

# *Market Flash*

**量子コンピューターの世界 No1**  
**～加速度化する新世界～**

2022.02



日本アルプス電子株式会社  
NIHON ALPS ELECTRONICS CO.,LTD.



## ～量子コンピューター～

これまでのコンピューターの世界は、「ムーアの法則」に従って進歩し続けてきた。しかし、その「ムーアの法則」の終焉が見えてきている。それに代わって注目されているのが量子コンピューターである。最近の新聞でもよくこの「量子コンピューター」という言葉を見かけるようになった。巨大IT企業や米国、中国政府の開発競争にしのぎを削っている。「量子コンピューター」は確かにこれからの化学・科学の世界を大きく変え、進化させる可能性を秘めている。しかし、いまにも実用化できるコンピューターのように誤解を招くような報道も多いようである。今月はこの「量子コンピューター」の世界を覗いてみた。

### 1. ムーアの法則

1965年、インテル創業者のゴードン・ムーアは、集積回路上のトランジスタの数が18か月ごとに倍増していくことに気づいた。つまり、コンピューターのコストは変わらないのに、性能は1年半ごとに倍増していた。ムーアはこの法則に気づき、今後5年、10年は続くのではないかと予測したのである。実際にはすでに60年になろうとしている今もこの法則は生きている。スマートフォンは1970年代のスーパーコンピューターと比べて大きさは1万分の1、価格も1000分の1、性能は100万倍になっている。

しかし、そのムーアの法則もそろそろ終焉を迎えようとしているのも事実である。それは物理的な原因である。集積回路の性能はチップ1枚あたりに搭載する数を増やすことによって実現してきた。1971年にはトランジスタ同士の距離は1万ナノメートル（1メートルの10億分の1）だった。それが、2000年にはおよそ100ナノメートル、今は既に5ナノメートルから3ナノメートルに近づこうとしている。これほど微細になると電子が飛び移るようになり、演算能力が阻害されるのである。この物理的原意により「ムーアの法則」は終わりを迎えようとしている。

### 2. 量子コンピューターの法則

では「ムーアの法則」の次に来るものは何か？

近未来を描いた著書「2030年：すべてが『加速』する世界に備えよ」で次のように書かれている。

テクノロジーの融合で破壊的变化は加速する

今、多くの産業に破壊的变化が起きていて、しかもこれからさらに大きな変化が起ころうとしているのは、テクノロジーの「コンバージェンス（融合）」の結果である。コンバージェンスを理解するには、基本から始めるのがいい。ムーアの法則は死が近いと言われるが、2023年には1000ドルクラスの普通のノートPCが、人間の脳と同じレベルのコンピューティング能力を持つようになる。その25年後には、同じクラスのノートPCが地球上の全人類の脳を合わせたのと同じ能力を持つようになる。

それ以上に重要なのは、このペースで進歩しているのは集積回路だけではないということだ。あるテクノロジーがデジタル化されると、**途端にムーアの法則にのっとなって「エクスポネンシャル（指数関数的）な」加速が始まる**。今このペースで加速しているテクノロジーの中には、人類が創造した中でも最も強力なイノベーションがいくつもある。量子コンピュータ、人工知能、ロボティクス、ナノテクノロジー、バイオテクノロジー、材料科学、ネットワーク、センサー、3Dプリンティング、AR、VR、ブロックチェーンなどだ。

注目すべきなのは、これまでバラバラに存在していた「エクスポネンシャル・テクノロジー」の波が融合しつつあるという事実だ。

レイ・カーツワイルが「**収穫加速の法則**」に従って計算したところ、**我々はこれからの100年で、2万年分の技術変化を経験することになるという。つまりこれからの1世紀で、農業の誕生からインターネットの誕生までを2度繰り返すくらいの変化が起きるのだ。**



## ～量子コンピューター～

### 3. 量子コンピューターとは？

量子コンピューターの仕組みを説明するのはとても難しい。インターネットや専門本などを読んでみてもいまだに理解できない部分が多い。多くの文献の中でもわかりやすい説明を書くと以下のようなものである。

量子コンピュータとは、「**量子力学特有の物理状態を積極的に用いて高速計算を実現するコンピュータ**」  
量子コンピュータの「量子」は量子力学の「量子」。

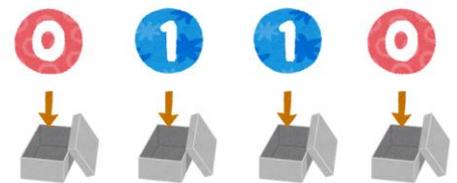
量子力学とは、大学レベルで学ぶ物理学の1つで、原子、電子などの非常に小さなものの動きを説明するために発展した理論。この量子力学によると、原子や電子、光の粒である光子などの微小なものや、超伝導などの非常に低温に冷やした物質においては、私達が普段目にしない不思議な現象が起きることが知られており、実際に実験的に確かめられている。

量子力学特有の物理状態である「**重ね合わせ状態**」や「**量子もつれ状態**」などが実現されている。そして、この量子力学特有の物理状態を積極的に用いてコンピュータを作ろうというのが、量子コンピュータである。これにより、これまでの計算よりもパワフルな**量子計算**と呼ばれる計算ができるようになる。

コンピュータと言われて皆さんが思い浮かべるのは、WindowsとかMacとかLinuxといったOSを搭載したコンピュータでしょう(厳密に言えば、OSはコンピュータではなくソフトウェアを動かすための基本ソフトのこと)。

