特集
Special Feature

［面白いぞ量子技術］

1 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

今井　浩 東京大学

量子コンピュータ

コンピュータは大まかにはハードウェアとソフトウェアからなっている．量子コンピュータは，

- ハードウェアが量子力学原理で動作し，
- ソフトウェアが量子力学制御の操作を行う

ものである．今のコンピュータは量子力学以前の力学である古典力学（ニュートン力学に代表される）で動作している．量子力学は古典力学より優れた点を持つが，量子力学に従って制御することなど，現在でもまだ完全に行うのは難しい．でも量子コンピュータならもっといいことができるのでは，という構想が 1980 年頃に複数示された．

1 つは数学者の Manin によるもので，1980 年に出版された『計算可能性と計算不可能性』という本の第 1 章最後の 3 段落[☆1]でその構想を語っている．これに触発された Kitaev は，1982 年には量子計算の研究を開始し 1990 年代半ばに量子位相推定アルゴリズムやトポロジカル量子計算等で量子計算基礎で大きな貢献をしている[☆2]．

今よく知られている構想の 1 つは，1981 年の The Physics of Compuation[☆3] という MIT Laboratory for Computer Science（LCS）と IBM が組織[☆4]した会議で，Feynman が行った Simulation of Physics という基調講演[2] である．その中で，Feynman は量子力学をコンピュータでシミュレーションすることは，従来コンピュータでは計算困難であるが，量子コンピュータであれば高速に行えるのではという考えを示している．

これらの共通することは，

> 量子コンピュータは，従来コンピュータのコンピュータでは計算困難な問題を，効率良く解くことができるだろう

という想い・研究プログラムである．根拠なく主張しているわけではなく，そのための基礎的課題の検討を行った上で研究コミュニティに刺激を与えている．その他の構想も含め，この時期が量子コンピュータの力が従来コンピュータのそれを凌駕する可能性が認識され，構想から量子コンピュータの研究へと展開するあけぼのとなっている．

本稿では，この展開以降の段階的変革をとげるあけぼのについて見ていきたい．

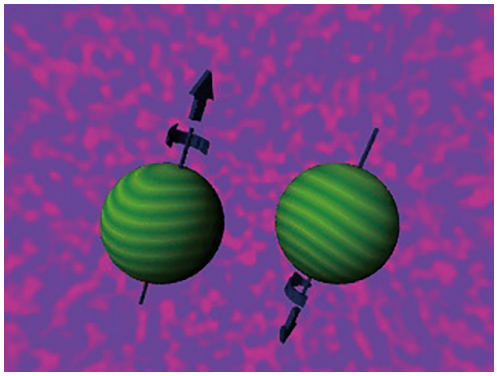
☆1 Manin[1] の Appendix に Kitaev による訳がある．
☆2 Kitaev の MacArthur Fellow 受賞ニュース，IEEE Spectrum, 2008.
☆3 MIT Endicott House の会議ページ
☆4 MIT LCS の前身組織の所長だった Fredkin と研究員の Toffoli（それぞれの名前を冠した可逆ゲートあり）と IBM 研究所で非可逆回路でのエントロピー消失と熱発生の原理などの研究を行っていた Landauer による．

1 量子ビット計算で初めてできること

量子コンピュータの力を調べる方向性が示されて，次に実際にその力を示す研究が出てきた．ここで基礎をおさえておこう．従来コンピュータは 0 か 1 かを表す 1 ビットを基本とする．量子コンピュータでは，それが 1 量子ビットとなる．1 量子ビットのイメージを図 -1 に示す．この図は一見地球が変な空間に浮かんでいるようにも見え，自転軸も傾いている．地球の場合，右手系で北極の方向のスピンになっており，それで 0 を表し，逆に南極方向のスピンで 1 を表す．スピンなので，実は球面分の自由度を持っており，まずはそのどの方向でも持てるとする（実際にはここを離散化）．

