

特集 / 量子情報と量子コンピュータ

量子情報理論のルーツ

小澤 正直

1. はじめに

ここ数年の間に量子情報と量子コンピュータの研究が素晴らしい勢いで進展した。毎年、大学が夏期休暇にはいる6月から8月にかけてヨーロッパの風光明媚な避暑地や伝統的な大学街に研究者たちが集まってくる。そこで発表される内容は一年ごとに進歩して、もはや将来の夢を語る場ではなくなりつつある。7年ほど前に量子テレポーテーションが可能であるという発表があったときは、そのネーミングになにかうさん臭いものを感じたものだったが、すでにインスブルック、ローマ、パサディナなどの研究室から、その実験に成功したという報告があいついでなされた。また、ショアが、量子コンピュータが実現すれば、現在、インターネットで利用されている暗号システムを瞬時に解読できるという結果を発表したときも、私の友人の何人かは量子コンピュータなんて実現するはずがないと力説したものだった。それが今では、巨額な研究費を獲得して、量子コンピュータ実現のプロジェクトを率いているそうだ。

これらの研究は、量子情報技術 (QIT) と呼ばれる次々世代の情報技術の展開をめざしていて、基本特許をめぐる競争も活発化している。ところで、英語ではしばしば、量子 (quantum) という言葉が、「魔法の」というような意味で使われるこ

とがある。量子情報技術としてマスコミで喧伝されているもののなかには、量子力学の草創期に思考実験として議論されていた不思議な現象が、あたかも人間のように巨視的な対象に対しても可能になるかのような内容のものもある。光子一個の状態がすでにテレポートできたからといって、そういうことがいつかは人間で実験されるようになるという話は SF のなかでしか通用しないだろう。とはいえ、20 世紀には円周率を何万桁も計算したり、月に着陸することができたが、200 桁の数を因数分解することはできなかった、ということをも 19 世紀の人々はまったく想像できなかったであろう。量子情報技術の未来を想像することは、もっと難しいに違いない。

ここでは、量子力学と情報科学という 20 世紀の 2 大科学思想がどのように合流して、量子情報理論という流れが生まれたのか、20 世紀の数理科学の流れを遡ってみよう。それによって、20 世紀の間に育ってきた新しい科学が、21 世紀に大きな飛躍を遂げるのか、世紀末の一時の流行に終わるのかを考える手がかりにできればと思う。

2. 量子情報

3 年ほど前に、米国物理学会の学会誌 Physical Review A に量子情報 (quantum information) と