量子コンピュータの現状と 教育について

今井 浩

明治学院大学情報数理学部(2024年度新設)

東京大学医科学研究所ヒトゲノム解析センター・客員研究員

情報学科・専攻協議会 総会・研究会@早稲田大学, 2025-07-26

IBM

IBM Quantum System One at UTokyo Hub (Location: Shin-Kawasaki)

IBM Quantum
System One

IBM Quantum
Kawasaki,
Japan
川崎, 日本

Processor type
Falcon

Partner
The University
of Tokyo
IBM Quantum

IBM Quantum System One	
Processor	Falcon
Qubits	127
Connectivity	127
Control	127
Readout	127
Control lines	127
Readout lines	127
Control electronics	127
Readout electronics	127

Quantum Innovation Initiative
Hosted by UTokyo

1量子ビット: 2パラメタで表現

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

上向きスピン

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

下向きスピン

0

量子力学
2パラメタで表現

1

ノルム1の2次元複素ベクトル

1量子ビット: 2パラメタで表現

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

$$\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

量子力学
0と1の重ね合わせ

Entangled State

$$\frac{1}{2} (|00\rangle + |11\rangle)$$

Spooky Action!

Quantum Correlation cannot be represented by Classical Correlation

Superposition of 6qubit among $2^6=64$ states

 Tensor Product

N.B. This state is not entangled.

$$\begin{aligned}
 &|0\rangle \otimes |1\rangle \otimes \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \otimes |1\rangle \otimes |0\rangle \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \\
 &= \frac{1}{2} (|011100\rangle + |010100\rangle - |011101\rangle - |010101\rangle)
 \end{aligned}$$

IBM量子コンピュータを使ってみる

習うより慣れよ的

EPR状態 $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ の測定

EPR状態を作成・測定する回路

```
epr_state = QuantumCircuit(2,2)
epr_state.h(0)
epr_state.cx(0,1)
epr_state.measure([0,1], [0,1])
```

回路を計算、結果・回路図出力

```
backend = Aer.get_backend('qasm_simulator')
job = execute(epr_state, backend, shots=1000)
counts = job.result().get_counts()
print(counts)
epr_state.draw()
```

1000回の試行で、00が481回、11が519回測定され、01, 11は測定されない。
{'00': 481, '11': 519}

量子回路

■図-3 Qiskitでのプログラムのシミュレータでの計算例。2量子ビットのEPR状態というエンタングルしたものを測定すると、00, 11のみ測定され、EPRの指摘した不思議なことが起きている。

今井浩:量子コンピュータのあけぼの-今そこにある量子コンピュータに触れよう. 情報処理, Vol.62, No.4 (2021), pp. e1-e7.

2022のNobel物理学賞のベース のCHSH不等式の計算

```
my_chsh_circuits[5].draw()
```

try

```
my_chsh_circuits[6].draw()
```

try

```
my_chsh_circuits[7].draw()
```

try

The CHSH inequality [link](#)

Imagine Alice and Bob are given each one part of a bipartite entangled system. Each of them then performs two measurements on their part in two different bases. Let's call Alice's bases A and a and Bob's B and b . What is the expectation value of the quantity $\langle CHSH \rangle = \langle AB \rangle - \langle Ab \rangle + \langle aB \rangle + \langle ab \rangle$?

Now, Alice and Bob have one qubit each, so any measurement they perform on their system (qubit) can only yield one of two possible outcomes: $+1$ or -1 . Note that whereas we typically refer to the two qubit states as $|0\rangle$ and $|1\rangle$, these are *eigenstates*, and a projective measurement will yield their *eigenvalues*, $+1$ and -1 , respectively.

Therefore, if any measurement of A , a , B , and b can only yield ± 1 , the quantities $(B - b)$ and $(B + b)$ can only be 0 or ± 2 . And thus, the quantity $A(B - b) + a(B + b)$ can only be either $+2$ or -2 , which means that there should be a bound for the expectation value of the quantity we have called

$$|\langle CHSH \rangle| = |\langle AB \rangle - \langle Ab \rangle + \langle aB \rangle + \langle ab \rangle| \leq 2.$$

Shorの量子多項式時間 素因数分解アルゴリズム

Shorの素因数分解前半

$$|i\rangle|0\rangle \mapsto |i\rangle|a^i \pmod{n}\rangle \quad (n = 15, a = 2)$$