このような一般的なコンピュータは、「量子コンピュータ」と比較する(classic computer)\*と呼ばれている。

古典コンピュータは、第二次世界大戦中に敵軍であるドイツ軍の暗号を解読する手法を数々考案したアラン・チューリングによってその動作原が考案されたとされており、「チューリングマシン」と呼ばれている原基づいたコンピュータは、ほぼ全てのコンピュータの基礎になっている



bitは「0」か「1」を表す

古典コンピュータでは、**情報の基本単位を「ビット」(bit = binary unitの略)**とし、それぞれを「0」か「1」の状態を取ることによって、2進数で数を保持し、**演算を行う。**

この数は、0または1のどちらかの状態を表すことができるが、**2つ以上の状態を同時に表すことができない。**実際のコンピュータでは、0か1の状態を表すのに、電圧をオン・オフで切り替えて行なっている。

これに対して、**量子コンピュータでは、状態の「重ね合わせ」という量子力学的な基本性質を用いる。**「重ね合わせ」とは、**2つまたはそれ以上の状態を同時に表すことができるということ。**

「重ね合わせ」は理屈上は分かりにくい原理だが、分かりやすく言えば「**コインが回っている状態**」のこと。コインが「表」や「裏」だと決まっているときには、「**コインが回転をやめて、倒れた状態**」のことを言う。

しかし、コインが回転しているときには「表」と「裏」が未決定の状態で、「**回転中**」という状態。いわば、観察するまでどちらかが分からない状態を「**重ね合わせ**」と呼ぶ。



## ～量子コンピューター～

実際には、もっと直感的に言えば、量子コンピュータの情報単位は、「重ね合わせ」により状態が2つ以上であり、0でもあり、1でもあり、2でもあり、3でもあるという状態になる。

しかし、重要なのは、観測されるときには、「0」か「1」か「2」か「3」のどれかが必ず観測されるということだ。

このような重ね合わせによる量子コンピュータの情報単位のことを、「量子ビット」(quantum bit=キュービット: qubit)と呼ぶ。

量子ビットは、例えばn量子ビットあれば、2のn乗の状態を同時に計算できることになる。

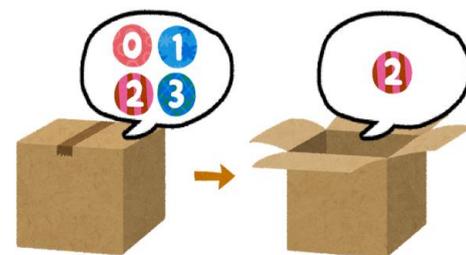
右の例では、「0」「1」「2」「3」は確率的に「重ね合わせ」られていると言える。「確率的」であるので、

実は量子コンピュータでは観測するごとに結果が違ってくる。

これを、「多世界解釈論」と呼ぶ。

イギリスの物理学者デイビッド・ドイッチュは「同時並行に存在する複数の世界で、同時並行に計算するものである」と表現している。

まるでSFの世界に感じられるものが、実際には現実に観測できるということになる。



「重ね合わせ」状態 必ずどれかが「観測」される



「観測」されるごとに違う値 = 「確率的」

量子コンピュータが具体的にどういった計算をしているのかを、金庫の暗証番号の解読方法を例に説明してみる。

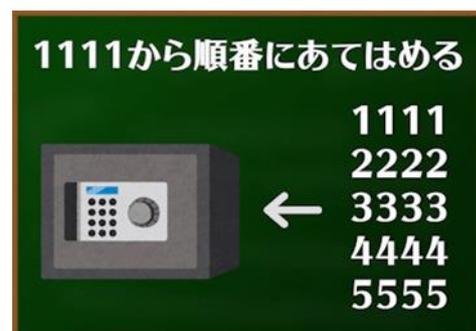
ここに5パターンの暗証番号を設定できる金庫がある。

設定できる番号は1111～5555までの数字。この中の一つの番号を金庫に設定したとする。

これを古典コンピュータが答を導き出す場合、1111から順に一つずつ試していくしか方法はない。いわゆる、しらみつぶし作戦である。

一方、量子コンピュータは『重ね合わせ』というものを使って、すべてのパターンを一度に試すことができる。

これは何通りもの計算を重ね合わせて、一度ですべてを考えることができるという量子の性質を使って計算しているからである。



量子コンピュータはこの重ね合わせの技術を使って、並列計算することができるので計算回数を格段に減らすことにより、スーパーコンピュータよりも圧倒的な速さで計算できるという仕組みである。

さて、このような説明で理解していただいたであろうか？

私自身は???である。

このレポートで全てを書こうと思ったら何十枚にも及ぶので、

仕組みについてより詳しく知りたい方には右の著書がおすすめである。

量子力学の仕組みからわかりやすく説明されている。





## ～量子コンピューター～

### 4. 量子力学の世界

量子コンピューターの仕組みを理解するには「量子力学」について知る必要がある。その内容をごくごく簡単にさわりだけご紹介したい（詳細は前述の著書を参照）

量子力学は、「日常生活よりもずっと小さな世界の仕組みをまとめた理論」である。ではどの程度小さな世界なのか？私たちの身の回りは全て原子という小さな粒で成り立っている。原子は物質の構成単位であり、量子の1つである。原子をさらに細かく見ると、マイナスの電気を持つ電子、プラスの電気を持つ陽子、そしてプラスでもマイナスでもない中性子というさらに細かい単位がある。電子、陽子、中性子などもすべて量子である。1個の原子の中では、中心にある陽子と中性子の周りを原子が回っている。

原子1個のサイズは約0.1ナノメートル。これはピンポン玉に例えると、原子：ピンポン玉はピンポン玉：地球と同等である。

身の回りを細かく見ていくと、すべて量子で成り立っており、世の中の物理現象を本当に支配しているのは量子力学と言える。しかし、量子力学の世界は、私たちの日常感覚とは全く異なる不思議な世界である。

