量子計算基礎

竹内勇貴

NTT コミュニケーション科学基礎研究所

量子情報に関する講演の流れ

	8/1 (月)	8/2 (火)	8/3 (水)	8/4 (金)
9:30 – 10:30		竹内勇貴 「量子計算基礎」	安田雅哉 「格子基底簡約とLWE/NTRU問題に対する格子攻撃」	古江弘樹 「多変数多項式暗号1:署名方式の構成」
10:50 – 11:50		水谷明博 「量子計算の古典検証」	國廣昇 「隠れ部分群問題から見る素因数分解，離散対数問題」	池松泰彦 「多変数多項式暗号2:安全性解析」
13:30 – 14:30	相川勇輔 「暗号数理入門」	相川勇輔 「同種写像暗号1:楕円曲線と同種写像グラフ」	成定真太郎 「符号暗号の高速求解手法の実装に向けて」	
14:50 – 15:50	竹内勇貴 「量子情報基礎」	守谷共起 「同種写像暗号2:鍵交換方式SIDHとCSIDH」	七島幹人 「コルモゴロフ複雑度とそのアルゴリズム/暗号理論的恩恵」	
16:10 – 17:10	廣政良 「格子暗号」	小貫啓史 「同種写像暗号3:デジタル署名方式SQISign」	山川高志 「計算量的安全な量子暗号の最近の進展」	

「量子情報基礎」→「量子計算基礎」

量子情報に関する講演の流れ

	8/1 (月)	8/2 (火)	8/3 (水)	8/4 (金)
9:30 – 10:30		竹内勇貴 「量子計算基礎」	安田雅哉 「格子基底簡約とLWE/NTRU問題に対する格子攻撃」	古江弘樹 「多変数多項式暗号1:署名方式の構成」
10:50 – 11:50		水谷明博 「量子計算の古典検証」	國廣昇 「隠れ部分群問題から見る素因数分解，離散対数問題」	池松泰彦 「多変数多項式暗号2:安全性解析」
13:30 – 14:30	相川勇輔 「暗号数理入門」	相川勇輔 「同種写像暗号1:楕円曲線と同種写像グラフ」	成定真太郎 「符号暗号の高速求解手法の実装に向けて」	
14:50 – 15:50	竹内勇貴 「量子情報基礎」	守谷共起 「同種写像暗号2:鍵交換方式SIDHとCSIDH」	七島幹人 「コルモゴロフ複雑度とそのアルゴリズム/暗号理論的恩恵」	
16:10 – 17:10	廣政良 「格子暗号」	小貫啓史 「同種写像暗号3:デジタル署名方式SQISign」	山川高志 「計算量的安全な量子暗号の最近の進展」	

「量子情報基礎」→「量子計算基礎」→「量子計算の古典検証」

「格子暗号」

量子情報に関する講演の流れ

	8/1 (月)	8/2 (火)	8/3 (水)	8/4 (金)
9:30 – 10:30		竹内勇貴 「量子計算基礎」	安田雅哉 「格子基底簡約とLWE/NTRU問題に対する格子攻撃」	古江弘樹 「多変数多項式暗号1:署名方式の構成」
10:50 – 11:50		水谷明博 「量子計算の古典検証」	國廣昇 「隠れ部分群問題から見る素因数分解，離散対数問題」	池松泰彦 「多変数多項式暗号2:安全性解析」
13:30 – 14:30	相川勇輔 「暗号数理入門」	相川勇輔 「同種写像暗号1:楕円曲線と同種写像グラフ」	成定真太郎 「符号暗号の高速求解手法の実装に向けて」	
14:50 – 15:50	竹内勇貴 「量子情報基礎」	守谷共起 「同種写像暗号2:鍵交換方式SIDHとCSIDH」	七島幹人 「コルモゴロフ複雑度とそのアルゴリズム/暗号理論的恩恵」	
16:10 – 17:10	廣政良 「格子暗号」	小貫啓史 「同種写像暗号3:デジタル署名方式SQISign」	山川高志 「計算量的安全な量子暗号の最近の進展」	

「量子情報基礎」→「量子計算基礎」→「量子計算の古典検証」→山川さんのトーク

「格子暗号」

本講演の目的

量子計算とその検証手法を理解すること!!

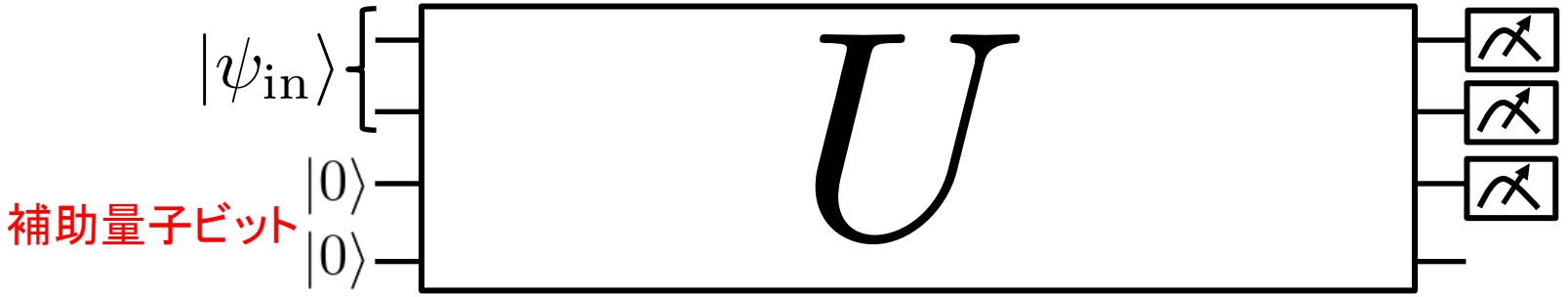
- 量子回路
- 量子計算で解けるとは？(**BPP**, **BQP**)
- 量子計算の検証

- モチベーション
- ハミルトニアンの基底状態エネルギー推定への帰着
- ポストホック検証 (森前-Fitzsimonsプロトコル)

量子回路

量子回路

量子計算は以下の図で表現出来る。



入力量子ビット
(2次元正規ベクトル)

量子ゲート
(ユニタリ行列)

出力ビット

Remark (Solovay-Kitaevの定理)
*H, T, CX*の組み合わせだけ考えればOK

→ 計算の効率(計算時間)は、*H, T, CX*をいくつ必要とするかで議論出来る

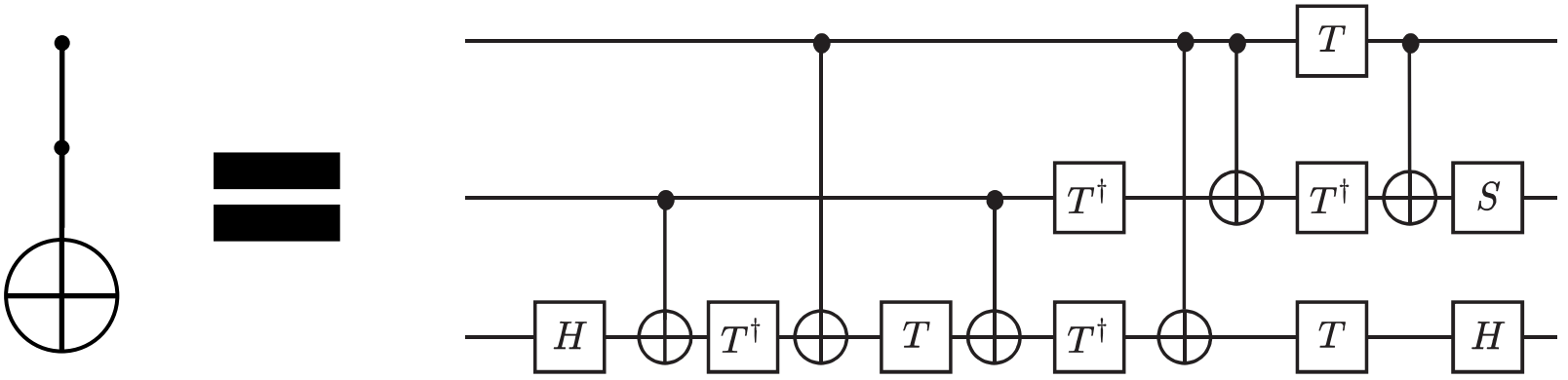
量子回路

量子計算 v.s. 古典計算

論理回路で多項式時間で解ける問題は、量子計算でも多項式時間で解ける。

- Toffoliゲートで任意のブール関数を計算出来る。
- Toffoliゲートは量子計算で効率良く実行可能。

※ $T^\dagger = T^7$



[M. Rahman and G. Paul, IEEE Trans. on Quant. Engineering **3**, 3100809 (2022)]

量子回路

量子計算 v.s. 古典計算

[D. Deutsch, Proc. R. Soc. London A **400**, 97 (1985)]

量子計算が古典計算より強い例: ドイチュの問題

f(0)=f(1) or *f(0)≠f(1)*を誤り無く判定するのにブラックボックスへの問い合わせが何回必要か？

古典の場合: 自明に*2*回必要

量子回路

量子計算 v.s. 古典計算

[D. Deutsch, Proc. R. Soc. London A **400**, 97 (1985)]

量子計算が古典計算より強い例: ドイチュの問題

f(0)=f(1) or *f(0)≠f(1)*を誤り無く判定するのにブラックボックスへの問い合わせが何回必要か？

古典の場合: 自明に2回必要

量子の場合: 1回でOK

量子回路

量子計算 v.s. 古典計算

[D. Deutsch, Proc. R. Soc. London A **400**, 97 (1985)]

