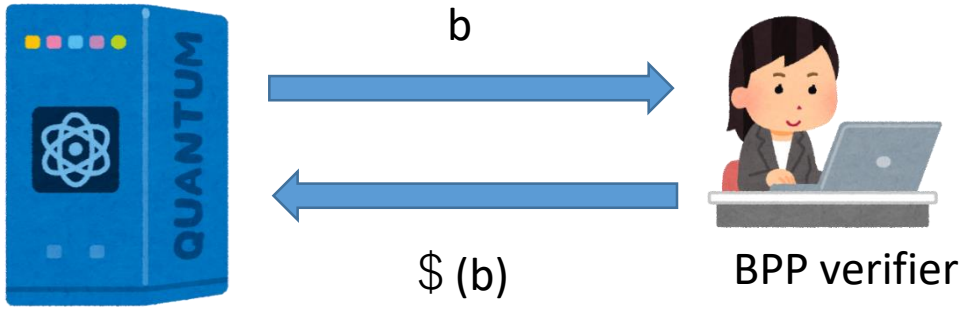
$$\$ = O(\sqrt{2^h})$$

BQP=BPPでない限り、これは避けれない

$$\langle \$ \rangle_b = \sum_w p(b,w)\$(b,w)$$

If |$(b,w)|<poly, the BPP verifier can estimate <$>_b by herself
→BQP is in BPP!

Open problem



$$\$ = O(\sqrt{2^h})$$

Can we make |$|<const?

One possible approarch: consider multiple rounds

まとめ

１．量子スプレマシー

弱い量子計算機であっても古典より強いことを計算量理論の強力な基盤に基づいて示す研究
→Google等が実現！？

量子と古典の境界を計算の視点から探るという
ファンダメンタルな研究でもある！

２．セキュアクラウド量子計算、量子計算の検証

ほぼ古典の利用者であっても、量子クラウドを安全に利用できる
→IBMがクラウドサービスを開始

対話型証明という基礎的な重要性もある！

END