

# 量子回路と量子アルゴリズムの基礎

---

東京大学大学院理学系研究科 量子ソフトウェア寄付講座 大久保毅

# コンテンツ

---

- 量子コンピュータと量子アルゴリズム
  - 量子コンピュータ？
  - 量子アルゴリズムの例
  - 量子超越性
- 量子回路の基礎
  - 基本的なゲート操作
  - 量子的な演算と量子測定
  - 古典シミュレーション
- 量子アニーリングの概略
- まとめ

# 量子コンピュータと量子アルゴリズム

# 古典コンピュータと量子コンピュータの情報単位

## 古典コンピュータ

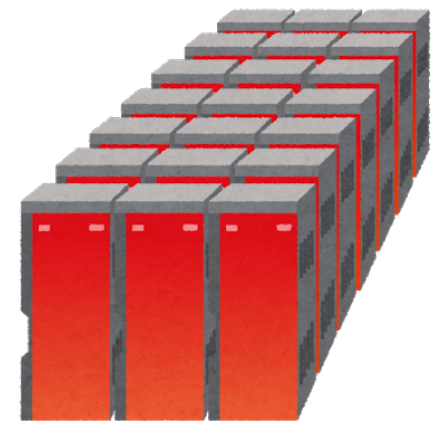
(例えば) 0と1の2状態 (bit) で情報 (状態) を表す

1 bit: 状態は"0" or "1"

2 bits: 状態は"00", "01", "10", "11"

⋮

$N$  bits: 状態は全部で $2^N$ 個



## 量子コンピュータ

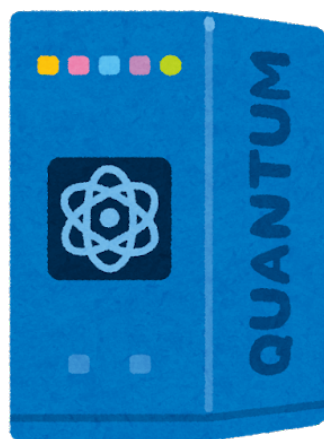
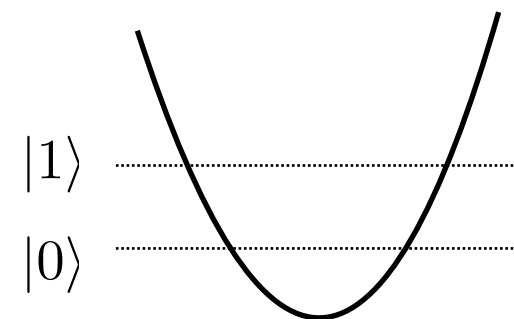
(例えば)  $2^N$  "準位"を持つ量子系 (qubit) で情報を表す

1 qubit: 状態は"基底"  $|0\rangle, |1\rangle$  の任意の重ね合わせ (線形結合)

### 重ね合わせの例

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \longrightarrow |\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

\*  $\alpha, \beta$  は一般に複素数



# 量子ビットの多体系

1 qubit ● 1つの量子ビットの状態は **2つの基底ベクトル** で表現される  
 $|0\rangle, |1\rangle$

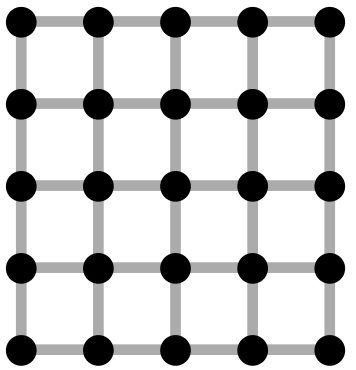
➡  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$  **2次元ベクトル**

2 qubits ●—● 2つの量子ビット系の状態は **4つの基底ベクトル** で表現される  
 $|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle$

(簡略化した表現:  $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ )

➡  $|\Psi\rangle = C_{00}|00\rangle + C_{01}|01\rangle + C_{10}|10\rangle + C_{11}|11\rangle = \begin{pmatrix} C_{00} \\ C_{01} \\ C_{10} \\ C_{11} \end{pmatrix}$  **4次元ベクトル**

$N$  qubits



状態を表すベクトルの次元  $2^N$

$$|\Psi\rangle = \sum_{\{i_1, i_2, \dots, i_N\}} \Psi_{i_1 i_2 \dots i_N} |i_1 i_2 \dots i_N\rangle$$

指数関数的に大きい!  
 $2^{10} = 1024 \sim 10^3$   
 $2^{20} \sim 10^6, 2^{100} \sim 10^{30}$

# 量子状態と確率

1 qubit状態 :  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$

➡ qubitが状態  $|0\rangle$  にいるか  $|1\rangle$  にいるかを観測すると

$$\begin{aligned} \text{確率 } P(|0\rangle) &= \frac{|\alpha|^2}{|\alpha|^2 + |\beta|^2} \text{ で状態 } |0\rangle \\ \text{確率 } P(|1\rangle) &= \frac{|\beta|^2}{|\alpha|^2 + |\beta|^2} \text{ で状態 } |1\rangle \\ &= 1 - P(|0\rangle) \end{aligned} \quad \text{が観測される}$$

