量子コンピューティング技術実用化への道のり

FUJITSU JOURNAL / 2018年2月20日

みなさんの会社のITチームも、重要なデータや電子メールには暗号化テクノロジーを適用することを常識として捉えていることでしょう。たとえば、RSA非対称公開鍵/秘密鍵を使うこともその1つです。それは素因数分解に関する数学的な問題を応用したもので、非常に強力な暗号化の方法と考えられています。この暗号化方式では、基本的に2つの大きな素数を掛け合わせて、その答えが公開鍵として公表される一方で、暗号から元のデータを復号するために用いられる秘密鍵は、その2つの素数のどちらかです。

このように説明すると、掛け算の問題が解ければ秘密鍵は簡単に見つけられるのではないか、と思われるかもしれません。確かにその通りで、不可能ではないのです。しかし、2048ビットキーに相当する617桁の10進数から正しい素因数を計算しようとすれば、一般的なPCでは6兆年もかかってしまいます。もちろんスーパーコンピュータを使えば比較的早く解けますが、それでも210億年。これは宇宙の年齢の1.5倍に相当する年月です。

では、もし暗号を解読するスピードを飛躍的に加速できる新しいタイプのコンピューティング方式が考え出されたとしたらどうでしょうか？　実は量子コンピューティング技術のおかげで、そ

れは徐々に実現しつつあります。量子コンピュータは、他とはまったく異なる科学の原理に基づいており、今までは一度に1つずつしかテストできなかったような可能性の選択肢を、すべて同時に処理することができるためです。どうすれば、そのようなことが実現するのでしょうか？　さあ、ここから少しの間、常識を忘れてください。

たとえば、スキーで丘から滑り降りているときに、目の前に木が現れたとします。そのままま っすぐ進むのは、あまり良い判断とはいえませんから、進路を右か左に変更することになるでしょう。ところが、量子コンピューティングの世界では、どちらか1つに決める必要はなく、同時に右と左の両方に進むことができます。これが、量子物理学の奇妙で驚くべき二元性なのです。

ちょっとした科学の話

その仕組みを理解するために、光の物理学に注目してみましょう。クリスティアーン・ホイヘンス が1670年に提唱したもので、光を波として扱うものです。彼の仮説は、100年後にトーマス・ヤングによって証明されました。ヤングは、二重スリット実験を行って、光が波の性質である回折と干渉を起こすことを実証したのです。この実験は、光源からの光を二重スリットを通して衝立に当てると干渉縞が現れるというものですが、基本的には池に石を投げ入れて作られる波紋と同じ現象といえます。

さらに100年以上経った1905年のこと、今度はアインシュタインが光の量子理論を提唱しました。それは、光が小さなエネルギーの塊であると考えるもので、その塊が「量子」です。ここから光の二元性が明らかになっていきます。つまり光は、波でもあり、粒子でもあるということです。彼の理論は、1920年代にルイ・ド・ブロイによってさらに進化しました。ド・ブロイの主張は、光が粒子として振る舞うのなら、粒子もまた波のように振る舞うというものです。この驚くべき考えは、やがて、トーマス・ヤングの実験と似た方法によって証明されることになります。物理学者たちが光の代わりに用いたのは、電子でした。そうして得られた回析パターンは、光のときと同じだったのです。また、ド・ブロイは電子の波長も確定することができましたが、あまりにも小さいため、観察は微視的な環境下でしか行えませんでした。

後にエルヴィン・シュレーディンガーは、さらに研究を進め、量子力学によって影響を受ける物理システムの時間的な振る舞いを表す式を定義しています。この式は、本質的には波動方程式で、任意のシステム内の物理量の確率を決定するものです。量子理論ではすべてが確率的に扱われるので、伝統的な物理学とは異なって決定論的ではありません。電子の存在確率も波の振幅の二乗で表されますが、この波を確率波と呼んで方程式の解も確率波となり、非常に重要な結論へとつながっていきます。

さらに不可解さを増す量子物理学

では、量子トンネリングについてお話ししましょう。粒子が壁に向かってスムーズな波形で動いていくと、壁に当たった粒子の波動関数は急激に変化することなく、滑らかに降下し、壁の反対側に小さな痕跡を残す場合があります。この現象は、確率的には小さくとも確実に起こりうることで、粒子が壁を通り抜けたことを意味するものです。この奇妙でまれな出来事を、量子トンネリングと呼んでいます。

もう1つの奇妙なものは、「重ね合わせ」という概念です。たとえば、aという波とbという波があり、これら2つの異なる波を合成するとします。その結果も波動方程式の解となりますが、ここでは確率波の話をしているので、量子的な考え方ではこのシステムの状態は、同時にaでもありbでもあるのです。この重ね合わせの能力こそが、量子理論と量子コンピュータを可能にする核心的な要素の1つになっています。