$ 0000\rangle$	$ 0\rangle$	$ 0\rangle 0\rangle$	$ 0\rangle 1\rangle$
$+ 0001\rangle$	$+ 1\rangle$	$+ 1\rangle 0\rangle$	$+ 1\rangle 2\rangle$
$+ 0010\rangle$	$+ 2\rangle$	$+ 2\rangle 0\rangle$	$+ 2\rangle 4\rangle$
$+ 0011\rangle$	$+ 3\rangle$	$+ 3\rangle 0\rangle$	$+ 3\rangle 8\rangle$
$+ 0100\rangle$	$+ 4\rangle$	$+ 4\rangle 0\rangle$	$+ 4\rangle 1\rangle$
$+ 0101\rangle$	$+ 5\rangle$	$+ 5\rangle 0\rangle$	$+ 5\rangle 2\rangle$
$+ 0110\rangle$	$+ 6\rangle$	$+ 6\rangle 0\rangle$	$+ 6\rangle 4\rangle$
$+ 0111\rangle$	$+ 7\rangle$	$+ 7\rangle 0\rangle$	$+ 7\rangle 8\rangle$
$+ 1000\rangle$	$+ 8\rangle$	$+ 8\rangle 0\rangle$	$+ 8\rangle 1\rangle$
$+ 1001\rangle$	$+ 9\rangle$	$+ 9\rangle 0\rangle$	$+ 9\rangle 2\rangle$
$+ 1010\rangle$	$+ 10\rangle$	$+ 10\rangle 0\rangle$	$+ 10\rangle 4\rangle$
$+ 1011\rangle$	$+ 11\rangle$	$+ 11\rangle 0\rangle$	$+ 11\rangle 8\rangle$
$+ 1100\rangle$	$+ 12\rangle$	$+ 12\rangle 0\rangle$	$+ 12\rangle 1\rangle$
$+ 1101\rangle$	$+ 13\rangle$	$+ 13\rangle 0\rangle$	$+ 13\rangle 2\rangle$
$+ 1110\rangle$	$+ 14\rangle$	$+ 14\rangle 0\rangle$	$+ 14\rangle 4\rangle$
$+ 1111\rangle$	$+ 15\rangle$	$+ 15\rangle 0\rangle$	$+ 15\rangle 8\rangle$

周期4
繰返し

$|0\rangle + |1\rangle$

$|0\rangle + |1\rangle$

$|0\rangle + |1\rangle$

$|0\rangle + |1\rangle$

$$|i\rangle|0\rangle \mapsto |i\rangle|a^i \pmod n\rangle \quad (n = 15, a = 2)$$

$\otimes$

$\otimes$

$\otimes$

$a = 2$

● 1のとき下の操作を適用

4 + 4 = 8
量子ビット

- $|0\rangle|1\rangle$
- $+|1\rangle|2\rangle$
- $+|2\rangle|4\rangle$
- $+|3\rangle|8\rangle$
- $+|4\rangle|1\rangle$
- $+|5\rangle|2\rangle$
- $+|6\rangle|4\rangle$
- $+|7\rangle|8\rangle$
- $+|8\rangle|1\rangle$
- $+|9\rangle|2\rangle$
- $+|10\rangle|4\rangle$
- $+|11\rangle|8\rangle$
- $+|12\rangle|1\rangle$
- $+|13\rangle|2\rangle$
- $+|14\rangle|4\rangle$
- $+|15\rangle|8\rangle$

後半部へ

→ 時間(入力から出力へ)

Shorの素因数分解前半

$$|i\rangle|0\rangle \mapsto |i\rangle|a^i \pmod{n}\rangle \quad (n = 15, a = 2)$$

