フレッシュマンに贈る量子計算の概略と基礎

―量子計算の考え方と量子ゲートのイメージを中心に―

小竹茂夫
Shigeo KOTAKE
（機械工学科　Department of Mechanical Engineering）

(Received September 1, 2005)

Abstract

This is the general introduction especially for the beginners on quantum mechanics and quantum information. Different from the other textbooks, this article emphasizes the image of quantum phenomena, such as superposition, and image of quantum calculation. Especially, basic concept of quantum mechanics , quantum calculation and quantum gate are explained here.

Key words: quantum computer, quantum gate, superposition

1. はじめに

量子コンピューターがどんなものであるか，その具体的な形を与えたのは，英国で宇宙論を専門にするドイッチェ（Deutch）であった．彼はなぜその着想を得ることができたのか？それについては，一冊の本が雄弁に語っているが，結局，彼自身によれば，「自分が，”多世界宇宙論”を信じているから」であるらしい．多世界宇宙の存在の真偽はともかくも，ある世界像の，それも従来の常識的な世界像とはまったく異なるそれについての真摯な思考の態度は，これまたまったく新しい創造を産みだすものらしい．数々の量子コンピューターと量子情報の理論が，数名の革新的な研究者達によってのみ進められてきた訳も同じ所にあるのだろう．量子コンピューターの研究を押し進めるには，多少とも従来の立場からは”非常識”とも思われる態度が必要なのかもしれない．（日常生活にこれを当てはめてもらっても困るが…．ちなみにドイッチェの顔写真からは，英国紳士的な気品が感じられる．）

ドイッチェの提案後，あまり省みられることのなかった量子コンピューターのアイディアは，時を経て，ショアー（Shore）による因数分解の高速アルゴリズムの可能性が示されると，大きな反響となって研究のブームを作った．十年ひと昔とは良く言ったものである．今では，日本でも多くの研究者達が，この分野に興味を注いでいる．十年前には，情報工学における量子力学の重要性を語っても，見向きもされなかったのが，最近

では，初年度の教科書すら発行されおり[1-4]，少しずつだが量子論の重要性は，広く認識されるようになってきている．もちろん，コンピューターへの応用が高まったことは，他のどれだけの分野への波及効果があるかは言う間でもないだろう．

もっとも，量子コンピューター自身の実現はまだまだ遠く（ひょっとすると数百年のオーダーで遠い），至急を要する産業分野の技術とはとても言えない．しかし，量子力学が理論思考の世界にも，理性的に入ってきたことを真摯に受け止めれば，今までの常識では得られなかったアイディアが，この分野を核に発展する可能性は否めない．思考する基盤を大きく変えることは，新たな世界像を築くことになるからである．

著者は，材料の分野の出身であり，どちらかと言うと，具体的な”もの”を対象に研究することが多く，”もの”に入る前の抽象概念を対象にするソフトウェアーやアルゴリズムを前に，当惑と躊躇の連続であった．そんな”ど素人”が，わざわざ専門を外したところで解説を試みたの訳なので，専門科が書くものとは，強調する点も議論する内容も自ずと違ってくる．ひょっとすると著者の思い込み違いもでてきてしまうかもしれない．

あえて誤謬を恐れずに，本報告をまとめるのは，むしろ新しい分野であるこの”量子コンピューター”が，従来の専門の枠に留まらない新規な分野であり，情報系から物理系，材料系まで含む幅の広い分野の進展があって始めて実現する総合物であるからである．（この点は，従来の古典コンピューターも同じであろう．）本分野は，また未だ発展途上にあり，今後，多くの人が独創性を発揮する必要がある．これまでに多くの解説書を目にするに至ったが，日本における研究者の多くが情報系に偏っていることを反映してか，この分野の基準で解説がなされていることが多く，筆者の様な分野からは敷居の高いのが現状である．その中で，本報告は，初学者向けに，厳密さよりもイメージを大切にし，具体的な話しも多く入れることにより，より”もの”に近い分野の人も”量子コンピューター”が何であるのかを理解する助けになればと思う．つまり，量子力学についても十分な知識がないことを前提とした量子コンピューターの基礎を理解するための入門書であり，表現もいささか砕けた感じで書いたことを御容赦願いたい．