その不思議な世界をよく実感できるシンプルな実験として、「2重スリットの実験」というものがある。スリットとは細長い隙間のこと。

図3  
水面を進む波を考えましょう。中央の隙間を通り抜けた波は、少し広がりながら又水面を進んでいき、後ろの壁にぶつかる。もっとも大きな波が当たるのは、後ろの壁のちょうど真ん中になる。

図4  
板に細長い隙間を2か所開けたとする。この場合、2つの波は、山と谷の波長が合う場合は強め合い、山と谷がちょうど逆転した場合には弱め合うことになる。  
2つの波は弱め合っ足り強め合ったりする。この現象を「干渉」という。  
ヘッドホンのノイズキャンセリング機能もこの現象を利用している。  
壁のちょうど真ん中のA地点は2つの隙間から同じ距離にある。この場合、A地点に達した2つの波は同じ振動のタイミングで重なり合い常に強め合う。しかし、A地点から左か右にずれていくと、到達する並みのタイミングがずれ、B地点、C地点、D地点と位置をずらしていくと、強め合って波が大きくなる位置と、弱め合って小さくなる位置が、縞模様のように交互に現れる。  
この結果、波の干渉によって壁に縞模様が現われるというのが、水面を進む波の2重スリット実験の結論となる。

図5  
それでは、水面の波に変わって1個の電子の場合を考えると、1つの隙間の場合は当然そのまま真っ直ぐ後ろの壁にぶつかる。  
次に隙間を2か所にした場合、右の隙間を通ったら壁の右寄りにぶつかり、左の隙間を通ったら壁の左寄りにぶつかるかと予想される。

図6  
実際にやってみると、予想に反する結果となる。  
まず電子1個を発射すると、壁にある1点にぶつかる。もう1個発射すると、今度は別の1点にぶつかる。これを繰り返していくと電子が当たった点が積み重なっていき、最後には電子が当たった位置と当たらなかった位置が縞模様のように交互に現れる。これは水面の実験において壁に波の大きな位置と小さな位置が縞模様のように並ぶ結果と似たものとなっている。  
1つの隙間をふさいで電子を発射してもこのような現象が起こらず、2か所の隙間を同時に通ることができる条件の時だけにこのような現象が起こる。  
これはサッカーボールなどのような大きな物質では決して起こり得ない現象である。