＊以降、量子状態は規格化されているとする

$$\langle\Psi|\Psi\rangle \equiv (\alpha^* \beta^*) \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \underline{|\alpha|^2 + |\beta|^2 = 1}$$

$$N\text{-qubit状態 : } |\Psi\rangle = \sum_{\{i_1, i_2, \dots, i_N\}} \Psi_{i_1 i_2 \dots i_N} |i_1 i_2 \dots i_N\rangle$$

➡  $2^N$ 種類の古典bit状態がそれぞれ確率的に観測される  
 $|010111\dots\rangle$

# 量子状態の古典計算困難性

量子状態の従う運動方程式＝シュレディンガー方程式

$$i\hbar \frac{\partial}{\partial t} |\Psi\rangle = \mathcal{H} |\Psi\rangle$$

$|\Psi\rangle$  : 量子状態 ( $2^N$ 次元のベクトル)

$\mathcal{H}$  : ハミルトニアン ( $2^N \times 2^N$ の行列)

(時間に依存しない場合)

$$\mathcal{H} |\Psi\rangle = E |\Psi\rangle$$

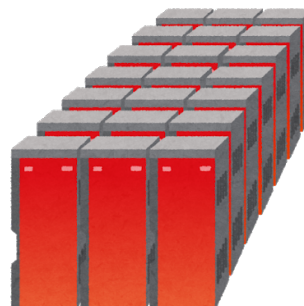
$E$  : エネルギー (数字)

指数関数的に大きな次元を持つベクトルの運動方程式

古典コンピュータでこの運動方程式を厳密に解くには、

膨大なメモリと膨大な計算時間が必要

スパコン富岳を用いても、50 qubits程度しか計算できない



# 制御された量子系と量子コンピュータ

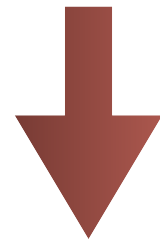
量子系を制御して望みの動作をさせる

➡ 古典計算機では計算できないことを"計算"できる可能性

＊情報を取り出せないと計算として意味がない

**量子コンピュータ＝高度に制御された量子系**

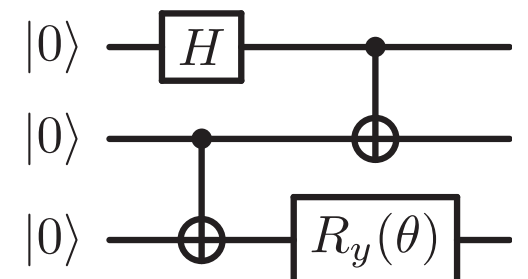
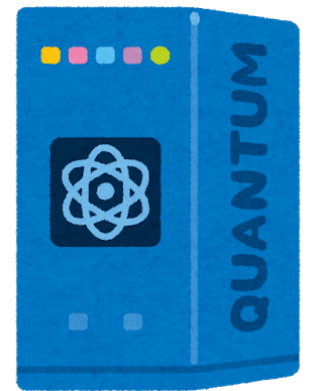
計算の目的に合わせて量子状態を変化（運動）させる



量子状態を変化させる操作の処方箋

||

**量子アルゴリズム**





# 量子アルゴリズムの例

## Shorのアルゴリズム (P. W. Shor, 1994)

素因数分解 :  $15 = 3 \times 5$ ,  $102 = 2 \times 3 \times 17$ ,  $10439 = 11 \times 13 \times 73$

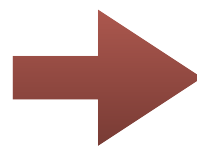
大きな数の素因数分解はどんどん"困難"になる

古典コンピュータでは、 $n = \log N$  ( $\sim$ 桁数) に対して  $\sim \exp n$  の計算時間

➡ 量子コンピュータでのShorのアルゴリズムを使うと、  
 $n$  の多項式の計算時間で素因数分解できる

古典コンピュータ

$\exp n$



量子コンピュータ

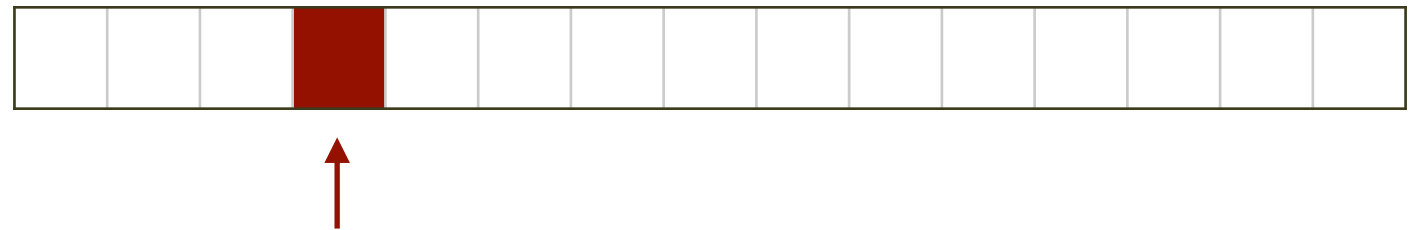
$n$  の多項式

指数関数の計算時間削減！

# 量子アルゴリズムの例

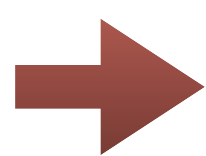
## Groverのアルゴリズム (L. K. Grover, 1996)

