量子計算の基礎

情報理論研究会

森前智行
(京都大学基礎物理学研究所)

４５分+５分

内容

- 量子計算基礎（２５分）
- 量子スプレマシー（１０分）
- 量子暗号（ブラインド量子計算・量子計算の検証）（１０分）

量子計算基礎

全般的な話
Clifford+Tパラダイム

量子計算と古典計算の違い

古典（確率的）計算

$$(p_1, \ldots, p_n) \rightarrow (p'_1, \ldots, p'_n)$$

計算機の状態：確率ベクトル
計算ステップ：確率行列をかける
最後に計算機がkという状態にいる確率：p_k

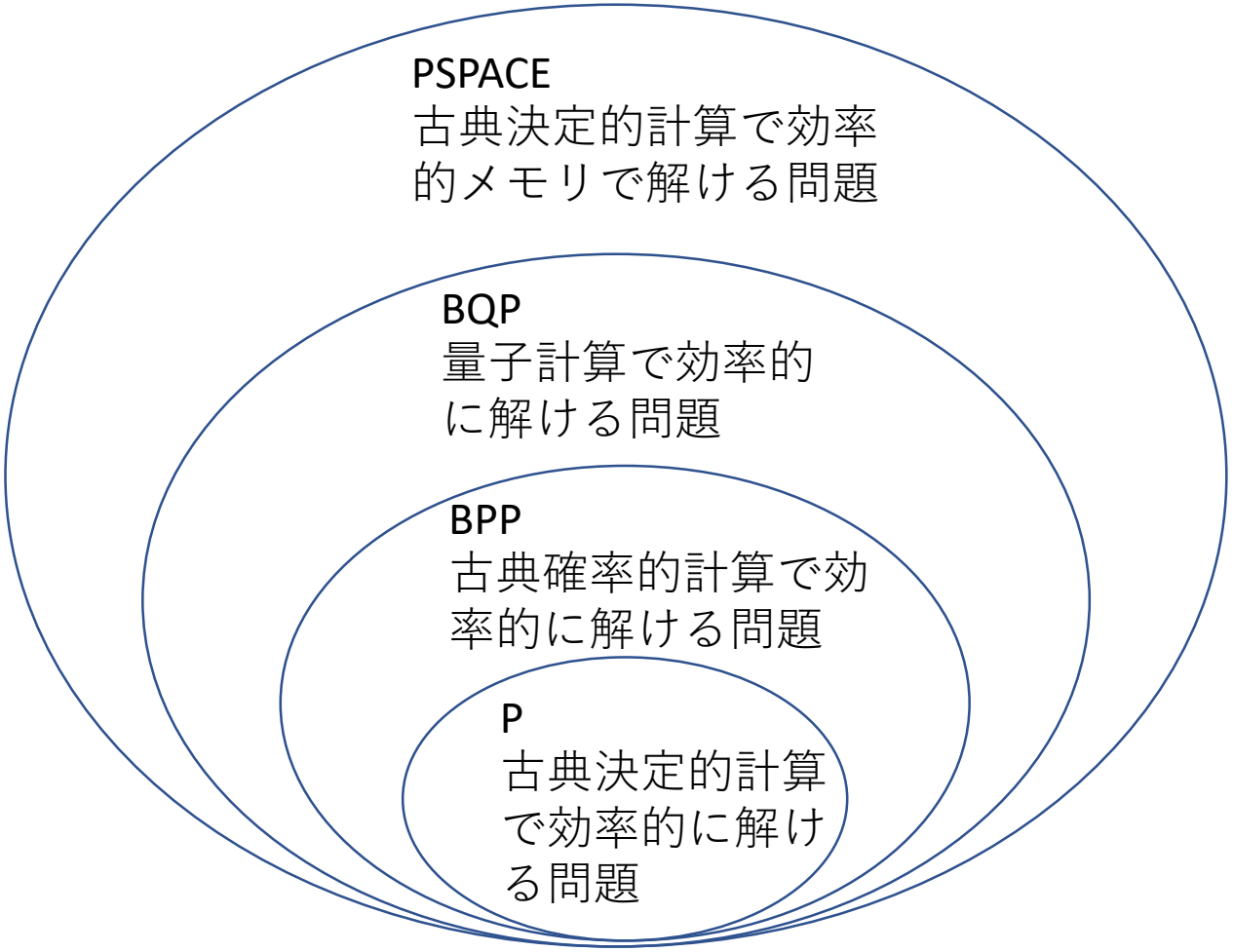
$$\sum_i p_i = 1$$

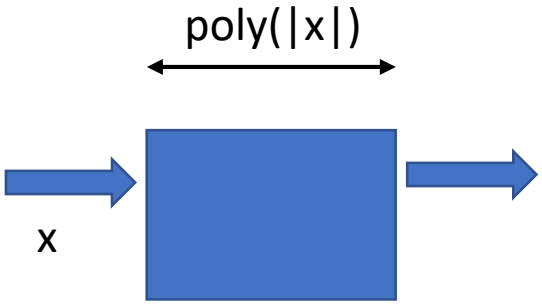
量子計算

計算機の状態：状態ベクトル　（複素線形空間のL2長さ１のベクトル）
計算ステップ：ユニタリ行列をかける
最後に計算機がkという状態にいる確率：$|c_k|^2$

$$\sum_i |c_i|^2 = 1 \quad (c_1, \ldots, c_n) \rightarrow (c'_1, \ldots, c'_n)$$

なぜこんな変な理論？→実験が説明できるから。





分かること１：BQP⊆PSPACE　量子計算機はなんでも解けるわけではない

分かること２：BQP≠BPP　→　P≠PSPACE　量子が古典より速いことを示すのは超難しい

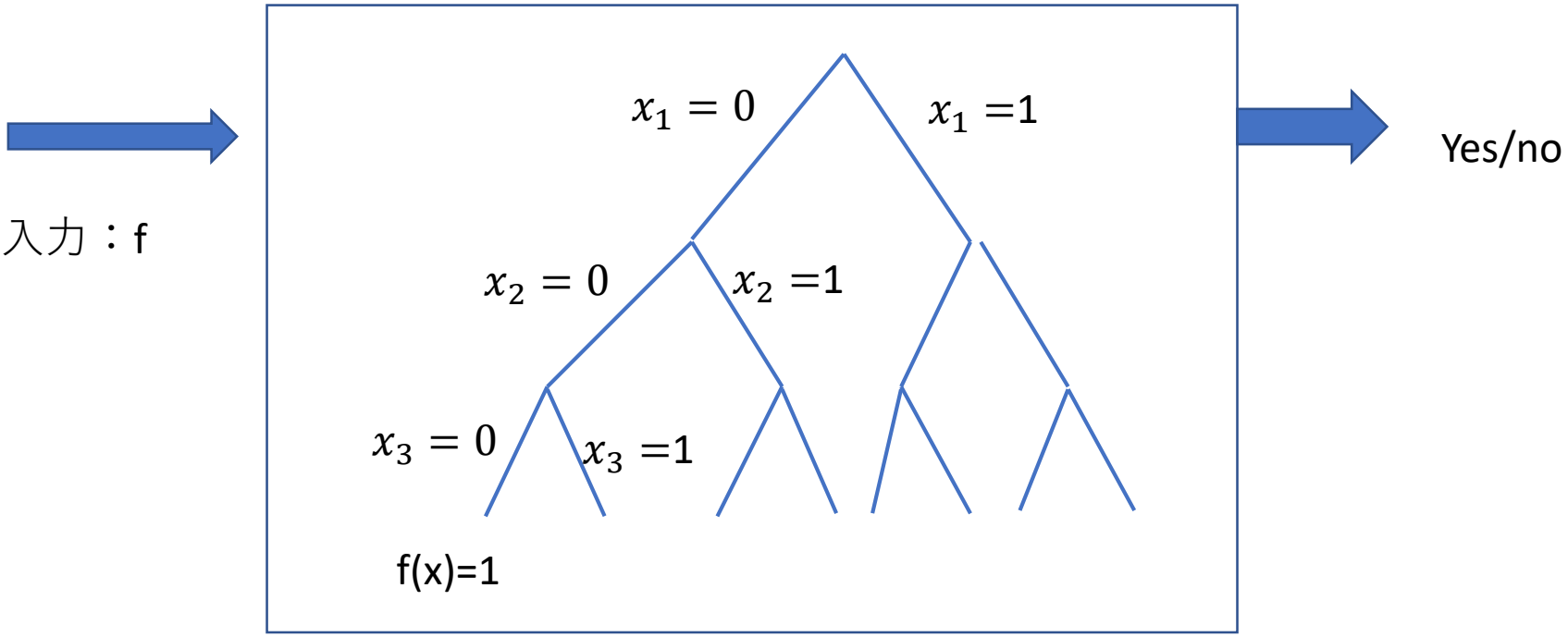
そうはいっても、皆量子計算は古典計算より速いと信じている
→後の量子スプレマシーで解説

