量子コンピュータへの挑戦

― 量子ソロバンから量子コンピュータへ ―

北　川　勝　浩*

The Road to Quantum Computer
—From Quantum Abacus to Quantum Computer—

Key Words: Public Key Cryptography, Factorization, Quantum Computer, Nuclear Magnetic Resonance, Spin Cooling

1．情報セキュリティへの衝撃

電子化された情報の秘密を守るために現在盛んに使われている公開鍵暗号の安全性は，何百桁もある大きな整数の因数分解が事実上不可能であるということによって保障されている．整数Nを因数分解するアルゴリズムは，2から$\sqrt{N}$までの整数で片っ端から割ってみるという最も原始的な方法だと，桁数とともに指数的に多くの手間がかかり，数百桁なら何億年以上という天文学的な時間がかかってしまう．もっと賢いやり方があるのではないかと思われるかもしれないが，これまでに知られている最も効率の良いアルゴリズムでさえ，この点について大した違いはない．桁数に対して指数的に手間が増える限り，計算機の速度がこれまで通り倍々ゲームで速くなったとしても，桁数をちょいと増やせば永久に追いつかれる心配はない．

もしも，桁数とともにせいぜい多項式でしか手間が増えないような因数分解アルゴリズムが存在すれば，話はまったく別である．そのようなアルゴリズムは存在しないと証明されたわけではないが，ほとんどの専門家は存在しないと信じている．したがって，1994年にAT＆TのShorが，量子コンピュータ上で因数分解を多項式時間で行うアルゴリズムを発見した時には，世界中に大きな衝撃が走った．それにもかかわらず，今日に至るまでその暗号を安心して使っていられるのは，Shorのアルゴリズムを実行できる量子コンピュータのハードウェアが実在しないからである．

2．量子コンピュータとは何か？

量子コンピュータというのは，情報の持ち方として，通常のビットのように0か1かではなくて，0と1との重ね合わせを許したものである．これを量子ビット(qubit)と呼ぶ．nビットのレジスタは，n桁の2進数のうち任意の1つを表すことができる．これに対して，n qubitの量子レジスタは，全てのqubitを0と1との等振幅の重ね合わせにすると，n桁の2進数全てを等振幅の重ね合わせとして持つことができる．この状態に，ユニタリー演算を施すと，たった一つの数に対する演算と全く同じ手間で，2^n通りの数に対する演算を並列に行うことができる．ただし，いくら並列計算ができても，結果を読み出そうとして観測すると，1つの場合しか生き残らないので，これだけで実際に計算が速くなるわけではない．計算の効率を上げるには，量子干渉によって，正解に到達する確率振幅は強め合い，不正解の確率振幅は弱め合うように，アルゴリズムを工夫しておく必要がある．Shorが発見したのは，正にこのようなアルゴリズムだったのである．

量子コンピュータのハードウェアには，アルゴリズムが意図した通り正しく干渉が起こるように，重ね合わせの位相を保つことが要求される．これは，qubitが外界から隔離されていない限り難しい．一方，コンピュータというからには，データを入力したり，プログラムしたり，結果を出力したりと，外部とのやり取りができなければならない．また，ユ

*Masahiro KITAGAWA
1958年9月28日生
1983年大阪大学大学院・工学研究科・電子工学専攻・修士課程修了
現在，大阪大学大学院・基礎工学研究科・物理系専攻・電子光科学分野，助教授，理学博士，エレクトロニクス，量子情報科学
TEL 06－6850－6339
FAX 06－6850－6341
E-Mail kitagawa@ee.es.osaka-u.ac.jp

ニタリー演算を行うには，qubit間に量子力学的な相互作用が必要である．これらを同時に満たすだけでも非常に難しいが，さらに量子コンピュータがその驚異的な能力を発揮するには，qubitの数が多くなければならないという要請がある．例えば，現在使われている公開鍵暗号を破るには，少なくとも数千qubitの量子コンピュータが必要と考えられるが，これら全ての条件を満たす本命の物理系は残念ながらまだ見つかっていない．光，イオン，半導体や超伝導など様々な物理系で実験が行われているが，1つのqubitが制御できたり，2qubit間の演算ができたりというゲート・レベルの話である．今のところ最も実験が進んでいるのは，溶液中の小さな分子の核スピンをqubitとして用いて，核磁気共鳴(NMR)によって制御するものであるが，それでもアルゴリズム・レベルで実現しているのはたったの2～3qubitである．これは，量子コンピュータというよりは，量子ソロバンと呼ぶべきかもしれない．

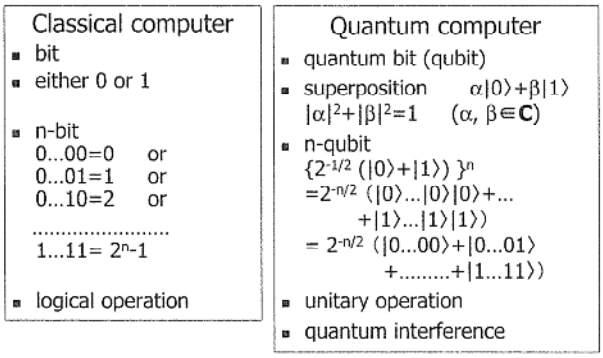

図1　通常のコンピュータと量子コンピュータ
ビットの代わりに重ね合わせを許した量子ビットを使うと，全ての可能性を同時に試すことができる．

3．もっとqubitを

私たちは，どんな物理系を使ったとしても，大規模な量子コンピュータの実現には共通する普遍的な問題がありそうだとにらんで，5～10年のタイムスケールで最も早くその領域に到達すると思われる分子の核スピンを用いた量子コンピュータの多qubit化の研究に取り組んでいる．まず，ひとつの問題は，分子を大きくして行くと，相互作用が無く直接演算できないqubitの組がどんどん増えてしまうということである．そのため，近接したqubit間の相互作用だけを使って大規模な演算を行う方法と，それに適した分子構造を研究している．この方面の研究は，たとえ将来分子でなく2次元的に配置された人工的なqubitを使うことになったとしても，必要になるだろう．