現在までの”量子コンピューター”の発展を担ってきたドイッチェにしてもショアーやグローバー（Grover）にしても，本業（？）は，宇宙論やCADのエンジニアなど，それぞれ異なった専門を持つ人々であり，共通の興味があったこと以外にどのようなつながりがあったのかは疑問である．今後，日本においても，第二のドイッチェ，ショアーが現れることを願い，これから量子力学および量子コンピューターを学ぶ人に何らかの参考になれば幸いである．

2．今なぜ量子コンピューターか？

2-1．夢を語る ― SF（サイエンス・フィクション）の世界が現実にやってきた―

近ごろのインターネットはちょっとした最新現代基礎用語の様相である．分からないことがあると goo（http://www.goo.ne.jp）を検索してみると良い．全世界のホームページに登録された最新用語の使用法が五万とでてくる．データー収集ロボットが全世界のリンクをくまなく探索・整理しているので，１，２ヶ月の遅れはあるものの貴方の書いた文章も検索上に引っ掛かる．

ちなみに「量子」と「コンピューター」のキーワードで検索してみると，研究者の他にSF（サイエンスフィクション）での使用が出てくる．例えば，子供達に人気のウルトラマン・ガイアでは，怪獣の出現は光量子コンピューターで予測されており，それを開発した天才少年・少女達が，地球防衛団として活躍する．量子コンピューターは，未来の最先端技術であり，怪獣や正義の味方と同じ世界の代物である（図1(a)）．

「世界中の有能な少年少女の天才科学者たちによって組織されたものが「アルケミー・スターズ」である．ここでは光量子コンピューターによって根源的破滅招来体と呼ばれる〈人類と地球に及ぶ危機〉

が予測されていた.」「ワームゾーンから出現した怪獣ゾーリムは, ヴァージョンアップしたガイアによって撃退された. しかし, 光量子コンピューター<クリシス>が暴走したことに, 関係者はショックの色を隠せなかった. そして『根源的破壊招来体』の意志によって汚染されていた<クリシス>は, すべての接続を解除され, 凍結されることになる.」

(a) 子供向けTV番組　ウルトラマン・ガイアより

「実験室における"スター・トレック"テレポテーションの成功

英国の物理学者の画期的な発明によって, 真の量子テレポテーションが初めて実現した. この革新的な実験において, 国際的な科学者チームは媒体を介在せずにフォトンの量子状態を移動させる事に成功した.「この実験で, 我々は光ビームを 1m テレポートした. 理論が実践に使え, 距離は問題ではない事がわかった」とウェールズ・バンゴア大学の電子工学／コンピューター・システム学部のサムエル・ブラウンシュタイン博士は語っている. 量子テレポテーションは人気のあるSFテレビ番組"スタートレック"で有名になった移動技術に類似しており, いずれも一つの場所における物理的存在物の完全な破壊と, 別の場所での復元が含まれて いる.」

(b) イギリス大使館　ビジネス情報より

図1　SFの世界が現実にやってきた

一方, 映画やTVで人気のスタートレックでは, 宇宙船から目的地への移動を転送装置によって行う.「beam-up!!」で昨年のアメリカ・サイエンス界の流行語対象となった量子テレポテーションは, この映画で人を瞬時に送り込む「転送」が実は実現可能であることを明らかにしたものであり, イギリス大使館では, 自国のこの研究の成果を画期的技術の例として紹介している（図 1(b)）. Scientific American の最新号の特集は, 量子テレポテーションで, 人が転送される装置図まで載っていた. SF まがいの技術を大まじめに自慢するところなど, サイエンスを産んだ国らしく, 日本人の我々にはまねのできないところである.

