

Champing at the bits

量子コンピューターはすぐそこに？

Nature Vol.440(398-401)/23 March 2006

J. MAGEE

量子コンピューターは、率直に言ってふしぎで難解な装置だ。しかし、いくつかのハードルが残っているものの、その実現の日は驚くほど近づいているらしい。この奇妙な装置はどのような道をたどって実現に向かっているのか、Philip Ball が研究の現状を取材した。

「実際に役に立つ装置を作るのに、あとどれくらい時間がかかるのか」。5年前、量子コンピューターの研究者に向かってこう尋ねたら、「推測さえできないほど先だ」という答えが返ってきただろう。しかし、もはや状況は変わっている。

「2020年までに実用的な量子コンピューターを実現するというのは、現実的な見通しだ」とオックスフォード大学（英国）量子計算グループのAndrew Steaneは話す。同大学の物理学者David Deutschも同じ意見だ。量子コ

ンピューターのアイデアを事実上考え出したDeutschは、最近の理論面の進歩を考えると、実用的な量子コンピューターは「今後10年以内に実現される可能性が大きい」と楽観的な構えをみせる。

こうした興奮の半面、克服しなければならないハードルも残っている。量子コンピューターを作るのは、まだとても、とてもむずかしい。その理由の一部は、自然には起こらないことを量子系にさせなければならないことにある。ミシガン大学アナーバー校（米国）の物理学者Chris

Monroeは、「前進してはいるが、そのペースはまだ極めてゆっくりだ」という。

また、たとえ今、量子コンピューターが実現したとしても、その上で走らせることのできるプログラムはほとんどないのが現状だ。実際、量子コンピューターは実現してもどうやら「すき間商品」にとどまりそうだ。つまり、ある作業には非常にすぐれているが、従来のパーソナルコンピューターのように何にでも使える装置ではないかもしれない。マサチューセッツ工科大学(MIT、

マサチューセッツ州ケンブリッジ)の量子物理学者 Isaac Chuang は「量子コンピューターが汎用のデスクトップマシンとはならないことは、ほぼ間違いのない話だ」と認める。

しかし、ほかの量子系を模擬する能力にすぐれている量子コンピューターは、科学研究のツールとしては画期的なものとなるかもしれない。従来の古典的なコンピューターでは、情報は1列のビット、つまり0あるいは1の値をとる2進法の数字として蓄えられる。これは量子コンピューターでも同じことなのだが、ただし、量子コンピューターにおける2進法の数字である「キュービット」は、原子やイオンの電子状態などの微視的な系の量子状態に蓄えられる。だから、量子コンピューターは本来的に、古典的なコンピューターよりも量子系を模擬するのに適しているはずなのだ。

「量子シミュレーター」は、分子や物質の基本的な量子的性質を正確にとらえることで、その構造や反応性を記述・予測するものになるはずだ。初期の量子コンピューターは、この種の仕事に取り組むことになるだろう。化学者や材料科学者、場合によっては分子生物学者にとっても興味ある計算を行うことになるのではないかと Steane は話す。

また、「わずか数ダースのキュービットが、従来のコンピューターでは手におえないような物理の問題を解明するかもしれない。たとえば高温超伝導や凝縮系の理論モデルの構築に、そうした量子シミュレーターが利用される可能性があると思う」と Monroe はいう。