量子計算が古典計算より強い例: ドイチュの問題

$$|00\rangle \xrightarrow{I \otimes X} |01\rangle \xrightarrow{H \otimes H} \frac{|00\rangle - |01\rangle + |10\rangle - |11\rangle}{2}$$

量子回路

量子計算 v.s. 古典計算

[D. Deutsch, Proc. R. Soc. London A **400**, 97 (1985)]

量子計算が古典計算より強い例: ドイチュの問題

$$|00\rangle \xrightarrow{I \otimes X} |01\rangle \xrightarrow{H \otimes H} \frac{|00\rangle - |01\rangle + |10\rangle - |11\rangle}{2}$$

$$\xrightarrow{\text{black box}} \frac{|0\rangle|f(0)\rangle - |0\rangle|1 \oplus f(0)\rangle + |1\rangle|f(1)\rangle - |1\rangle|1 \oplus f(1)\rangle}{2}$$

$$|\pm\rangle \equiv \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$$

量子回路

量子計算 v.s. 古典計算

[D. Deutsch, Proc. R. Soc. London A **400**, 97 (1985)]

量子計算が古典計算より強い例: ドイチュの問題

$$|00\rangle \xrightarrow{I \otimes X} |01\rangle \xrightarrow{H \otimes H} \frac{|00\rangle - |01\rangle + |10\rangle - |11\rangle}{2}$$

$$\xrightarrow{\text{black box}} \frac{|0\rangle|f(0)\rangle - |0\rangle|1 \oplus f(0)\rangle + |1\rangle|f(1)\rangle - |1\rangle|1 \oplus f(1)\rangle}{2}$$

$$= \begin{cases} |+\rangle \otimes \dfrac{|f(0)\rangle - |1 \oplus f(0)\rangle}{\sqrt{2}} & (f(0) = f(1)) \\ |-\rangle \otimes \dfrac{|f(0)\rangle - |1 \oplus f(0)\rangle}{\sqrt{2}} & (f(0) \neq f(1)) \end{cases}$$

量子回路

量子計算 v.s. 古典計算

[D. Deutsch, Proc. R. Soc. London A **400**, 97 (1985)]

量子計算が古典計算より強い例: ドイチュの問題

$$|00\rangle \xrightarrow{I \otimes X} |01\rangle \xrightarrow{H \otimes H} \frac{|00\rangle - |01\rangle + |10\rangle - |11\rangle}{2}$$

$$\xrightarrow{\text{black box}} \frac{|0\rangle|f(0)\rangle - |0\rangle|1 \oplus f(0)\rangle + |1\rangle|f(1)\rangle - |1\rangle|1 \oplus f(1)\rangle}{2}$$

$$\xrightarrow{H \otimes I} \begin{cases} |0\rangle \otimes \dfrac{|f(0)\rangle - |1 \oplus f(0)\rangle}{\sqrt{2}} & (f(0) = f(1)) \\ |1\rangle \otimes \dfrac{|f(0)\rangle - |1 \oplus f(0)\rangle}{\sqrt{2}} & (f(0) \neq f(1)) \end{cases}$$

量子計算で解けるとは？

計算量クラス

簡単のため、約束問題(YES, NOで答えられる問題)だけを考えることにする。

× 1+1=?

○ 1+1=2?

BPPと呼ばれる計算量クラスに入っている問題が、古典計算機(論理回路、確率的チューリング機械)で効率良く解ける問題。

- **BPP**

量子計算で解けるとは？

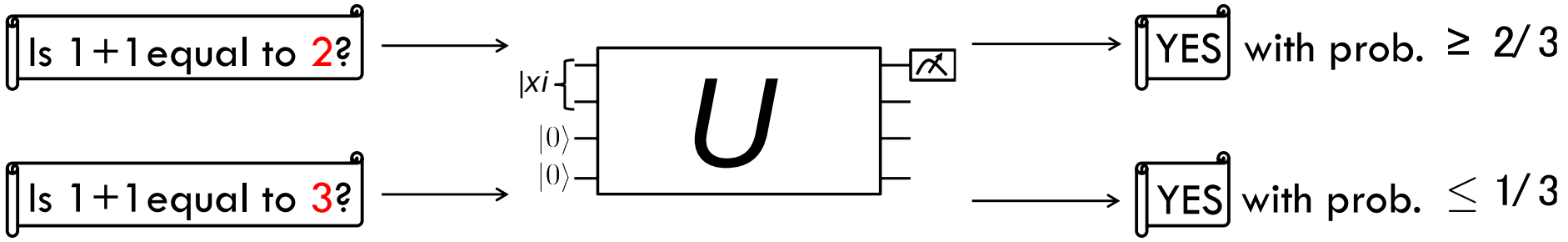
計算量クラス

量子計算機(量子回路)で効率良く解ける問題を定義するために、**BPP**の量子版**BQP**を定義する。

- **BQP** [E. Bernstein and U. Vazirani, SIAM J. Comput. **26**, 1411 (1997)]

以下を満たす時、約束問題*L*が**BQP**に入ると言う。
下記の条件を満たす多項式サイズ*(H,T,CX*が多項式個*)*の量子回路の作り方を、決定論的チューリング機械で多項式時間で出力出来る。

1. $x \in L_{\rm yes}$ (答えがYES)の時、量子回路が*1*(YES)を出す確率は $p_1 \geq 2/3$
2. $x \in L_{\rm no}$ (答えがNO)の時、　〃　$p_1 \leq 1/3$



量子計算で解けるとは？

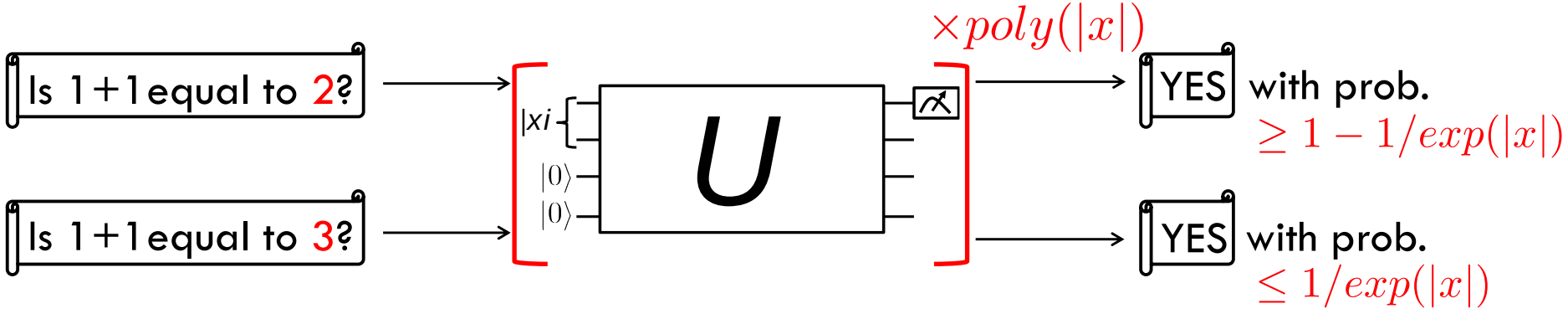
計算量クラス

量子計算機(量子回路)で効率良く解ける問題を定義するために、**BPP**の量子版**BQP**を定義する。

- **BQP** [E. Bernstein and U. Vazirani, SIAM J. Comput. **26**, 1411 (1997)]

以下を満たす時、約束問題*L*が**BQP**に入ると言う。
下記の条件を満たす多項式サイズ*(H,T,CX*が多項式個*)*の量子回路の作り方を、決定論的チューリング機械で多項式時間で出力出来る。

1. $x \in L_{\mathrm{yes}}$ (答えがYES)の時、量子回路が*1*を出す確率は $p_1 \geq 1 - 1/exp(|x|)$
2. $x \in L_{\mathrm{no}}$ (答えがNO)の時、 〃 $p_1 \leq 1/exp(|x|)$



量子計算で解けるとは？

BQPの性質

BQPは補集合のもとで閉じている。(**BQP** = **coBQP**)

- **coBQP**

以下を満たす時、約束問題*L*が**co**BQPに入ると言う。
下記の条件を満たす多項式サイズ*(H,T,CX*が多項式個*)*の量子回路の作り方を、決定論的チューリング機械で多項式時間で出力出来る。

1. 答えがNOの時、量子回路が*1*を出す確率は $p_1 \geq 2/3$
2. 答えがYESの時、　〃　$p_1 \leq 1/3$

※ complementのイメージ
BQPでは与えられた問題の答えがYESかどうかを聞いている (e.g., *N*は素数？)
→ YESインスタンスが与えられたら、YESと答えたい

coBQPでは与えられた問題の答えがNOかどうかを聞いている (e.g., *N*は合成数？)
→ NOインスタンスが与えられたら、YESと答えたい

$X \equiv |1\rangle\langle 0| + |0\rangle\langle 1|$

量子計算で解けるとは？

BQPの性質

BQPは補集合のもとで閉じている。(**BQP = coBQP**)