ここまで書くと, いったい何が研究で, 何がフィクションなのか分からなくなってくる. 近ごろの物理系の学術雑誌は, サイエンス・フィクションまがいの話しが目白押しである. 生物系の話しが, 今にも新薬に役立ちそうな堅実な発見が次々になされているのに対して, 物理界は, 浮いた話しが多い. やはり物理は終焉[5]なのかな？と思ったりもするが, 従来の古典力学を飛び越えたところの量子力学への橋渡しが, 今進行しているのだろう. フィクションの夢が, 現実になりつつある, 少なくとも科学的・理性的にこのことが証明されつつある, そんな分野なのだろう.

日本では, ともすると ”サイエンス＝堅実・実証 ”の観があり, あまり大風呂敷な話しをすることは少ない. それに比べてアメリカとイギリスでは, フィクションめいた話しを大まじめに議論しており, 世間もそれを楽しんでいるかの観がある.

2-2. でも, やっぱり役に立つ ― 活気づく研究現場

現代の科学は, 科学・技術という言葉通り, 自然の仕組みの裏に応用が必然のように待ち構えている社会である. 応用がなければ, どんな発見も見向きもされないが, 一度その有用性が認知されるや, 莫大な資金と人が, 資本主義, 市場経済の名のもとに流れ込んでくる. 役に立つことばかりを強調することは, 知を愛する意味からは, 残念な気もするけれど, 職業としている以上, しかたがない.

フィクションめいた頃の量子コンピューターは, ドイッチェさん達の変わった試みとしてあまり世間受けはしていなかった. それが, 1994 年のショアーの発見以来, 量子コンピューターの実用への可能性は, 一挙に押し上がった. 現代の電子マネーのセキュリティは, 素因数分解の計算時間が桁数に応じて指数関数で増加する

性質を応用したもので，30 桁の素因数分解は現在の最速コンピューターで宇宙の寿命の百倍（1 兆年）近くかかる．ショアーの示した量子アルゴリズムは，これを数時間のオーダーにしてしまうのだから，周囲が驚いたのも無理はない．これに負けない絶対に解けない暗号を送る手段を作る方法も，量子暗号として開発されつつあり，量子の応用が花盛りなのがこの分野である．

そんな背景もあってか，日本でも，大学を始め，企業の研究者がこぞって研究を始めた．いったい，1994 年以前はどうだったのだろうか？といぶかしくなる．これ以降の量子計算分野での歩みを簡単に図にまとめた（図 2）．雨上りの後の筍のようとは，このことだろうか？（ちなみに，筆者など，この枠の中にも入れてもらっていない後発の研究者である．筍の後の雑草か？）

1999 年には，NEC の研究者による量子コンピューターの成功（といっても 1bit）を大々的に報じた（朝日新聞）．学生や市民の会話にも登り，専門外の人も知るところとなり，一挙に市民権を得たようだ．日本でも各新聞で取り上げられるようになったのはこの頃で，一挙に量子コンピューターは”役に立つかもしれない”という期待が高まったのだろうか？米国での量子コンピューターのフィーバーぶりは，日本とは比べものにならないようだから，遅く始まった国内の動きを笑うわけにはいかない．むしろ，米国のまねではない，独自な研究成果が上がることを期待したい．

1980年 Benioff (Argonne National Lab.)
「古典チューリング機械にできることは量子系にもできる」
1982年 Feynman (Caltech)
「量子系は、古典チューリング機械以上の能力があるかも知れない」
1985年 Deutsch (Oxford)
「量子チューリング機械の基本概念を定式化」
1994年 Shor (AT&T)
「大きな整数の効率的な素因数分解アルゴリズムを提案」
1995年 Deutsch (Oxford)
「２種類の基本ゲートの組み合わせでユニバーサルな量子計算の原理化」
1995年 Monroe (NIST)
「イオントラップによる2bitの制御NOTゲートの実現」
1995年 Kimble (Caltech)
「量子電気力学キャビティーによる2bitの制御NOTゲートの実現」
1996年 Grover (Bell Lab.)
「データ検索アルゴリズムの発見」
1997年 Chuang (IBM) and Jones (Oxford)
「NMRによる2bit量子計算機の実現！！」
1998年 Kane (New South Wales)
「Si半導体中のPの核スピンによる量子計算機のアイデアを提案」

