計算機アーキテクチャ 140－1
（2000．11．29）

量子計算の科学

今井 浩

東京大学理学系研究科情報科学専攻

ERATO 今井量子計算機構プロジェクト，科学技術振興事業団

imai@qci.jst.go.jp

あらまし VLSIの集積度の向上に伴って，量子効果の影響が考えられるまでの微細な世界が目前に迫ってきて，それを乗り越えるための様々な事柄がデバイス研究から新計算モデルの確立まで考えられている．量子計算は量子力学原理に基づいて計算を行うという計算モデルで，1980年頃から研究がされてきて，90年代後半で素因数分解問題を通して既存の計算モデルを超える計算能力が示され，注目されている．この量子計算について，これまでの流れを概説し，そのモデルを説明して，新たに量子情報科学を目指すことについて述べる．

キーワード 量子計算，量子コンピュータ，量子情報，量子暗号，量子通信，量子情報科学

Quantum Computing Science

Hiroshi Imai

Department of Information Science, University of Tokyo

ERATO Quantum Computation and Information Project, JST

imai@qci.jst.go.jp

Abstract The speed-up of VLSI with the current technology will face a big problem caused by quantum effects in near future, and research on both new device technology and new computing models have been performed. Quantum computing is a new computing discipline based on the quantum physics and utilizing fundamentals of quantum mechanics. This new computing paradigm has been investigated since 1980's, and, in the latter half of 1990's its computing power outperforming that of the current computing model has been revealed. In this paper, trends in quantum computing are summarized with an outline of its model, and the importance of quantum computing science research is described.

Key words Quantum Computing, Quantum Computer, Quantum Information, Quantum Cryptography, Quantum Communication, Quantum Computing Science

1　今そこに見える限界

コンピュータの高速化に多大な寄与をしてきたVLSIの高速化は，1,2年で倍近くという集積密度の向上によって高速化が実現されてきた．現在のCMOS技術の枠組は，2010から2020年頃には微細化が進む結果，トンネル効果など量子効果が顕在化するために，限界に達して壁にぶつかると予想されている．たとえば，20～30nmより小さいチャネル長を実現するのは難しいだろうと予想されている．

では，チップの性能向上はそこで終るのだろうか? 20世紀最終段階でこれだけ情報技術が社会インフラとなるのに，チップの性能向上は本当に大きな貢献をしてきた．限界を具現化したVLSIチップができて，それ以上にはもはや進展はなく，情報技術は並列処理など他の道を模索して進むことになるのだろうか?

コンピュータの高速化に関する要求は，際限のない人間の欲望と同じく留まるところがないとされたりする[9]．飛行機ならジャンボを超える1000人乗りの飛行機を作る技術があっても，車なら時速300kmの高速車を作る技術があっても，万が一の事故が起った際の社会影響や人間の制御限界などで，決してそれが広く普及はしないのに対し，コンピュータが今のように社会の隅々まで配置されて，それがどんどん性能向上していくのには何ら心理的障害がないというのである．

では，VLSIの高速化の量子効果による壁は乗り越えられるのだろうか? この壁を乗り越えるための並列処理や，全く新しい技術としてたとえばDNAを計算に使うDNA計算など，種々の挑戦がなされている．それらの挑戦では単純化すると，デザインルールで数十ナノメートルになって量子効果が現れてCMOSが限界に達するという

「量子効果＝既存計算モデルへの障害」

という図式になっていた．量子トランジスタなる量子力学の世界で動く素子も研究されているが，それは既存の計算モデルを実現することを目指している点では上の図式に対抗はするものの，あくまでも既存計算モデルの枠組みの中であり，量子効果があっても今までと同じことがより高速にできるようにという姿勢である．

2　量子計算モデルが提唱されるまで

これに対して，ニュートン力学ではもう予測できない，量子力学こそが支配する世界の様々な物理現象を，新しい計算原理として扱うという発想の転換が提唱されている．すなわち，このアプローチでは