- **coBQP**

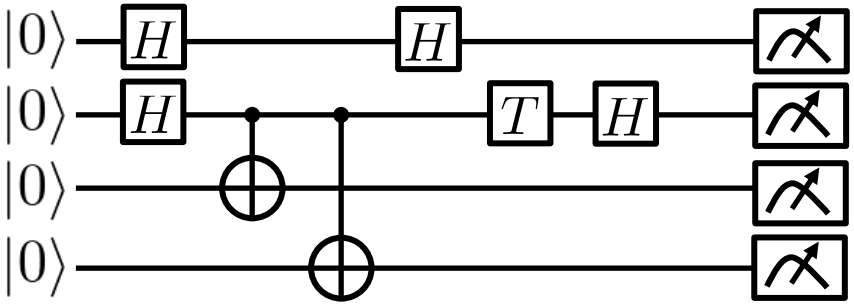
以下を満たす時、約束問題*L*が**co**BQPに入ると言う。
下記の条件を満たす多項式サイズ*(H,T,CX*が多項式個*)*の量子回路の作り方を、決定論的チューリング機械で多項式時間で出力出来る。

1. 答えがNOの時、量子回路が*1*を出す確率は $p_1 \geq 2/3$
2. 答えがYESの時、　〃　$p_1 \leq 1/3$

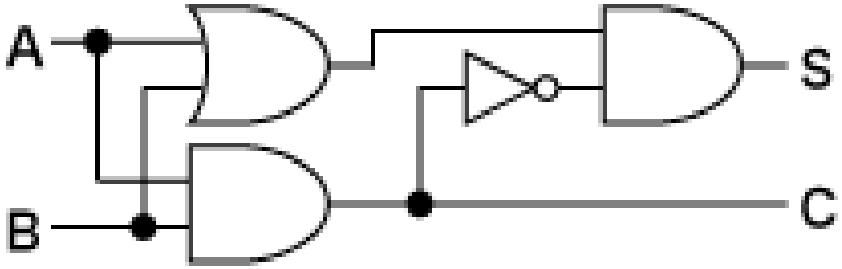
(証明)

量子計算の検証のモチベーション

量子計算の(1つの)ゴール: 古典計算に対して優位性がある計算の実現



量子回路

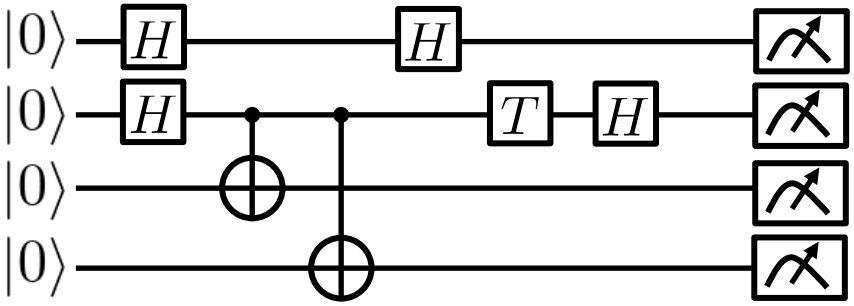


[https://ja.wikipedia.org/wiki/加算器]

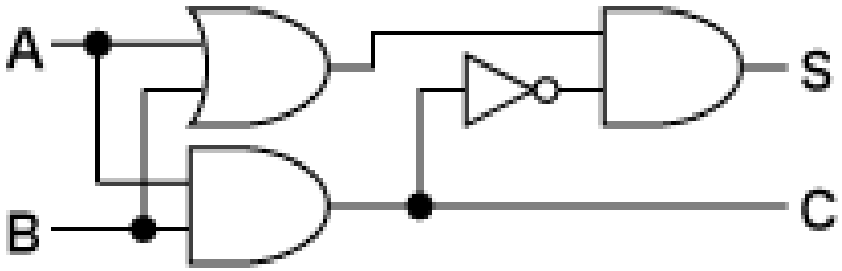
古典(論理)回路

量子計算の検証のモチベーション

量子計算の(1つの)ゴール: 古典計算に対して優位性がある計算の実現



量子回路



[https://ja.wikipedia.org/wiki/加算器]

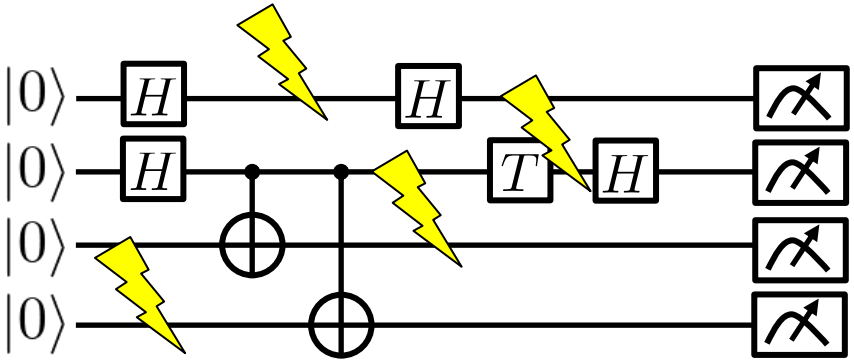
古典(論理)回路

- 素因数分解
- 離散対数の発見
- 隠れ部分群問題
- Jones多項式の近似
- 分配関数の近似
- (構造のない)データベース探索
- 可解群の位数の計算
- 周期発見
- 連立方程式
- 衝突発見

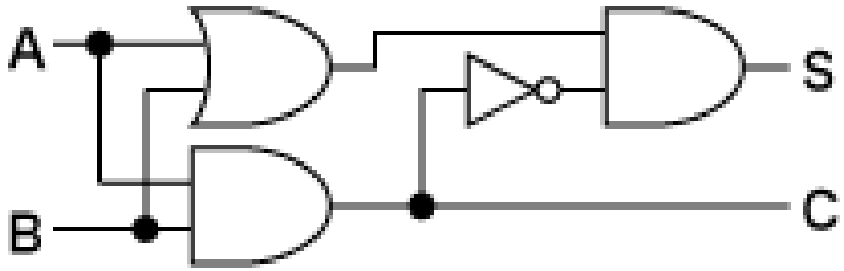
etc…

量子計算の検証のモチベーション

量子計算の(1つの)ゴール: 古典計算に対して優位性がある計算の実現

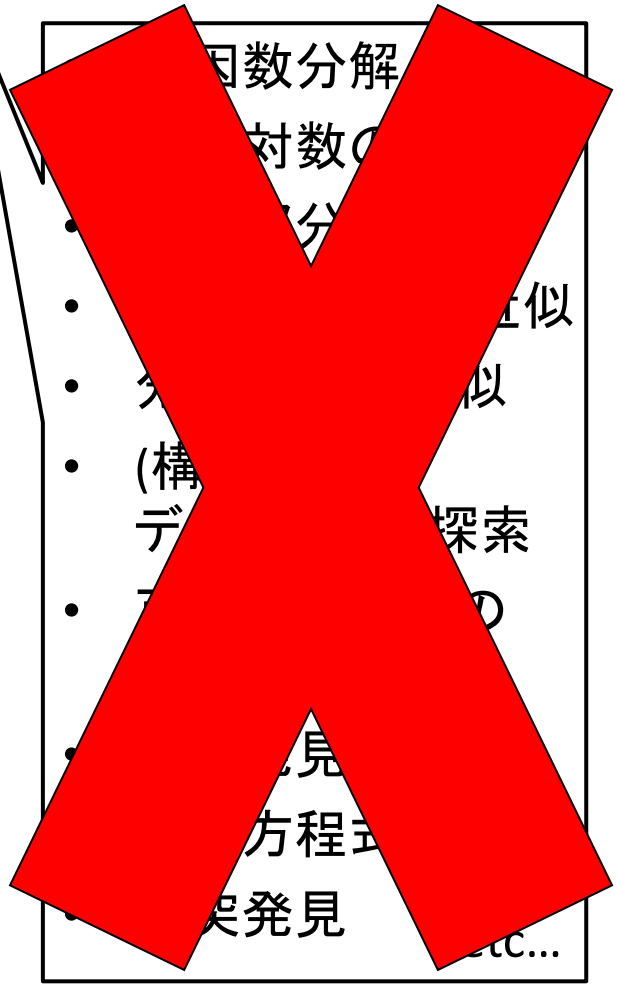


Noisyな
量子回路



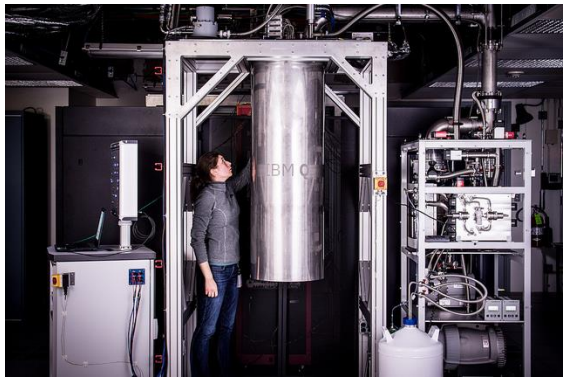
[https://ja.wikipedia.org/wiki/加算器]

古典(論理)回路



量子計算の検証のモチベーション

クラウド量子計算



[※1]

サーバ
(量子計算機)

この問題を解いて

答え

ユーザ

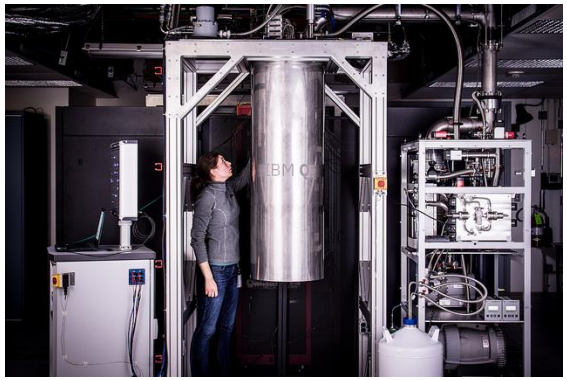
- サイズが大きい
- 定期的なキャリブレーションが必要
- 多くのアーキテクチャにおいて極低温(< 50 mK)が必要

