技術動向レポート

量子コンピュータの金融分野への適用の見通し

サイエンスソリューション部
チーフコンサルタント　宇野　隼平

近年、海外のITメーカーを中心に量子コンピュータ開発への参入が相次いで発表され、量子コンピュータ業界の動向に大きな注目が集まっている。本稿では、量子コンピュータの概要、近年の動向について紹介するとともに、金融分野への適用の見通しについて紹介する。

1. はじめに

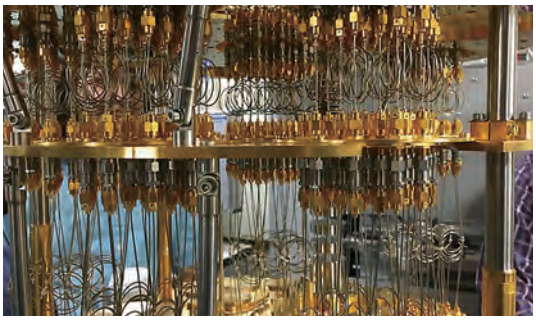
近年、従来のコンピュータとは全く異なる原理に基づいて動作する量子コンピュータの開発競争が本格化しており、大きな注目を集めている。

量子コンピュータの実現方式のひとつである「量子ゲート方式」に関しては、IBMにより2017年11月に50ビットのプロセッサーのプロトタイプの構築が発表された(1)ほか、intelにより2018年1月に49ビットプロセッサーの開発(2)、Googleにより2018年3月に72ビットのプロセッサーが相次いで発表されている(3)。図表1にIBMの量子コンピュータIBM-Qの画像を示す。

また、量子コンピュータの別の実現方式である「量子イジング方式」に関しては、D-Wave社により2011年に128ビットのD-Wave Oneが発表されたのを皮切りに、その後256ビット、512ビット、1024ビットと更新を重ね、現在の最新版として2017年1月に2048ビットのD-Wave 2000Qが公開されている(4)。

こうした開発競争の原動力となるのは、量子コンピュータを用いることにより従来の方式に基づくコンピュータの限界を超える高速化が実現され、これまで計算時間の関係で解くことが出来なかった問題を解決することが期待されているためであり、今後、開発競争が更に激しくなっていくと考えられる。

図表1　IBM-Q



（出典：https://www.flickr.com/photos/ibm_research_zurich/）
（左図：量子コンピュータIBMQの内部構造、右図：希釈冷凍機に取り組むIBMの研究者）

2. 量子コンピュータの概要

従来のコンピュータは、使用する全てのデータを0または1のビット列により表現しており、ビット列に対して操作を行うことで演算を行っている。一方で量子コンピュータは、量子力学の重ね合わせの原理を使うことにより、0と1の両方の状態を同時に取るような重ね合わされたデータを表現するビットを作成することが可能であり（図表2及び図表3参照）、また重ね合わされた複数のビットを同時に操作することにより、従来のコンピュータでは達成できないような高速計算を行うことが期待されている[(5)]。例えば50ビットの量子コンピュータでは、2^{50}個（約10^{15}個）の全てのデータに対して同時に演算を行うことが可能であり、従来のコンピュータが解くのに非常に多くの時間がかかっていた問題に対して、飛躍的な速度向上がなされる可能性がある。例えば、3.2節で後述する素因数分解では、図表4に示すように、従来のコンピュータでは、素因数分解する量に応じて指数関数的に計算量が増加するのに対して、量子コンピュータでは、単に多項式的に計算量が増加するだけであることが知られており、大きな数に対しては量子コンピュータのほうが高速に素因数分解することが可能であることが予想される。

現在、量子コンピュータには様々な実現方式があるが、特に「量子ゲート方式」と「量子イジング方式」という2つの方式に注目が集まっている。量子ゲート方式では、従来のコンピュータと同様に、データを収めたビットに対して操作を行うゲートを組み合わせた回路を作成し演算する。量子ゲート方式は、従来のコンピュータと同様の汎用的な計算を行うことが可能であるが、現状では、数十個という比較的少ない量子ビットまでしか扱うことが出来ない。