ところが問題は、量子状態にあるシステムの観察や計測ができないという点です。現実の世界における相互作用は、それがどのようなものであってもシステムを量子状態から離脱させ、古典的で観察可能な物理学の世界に引き戻してしまいます。つまり、観察することで変化が起こり、よく知られた状態に戻ることを強いられるというわけです。シュレーディンガーは、このことを、箱に入れた猫に関する実験を通じて説明しました。再度強調しますが、箱に入れた猫に関する実験、です。その猫は理論上の存在で、毒入りのフラスコと共に箱の中に収められています。そして、フラスコは50%の確率で起こる放射能崩壊によって壊れて毒を放出するのです。量子状態において、その猫は同時に2つの状態を取りうると考えられます。生きているかもしれないし、死んでいるかもしれません。そして、蓋を開けたときに量子状態が破られます。猫は生きているか、死んでいるかのどちらかの状態にありますが、両方の状態にないことだけは明らかです。しかし、蓋を開けるまでは、どちらもありうることになります。

もう1つの特有の効果は、一緒に生成されて同じ量子状態にある複数の粒子が、共有する波動関数を通じて結合している、あるいは絡み合っていることから生じるものです。それらの粒子を引き離しても実際には絡み合ったままなので、片方に変更を加えると、もう片方にもその変更が反映されます。しかも、両者の距離がどんなに離れていても、この効果は瞬時に現れるのです。

この重ね合わせと絡み合いのコンビネーションは、計算速度自体を速めるのではなく、すべての可能性を同時に計算できるという能力によって、コンピュータの処理速度を驚異的に向上させることができます。情報の最小単位であるビットの値は、古典的には0か1ですが、量子ビットは同時にその両方であることが可能で、これは、すべてが同時に起こることを意味するものです。その結果、個々の可能性を一度に扱えるようになり、まさに超弩級の並列コンピューティングが実現することになります。ただし、意味のある計算を行えるだけの時間、コンピュータの量子状態を維持できるかどうかは、大きな挑戦です。そうできれば望ましいものの、実際に作るのは本当に大変なことだといえます。しかし、もしその方法が明らかとなれば、現在使われている暗号化の方式は終焉を迎えるでしょう。

真の量子コンピューティングを実現するには、まだ明らかに時間がかかるので、RSA方式の暗号化と秘密鍵は今のところ安全です。しかし、真の量子コンピューティングではなく、単に処理速度の向上を目的としたらどうなるでしょうか？　実は、その点に着目した富士通は、量子力学からインスピレーションを得て、普通のデジタル回路上で量子的な技術を使ったハードウェアを用いることで、非常に高速な処理速度を実現するプロジェクトを成功させています。

その成果が「デジタルアニーラ」であり、この新アーキテクチャコンピュータは、組み合わせ最適化問題に関する分野の計算処理を高速化するためにデザインされました。つまり、有限の可能性の中から最善のものを見つけ出す能力に長けているということです。応用分野としては、たとえば、最短あるいは最安の旅程や最も効率的なルートの探索、最良の交通状況の管理とスケジューリングなどがあります。これが可能なのは、最適化のプロセスにおいて、量子トンネリングを模した処理により、検索や候補の状態の判定を同時に行えるためで、量子コンピューティングの恩恵を部分的に受けているのです。この方式のメリットは、標準的なテクノロジーを使うことで、生産や運用をはるかに簡単に行え、必要なエネルギーも小さくて済むというところにあります。

説明のために、古典的な「巡回セールスマン問題」を取り上げてみましょう。これは、ある都市を出発したセールスマンが、すべての都市を巡回する際に移動距離が最小になるような順番を決めるという問題ですが、「デジタルアニーラ」の解析速度は従来のシミュレーションによる方法と比べて1万7千倍も高速であり、ロジスティックスの最適化などに向いています。ムーアの法則に基づくチップの進化によってこの処理速度の差を実現しようとすれば、25年に渡る14世代分の改良が必要となるため、これがいかに重要な進歩であるかがわかるはずです。

この新しいアプローチは、災害管理、IoT向けアプリ、交通の最適化、分子のデザイン、そして医薬品のオーダーメイドなどの複数の産業分野に、大きなメリットをもたらす可能性を秘めています。しかも、まだ応用は始まったばかりなのです。富士通は、2018年からこの新しいテクノロジーを商業化していきます。さあ、もう一度、ご自身の常識を呼び戻し、量子的なコンピュータがあなたのビジネスにとって何ができるのかを考えてみてください。

FUJITSU JOURNAL　/　2018年2月20日