非構造化データの探索：  $N$ 個のデータ中で特定の"アタリ"はどこ？



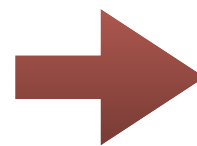
古典コンピュータ：

基本的には一つ一つ"箱"をチェックしていく  $\sim O(N)$



量子コンピュータでのGrover のアルゴリズムを使うと、  
 $\sim O(\sqrt{N})$  の計算時間で探索可能

古典コンピュータ  
 $\sim O(N)$



量子コンピュータ  
 $\sim O(\sqrt{N})$

"2乗"の計算時間削減！

# 量子アルゴリズムの例

## 量子アニーリング (T. Kadowaki and H. Nishimori, 1998)

組み合わせ最適化問題：(例) 巡回セールスマン問題

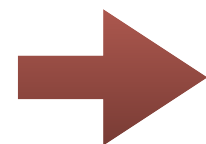
古典コンピュータ：

最適解の探索→NP困難

(問題サイズに対して指数関数の時間)

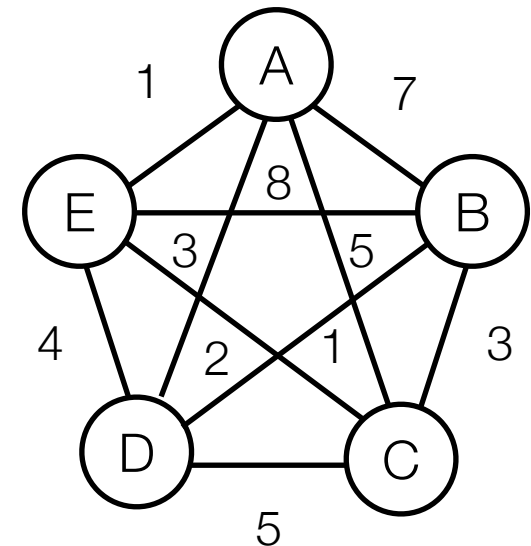
近似解の探索→シミュレーテッド・アニーリング

(**"温度"ゆらぎ**を上手に利用して解を探索する)



量子系を用いた量子アニーリング

**量子ゆらぎ**を上手に利用して解を探索



- 特定の例で、古典的なシミュレーテッド・アニーリングより効率的との結果はある
- 一般的に量子アニーリングがその他の古典アルゴリズムに**勝る**という証明はまだない

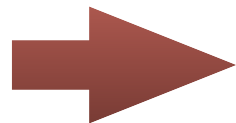
# 量子アルゴリズムの例

## 変分量子アルゴリズム (Review: M. Cerezo *et al.*, Nature Reviews Physics, 3, 525 (2021))

種々の最適化問題を

- ・ 量子コンピュータ上で量子状態として表現した「試行関数」
- ・ 古典コンピュータによる試行関数パラメタの最適化

により、近似的に解く



- ・ 試行関数の評価に量子コンピュータを用いる点で優位？
- ・ 一般に、量子コンピュータでのノイズの影響が小さい

- ・ 分子系の量子化学計算、物性物理の基底状態計算、ダイナミクス計算、量子機械学習...
- ・ 現在実現している、NISQ (Noisy Intermediate Scale Quantum) 量子コンピュータで有効に働くとの期待
- ・ 一般に、**古典コンピュータに勝るという証明はない**

# 量子超越性・量子優位性

---

量子コンピュータで、古典コンピュータが（現実的な時間で）  
解けない問題を解く

- 2019年, Google の超伝導量子ビットコンピュータ

F. Arute, *et al.*, "Quantum supremacy using a programmable superconducting processor", Nature, 574, 505 (2019).

問題：ランダムな量子回路の出力サンプリング

古典コンピュータ = 10,000年（という主張）

量子コンピュータ = 200秒

- 2020年, 中国科学技術大学の光量子コンピュータ

H.-S. Zhong, *et al.*, "Quantum computational advantage using photons", Science, 370, 1460 (2020).