$ 0000\rangle$	$ 0\rangle$	$ 0\rangle 0\rangle$	$ 0\rangle 1\rangle$
$+ 0001\rangle$	$+ 1\rangle$	$+ 1\rangle 0\rangle$	$+ 1\rangle 2\rangle$
$+ 0010\rangle$	$+ 2\rangle$	$+ 2\rangle 0\rangle$	$+ 2\rangle 4\rangle$
$+ 0011\rangle$	$+ 3\rangle$	$+ 3\rangle 0\rangle$	$+ 3\rangle 8\rangle$
$+ 0100\rangle$	$+ 4\rangle$	$+ 4\rangle 0\rangle$	$+ 4\rangle 1\rangle$
$+ 0101\rangle$	$+ 5\rangle$	$+ 5\rangle 0\rangle$	$+ 5\rangle 2\rangle$
$+ 0110\rangle$	$+ 6\rangle$	$+ 6\rangle 0\rangle$	$+ 6\rangle 4\rangle$
$+ 0111\rangle$	$+ 7\rangle$	$+ 7\rangle 0\rangle$	$+ 7\rangle 8\rangle$
$+ 1000\rangle$	$+ 8\rangle$	$+ 8\rangle 0\rangle$	$+ 8\rangle 1\rangle$
$+ 1001\rangle$	$+ 9\rangle$	$+ 9\rangle 0\rangle$	$+ 9\rangle 2\rangle$
$+ 1010\rangle$	$+ 10\rangle$	$+ 10\rangle 0\rangle$	$+ 10\rangle 4\rangle$
$+ 1011\rangle$	$+ 11\rangle$	$+ 11\rangle 0\rangle$	$+ 11\rangle 8\rangle$
$+ 1100\rangle$	$+ 12\rangle$	$+ 12\rangle 0\rangle$	$+ 12\rangle 1\rangle$
$+ 1101\rangle$	$+ 13\rangle$	$+ 13\rangle 0\rangle$	$+ 13\rangle 2\rangle$
$+ 1110\rangle$	$+ 14\rangle$	$+ 14\rangle 0\rangle$	$+ 14\rangle 4\rangle$
$+ 1111\rangle$	$+ 15\rangle$	$+ 15\rangle 0\rangle$	$+ 15\rangle 8\rangle$

周期4
繰返し

Peter Shorの量子計算・量子情報への貢献

量子計算での重要問題での指数加速可能性を提示
量子コンピュータ基礎

- RSA公開鍵暗号等を破る量子計算高速素因数分解(1994)
- 量子誤り訂正符号CSS, 耐故障量子計算、量子通信路定理 (Shannon prize 2025)

量子フーリエ変換

- **量子計算の社会的有用性：**

量子計算機が社会的にインパクトを与える問題を解けることを示した。

- **量子計算の実現性：**

量子誤り訂正・耐故障性を提案して量子計算機が実現可能であることを示した

FOCS国際会議, SIAM J. COMP/Review

RSA-2048 = (10進671桁, 2進数2048bit)

```

2519590847565789349402718324004839857142928212620403202777713783604366202070
7595556264018525880784406918290641249515082189298559149176184502808489120072
8449926873928072877767359714183472702618963750149718246911650776133798590957
0009733045974880842840179742910064245869181719511874612151517265463228221686
9987549182422433637259085141865462043576798423387184774447920739934236584823
8242811981638150106748104516603773060562016196762561338441436038339044149526
3443219011465754445417842402092461651572335077870774981712577246796292638635
6373289912154831438167899885040445364023527381951378636564391212010397122822
120720357
    
```

現在使われている長さの鍵—今のスパコンでは無理!
←大規模・精緻な量子コンピュータなら破れる

社会インパクト：

- 耐量子計算機暗号PQCの標準策定・新たな公開鍵暗号に移行 (米国では2035に移行)
- 量子コンピュータに関する研究分野を拡大することに貢献

1st ERATO/AQIS Confernece on Quantum Information Science @UTokyo, 2001

2nd ERATO/AQIS Confernece on Quantum Information Science @UTokyo, 2002

Organized by JST ERATO
Quantum Computation & Information

Peter Shor

量子素因数分解

1994

おそらく重要
指数爆発的
スピードアップ

Alexei Kitaev

量子位相推定

1995

教科書のアルゴリズム
←Near-term では無理
→Fault-Tolerant QC実現へ

量子力学シミュレーション 1996~

量子化学VQE 2014~

量子近似最適法 2014~

量子機械学習 2015~

量子線形方程式解法 2008~

量子特異値変換 2018~

IBM Quantum Roadmap

<https://www.ibm.com/quantum/technology>

2020年頃より毎年更新・公開
 これまでの達成事項チェック

Introduction to Quantum Computing in the Utility-Era

The goal of this course is to learn how to implement utility-scale applications on a quantum computer. To achieve the goal, the course covers from the basics of quantum information to recent advances of quantum algorithms for noisy quantum devices as well as circuit optimization and error mitigation techniques to maximize results. The course also introduces how to implement quantum algorithms using open-source framework of quantum computing and real quantum devices with more than 100 qubits. The course is intended to help students understand The potential and limitations of currently available quantum devices.