図2 量子計算の歩み

2-3. 人と機械の間 ― 人間に近いコンピューター

ともすると量子コンピューターの期待される成果には，高速ばかりが強調されがちである．計算機の高速化は現在に始まったことではなく，PentiumIIIが PentiumIVに格上げされるのと違わない印象を持たれるかもしれない．しかし，脳や意識の問題を考えている研究者の中には，これにそれ以上の期待を寄せている人々がいる．

依然として機械と人間との間には埋められない溝がある．それは，意識の問題であり，認識の問題であり，創造性の問題である．以前の人工知能の研究者達は，コンピューターの計算速度やメモリーが，現在の人間の能にまで近づけば，機械にも人間に近い行動が可能となると信じている向きがあった．しかし，数年置きに一桁ずつ処理速度が向上し，メモリーが人間の脳に近くなった今でも，この問題を解決する手段は見出せてはいない．人の意識や脳を研究している科学者達の中には，このハードな機械では解決のつかない脳の問題を量子

力学的な効果によるものと考える人々がいる．冶部真理さんや保江邦夫氏は，脳における量子場の可能性を示唆し，ペンローズやハメロフは脳の思考そのものを量子現象に帰結させようとしている．（これらの真偽は，筆者には分からないが，最近，多くの本に紹介されている話題ではある．）

このアナロジーから，量子コンピューターは，従来の古典コンピューターにはまねのできない意識の問題を解決しうると考えている訳だが，意識を持つコンピューターを作る技術ができたとしたら…これは単に速いコンピューターを作るところではないとんでもないブレークスルーである．ただ速いコンピューターではない，何かがあるとにらんでいるのだろう．

ただ，脳自身が量子力学的であるかどうかは不明だし，未知のものに未知の能力を期待するのは，無理なからぬ事だが，ちょっと飛躍し過ぎかもしれない．小生が考えるに，指数関数的に場合の数が増加するNP(Non-Polynomial)問題に適応した場合，量子コンピューターには，有効なアルゴリズムが存在する可能性があり，この種の問題が，画像や音声認識，制御など，機械が人間的振る舞いが要求されるヒューマロイドの分野には多数存在することは確かである．

2-4．　量子コンピューターの近未来

コンピューターの能力段階を，俗に，第一世代，第二世代…，第五世代と名付けて国家プロジェクトが進んでいる．この中で，ひと昔前のニューロコンピューターやファジイコンピューター，光コンピューターのように，一時騒がれて，ブームの去ってしまった観のある研究も多い．（ブームと重要さは，必ずしも一致しないのだが…）量子コンピューターが，一時のブームにすぎない流行のものか，はたまた革命的な計算手法の萌芽であるかは，まだ誰にも分からない．

筆者は，この問いに関しては，”YES”とも”NO”とも答えうると考えている．すなわち，すぐに実現可能ではないハードウェアーの状況を考えると，当分（ひょっとすると百年のオーダーで），この計算手法を使いこなす事はできないであろう意味から，現状においては，一時のブームにならざる得ない．（常温超伝導のブームは去っても，その可能性と重要性はなくなっていないのに等しい．）また，古典力学が量子力学でとって変わられたような大変革が，思考の中でも起こっている意味から，量子コンピューターは，人の思考法の可能性を大きく変える画期的な存在であると思う．量子コンピューターが与える意味について，この後の章で，もう少し詳しく議論する事にする．

3．量子コンピューターの意味

3 1．実在の”粒子性”と”量子性”