スピンを使って

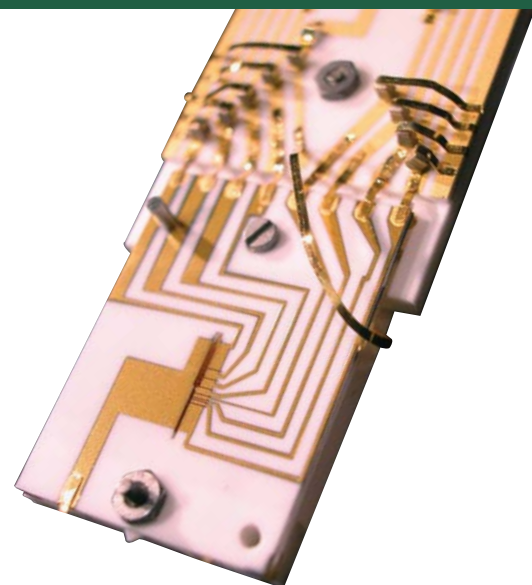
実際、量子シミュレーションはすでに、原子や分子の原子核スピンのキュービットを蓄えることにより、実行可能だ。キュービットの測定や操作には核磁気共鳴を使う。研究者はこれを「コンピューター」とよんでいて、MITの理論研究者 Seth Lloyd によると「いかなる古典的スーパーコンピューターよりもはるかに高速だ」とい

う。Lloyd と、MIT の同僚である David Cory はこの技術を使い、フッ化カルシウムやその他の物質の結晶中の量子系など、さまざまな量子系のシミュレーションを行っている。「結晶は10の18乗個ものスピンを含むので、このような系のシミュレーションは最も高速な古典的コンピューターをもってしても不可能だ」と Lloyd は話す。Lloyd たちが取り組むこの方法では、模擬できる系についての制約があるが、完全に機能するシミュレーターも2020年までには難なく実現できるようにになると Lloyd は予想する。

量子コンピューターはデータの蓄積と操作を量子的に行う。量子コンピューター実現の鍵と、またそのむずかしさの原因はここにある。古典的なコンピューターではビットは1あるいは0と明確に決まっている。しかし、量子力学に支配されるキュービットは「状態を重ね合わせたもの」になる。つまり、従来のコンピューターでは不可能な、1と0が混じりあった状態にあるわけだ。これは、量子コンピューターが情報を蓄積できる容量は、従来のコンピューターよりもはるかに大きいことを意味する。

量子的な演算装置では、一度に2つ以上のキュービットで計算を行うこともできる。これには、キュービットが相互に依存するようにさせているもつれ合い(エンタングルメント)という別の量子的性質を利用する。個々のキュービットの測定結果は測定の瞬間までわからないが、もつれた状態のふしぎな性質のため、1つのキュービットの測定は即座に別のキュービットに影響をもたらす。もつれた状態は自然にはふつつ存在しない。量子コンピューターを研究しているエンジニアたちは、キュービットを互いに相互作用させ、もつれた状態を作り出さなければならない。

重ね合わせを利用することにより、1台の量子コンピューターが事実上、同時に走る複数の古典的コンピューター群と同じ動きをする。そして量子のもつれ合いを利用すると、これらの「並列コンピューター」が互いにリンクすることになる。し



閉じ込める：この回路は、電極の上にイオンをトラップする。

かし残念ながら、この強力な並列プロセッサにはアキレス腱がある。量子的な重ね合わせは、少なくとも計算をするのに必要な時間、安定でなければならない。しかし、キュービットがその環境と相互作用するやいなや、壊れやすい重ね合わせ状態は不安定になる。これがデコヒーレンス(干渉性の消失)とよばれるプロセスで、量子コンピューターから情報が漏れ出す原因となる。デコヒーレンスをもつれた状態にとって特に問題となる。1つのキュービットのデコヒーレンスがほかのキュービットにも影響するからだ。

デコヒーレンスを防ぐには、制御されずに起きる環境との相互作用を減らさなければならない。量子系を極低温に冷やすことは、その1つの手段となる。しかし、迷い込む電磁場からキュービットを保護することも必要かもしれない。研究では、実際に特定のキュービットのデコヒーレンスを数秒間以上防ぐのはむずかしいことがわかっている。しかし、原理的には可能はずだ。「トラップされたイオンにコードされたキュービットが、コヒーレンス時間によっていつまでも制約されるとはだれも考えていない」と Monroe は話す。