「量子力学原理＝新計算モデルのパワー」

という図式である．この新計算モデルを量子計算モデルといい，このモデルを実現するコンピュータが量子コンピュータである．

量子計算の夢を明示的に語ったのは物理学者のFeynmanであり，1980年代初頭である．彼自身は，量子コンピュータを使って量子力学計算を速く行う夢をもっていたようだ．また，量子コンピュータを現在のコンピュータでシミュレートすると指数時間かかると予想していた．

Feynmanが1980年頃にそのような夢を語る前にも，量子コンピュータに通じる研究があった．それは回路の集積化が進んで量子効果が起こる前から問題と認識されている回路の発熱についてである．計算による情報損失を情報量としてとらえ，それが熱力学のエントロピーに変換されて発熱するという図式に対しては，情報損失を発生させない回路，すなわち完全に可逆な計算(出力から入力がユニークに計算できる)を実現する可逆回路の研究が1970年代にBenettによってなされている．可逆回路が現在の回路理論で可能であることは示されたが，残念ながら必要な素子数が爆発的に大きくなってしまうため，実用にはなっていない．

計算に活用しようという量子力学の基本は，以降で述べるように重ね合わせ状態とその上のユニタリ変換である．ユニタリ変換は可逆であるので，それに対応する回路で計算する限り，可逆計算となる．さらに，現在の回路で可逆計算で素子数爆発を招いた点を，重ね合わせ状態で多数の状態をまとめて表現することによって量子素子数をある程度おさえたままで計算できる可能性が出てくる．

Feynmanの夢を具体的にコンピュータのモデルとして提示したのが，Deutschで，物理の観点から1985年に量子コンピュータのモデルを提唱した．このモデルの素直なところは，定義より，量子コンピュータのモデルは既存の計算モデルを特殊な場合として含んでいることである．したがって，その特殊さがどのくらいになるのか，逆の言い方をすれば既存の計算モデルでできなくて，量子計算モデルで効率よくできることは何なのかということが問題になる．以降，どちらかといえば人工的な問題を題材に，量子計算モデルが既存の計算モデルを凌駕する計算パワーを持つことなどが議論されていたが，物理的実現の難しさと，既存コンピュータとの差の大きさが認識され

ずに量子計算モデルの精緻化の研究など地道になされていたというのが1990年代前半の状況であった.

3 コンピュータ科学からの量子計算アルゴリズム開発

量子コンピュータの研究は1990年代後半爆発的に増えた. 実は, 電子マネーなど現在の情報インフラを支えるRSAなど公開鍵暗号システムが依存している計算量仮説 (一方向関数の存在を仮定) が, 量子コンピュータが実現されると破られるという研究結果がコンピュータ科学でのブレークスルーがあったからだ. このRSA暗号など公開鍵暗号は, 素因数分解や離散対数問題の難しさ (計算量仮説のもとで保証される) によって安全性が保たれており, それが量子コンピュータで難しくなく簡単に解けてしまうというのである. 楕円暗号など代数曲線に基づく先端暗号系も, 代数曲線上の有限群の離散対数問題を使い, 基本的には同じように解けてしまう.

これは1994年にShorが示したブレークスルーである. Shorはコンピュータ科学の理論で成果をあげていたBell研の研究者で, 量子コンピュータ上でのフーリエ変換能力の威力に気づいて, このブレークスルーを巻き起こした.

これは一大センセーションを巻き起こした. 帰結として, 物理学者が多く量子コンピュータ実現へ向けての研究を開始するとともに, コンピュータ科学者は他の今のコンピュータでは難しい問題が量子コンピュータで早く解けないかとブレークスルーを目指した研究に邁進している.

4 量子コンピュータの仕組み: 概説

量子コンピュータを実現するには, まず量子ビットと呼ばれるものを実現するデバイスが必要である. 今のコンピュータで1ビットというと, 0か1かをとるもので, 全ての基本となっている. 量子ビットというのは, 0と1の間の状態も量子力学にそってとれるものである. 電子スピンのイメージだと, 上を向いていれば1, 下を向いていれば0, どこか他のところを向いているとその向いてる角度から0と1が混ざった状態を量子的に表現するわけだ.