前章では，量子コンピューターを取り巻く最近の状況について言及したが，この章では，量子コンピューターというトッピックの意味について考えて見たい．近未来における実現可能性が難しい事を考えると，経済的とか産業的意味を述べるものではないが，現実を見越した取り組みについては，最終章において述べたい．

量子論は，２０世紀初頭に生まれて，2000 年の 12/5 には，満百歳を迎えるが，その物理学に及ぼした意味は，従来の科学を古典物理学と呼び，量子論の関わる分野を現代物理学と呼ぶ事からも明らかであろう．簡単に言えば，古典物理においては，現実に存在する”もの”は，観測する，しないに関わらず，粒子もしくは波であり，現代物理においては，観測以前の”もの”は，波動関数（粒子であり且つ波）であり，観測以後は，粒子である．（量子力学では，観測の話しはタブーである．諸説入り乱れて，誰もが納得するコンセンサスが得られていないのである．）この世界は，”もの”のみからなっているとする唯物主義が，近代科学の常識とすれば，この”もの”の概念が大きく揺らいだのが，量子論の登場だったのだ．

この”もの”を哲学の難しい言葉で，”実在”と呼ばせてもらうならば，”実在”が，日常の概念である”粒子”ではないといった魔化不思議な主張が量子力学であり，これを半ば手法として認める事により，様々な物

理現象の説明（Why?）がなされてきたのが，これまでの量子力学の主な成果であった.

従来のコンピューターを古典コンピューターと言わせてもらうと，どんなに最先端コンピューターがミクロな半導体技術の結晶であっても，これらのコンピューターは，多くの”0”か”1”からなるbitの集まりである.（詳しい説明は，後でおこなう.）つまり，古典コンピューターは，”ON”か”OFF”かしかないスイッチの集まりであり，どの時点で見ても，スイッチ（”粒子”）は，”ON”の位置か，”OFF”の位置かに実在する．量子コンピューターは，この粒子的描像であったスイッチの実在を波動関数として取り扱ったものであり，覗かない（観察しない）限り，スイッチの位置は，”ON”と”OFF”との重ね合せ状態にある.（つまりどちらとは，決まってはいない.）さらに，スイッチの実在は，波動の振幅であり，絶対値の和が１になる粒子性も同時に備えた，変わった波である．この波は，振幅の他に位相を持ち，波動関数と呼ばれる複素数で表現される．コンピューターを構成する実在を”粒子性”から解放し，新たに”波動関数”として捉え直し，”量子性”としたのが量子コンピューターであり，ここに革命的意味合いがある.

3-2．量子論の範疇　（”WHY”と”WHAT”）

大学生ともなれば，量子力学の話しを，どこかで聞いた事があるに違いない．きっと，複雑な偏微分方程式を解いた記憶から，難しくて，敬して遠ざけたい科目であったかもしれない.（かく言う筆者も，学生時代はちんぷんかんぷんだった．経路積分ともなれば，今だってどこまで分かっているか怪しい.）ようやく求まった波動関数から，原子や分子，金属や半導体の性質が次々と明らかにされていく訳だが，手続きの複雑性と取り扱う現象の非日常性から，その有用性をかみしめるまでにはなかなかならない．ミクロな現象を理解するには，この学問が必須であることは分かっても，所詮，分野が限られるので，化学や半導体を専門としない限り，”関係ない”と思って良かったはずだ.

事実，日本の多くの工学部でも，化学系・電気系と物理工学を除いて，機械，建築，情報系の学科で，量子力学を教えるところは少ないし，これを必須と考える教授陣も少ない．機械的な様々な現象は，それぞれ材料パラメーターとして整理されており，その現象がどこから来るのかに注意する必要はないし，波動関数を解いて家を設計する必要もない．情報系も扱うコンピューターが，古典コンピューターだけであれば，当然，古典物理による理解しかいらないだろう.