問題：Gaussian Boson sampling (量子回路の出力サンプリング)

古典コンピュータ = 6億年（という主張）

量子コンピュータ = 200秒

# 量子回路の基礎

# 量子回路

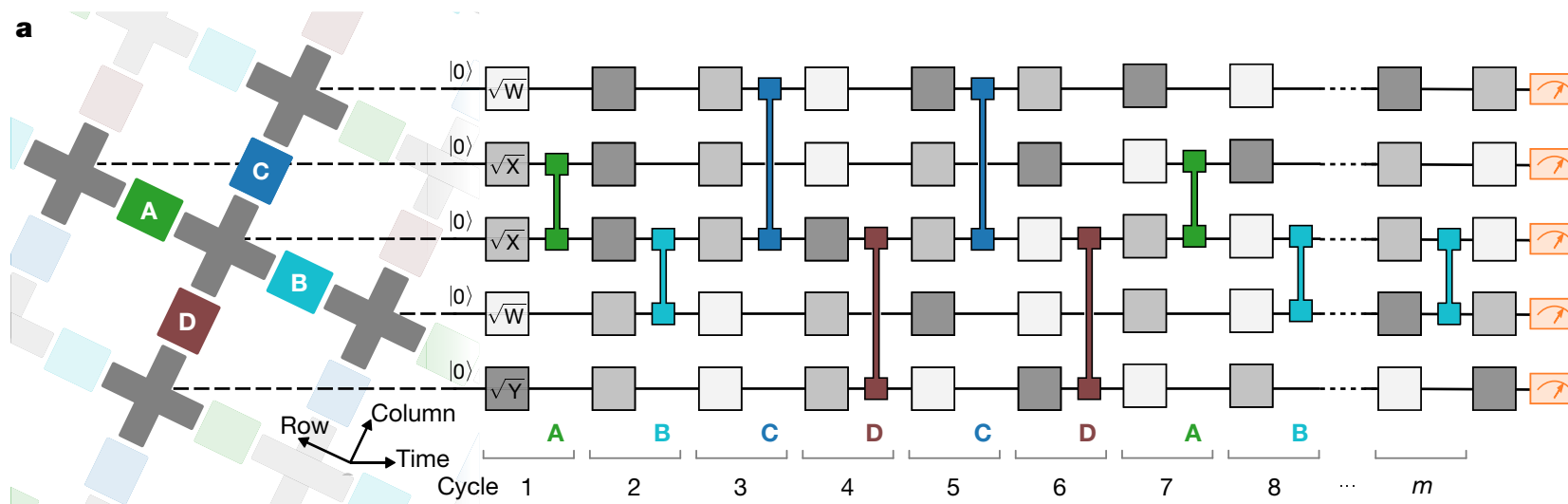
量子回路：

量子ビットに演算するゲート操作の回路図

- 量子ビットの初期状態を準備
- 順番に「量子ゲート」を演算する
  - 量子ゲートはユニタリ行列  $UU^\dagger = U^\dagger U = I$
  - 1qubit、または2qubitに作用するものが基本
- 最後に「測定」して情報（計算結果）を得る

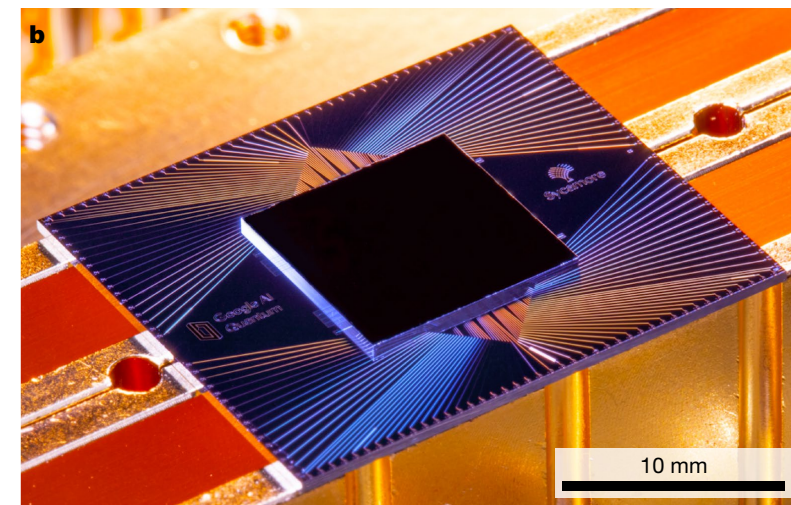
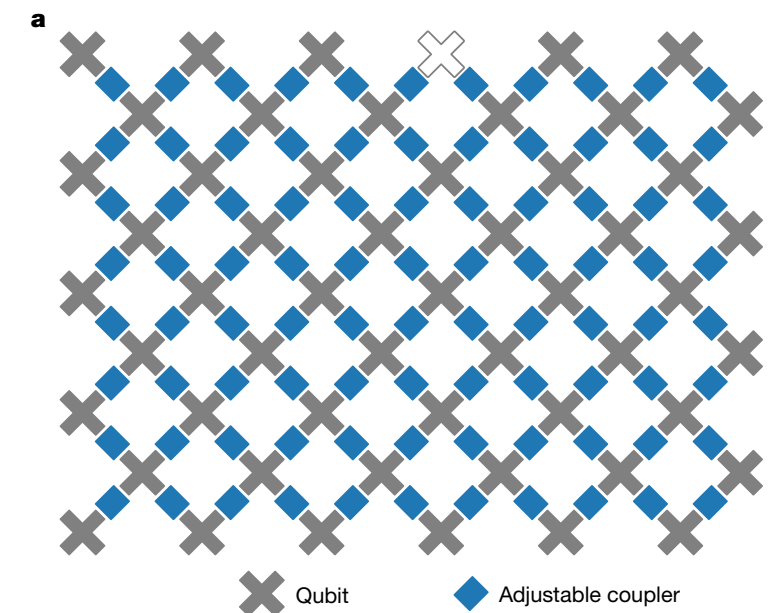
googleの"量子超越" 回路

