2-1　量子コンピュータ・アルゴリズム8

束野 仁政

「スーパコンピュータで解くのに1万年かかる特定の問題をグーグルが量子コンピュータを使って200秒で解いた」との報道が先日ありました．大きく報道されたため，これを見て量子コンピュータに興味を持った方も多いと思います．一方で，量子コンピュータはまだ発展途上であり，私たちの生活に欠かせないレベルで利用されるには10年はかかるとも言われています．前向きに捉えると，今から学んでおけば10年後に量子コンピュータ人材として活躍できるかもしれません．

そこで今回は，量子コンピュータのアルゴリズムについて，これまでとこれからを紹介します．

これまで

● ドイッチュ-ジョサのアルゴリズム

1980年代にファインマンやドイッチュらによって，量子コンピュータの概念が提唱されました．しかし，当時は量子コンピュータを使って高速に計算できるアルゴリズムは発見されていませんでした．古典コンピュータよりも高速に問題を解ける量子コンピュータのアルゴリズムが最初に発見されたのは1990年代に入ってからでした．そのアルゴリズムはドイッチュ-ジョサのアルゴリズムと言います（**表1**の項1）．

ドイッチュ-ジョサのアルゴリズムを使うと，与えられた関数が定数関数（関数の出力が一定）かバランス関数（「$f(x)=0$になるxの個数」と「$f(x)=1$になるxの個数」が等しい関数）かを1回関数を実行するだけで判定できます．詳しくは文献(1)を参照してください．

● ショアのアルゴリズム

ドイッチュ-ジョサのアルゴリズムは，現実の問題というよりも，人工的な問題を解決するものでした．現実の問題を解決するアルゴリズムが登場したのは1994年，ショアのアルゴリズムでした（**表1**の項2）．大きな数の因数分解は古典コンピュータにとって難しい問題ですが，ショアのアルゴリズムを利用すれば，理論的には高速で因数分解できます．また，ショアのアルゴリズムを応用すれば，RSA暗号や楕円曲線公開鍵暗号を（理論的には）高速に解読できることが分かりました．

楕円曲線公開鍵暗号はインターネット通信で使われているためインパクトは大きく，量子コンピュータが注目されるきっかけになりました．ただし，現在の量子コンピュータはノイズが多いため，インターネット通信で利用している楕円曲線公開鍵暗号を解読可能な量子コンピュータの登場には10年以上かかるでしょう．

その後，量子コンピュータのアルゴリズム研究は進み，幾つものアルゴリズムが発見されました（**表1**の項3や4）(4)．

これから

● 誤り訂正

量子コンピュータに限らず，実世界にはノイズがつきものです．例えば，CDが少し傷ついただけで読み取れなくなったり，QRコードが少し汚れていただけで読み取れなくなったりしたのでは，実世界では利用できません．

ノイズがあっても正しく計算するために，誤り訂正と呼ばれる技術があります．これによって多少の傷や汚れがあっても，CDやQRコードを読み取れます．この誤り訂正の概念を量子コンピュータで実現したものが量子誤り訂正です（**表1**の項5）．詳しくは文献(2)を参照してください．

誤り訂正を行うには，計算に利用したい量子ビット以外に，誤り訂正用の量子ビットが必要です．そのため現在実現している数十量子ビットの量子コンピュータではほとんど誤り訂正できず，ノイズが多い計算となってしまいます．長期的にはハードウェア技術の向上でノイズを減らしたり，大量の量子ビットを実現して現実的な計算ができるようにする必要があります．