量子コンピュータ ― 計算の新しい可能性

日本数学会・日本物理学会 合同
市民講演会
２００８年3月２２日

根本香絵（国立情報学研究所）

情報処理のもつ処理能力は，1960 年代にムーアが予言したように 18 ヶ月に 2 倍ほどの速さで，実に半世紀という長い時間にわたって発展してきた．半導体技術がその黎明期にあっても，半世紀もの時間を隔て十分に成熟した現在にあっても，ほぼいつも同じ速さで前進を遂げていることに，実にあらためて驚く．しかし，速さだけでない．記憶媒体の記憶量も同じように大きくなった．こうした情報処理技術の発展は，ここ数年周辺領域にその情報処理の方法でこれまでにない大きな変化をもたらしつつある．これまで不可能であったような規模の情報処理能力で初めて可能になる新しいアプローチが生まれつつある．この情報処理の新しいステージに時を同じくして，情報技術の発展を支えてきた半導体技術に量子限界が見え始めているのは興味深い偶然である．その発展を根底から揺るがすこの限界がもたらしているのがもうひとつの新しい流れ，量子情報処理である．

量子情報処理はミクロな世界に現れる量子的な性質を有効に活用し，従来の情報処理の能力を凌駕する情報処理を実現しようというものである．量子的な性質を有効利用するためには，情報処理の方法そのものも量子性に即してそっくり変えなければならない．もちろん量子情報処理は古典情報処理を含むと考えれば，量子情報の基本単位はビットを含む量子ビットで与えられるのは自然である．量子計算とは，手短に言えば「量子性」という原理に基づいて，情報処理を行う計算方法である，しかし狭義には古典計算では効率的に模倣できないという条件がつく．時に古典計算では効率的に模倣できない量子計算のことを真の量子計算といって区別する場合がある．この場合はもちろんその量子コンピュータの処理速度に注目しているわけで，古典的には（時間がかかりすぎて）実行不可能な量子計算の可能性を意味する．しかしながら，量子情報処理の優位性は真の量子計算だけにあるのではない．まず，量子性を理解することは従来の古典計算の発展に欠かせない．技術の発展に伴ってこれから出てくる量子効果をうまく制御して情報処理を行うことで，古典的な技術の発展を支えることができるのであるし，もっと積極的な量子性の有効利用には量子鍵配送などの安全な通信があり，その先には長距離量子通信や量子高精度測定，量子イメージング技術などがある．量子鍵配送は実はすでに実用に近い量子技術である．秘密鍵を 2 人の利用者 Alice と Bob の間で安全に共有す

る方法で，理論的には安全性が保障されている．ただし，量子情報処理の基本単位である量子ビットをひとつずつ扱う量子鍵配送と他の量子情報処理には実現化の難易度に実に大きな開きがある．そこに横たわるのはエンタングルメントとスケーラビリティである．

エンタングルメントとは，いわば２つの区別できる物理系が２つでひとつの状態を呈し得る性質をいう．一種の量子的な非局所性と考えてよい．量子状態はその物理系が記述される Hilbert 空間上の状態ベクトルとして表わせる．（簡単にするためにここでは古典的な混合は考えず，量子力学的に純粋なアンサンブルで考えよう．）量子ビットで考えると，量子ビットを表現するための Hilbert 空間は，古典的なビット情報に対応する０と１を測定値とする測定量の固有ベクトルを２つの基底状態として張る空間である．したがって，２つの量子ビットがあるときには００，０１，１０，１１に対応する４つの基底ベクトル{|00>, |01>, |10>, |11>}が張る Hilbert 空間をその表現空間にとる．ここでは状態表示に Dirac のケットベクトルをとった．このとき，任意の状態はこれら基底ベクトルの線形重ね合わせであるので，(|00>+|11>)/√2 といった状態もとり得るが，この状態は２つの量子ビットのひとつずつの量子ビットについての状態の直積で表わすことができない．これがエンタングルメントである．エンタングルした状態は，系全体の状態が各々の量子ビットの状態の直積で表わすことができないことで定義され，エンタングルしているとときには，量子ビットひとつずつの状態というものが規定できず，２つの量子ビットでひとつの状態になっていることを意味する．一方エンタングルしていないときはセパラブルであると言われ，量子ビットひとつずつについての状態を規定でき，系全体の状態はその２つの状態の直積状態になっている場合である．これは量子ビットが量子ディットと高次元になっても，たくさんの量子ビットを扱う場合でも基本的に同じである．