※1https://www.popularmechanics.com/technology/a29105270/most-powerful-quantum-computer/

量子計算の検証のモチベーション

クラウド量子計算

- サーバはお願いした計算を
  正しく行ってくれただろうか？
- そもそも、サーバは本当に
  量子計算機を持っているのだろうか？



[※1]

サーバ
(量子計算機)

この問題を解いて

答え

ユーザ

- サイズが大きい
- 定期的なキャリブレーションが必要
- 多くのアーキテクチャにおいて極低温(< 50 mK)が必要

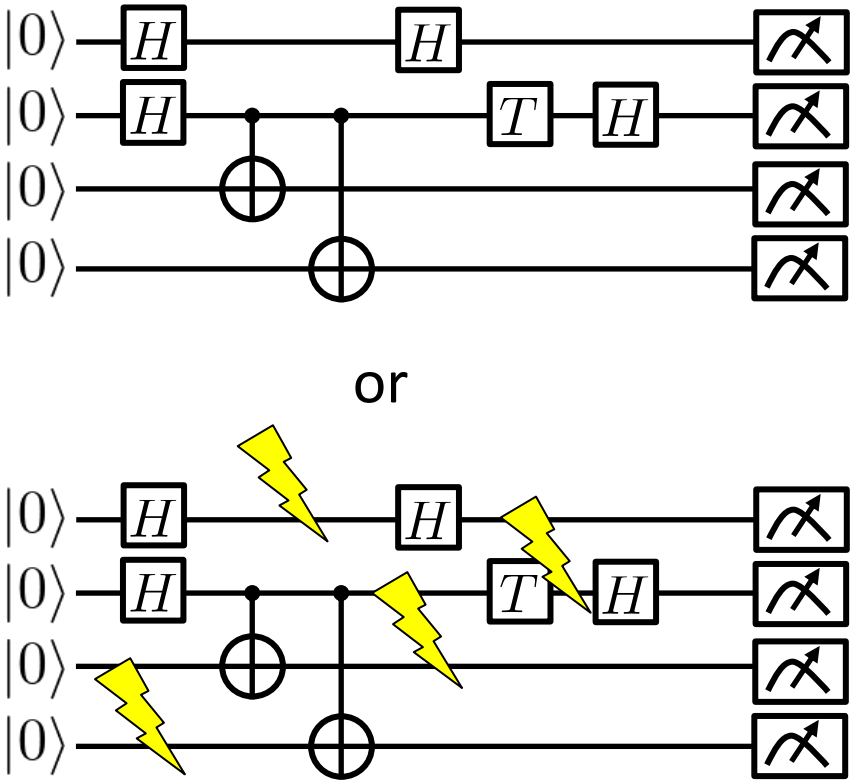
※1https://www.popularmechanics.com/technology/a29105270/most-powerful-quantum-computer/

※1https://perimeterinstitute.ca/people/daniel-gottesman

量子計算の検証のモチベーション

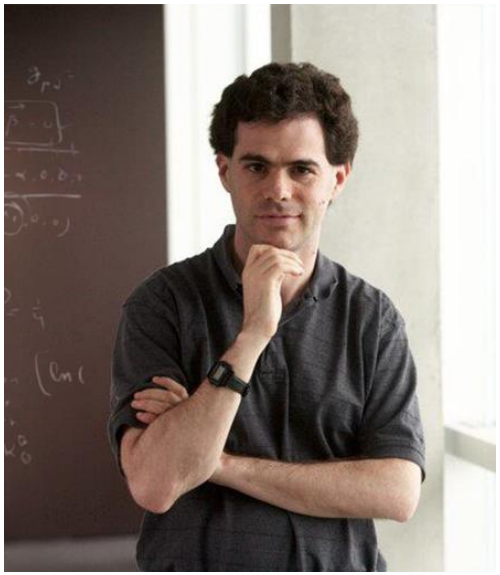
Q: 量子計算機が(充分)正しく動作しているか効率良く判定出来るのか？

2004年頃



or

[※1]



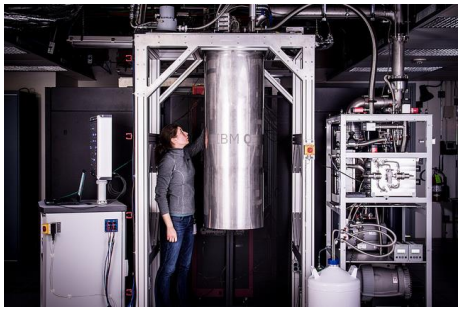
D. Gottesman

量子計算の検証

ポストホック検証(Morimae-Fitzsimonsプロトコル)

[J. F. Fitzsimons, M. Hajdušek, T. Morimae, PRL **120**, 040501 (2018)]

[※1]



②問題を量子計算機で解く

①この問題の答えはYES, NOどっち？

③答えは*b*(=YES or NO)です

④MFプロトコル (1ラウンド量子通信)

*b*が正しい時、受理確率は$p_{\mathrm{acc}} \geq 1 - 1/exp(|x|)$
*b*が正しくない時、$p_{\mathrm{acc}} \leq 1/exp(|x|)$

※1https://www.popularmechanics.com/technology/a29105270/most-powerful-quantum-computer/

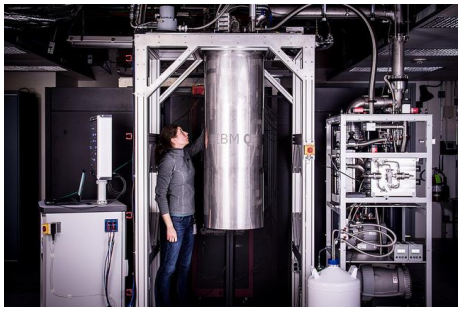
※1https://www.popularmechanics.com/technology/a29105270/most-powerful-quantum-computer/

量子計算の検証

ポストホック検証(Morimae-Fitzsimonsプロトコル)

[J. F. Fitzsimons, M. Hajdušek, T. Morimae, PRL **120**, 040501 (2018)]

[※1]



②問題を量子計算機で解く

①この問題の答えはYES, NOどっち？

③答えは*b*(=YES or NO)です

④MFプロトコル (1ラウンド量子通信)

*b*が正しい時、受理確率は$p_{\mathrm{acc}} \geq 1 - 1/exp(|x|)$
*b*が正しくない時、$p_{\mathrm{acc}} \leq 1/exp(|x|)$

以降では、MFプロトコルの仕組みを理解するために、
任意の**BQP**問題がローカルハミルトニアン問題(の特別ケース)
に帰着出来ることを紹介する。

量子計算の検証

*k*ローカルハミルトニアン問題

[A. Kitaev, A. Shen, M. N. Vyalyi, *Classical and Quantum Computation* (2002)]

*n*量子ビットハミルトニアン(*2^n* ×*2^n*エルミート行列)

$$H = \sum_{i=1}^{poly(n)} H_i$$

(任意の*i*に対して、H_iは高々*k*量子ビットにしか作用しない)

と、$b(n) - a(n) \geq 1/poly(n)$を満たす2つの関数$a(n), b(n)$が与えられる。
以下のどちらが成り立つか判定せよ。

1. *H*の基底状態エネルギー(最小固有値)は$\lambda_{\min} \leq a(n)$
2. 〃 $\lambda_{\min} \geq b(n)$

ただし、どちらかが必ず成り立つことが約束されている。

量子計算の検証

*k*ローカルハミルトニアン問題

[A. Kitaev, A. Shen, M. N. Vyalyi, *Classical and Quantum Computation* (2002)]

*n*量子ビットハミルトニアン(*2^n* ×*2^n*エルミート行列)

$$H = \sum_{i=1}^{poly(n)} H_i$$

(任意の*i*に対して、H_iは高々*k*量子ビットにしか作用しない)

と、$b(n) - a(n) \geq 1/poly(n)$を満たす2つの関数$a(n), b(n)$が与えられる。
以下のどちらが成り立つか判定せよ。

1. $\langle\psi|H|\psi\rangle \leq a(n)$を満たす*n*量子ビット状態$|\psi\rangle$が存在する。
2. 任意の$|\psi\rangle$に対して、$\langle\psi|H|\psi\rangle \geq b(n)$

ただし、どちらかが必ず成り立つことが約束されている。

量子計算の検証

*k*ローカルハミルトニアン問題

[A. Kitaev, A. Shen, M. N. Vyalyi, *Classical and Quantum Computation* (2002)]

*n*量子ビットハミルトニアン($2^n \times 2^n$エルミート行列)

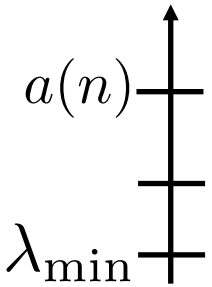
$$H = \sum_{i=1}^{poly(n)} H_i$$

(任意の*i*に対して、H_iは高々*k*量子ビットにしか作用しない)

と、$b(n) - a(n) \geq 1/poly(n)$を満たす2つの関数$a(n), b(n)$が与えられる。
以下のどちらが成り立つか判定せよ。

1. $\langle\psi|H|\psi\rangle \leq a(n)$を満たす*n*量子ビット状態$|\psi\rangle$が存在する。
2. 任意の$|\psi\rangle$に対して、$\langle\psi|H|\psi\rangle \geq b(n)$