人の科学に関わる行動には，大きく分けて３つのものがあると言われている．一つは，科学そのものであり，自然現象を理解しようとし，その理由を明らかにする”説明知”であり，英語で言うと”WHY”にあたる．次に，工学の分野に近いが，科学で明らかになった自然の仕組みを応用して，何か”もの”を作る行為であり，英語の”WHAT”にあたる．さらに，この”もの”を作る手段として，やはり科学的法則を応用する”HOW”があるが，”WHAT”と”HOW”は”WHY”よりは，応用と言う点においてより近いかもしれない．日本人自身が，創造性が無いと卑下するのは，この中の”WHY”と”WHAT”で，”HOW”については，”遂行知”的観点が強く，得意な分野である事は間違いがない.（この”説明知”的分野が弱いことから，日本の大学教育について考える向きもあるのだが，筆者自身が，日本の教育典型であることから，あまり偉そうなことは言えない.）

先程，量子力学が生まれて百年と書いたが，その中心は，自然現象を理解する”WHY”中心の営みであり，その理解から半導体や原子エネルギーなどの応用は進んだものの，誰かがそれを明らかにしてしまえば，後は古典物理で設計・製作する世界である．唯一，nmでの物質設計が可能な半導体を除けば，まだまだ真に”量子力学”を理解して，何かを作ったり，作り方を考える応用（工学）の分野には，至っていないのかもしれない．量子力学の受け持つ範疇は，まだまだ”WHY”の領域が大きく，現状では”WHAT”や”HOW”の領域に力を発揮している訳ではないのだろう.

3-3．科学と技術の歴史的展開 ― 自然理解から道具へ

人間の歴史を振り返ってみると，中世における知の停滞の後に始まった科学も，様々な経過を経て今日に至っ

ていることが分かる（図3）．最初の200年間は，ニュートン（Newton）やデカルト（Descartes）に始まる自然の理解に勤めた時代であり，このころ科学の基礎が出来た．つまり，WHYの時代であった．産業革命に始まり現在に至る次の200年は，科学の産業への応用と科学自体の深まりが，同時進行していった時代であり，科学的知識を”もの”やその”もの”の生産手段へと応用し，それ自体を目的とした”WHY”と”WHAT”の時代であった．ガリレイ（Galilei）一人が，例え，光の不思議を理解し，望遠鏡を作ったとしても，真に光学機器が発展したのは，科学が産業への強力な推進力であることを大衆が認めた19世紀になってからであった．