このような 1 量子ビットだけで簡単な量子計算する量子暗号方式に触れよう．Bennett, Brassard は 1984 年の国際会議での招待論文の中で，現在 BB84 と呼ばれる量子鍵配送方式を提案した．Shannon の完全秘匿性に関する定理から，平文と同じ長さのランダムな秘密鍵を 2 者間で共有できると，情報理論的に安全という究極の基準での安全性を実現できる．従来計算・通信のレベルではその高いレベルを有する暗号方式はなく，BB84 は量子力学での不確定性原理を用いて初めて達成したものである．

量子計算としては，1 量子ビットを回転（ユニタリ変換）し，標準的な測定を行うだけである．実現にあたっては，1 量子ビットを伝送する 1 光子（1 粒子の光；光は量子力学では波でもあり粒子でもある）が理想であるが，その生成がまだ難しいので，現在の量子暗号システムでは弱いレーザ光を用い，ソフトウェアとして光強度をデコイ（おとり）とし，統計処理することで，セキュリティ要求に応じた安全性を保証するものが開発されている．日本でもこの量子暗号が事業化されていることは，種々 CM を通じてご存知と思う[☆5]．



■図 -1　2 つのスピン：左側は右手系で上向きで 0 を，右側は下向きで 1 を表現．|01〉と表される．

ここで量子力学の概念が出てきて壁を感じる方もいるかもしれないが，その壁は量子コンピュータ自体を使うことで乗り越えられるのだというのを見ていこう．

量子計算を線形代数・プログラムで理解する

量子力学の理解は，きちんと深く量子計算を極めるには必要であろう[☆6]．一方で，大学学部の量子力学講義（2，3 学期にわたる）ものを知っていないと，量子計算が理解できないわけではない．基本，大学入門数学での線形代数が理解できていれば取り組むことができる．

量子暗号 BB84 を自分で送信者・受信者を演じて，今利用可能な量子コンピュータのクラウドサービスを使って実現してみよう．量子ビットで 0, 1 を表現するのに 2 次元ベクトルを使って

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

と表現し[☆7]，必要な操作は 2 × 2 行列で

☆5 このように，量子コンピュータ構想が示された 1980 年代初めのあけぼのから，すぐに情報セキュリティの核となる量子暗号方式が提案され，その後息の長い研究開発を通して社会実装に至っている，というすごさも理解していただけるとありがたい．

☆6 さらには無限次元の場合で関数解析とかも分かっているとためになるし，トポロジカル量子計算ではトポロジーの基礎も分かっていた方がよい．

☆7 量子力学の Dirac の ket 記法の |0〉, |1〉 を初めて見た人は，単に縦ベクトルで，0, 1 を表現するものと理解を．

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

などを使って，Python 流に操作の中核部分を書いて

```
qc = QuantumCircuit(q, c)
qc.h(q)
qc.measure(q, c)
qc.draw()
```

とすると，初期はデフォルト 0 が符号化されてたところを，

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

となり，量子力学の最も基本的な測定法では，測定結果は 0, 1 を等確率で得ることになる[☆8]．すなわち，初期状態に関する情報は何も得られなくなっていて，量子不確定性がこの小さな事例で発現している．一方，`qc.h(q)`を`qc.X(q)` で取り替えると，

$$X|0\rangle = |1\rangle \qquad (\text{同様に } X|1\rangle = |0\rangle)$$

出力は必ず 1 となり，初期値 0 の否定を計算したことになる（X は NOT 操作）．

1 量子ビット演算として H に加えシフト行列 S と T ゲート T を用い，2 量子ビット演算で制御 NOT という 4 × 4 の行列を量子計算を実行する量子回路の基本ゲートとすると，これらを繰り返し適用していくことによって，n 量子ビットに掛ける任意の $2^n \times 2^n$ のユニタリ行列を指定精度内で近似することができる[☆9]．図 -1 に加え，6 量子ビットのスピンを図 -2 に示す．