キュービットはデコヒーレンスを避けるため、環境から切り離される必要がある。一方、計算を行うためにはキュービットは互いに強く相互作用しなければ

ならない。そして、重ね合わせ状態にあるキュービットは、情報を読み出すことができるよう、必要なときには環境と強く相互作用することが可能でなければならない。これは非常にむずかしいまるで綱渡りのような操作で、まだ完全に理解されていない直観に反するような法則に支配されるものである。

間違いやすい計算機

このデコヒーレンスのため、量子コンピューターは論理ゲートを使ってキュービットを処理するとき、古典的なコンピューターよりもはるかに高率で誤りをおかしてしまう。「現代のトランジスタの誤り率は、 10^{14} 回程度以上のスイッチング動作に1回あるかどうかだ。これに比べて、私たちが現在想定する最もすぐれた量子ゲートでも、少なく見積もって 10^7 回に1回ほどの誤り率になるだろう」と Chuang は話す。当初、これでは量子コンピューターはあまりに誤りが多く、実用にならないだろうと考える研究者もいた。しかし、1990年代に考案された量子誤り訂正コードのおかげで^{1,2}、今では 10^5 回に1回という高い誤り率でも訂正が可能になった。

量子コンピューターの基本的な原理について2002年には、理論家たちによってその概略が解明された（「量子コンピューターの満たすべき条件」を参照）。しかし、現実の装置として作り上げるのにどのような方法がベストであるかは、大きな問題として残っている。現在研究されている方法の多くは、トラップの中に保持された原子やイオンを使って量子コンピューターを作るというやり方だ。イオントラップ型量子コンピューターでは、キュービットは電磁場で閉じ込められたイオンの電子状態にコードされる。イオンは静電的な反発力を通じて互いに相互作用し、レーザービームでいっせいに揺ることにより、もつれ合わされる。こうしたイオンの量子状態は、別のレーザーを照射して蛍光発光させることで読み出すことができる。このレーザーの波長は、イオンの電子状態に依存する。

しかし、キュービットの数が多いほど、その集団の複雑な振動状態を読み出すことはむずかしくなる。この問題を回避する方法の1つは、イオンのほとんどを容器に保持し、容器から演算室へと運ばれた少数のイオンだけを

使って各計算ステップを行うことだ。つまり、イオンの量子状態を変化させず、イオンが移動の途中でその「記憶」を失わないようにしながら、イオンをあちこちに往復させなければならない。