ただし、どちらかが必ず成り立つことが約束されている。



Remark 1:
基底状態では無くても良い。

量子計算の検証

kローカルハミルトニアン問題

[A. Kitaev, A. Shen, M. N. Vyalyi, *Classical and Quantum Computation* (2002)]

n量子ビットハミルトニアン($2^n \times 2^n$エルミート行列)

$$H = \sum_{i=1}^{poly(n)} H_i$$

(任意のiに対して、H_iは高々k量子ビットにしか作用しない)

と、$b(n) - a(n) \geq 1/poly(n)$を満たす2つの関数$a(n), b(n)$が与えられる。
以下のどちらが成り立つか判定せよ。

1. $\langle\psi|H|\psi\rangle \leq a(n)$を満たすn量子ビット状態$|\psi\rangle$が存在する。
2. 任意の$|\psi\rangle$に対して、$\langle\psi|H|\psi\rangle \geq b(n)$

ただし、どちらかが必ず成り立つことが約束されている。

Remark 2:
純粋状態だけでOK

$$\mathrm{Tr}[H\rho] = \sum_i p_i \langle\psi_i|H|\psi_i\rangle \leq \langle\psi_{\max}|H|\psi_{\max}\rangle$$

Remark 1:
基底状態では無くても良い。

量子計算の検証

*k*ローカルハミルトニアン問題

[A. Kitaev, A. Shen, M. N. Vyalyi, *Classical and Quantum Computation* (2002)]

*n*量子ビットハミルトニアン($2^n \times 2^n$エルミート行列)

$$H = \sum_{i=1}^{poly(n)} H_i$$

(任意の*i*に対して、H_iは高々*k*量子ビットにしか作用しない)

と、$b(n) - a(n) \geq 1/poly(n)$を満たす2つの関数$a(n), b(n)$が与えられる。
以下のどちらが成り立つか判定せよ。

1. $\langle\psi|H|\psi\rangle \leq a(n)$を満たす*n*量子ビット状態$|\psi\rangle$が存在する。
2. 任意の$|\psi\rangle$に対して、$\langle\psi|H|\psi\rangle \geq b(n)$

ただし、どちらかが必ず成り立つことが約束されている。

目標:
YESの時は1を、NOの時は2を満たすようなエルミート行列を見付けたい。

$u_0 \equiv I^{\otimes |x|}$

量子計算の検証

ヒストリー状態

[A. Kitaev, A. Shen, M. N. Vyalyi, *Classical and Quantum Computation* (2002)]

問題が**BQP**に含まれているということは、定義より、任意のインスタンス*x*に対して

$$U(|x\rangle|0^m\rangle)$$

s.t.

1. *m*はインスタンスサイズ*|x|*の多項式
2. *1*量子ビット目を測定した時に*1*が出る確率は、
   - YESの時 $p_1 \geq 1 - 1/exp(|x|)$
   - NOの時 $p_1 \leq 1/exp(|x|)$
3. *U*は多項式個の$u_i \in \{H, T, CX\}$で構成される: $U = \prod_{i=1}^{T} u_i$

を満たすユニタリ*U*が存在する。

$u_0 \equiv I^{\otimes |x|}$

量子計算の検証

ヒストリー状態

[A. Kitaev, A. Shen, M. N. Vyalyi, *Classical and Quantum Computation* (2002)]

問題が**BQP**に含まれているということは、定義より、任意のインスタンス*x*に対して

$$U(|x\rangle|0^m\rangle)$$

s.t.

1. *m*はインスタンスサイズ*|x|*の多項式
2. *1*量子ビット目を測定した時に*1*が出る確率は、
   - YESの時 $p_1 \geq 1 - 1/exp(|x|)$
   - NOの時 $p_1 \leq 1/exp(|x|)$
3. *U*は多項式個の$u_i \in \{H, T, CX\}$で構成される: $U = \prod_{i=1}^{T} u_i$

を満たすユニタリ*U*が存在する。

このユニタリを使って、以下のように**ヒストリー状態**を定義する:

$$|h\rangle \equiv \frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} u_t \ldots u_1 u_0 (|x\rangle|0^m\rangle)|t\rangle$$

$u_0 \equiv I^{\otimes |x|}$

量子計算の検証

ヒストリー状態

[A. Kitaev, A. Shen, M. N. Vyalyi, *Classical and Quantum Computation* (2002)]

問題が**BQP**に含まれているということは、定義より、任意のインスタンス*x*に対して

$$U(|x\rangle|0^m\rangle)$$

s.t.

1. *m*はインスタンスサイズ*|x|*の多項式
2. *1*量子ビット目を測定した時に*1*が出る確率は、
   - YESの時 $p_1 \geq 1 - 1/exp(|x|)$
   - NOの時 $p_1 \leq 1/exp(|x|)$
3. *U*は多項式個の$u_i \in \{H, T, CX\}$で構成される: $U = \prod_{i=1}^{T} u_i$

を満たすユニタリ*U*が存在する。

このユニタリを使って、以下のように**ヒストリー状態**を定義する:

$$|h\rangle \equiv \frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} u_t \ldots u_1 u_0 (|x\rangle|0^m\rangle)|t\rangle$$

ステップ数の2進数表示(*log*量子ビット)

$x = x_{|x|} \ldots x_2 x_1$

量子計算の検証

ハミルトニアンの構成

[A. Kitaev, A. Shen, M. N. Vyalyi, *Classical and Quantum Computation* (2002)]

$$|h\rangle \equiv \frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} u_t \ldots u_1 u_0 (|x\rangle|0^m\rangle)|t\rangle$$

YESの時にヒストリー状態のエネルギーが低くなるようなハミルトニアンを作りたい

- 性質

1. ステップ*t=0*(計算開始前)で、入力は*x*になっている。

$$H_{\text{in}} \equiv \sum_{i=1}^{|x|} H_{\text{in},i}$$

$$H_{\text{in},i} \equiv (I - |x_i\rangle\langle x_i|)_i \otimes I^{\otimes m} \otimes |t=0\rangle\langle t=0|$$

量子計算の検証

ハミルトニアンの構成

[A. Kitaev, A. Shen, M. N. Vyalyi, *Classical and Quantum Computation* (2002)]

$$|h\rangle \equiv \frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} u_t \dots u_1 u_0 (|x\rangle|0^m\rangle)|t\rangle$$

YESの時にヒストリー状態のエネルギーが低くなるようなハミルトニアンを作りたい

- 性質

1. ステップ*t=0*(計算開始前)で、入力は*x*になっている。

ヒストリー状態のエネルギーは

$$\langle h|H_{\text{in}}|h\rangle = \sum_i \langle h|H_{\text{in},i}|h\rangle = \sum_i \frac{\langle x|(I - |x_i\rangle\langle x_i)_i|x\rangle}{T+1} = 0$$

量子計算の検証

ハミルトニアンの構成

[A. Kitaev, A. Shen, M. N. Vyalyi, *Classical and Quantum Computation* (2002)]

$$|h\rangle \equiv \frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} u_t \dots u_1 u_0 (|x\rangle |0^m\rangle) |t\rangle$$

YESの時にヒストリー状態のエネルギーが低くなるようなハミルトニアンを作りたい

- 性質

2. ステップ*t=T*(計算終了時)で、*1*量子ビット目が*1*になっている確率は高い。
(∵**BQP**の定義より)

$$H_{\text{out}} \equiv (|0\rangle\langle 0|)_1 \otimes I^{\otimes m} \otimes |t=T\rangle\langle t=T|$$

量子計算の検証

ハミルトニアンの構成

[A. Kitaev, A. Shen, M. N. Vyalyi, *Classical and Quantum Computation* (2002)]

$$|h\rangle \equiv \frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} u_t \dots u_1 u_0 (|x\rangle|0^m\rangle)|t\rangle$$

YESの時にヒストリー状態のエネルギーが低くなるようなハミルトニアンを作りたい

- 性質

2. ステップ*t=T*(計算終了時)で、*1*量子ビット目が*1*になっている確率は高い。
(∵**BQP**の定義より)

$$H_{\text{out}} \equiv (|0\rangle\langle 0|)_1 \otimes I^{\otimes m} \otimes |t=T\rangle\langle t=T|$$

この時、エネルギーは

$$\langle h|H_{\text{out}}|h\rangle = \frac{(\langle x|\langle 0^m|)U^\dagger (I - |1\rangle\langle 1|)_1 U(|x\rangle|0^m\rangle)}{T+1} = \frac{1-p_{\text{acc}}}{T+1} \leq \frac{1}{exp(|x|)}$$

量子計算の検証

ハミルトニアンの構成

[A. Kitaev, A. Shen, M. N. Vyalyi, *Classical and Quantum Computation* (2002)]

$$|h\rangle \equiv \frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} u_t \dots u_1 u_0 (|x\rangle|0^m\rangle)|t\rangle$$

YESの時にヒストリー状態のエネルギーが低くなるようなハミルトニアンを作りたい

- 性質

3. ステップが*t-1* → *t*になった時、u_tがかけられる。

$$H_{\mathrm{prop}} \equiv \sum_{t=1}^{T} H_{\mathrm{prop},t}$$

$$H_{\mathrm{prop},t} \equiv \frac{I^{\otimes(|x|+m)} \otimes (|t-1\rangle\langle t-1| + |t\rangle\langle t|) - u_t \otimes I^{\otimes m} \otimes |t\rangle\langle t-1| - u_t^{\dagger} \otimes I^{\otimes m} \otimes |t-1\rangle\langle t|}{2}$$

