第 89 回 JIPDEC セミナー講演レポート

非技術者が知っておきたい「量子」の話-社会とビジネスはどう変わる？-

国立研究開発法人産業技術総合研究所
ナノエレクトロニクス研究部門
エレクトロインフォマティクスグループ
主任研究員　松崎　雄一郎氏

量子とは何か？

量子の定義はいろいろあるが、その 1 つとして「量子とは連続的にではなく飛び飛びの量しか出すことができないもの」ということができる。例えば、水をコップに注ぐ場合の量は切れ間なく連続した値を入れることができるが、人を数える時は 1 の次は 2 となる。

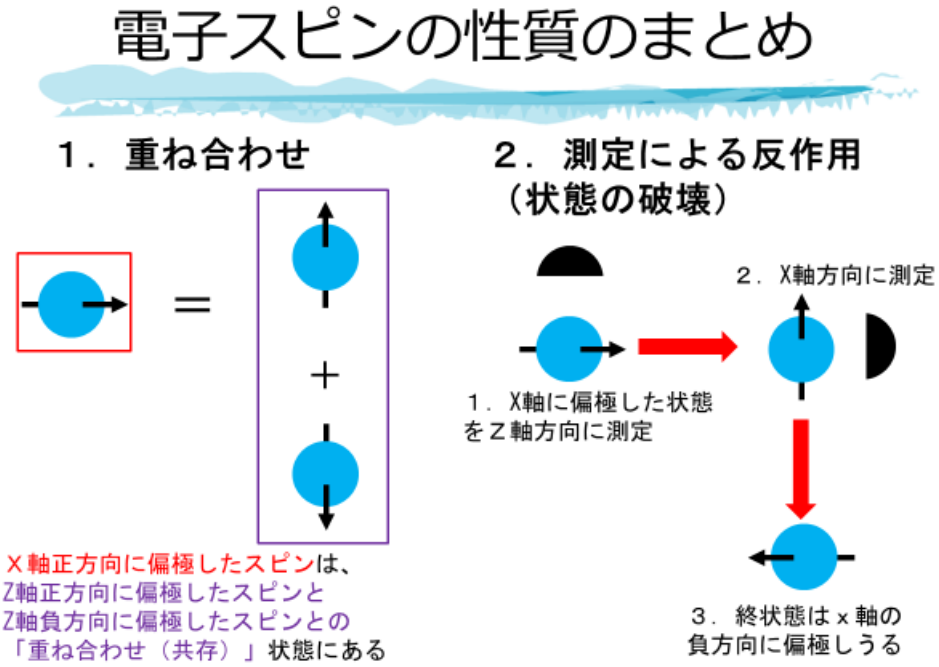
これまで、古典的な電磁気学により、磁石は連続的な磁場（の値）が発生可能と考えられていたが、近年、非常に微視的な領域ではこの説が破綻していることが判明し、そこから量子力学に注目が集まるようになった。

量子力学の領域では、最小の磁石（＝電子スピン）は離散的で確率的な値しか出さないという性質を持っている。この性質が、量子力学でよく聞かれる「重ね合わせ」の原理に密接に関係してくる。横向きの電子スピンは、実際に磁場センサで測定するまで上向きとなるか下向きとなるかはわからない。つまり、人間が測定しようとしない限りは両方の状態が共存している状態であり、これを「重ね合わせ」の状態という。「重ね合わせ」という概念は、我々の日常生活にはない感覚なのでなかなか理解が難しいところではある。

「重ね合わせ」は非常にノイズに脆弱で、少しの熱雑音や磁場ノイズで簡単に壊れてしまうため、我々が生活する mm、cm の世界では「重ね合わせ」を観測するのは難しい。しかし、ナノメーター、オングストロームといった微視的な世界では「重ね合わせ」状態を作り

制御することが可能となるため、これを積極的に利用しようとするのが量子情報である。

もう１つの量子の重要な性質として「測定の反作用」がある。人差し指で頬を押すと、指にも反発力を感じるのと類するもので、測定により上下いずれかの向きになった電子スピン（横向きに対して「重ね合わせ」状態にある）を再度横方向から測定すると、当初の横向きの状態とは異なる値になる（＝測定が状態を壊す）可能性があるというものである。この反作用は、構造変化やノイズ除去をどれだけ行っても取り除くことができない性質で、量子暗号や量子センサ、量子コンピュータの実現に用いられている。量子的な世界では、「測定が状態を壊しうる」ことが重要な点となる。