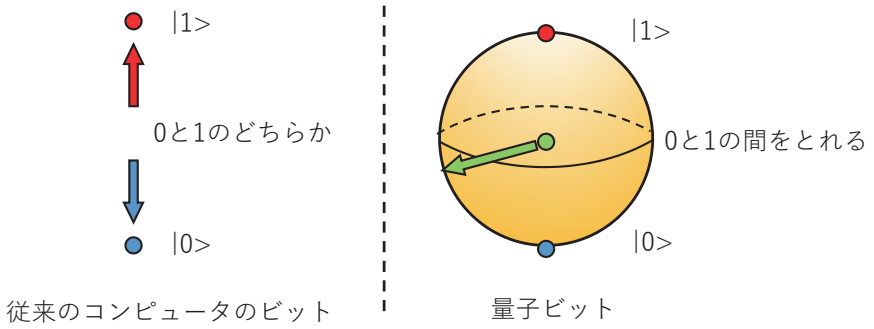
量子コンピュータのもう一つの方式である量子イジング方式は、組合せ最適化問題を解くことを目指した量子コンピュータであり、汎用的な目的のためには使用できない一方で、数千ビットの量子コンピュータが既に利用可能な状態となっており、近い将来、実用的なアプリケーションが出てくることが期待されている。ただし、量子イジング方式の量子コンピュータが、従来のコンピュータより速度が向上するかどうかは、現在までのところ理論的、実験的に確認されておらず、今後、更なる研究が必要である。

量子コンピュータは現在、企業毎に様々なテクノロジーにより実現されている（図表5参照）。各テクノロジーには一長一短があり、定まったものは無い[(6)]。例えば、量子ゲート方式では、IBM、Google、Alibaba、Rigetti 等は超伝導素子、Microsoft はエニオン、IonQ はイオントラップ、Xanadu は光量子のテクノロジーを用いて実現しており、また、量子イジング方式では、D-Wave、Qilimanjaro は超伝導素子、NTT は光量子により実現している。

また、量子コンピュータの開発とともに、量子コンピュータを使用するためのソフトウェアも開発が進んでおり、IBM の Qiskit、Microsoft の QDK、Google の Cirq、Rigetti の Forest 等が広く使用されている[(7)]。これらのソフトウェアにより、容易に量子コンピュータのプログラミングを行うことができる環境が整備されつつある。

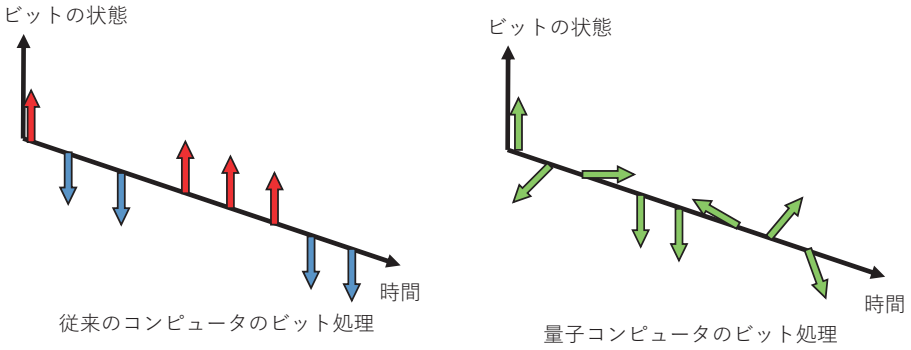
量子コンピュータの産業への応用の検討も各所で始まっている。例えば、国内の動きとして、2018年5月に、慶應義塾大学に量子コンピュータ研究拠点「IBM Q ネットワークハブ」が設立された[(8)]。IBM Q ネットワークハブは、ゲート方式の量子コンピュータを用いた実用的なアプリケーションの研究開発を、産学連携により行うことを目的に掲げており、IBM や大学の研究者のほか、金融業界からみずほフィナンシャル