量子計算の検証

ハミルトニアンの構成

[A. Kitaev, A. Shen, M. N. Vyalyi, *Classical and Quantum Computation* (2002)]

$$|h\rangle \equiv \frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} u_t \dots u_1 u_0 (|x\rangle|0^m\rangle)|t\rangle$$

YESの時にヒストリー状態のエネルギーが低くなるようなハミルトニアンを作りたい

- 性質

3. ステップが*t-1* → *t*になった時、u_tがかけられる。

ヒストリー状態のエネルギーは

$$\langle h|H_{\mathrm{prop}}|h\rangle = \sum_{t=1}^{T} \langle h|H_{\mathrm{prop},t}|h\rangle = \sum_{t=1}^{T} \frac{2 - 2\mathrm{Re}\left[\langle h|(u_t \otimes I^{\otimes m} \otimes |t\rangle\langle t-1|)|h\rangle\right]}{2(T+1)} = 0$$

$\because \langle h|(u_t \otimes I^{\otimes m} \otimes |t\rangle\langle t-1|)|h\rangle = (\langle x|\langle 0^m|)(u_0^\dagger \dots u_t^\dagger) u_t (u_{t-1} \dots u_0)(|x\rangle|0^m\rangle) = 1$

量子計算の検証

ハミルトニアンの構成

[A. Kitaev, A. Shen, M. N. Vyalyi, *Classical and Quantum Computation* (2002)]

$$|h\rangle \equiv \frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} u_t \dots u_1 u_0 (|x\rangle |0^m\rangle) |t\rangle$$

3つの性質をまとめて、ハミルトニアン

$$H = H_{\text{in}} + H_{\text{prop}} + H_{\text{out}}$$

を定義すると、YESの時のヒストリー状態のエネルギーは

$$\langle h|H|h\rangle = 0 + 0 + \frac{1}{exp(|x|)} = \frac{1}{exp(|x|)}$$

となり、とても小さい!!

量子計算の検証

ハミルトニアンの構成

[A. Kitaev, A. Shen, M. N. Vyalyi, *Classical and Quantum Computation* (2002)]

$$|h\rangle \equiv \frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} u_t \dots u_1 u_0 (|x\rangle |0^m\rangle) |t\rangle$$

3つの性質をまとめて、ハミルトニアン

$$H = H_{\text{in}} + H_{\text{prop}} + H_{\text{out}}$$

を定義すると、YESの時のヒストリー状態のエネルギーは

$$\langle h|H|h\rangle = 0 + 0 + \frac{1}{exp(|x|)} = \frac{1}{exp(|x|)}$$

となり、とても小さい!!

NOの時にちゃんとエネルギーは高くなるのか？

量子計算の検証

ハミルトニアンの構成

[A. Kitaev, A. Shen, M. N. Vyalyi, *Classical and Quantum Computation* (2002)]

✓ NOの時にエネルギーが高くなる直感的なイメージ

1. ヒストリー状態の場合

$$|h\rangle \equiv \frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} u_t \dots u_1 u_0 (|x\rangle |0^m\rangle) |t\rangle$$

YESの時と同様、

$$\langle h|H_{\rm in}|h\rangle = 0\,, \quad \langle h|H_{\rm prop}|h\rangle = 0$$

しかし、

大きい!!

$$\langle h|H_{\rm out}|h\rangle = \frac{1-p_{\rm acc}}{T+1} \geq \frac{1-1/exp(|x|)}{T+1}$$

量子計算の検証

ハミルトニアンの構成

[A. Kitaev, A. Shen, M. N. Vyalyi, *Classical and Quantum Computation* (2002)]

✓ NOの時にエネルギーが高くなる直感的なイメージ

2. 異なるユニタリ行列を使った場合

$$|h\rangle \equiv \frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} v_t \dots v_1 v_0 \left(|x\rangle|0^m\rangle\right)|t\rangle$$

適切なユニタリ行列を使えば、

$$\langle h|H_{\text{in}}|h\rangle = 0\,, \quad \langle h|H_{\text{out}}|h\rangle = 0$$

と出来るが、計算方法が正しくないため、

$$\langle h|H_{\text{prop}}|h\rangle$$

が大きくなってしまう。

量子計算の検証

ハミルトニアンの構成

[A. Kitaev, A. Shen, M. N. Vyalyi, *Classical and Quantum Computation* (2002)]

✓ NOの時にエネルギーが高くなる直感的なイメージ

3. 異なる入力を使った場合

$$|h\rangle \equiv \frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} u_t \dots u_1 u_0 (|y\rangle |0^m\rangle) |t\rangle$$

異なる入力を使えば、

$$\langle h|H_{\rm prop}|h\rangle = 0\,, \quad \langle h|H_{\rm out}|h\rangle = \frac{1}{exp(|x|)}$$

と出来るが、入力が正しくないため、

$$\langle h|H_{\rm in}|h\rangle \geq \frac{1}{T+1}$$

大きい!!

量子計算の検証

ハミルトニアンの構成

[A. Kitaev, A. Shen, M. N. Vyalyi, *Classical and Quantum Computation* (2002)]

一般に、NOの時には、どんな量子状態に対しても、

$$\langle\psi|H|\psi\rangle \geq \frac{1}{4(T+1)^3}$$

が成り立つことが示されている。[D. Aharonov and T. Naveh, arXiv:quant-ph/0210077]

量子計算の検証

ハミルトニアンの構成

[A. Kitaev, A. Shen, M. N. Vyalyi, *Classical and Quantum Computation* (2002)]

一般に、NOの時には、どんな量子状態に対しても、

$$\langle\psi|H|\psi\rangle \geq \frac{1}{4(T+1)^3}$$

が成り立つことが示されている。[D. Aharonov and T. Naveh, arXiv:quant-ph/0210077]

Lemma 1 Let H_1 and H_2 be two Hermitian positive semi-definite matrices, and let N_1 and N_2 be the eigenspaces of the eigenvalue 0, respectively. If the angle between N_1 and N_2 is some $\theta > 0$, and the second eigenvalue of both H_1 and H_2 is $\geq \lambda$ then the minimal eigenvalue of $H_1 + H_2 \geq \lambda \sin^2(\theta/2)$.

量子計算の検証

ハミルトニアンの構成

[A. Kitaev, A. Shen, M. N. Vyalyi, *Classical and Quantum Computation* (2002)]

一般に、NOの時には、どんな量子状態に対しても、

$$\langle\psi|H|\psi\rangle \geq \frac{1}{4(T+1)^3}$$

が成り立つことが示されている。[D. Aharonov and T. Naveh, arXiv:quant-ph/0210077]

Lemma 1 Let H_1 and H_2 be two Hermitian positive semi-definite matrices, and let N_1 and N_2 be the eigenspaces of the eigenvalue 0, respectively. If the angle between N_1 and N_2 is some $\theta > 0$, and the second eigenvalue of both H_1 and H_2 is $\geq \lambda$ then the minimal eigenvalue of $H_1 + H_2 \geq \lambda \sin^2(\theta/2)$.

2つの空間から取ってきたベクトルの最小角度

$$\cos^2(\theta) = \max_{|\psi\rangle \in N_2}\{\langle\psi|\Pi_{N_1}|\psi\rangle\}$$

量子計算の検証

ハミルトニアンの構成

[A. Kitaev, A. Shen, M. N. Vyalyi, *Classical and Quantum Computation* (2002)]

一般に、NOの時には、どんな量子状態に対しても、

$$\langle\psi|H|\psi\rangle \geq \frac{1}{4(T+1)^3}$$

が成り立つことが示されている。[D. Aharonov and T. Naveh, arXiv:quant-ph/0210077]

$H_{\mathrm{in}} + H_{\mathrm{out}}$ H_{prop}

Lemma 1 Let H_1 and H_2 be two Hermitian positive semi-definite matrices, and let N_1 and N_2 be the eigenspaces of the eigenvalue 0, respectively. If the angle between N_1 and N_2 is some $\theta > 0$, and the second eigenvalue of both H_1 and H_2 is $\geq \lambda$ then the minimal eigenvalue of $H_1 + H_2 \geq \lambda \sin^2(\theta/2)$.

量子計算の検証

ハミルトニアンの構成

[A. Kitaev, A. Shen, M. N. Vyalyi, *Classical and Quantum Computation* (2002)]

一般に、NOの時には、どんな量子状態に対しても、

$$\langle\psi|H|\psi\rangle \geq \frac{1}{4(T+1)^3}$$

が成り立つことが示されている。[D. Aharonov and T. Naveh, arXiv:quant-ph/0210077]

$H_{\mathrm{in}} + H_{\mathrm{out}}$ H_{prop}

Lemma 1 Let H_1 and H_2 be two Hermitian positive semi-definite matrices, and let N_1 and N_2 be the eigenspaces of the eigenvalue 0, respectively. If the angle between N_1 and N_2 is some $\theta > 0$, and the second eigenvalue of both H_1 and H_2 is $\geq \lambda$ then the minimal eigenvalue of $H_1 + H_2 \geq \lambda \sin^2(\theta/2)$.

基底変換
+
ランダムウォークの理論

$$\frac{1}{2(T+1)^2}$$

量子計算の検証

ハミルトニアンの構成

[A. Kitaev, A. Shen, M. N. Vyalyi, *Classical and Quantum Computation* (2002)]

一般に、NOの時には、どんな量子状態に対しても、

$$\langle\psi|H|\psi\rangle \geq \frac{1}{4(T+1)^3}$$

が成り立つことが示されている。[D. Aharonov and T. Naveh, arXiv:quant-ph/0210077]

$H_{\rm in} + H_{\rm out}$ $H_{\rm prop}$

Lemma 1 Let H_1 and H_2 be two Hermitian positive semi-definite matrices, and let N_1 and N_2 be the eigenspaces of the eigenvalue 0, respectively. If the angle between N_1 and N_2 is some $\theta > 0$, and the second eigenvalue of both H_1 and H_2 is $\geq \lambda$ then the minimal eigenvalue of $H_1 + H_2 \geq \lambda \sin^2(\theta/2)$.

