

特集 / 量子アルゴリズムの新地平

量子計算研究の必然と展開

今 井 浩

「計算の本質を研究していくと、量子計算が必然的に研究対象になる」と聞くとどう思われるだろうか。本稿では、この必然性を解説していきながら、21 世紀に入ってから量子計算の新展開をまとめるこの特集に触れていきたい。

1. 古典計算過程を行列乗算で表現すると

「計算とは何か」を考えるのは、情報科学の本質である。計算可能であるとは何かについては、1930 年代に Turing, Church, Post らによって独立に考えられ、1 つの解決をみた（このあたりについては、量子計算におけるブレイクスルー・金字塔となっている Shor⁸⁾ の論文の“はじめに”を、今井⁵⁾ の紹介にもあるように是非読んで頂きたい）。そこでは状態の遷移というのが計算の本質として捉えられた。特に、Turing マシンは、今の時刻のコンピュータの状態によって次の時刻の状態を決める遷移関数を導入していて、この観点が顕著である。この Turing マシンの遷移関数が、 λ , 帰納関数とともに、今の計算理論の基礎となっている。

計算を状態遷移と捉える見方を、古典計算（量子計算に対する用語で、今までの計算をこう呼ぶ）でまず述べよう。プログラムでは、プログラムのどこを実行しているかも含めその時点のすべての

データの値によって、次の時点のデータの値が決まる。普通のプログラム言語なら、ある変数に代入操作がされてそのデータが更新されたり等である。入力データのサイズを n とし、そのプログラムが作業用メモリも含めて計算過程で最大にもつメモリサイズを $s(n)$ とする。 $s(n)$ は領域計算量と呼ばれる。今、話を簡単にするために各データは 0 か 1 しか値をとらないとする（普通の場合は 1 ワード 32bit で 0,1 を 32 個もっているわけだが、定数倍の範囲内なのでこれで一般性を失わない）。プログラムの長さは n には依らないので、プログラム中には定数 c 個の操作があるとしてよい。

すると、このプログラムは計算過程の時刻 t で、 $2^{s(n)}$ パタンとりうる内部データのパタンと、 c 個の操作のうちの 1 つを適用して次の時刻 $t+1$ の状態に遷移する。内部データのパタンと操作のすべての対 $c2^{s(n)}$ 個を考えて、時刻 t での状態を $c2^{s(n)}$ 次元の特徴ベクトル $\chi(t)$ で表現すると、計算は

$$\chi(t+1) = P\chi(t)$$

という遷移行列 $P = (p_{ij})$ によって表現される。 p_{ij} は内部パタンと操作の対の j 番目が適用されて次に i 番目になるときに 1 の値をとり、そうでないとき 0 である。遷移行列 P の各列は、ちょうど 1 つの 1 をもち、他の要素は 0 となっている。これは計算が確定的 (deterministic) であること