図表2　従来のコンピュータのビット(0,1)と量子ビット(0～1)の違いのイメージ



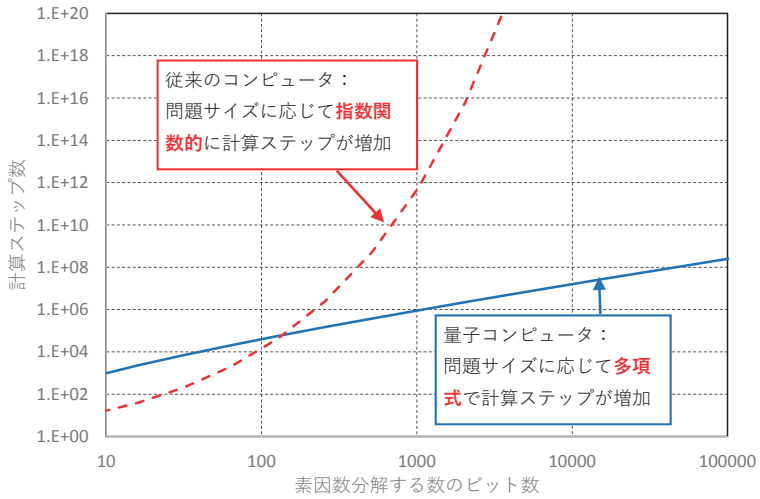
（資料）各種資料に基づきみずほ情報総研作成

図表3　従来のコンピュータと量子コンピュータのビット処理の違いのイメージ



（資料）各種資料に基づきみずほ情報総研作成

図表4　従来のコンピュータと量子コンピュータのビットの計算量の比較の例



（資料）各種資料に基づきみずほ情報総研作成

図表5　量子コンピュータの実現方式の一例

量子ゲート方式

テクノロジー	企業名
超伝導素子	IBM
	Google
	Alibaba
	Rigetti
エニオン	Microsoft
イオントラップ	IonQ
光量子	Xanadu

量子イジング方式

テクノロジー	企業名
超伝導素子	D-Wave
	Qilimanjaro
光量子	NTT

（資料）各種資料に基づきみずほ情報総研作成

グループ、三菱 UFJ フィナンシャル・グループ、化学業界から JSR、三菱ケミカルの4社が参画している。著者もみずほフィナンシャルグループの一員として本活動に参画し、IBM-Q の実機を使用した研究活動を行っている。

また、IBM はこの他にも、「IBM Research Frontiers Institute（RFI）」という企業とともに基礎研究を行うコンソーシアムを2016年から開始しており[(9)]、このコンソーシアムの中で量子コンピュータを主要な研究テーマの一つとして掲げている。国内の RFI 参加企業として、JSR、本田技研、日立金属、キャノン、長瀬産業が公表されている。

この他、大阪大学には量子情報・量子生命研究部門が設置され、「資源・エネルギーや医療など社会問題解決への貢献や事業化も含めた社会実装をめざす」としている[(10)]。また、東北大学・東京工業大学は、イジング方式の量子コンピュータを利用して産業界とともに実社会の問題を解決することを目的とした「量子アニーリング研究開発コンソーシアム（仮称）」を2019年4月に発足することを表明し[(11)]参画企業を募っており、既にいくつかの国内企業が参加を発表している。

3. 金融分野への適用の見通し

このように、国内外の企業、研究機関が盛り上がりを見せている量子コンピュータ業界であるが、現在までのところ発表されている量子コンピュータはビット数が少なく、またビットの量子状態を保つことが困難であることに起因するノイズが大きいため、実用的なアプリケーションはまだ見つかっていない。以下、本稿では、大規模な量子コンピュータが将来的に実現された場合における金融業界への適用の見通しについて紹介する。

(1)金融商品の価格決定及びリスク評価

金融派生商品の価格決定や、資産リスク評価指標である Value at Risk 等の算出の際にモンテカルロ法が広く使用されており、様々な未来にありうるシナリオを計算機上で生成し、各シナリオにおいて評価した金融商品や資産価値の結果を処理することで、計算を行っている。モンテカルロ法を用いた計算で正確な値を得るためには非常に多くのシナリオを考慮する必要があり、多くの計算機資源が必要となるため、ゲート式の量子コンピュータによる高速化が期待さ

れている。

近年、現在モンテカルロ法が使用されているような計算に対して、量子コンピュータのビットの重ね合わせを利用した計算手法が提案された[12][13]。量子コンピュータでは、ビットの重ね合わせによる複数のシナリオの同時計算を行うことが可能なため、従来のコンピュータのモンテカルロ法よりも高速に計算を行うことができる可能性がある。現在までのところ、量子コンピュータでのモンテカルロ計算は単純なモデルでの検証計算のみが実施されているだけであり[13]、従来のコンピュータより高速に計算しているとまでは言い難いが、将来的に非常に大規模な量子コンピュータが実現されれば、高速な計算が可能になることが期待される。