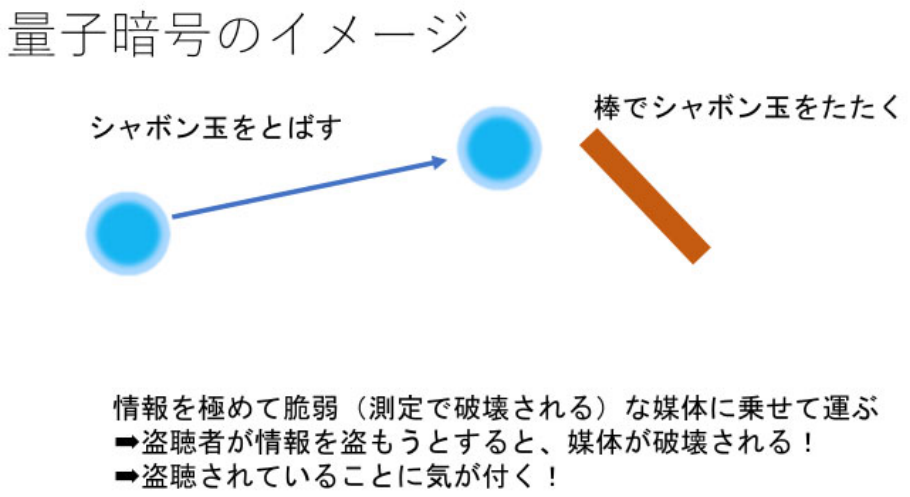


量子暗号

量子暗号はすでに商品化されている。量子コンピュータが絶対零度に近い極低温の環境でないと「重ね合わせ」を維持できないのに対し、量子暗号は光を使用し室温でも「重ね合わせ」を長時間維持できるため、早くから商用化されている。

量子暗号の最大の特長は「安全性の高さ」である。現在利用されている古典暗号は「現在のスパコンでは解読に時間がかかる」だけで、原理的には解読可能であり、また、解読するためのアルゴリズムを誰かが発見すればすぐに解読されてしまう。一方、量子暗号は量子力学が正しい限り、どのような高性能の量子コンピュータが開発されたとしても安全性が保証される。

量子暗号では、微弱な光の偏光が電子スピンの役割を果たしている。光を使用する利点は、重ね合わせの維持が容易、電子スピンに比較し長距離飛行が可能という点が挙げられる。また、情報を光という極めて脆弱な媒体で運ぶため、途中で第三者が盗聴（測定）しようとすると媒体が破壊され状態が変化するため検知することができる。



量子暗号の課題としては、量子暗号で使用する光は非常に微弱であり、光ファイバーに吸収されやすいため、現段階では実現しているのは数百 km から千 km に留まるため、実用に向けて長距離化が大きな課題である。また、量子性装置は非常に複雑なため、配信速度の向上も難しい課題である（現在は kbps から Mbps 程度）。

現在、世界各国が量子暗号の開発に取り組んでいるが、中でも中国は特に力を入れており、量子暗号用の衛星打ち上げを行い、2017 年に世界初の衛星－地上間（約 1200km）の量子暗号通信を成功させている。宇宙空間は空気がないため、光が通りやすく吸収されづらいので距離を延ばすことができる。また、欧州は世界初の量子暗号商用化に成功しており、長距離化の研究も世界一である。一方、米国は量子コンピュータでは群を抜いており、量子暗号に関しても最近動きが出てきている。日本では、様々な研究所・企業が連携して東京内で量子暗号ネットワークを構築している。

量子コンピュータ

1994 年に量子コンピュータを使用することにより素因数分解が短時間で可能となる画期的なアルゴリズムが発見され、そこから爆発的なブームが始まった。現在インターネット等

で使用されている RSA 公開鍵暗号は素因数分解を使用しており、現在のコンピュータでは解読に数十億年かかるので安全とされていたが、量子コンピュータが登場すると数分で解読されてしまうことになるため、社会的なインパクトは大きかった。ここから、世界中で基礎研究が急激に進展したが、実際に動作させることができるのは数量子ビットにとどまり、その後、実用に必要な数百万数千万程度を集積させることは困難という悲観的観測が支配的になり 2005 年～2011 年頃は長い冬の時代を迎えた。

