

埋もれる原石を探して

コンピュータで演算を行う場合、数値は全て0と1の数字列で表現されている。例えば4ビットの場合は、0と1の組み合わせで出来る4桁の数字のことであり、全部で16通りの数値が表現可能である。

近年この計算機理論に、物理学の量子力学の理論を応用した「量子情報理論」が盛り上がりを見せている。未だ実用化のめどは立っていないが、その理論を元に設計された「量子コンピュータ」は超並列計算を可能にし、現在問題になっている多くの計算を超高速度で処理できると言われている。この超並列計算を可能にしたのは、複数の状態を確率的に重ね合わせて同時に実現できるという量子力学の「重ね合わせの原理」である。

量子コンピュータの計算でもまずは0と1を表現できる素子を用意する。ここまでは従来のものと同じである。違うのは、この0と1が確率的に両方存在するという不思議な状態を作れるということである。例えば20%の確率で0、80%の確率で1といった具合だ。先ほどの4ビットの例をとると、16通りの数値を1状態で記述することが出来るようになる。古典コンピュータでは16通りの数値があれば、それら1つ1つに対して16回演算を行う必要があったが、量子コンピュータではそれらが1回の演算で済んでしまうのである。これが“超”並列計算と言われる所以である。

この超並列計算によって何が出来て、何が出来

なくなるのか。1994年にベル研究所のショア博士によって考案されたアルゴリズムを使えば、素因数分解を高速で処理できるようになる。これにより、「大きな整数の素因数分解は現実的に計算不能」という事実を元に作成されたRSA公開鍵暗号は瞬間に解かれてしまい、まったく意味を成さなくなる。逆にこの量子情報理論を使ってより解読の難しい暗号を作ろうという試みもあり、もし可能になれば多くの金融機関が恩恵を被れるかもしれない。

このように、ある分野の問題に対して別の分野の理論を導入することによって、新しい英知を生み出すことが出来る。先日、伊藤清京都大学名誉教授が、数学の応用で画期的な業績を挙げた数学者を表彰する「ガウス賞」の第一回受賞者に選ばれた。伊藤名誉教授が1942年に考案した確率積分という領域は、確立された当初は数学の一領域に過ぎなかった。しかしそれが1973年にロバート・マートン・ハーバード大学教授らがオプションのブラッキング理論に応用したことによって、その後金融工学の領域は爆発的に進歩したのである。

上記は過去の例だが、昨今でも心理学を応用して投資家心理を解明する「行動ファイナンス」など、異分野を金融に応用する新しい理論が少しずつ現れてきている。異分野には、まだまだ磨けば光る原石が埋もれているかもしれない。(中村智光)