Contents:

- 1: Invitation to the Utility era/Basics of Quantum Information
- 2: Quantum Algorithms: Quantum Teleportation
- 3: Quantum Algorithms: Grover's algorithm
- 4: Quantum Algorithms: Phase Estimation
- 5: Quantum Algorithms: Variational Quantum Algorithms (VQA)
- 6: Quantum Simulation, Time Evolution
- 7: Classical Simulation
- 8: Sample-based Quantum Diagonalization
- 9: Quantum Circuit Optimization
- 10: Quantum Noise Model and Quantum Error Mitigation
- 11: Creating Large Scale GHZ State based on Hardware Topology and Qubits Fidelity
- 12: Reproducing Nature paper – 2D Ising model simulation
13. Final Project

University of Tokyo Quantum Computational Theory Course @ Imai Lab (2019-2023)

- Delivering course in collaboration since 2019
- Department of Computer Science, Registered under CS, PHY, MI)
- 14 weeks during Spring Semester
- Material co-developed by IBM Research - Tokyo and UTokyo
- Focuses on teaching students how to program and execute quantum circuits using Qiskit
- Reached 500+ students so far (100+ students complete the course each year)

From gates, circuits, measurements to quantum algorithms and applications in machine learning, optimization, and chemistry.

Weekly quizzes to test understanding of lectures each week

Students participated in Challenge for extra credit IBM Quantum

Originally started around 2009 by Francois Le Gall in G30 projects! w/o use of quantum computers

University of Tokyo Quantum Computational Course @ Sato Lab (2024-)

- For the first time, educators and students can exploit 100+ qubit systems in classrooms.
- The Spring 2024 course at UTokyo is the First Utility-scale quantum computation course offered in the world.
- Students learn utility-scale workflow and implement the nature paper using Qiskit by the end of the course.
- Designed to provide practical skills to help students become part of the workforce that can bring useful quantum computing.

Implementation of the utility paper

Trotter Circuit

Create a circuit to simulate the time evolution of the kicked Ising model. First, let's make one circuit that is its building block. The Hamiltonian is

$$H = -J \sum_{(i,j)} Z_i Z_j + h \sum_i X_i.$$

The unitary gate for trotter are

$$e^{-iH_Z \delta t} = \prod_{(i,j)} e^{i\delta t Z_i Z_j} = \prod_{(i,j)} R_{ZZ}(-2J\delta t)$$

$$e^{-iH_X \delta t} = \prod_i e^{-i\delta t X_i} = \prod_i R_{XX}(2h\delta t),$$

```
[1]: import numpy as np
      from qiskit import QuantumCircuit
      from qiskit.circuit import Parameter
```

```
[2]: theta_h = Parameter("$\\theta_h$")
      theta_j = Parameter("$\\theta_j$")

      qc = QuantumCircuit(2)
      qc.rx(theta_h, [0, 1])
      qc.rzz(theta_j, 0, 1)
```

標準カリキュラム

量子技術分野全体を俯瞰する共通カリキュラムの雛形を公開しています。

既存の学部学科教育において量子技術分野を強化する科目構成や学科の再編成や新設の参考となるように必須・選択科目を整理しています。

学部前期 (1、2年生) >

学部後期 (3、4年生) >

博士前期課程 (1、2年生) >

量子技術高等教育拠点

© Quantum Academy of Science and Technology reserved.

<https://qacademy.jp/curriculum/>

量子技術高等教育拠点は、文部科学省 Q-LEAP 人材育成プログラムの共通的なコアプログラムとして、「量子技術高等教育拠点標準プログラムの開発」に基づき運営されています。

カリキュラム標準モデル

学部前期（1、2年生）

※スパイラル方式

スパイラル方式とは、学生がカリキュラムを進む中で、同じ学習テーマについて繰り返し学ぶ機会をもつ方法で、学年が上がるごとに同じテーマでも内容の難易度が増すように設計する方法である。新しく学ぶ内容に対して、すでに学んだ内容を結びつけることができるようになっていることを特徴とする。スパイラル方式を採用することで、同じテーマの学びを繰り返す機会を得ることで知識が定着しやすいこと、簡単な概念から複雑な概念への発展において論理的な理解を助ける、初期に習った基礎的な事項について、より高度な内容へ応用する機会を持ちやすい、といった利点があると考えられている。

量子技術必修科目

量子技術選択科目

従来科目

カリキュラム標準モデル

学部後期（3、4年生）

量子情報基礎科学

量子情報物理学

量子デバイス

量子計算機工学

量子ネットワーク・通信

共通科目

量子計算基礎

量子通信基礎

量子暗号基礎

テクニカルライティング

機械語

機械学習

圏論

確率論

線形代数発展

微積分発展

推定理論

数理統計学

最適化

アセンブリ言語

エンタングルメント理論基礎

量子シャノン理論基礎

量子アルゴリズム

量子暗号数理

符号理論

幾何学

アルゴリズム発展

計算量理論
(チューリングマシン入る)