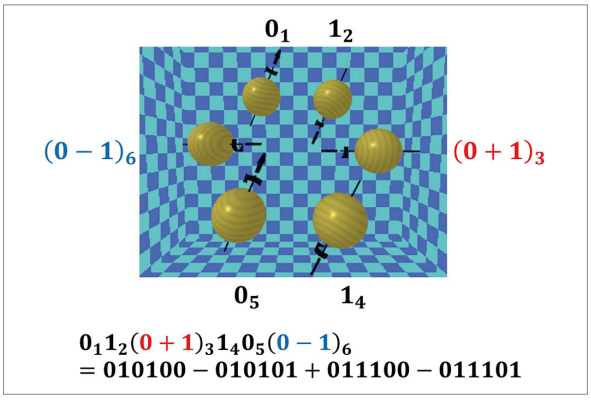
すると，量子計算は n 個の 0 を表す n 量子ビットを初期状態に，所望の結果を得られる量子回路で計算し，最後に測定することで出力を得ることともいえる．ハードウェアで，これら基本ゲートを実現する操作を行えると，量子力学の世界では 2^n 次元の演算が基本ゲートの適用回数の時間で計算でき，測定をすれば所望の n ビットの出力を得ることができるのが，量子コンピュータが従来のコンピュータを凌駕し得るだろうと信じたくなる理由である．

量子計算だからできること

1 量子ビットでの量子計算・量子情報処理では，1980 年代に醸成された量子暗号の研究が始まり，現在では事業化も通して社会に浸透するレベルになっている．しかし，実際にはその過程で停滞もあった．日本の場合は，2000 年頃からの NICT や JST のプロジェクトを通して現状まで突破してきたところであるが，BB84 の原論文が当初国際会議で評価されず，招待論文の機会に発表されていることなど，新奇分野・原理であるがゆえの評価されにくい時期もあった．

そういう停滞時期を打破したのは，量子計算だからこそ初めて可能になることを社会的インパクトが大きい問題で示した 1994 年の Shor[3] の量子多項式時間の素因数分解アルゴリズムである．このブレークスルーをもたらしたアルゴリズムは次の 2 点で卓越している．

(a) 1978 年提案の RSA 公開鍵暗号系は，インター



■図 -2　6 つのスピン水平向きのスピンは各々 0, 1 を半々の違う重み（振幅）で合成した状態．これは単純な状態で，後述の量子エンタングルメントがあると，このような表現はできない意．

☆8　こういうのが量子力学の不可思議なところ．

☆9　量子力学では 1 量子ビット 2 つを合成して，1 つの 2 量子ビットにすることは，テンソル積（Kronecker 積）をとることに対応する．

ネットでの基盤技術となっているところを，その安全性を素因数分解の計算困難さにおいていた．Shor のアルゴリズムは，ひとたび量子コンピュータが大規模問題を解けることになると，RSA 暗号の安全性が崩壊してしまうことを意味し，社会インパンパクトが大きい．

(b) 量子計算のアルゴリズム論の観点で，非常に巧妙に構築されており，そこから一連の量子計算で効率良く解く枠組みを提供したこと．

(a) については，過大に思われる方もいるかもしれないが，共通鍵暗号の世界標準 AES などを制定している NIST が，2016 年から大規模量子コンピュータが存在しても安全な公開鍵暗号を選定するプロジェクトを進めている．インターネットのセキュリティは社会インフラで，それを更新するには十分な余裕期間が必要という考えもあるかもしれない☆10．

(b) については，Shor のアルゴリズムのポイントは 2^n 次元の離散フーリエ変換を使うという点だけではないことである．確かに，量子コンピュータで $O(n^2)$ で計算できるという先行研究をうまく使った部分は重要で，それは Shor のアルゴリズムの後半部分であって，前半部分では位数発見問題という周期関数の周期を求める問題への変換が行われているところも重要な貢献であることを紹介しておく．量子計算を量子回路でのゲートセットを限定して部分クラスを考える理論から，前半部の巧妙さが鍵となっていることも示唆されている．また，Shor の位数発見問題への変換は，Miller の 1976 年の素因数分解の従来の計算量に関する論文での 1 つの成果であることも指摘しておきたい．すなわち，量子アルゴリズムというのは，量子計算で新しいものを考えることだけではなく，従来の計算方式でのアルゴリズムをベースにして量子の風味を加えて劇的な高速化を実現することができる典型例となっている．

