未来のコンピュータと言われる量子コンピュータ。
量子力学の原理を動作原理とし、従来の不可能を可能にするテクノロジーです。
現在のコンピュータでは宇宙の年齢ほどの長い時間がかかってしまう計算でも、
極めて短時間で解いてしまいます。
しかしその実現には、コンピュータ上で効率よく機能する量子アルゴリズムが不可欠です。
最先端技術のロジックを研究する外山政文先生に、お話を伺いました。

コンピュータサイエンス学科
外山　政文 教授

量子コンピュータの頭脳 ——量子アルゴリズム

2つの状態が重なりあった量子ビット

私たちが普段使う従来型のコンピュータ（量子コンピュータに対して「古典コンピュータ」と呼びます）では、全ての情報は0と1の組み合わせで表現されます。これを「ビット（bit）」と呼びます。古典コンピュータの中では、このビット列を変換し異なる状態にすることを繰り返して計算を行っています。

ドイチ（David Deutsch、1953-）という物理学者が考案した量子コンピュータも、同じような $|0\rangle$、$|1\rangle$という「量子ビット」を操作する機械ですが、この $|0\rangle$、$|1\rangle$は数学的な0と1を意味するのではなく、いわゆる“量子”の“状態”を表しています。この“量子状態”という概念に量子力学の不思議が凝縮しているのですが、量子状態としての量子ビットは上記の古典ビットとは違い、0か1かだけではなく、その“中間的”な状態も取ることができます。

中間というと0.5などの値を思い浮かべるかも知れませんが、そうではありません。0の状態 $|0\rangle$ と1の状態 $|1\rangle$ の両方を、同時にとることができるのです。この私たちの日常経験の常識に反した量子ビットの奇妙な性質は、量子コンピュータが量子力学の原理に基づいているためです。

量子力学は、ミクロの世界での物質の振る舞いを明らかにする力学で、直観とは全く異なる世界像を受け入れることを私たちに強います。だからこそ、量子コンピュータは従来のコンピュータとは全く異なるコンピュータになるのです。

1つの量子ビットは、上記のように $|0\rangle$と $|1\rangle$ がある確率で重なり合った状態をとります。この重ね合わせ状態は誰も見ていない時は保たれますが、その状態を観測すると、例えば50%の確率で $|0\rangle$に、50%の確率で $|1\rangle$になります。量子力学では、これを測定による状態の収縮と言いますが、実は、これが量子計算にとって重要な要素になります。

ただの箱に命を吹き込む量子アルゴリズム

古典ビットは、例えば、3つ並べた<000>や<010>といった個々の情報を個別にしか扱えません。しかし、量子ビットでは、$|000\rangle$から $|111\rangle$まで、8つの全ての状態を同時に扱えるのです。40個量子ビットを並べれば、扱える状態は1兆にもなります。この1兆個の状態に対してある処理を行うと1兆個の重ね合わさった全ての状態に対して並列的にその処理が行われます。

しかし先に述べたように、1兆個の状態に同時に処理が行えたとしても、一度測定すれば、その中のどれか1つの状態が確率的に選択されてしまいます。そこで最終的には、欲しい答が選択される確率を高めることが必要になります。この測定という処理に至るまでにいかにして重ね合わせ状態を効率よく処理（制御）するかを考えるのが量子アルゴリズムの研究です。私たちの使っているパソコンで計算処理をする場合でも、目的に対して最適な処理のルール、すなわちアルゴリズムを与える必要があります。量子コンピュータのハードウェアだけが実現されても、実際には量子ビットをどのように操作して目的の状態に持っていくかというアルゴリズムなしにはほとんど意味のある計算が行えません。

実用性があると言われる量子アルゴリズムは、現在わずか2種類だけです。一つは、大きな桁数の素因数分解に威力を発揮するショアのアルゴリズムです。そしてもう一つが、私が最近その改良を目的として手がけたグローバーのアルゴリズムです

グローバーのアルゴリズムの欠点を克服

グローバーのアルゴリズムは、量子探索アルゴリズムとも呼ばれ、大量のデータの中から、ある条件に合致するデータを見つけるためのアルゴリズムです。N個の状態に対し、古典コンピュータが平均 $\frac{N}{2}$ 回の探索を行わなければいけないのに比べて、$\sqrt{N}$回程度の探索回数で求めるデータを見つけることができます。従って、データ数が増えれば増えるほど、威力を発揮するのです。

本来このアルゴリズムは「求めたい状態の数」を予め知っていないと高い効率の探索ができないのですが、私が最近発表した「多重位相整合」という方法では、その情報を一切知らなくとも上手く答えを見けることができます。

これは、「実用的な量子コンピュータができたとしたら」という仮定に基づいた、とても数学的で抽象的な分野の研究です。今はまだ理論のみに留まっていますが、やがて量子コンピュータの実用的なハードウェアが実現し、この研究が目に見える形で役立つ日がやってくることを期待しています。

量子力学の不思議と面白さ

量子力学は、ミクロの世界を扱う物理学で、20世紀初めに生まれ1930年代には一応理論的完成を得た学問分野です。しかし、その原理に関しては未だにはっきりしない問題が残されています。量子情報ではそのような量子力学の原理が情報処理や量子コンピュータのプロトコルや動作原理と直結しています。そして、量子情報の研究の進展に伴って逆に量子力学の原理的な問題が再検討されるという大変おもしろい時代を迎えています。実際、1927年に発見された不確定性原理が、今日になり小澤の不等式の発見によって書き換えられるという新しい展開を迎えています。この不確定性原理に象徴されるように、ある意味で“あいまいさ?”が最大の売り物であった自然科学としての量子力学が、今や確定的な結果に導く情報処理科学へと変貌しつつあります。

量子力学が記述するミクロの世界では、私たちが見慣れたマクロな世界の常識が通じません。ミクロの粒子の挙動は確率的にしか予測ができないし、測定して初めてミクロの粒子の状態が確定します。例えば、電子はスピン $\frac{1}{2}$ を持っていると言います。これを古典的な自転というイメージで捉えるのは間違いで、量子力学でしか記述できません。この電子のスピンの基本的な状態は2つで、しばしば、上向きスピン状態・下向きスピン状態などと呼ばれます。電子はこの二つの状態が同時に存在する“重ね合わせ状態”をとることができ、これが量子コンピュータの基本原理となっています。