## ～量子コンピューター～

図3 水面を進む波が1つの隙間を通り抜けた場合

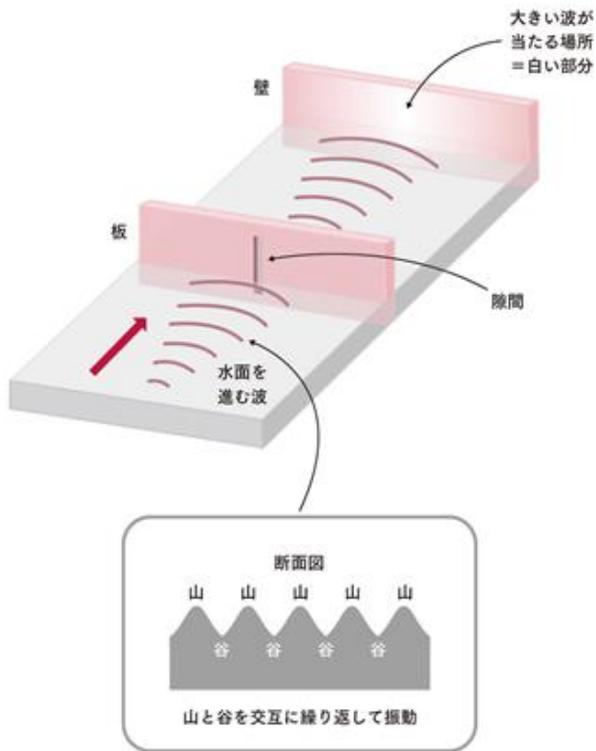


図4 水面を進む波が2つの隙間を通り抜けた場合

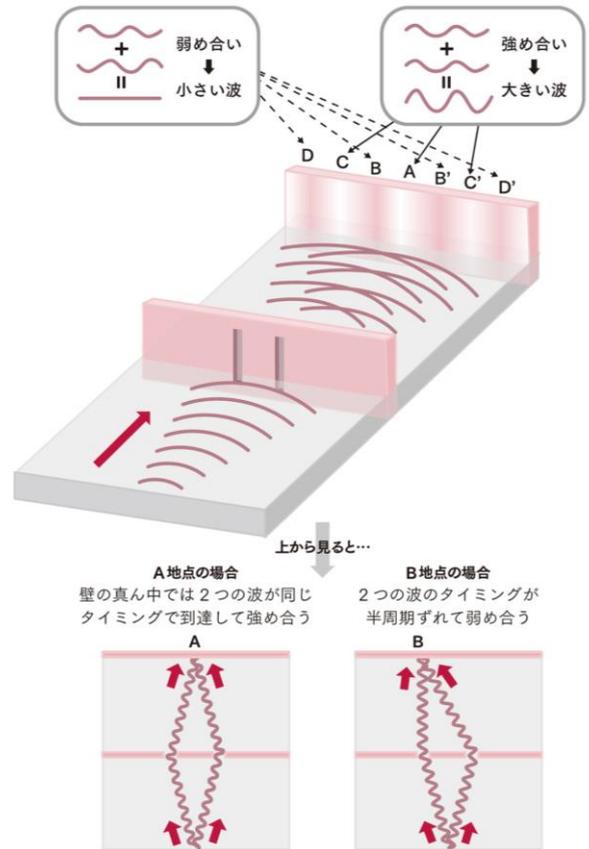


図5 電子で同じ実験をするとどうなるか？

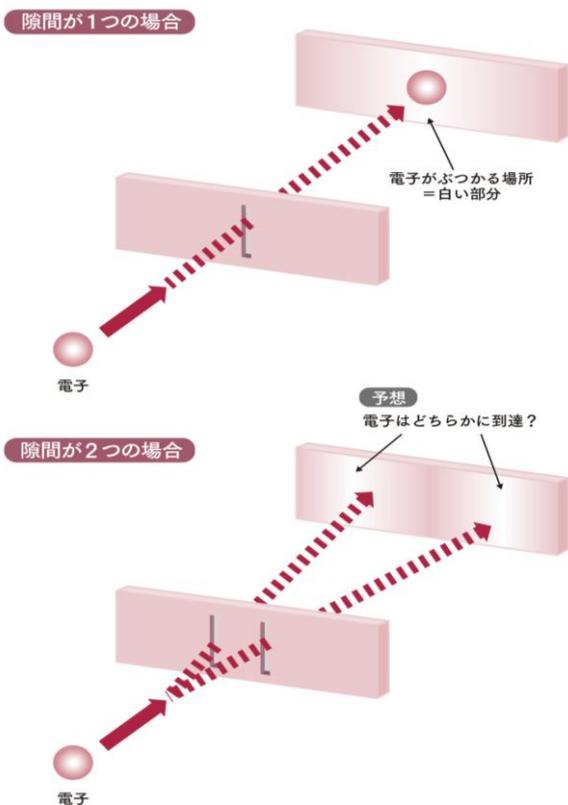
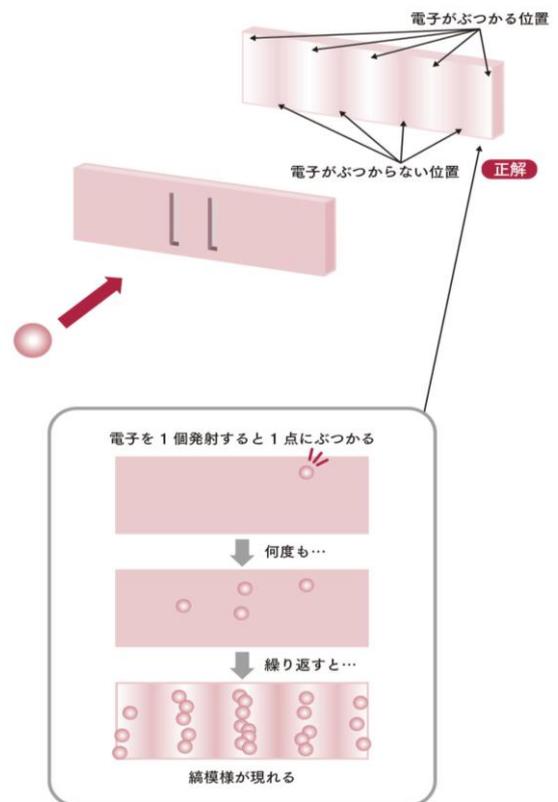


図6 電子で2重スリット実験を行った場合の実際の結果





## ～量子コンピューター～

この現象をどう説明できるか？1つの電子が2つに分裂したものでないとすると、  
「電子は左を通った可能性と、右の隙間を通った可能性があり、どちらの可能性にも確定できずに、両方の可能性を『重ね合わせた』状態になっている。2つの波を重ねると干渉が起きるよう、1個の電子の中で2つの可能性が重ね合わさることで干渉が起こる」  
つまり、電子はどちらの隙間を通過したかの2者択一ではなく「重ね合わせ」という状態になって両方の隙間を同時に通り抜けたと考えられる。

図7 2重スリット実験の縞模様は「重ね合わせ」によって起こる

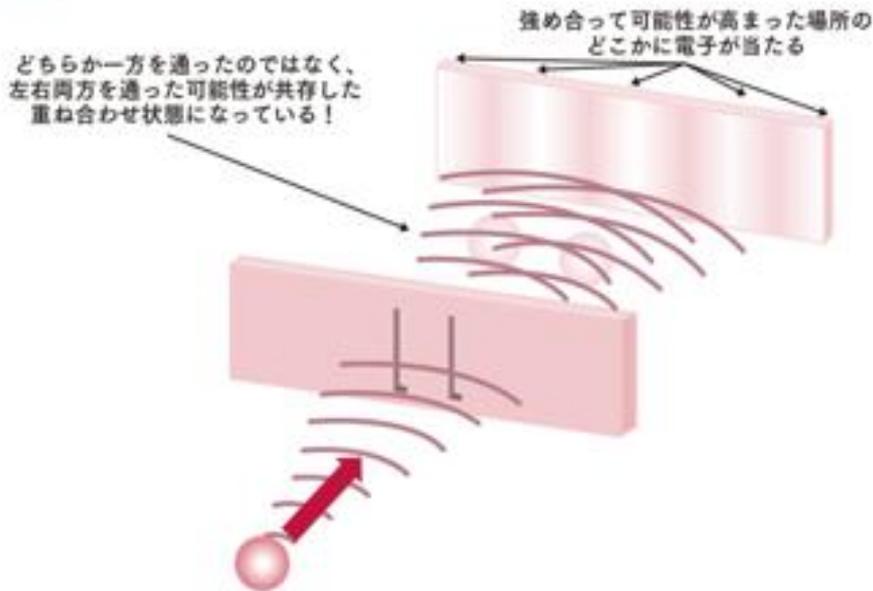


図7  
干渉による縞模様を具体的に説明するには、電子は「粒でもあり、波でもある」と考える。  
1個の電子が波のように広がり異なる複数の場所に存在する可能性を持ちながら進む。これが「重ね合わせ」という状態。電子が波のように進み隙間を同時に通って干渉を起こす。しかし、電子の波を壁に充てて、電子がどこにあるかを調べようとした瞬間に、電子はまた1個の粒となって1か所に現れる。