たくさんの量子ビットが集まったのが, 量子コンピュータの内部状態である. その上に, 量子力学で許された操作を行っていくことが計算に対応する. 実際には, コンピュータの単位操作としていくつかのユニタリ変換が指定されていて, それを状態に対して適用していく. 先にも書いたように, ユニタリ変換は可逆である. そして, 量子ビットの集まりの上でユニタリ変換をしていくと, 現在のコンピュータでは指数爆発的に増えてしまう情報を, 量子重ね合わせ状態としてコンパクトに保持する. もちろん, これは重ね合わせ状態なので, 爆発的個数あるものを重ね合わせをしてしまってるので, そこから所望の情報を取り出すのに工夫がいる.

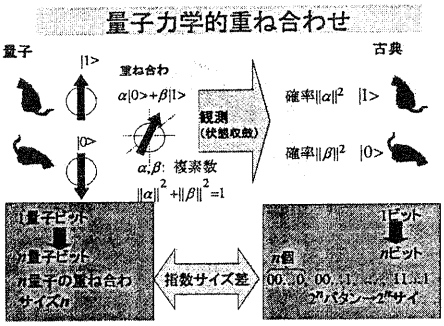

図 1: 量子重ね合わせ状態

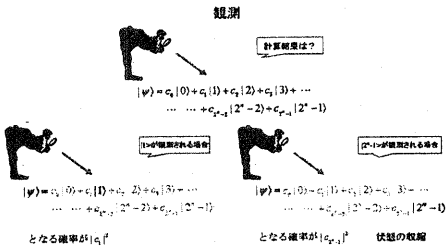

図 2: 量子状態の測定

重ね合わせ状態から情報を取り出すのが観測という操作である. これは, 量子重ね合わせで各基底の状態について, その重みとして複素数が与えられていたとき, それのノルム・原点からの距離の2乗 (これを振幅と呼ぶ) の確率で, その基底の状態が観測されるというものである. ここで, 確率的な挙動が入ってくる.

量子アルゴリズムでは, 入力を量子ビットが純粋に集まった状態として表現して, それにうまくユニタリ変換をかけていくことにより, 求めたい基底の状態の振幅が増えるようにしていって, 最後に観測によって所望の状態を高い確率でえようとする.

量子アルゴリズムの素直なところは, 既存のコンピュータのアルゴリズムを全てそのままで非常に特別な場合として含むことである. これは, 他の新パ

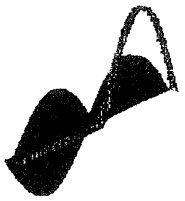

図 3: 量子干渉効果

ラダイムに基づく計算方式とは異なる点と言える．

5 代表的量子アルゴリズム

5.1 Shor のアルゴリズム

Shor が示したのは，素因数分解すべき整数に関する量子状態を量子ビットで表現し，その上でユニタリ変換として離散フーリエ変換という量子コンピュータならではで高速に行える変換を用いて，素因数分解を行うのに必要な周期の情報を見つけやすくし，ある確率でそれを観測して答えを見つけるというものである．実際，素因数分解の現在の枠組みのコンピュータによる解法では，確率的挙動を使うことが本質的であるとの認識がされていて，計算量理論分野で NP∩co-NP, RP∩co-RP など調べられていたわけであるが，Shor は彼自身の確率アルゴリズムの研究での成果・知見から，量子コンピュータなら素因数分解が多項式時間で解けることを明らかにした．同時に，有限群上の離散対数問題についても，群演算に関する基本的なオラクルを仮定したときに，同じく多項式時間で解けることを示した．

5.2 Grover のアルゴリズム

1996 年の Grover の量子探索アルゴリズム [4] も興味深い．これは n 個の未整列なインデックスから，あるインデックスを $O(\sqrt{n})$ 時間で探すことができる．これは「振幅の増幅」という手法を用いており，量子アルゴリズムの例としても非常にわかりやすく，SAT など NP 完全問題に幅広く応用ができる．