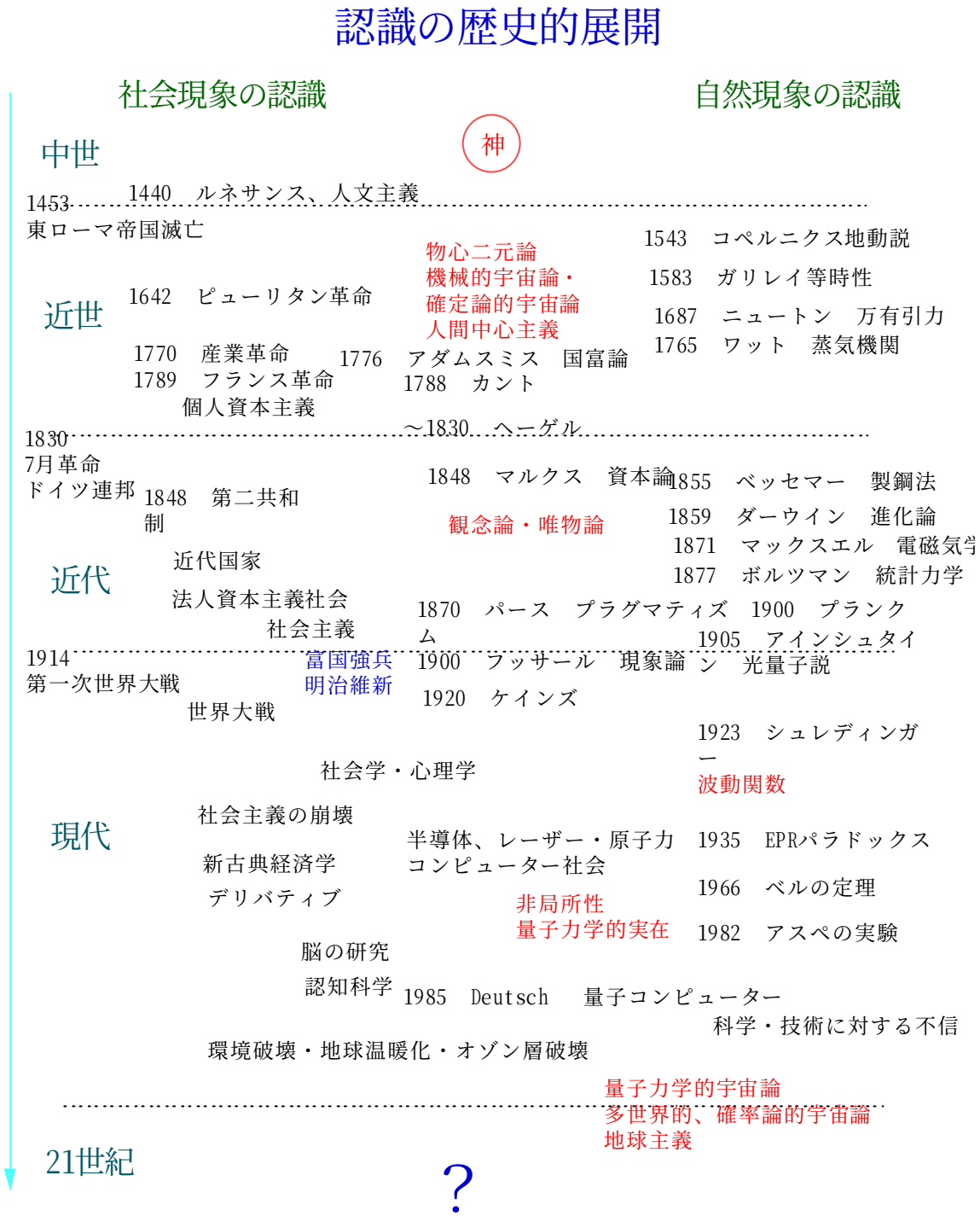


図 3　認識の歴史的展開

どんなに科学的進歩が早くなって，昨日見つけた事実を今日には応用しようとする今の時代においても，それが大きな変革であった場合には，それを一般の社会が理解し，使いこなすようになるにはそれ相当の時間を要する．今までの科学と技術の歴史が，それを物語っている．量子力学が登場してきたのは，この１世紀のことであり，現在の現象解明中心の立場は，古典物理が産業革命以前にとってきた傾向と良く似ている．

近年，生物における DNA が，生物をゲノムの観点から理解するためばかりでなく，遺伝子治療，遺伝子組み換え作物に代表されるゲノムそのものへの応用と変化してきているように，量子論も自然を理解するためばかりではなく，量子論そのものを使った応用が芽生えつつある．つまり，”WHY ”から ”WHAT ”への変化がおこりつつある．

詳しくは後で述べるが，量子コンピューターは，波動関数のもつ超並列性と干渉性を兼ね備えた，従来の古典コンピューターにはない特性を持ちうる．そのため，組み合せ問題など指数関数的に場合の数が増加する場合には，しらみ潰しにしか対処できない従来の手法は無力であり，量子論的アルゴリズムが現在唯一の確定的解を示しうる．この計算機を動かすアルゴリズムが量子力学にしたがう以上，これが関わる解析，シミュレーション，制御，管理，検索，決定，推論といった広い人の “ もの ” の考え方の中に，量子力学を必要とすることになる．調度，三段論法である演繹法のように，量子力学による道筋を通して解を得る思考法を要求する．量子力学での原理が，人の考え方の中に入って来ることにより，”自然理解 ”から ”思考法 ”の広がりの中へ，一歩足を踏み入れたのが，今回の ” 量子コンピューター ” の意味であると考える．