このような量子の振る舞いは、日常的な感覚とかけ離れている。なぜそうなっているのかは解明されていない。世界がそのようにできているとしか言いようがない。  
そして、電子が壁に当たって1か所に存在する粒として表れる瞬間に、重ね合わせた複数の場所のどの場所に電子が現れるかは確率的に決まる。1回1回の電子の当たる位置を確実に予測することは、原理的に不可能なのである。あのアインシュタインもそんな偶然などないと反論をしていたが、その後の研究により、現実の量子の世界はやはり「確率的」であることが明らかになっている。



## ～量子コンピューター～

電子の重ね合わせという現象についてみてきたが、この重ね合わせにもいろいろある。重ね合わせの具合が変われば、壁にできる縞模様のパターンも変わるのである。

この重ね合わせの具合を決定する要素としては、2つの波の「**大きさの比**」と「**振動のタイミングのずれ**」がある。

### 図9

電子をちょうど真ん中から発射すると、2つの隙間を通り抜けた電子の波は同じ大きさになる。この場合、壁に当たる直前までは、2つの可能性が50%ずつの割合で重ね合わさって、壁のどちらに当たるかも50%の確率になる。

### 図10

しかし、それが少し偏っていたらどうなるであろう。図のように左の隙間を通り抜けた波よりも、右の隙間を通り抜けた波の方が大きくなる。

このように、波の大きさの比は、複数の可能性を重ね合わせる割合を決める要素である。この割合が変われば、壁にできる縞模様の濃淡が変わる。これは、2つの波が出会った時の強め合いや弱め合いの具合が波の大きさの比によって変わるからである。⇒この変化を「**干渉**」という

量子コンピューターは、このような「**重ね合わせ**」や「**干渉**」をうまく利用して問題を解き明かす。前に見たように鍵の暗証番号がわからないような場合でも、量子コンピューターは古典コンピューターのように一つ一つ試していくのではなく、「**重ね合わせ**」を使って4パターン（4桁の暗証番号の場合）の番号をすべて重ね合わせて同時に試してみることができる。試した後は、鍵が開かない3パターンと、鍵が開く1パターンの可能性が全て重ね合わさっている。最後に、**うまくいきそうな4パターンを「干渉」させて、鍵が開いたパターンだけを見つけ出す。**

### 図11

上記の様子を示したのが図11である。4個の隙間を使った4重スリット実験を考えてみる。4個の隙間にはどれか1つ「**当り**」があり、その隙間にだけ電子の進むタイミングを少し遅らせるような仕掛けがしてあるとする。これまでのコンピューターでは電子1回1回発射して壁に当たるタイミングを見て、どれが「**当り**」かを見分ける。