6 量子計算の原理: 理論

古典コンピュータと量子コンピュータの違いを理解するためには，まず，1 ビットを考えるとよい．古典ビットは 1 と 0 の 2 状態のうちのどちらか 1 つをとる．古典的な確率的ビットは確率 α で 1 を，確率 β で 0 をとり，$\alpha+\beta=1$ という性質をみたす．量子ビット (qubit) は後者によく似ている．量子ビットは，複素 2 次元空間の点 (α,β) で，$\|\alpha\|^2+\|\beta\|^2=1$ を満たすものである．量子ビットを観測すると，確率的ビットのように確率 $\|\alpha\|^2$ で 1 をとり，確率 $\|\beta\|^2$ で 0 をとる．

より一般的に n ビットを考える．古典 n ビットは $m=2^n$ 個の状態のうちのどれか一つをとりうる．量子 n ビットは複素 m 次元空間で l_2 ノルムが 1 のものである．この空間の m 個の基底状態を $|q_1\rangle,|q_2\rangle,\ldots,|q_m\rangle$ と表したとき，一般の量子 n ビット ψ は複素数の係数をもつこれらの線形結合

$$\psi=\alpha_1|q_1\rangle+\alpha_2|q_2\rangle+\ldots+\alpha_m|q_m\rangle.$$

となり，条件より ψ の l_2 ノルムは，

$$||\psi||=\sqrt{\|\alpha_1\|^2+\|\alpha_2\|^2+\ldots+\|\alpha_m\|^2}=1.$$

を満たす．ψ は $|q_1\rangle,|q_2\rangle,\ldots,|q_m\rangle$ の基底状態の重ね合わせと呼ばれ，$\alpha_1,\ldots,\alpha_m$ は各基底に対する振幅と呼ばれる．量子状態で量子 n ビットはこの $m=2^n$ 個という n の指数個の基底状態を，それぞれの振幅で重ね合わせたコンパクトに表現しており，これが並列性の源となる．

複素数の振幅を用いられることは量子計算の有用性の本質となっている．2 つの量子ビットをさらに重ね合わせたとき，複素数の振幅が正負で帳消ししたり，増幅したりする．振幅の 2 乗が次に述べるように確率に対応するのだが，単に確率的な計算モデルではこの帳消し・増幅という操作はできなかった．これを量子干渉効果と呼ぶ．

量子計算は 2 種類の変換をする．1 つはユニタリ変換である．ユニタリ変換は $l_2(Q)$ 上の線形な変換 U であり，l_2 ノルムを保存し，重ね合わせ状態を他の重ね合わせ状態に変換する．重ね合わせ状態は 2^n 個の状態を重ね合わせたものであったから，単にこの上で 1 回のユニタリ変換を掛けるだけでその 2^n 個の状態を変換していることになり，これが量子計算の並列性と呼ばれるものである．

2 つめは観測である: 観測は $\psi=\alpha_1|q_1\rangle+\alpha_2|q_2\rangle+\ldots+\alpha_m|q_m\rangle$ という重ね合わせのとき，確率 $\|\alpha_i\|^2$ で $|q_i\rangle$ を与える．観測後，状態は $|q_i\rangle$ になる．

7 量子回路: 理論

量子回路（図 4）は具体的な量子計算の操作の表現，アルゴリズムの表現に優れている．量子回路では 1 量子ビットを横線で書きワイヤと呼ぶ．時間は左か

ら右へ流れているとする．そしてその線の上に1量子ビットに対するユニタリ変換をワイヤの上に書き，これを量子ゲートと呼ぶ．複数ビットに相互的に作用するときは相互作用するワイヤ間を縦線でつなぐ．各ビットはゲートを通過すると，そのユニタリ変換を受ける．