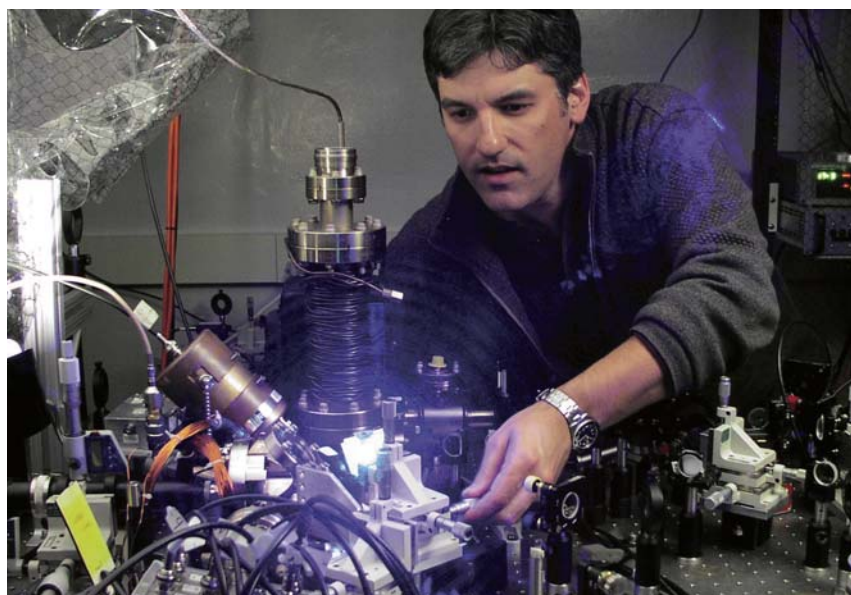
勝者はだれか

こうした問題の解決は容易ではないが、最近の進歩は励みとなる。「イオントラップチップは、ほかの方法に先んじて実用的なコンピューターの作製につなげることができそうなポジションにある」と Steane は話す。たとえば昨年12月、Monroeの研究チームは標準的な微細加工技術を使い、半導体チップ上にイオントラップを作ったことを報告した³。このトラップは個々のカドミウムイオンを1時間以上にわたって保持し、研究者たちはその間に、あるトラップ場所から別のトラップ場所へうまくイオンを動かすことができた。

米国標準技術研究所（コロラド州ボルダー）の David Wineland のグループも同じようなアイデアを研究している。彼らの方法では、イオンはチップの表面にエッチングされた電極の上にトラップされている⁴。Wineland は「Monroeの方法も私たちの方法も、すでに確立された加工技術を使うという利点がある。最終的に開発競争の勝者を決めるのは、単純にどの製作方法が最も簡単か、ということになるのかもわからない」と話す。

Monroe はこれまで成功を収めてきたにもかかわらず、長期的な見通しに関しては慎重な姿勢をみせる。「多くの研究グループが複雑なイオントラップチップを作ろうと競争している。しかし、イオントラップという方法が最終的にほかの量子技術に劣らないものであるかという保障はまだない」と彼は話す。

イオンの代わりに、トラップされた中性原子を使ってキュービットをコードしている研究者もいる。原子は、イオンよりも環境との相互作用が弱いという利点がある。しかし、原子どうしの相互作用



光でそっと捕捉する：量子計算を行わせるため、Chris Monroe がレーザービームを1列に並べてイオンをトラップしようとしている。

も弱い。原子はレーザービームでトラップされる。交差したレーザービームで作られた干渉パターンを使えば、数百個の原子が卵ケースのような「光の格子」の中に保持される。トラップに使うビームを調節することで、原子どうしが相互作用するよう卵ケースのくぼみを互いに近づけることも可能だ。

原子で量子計算を行う方法の1つは、より大きな格子の中で、もつれ合った原子の分離したクラスター（集団）を作ることだ。この方法は、オーストリアのインスブルック大学の Hans Briegel、Ignacio Cirac、Peter Zoller たちが1990年代後半に初めて提案した。Deutschもこの量子計算方法について、キュービットを扱う方法とし、ほかの方法よりも「はるかに物理的に実現しやすい」と話している。

標準的な方法と異なり、クラスターによる計算では個々の粒子の操作をしなくてすむ。その代わりに、計算を行う前に、いくつかのキュービットを集めて多数の粒子のもつれ合い状態を作っておく。そして、計算が実際に行われると同時に、クラスター中の個々のキュービットで一連の測定を行い、答えを読み出す。この「ワン・ステップ」な特徴ゆえ、この方法は魅力的だが、現在マックスプランク量子光学研究所（ドイツ、ガルヒング）に所属する Cirac は、この方法はほかの方法よりもずっと多くのキュービットを必要とし、そのため誤り訂正手続きが複雑なものになることを認めている。

量子ドットという方法

量子コンピューターを作るためのアイデアは、このほかにもたくさんある。あるものは超伝導デバイスを使い、超伝導そのものが量子現象であるという事実を利用する。個々の粒子を使う系と異なり、この方法ではキュービットは超伝導回路だ。超伝導回路は、電荷や磁束などの多数粒子系の量子状態を備え、古典的な電磁力で相互作用することができる。

キュービットを光子の量子状態にコー

量子コンピューターの満たすべき条件

米国の専門家たちが、今後10年間の量子コンピューター研究についてまとめた現時点の指針 (<http://qist.lanl.gov/>)。この指針では、実用的なコンピューターが備えるべき要件を挙げている⁸。