NP

$$f : \{0,1\}^n \ni x \mapsto f(x) \in \{0,1\}$$ f(x)はpoly(|x|)時間で計算可能

f(x)= 1 なるxは存在するか？　　しらみつぶしにやると2^n時間かかる

NP：並行宇宙に分かれて計算できる架空のマシンで効率的に解ける問題の集合

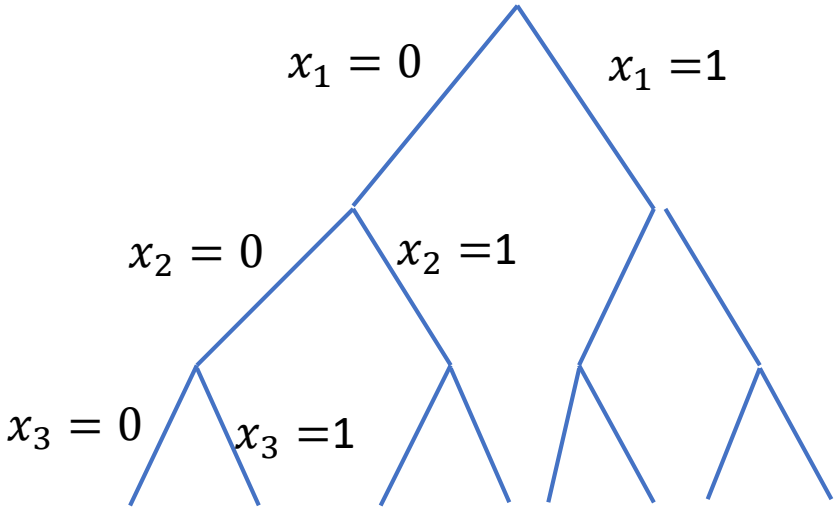


NPのもう一つの定義

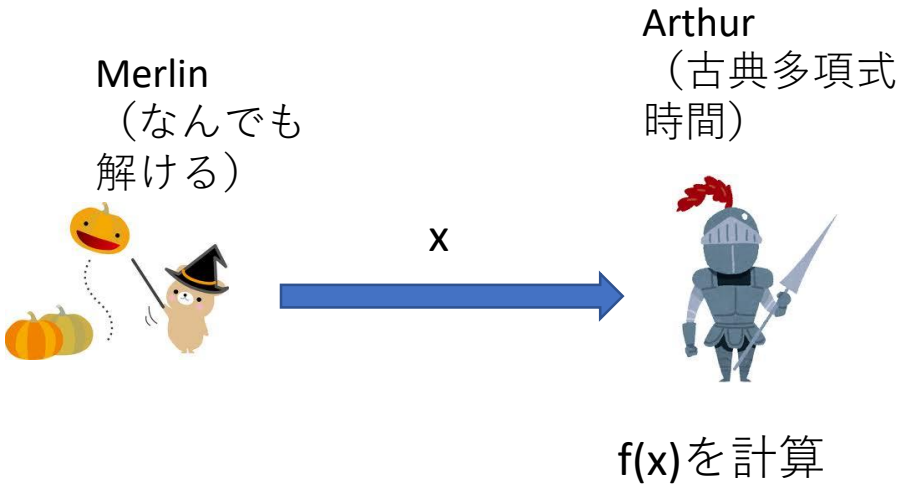
$$f : \{0,1\}^n \ni x \mapsto f(x) \in \{0,1\}$$

f(x)= 1 なるxは存在するか？

NP：答えの正しさは効率的にチェックできる問題の集合

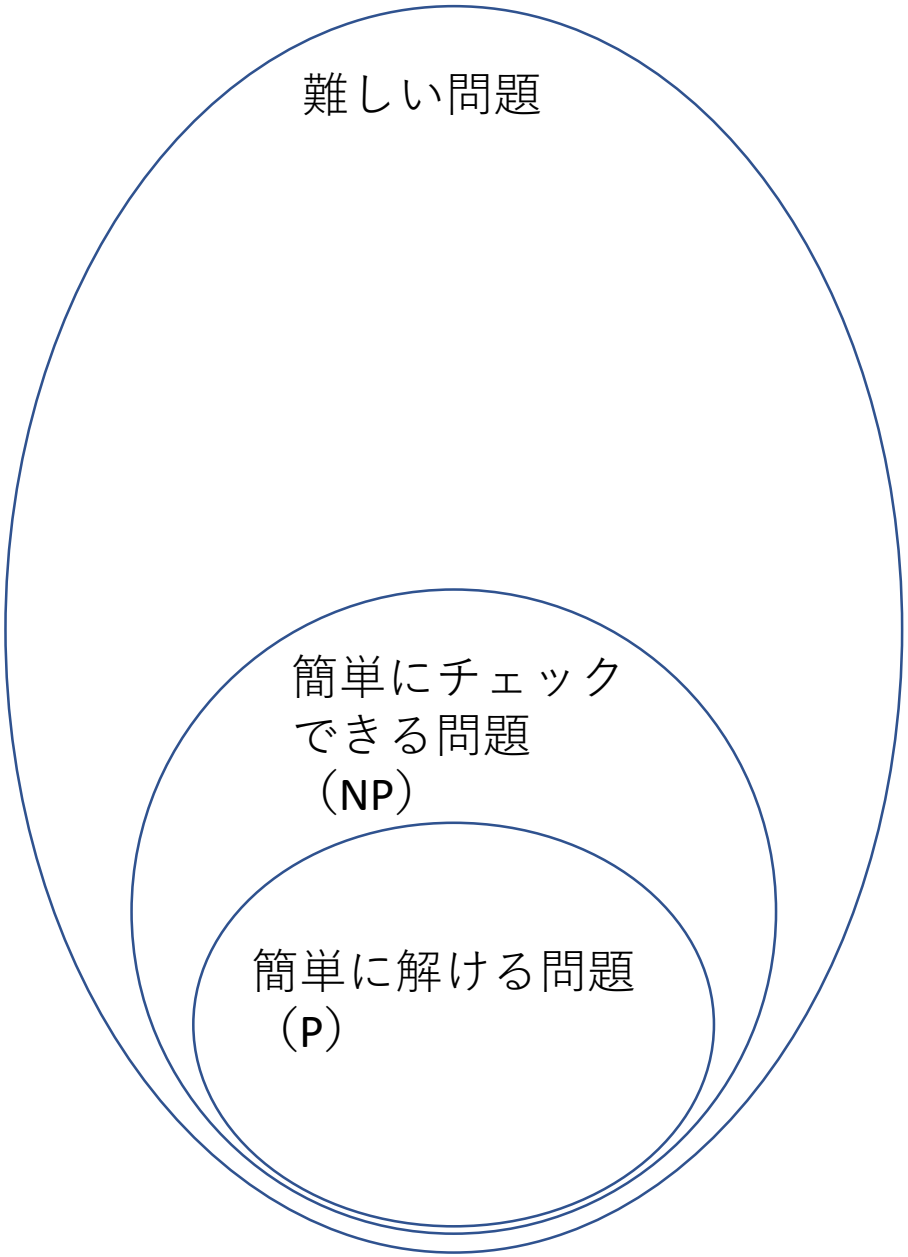


f(x)=1



MerlinとArthurが存在して
YES:あるMerlinのメッセージに対し
Arthurは必ずYESを出す
NO：どんなMerlinのメッセージに対して
もArthurはYESを出さない