### 図12

しかし、量子コンピューターでは、たった1回の発射で4個の隙間の様子を同時に調べることができる。



## ～量子コンピューター～

図9 電子を真ん中から発射した場合の重ね合わせ具合

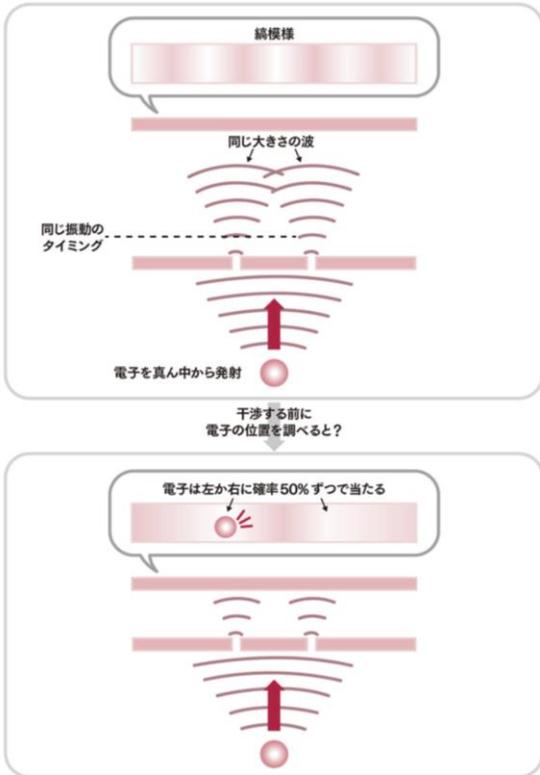


図10 電子を右に偏った位置から発射した場合の重ね合わせ具合

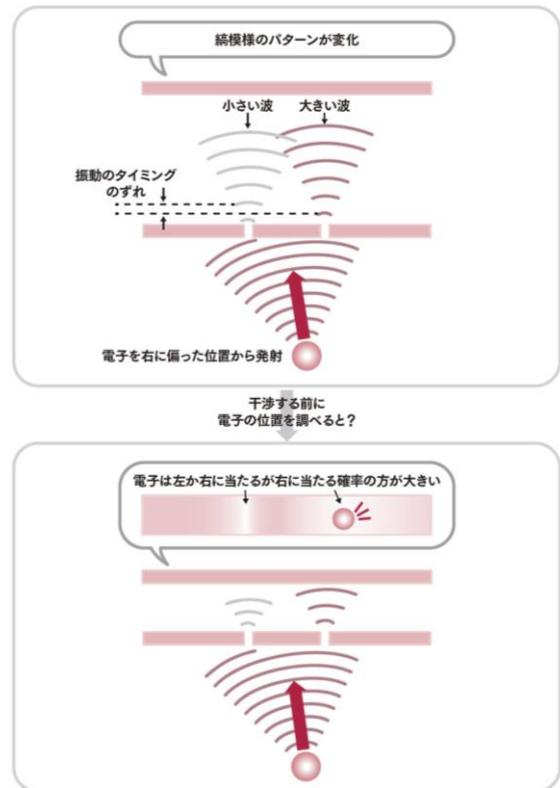


図11 4重スリット実験でしらみつぶしに「当たり」の隙間を探す方法

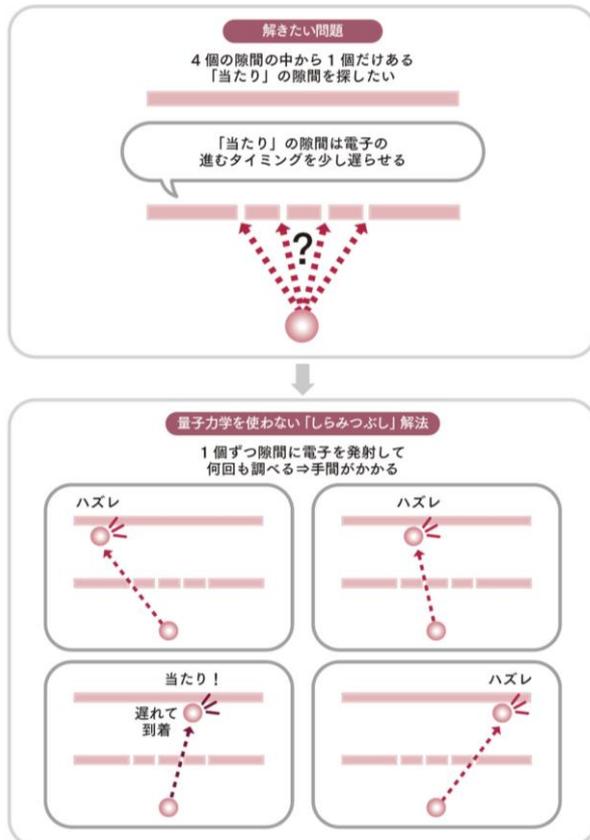
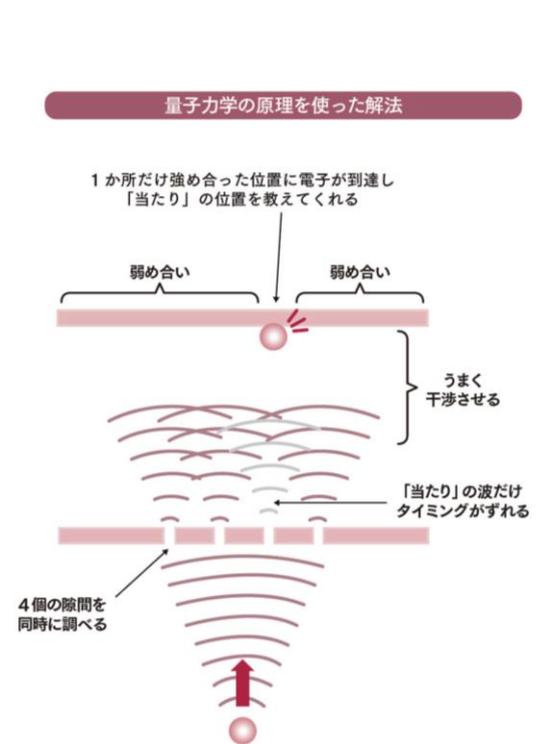


図12 4重スリット実験で量子力学の原理を使って「当たり」の隙間を探す方法





## ～量子コンピューター～

このように量子コンピュータが計算を早く行う仕組みは、この多重スリットの実験と同じである。1つずつ計算を行う代わりに、何通りもの計算を重ね合わせて同時に行った後に、干渉によって「当り」に相当する計算パターンだけを探し当てるといったもの。量子コンピュータはこのような量子力学特有の現象を使って、全く新しい問題の解き方ができる。

このようにみても量子力学はわかったような、わからないような・・・日常の現象とは違った現象が現れる世界だ。著書の中でもサッカーボールを使ってもこのような現象は絶対に現れないとしている。なぜでしょうか？この問いに対する正確な答えはまだよくわかっていないとのことだ。しかしその有望な理由の一つとして、「それは、重ね合わせや干渉を起こす波の性質が、周囲からの影響によって壊れてしまうことです。波の性質が壊れると、ある1点に存在する粒としての性質だけが残って、重ね合わせは消えてしまうのです。さらに、多数の粒からなる大きな物質ほど、波の性質は壊れやすくなります。この結果、日常的なスケールの世界では重ね合わせや干渉が起こらない、というわけです」

と説明している。どうも量子のようなミクロの世界では我々が通常目にするものと違う世界の現象が起こっている、と考えるしかないようである（もちろん専門家はそれを見つけ出そうと日夜研究しているのであるが・・・）

（実際にどれくらいの大きな物質まで重ね合わせや干渉が起こるかは重要な研究のテーマとなっている）

### 5. 量子コンピュータの仕組みのおさらい

まず現在のコンピュータの仕組みは、トランジスタという電気的なスイッチがたくさん集まって計算をしている。このスイッチによって電流をONの状態と、電流を通さないOFFの状態を作ることによって、「0」か「1」という2通りの数字を表し、スイッチをたくさんつなげてONとOFFを連鎖的に切り替えていくことで計算を行う。トランジスタは1秒間に10億回以上という超高速でONとOFFを切り替え高速で計算しているのである。