F. Arute, *et al.*, Nature 574, 505 (2019)



googleの"量子超越" 回路

F. Arute, *et al.*, Nature 574, 505 (2019)



# 典型的な量子ゲート

---

$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$  の二つのベクトルで状態を表す

## 1 qubit ゲート

## 量子回路での記号

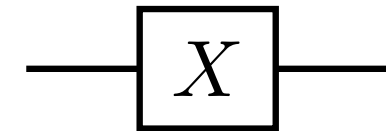
- $X$  ゲート (NOT ゲート)

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \rightarrow$$

ビットを反転

$$X|0\rangle = |1\rangle$$

$$X|1\rangle = |0\rangle$$



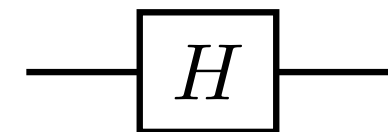
- $H$  (Hadamard) ゲート

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \rightarrow$$

重ね合わせ状態を生成

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

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





# 典型的な量子ゲート

$$|\Psi\rangle = C_{00}|00\rangle + C_{01}|01\rangle + C_{10}|10\rangle + C_{11}|11\rangle = \begin{pmatrix} C_{00} \\ C_{01} \\ C_{10} \\ C_{11} \end{pmatrix}$$

## 2-qubit ゲート

## 量子回路での記号

- CX (Controlled-NOT) ゲート 1番目のビットに依存して  
2番目のビットを反転

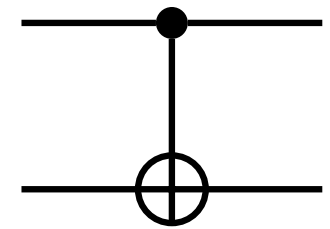
$$CX = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \rightarrow$$

$$CX|00\rangle = |00\rangle$$

$$CX|01\rangle = |01\rangle$$

$$CX|10\rangle = |11\rangle$$

$$CX|11\rangle = |10\rangle$$



- CZ (Controlled-Z) ゲート

$$CZ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \rightarrow$$

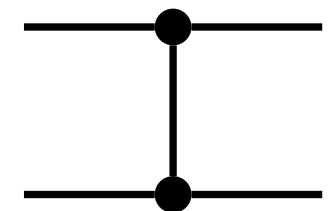
|11>にマイナス符号がつく

$$CZ|00\rangle = |00\rangle$$

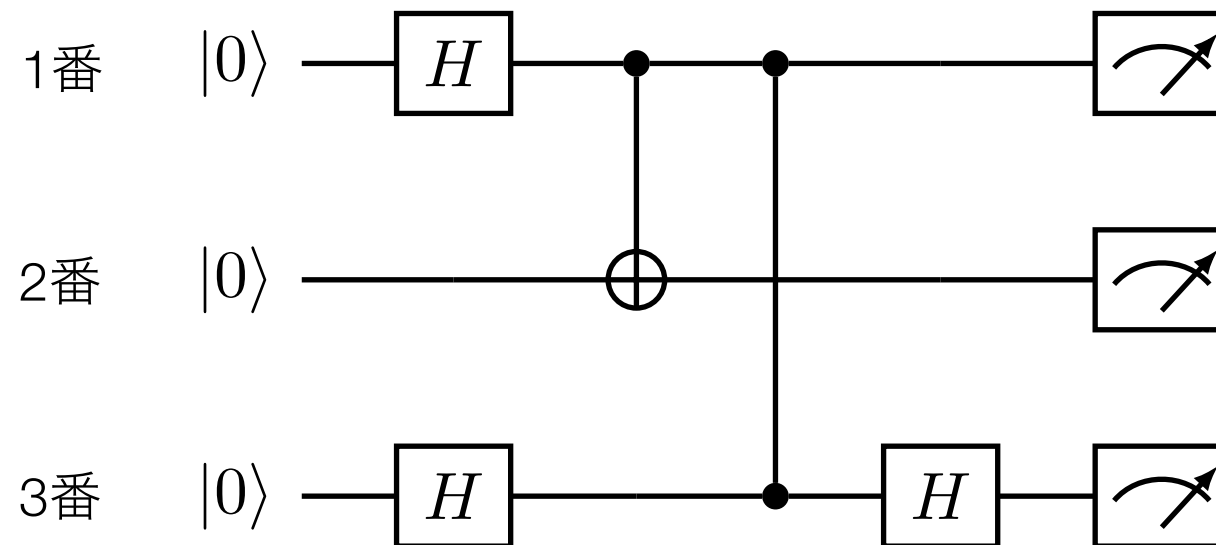
$$CZ|01\rangle = |01\rangle$$

$$CZ|10\rangle = |10\rangle$$

$$CZ|11\rangle = -|11\rangle$$



# 量子回路の例



## 動作確認

$$H_1, H_3 \quad |000\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$= \frac{1}{2}(|000\rangle + |001\rangle + |100\rangle + |101\rangle)$$