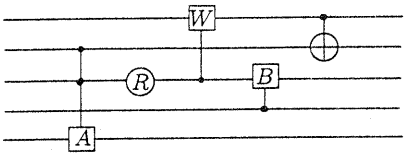

図 4: 量子回路

n 量子ビットは複素 2^n 次元ベクトルであるので，これに対する操作は $2^n \times 2^n$ ユニタリ行列で表す．任意の $2^n \times 2^n$ ユニタリ行列は以下の2種類の基本ゲートに分解でき，量子回路の計算時間は以下の2種類の基本ゲートの使用個数と定められる．

U ゲート （図 5）1量子ビットに対するユニタリ変換は任意の 2×2 ユニタリ行列で表せる．これを U ゲートと呼ぶ．

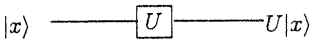

図 5: U ゲート

制御 NOT ゲート (Controlled-NOT) （図 6）制御 NOT ゲートはビット間の相互作用を行う．制御 NOT ゲートは図 6 のように書く．• は制御ビットを表していて，制御ビットが 1 のときのみ，第2ビットに NOT を施す．

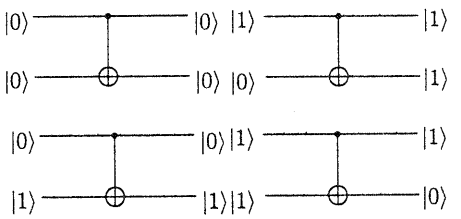

図 6: 制御 NOT

8 量子通信・量子暗号・量子情報

量子コンピュータは既存の計算モデルを含んだ素直なモデルだといったが，それは量子力学がそれだけ普遍的であることを言っている．実際，量子力学の情報技術での応用というのは，計算より前に情報通信の分野で始まっている．

より大容量の通信の実現を目指す量子通信では，Shannon の古典通信理論にとってかわる量子通信理論が確立されようとしている．そこでは，量子統計の推定・検定の理論の構築も基礎となる．量子通信路符号化定理もかなり成熟してきた．

また，観測による状態収束という量子力学原理に基づいて，完全に安全な暗号として量子暗号も研究されている．量子力学が保証するのは，もしそれが盗聴されていると，量子系の観測理論によって，状態が変ってしまい，盗み見たことを検出できるということだ．すなわち，現在セキュリティシステムが計算量仮説という現在のコンピュータに関する妥当な仮説に基づいていたのに対し，量子力学は原理として盗聴を検出することを保証する．

9 量子計算・通信のシステム実現

量子計算は，情報・物理にまたがる新学際研究分野であり，もちろん量子コンピュータの実物を作るには物理研究の推進が不可欠である．現在，NMR を用いて電子スピンを制御する既存の量子関係実験が使える環境を活用して，数量子ビットの実験ができている．また，今のコンピュータが集積化によって高度化を果たしてきたのと同じように，将来的には量子ビットを集積化することが必要で，その方向で期待されてる固体デバイスの研究も盛んで，超伝導ジョセフソン接合を用いた量子1ビット実現は2年ほど前に大きな反響をもたらしている．

量子通信・量子暗号の実験は，さらに進んでおり，実用も近いと思わせる．量子テレポテーションは，SF の瞬時移動と似た命名がされているが，量子状態の遠隔移送や量子回路への応用が考えられている．また，共通鍵暗号システムを支えるための鍵配送を安全に行う量子暗号実験も行われている．

10 量子計算から量子情報科学へ

量子力学では，その観測の理論や状態の記述が日常の常識と全く相容れない面があり，一見不可解な理論である．それに対して，情報通信理論，アリゴリズム論などの分野（以後，仮に情報科学と総称する）では，日常的直感がわりと素直に反映されて理論が構成されている．では，量子力学的な観測理論と状態記述に基づいた情報科学はどのようなものになるかというと，この問は情報科学の裾野を広げる上で