NPは計算機科学において非常に重要な概念



まず気になるのは簡単に解けるか？

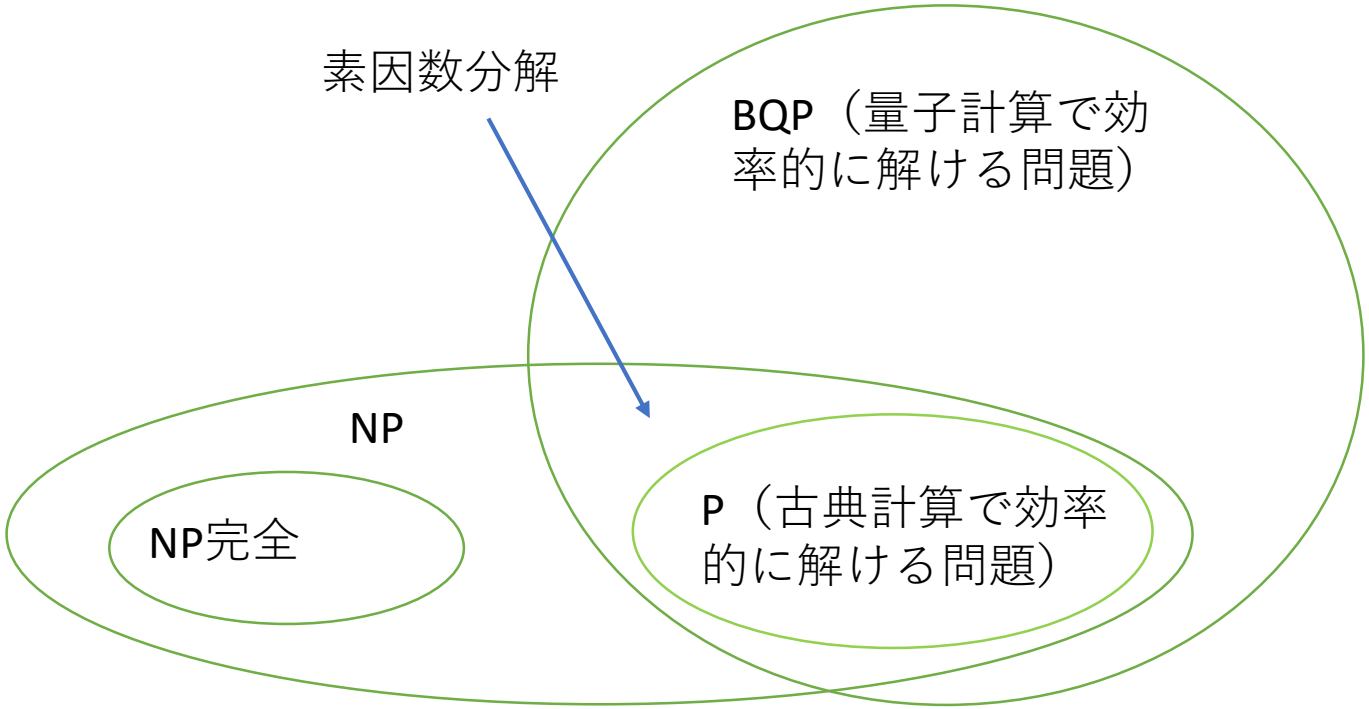
→多くの問題は簡単に解けない

難しい問題の中でも、「簡単にチェックできる」という良い性質を持つサブクラスは非常に重要

アルゴリズム、暗号。。。

簡単な問題は暗号には使えない。かといって、難しい問題も扱えない。難しいけど、何かは簡単にできる、という非対称性がうれしい！

NPと量子計算の関係

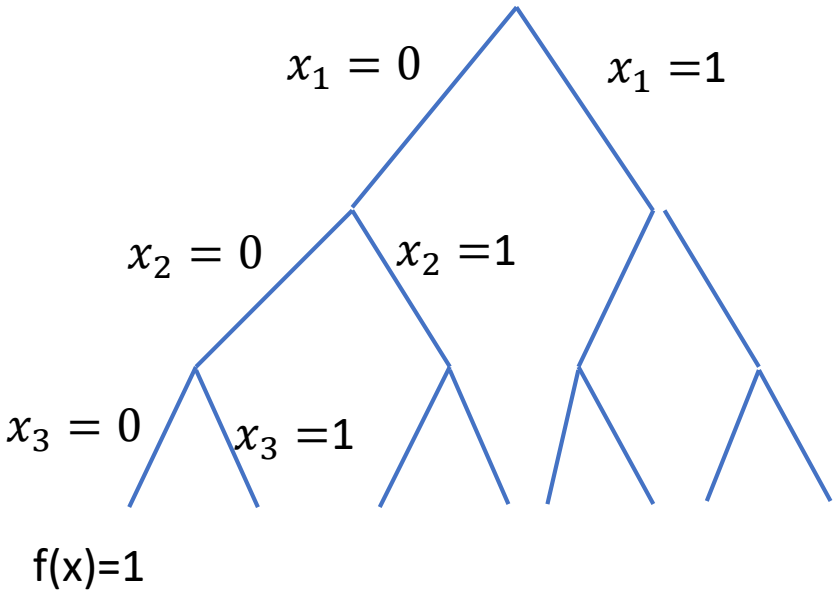


NP完全問題：NPの中で最も難しい問題（任意のNP問題がこれに帰着できる）
NP完全問題は量子計算では効率的に解けないだろうと信じられている

よくある誤解

$$f : \{0,1\}^n \ni x \mapsto f(x) \in \{0,1\}$$

f(x)= 1 なるxは存在するか？



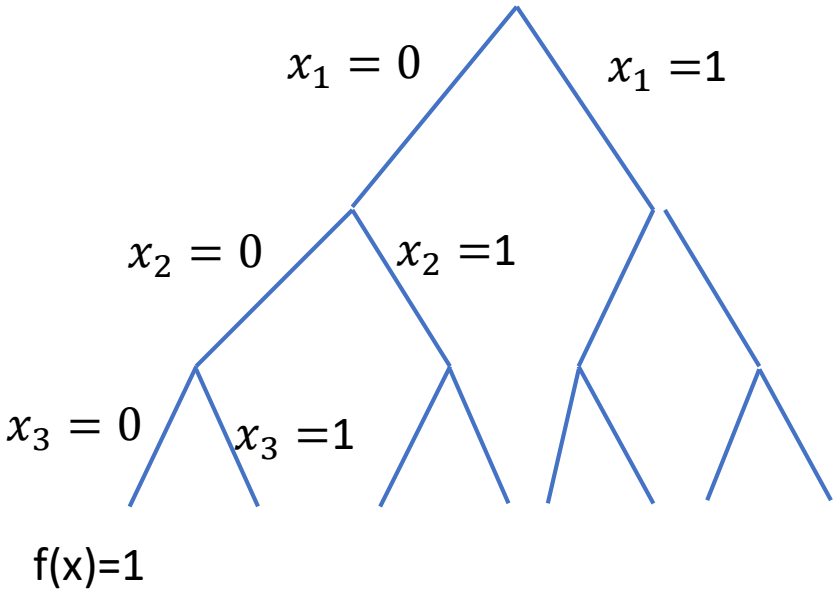
量子計算機は重ね合わせをつかってすべての指数個のパターンを一度に並列処理できる

→まちがい！

$$(c_1, \ldots, c_n) \qquad \sum_i |c_i|^2 = 1$$

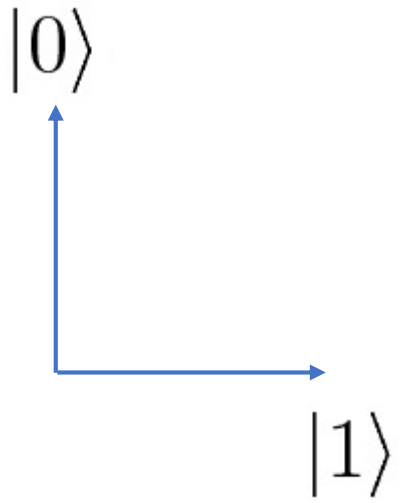
$$f : \{0,1\}^n \ni x \mapsto f(x) \in \{0,1\}$$

f(x)=１なるxは存在するか？



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、
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)]

