



特集
量子コンピュータと量子計算

編集にあたって

河野 泰人 [NTT コミュニケーション科学基礎研究所] kawano@theory.brl.ntt.co.jp

白木 善尚 [湘南工科大学] shiraki@info.shonan-it.ac.jp

インターネットの爆発的な普及に伴い、近年、コンピュータへの期待は高まり続けている。コンピュータの処理能力を測るために、重要で分かりやすい尺度が計算速度である。高速コンピュータのランク付けは半年に一度行われており、その注目度は非常に高い。2006年6月時点での世界最速のコンピュータは、IBMのBlue Gene/Lである。高速コンピュータの開発はその国の技術水準を示す最も重要な指標の1つであり、開発競争は国家の威信をかけた戦いでもある。

コンピュータの高速化競争の影で、ひそかに進んでいる戦いがある。量子コンピュータをめぐる競争である。量子コンピュータでは、光子や電子スピンなどの量子状態を用いて情報が表現される。量子状態を使うと、0と1のデジタル情報だけでなく、それらの重ね合わせ状態の表現が可能になる。この重ね合わせ状態は、量子ビットと呼ばれ、量子コンピュータにおける情報表現の単位である。量子コンピュータの性能は、演算に用いる量子ビットの数に大きく依存する。量子ビットの数が百を超える量子コンピュータがハードウェアで実現できると、従来のコンピュータでは解けなかった問題の一部が、短時間で解けるようになると予想されている。残念ながら、現時点で最大の量子コンピュータの量子ビット数は、一桁でしかない。量子ビットの数が百を超える量子コンピュータの開発には、まだ何十年もかかるといわれている。しかし、従来型コンピュータの速度性能の限界が見えはじめる中、量子コンピュータのハードウェア開発は、世界の主要研究機関の大きな目標の1つになっている。

量子コンピュータのハードウェア開発と並んで、アルゴリズム開発も重要である。量子コンピュータの能力を引き出すためには専用のアルゴリズムが必要不可欠となる。従来のアルゴリズムをそのまま転用しても、量子コンピュータの計算は速くならない。量子コンピュータの情報処理能力を引き出すための鍵を握るのは、量子アルゴリズムである。しかし、その研究の歴史は浅く発展途上にある。

本会誌における過去の量子コンピュータの記事を概観しよう。西野哲朗氏による《解説》『量子コンピュータ』(1995年4月号)、竹内繁樹氏による《情報処理最前線》『「量子計算機」の現状と今後』(1999年12月号)、今井浩氏、松本啓史氏、富田章久氏らによる《解説》『量子情報処理による新ムーアの法則—量子ビット並列による高速化—』(2002年11月号)。また、量子コンピュータと暗号の関係に関しては、小柴健史氏による《解説》『量子コンピュータは公開鍵暗号にとって脅威なのか?』(2006年2月号)などがある。

本特集では、量子コンピュータをめぐる最前線の技術について、系統的に分かりやすく解説することを試みる。はじめに、1.と2.で量子コンピュータの計算原理と最近の研究展開に関して、ハードウェアも含めて概説する。次に、3.と4.では、量子アルゴリズムの中で最も有名な、Shorの因数分解アルゴリズムとGroverの検索アルゴリズムについて、最新の研究動向を交えながら解説する。続く5.では、量子アルゴリズムの自動的な設計に関する研究の最新動向を解説する。6.は、量子コンピュータと従来のコンピュータとの協調計算がもたらす、計算能力の向上に関する解説である。最後の7.では、量子通信ネットワークで結合された量子コンピュータが協調的に計算を実行する際に必要となる、量子通信量に関する研究を解説する。

革新的な技術は地道な成果の積み重ねの上に初めて成り立つ。量子コンピュータの研究も同様に、長い基礎研究を経てようやく実りあるものになりつつある。1985年にDeutschが量子コンピュータの数学的モデルを提案してから、今年で21年経つ。この間、数多くの研究努力に支えられ、量子コンピュータの研究が少しずつ着実に進んできた。実用的な量子コンピュータが完成するまでに、何年かかるのかは誰にも分からない。しかし、人類の歴史に、新しい可能性をもたらすことは間違いのない。本特集によって、量子コンピュータの研究にささやかな貢献ができれば、と願っている。(平成18年11月9日)