Peter Shor：Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer

SIAM Journal on Computing, Vol.26, No.5, pp.1484-1509（1997）

Shor の論文は，そのアルゴリズム開発でのひらめき，理論的解析の深さと美しさだけでも名論文に値するものだが，最も重要な点は 21 世紀の直前に新しいコンピュータモデルとしての量子力学原理を情報処理に用いた量子コンピュータの研究を先導したということだ．色々な観点はあるかもしれないが，この論文が 21 世紀で量子計算と呼ばれている分野を爆発的に広め，いま少し歴史のあった量子情報をも巻き込んで量子情報処理研究の推進力になったのだ．

結果は論文タイトルの通りで，量子コンピュータなら，素因数分解問題も離散対数問題も多項式時間で高速に解ける，というものである．今のコンピュータではこの 2 つの問題とも超難問として知られており，たとえば以下に述べる RSA 暗号の関係で挑戦問題として 10 進で 174 桁の素因数分解問題が出ている．既存の 10 進 150 桁程度の素因数分解例は，大規模分散計算で多大な時間をかけてやっと解いていたのが，量子コンピュータならあっという間に解けてしまうのだ．

この論文の元は，1994 年の 35th IEEE Annual Symposium on Foundations of Computer Science（FOCS）で発表され，その時点から種々のブレークスルーをもたらした．第 1 に，量子コンピュータができてしまうと，今 21 世紀の当初にあたって e-Japan 等電子政府を企図する時代の社会基盤としての公開鍵暗号系の安全性が崩壊するということである．素因数分解の難しさに安全性の基盤を持つ RSA 暗号系もしかり，離散対数計算の難しさを用いるものもしかりで．理論の論文が，今普及してさらに広まろうとしている社会基盤に対する直接的な警鐘を鳴らしたのである．

第 2 に，物理研究者を情報処理の世界にまったく新しい土俵で引きずり込んだことである．デバイス研究者ほど Moore の経験則が近々頭打ちとなり，CMOS VLSI の高速化が限界に達することを痛感しているといい，それに対して Shor のこの成果は，「では量子コンピュータを作ろう」という世界規模での大規模プロジェクトを立ち上げる主要因となった．Shor 自身，この論文を提示したときに物理系研究者から量子状態というのは安定でなく，そんなものを精度よく制御して計算するのは無理だという批判にさらされた．それに対して Shor は，量子誤り訂正機構を提案し，量子状態に誤りがあっても正しい計算を進める原理を示し，それに後押しされて物理の研究者もどっと量子コンピュータ研究に参入したという経緯も象徴的である．

第 3 は，それまで量子力学を情報処理に使う試みとして量子通信と量子暗号が先行していたが，その時点ではまだ細々という感もあったのを，Shor のアルゴリズムが開いた量子計算ともどもで，量子情報処理パラダイムを展開させたということだ．今のコンピュータは von Neumann らによる EDVAC などを祖としているが，その開発当時である 1950 年頃は情報処理もまだ黎明期で，計算と通信も非常にまだ近い分野であった．現在の非常に多岐に渡る情報処理の広大な分野で，再び量子情報というキーワードをもとに，1950 年頃の熱気を体現できる機会を我々に与えたのである．

最後にこの論文の Introduction を情報技術者・物理研究者の方を含めぜひ読んでいただきたいというお願いをしたい．上ではインパクトの面から紹介したが，そのようなことは Introduction では数行しか触れられていない．Church，Post，Turing の計算可能性から始まり，計算の理論がいかに進展してきたかが語られている．Church の提唱，物理的実現に関する量的 Church の提唱，アナログ計算での精度の問題，量子コンピュータは量子アナログ性も使いながらディジタル計算であること，そして 1980 年頃に物理の方から Benioff，Feynman そして量子 Turing 機械を提案した Deutch によって創始された量子コンピュータへと展開している．まさしく「計算とは何か」の歴史を語っており，その最先端が量子計算に至るある種必然性まで感じさせるのだ．Shor は生粋のコンピュータ科学者で，MIT での博士論文の組合せ解析の卓越さ，計算幾何でのランダム抽出パラダイムの展開などそれ以前の大きな業績から，さらに一歩抜きん出た成果を出したのがこの論文なのである．

（平成 15 年 11 月 17 日受付）

今井　浩／東京大学情報理工学系研究科，JST ERATO 今井量子計算機構
imai@is.s.u-tokyo.ac.jp