- 1 大きさの変更が可能でなければならない。無限につけ加えることができるキュービットのセットが必要である。
- 2 すべてのキュービットを、たとえば全部が0、といった単純な初期状態にセットできなくてはならない。
- 3 キュービット間の相互作用は、量子論理ゲートを作るのに十分な程度に制御可能でなければならない。
- 4 論理ゲートを使って操作を行うため、デコヒーレンス時間はゲート操作時間よりもずっと長くなければならない（だいたい数ミリ秒から数秒）。
- 5 読み出し可能でなければならない。
- 6 コンピューターをネットワークするため、固定型キュービットを弾道型キュービットへ変えること、およびその逆が可能でなければならない。
- 7 弾道型キュービットを特定の場所から場所へと、正確に移動させることが可能でなければならない。

ドし、光学的な量子コンピューターを作りたいと考える研究者や、量子ドットとよばれる半導体材料中の小さなスペックでキュービットを作りたいと考える研究者もいる。「量子ドット系と、超伝導による方法でなされた成果が特に印象的だった」と Chuang は話す。こうした方法はイオントラップと比べてより簡単に規模を大きくすることができ、読み出しのために従来のデータ転送系につなげるのも容易かもしれない、と彼は説明する。

量子ドットは初めての実用的な量子コンピューターを実現する方法とはならないかもしれないが、やがてはイオントラップチップなどのほかのシステムよりもすぐれた性能をもつはずだと Steane は話す。その主な理由は、イオンよりもずっと軽い電子にキュービットをコードするため、当然ながら時間スケールが短くなるからだ。しかし Steane は、「この研究分野にはさまざまな可能性があり、実現を狙う主な方法のどれもまだ研究の速度を落とすには時期尚早だ」とも語る。

量子コンピューターの実現にあたって

は、ハードウェアを作るというハードルが本質的に存在し、このため、課題は工学的な問題だといわれることが多い。しかし、理論にも課題はある。今のところ、量子コンピューターの上で走り、解くことができる形に翻訳された計算問題はまったくといえるほどない。

実際、量子コンピューターは現在、2つの芸しかもたない神童のようなものだ。1994年、今はMITにいる Peter Shor が、量子コンピューターで従来のコンピューターよりも指数関数的に高速で整数の因数分解を行うことができるアルゴリズムを考案した。因数分解は、暗号技術において暗号鍵を作り、解読するのに必要なことから重要な問題だ。1996年には、現在ルーセントテクノロジーズ社（ニュージャージー州マリーヒル）に所属する Lov Grover が、極めて高速にデータベースを検索できる量子アルゴリズムを発表した。

こうしたアルゴリズムの両方はすでに、核磁気共鳴と光学技術を使って実行されているが、これらの方法は規模を大きくするのがむずかしい。昨年末、



トラップに捕まる：半導体チップ上の2つの電極間に1個のカドミウムイオンが保持されている。

Monroe の研究グループは、トラップ中の2個のカドミウムイオンを使って Grover 型の検索に成功したことを報告した⁵。もっとも、検索したのはたった4項目しか含まれていないデータベースで、元より取るに足らない作業だ。しかし Monroe によると、研究グループでは今後数年のうちに数十ダースのキュービットへと規模を拡大することを計画しているという。

「Shor の発明から10年が経過したが、新しい量子アルゴリズムがほとんど開発されなかったのは衝撃的だ」と Chuang は話す。わずかな開発例として、NEC ラボラトリーズアメリカ（ニュージャージー州プリンストン）の

Sean Hallgren が作った、整数論の問題を解くアルゴリズムがある⁶。

新しいアルゴリズムの考案を試みる研究者にとっての大きな障害は、どういう問題に量子計算が最も有効かをまず見極めなければならないことだ。この点においてはクイーンズランド大学（オーストラリア）の理論家 Michael Nielsen たちが最近、量子アルゴリズムを見つけるという全般的な問題は、幾何学からアイデアを借りることによって比較的容易になりうることを示し、前進がみられた⁷。