量子ビット



$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \alpha|0\rangle + \beta|1\rangle$$

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \begin{aligned} X|0\rangle &= |1\rangle, \\ X|1\rangle &= |0\rangle \end{aligned}$$

$$(\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \delta|1\rangle)$$

$$\alpha|0\rangle \otimes |0\rangle + \beta|1\rangle \otimes |1\rangle$$

量子ゲート

Universalゲートセット

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

$$CNOT = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$$

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

$$\begin{aligned} H|0\rangle &= |0\rangle + |1\rangle \equiv |+\rangle, \\ H|1\rangle &= |0\rangle - |1\rangle \equiv |-\rangle \end{aligned}$$

任意の n 量子ビットユニタリが実現できる

量子ゲート

Universalゲートセット

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

$$CNOT = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$$

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

Cliffordゲート

任意の n 量子ビットユニタリが実現できる

Cliffordゲートの性質

$$
\begin{aligned}
HXH &= Z, \\
HZH &= X, \\
SXS^\dagger &= iXZ, \\
SZS^\dagger &= Z, \\
CNOT(X \otimes I)CNOT &= X \otimes X
\end{aligned}
$$

パウリのテンソル積をパウリのテンソル積にうつす

$$C(P_1 \otimes P_2 \otimes ... \otimes P_n)C^\dagger = P_1' \otimes ... \otimes P_n'$$

$$TXT^\dagger = \frac{X - Y}{\sqrt{2}}$$

Gottesman-Knill

Clifford gateのみの量子計算は古典で効率的にシミレート可能（Gottesman-Knill）

Clifford gateのみで、大きなエンタングルメント状態を作ることができる
→量子性があるからといって高速だとは限らない

$$|0...0\rangle + |1...1\rangle$$

$$|0\rangle^{\otimes n} = \{Z_1, Z_2, ..., Z_n\}$$

H

$$|0\rangle^{\otimes n-1} \otimes |+\rangle = \{Z_1, Z_2, ..., Z_{n-1}, X_n\}$$

$$|0\rangle^{\otimes n} = \{Z_1, Z_2, ..., Z_n\}$$

H

$$|0\rangle^{\otimes n-1} \otimes |+\rangle = \{Z_1, Z_2, ..., Z_{n-1}, X_n\}$$

T

$$TXT^\dagger = \frac{X - Y}{\sqrt{2}}$$

$$|0\rangle^{\otimes n-1} \otimes (T|+\rangle) = \{Z_1, ..., Z_{n-1}, X_n\} \cup \{Z_1, ..., Z_{n-1}, Y_n\}$$

Tがlog個までならセーフ。Poly個になるときつい

Cliffordゲート: 古典的
Tゲート: 量子高速性のリソース

→ Tが増えると古典シミレート複雑さはどうなるか？

Clifford＋t個のTゲートからなる量子回路の古典シミレート時間

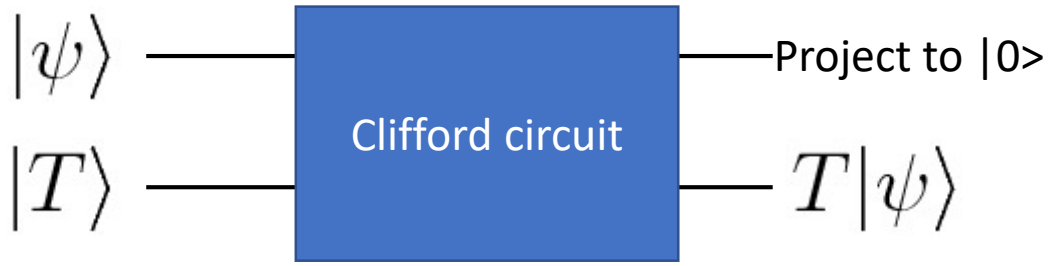
トリビアルな下限: *poly(t) time* (assuming BQP≠BPP)

トリビアルな上限: 2^t time (brute force)

ノントリビアルな上限： $2^{0.468t}$ time [Bravyi-Smith-Smolin-Gosset].

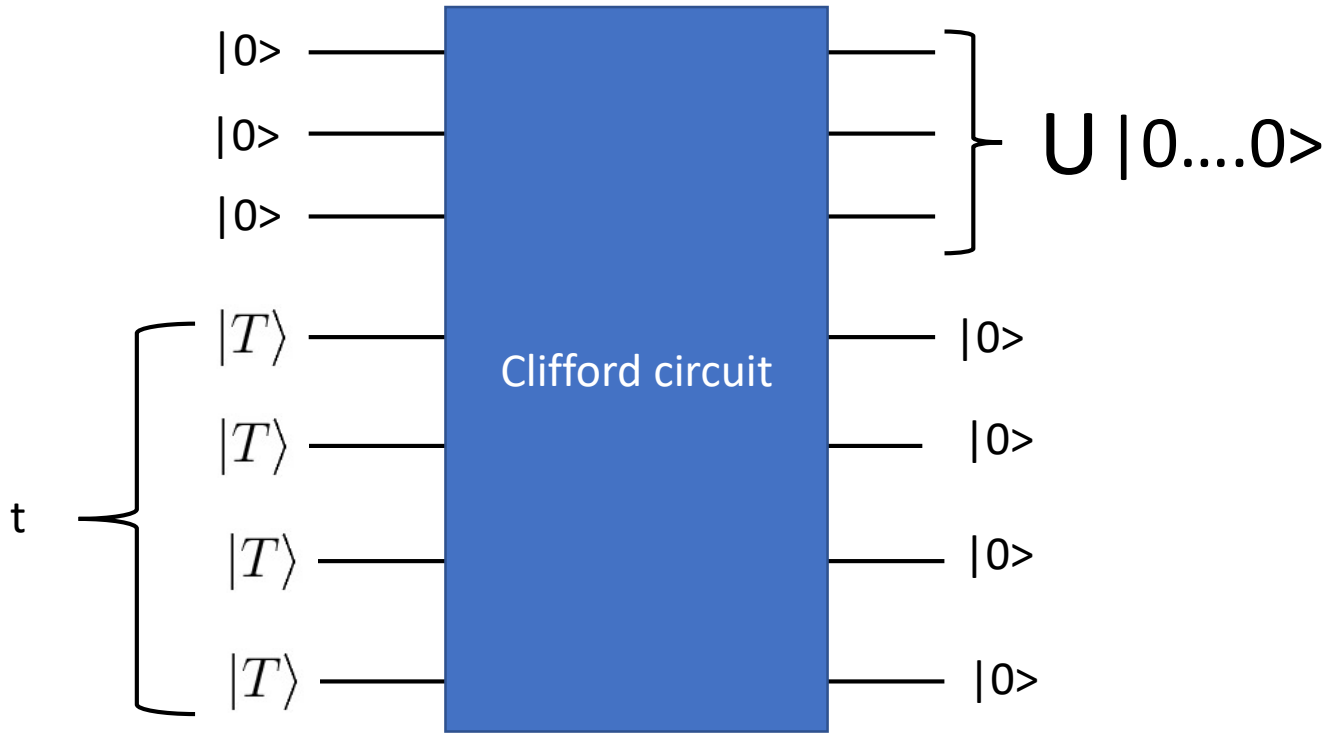
ここからは少し難しくなります。（知っている人向け）

Magic state gadget



$$|T\rangle = \cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle$$

U:クリフォードとt個の Tゲート。



スタビライザーランク

Clifford circuit

$$\langle 0^n|U|0^n\rangle = \sqrt{2^t}\langle 0^{n+t}|W(|0^n\rangle \otimes |T\rangle^{\otimes t})$$