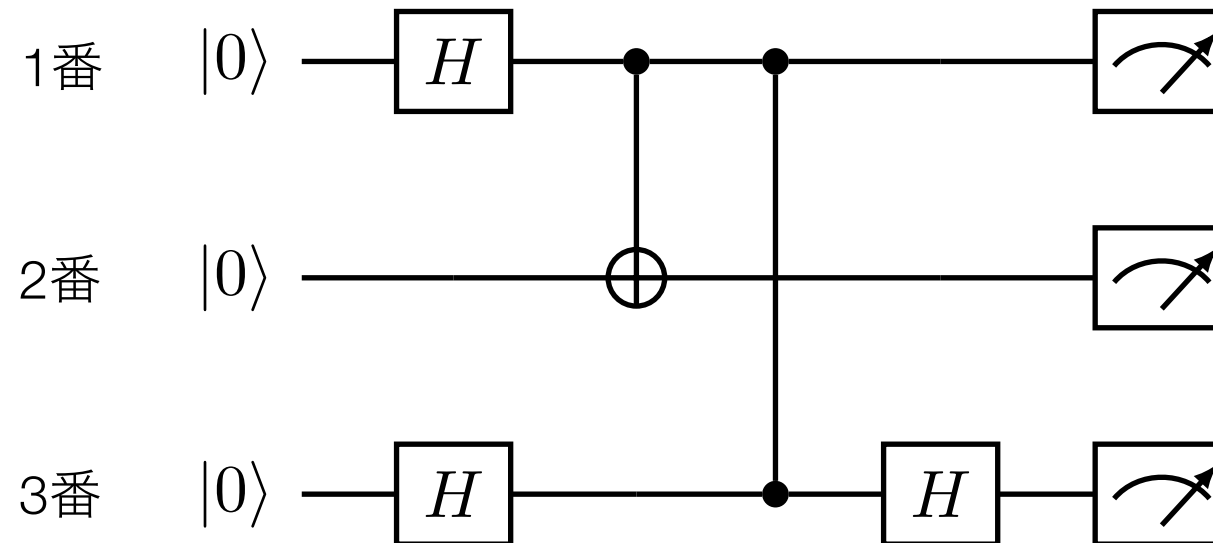
状態の分岐

$$CX_{12} \rightarrow \frac{1}{2}(|000\rangle + |001\rangle + |1\textcolor{red}{1}0\rangle + |1\textcolor{red}{1}1\rangle)$$

$$CZ_{13} \rightarrow \frac{1}{2}(|000\rangle + |001\rangle + |110\rangle - |111\rangle)$$

$$= \frac{1}{2}((|00\rangle + |11\rangle) \otimes |0\rangle + (|00\rangle - |11\rangle) \otimes |1\rangle)$$

# 量子回路の例



動作確認

$$\begin{aligned}
 H_3 & \frac{1}{2} ((|00\rangle + |11\rangle) \otimes |0\rangle + (|00\rangle - |11\rangle) \otimes |1\rangle) \\
 & \rightarrow \frac{1}{2} ((|00\rangle + |11\rangle) \otimes \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \\
 & \quad + (|00\rangle - |11\rangle) \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)) \\
 & = \frac{1}{\sqrt{2}} (|000\rangle + |111\rangle)
 \end{aligned}$$

状態の干渉

# 量子回路における量子的な演算

---

- **並列性**

- 量子的な重ね合わせ状態を入力すれば、最終状態は対応する出力の重ね合わせになる

- **分岐**

- $H$ ゲートなどにより、状態が"分岐" ( $|0\rangle, |1\rangle$  で見た場合)

- **干渉**

- 重ね合わせの係数は、場合によってはキャンセルし、消える

- **測定による収縮**

- 測定した基底のいずれか一つの状態になる

# 量子状態の測定

## 典型的な量子測定

例：1qubitのz基底 ( $|0\rangle$ 、 $|1\rangle$ ) での測定

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \xrightarrow{\text{(密度行列)}} \rho = |\psi\rangle\langle\psi| = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \begin{pmatrix} \alpha^* & \beta^* \end{pmatrix} \\ = \begin{pmatrix} |\alpha|^2 & \alpha\beta^* \\ \beta\alpha^* & |\beta|^2 \end{pmatrix}$$

  
(非選択的射影測定)

$$\rho \rightarrow \rho' = \begin{pmatrix} |\alpha|^2 & 0 \\ 0 & |\beta|^2 \end{pmatrix}$$