これは、量子操作の数、ひいてはアルゴリズムを実行するのにかかる時間は、本質的には、量子操作が可能なすべての列によって定義される幾何学的

科学計算における画期的事件

プロトタイプの時代 1960年代以前

1946 最初のデジタル電子計算機と広く考えられている ENIAC が正式に公表される。ENIAC は第二次世界大戦中に弾道計算を行うために作られ、乱数研究、風洞設計、気象予報などのさまざまな科学分野で計算を行った。気象の24時間先までの数値予報を初めて行うも、計算には約24時間を要した。

1951 Marvin Minsky がニューロンネットワークを模した初めての装置、SNARCを開発。Minsky は後にマサチューセッツ工科大学 (MIT) の研究者となった。

1954 IBM の John Backus たちが科学技術計算用のプログラミング言語 Fortran の開発を始める。

1956 マンチェスター大学 (英国) などの研究をもとに、ロスアラモス国立研究所 (米国ニューメキシコ州) が MANIAC を開発し、チェスを初めから終わりまで行うことができる最初のコンピューターとなる。後の1996年には、IBM の「ディープ・ブルー」がチェスの世界王者 Garry Kasparov を破ることになる。

1959 ケンブリッジ大学 (英国) の John Kendrew がコンピューターを使い、結晶データからミオグロビンの立体構造を決定。

大型汎用コンピューターの時代 1960年代

1962 MIT・リンカーン研究所の Charles Molnar と Wesley Clark が、米国立衛生研究所の研究者用に「ラボラトリー・インスツルメント・コンピューター」(LINC) を作製。リアルタイムでのデータ処理を目的とした、初めての実験室用コンピューターとなった。

1963 コンピューター制御による初のロボットアーム「ランチョアーム」が米国カリフォルニア州で開発される。

1966 MIT の Cyrus Levinthal が、タンパク質構造の決定と解析を行う初のプログラムを完成。

1967 米国防総省が、インターネットのもととなった ARPANET を研究用ネットワークとして提案する。

1969 気象学者の真鍋淑郎と海洋学者 Kirk Bryan が、初めての海洋・大気結合大循環モデルの計算結果を発表。後に地球温暖化に関する強力な研究ツールとなる気候シミュレーションの先駆けとなった。

ワークステーションの時代 1970年代

1971 最初のコンピューター断層撮影 (CT) スキャナーのプロトタイプが作られ、医療用画像におけるコンピューターの潜在能力を示す。

1971 米国のブルックヘブン国立研究所 (ニューヨーク州アプトン) にタンパク質データバンクが設立される。

1972 ヒューレットパッカード社が、初めての手のひらサイズの科学電卓 HP-35 を発売し、エンジニアが使う計算尺は時代遅れに。

1976 ロスアラモスで Seymour Cray が最初の「クレイ」スーパーコンピューターを完成。大量のデータが短時間で処理可能に。

空間における2点間の最短経路を見つけることで計算できるという考えだ。「古典的な類似物のない、本当に画期的なアイデアだ。新しいアルゴリズムを作る可能性のあるさまざまな方法や、既存のアルゴリズムを最適化するいろんな方法を切り開く」とLloydは話す。

しかし、量子情報の処理装置のすべてが複雑なアルゴリズムを必要とするわけではない。その多くは、原子時計や光通信技術などの既存の技術を改良する目的で量子法則を応用した、特定用途用のツールとなるだろう。「おそらく、『量子中継器』などの基本的な装置をまず実現させることになるだろう。これは、誤り訂正のために光子の

キュービットを原子のキュービットに変え、光ファイバーで長距離を伝送させるため再び光子のキュービットに戻すといった装置だ」とMonroeは話す。

次の大きな目標として引き合いに出されることがある量子脳と比べて、こうした装置がやけに地味に思えるとしたら、そう思えることには慣れてしまうし、かしかたがないのかもしれない。しかし、Lloydは将来の見通しについて楽天的だ。「確かに、汎用性のある量子コンピューターよりも先に、特定用途に合わせた量子コンピューターが作られることになりそうだ。それは認める。でも、だからといって近い将来に『グランド・セフト・オート』（米国で人気の犯罪アク