Clifford and t T-gates

$$= \sqrt{2^t}\sum_{i=1}^{\chi} c_i \langle 0^{n+t}|W(|0^n\rangle \otimes |\phi_i\rangle)$$

$$|T\rangle^{\otimes t} = \sum_{i=1}^{\chi} c_i |\phi_i\rangle$$

Stabilizer state (Clifford gates on |0…0>)

Complex numbers

$$\chi \leq 2^{0.468t}$$

U can be classically simulated in $2^{0.468t}$ time.
[Bravyi-Smith-Smolin-Gosset]

$2^{0.468t}$ -time はさらに改善できるか？

例えば $2^{0.001t}$-timeとか。。。

しかし、$2^{o(t)}$ は無理!

[TM and Tamaki, QIC2019]:

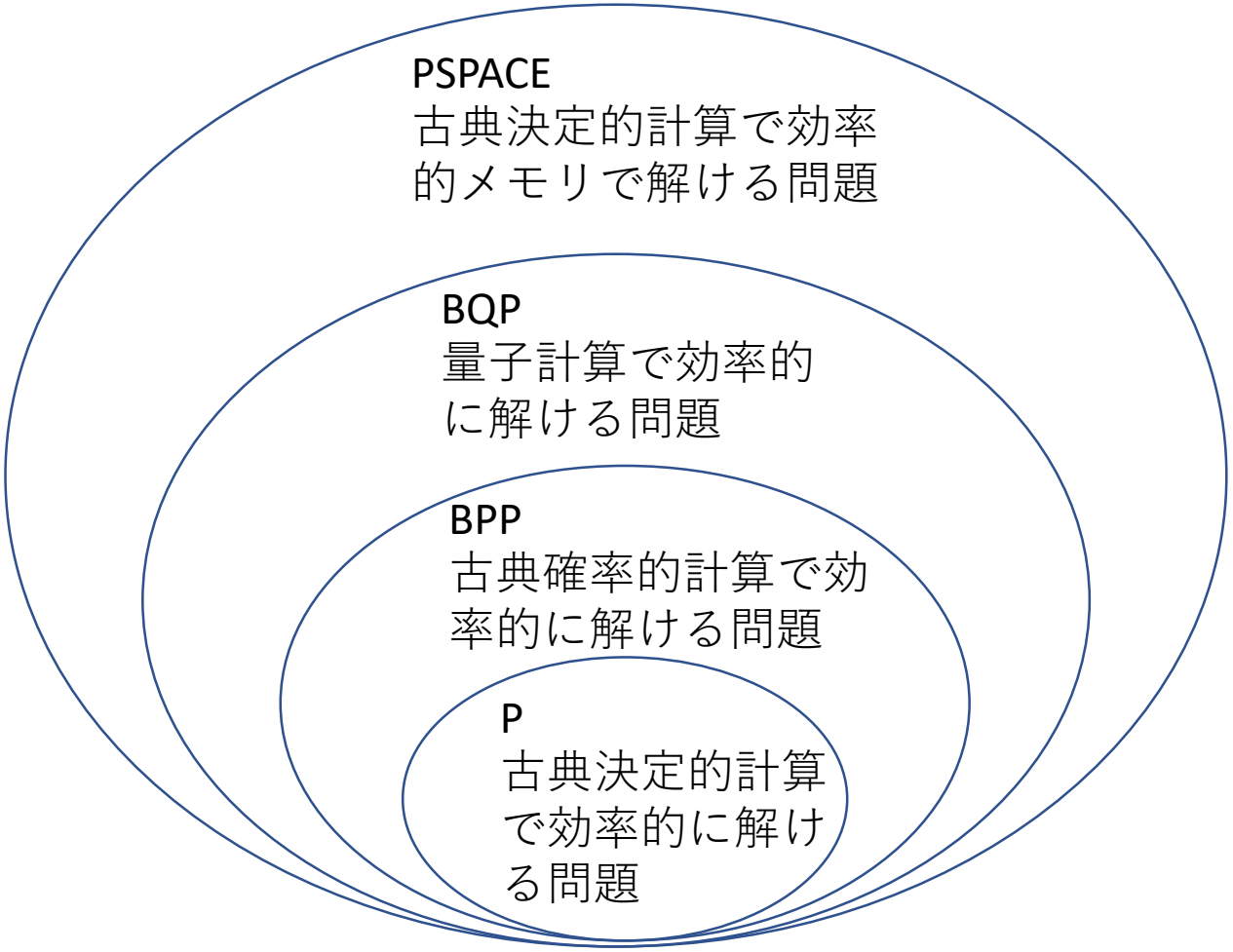
ETHのもとでは、Clifford と t個の Tゲートからなる 量子計算は古典では$2^{o(t)}$時間ではシミレートできない。

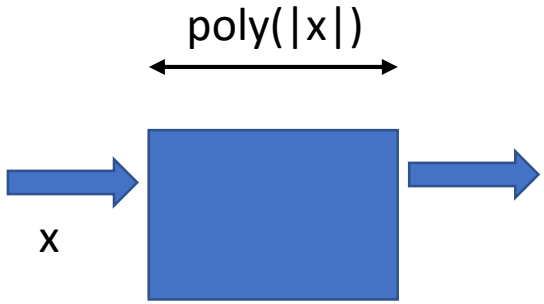
ETH

n変数の3-CNF-SATは $2^{o(n)}$ 時間では解けない。

P≠NP：ある種の難しい問題は多項式時間では解けません
Exponential time hypothesis（ETH）：指数時間かかります。

量子スプレマシー





BQP≠BPP　→　P≠PSPACE　量子が古典より速いことを示すのは超難しい

そうはいっても、皆量子計算は古典計算より速いと信じている

グローバータイプ

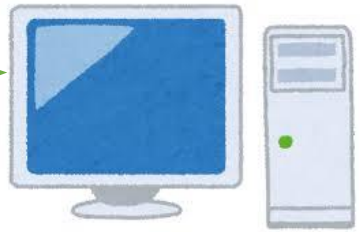
私の勝ち

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！

古典のベストはアップデートされる可能性がある

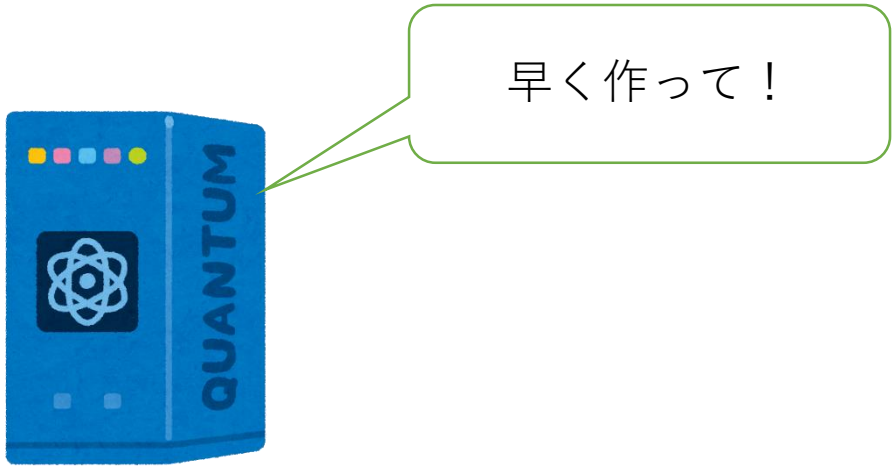
さらなる問題点

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]

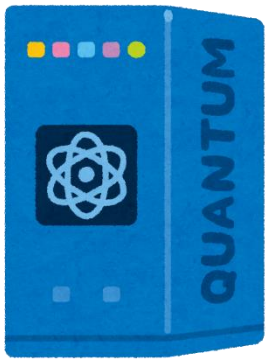


サンプリング問題

量子計算機がある確率分布でランダムなビット列を吐き出す

それと同じ確率分布でビット列を出せ　（なんの役に立つかは不明）

量子計算機



01011100….