☆10 一方で，現時点ですぐに危惧を持つ必要はないことは，IPA の情報発信にもある．

Shor のアルゴリズムは（a）のような社会的インパクトも与えている一方，2 つの大きな未解決課題を提示している．

- 従来コンピュータでは，スパコンをもってしても素因数分解は計算困難である，ということが妥当だと思われてきたが，将来もしかして天才が従来コンピュータで高速に素因数分解を実行できることを示す可能性はゼロではない☆11．
- 量子コンピュータで Shor のアルゴリズムを RSA 暗号破りに適用する場合，数百万量子ビットの誤り訂正可能な量子コンピュータ実現が必要で，それはまだ先であると思われており，かなりの課題を解決していかないといけないと予想されている．

Shor のアルゴリズムは，量子アルゴリズムで社会に影響を与えた最初のものであり，その拡張の Kitaev の位相推定アルゴリズムも含め，今後とも量子アルゴリズム研究での核をなすことは確かである．

量子計算だからできること 2

量子力学は，それ以前の力学（古典力学）での常識と合わない新奇性がある．量子力学の理論構築時に，本当にその理論が正しいのか，自然の摂理を表しているのかについて，議論がなされていた．たとえば，Physical Review の 1935 年の論文では，Einstein, Podolsky, Rosen によるその新奇性に関しての量子力学批判の論文（EPR 論文と呼ばれる）が 5 月に掲載されたのち，10 月には Bohr による反論を記述した論文が計算されるなど☆12．

実はこれは最初に述べた，量子コンピュータ vs. 従来コンピュータの図式でも同様であり，上記では

☆11 量子アルゴリズム周辺で，従来方式では効率良く解けないと仮定していたのに，実際にはすぐにその仮定が間違っていたことが示された事例が結構ある．素因数分解問題の研究はもう半世紀近く行われてまだ見つけられてないので，そうたやすく解けないと思われているものの．

☆12 ちなみに両論文は同じタイトルである：Can Quantum-Mechanical Description of Physical Reality be Considered Complete?

Shor のアルゴリズムがこの図式で量子側でのブレークスルーをもたらしたものであることを述べた．前段落での量子力学理論に関する論争点も，実はこの計算での図式に発展させることができ，2020 年 1 月に大きな成果が出ているので紹介しよう．

EPR 論文の指摘は，現在量子エンタングルメント（あるいは量子もつれ）☆13 と呼ばれる概念が引き起こす不思議について論じている．それが不思議ではなく，実際に量子力学が成立しているのだと示すために，Bell は不等式に着目した．この不等式は古典確率では必ず成り立つ相関確率に関するもので，量子力学実験から量子エンタングルメントを通じて得られる量子測定確率ではその不等式が破れてしまうことを理論として示したものである．Bell の示した不等式は，ある意味皆がよく知っているもので，三角形で成り立つ三角不等式と対応している．誤解をおそれずイメージでいえば，量子エンタングルメントしている量子状態からの量子測定確率で対応する三角形を書くと，三角不等式が成立してないという不思議なことになる．ここでは，IBM Quantum Experience を用いて，2 量子ビットで量子エンタングルメントした状態（EPR 状態）を計算・測定するプログラム例を図 -3 に示している．

量子力学実験の観点では，三角形では実験が困難ということで，三角不等式を拡張した CHSH 不等式というものが，通常の教科書で単に Bell 不等式として紹介されている．そして，1982 年には Aspect らのグループが光学実験で量子効果で CHSH 不等式の破れる結果を得ている．

CHSH 不等式は，情報科学のグラフと最適化の理論の言葉を使うと，完全 2 部グラフ $K_{2,2}$ に対する相関多面体の満たす不等式である．より一般の 2 部グラフをベースとして拡張した枠組みでの一般化 Bell 不等式を構成することができる．この拡張は，計算量理論の分野でのランドマークとなる結果である 1986 年の Goldwasser らによる多証明者対話証明の理論とまさしく対応することが分かっている．2 証明者対話証明のゲームの値が古典確率の上限に対応し，それを 2 証明者の間に量子エンタングルメントがある場合の対話証明ゲームの値がその上限を超えることが Bell 不等式の破れに対応する図 -4.