密度行列の非対角要素が消失  
(混合状態になっている)

  
(選択的射影測定)

$$\rho' \rightarrow \begin{cases} \rho_0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = |0\rangle\langle 0| & \text{(確率 } |\alpha|^2) \\ \rho_1 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = |1\rangle\langle 1| & \text{(確率 } |\beta|^2) \end{cases}$$

1つの純粋状態に

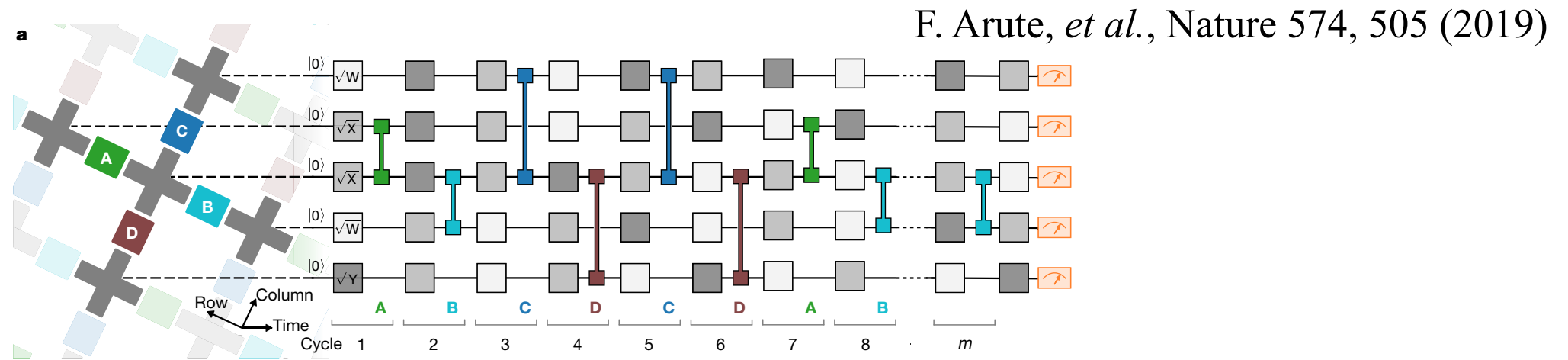
# 量子回路に基づく量子アルゴリズムのエッセンス

---

- 初期状態として ( $H$ ゲートなどにより) 多数の基底の重ね合わせ状態を準備
- 量子並列性の計算への活用
- 初期は測定で、多数の状態が同程度の確率で出現
- 目的に応じて種々のゲートを演算し量子状態を操作することで、答えが高確率で実現するようにする
- 測定により、高い確率で答えを測定できる

# 古典コンピュータによる量子回路のシミュレーション

量子回路は小さな**行列**、**テンソル**がつながった**テンソルネットワーク**



➡ 量子回路のシミュレーション=テンソルネットワークの**縮約**

古典コンピュータでの計算：

（実際の時間発展ではなく）最適な順番でテンソルの縮約計算を行うことで、計算コスト、メモリコストが低下

最先端の計算： Y. A. Liu, *et al.*, Gordon bell Prize in SC21 (2021),

Googleが量子超越を主張した**ランダム量子回路の古典サンプリング**

10,000年  
(最初の見積もり) ➡ **304秒！** (cf. 量子コンピュータ=200秒)