ところが、2011 年に D-Wave が商用量子コンピュータの販売開始を公表したことで量子コンピュータ実用化への期待が一気に高まり、第二次量子コンピュータブームが起き、現在では Google、IBM、Intel 等大企業だけでなくベンチャー企業も参入している。ただし、ここで重要な点は、量子コンピュータと呼ばれるものは 2 種類あり、2011 年に D-Wave が販売開始したのは、以前より世界各国で研究開発が行われていたどんな問題も（さらに一部の問題は高速に）解くことができる汎用型量子コンピュータではなく、組合せ最適化問題（関数の最小化）に機能特化したアニーリング型量子コンピュータだという点である。

アニーリング型量子コンピュータ

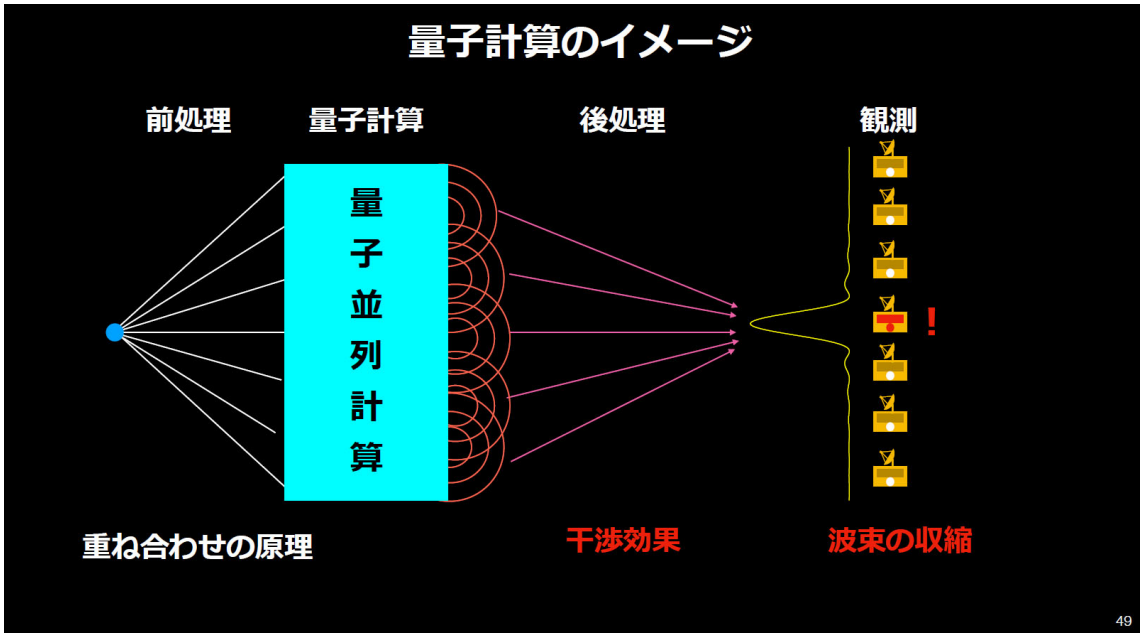
量子アニーリングがドラスティックなスピード向上をもたらすかどうかはまだ理論的に決着していない。現時点での実装の仕方では、せいぜい多項式時間程度のスピードアップ程度が限界と考えられている。また致命的な問題として、古典的コンピュータの半導体が備えているエラー訂正機構をどのように実装できるかが判明していない。2000 量子ビット程度であればエラー訂正なしでも機能したとしても、今後何万ビット、何億ビットと大規模集積

化するほどエラーも増え、正しい答えを出さないのではないかという懸念がある。

しかし、汎用性を排除し一気に実用化に進め、量子コンピュータへの期待を高めた点でD-Wave の功績は大きい。また、組合せ最適化問題自体は応用範囲が極めて広い（画像解析や機械学習、金融投資の最適化、車の自動運転における経路探索、生産計画の最適化等）ので、これまでとは全く異なるアプローチを可能とする点、実機をもとに現在整備されていない量子アニーリングの理論構築が可能となる点、で意義があると考える。

汎用型量子コンピュータ

汎用型は、実現は相当難しいが成功すれば社会へのインパクトが大きいと言われている。量子コンピュータは重ね合わせの原理を使って並列計算を行うため、非常に高速な処理が可能となるが、それを最終的な解に収束させることが難しい。素因数分解に関しては、1994年にアルゴリズムが発見されたが、その他に関しては良いアルゴリズムがなかなか発見されず、ここが汎用型量子コンピュータの難しさということができる。