また、インターネットでは情報のやり取りをするときは、光ファイバを使って光の信号をやり取りする。光のONとOFFで「0」と「1」をあらわし光を付けたり消したりする動作を繰り返して情報を送る仕組みになっている。

この「0か1」という情報の単位を「ビット」という。コンピュータでは文章も、画像も、音楽もこの「0」か「1」に置き換えて表している。

量子コンピュータでは、「0と1の重ね合わせ」を情報の単位に用いる。この情報単位を量子ビットと呼ぶ。量子ビットの個数が増えると、たくさんの情報を重ね合わせることができるようになる。例えば、通常のビットが2個ある場合、「00」、「01」、「10」、「11」という4パターンの中のどれか1つの情報しか表せないが、量子ビットが2個ある場合は、それら4パターンの全てを重ね合わせて同時に持つことができる。量子ビットの数が増えるごとに、重ね合わせられるパターンの数が2倍になります。量子ビットがn個あれば、2のn乗パターンの全ての情報を重ね合わせて持つことができるのである。n = 10の場合は、約1000パターン重ねられることになる。少ない個数でも膨大なパターンの情報を重ね合わせて同時に持つことができるのが、量子ビットの驚くべき能力なのである。

ただ、「0と1の重ね合わせ」と言っても、「0」と「1」に対応する波の大きな比が違ったり、振動のタイミングの差が異なれば、それは異なる情報を持つ量子ビットということになる。このように量子ビットは「0」と「1」の情報が重ね合わせて同時に存在するという事実だけでなく、その2つの「重ね合わせ具合」によって情報を表現しているというのが大きな特徴となる。

量子コンピュータはこの量子ビットを重ね合わせ一定の方式（量子論理演算）で計算していく仕組みになっている。この方式の仕組みなどについてはさらに難解な話になり、ここで簡潔に説明するのは難しいためご興味ある方は、この著書「量子コンピュータが本当にわかる！」をご一読ください。



## ～量子コンピューター～

### 6. 量子コンピュータの速さに関する誤解

これまでの説明で量子コンピュータは重ね合わせによって現在のコンピュータよりも計算が2のn乗早くなるような印象があるが、それは誤解で、実際に量子コンピュータで高速化できる計算の種類は限られている。簡単な例でいうと、複数のパターンの中から最適なものを選び出す「組み合わせ最適化問題」。サラリーマンが複数の都市にいるお客様を1回ずつ訪問して元の場所に戻りたいとする。どのような順番で各都市を回るのが最短経路になるでしょう？この問題は循環セールスマン問題と呼ばれている「組み合わせ最適化問題」の1つである。都市がA,B,Cの3都市の場合、最初に訪れるパターンは3通り、2番目に訪れる都市は2通り、3番目に訪れる都市は1通り、従って、 $3 \times 2 \times 1 = 6$ 通りとなる。そのすべての距離を調べれば最適化がすぐわかる。しかし、この都市の数が増えるとパターンは爆発的に増加する。都市の数がnだとすると、経路は $n \times (n - 1) \times \dots \times 2 \times 1$ 通りとなる。N = 10だとすると、約363万通り、n = 20では約243京通り、n = 30ではその100兆倍の経路があることになる。この場合、1秒間に1京回の計算をするスーパーコンピュータでも、全てのパターンを調べるのに1億年かかることになる。

整数を素数の掛け算に分解する素因数分解も、現在のコンピュータで解くのが難しい問題とされている。これらの問題を量子コンピュータで重ね合わせの方式によりより早く計算ができる。現在のコンピュータで解く計算回数が2のn乗回で、量子コンピュータではnの2乗回だとすると、規模が増えるたびに、現代のコンピュータでは2倍ずつのペースで計算回数が増えていくが、量子コンピュータでは増え方のペースがゆっくりとなる。n = 10であれば計算回数の違いは10倍程度だが、n = 30なら100万倍までに広がることになる。これが量子コンピュータでは現代のコンピュータより格段にスピードが速いと言われるゆえんである。しかし、それが全ての計算においてではないという点から、量子コンピュータになれば全ての世界が変わるというのは誤解なのである。

現在、量子コンピュータで高速化できる計算は、大まかに分類すると60種類程度見つかっている。インターネット上の“Quantum Algorithm Zoo”（量子アルゴリズム動物園）というホームページにまとめられている。

### 7. 量子コンピュータの得意問題

量子コンピュータを使うと高速化する計算方法の代表例が、「クローバーの解法」と「ミクロな化学の計算」である

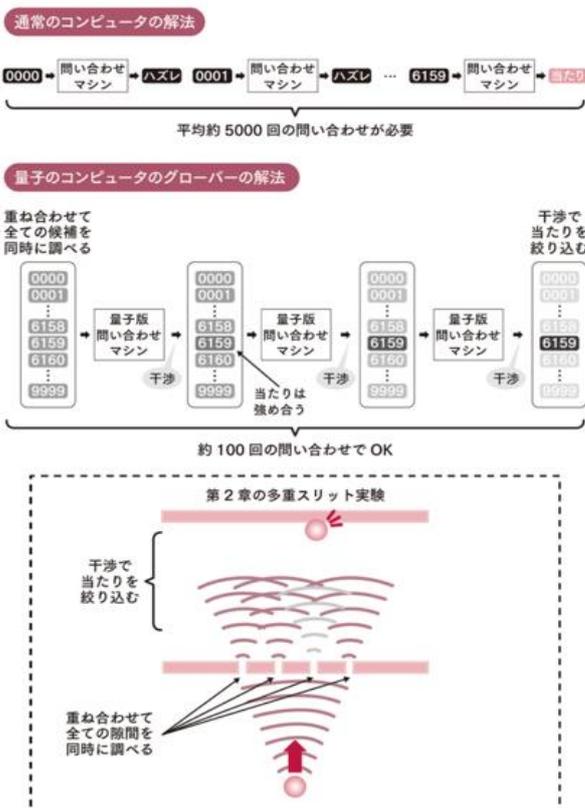
「クローバーの解法」とは、「複数のある候補の中から、ある条件を満たすものだけを効率よく探し出す」というもので、発案者の名前を付けて「クローバーの解法」と呼ばれている。