# 量子アニーリングの概略



# 量子アニーリング

T. Kadowaki and H. Nishimori, Phys. Rev. E 58, 5355 (1998).

系のパラメタをゆっくりと変化させ

徐々に、欲しい系にする

$$\mathcal{H} = \mathcal{H}_0 + \Gamma(t)\mathcal{H}_1$$

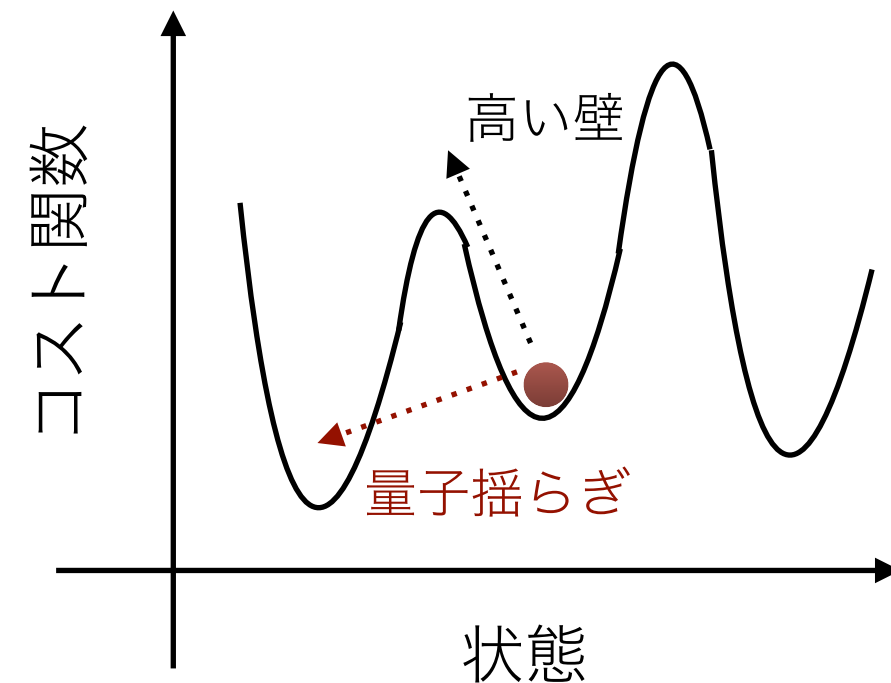
元のコスト関数

量子揺らぎ

$t = 0$  :  $\Gamma(t)$  = とても大

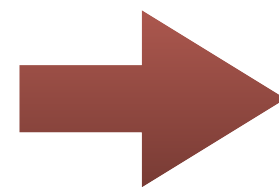
長時間 :  $\Gamma(t) \rightarrow 0$

素朴なアイデア



量子系は、初期状態からシュレディンガー方程式

$$i\hbar \frac{\partial}{\partial t} |\Psi\rangle = \mathcal{H} |\Psi\rangle$$



長時間で、コスト関数の最小値  
に対応する状態が実現？

に従って、時間発展

# 量子アニーリングと断熱時間発展

$$\mathcal{H} = \mathcal{H}_0 + \Gamma(t)\mathcal{H}_1 \quad \longrightarrow \quad \mathcal{H} = \frac{t}{\tau}\mathcal{H}_0 + \left(1 - \frac{t}{\tau}\right)\mathcal{H}_1$$

少し変形

$$t = 0 : \mathcal{H} = \mathcal{H}_1$$

$$t = \tau : \mathcal{H} = \mathcal{H}_0$$

時間間隔  $\tau$  で  
系を  $H_0$  に変化させる

## 断熱定理 (ざっくり)

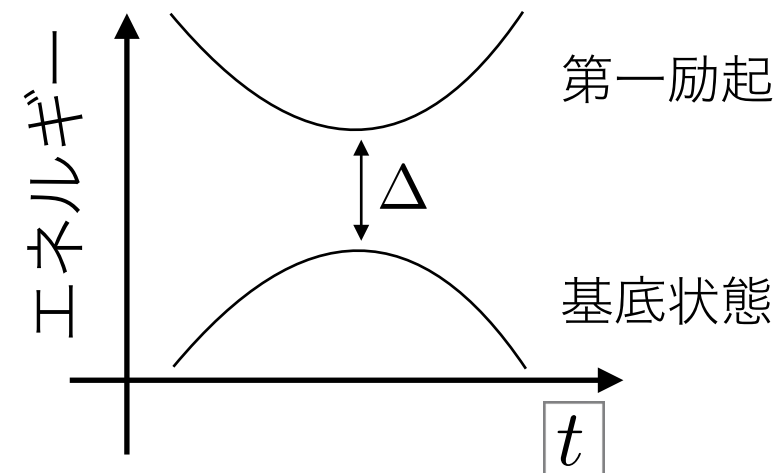
初期状態が  $H_1$  の最低エネルギー状態のとき  
 $\tau$  が十分に大きい (系の変化が十分にゆっくりの) 場合には、  
 $t = \tau$  で、 $H_0$  の最低エネルギー状態になる

\* どれくらいゆっくり?

最低エネルギー状態 (**基底状態**) と二番目低い状態  
(**第一励起状態**) との **最小のエネルギー差  $\Delta$**  で決まる

$$\tau \sim \frac{1}{\Delta^2}$$

\*  $\Delta$  が小さいと、ゆっくり  
変化させる必要がある



# 量子ビットでの量子アニーリング

コスト関数：  
(イジング相互作用で表現)

$$\mathcal{H}_0 = \sum_{i,j} J_{ij} \underline{Z_i Z_j}$$

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$Z_i Z_j |00\rangle = |00\rangle$$

$$Z_i Z_j |01\rangle = -|10\rangle$$

$$Z_i Z_j |10\rangle = -|01\rangle$$

$$Z_i Z_j |11\rangle = |11\rangle$$

量子揺らぎ：  
("横磁場")

$$\mathcal{H}_1 = - \sum_i \underline{X_i}$$

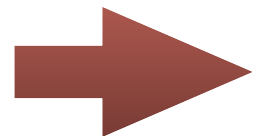
$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$X_i \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$X_i \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = -\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

重ね合わせ状態が基底状態

初期状態を $|0\rangle$ と $|1\rangle$ の  
重ね合わせ状態にして  
ゆっくり時間発展



コスト関数の  
最小値を与え  
る状態が実現

## \* 実用上の問題

- 解きたい問題をどうイジング相互作用で表現するか
  - エネルギー差 $\Delta$ をできるだけ大きくした方が有利