この拡張のもと，Einstein らの EPR 論文が指摘した量子エンタングルメントの不思議は，量子力学の表現空間は線形代数が表す有限次元の空間を超え，無限次元空間も考えて関数解析の対象となることも関係している．2 証明間の量子エンタングルメントの度合いが限られる場合は，計算量理論で NEXP という量子エンタングルメントがない場合のクラスと同等のことが示されていたが，Ito, Vidick[4] が量子エンタングルメントが少なくとも量子計算のパ

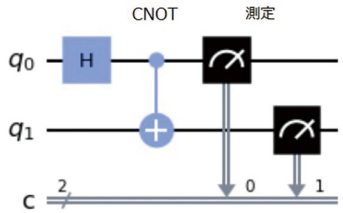
```
# EPR状態を作成・測定する回路
epr_state = QuantumCircuit(2,2)
epr_state.h(0)
epr_state.cx(0,1)
epr_state.measure([0,1], [0,1])

# 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



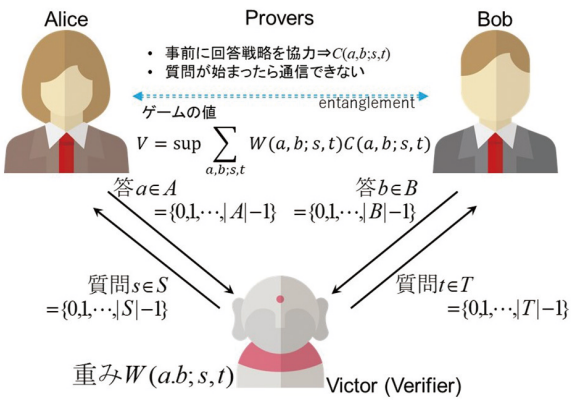
■図 -3　Qiskit でのプログラムのシミュレータでの計算例．2 量子ビットの EPR 状態というエンタングルしたものを測定すると，00, 11 のみ測定され，EPR の指摘した不思議なことが起こっている．

☆13 複数量子ビットがエンタングルしていると，各量子ビットを図 -1 に示したようなスピンで表現できなくなっており，量子力学で独特な複雑な構造になっている．

ワーを真に増進する方向で有効であるという大きな結果を 2012 年に示した．それ以来，2 証明者間の量子エンタングルメントの量の上界を与えない一般の場合の解析が先端研究での目標になっていたが，次第に計算不可能なクラスまで難しくなるのではと研究者が予想しはじめ，ついに 2020 年に対話証明のゲームの値の計算が計算不可能になってしまうことが示された[5]．より具体的には，そのゲームの値が計算できると，Turing マシンの停止問題という計算不可能な問題が解けることになるというものである．1936 年に Turing による計算の定義が Turing マシンの有限時間停止性によって与えられて以来，それが計算の定義として 100 年近く認められてきており，量子計算の観点からその定義を再考することもできるかもしれない．

量子コンピュータシステムのあけぼの

本会に量子ソフトウェア研究会が設置された 1 つの原動力は，もっと将来のことと研究者の中で思われていたかもしれない量子コンピュータシステムの実現スピードが上がり，数十量子ビットのデバイスも出てきて，それを制御するソフトウェアも構築され，いよいよ皆が量子コンピュータを使える時代が来た点にある．2，3 年後に 1,000 量子ビットを超



■図 -4　一般化 Bell 不等式に対応する 2 証明者対話証明ゲーム：おおざっぱには，情報交換できない 2 名の家庭教師に個別にうまく質問する学生は，1 名の家庭教師に学ぶ場合より学習能力が大きくなる図式．

えるロードマップも示されたりしている．その点，本章のタイトルのように，ユーザが実際に使える量子コンピュータシステムと呼べるものがまさしく到来したというのである．一方，すでに来たのであれば，あけぼのの時期は超えつつあると思われるかもしれない．しかし，上記でできて広くユーザに供されているのは，まだまだ発展段階初期の量子コンピュータである．量子力学で Schrödinger 方程式に代表される連続量の世界の影響を受けたアナログ性もまだ有することや，量子状態が脆いことによるデコヒーレンスエラー，ゲート操作のエラー，測定エラーなどによる限界[☆14]がある．

それら限界を乗り越えていくという観点からは，まさしく近未来量子コンピュータを大規模化・誤り訂正可能化・耐故障性保証する前のあけぼのの状態である．このような量子コンピュータシステムのあけぼの・曙光がやうやう差し込んできたところで，それを確とした陽光にしていく時期である．たとえば，本稿の第 1 章の書き出しで量子コンピュータのハードウェアとソフトウェアの記述が，従来コンピュータのきれいにレイヤ化された世界と違うなどといった違和感を持たれた方は，今このタイミングが最も面白い研究開発段階であることに思い至る可能性が高い．このような時期というのは，まさしく半世紀以上前に今のコンピュータの原型が発明されて動作し始めた黎明期に匹敵するもので，ぜひ多数の方が参画して未来を拓いていただけることを望むところでである．