古典計算機

01011100….

多項式階層が第二レベルで崩壊しないと仮定したら、

量子計算機は古典計算機より高速にサンプルできる

多項式階層が崩壊しない　≒　P≠NP　（超大雑把）

「弱い」マシンでもOK！

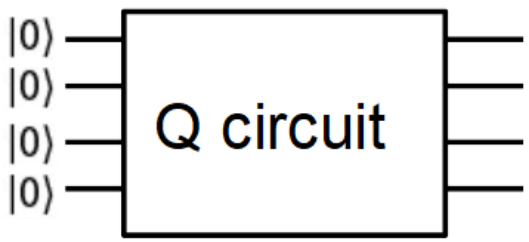
深さが４しかない量子回路
Terhal and DiVincenzo 2004

相互作用無し光子を使った量子計算機(Boson Sampling)
Aaronson and Arkhipov 2011

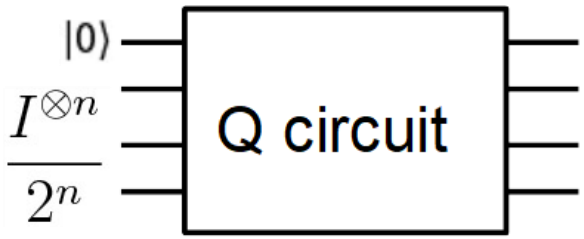
交換するゲートのみ(IQP)
Bremner, Montanaro, and Shepherd 2016

ゲートがランダムに作用する量子回路
Fefferman et al. 2018

One-clean qubit model
TM, 2017



通常の量子計算



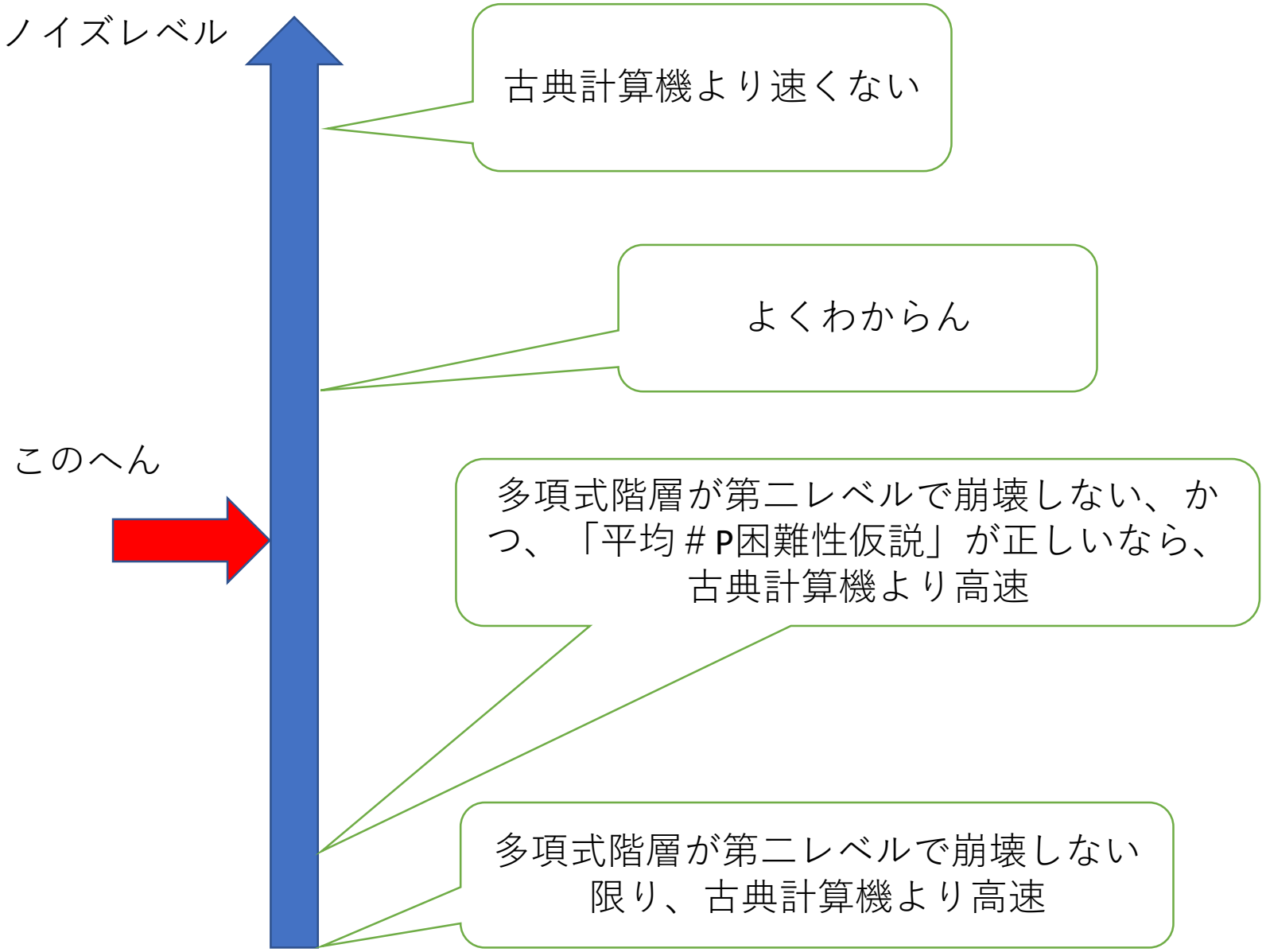
One clean qubit model

Googleの実験

読売新聞　２０１９年１０月２４日

１万年かかる計算、３分２０秒で…量子計算機がスパコン超え

残念ながら、Googleマシンはノイズが大きすぎて、量子超越性理論は使えない。。。



えっじゃあ「古典計算機では１万年かかる」の根拠は？

→彼らが考えた「ベスト」の古典アルゴリズムで、１万年かかるというだけ。

→量子スプレマシー理論のように、「多項式階層が崩壊しない」とかで保証されたものではない。

実際、直後に

IBM：実際はもっとメモリ使えるから2.5日でできるよ。

アリババ：テンソルネットワーク使うと20日でできるよ。

Barak：もっと直接的な高速アルゴリズムあるよ。（確率分布完全に計算しなくても、クロスエントロピーベンチマークを破れるような古典シミレーションを直接的につくれるよ。）

もっとノイズが大きくてもよいスプレマシー理論を作る必要がある。（難しい！）
もっとノイズの小さい実験を頑張ってやる必要がある（量子誤り訂正）
検証可能な量子スプレマシーの必要性

