

特集／量子コンピュータの進展

はじめに

西野 哲朗

現在の量子コンピュータ研究は、狭義には、D. Deutsch の 1985 年の論文で量子 Turing 機械が定式化されたところから始まったと考えられる。当初は、Deutsch 自身が、量子 Turing 機械を平行宇宙論を研究するための思考の道具と考えていたようで、コンピュータサイエンティストにはあまり知られていない研究だった。

しかしその後、研究者の交流を通じて、1993 年頃から、量子 Turing 機械は米国のコンピュータサイエンティストの知るところとなった。そして、1994 年の P. Shor の論文によって、量子 Turing 機械上では、整数の因数分解が高速に行えることが数学的に証明され、それ以来、量子 Turing 機械を物理的に実現する量子コンピュータの開発研究が注目を集めるようになった。というのは、整数の因数分解が高速に行えると、現在、広く使用されている RSA 公開鍵暗号が破られてしまうからである。

量子 Turing 機械は、そのままの形では物理的に実現することが難しいため、量子コンピュータとしてどのような実現形態があり得るかについて盛んに研究が行われた。そのような研究は、量子 Turing 機械と等価な計算モデルについて研究する形で進められた。1994 年に A. Yao が、やはり Deutsch によって考案された量子回路という計算モデルが量子 Turing 機械と等価な計算能力を持つことを証明した。この論文を契機として、量子コンピュータの実現に向けては、量子回路の実現研究が主流になっていった（本特集では、このタイプのコンピュータを量子ゲート式コンピュータ

と呼んでいる）。

2000 年頃に断熱量子計算という枠組みも提案された。これは、当初、量子アナログコンピュータの実現方式として提案されたが、その後、断熱量子計算のモデルは、量子回路と等価な計算が行えることが数学的に示された。ここで、2 つの計算モデルが等価であるとは、計算を実行する際の 2 つのモデルの計算能力と計算時間がほぼ等しいことを意味している。この断熱量子計算の枠組みで、量子コンピュータの実装を目指しているのが量子アニーリングマシンである。

ということで、現状では、量子コンピュータの実現研究というのは、量子回路を物理的に実現する研究であると言える。量子回路と等価な量子コンピュータを実現する際に、どのような実現方法が可能なのか？ どのくらい大規模なコンピュータが実現できるか？ その実現された量子コンピュータを用いてどのような問題が解けるのか？ という具体的な目標に向けての研究が、近年、活況を呈している。最近、量子アニーリングマシンが様々な企業からの注目を集め、実用化に対する期待はより高まっており、この分野の進展は今後ますます注目されるであろう。

そこで本特集では、そういった量子コンピュータ研究の現状をまとめるとともに、その進展についても展望したい。量子コンピュータの仕組み、原理、アルゴリズムなどの基礎的な解説から、実現に向けた研究の紹介や課題、将来の実用に向けての期待などを取り上げる。また、量子コンピュータと