ションゲーム)の量子コンピューター版でみんなが遊んでいるという可能性がないわけではない」とLloydは話した。

Philip BallはNatureの編集顧問。

1. Shor P. W., *Phys. Rev.*, **A52**, R2493 - R2496 (1995).
2. Steane A. M., *Phys. Rev. Lett.*, **77**, 793 - 797 (1996).
3. Stick D., et al. *Nature Phys.*, **2**, 36 - 39 (2006).
4. Seidelin S., et al. preprint at <http://www.arxiv.org/quant-ph/0601173> (2006).
5. Brickman K.-A., et al. *Phys. Rev.*, **A72**, 050306(R) (2005).
6. Hallgren S., et al. in Proc. 34th Annu. ACM Symp. Theor. Comput., 653 - 658 (ACM, New York) (2002).
7. Nielsen M. A., Dowling M. R., Gu M. & Doherty A. C., *Science*, **311**, 1133 - 1135 (2006).
8. DiVincenzo D. P., *Fortschr. Phys.*, **48**, 771 - 783 (2000).

パーソナルコンピューターの時代 1980年代

1983 Danny Hillis が並行処理を行う最初のスーパーコンピューター「コネクションマシン」を開発。流体フローのシミュレーションや人工知能に利用される。

1985 学術用の高性能計算機がないとの報告を受け、米国立科学財団が国立スーパーコンピューティングセンターを5か所設立。

1989 素粒子物理学研究所 CERN (スイス、ジュネーブ) の Tim Berners-Lee がワールドワイドウェブを開発。世界各地の物理学者による共同研究を支援するのが目的だった。

インターネットの時代 1990年代

1990 広く利用されているバイオインフォマティクスプログラム BLAST (Basic Local Alignment Search Tool) が開発される。アミノ酸や塩基対の特定配列に関する迅速なデータベース検索が可能に。

1996 George Woltman が異質なデータベースを組み合わせ、GIMPS (Great Internet Mersenne Prime Search) を発表。9個の巨大なメルセンヌ素数 ($2^n - 1$ の形で表される) を発見するプロジェクトとなる。そのうちの1つは9,152,052桁の数字である。

1996 Craig Venter がショットガン法を開発。コンピューターで DNA コードの大断片をつなぎ合わせる方法で、全ヒトゲノムの解読時間が短縮されることになった。

1998 核磁気共鳴を利用して動く最初の量子コンピューターが開発される。

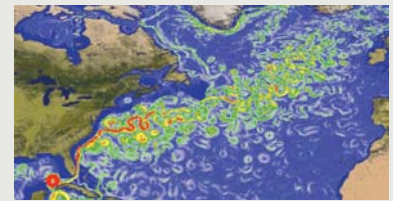
インブリットコンピューティングの時代 21世紀

2001 米国で国立バーチャル天文台プロジェクトが発足し、天文学の巨大なデータセットの探索法を開発する。



2001 米国立衛生研究所が、多数の施設間でデータを共有化するためのスーパーコンピューターのグリッド、BIRN (Biomedical Informatics Research Network) を立ち上げる。

2002 日本で「地球シミュレーター」が運用開始に。毎秒35兆以上もの演算を行い、地球のプロセスのモデル化を進める。



2005 IBM 社の「ブルージーン」ファミリーのコンピューターとして新たに「ブルーブレイン」が登場。脳の最も複雑な領域である新皮質で生じている神経の働きをモデル化を目指す。

2007 CERN (スイス) に LHC (Large Hadron Collider; 世界最大の素粒子加速器) が設置される予定である。膨大なデータ量が予想され、かつてない処理能力が必要とされる。

(年表作成: Jacqueline Ruttimann)