例えば4桁の暗証番号の1つを当てる場合、数字の候補は「0000」から「9999」まで1万通りある。当てずっぽに入れて当たるまで平均すると5000回の問い合わせが必要になる。

一般的には、数字がN通りあれば、平均問い合わせ回数は約 $N / 2$ となる。4桁の暗証では、 $\sqrt{N} = 100$ 回となる。通常やり方では5000回の問い合わせが必要だったので約50分の1の手間で正解がみつけれられる。

量子力学の実験「多重スリット実験」でみたように、「複数の隙間の中に1個だけある当たりの隙間を見つける」原理で、クローバーの解法でも「0000」から「9999」までの答えの候補を全て重ね合わせて同時に調べ、その後うまく干渉させることで望んだ答えだけを浮かび上がらせるというテクニックで計算を高速化しているのである。

図3 通常のコンピュータの解法とグローバーの解法の比較





## ～量子コンピューター～

「**マイクロな化学の計算**」とは、

物質中の電子の振る舞いを正確に計算するもの。物質の持つ多くの性質は、物質中の電子が決めているので、物質中の電子の振る舞いがわかれば、その物質の色や形から、化学反応の起こり方まで予測することができるのである。これができるれば、例えばソーラーパネルや電池の優れた材料やよく効く薬の開発など、世の中に役立つ新しい物質を発見するのに役立つのである。

電子は量子力学にしたがっているので、電子の振る舞いを解き明かすには量子力学のルールに基づいて計算する必要がある。量子コンピュータの開発はこの発想から生まれたものである。

量子コンピュータを使って、電子の軌道への入り方や、そのときのエネルギーが計算できると、その分子の性質がよくわかる。分子の性質とは、例えばその分子がどのような形をしているか、別の原子や分子とぶつかったときにどのような化学反応を起こすのか、光を当てるとどのような応答を示すかといったこと。計算によって分子の性質がわかるようになれば、新しい機能を持った分子や材料を設計することができる。例えば、**病気の原因となる分子とぶつかるとその働きを抑えてくれるような薬の分子を見つけられる可能性もある。電気自動車に乗せられるような軽くて高性能な電池など、世の中をもっと便利にする素材が設計できるかもしれない。**さらには、太陽の光を効率良く吸収してエネルギーに変えるソーラーパネル用の材料を開発して、地球のエネルギー問題を解決できるかもしれない。

量子コンピュータを使って化学の計算が効率よくできれば、世の中に大きな変化をもたらす可能性がある。この種の化学の計算は量子コンピュータの最も重要な応用分野の1つである。

図9 量子コンピュータが得意な問題の具体例

### <その他の分野>

前述のように素因数分解の量子コンピュータの得意分野である。

1994年にシエアが考案した解法である。

15 = 3×5のように整数を素数の掛け算に分解する計算だが、数字の桁数が増えると劇的に難しくなる。現代のスーパーコンピュータでも数百桁の数の素因数分解は現実的な時間では解けない。

量子コンピュータでは原理的にはかなり高速化できるとされている。

しかし、もし量子コンピュータで素因数分解が高速に溶けてしまうと、現在のインターネットでの安全な通信を可能にしているRSA暗号が簡単に破られてしまうのである。

(この点については次回のレポートで)

量子コンピュータではこのほか、連立一次方程式を解く計算を高速化できることもわかっている。

連立一次方程式を解く計算は、実はあらゆる科学技術の土台となっている。コンピュータシミュレーションやロボットの制御、機械学習やデータ分析、画像処理など、ありとあらゆる分野で大規模な連立一次方程式を解くことが要求されている。

	例 1：グローバーの解法	例 2：マイクロな化学計算の解法
問題のイメージ		
計算高速化のポイント	重ね合わせて並列処理 + 干渉で絞り込み	量子コンピュータは電子が従う量子力学のルールを自然に表現できる
応用分野の例	データベース検索・組合せ最適化問題	機能性材料や薬の開発

	例 3：ショアの解法	例 4：連立一次方程式の解法
問題のイメージ		$\begin{cases} 3x + 2y - z = 2 \\ -x + y + 2z = 6 \\ 2x - 4y - 3z = -5 \end{cases}$ $(x, y, z) = (? , ? , ?)$
計算高速化のポイント	重ね合わせと干渉を使った量子フーリエ変換で周期を高速に見つける	数の足し引きを波の足し引きに置き換えて計算させる
応用分野の例	暗号解読	シミュレーション・制御・機械学習・データ分析・画像処理

量子コンピュータは、このように化学・科学技術分野で革新的な開発ができる可能性を持っているのである。

仕組みについて少しでもご理解いただけたらどうか。正直私自身なんとなく分かった程度である。

量子コンピュータは世界で開発競争が起こっている。本当の量子コンピュータまではまだまだ研究が必要ではあるが、各国とも安全保障の面からもいち早く開発を完成させるべく予算化して動いているのである。

次回レポートでは、その開発状況と先ほど出てきたインターネットの暗号の危機についてまとめてみたい。