も，また量子力学の基礎から見直す意味でも，非常に興味深い問題となる．この様な問題を扱う一連の研究を，量子情報科学と呼ぼう．

量子コンピュータの実現を考えたとき，それは新しいデバイスの開発だけで済む問題ではない．量子コンピュータはその基本原理から熱的なノイズに極端に弱く，これはデバイスの精度向上だけで克服できるとは到底思われない．実際，Shor のアルゴリズムの提案からブームの到来までいささかの間があるのは，物理学の専門家達がこの点に強い懸念を示したからだともいえる．熱の効果を考えると，メモリーの保持すら難しい．それに対して Shor は，コンピュータの構造に少しゆとりを持たせてやれば，ある種のノイズに対抗してメモリーを保持することができることを示した．これは，古典通信理論の誤り訂正符号の量子版であり，量子誤り訂正符号とよばれ，現在，最も研究が盛んな分野の１つとなっている．

誤り訂正符号に端的に現れるように，量子コンピュータの実現のためには，物理的な研究だけでなく，より実現が容易な構造を開発することが重要である．例えば，簡潔で作りやすい回路の研究は回路最適化とよばれており，コンピュータ科学の重要な一分野である．また，システムを精密に制御する一連の方法は，古典系では制御理論として体系化されている．ノイズに対抗するための研究が通信理論の一分野であることは，先にのべた通りである．また，何でも現在のコンピュータでシミュレーションしてものを設計・検討する時代で，量子計算を既存コンピュータでシミュレートすることも実現への近道である [8]．つまり，量子コンピュータ科学はもちろん，量子情報理論全般を広く，そしてインターラクティブに研究することが量子コンピュータ実現のための必須である．

また，量子コンピュータが実用化したとして，その効率的運用の研究にコンピュータ科学の発展が必要なことは自明であると思われる．特に，アルゴリズムの開発は最も重要である．量子コンピュータは，在来型のコンピュータができる計算はすべて実行できる．しかし，量子コンピュータの方が飛躍的に高速になるアルゴリズムは，実用的なものに限ると，数えるほどしかない．このままでは，高コストの量子コンピュータは暗号解読専用として，特殊な目的に使われるに止まってしまう．量子パワーを活用した新アルゴリズムの発見が必要であり，それが実現に向けての気運を盛り上げるためにも役立つ．

11　おわりに

この量子情報科学からの量子計算の研究は，まさしく量子計算の科学の１つの本質をついている．もちろん，量子計算の科学のもう１つの軸は物理的に量子コンピュータを実現することであり，これらは車の両輪として，互いに相乗効果を与えて進んでいくものである．ちょうどこの 10 月から科学技術振興事業団の ERATO 量子計算機構プロジェクトで，量子情報科学の面から光を軸に物理へも手を広げた５年プロジェクトが立ち上がったところである [2]．そこで是非とも量子情報科学での新しいコンセプトを提示したいと思っており，ご支援を賜れば幸いである．

参考文献

[1] D. Deutsch, “Quantum theory, the church-turing principle and the universal quantum computer”, Proc. Roy. Soc. London, Vol. A, No. 400, pp. 97–117, 1985.

[2] ERATO Quantum Computation and Information Project: http://www.qci.jst.go.jp/

[3] R. P. Feynman, “Simulating physics with computers”, International Journal of Theoretical Physics, Vol. 21, pp. 467–488, 1982.

[4] L. K. Grover, “A fast quantum mechanical algorithm for database search”, Proceedings of 28th ACM Symposium on Theory of Computing, pp.212-219, 1996.

[5] J. Gruska, “Quantum Computing”, McGrawHill, 1999.

[6] 細谷暁夫, “量子コンピュータの基礎”, サイエンス社, 東京, 1999.

[7] P. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer”, SIAM Journal on Computing, Vol. 26, pp. 1484–1509, 1997.

[8] 徳永裕己, 長井歩, 山崎智弘, 今井浩, “量子計算汎用シミュレーションシステム,” 第３回量子情報技術研究会, 2000.

[9] C. P. Williams and S. H. Clearwater, “Explorations in Qunantum Computing”, TELOS, 1998; 邦訳: 西野哲朗, 荒井隆, 渡邊昇訳, “量子コンピューティング,” シュプリンガー・フェアラーク東京, 2000.