量子情報における群論

量子情報で使う情報数学

量子計算モデリング

色々な量子計算モデル

Quditの量子力学

CV系の量子力学

場の理論基礎

相対性理論

量子力学

統計力学

量子統計物理・固体物性基礎

量子高精度測定と量子センサー

量子情報処理デバイス概論

量子光学と光子デバイス基礎

超伝導量子ビット技術と
マイクロ波制御技術基礎

冷却原子・イオントラップ基礎

量子オートマトン
と量子チューリング機械

量子計算機のための
古典コンパイラ基礎

量子計算機のための
古典アーキテクチャ基礎

量子計算機のための
古典OS基礎

誤り耐性
量子コンピュータ基礎

スパイラル方式

量子通信プロトコル

量子通信システム

量子鍵配送システム

量子技術必修科目

量子技術選択科目

従来科目

カリキュラム標準モデル

博士前期課程（1、2年生）

量子情報基礎科学

量子計算理論発展

量子アルゴリズム発展

量子プログラミング言語

量子符号理論

量子シャノン理論発展

量子暗号発展

量子誤り訂正

量子機械学習

量子情報幾何

量子情報物理学

エンタングルメント理論発展

量子入出力の量子プロトコル

非定型量子アルゴリズム

量子熱力学

量子シミュレーション

量子情報のための数値計算手法 (SDP, MLなど)

量子デバイス

推定理論と量子デバイス評価

量子制御理論

量子制御理論

量子計算機工学

量子コンパイラ基礎

量子アーキテクチャ基礎

量子計算機のための
古典コンパイラ実習

量子計算機のための
古典計算機アーキテクチャ実習

量子計算機のための
古典OS演習

誤り耐性量子コンピュータ
アーキテクチャ

誤り耐性量子コンピュータ・
量子機械言語とコンパイラ設計

量子ネットワーク・通信

スパイラル方式

- 微分方程式・複素解析
- 信号及び通信
- グラフ理論及び群論
- 情報理論
- 暗号理論

量子通信理論

量子暗号システム

量子ネットワーク科学

共通科目

アントレプレナーシップ

量子技術と法整備

先端科学のパブリックリレーションズ

量子技術必修科目

量子技術選択科目

従来科目

明治学院大学 情報数理学部 カリキュラムツリー

・学部新設
→カリキュラムをゼロから構築
新規教員も多数
⇒これを利点に!

・それまで文系総合大学であった明学で理系学部を新設して文理を含む総合大学へと展開する点については以下記事参照

明治学院大学情報数理学部 文系大学での新情報系学部設置と文理融合ーAI・量子コンピュータの先端教育ー, 今井浩, 大学時報2025年1月号, No.420

<https://daigakujihou.shidairu.or.jp/list/contents/?jihou=420>

Bloch球—1量子ビットのモデル

- 密度行列により混合状態を表現可
- ベクトルは純粋状態まで

EPR State (entanglement)

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

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \text{Hadamard 行列}$$

$$H|0\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

$$H|1\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

$$\frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \neq (\alpha_0|0\rangle + \alpha_1|1\rangle)(\beta_0|0\rangle + \beta_1|1\rangle)$$

$$\frac{1}{\sqrt{2}} (|00\rangle + |10\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$\begin{aligned} \therefore \\ \alpha_0\beta_0 &= 1 \\ \alpha_0\beta_1 &= 0 \\ \alpha_1\beta_0 &= 0 \\ \alpha_1\beta_1 &= 1 \\ \text{no solution} \end{aligned}$$

ゲート：行列に対応

出力ベクトル = 行列 × 入力ベクトル

1qubitゲート：2次正方行列

2qubitゲート：4次正方行列

**Entangled state
(EPR state)**

情報系での量子計算の教育

- 「量子力学」講義をベースにする必要はない
 - 知っているると研究に役立つことはあり
- 線形代数をベースに量子計算・量子情報コース
 - 情報系の基礎ももちろん有用
 - アルゴリズムと計算量理論
 - 情報理論
 - 符号理論
 - プログラミング
 - アーキテクチャ
 - などなど
- コンピュータは計算して結果を出すことが大切
- 強力な量子コンピュータはまだ時間がかかる中、確かな基盤の上に華が開き、広く展開できる

量子コンピュータ

身近なものに