

# 動かしながら始める 量子コンピュータ

第1回 量子用ライブラリを試す

束野 仁政

## ● 連載のねらい

最近、ニュースなどで扱われることが増えてきた量子コンピュータですが、どのような原理で動作し、どのような問題を解決し、どのように扱えるのかを本稿で紹介いたします。

筆者は、プログラマの立場から量子コンピュータについて調べ、将来訪れるであろうIT業界の変化に思いをはせています。ただ、ブームになりつつある量子コンピュータですが、プログラマ向けに入門となる文章はまだ少ないのが現実です。

本連載では、できるだけプログラマに分かりやすく紹介するよう心がけました。しかし、数学の知識が必要となるケースもあるので、忘れてしまった方はこれを機に確率や行列について復習していただければと思います。

## ● とりあげる内容

第1回では、量子コンピュータの強みや基本演算について説明した後、量子コンピュータのプログラミングの準備を行います。プログラミングにはQiskitを使います。これは、Python上で動作するため、事前にPythonをインストールする必要があります注1。

第2回と第3回では量子コンピュータで使われているアルゴリズムについて、プログラミングによるシミュレーションを交えながら紹介します。第2回では「ドイッチェ-ジョサのアルゴリズム」、第3回では「量子誤り訂正」という量子アルゴリズムを紹介します。

注1: インストールについては、Python.jp 環境構築ガイド:  
<https://www.python.jp/install/install.html>を参考にしてください。

## 量子コンピュータが期待される理由

量子コンピュータは、さまざまな分野の問題解決が期待されています。そのうちの幾つかを紹介します。

### ● 暗号解読の高速化

RSA暗号、楕円曲線暗号といった、主要な公開鍵暗号を高速に解読できます。公開鍵暗号はインターネット通信の暗号に利用されているため、暗号を解読できる大きさの量子コンピュータが実現するまでに、別方式の暗号に移行する必要があります。

### ● 創薬や材料開発の高速化

分子が時間的に構造変化する様子を高速にシミュレーションできます。これにより、創薬や材料開発の高速化が期待されています。

### ● 行列計算やクラスタリングの高速化

ある種の行列計算を高速に行えます。これにより、サポート・ベクタ・マシンやクラスタリングといった機械学習を高速に行えます。

## 古典コンピュータとのちがい

### ● 古典コンピュータは1ビットの情報枠に0か1の片方しか持てない

まずは、古典コンピュータの原理について解説します。古典コンピュータが持つ情報は、古典ビット(bit)という単位で表されます。1ビットは0または1のどちらか一方を表現できます。この古典ビットを複数使用し、大きな情報を表現できます。

例えば、3個の古典ビットを使用すれば、8種類の値を表現できます(表1)。各古典ビットは2種類の情