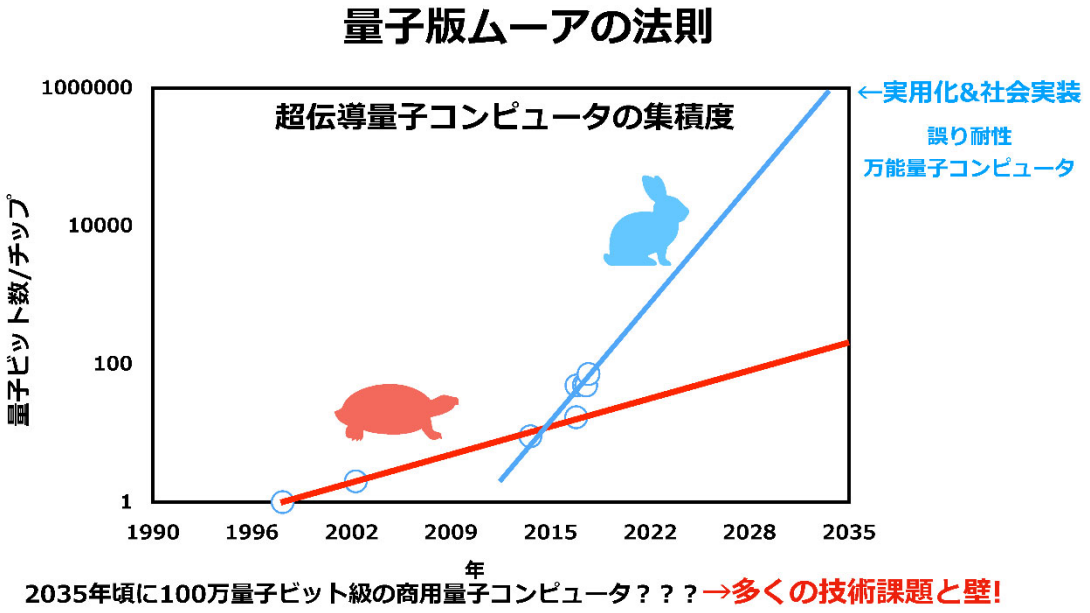


素因数分解の量子アルゴリズムでは、古典コンピュータで宇宙の寿命以上かかると言われる RSA2048（10 進数 617 桁）を約 1 時間程度で解読することが可能となる。素因数分解以外には、分子の化学反応・相互作用のシミュレートを行う量子化学計算、古典機械学習を高速化させる量子機械学習に期待が高まっている。創薬は、現在、経験や勘に基づくトライアンドエラーで行われているが、分子の化学反応・相互作用をシミュレートすることで、効率的な検証が可能となる。また、人工肥料合成で行われている窒素をアンモニアに変えるメカニズムや、超伝導と温度の関係を解明することで、食糧やエネルギーの問題を解決に導く

可能性がある。

また、すでに現在活用が進んでいる機械学習に対しても、非常に効果が期待できると考えられている。膨大なデータを読み込み、そこから傾向や意図を導き出す機械学習では、学習データが少なければ計算は早いが結果の信頼性に欠け、学習データが多ければ信頼性は高まるが計算に膨大な時間がかかる。量子コンピュータを使用すれば、高速で高い信頼性の結果を導き出すことが可能となる。これを実現するには、量子的な重ね合わせの状態を維持したまま大量の古典的なデータを保存するための量子的なランダムアクセスメモリ（QRAM）が必要となるが、この構成が極めて難しく今後の研究課題となっている。

量子コンピュータの開発状況は、実用には百万、数千万量子ビットが必要だが現状で実現しているのは 100 量子ビットに満たないレベルである。しかし、近年開発スピードは非常に高まっているので、2035 年頃には 100 万量子ビット程度の集積が可能となり、実用の目途が立つ可能性がある。



まとめ

このほか、量子センサの研究等も進んでいる。量子センサは、医療や材料探索等アプリケーションの幅が広く将来性もあると思われる。ただし、現状では古典的センサと性能差があまりないため、実現化のインパクトという点では、量子コンピュータの方が大きいと思われる。

私自身は、現在、これら量子暗号、量子コンピュータ、量子センサを組み合わせたハイブ

リッド型アーキテクチャの研究を行っている。例えば、量子秘匿センサは、量子センサで患者の状態を計測しその個人データを量子暗号で送信することで、盗聴もできずセンサ内にデータが残らないため個人情報保護を強化することができるもので、IoT への活用も視野に入れている。