量子暗号

（ブラインド量子計算・量子計算の検証）

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）

A国の司令官

B国の盗聴者

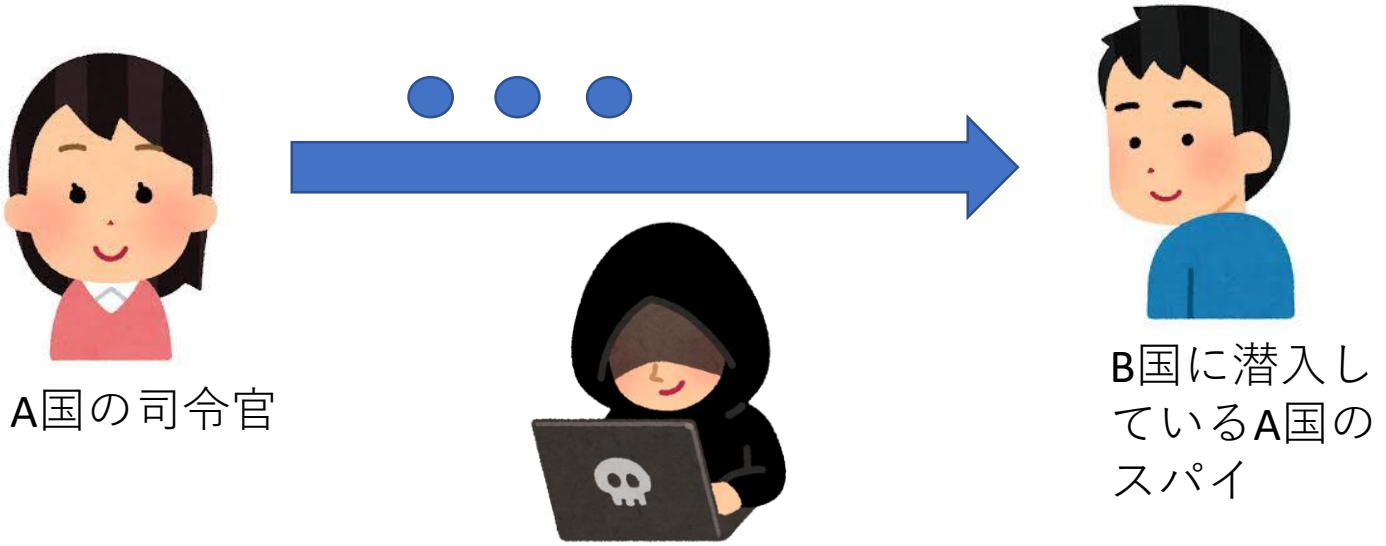
B国に潜入しているA国のスパイ

今では一般の人が日常的に使用している

電子署名、認証、電子マネー。。。

（狭い意味での）量子暗号

光子等の量子的な粒子を送れば、盗聴不可能な暗号が可能！



もう少し正確には、量子鍵配送（QKD）
（鍵配送問題が解決。情報理論的安全性が達成！）

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

電子署名、認証、電子マネー。。。

（広い意味での）量子暗号

1．量子を使って様々な暗号プロトコル実現する研究
（QKD、ブラインド量子計算、量子計算の検証、ゼロ知識証明、
量子マネー、量子秘密分散、量子多者間計算。。。）

2．古典暗号の量子攻撃に対する安全性を調べる研究（耐量子暗号）

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！！

ブラインド量子計算

量子サーバー

通信路（古典）

利用者（古典計算のみ）

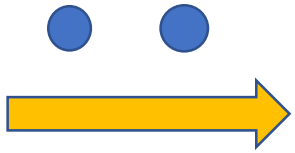
サーバーに計算内容を秘密にしたまま量子計算を委託できるか？

古典でも重要なテーマ：Garbled circuit、 Fully-homomophic encryption等

BFKプロトコル

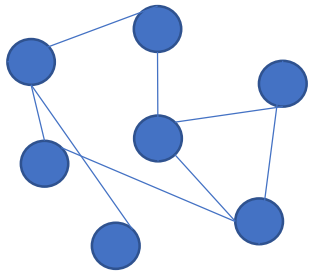
利用者が少し量子なら可

利用者



量子ビット
（暗号鍵）

サーバ

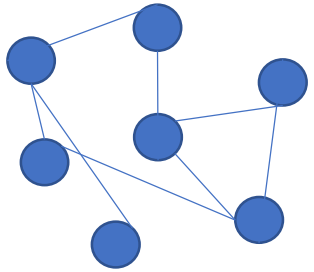


グラフ状態作る

利用者

古典通信
（暗号化）

サーバ



測定型量子計算実行

Broadbent, Fitzsimons, Kashefi, FOCS2009

情報理論的安全性！

Open problem

量子サーバー

通信路（古典）

利用者（古典計算のみ）

完全古典利用者のブラインド量子計算は可能か？

（１）情報理論的安全性はNegativeな結果[Aaronson et al., TM et al.]

（２）計算量的安全性なら可能（LWE仮定）[Mahadev, FOCS2018]

量子計算の検証

量子サーバー

通信路（古典）

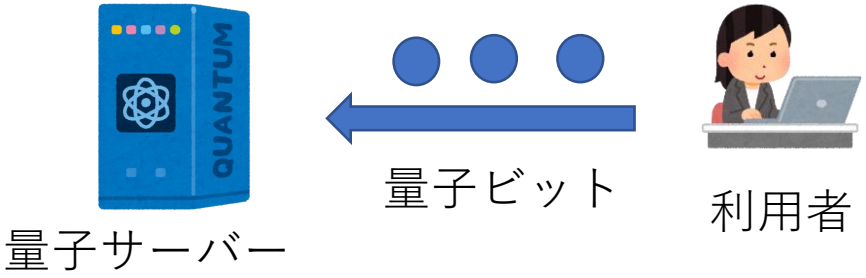
利用者（古典計算のみ）

クラウドが正しい量子計算をしているのかチェックできるか？

Googleが超越性を出したことを確認できるか？

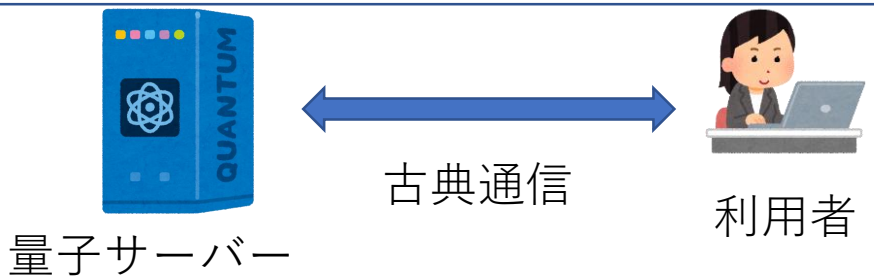
→かなり非自明な問題：量子計算は古典計算機でシミレートできないからこそ意味があるのに、そのせいで古典計算機で検算できなくなってしまうという皮肉なジレンマ！

利用者が少し量子なら可能



利用者が量子ビットを作れる[Fitzsimons-Kashefi, 2017]

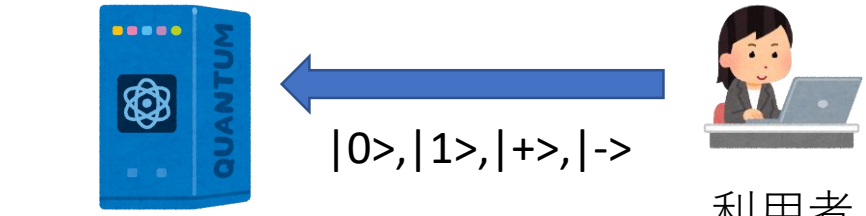
利用者が量子ビットを測定できる[Hayashi-Morimae, 2015; Morimae-Fitzsimons, 2018]



あるいは、LWE仮定のもとで、計算量理論的に可能！ [Mahadev, 2018]

完全古典＋情報理論的安全性で可能かはまだ未解決！

Remote state preparation

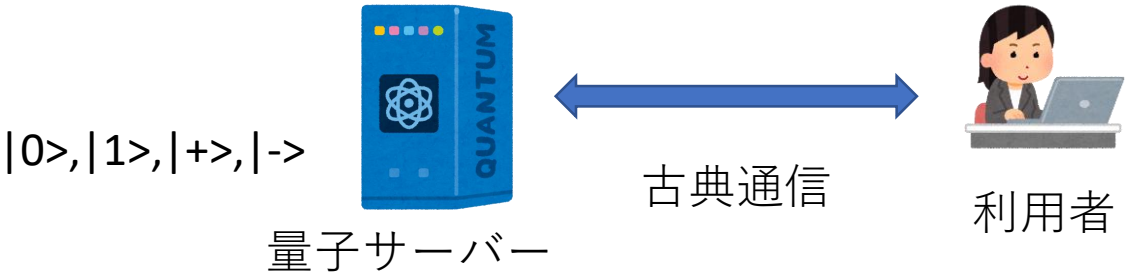


BB84状態を送れれば、いろんなことができる
（QKD、量子マネー、ブラインド量子計算、量子計算の検証。。。）

→量子チャネルと、量子ビット生成デバイスが必要

Remote state preparation
耐量子暗号＋古典通信で実現！！

[Andru and Vidick, FOCS2019; Cojocaru et al., ASIACRYPT2019]