$\geq \frac{1}{2(T+1)}$

基底変換
+
ランダムウォークの理論

$\frac{1}{2(T+1)^2}$

量子計算の検証

ハミルトニアンの構成

[A. Kitaev, A. Shen, M. N. Vyalyi, *Classical and Quantum Computation* (2002)]

一般に、NOの時には、どんな量子状態に対しても、

$$\langle\psi|H|\psi\rangle \geq \frac{1}{4(T+1)^3}$$

が成り立つことが示されている。[D. Aharonov and T. Naveh, arXiv:quant-ph/0210077]

以上より、**BQP**問題の答えは、

適切なハミルトニアンの基底状態エネルギーの大小

で判断できる。

量子計算の検証

ハミルトニアンのlocality

上記で構成したハミルトニアンは

$$H_{\mathrm{out}} \equiv (|0\rangle\langle 0|)_1 \otimes I^{\otimes m} \otimes |t = T\rangle\langle t = T|$$

等のように、ステップ数の2進数表現を含んでいるため、

logローカル

量子計算の検証

ハミルトニアンのlocality

上記で構成したハミルトニアンは

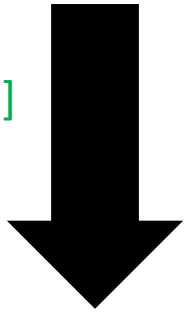
$$H_{\mathrm{out}} \equiv (|0\rangle\langle 0|)_1 \otimes I^{\otimes m} \otimes |t = T\rangle\langle t = T|$$

等のように、ステップ数の2進数表現を含んでいるため、

logローカル

[A. Kitaev, A. Shen, M. N. Vyalyi, *Classical and Quantum Computation* (2002)]

[J. D. Biamonte and P. J. Love, PRA **78**, 012352 (2008)]



- ステップ数のunary表現
- 摂動論

etc…

2ローカル

量子計算の検証

$$\forall i,j,\ p_{i,j} > 0 \quad \text{s.t.} \sum_{i<j} p_{i,j} = 1$$

$$\forall i,j,\ s_{i,j} \in \{+1,-1\}$$

ハミルトニアンのlocality

上記で構成したハミルトニアンは

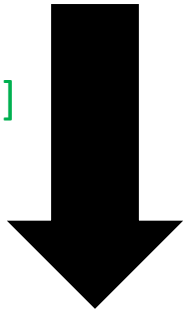
$$H_{\text{out}} \equiv (|0\rangle\langle 0|)_1 \otimes I^{\otimes m} \otimes |t=T\rangle\langle t=T|$$

等のように、ステップ数の2進数表現を含んでいるため、

logローカル

[A. Kitaev, A. Shen, M. N. Vyalyi, *Classical and Quantum Computation* (2002)]

[J. D. Biamonte and P. J. Love, PRA **78**, 012352 (2008)]



- ステップ数のunary表現
- 摂動論 etc…

2ローカル

特に、

[T. Morimae, arXiv:2003.10712]

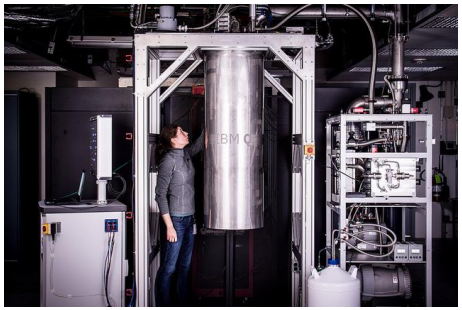
$$H \equiv \sum_{i<j} \frac{p_{i,j}}{2} \left(\frac{I^{\otimes n} + s_{i,j} X_i \otimes X_j}{2} + \frac{I^{\otimes n} + s_{i,j} Z_i \otimes Z_j}{2} \right)$$

量子計算の検証

Morimae-Fitzsimonsプロトコル

[T. Morimae, arXiv:2003.10712]

[※1]



①この問題の答えはYES, NOどっち？

③答えは*b*(=YES or NO)です

④MFプロトコル (1ラウンド量子通信)

②問題を量子計算機で解く

*b*が正しい時、受理確率は$p_{\mathrm{acc}} \geq 1 - 1/exp(|x|)$
*b*が正しくない時、$p_{\mathrm{acc}} \leq 1/exp(|x|)$

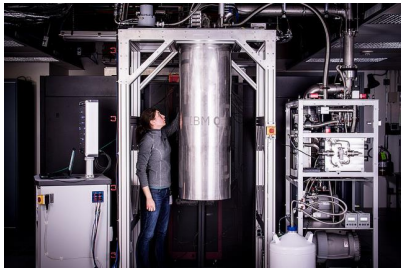
※1https://www.popularmechanics.com/technology/a29105270/most-powerful-quantum-computer/

量子計算の検証

Morimae-Fitzsimonsプロトコルの詳細

[T. Morimae, arXiv:2003.10712]

- サーバが送った答えがYESだった場合



ρ ⟶

[※1]

YESが正しい場合: $\rho = |h\rangle\langle h|$

本当はNOが正しい場合: ρは任意の量子状態

※1https://www.popularmechanics.com/technology/a29105270/most-powerful-quantum-computer/

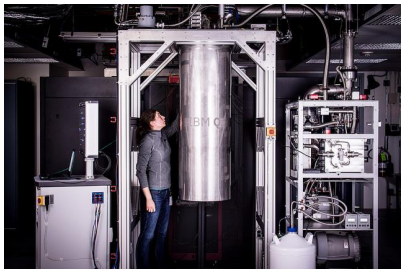
※1https://www.popularmechanics.com/technology/a29105270/most-powerful-quantum-computer/

量子計算の検証

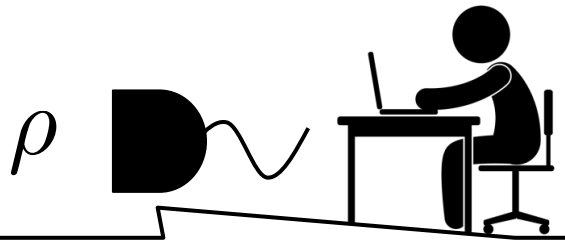
Morimae-Fitzsimonsプロトコルの詳細

[T. Morimae, arXiv:2003.10712]

- サーバが送った答えがYESだった場合



[※1]



1. $p_{i,j}$の確率で、ペア*(i,j)*選ぶ。
2. *1/2*の確率で
$$Z_i \otimes Z_j \quad \text{or} \quad X_i \otimes X_j$$
を選ぶ。
3. 前者の時は、*i,j*番目の量子ビットを計算基底で測定
後者の時は、*i,j*番目の量子ビットに*H*をかけた後、計算基底で測定
4. 測定結果の足し算をaとし、
$$-s_{i,j} = (-1)^a$$
となれば受理する。

量子計算の検証

Morimae-Fitzsimonsプロトコルの詳細

[T. Morimae, arXiv:2003.10712]

- サーバが送った答えがYESだった場合

この時の受理確率は

$$
\begin{aligned}
p_{\mathrm{acc}} &= \sum_{i<j} \frac{p_{i,j}}{2} \left(\mathrm{Tr}\left[\rho \frac{I^{\otimes n} - s_{i,j} X_i \otimes X_j}{2} \right] + \mathrm{Tr}\left[\rho \frac{I^{\otimes n} - s_{i,j} Z_i \otimes Z_j}{2} \right] \right) \\
&= \sum_{i<j} \frac{p_{i,j}}{2} \left(1 - \mathrm{Tr}\left[\rho \frac{I^{\otimes n} + s_{i,j} X_i \otimes X_j}{2} \right] + 1 - \mathrm{Tr}\left[\rho \frac{I^{\otimes n} + s_{i,j} Z_i \otimes Z_j}{2} \right] \right) \\
&= 1 - \mathrm{Tr}\left[\rho H \right]
\end{aligned}
$$

$$
\begin{cases}
\geq 1 - \dfrac{1}{exp(|x|)} & \text{(本当にYESの時)} \\
\leq 1 - \dfrac{1}{4(T+1)^3} & \text{(本当はNOの時)}
\end{cases}
$$

量子計算の検証

Morimae-Fitzsimonsプロトコルの詳細

[T. Morimae, arXiv:2003.10712]

- サーバが送った答えがYESだった場合

この時の受理確率は

$$
\begin{aligned}
p_{\mathrm{acc}} &= \sum_{i<j} \frac{p_{i,j}}{2} \left(\mathrm{Tr}\left[\rho \frac{I^{\otimes n} - s_{i,j} X_i \otimes X_j}{2} \right] + \mathrm{Tr}\left[\rho \frac{I^{\otimes n} - s_{i,j} Z_i \otimes Z_j}{2} \right] \right) \\
&= \sum_{i<j} \frac{p_{i,j}}{2} \left(1 - \mathrm{Tr}\left[\rho \frac{I^{\otimes n} + s_{i,j} X_i \otimes X_j}{2} \right] + 1 - \mathrm{Tr}\left[\rho \frac{I^{\otimes n} + s_{i,j} Z_i \otimes Z_j}{2} \right] \right) \\
&= 1 - \mathrm{Tr}\left[\rho H \right]
\end{aligned}
$$

$$
\begin{cases}
\geq 1 - \dfrac{1}{exp(|x|)} & \text{(本当にYESの時)} \\
\leq 1 - \dfrac{1}{4(T+1)^3} & \text{(本当はNOの時)}
\end{cases}
$$