先ほどの(|00>+|11>)/√2 という状態は最大にエンタングルした状態でこれ以上はエンタングルできないという状態にある．どの程度エンタングルしているかを表わすのに，さまざまなエンタングルメント測度が考えられてきた．純粋状態にある２体間のエンタングルメントでは，エンタングルメントの程度は尺度によらず，最大にエンタングルしている状態からエンタングルしていないセパラブルな状態まで順序づけることができる．特に 2 量子ビットのエンタングルメントではこれらの量はよく調べられていて，エンタングルメント測度の間の関係はよく知られている．しかし，古典的な混合を含む混合状態も扱おうとすると，パラメータの数が一気に増えその関係は複雑化する．また，たくさんの量子ビットを扱う場合には，全く事情が違う．非常に多くの種類のエンタングルメントがあることがわかっており，最大にエンタングルした状態を一意に定義する意味

がなくなるし，2 量子ビットでは有効であったエンタングルメント測度や基準がうまく適応できない場合が出てくる．また 2 量子ビットの場合にはなかった束縛エンタングルメントという取り出すことのできないエンタングルメントも出現する．このようなエンタングルメントを始めとした量子非局在性は，量子性の理解にとどまらず，量子統計物理への応用や量子通信プロトコルなどの開発に大変重要な位置を占め，活発な研究が行われている．

本題にもどって，このエンタングルメントがなぜ量子情報処理の発展の鍵になっているのかを考えよう．古典的なビットと量子ビットの違いはその状態のとり得る空間の広さにある．古典的なビットは量子状態が基底状態しかとれない場合に相当するのに対して，量子ビットでは状態が連続的に Hilbert 空間上を自由に移動できる．この自由度を最大限に利用するには，エンタングルメントが必要である．もちろん，エンタングルメントした状態が点在しているように制限された空間上では，量子計算は真の量子計算を達成できないことがわかっているので，エンタングルメントがあれば十分というわけではない．むしろ必要な条件と考えられる．ところで，量子計算の優位性がどこから来ているのかというのはそれほど自明でない．もちろん，Hilbert 空間の自由度だといってしまえば一網打尽的だが，それで，実際に何が必要十分な量子性であるのかというとそれほどははっきりしていないのだ．その尺度として，ひとつには量子計算のユニバーサリティがある．実行可能なゲートの集合を考えて，それが任意の精度で任意の時間発展を構成できるときに，そのゲートセットはユニバーサリティを満たすという．ゲートセットが直接的にユニバーサルなゲートセットでなくても，任意の時間発展を模倣できれば計算のユニバーサリティを回復できる．例えば，1 量子ビット回転だけのゲートセットはユニバーサリティを満たさないし，エンタングルメントを生成しても，とり得る状態が Hilbert 空間上で点在しているようなゲートセットの場合ではユニバーサリティを満たさず，つまり真の量子計算を達成できず，効率的に古典計算機上で模倣可能であることがわかっている．しかし，ユニバーサリティを満たさず，効率的に古典的に模倣可能でないクラスの量子計算はあるのかなど，優位性の本質に迫るにはもう一歩というところである．

このように多くの量子情報処理に必要条件となるエンタングルメントであるが，これを生成させたり，つまりエンタングルメントの量を変えたりするには，量子ビット間の相互作用が必要である．ここに実現化が難しい理由がある．もちろん自然界には放っておいても相互作用したがる量子ビットもたくさんある．しかし，量子情報処理をするには，私たちが思うように，決められた量子ビットとのみ相互作用させる必要があるわけであるが，その制御は難しく，量子ビットは勝手に違う量子ビットや環境とも相互作用

しがちであるから，量子コヒーレンス（量子的な性質を保つこと）の維持が難しい．一方量子鍵配送に用いられる光子は，量子コヒーレンス時間が長いが，光子同士はなかなか相互作用しない．量子鍵配送には都合がいいが，もっと複雑な量子情報処理には，光子同士が相互作用し，エンタングルメントを生成する必要がある．つまり，物理的には，相互作用しやすければ，処理はできるが量子性が保てないし，相互作用しなければ，雑音は少ないが処理ができない，というようにトレードオフ的な関係になっていて，そこを乗り越えて量子制御する方法が見つけるのが大問題なのである．

もちろん，イオントラップや線形光学量子情報処理，超伝導量子ビットなどの物理系では，数量子ビットの制御まで実現化しており，量子情報処理の基本素子の原理の検証が行われている．これらの実験は，系の性質に合わせて細密な量子制御を行うことで初めて可能となるものだ．したがって，そこに量子ビットを加えて系を大きくしようとすると，状況が変わってしまうのである．これがスケーラビリティの問題だ．

問題を解くためには，ある数の量子ビットを用意する必要がある．この問題の規模が大きくなれば，より大きな数の量子ビットが必要になる．このときに，必要になる量子ビットの数が指数的に増えなければ，その量子情報処理系はスケーラビリティを満たす．しかし，実際には指数的な増加をしなくても，その増加の程度が大きければ，実際にはそのような情報処理系は実現することができない．それ以上に，物理系は 3 次元空間に収まらねばならず，どんな量子ビットにもサイズがあり，量子ビットの測定をするためにはそこにアクセスするための道筋が必要でそれも無限小というわけにはいかないから，実現化できるスケーラブルな量子情報処理系というのは，理論が示すスケーラビリティよりもずっと厳しい．実現化においては，この実現系上のスケーラビリティを満たすシステムの開発が重要なテーマである．