(2)暗号解読によるリスク

量子コンピュータを用いた最も重要な影響の一つとして、暗号に関するセキュリティ面の影響が挙げられる。

現在、ネットバンキングなどのインターネットを通じた通信において、第三者による情報の盗聴や改ざんを防ぎ情報の秘匿性を保つために暗号技術は欠かせない技術である。暗号技術を使用した通信では、送信者が暗号化鍵を使用して情報を暗号化し、受信者が復号鍵を使用して情報の復号を行う。暗号技術は、大まかに分類すると、鍵の性質により、共通鍵暗号方式と公開鍵暗号方式に分類される。

共通鍵暗号方式は暗号化鍵と復号鍵として同一のものを使用する暗号技術である。共通の鍵を使用するため、送信者と受信者で鍵を事前に共有するための何らかの方法が必要である。

公開鍵暗号方式は、暗号化鍵と復号鍵が異なるものを使用する暗号技術である。情報の受信者は暗号化鍵を公開し、送信者は公開された暗号化鍵を使用して情報を暗号化し送信する。第三者は、暗号化鍵を入手することは可能であるが、復号鍵を入手しない限り情報を盗聴、改ざんすることは事実上不可能であるとされている。

公開鍵暗号方式の多くは、素因数分解問題や離散対数問題等の問題を解くことが、従来のコンピュータでは困難であることに基づいているが、ゲート方式の量子コンピュータを用いることで、これらの問題を指数関数的に高速に計算できることが示唆されている[14][15]。このため、もし大規模な量子コンピュータが実現されれば、現在使用されている公開鍵暗号の大部分が安全でなくなる可能性がある。

近年の量子コンピュータの急速な発展状況を受けて、米国国家安全保障局(NSA)により2015年8月に量子コンピュータの脅威に対する懸念が示されており[16]、また米国国立標準技術研究所(NIST)では、耐量子暗号の標準化に向けた活動が行われている[17]。

現在公開鍵暗号としているRSA等の暗号を解くためには、数万から数十億の量子ビットが必要であると見積もられており[18][19]、直ぐに公開鍵暗号が解読されるというわけではないが、2030年頃までに暗号が解けるような量子コンピュータが実現するという見積もりもあり[20]、また比較的少ない量子ビット数で素因数分解を実現するようなアルゴリズムも提案されてきている[21][22]。

システムの大規模な入れ替えには、計画から実装まで数年から十年程度の期間を要すると考えられるため、専門家からの情報収集等により動向を把握するとともに、予めシステムの更新に関する検討を行うことも重要であると考えられる。

(3)資産の組み合わせの最適化

金融分野においても、イジング型の量子コンピュータを用いて計算可能なような最適化問題

の例がいくつか提案されている。例えば、D-Waveの量子コンピュータを用いて、比較的単純な例ではあるが、利益を最大化するように資産を組み合わせ、ポートフォリオの最適化を行った例が報告されている(23)。また、異なる市場での商品価格差を利用して利益を挙げる裁定機会の問題に関しても、D-Waveの量子コンピュータを使用した例が報告されている(24)。

一方で、量子イジング型のコンピュータでは、イジングモデルと呼ばれる特殊な型の問題に最適化問題を落とし込まなければいけないこと、ビット数が少なく離散的な変数に関する最適化問題しか解くことが出来ないことから、まだ現実的に適用可能な問題は見つかっておらず、引き続きハードウェアの発展に注視するとともに、適用可能な問題の検討を行っていく必要がある。

4. 結び

量子コンピュータは10年ほど前まで、数ビットを使った計算を行うのがやっとの状況だったのに対して、ここに来てゲート方式では数十ビット、イジング方式では数千ビットを扱うことが出来るようになってきている。扱えるビット数が急速に増加している状況に伴い、世間からの注目が大きくなることで、更に開発競争が激化しビット数の増加につながる可能性もある。