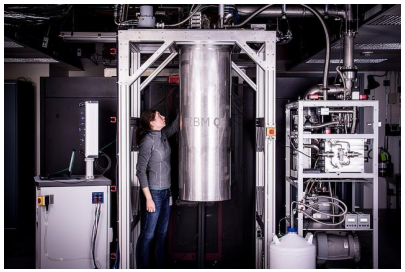
差が*1/poly*あるので、
差を“ほぼ”*1*に増幅出来る。

量子計算の検証

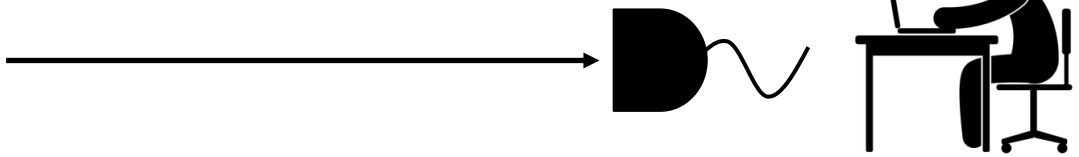
Morimae-Fitzsimonsプロトコルの詳細

[T. Morimae, arXiv:2003.10712]

- 受理確率の差の増幅



ρ



[※1]

※1https://www.popularmechanics.com/technology/a29105270/most-powerful-quantum-computer/

※1https://www.popularmechanics.com/technology/a29105270/most-powerful-quantum-computer/

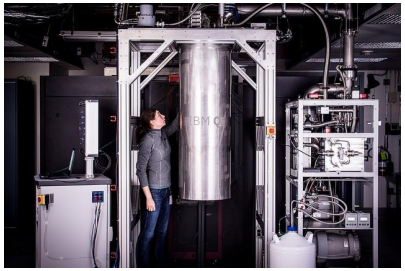
量子計算の検証

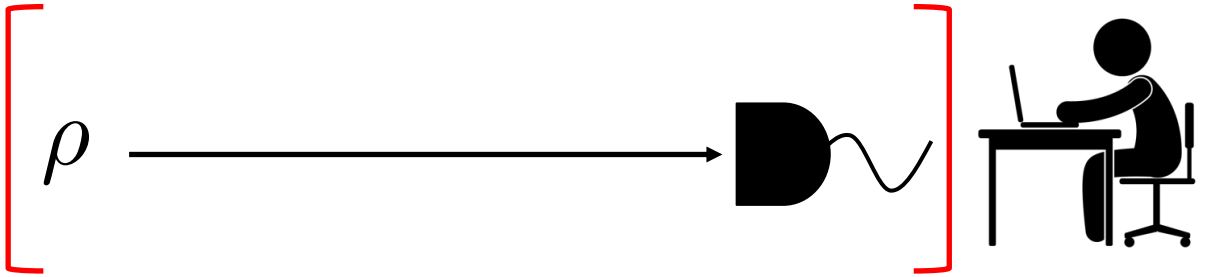
Morimae-Fitzsimonsプロトコルの詳細

[T. Morimae, arXiv:2003.10712]

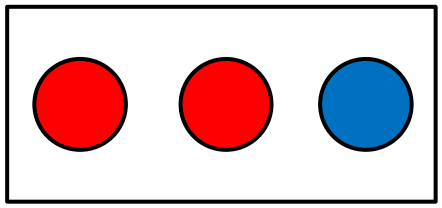
- 受理確率の差の増幅

[※1]





- イメージ



1回だけ引く場合

赤: *2/3* → 増える → 赤: *8/27+12/27=20/27*

青: *1/3* → 減る → 青: *6/27+1/27=7/27*

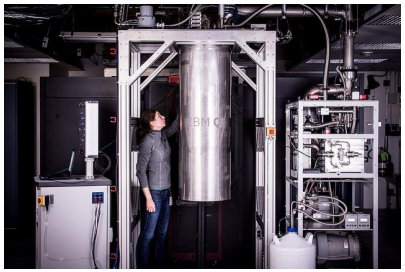
3回引いて多数決を取る場合

量子計算の検証

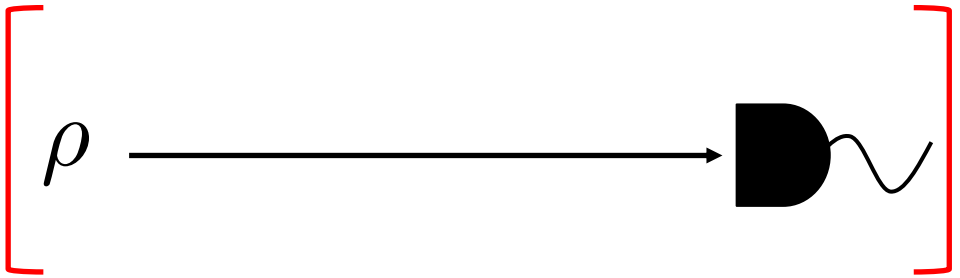
Morimae-Fitzsimonsプロトコルの詳細

[T. Morimae, arXiv:2003.10712]

- 受理確率の差の増幅



[※1]



$\times poly(|x|)$

正しい時、受理確率は $p_{\mathrm{acc}} \geq 1 - 1/exp(|x|)$

正しくない時、 $p_{\mathrm{acc}} \leq 1/exp(|x|)$

※1https://www.popularmechanics.com/technology/a29105270/most-powerful-quantum-computer/

量子計算の検証

Morimae-Fitzsimonsプロトコルの詳細

[T. Morimae, arXiv:2003.10712]

- サーバが送った答えがNOだった場合

BQP = **coBQP**より、オリジナルの問題の補問題を考えることで、同じ議論が可能

例) 整数Nはk以下の素因数を持っているか？

整数Nはk以下の素因数を持っていないか？

量子計算の検証

Morimae-Fitzsimonsプロトコルの詳細

[T. Morimae, arXiv:2003.10712]

- サーバが送った答えがNOだった場合

BQP = coBQPより、オリジナルの問題の補問題を考えることで、同じ議論が可能

例) 整数Nはk以下の素因数を持っているか？

⇓

整数Nはk以下の素因数を持っていないか？

オリジナルの問題の答えがNOの時、
補問題の答えはYES

⇒ NOインスタンスに対しても、対応したヒストリー状態が存在する

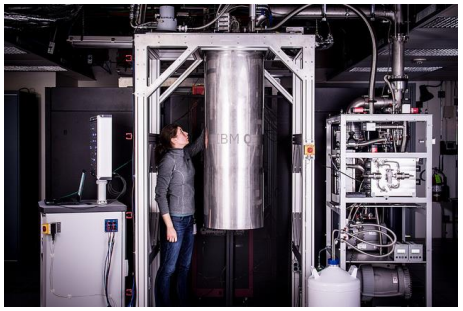
※1https://www.popularmechanics.com/technology/a29105270/most-powerful-quantum-computer/

次の水谷さんのトークでは

ポストホック検証(Morimae-Fitzsimonsプロトコル)

[J. F. Fitzsimons, M. Hajdušek, T. Morimae, PRL **120**, 040501 (2018)]

[※1]

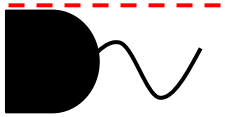


②問題を量子計算機で解く

①この問題の答えはYES, NOどっち？

③答えは*b*(=YES or NO)です

ρ



*b*が正しい時　$p_{\mathrm{acc}} \geq 1 - 1/exp(|x|)$

*b*が正しくない時 $p_{\mathrm{acc}} \leq 1/exp(|x|)$

④MFプロトコル (1ラウンド量子通信)

欠点: 検証者(ユーザ)に1量子ビットの量子測定が必要

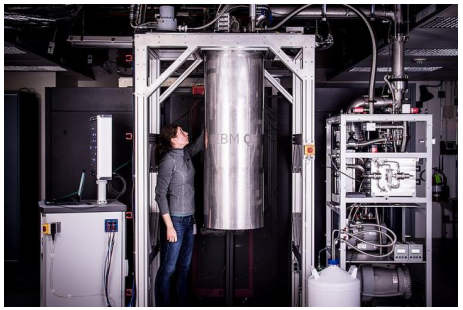
※1https://www.popularmechanics.com/technology/a29105270/most-powerful-quantum-computer/

次の水谷さんのトークでは

ポストホック検証(Morimae-Fitzsimonsプロトコル)

[J. F. Fitzsimons, M. Hajdušek, T. Morimae, PRL **120**, 040501 (2018)]

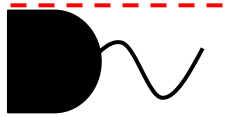
[※1]



②問題を量子計算機で解く

①この問題の答えはYES, NOどっち？

③答えは*b*(=YES or NO)です

ρ → 

*b*が正しい時　$p_{\mathrm{acc}} \geq 1 - 1/exp(|x|)$

*b*が正しくない時 $p_{\mathrm{acc}} \leq 1/exp(|x|)$

④MFプロトコル (1ラウンド量子通信)

欠点: 検証者(ユーザ)に1量子ビットの量子測定が必要

[U. Mahadev, FOCS2018]

→ 耐量子計算機暗号で、検証者を古典に出来る