この問題を解決するために量子バスという考え方が最近注目され始めている．Qubus 量子コンピュータはその旗頭と言ってもいい．Qubus は Quantum bus つまり量子バスからきている．量子ビット間をつなぐ飛ぶ量子ビットの必要性や，量子バスを使ったゲートの構成方法などは前から考えられていたが，Qubus 量子コンピュータは量子バスを補助的な道具立てとせずに，量子バスと量子ビットの間の相互作用を基本原理として構成する量子情報処理の方法であるところが特徴的である．そのような素子が開発できれば，それを組み合わせることで，スケーラブルな量子情報処理系を構成することができる．また，その原理は量子ゲートから長距離量子通信まで応用でき，物理的なスケールによらず適応可能だ．このような Qubus 量子コンピュータの基本相互作用には，Qubus と量子ビットという２つの異なる性質，または物理系が自然とハイブリッドな構成となり，

それぞれの系のよいところをうまく利用することが可能になっている．また，広くさまざまな物理系，物理的性質を用いることができ，その組み合わせは多様で，インターフェースを内蔵している．そのため分散型の量子情報処理が可能で，長距離量子通信とあわせて量子ネットワークの構成を可能にする．しかし高い自由度と拡張性をもつ Qubus 量子コンピュータの基本素子をどの物理系で構成するのがよいのかはまだわかっていない．このような系の開発と可能性の開拓は今後の発展に期待したい．

Qubus 量子コンピュータの素子は量子デバイスとしても重要で，実現化にはその中核となる相互作用の物理的性質の解明が欠かせない．ところがこのような相互作用は，非線形な物理系であり，その量子性の解明は自明でない．実際，量子系における非線形系はこれまであまり論じられなかった．それはもちろんこのような系が複雑で，量子的に扱おうとすると数理的に手が負えないのと，実験的にも測定不可能であったからに他ならない．しかしながら量子情報処理研究の発展によって，量子状態を生成したり，量子性を直接観測することが可能になってきて，こういった量子的に新しい性質を持つ物理系に手が届くようになってきており，これからの展開が楽しみである．しかし，非線形な量子物理系や多体量子系を数理的に扱うのはとても限られていることには変わりないし，またこのような問題を計算科学の力でどこまで解明できるのかも不透明だ．チャレンジングなテーマではあるが，物理的にも数学的にも，そして情報科学的にもおもしろい問題が山積みであることは間違いない．

量子情報処理は量子物理学を中心に数学，情報学などいろいろな学問分野が集まる学際的な研究領域であり，そのため，量子情報処理という関心がどれほどの意義を持つのかは人によって意見が分かれるところであろう．しかし，この今までにない新しい試みから，学際的な概念の交流を通して，物理学や数学，情報学により深い理解が生まれたことは事実であるし，それらはこれから量子技術とともに私たちの文化や生活に大きな影響を持っていくだろう．量子情報処理は比較的若い研究分野でありながら，すでに岐路にある．それぞれの専門分野へ分化しつつあるわけだが，これからも学際的な，そして価値が不明瞭なほど混沌とした部分を持ち続けていってほしいと思う．そして，そのようなところからこそ，これまでにはない本当に新しい概念が生まれ，それがまた半世紀といった長い時間をかけて洗練されていくことが期待できる．私たちの英知を結集して，それだけの価値のあるものを見つけ出し，磨きをかける勇気を持ちたい．それには，混沌とした領域で，数学者，物理学者がともに泥にまみれることも必要ではないかと思うし，そういう領域こそが数学，物理学の他の研究分野をも活性化させる力があるのではないかとも思う．かつて量子力学がそうであったように，量子情報科学の中から将来に向けて新しい数学が生まれていけば，それほどうれしいことはない．

参考文献

１．根本香絵，池谷瑠絵，ようこそ量子ー量子コンピュータはなぜ注目されているのか，丸善ライブラリー (丸善，2006)

２．S. L. Braunstein (ed.), Quantum Computing, (Wiley-VCH, 1999)

３．S. L. Braunstein and H. –K. Lo (eds.), Scalable Quantum Computers (Wiley-VCH, 2001)

４．C. H. Bennett and G. Brassard, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, pp 175-179, (IEEE Press, 1984)

５．W. K. Wootters, Phys. Rev. Lett., 80, 2245 (1998)

６．Tzu-Chieh Wei, et. al, Phys. Rev. A 67, 022110 (2003)

７．D. Gottesman, Proceedings of the XII International Colloquium on Group Theoretical Methods in Physics, pp 32-43, (International Press, 1998)

８．K. Nemoto, Phys. Lett A 344, 104 (2005)

９．T. P. Spiller, et. al, New J. Phys. 8, 30 (2006)