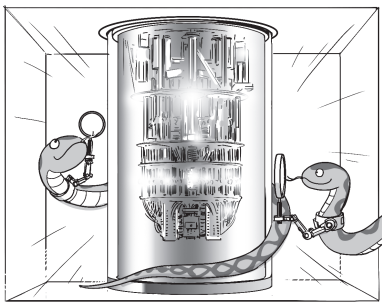
ちょこっと未来

動かす 量子コンピュータ

第1回　古典ビットと量子ビット…計算ルールの違い

束野 仁政



近年，量子コンピュータの研究開発が活発になり，関連するニュースも増えています．クラウド・サービスとして量子コンピュータが公開されるようになり，なかには無料で利用できるものもあります．一方で，過度な期待からか，量子コンピュータに対する誤解も多いように感じます．この連載では，量子コンピュータとはどんなものなのか，何に使えるのかをプログラマの視点から解説していきます．

今回は量子コンピュータの特徴的な基本計算ルールである重ね合わせ状態について解説します．使用する言語はPython，開発環境はGoogle Colaboratoryを想定しています．詳しくは本誌サポート・ページ（https://interface.cqpub.co.jp/ail01/）をご覧ください．

量子コンピュータってどんなもの？

● ざっくり４つの特徴

量子コンピュータは量子力学の原理に従って計算するコンピュータであり，既存のコンピュータにはない，次の特徴があります．

① 情報の単位は量子力学の性質を持つ量子ビット
② 2つ以上の状態を重ね合わせ状態として同時に表現可能
③ 2つ以上の量子ビットが相関関係となるもつれ状態を構成可能
④ 量子力学に従った計算（巨大なユニタリ行列の掛け算）を高速に実行可能

● 情報の単位は量子ビット

量子ビットを物理的に実現するにはさまざまな方法がありますが，量子力学的な性質が現れる原子や電子，光子などのミクロな粒子を利用することが多いです．

● 動作は行列やベクトルで表現可能

量子コンピュータの動作は行列やベクトルを使って表せます．そのため，計算時間やメモリなどの資源を無限に使うことが可能ならば，古典コンピュータ[注1]で量子コンピュータをシミュレーションできます．古典コンピュータは，量子力学の原理に従った計算をシミュレーションできますが，高速にシミュレーションできるわけではありません．量子コンピュータをシミュレーションできるだけでは，量子コンピュータとは言えません．

● 量子コンピュータで処理すると速いアルゴリズムがある

▶代表的なもの…RSA暗号，ショア，クローバー

量子コンピュータが高速に動作するためには，量子アルゴリズムという量子コンピュータ特有のアルゴリズムが必要です．従って高速な量子アルゴリズムが発見されている計算だけ速くなります．主な量子アルゴリズムは，次のサイトで公開されています．

https://www.qmedia.jp/algorithm-zoo/

代表的な量子アルゴリズムとしては，RSA暗号，楕円曲線暗号を高速に解読できるショアのアルゴリズム，総当たり計算を高速化するグローバーのアルゴリズムなどが知られています．

▶巨大なユニタリ行列

量子コンピュータはなぜ速いのでしょうか．この質問には，さまざまな観点での回答があり得ます．プログラミングが好きな方に親しみやすいと思われる計算ルールという観点で次に説明します．

例えばGPUで機械学習やグラフィックの処理が高速になる理由として，行列計算が速いという説明があります．同じような観点から見ると，量子コンピュータは，巨大なユニタリ行列[注2]の掛け算が速いと言えます．

ここでの巨大とは，行列のサイズがビット数に対して指数関数的に大きなものです．古典コンピュータで行列計算をする場合，行列のサイズが指数関数的に大

注1：私たちが普段利用している既存のコンピュータを量子コンピュータと区別するため，古典コンピュータと呼びます．
注2：ユニタリ行列についてはこの連載中に説明する予定です．今の段階ではそんな種類の行列があるんだと頭の片隅に置いておくくらいで大丈夫です．

プログラムは本誌サポート・ページから入手できます．
https://interface.cqpub.co.jp/2303py/