現在のビット数では、まだ現実的なアプリケーションを見つけるのは難しいかも知れないが、急速に発展している量子コンピュータに触れてみて、今後、大規模な量子コンピュータが実現された場合に実現できそうなことについて見極めておくのは重要であると考えられる。引き続き量子コンピュータの急速な発展が続くとともに、多くの人が量子コンピュータにふれることで、本稿の想定よりも遥かに広い範囲に量子コンピュータが適用されていくことを期待したい。

注

(1) IBM ホームページ
https://www-03.ibm.com/press/us/en/pressrelease/53374.wss

(2) intel ホームページ
https://newsroom.intel.com/news/intel-advances-quantum-neuromorphic-computing-research/

(3) Google AI ホームページ
https://ai.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html

(4) D-Wave ホームページ
https://newsroom.intel.com/news/intel-advances-quantum-neuromorphic-computing-research/

(5) もう少し詳しく言うと、量子コンピュータでは、最終的には重ね合わさったデータの内の一つしか読み出すことが出来ないため、目的とするデータを得るためには、量子の干渉の性質を用いて、誤った結果を示すデータを相殺する必要がある。多くの問題では相殺する方法は非自明であり、このため、任意の並列計算可能な問題に量子コンピュータが適用可能というわけではない。

(6) QUANTUM COMPUTING REPORT ホームページ
https://quantumcomputingreport.com/scorecards/qubit-count/

(7) QUANTUM COMPUTING REPORT ホームページ
https://quantumcomputingreport.com/resources/tools/

(8) 慶應義塾大学ホームページ
https://www.keio.ac.jp/ja/news/2018/5/22/27-44149/

(9) IBM ホームページ
https://www.ibm.com/think/jp-ja/business/research-frontiers-institute/

(10) 大阪大学ホームページ
http://otri.osaka-u.ac.jp/images/pressrelease180701.pdf

(11) 東北大学ホームページ
https://www.tohoku.ac.jp/japanese/2018/07/press20180719-01-renkei.html

(12) P. Rebentrost, B. Gupt, and T. R. Bromley「Quantum computational finance: Monte Carlo pricing of financial derivatives」Phys. Rev. A 98, 022321（2018年）

(13) S. Woerner and D. J. Egger「Quantum Risk Analysis」arXiv:1806.06893（2018年）

(14) P. W. Shor「Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer」SIAM Journal of Computing, volume 26, no 5, pp. 1484-1509（1997年）

(15) P. W. Shor「Algorithms for Quantum Computation: Discrete Logarithms and Factoring」IEEE Computer Society Press, pp. 124–134（1994年）.

(16) Neal Koblitz and Alfred J. Menezes「A riddle wrapped in an enigma」http://eprint.iacr.org/2015/1018.pdf（2015年）
(17) NIST ホームページ
https://csrc.nist.gov/projects/post-quantum-cryptography
(18) T. Kleinjung, K. Aoki, J. Franke, A. Lenstra, E. Thome, J. Bos, P. Gaudry, A. Kruppa, P. Montgomery, D. Osvik, H. te Riele, A. Timofeev, and P. Zimmermann「Factorization of a 768-bit RSA modulus」CRYPTO'10, pp.333-350（2010年）
(19) A. Fowler, M. Mariantoni, J. Martinis, and A. Cleland「Surface codes: Towards practical large-scale quantum computation」Phys. Rev.A, 86:032324（2012年）
(20) NIST ホームページ
https://csrc.nist.gov/csrc/media/publications/nistir/8105/final/documents/nistir_8105_draft.pdf
(21) E. Martin-Lopez, A. Laing, T. Lawson, R. Alvarez, X. Q. Zhou, and J. L. O'brien「Experimental realization of Shor's quantum factoring algorithm using qubit recycling」Nature Photonics 6, 773（2012年）
(22) Eric R. Anschuetz, Jonathan P. Olson, Alán Aspuru-Guzik, Yudong Cao「Variational Quantum Factoring」arXiv:1808.08927（2018年）
(23) G. Rosenberg, P. Haghnegahdar, P. Goddard, P. Carr, K.Wu, and M. L. de Prado「Solving the Optimal Trading Trajectory Problem Using a Quantum Annealer」IEEE
Journal of Selected Topics in Signal Processing 10, 1053（2016年）
(24) Gili Rosenberg「Finding Optimal Arbitrage Opportunities Using a Quantum Annealer」
https://1qbit.com/whitepaper/arbitrage/（2016年）