ユーザの住む巨視的な世界と微視的な量子コンピュータとのインタフェースの問題も重要である．分子一個が一台の量子コンピュータとして動作しても，NMRの場合はたった一個の核スピンでは信号が弱すぎて検出できないので，溶液中の無数の分子を使って信号強度を数で稼ぐという戦略を取らざるを得ない．ところが，熱平衡状態でたまたま同じ初期状態にある分子の数はqubitの数とともに指数的に減少するので，10qubit以上では巨視的な信号が得られなくなってしまうという深刻な問題がある．これを解決するには全ての分子の核スピンの向きを揃えてやれば良いが，単純に温度を下げると固体になってしまい，qubitの位相が乱れやすくなるという問題がある．そこで，私たちは，溶液のまま分子の核スピンだけを冷却する方法を研究している．光照射によって電子のスピンが揃う性質を持つ分子を利用して，まず冷えた電子スピンを用意する．これと核スピンをうまく結合することができれば，核スピンを冷やすことができる．温まった電子スピンは再び光照射によって冷却できるので，このプロセスは核スピンのエネルギー緩和時間内なら何度でも繰り返すことができる．つまり，電子スピンを冷媒として循環させて核スピンを冷やすのである．この方法は固体では実験的にも可能性が示されているが，液体では激しい分子運動によって電子スピンと核スピンの

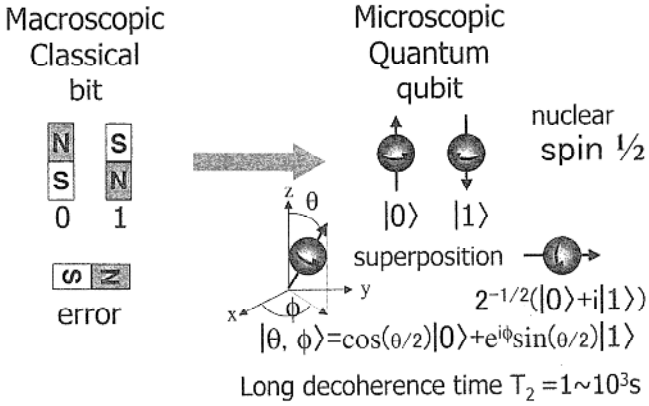

図2　通常のビットと量子ビットの違い
巨視的な磁石では重ね合わせは成り立たないが，それを極限まで微小化した核や電子のスピン1/2では重ね合わせが成り立つ．

相互作用が平均化されて消えてしまうため，何らかの工夫が必要となる．しかし，この技術が確立すれば，NMRの感度を何桁も飛躍的に向上することができるので，量子コンピュータの初期化にとどまらず，NMRを分析手段として利用している化学や生物など多くの分野に恩恵をもたらすことが期待される．これまでほぼ超伝導磁石の進歩のみによって支えられて来たNMRの感度改善もそろそろ限界に達しつつあるので，核スピンの冷却は21世紀のNMRの新たな可能性として注目されるだろう．

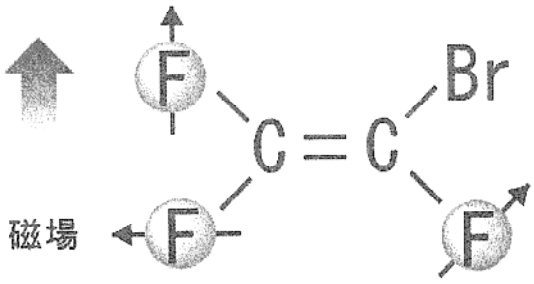

図３　量子コンピュータとしての分子
この分子は，フッ素核のスピン1/2を量子ビットとする3qubitの量子コンピュータとして使える．

４．量子コンピュータの将来

量子コンピュータは，まだ２～３qubitのものが誕生したばかりで，今後どのように発展して行くのか予測することはほとんど不可能である．それは，量子コンピュータに必要な技術が，従来の技術の延長線上にない全く新しい種類のものだからである．重ね合わせは原子や分子のようなミクロの世界では成り立つことが分かっていても，回路やコンピュータのようなマクロな世界では通常は成り立たない．もしも，私たちがいつも使っているコンピュータで，重ね合わせが成り立っていたならば，有名なシュレディンガーの猫のパラドックスと同じくらい気持ち悪い．しかし，量子コンピュータを作るとはそういうことである．方向としては２つ考えられる．１つは，マクロな世界で重ね合わせが成り立つような状況を作り出すこと．半導体や超伝導を使ったものは，どちらかと言えば，この方向を目指していると言えるだろう．もう１つは，コンピュータをミクロな世界に作ってしまうという方向で，分子を使ったものはこちらになるだろう．いずれにしても，未踏の領域であり，いくつものブレークスルーが必要となるだろう．今のところ見えるのは青い棘ばかりで，まだ花の色は分からない．