古典通信で、「送ったのと同じ状況に」BB84状態をリモートに作れるのは信じがたい。。。

送った場合：サーバーは状態知らない＋クローン不可

古典通信：サーバーは状態完璧に知れる＋好きなだけクローン可

$$\sum_x |x\rangle \otimes |0^m\rangle \rightarrow \sum_x |x\rangle \otimes |f(x)\rangle$$

測定

$$(|x_0\rangle + |x_1\rangle) \otimes |y\rangle$$

これを二つ作ることは不可能：できたらclaw-freeが破れる

量子暗号プロトコルはもともとは情報理論的安全性が多かった。

量子を使うことにより情報理論的安全なプロトコルを達成：
QKD、ブラインド量子計算、量子計算の検証、量子マネー

→それだけではできないタスクがある。。

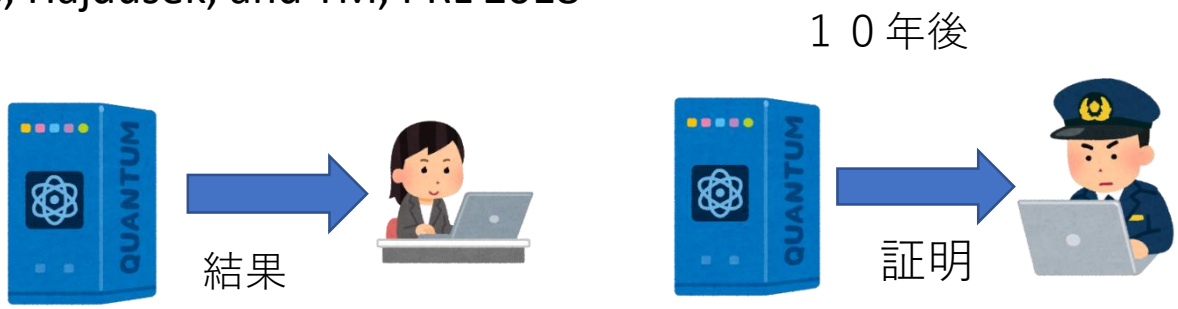
完全古典ブラインド量子計算、量子計算の古典検証、Public verifiable量子マネー。。。

→計算量的安全性（耐量子暗号）も使ったハイブリッドを考えると可能！

END

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！

その後の発展

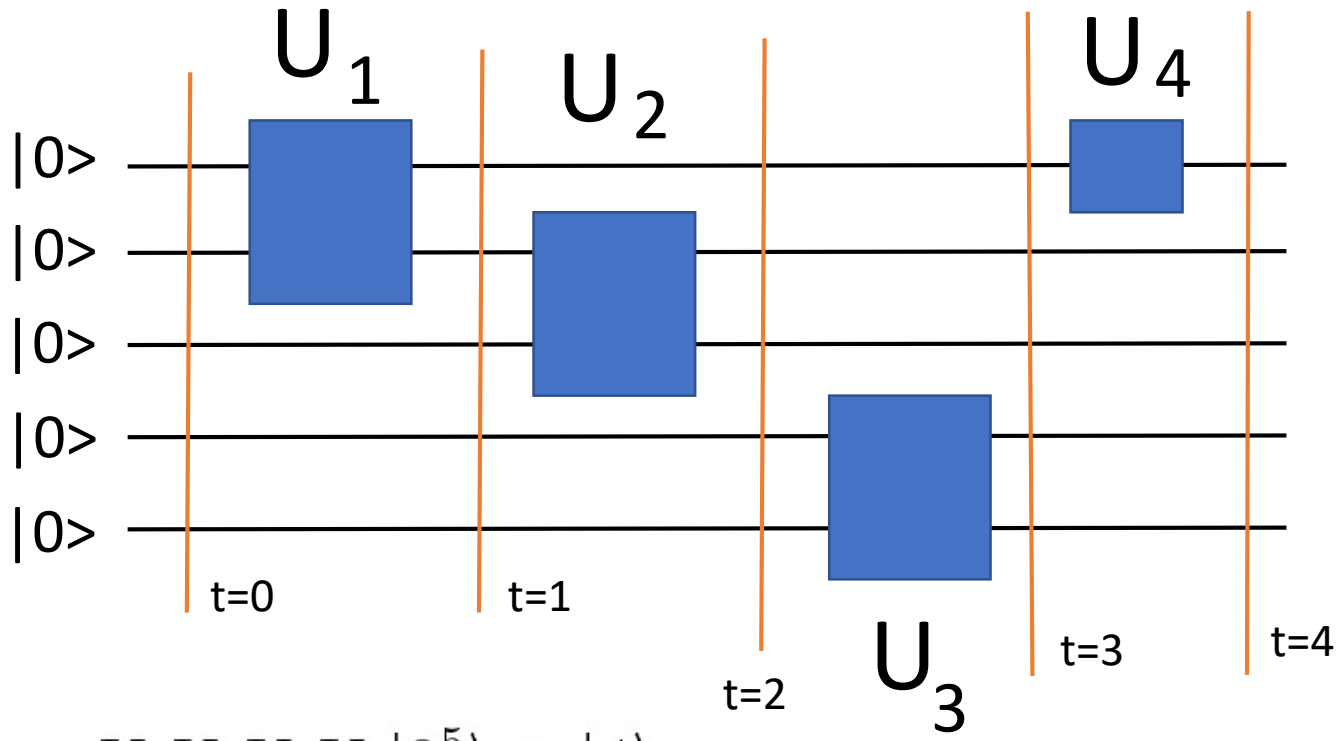
Mahadev FOCS 2018

Morimae-FitzsimonsプロトコルとLWEを組み合わせて、完全古典検証者による量子計算の検証を達成！！

ほかにも

[Andru and Vidick, FOCS2019]
[Alagic et al. 2020]
[Broadbent and Grilo, 2020]
[Chia, Chung, and Yamakawa, 2020]
[Cojocaru, ASIACRYPT2019]

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！

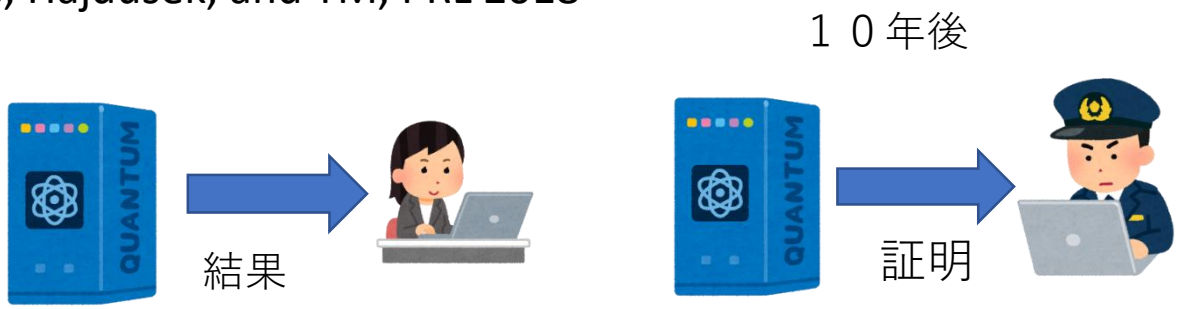
$$H = \sum_i (\alpha X_i X_{i+1} + \beta Z_i Z_{i+1} + \gamma X_i + \delta Z_i)$$

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]