一般のユーザ向けに，量子コンピュータのクラウドサービスが提供されている．2016 年に開始された IBM Quantum Experience がさきがけで，そこ

☆14 ちなみにこのような限界を書くと，現時点の量子コンピュータシステムは有用なのかという疑問がわいてくるかもしれないが，このレベルの量子コンピュータで効率良く解ける問題というのが多様に開拓されつつあることを念のため書いておきたい．代表例は，本稿で述べた Shor の位数発見アルゴリズムを拡張した Kitaev の位相推定の部分を，量子コンピュータと従来コンピュータでそれぞれ得手の部分を担当して反復計算する変分量子固有値推定アルゴリズムがある．そこでは，文中で述べた n 量子ビットで 2^n 次元の行列を扱える点を活用して，量子コンピュータでそのような行列（Hamiltonian）の 2 次形式計算が n の低次のオーダの時間で計算できることを活用する．

では現在 15 量子ビットまでの種々の特徴を持ったマシンをフリーに使うことができる．その際には，5 量子ビットの場合なら，5 線譜に音符を書くようにゲートを配置して実行できる．そこで構成した量子回路を通して，ユニタリ行列を軸にした線形代数をある面学ぶこともできる．現在では，多くの IT ベンダがクラウドサービスの提供を開始しているところでもあり，習うより慣れろというだけではないが，今そこにある量子コンピュータシステムのサービスを使ってみない手はない．特に若手の方々は，現在のコンピュータが確立されて以来結構な年数が経っているところで，次世代の新奇のコンピュータの黎明期を楽しまない手はないのでは．ぜひ体験して未来を感じ，そして作っていっていただきたい．

参考文献

1) Manin, Y. I : Classical Computing, Quantum Computing, and Shor's Factoring Algorithm. Ast'erisque, 266, S'eminaire Bourbaki, exp. No.862, pp.375-404 (2000).
2) Feynman, R. P. : Simulating Physics with Computers. Int. J. of Theore. Phys., 21, 6/7, 6, pp.467-488 (1982).
3) Shor, P. : Algorithms for Quantum Computation : Discrete Logarithms and Factoring. Proc. 35th Annual Symp. on Found. of Comp. Sci. (FOCS), pp.124-134 (1984).
4) Ito, T. and Vidick, T. : A Multi-prover Interactive Proof for NEXP Sound against Entangled Provers. Proc. 53rd Annual Samp. on Found. of Comp., pp.243-252 (2012).
5) Ji, Z., Natarajan, A., Vidick, T., Wright, J. and Yuen, H. : MIP*=RE. arXiv:2001:04383 (2020).

(2021 年 1 月 23 日受付)

■今井　浩（正会員）　imai@is.s.u-tokyo.ac.jp

東大計数工学科 1981 年卒業，同情報工学専門課程 1986 年修了，工学博士．1986 年九大情報工学科助教授を経て，1990 年より東大情報科学科，現在東大情報理工学・コンピュータ科学専攻教授．JST ERATO 今井量子計算機構研究総括・同 ERATO-SORST（2000 ～ 2011 年）．本会量子ソフトウェア研究会主査．