以上の話しをまとめると，筆者が考える ” 量子コンピューター ” の重要性とは，

１．計算の担い手を ” 粒子 ” から ” 量子 ” に変えることにより，計算原理に量子論を取り入れることを可能にした点，

２．人間の思考に量子論的な，超並列的，干渉的思考過程を取り入れることを可能にした点，であった．

この点において，” 量子コンピューター ” は，従来のコンピューターを陵駕する革新的な技術でありうる．

次章以降では，この革新的なコンピューターの概念について，より具体的な話しを進めたい．

４．量子の不思議な振る舞い

この章では，量子コンピューターを説明する前に，量子そのものの持つ，古典的描像か理解できない不思議な性質を紹介する．ここでは身近な量子粒子である ” 光 ” の現象に沿いながら，量子コンピューターの働きを具現する具体的な実験も交えて，説明を行いたい．本報告では，実験のしやすさから ” 光 ” を取り上げるが，同じ量子粒子である ” 電子 ” や ” 原子核（のスピン）” なども，有力な量子コンピューターの候補であり，これらの量子性の違いについては，少し後で議論したい．簡単な概念としての量子論の説明であり，イメージを大切にしているため，厳密性にはやや欠けるきらいもあるが，ご容赦願う．詳しくは量子論の専門を参照すること．

４-１．忍者赤影，分身の術

筆者が子供の頃（ずいぶん昔だが），忍者のヒーローが活躍するテレビ番組があり，主人公の赤影は，時折，分身の術を使った．西遊記の孫悟空も，毛を抜いて，フッと吹くとたちまち多くの分身が現れて，どんなに強い，多くの敵ももろともしなかった．時たま忙しい時，分身の術が欲しくなるのは，筆者だけではあるまい．実は，量子コンピューターの特徴の一つに，この分身の術（超並列性）がある．古典コンピューターにも並列計算機が存在することから，” 超 ” の字をつけたものと考えられる．まったく魔法のようであるが，光について言えば，日常に経験していることである．

今，図４に示すように，光源から絞りを通った光が，レンズの通り，平行光になった場合を考えよう（当然，光源の位置はレンズの焦点距離でなければならない）．光源で，一点に存在していた光は，その後，広がって

平行光の様々な位置に，等しい確率で存在する．可視光で，100W の光の場合，約 10^{21} 個の光子からなるが，光が $1m^2$ に広がった場合，原子の大きさあたりに約１個の光子が存在することになる．

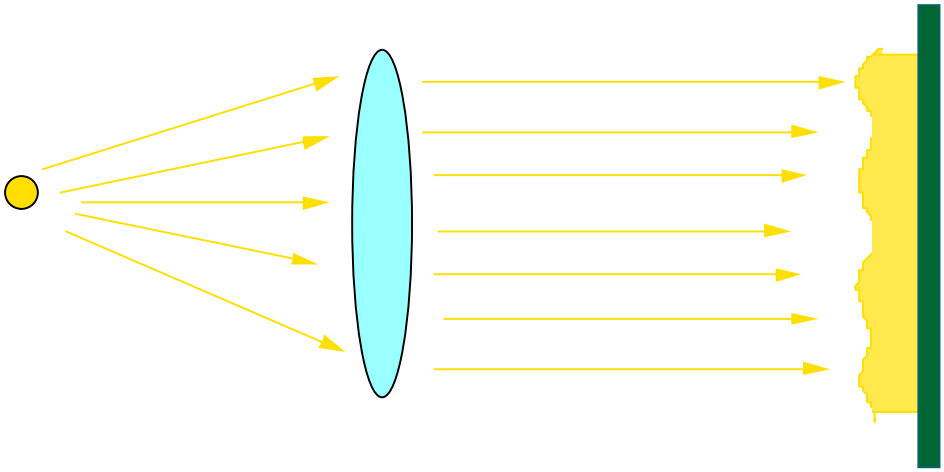


図 4　光とレンズによる分身の術

多数の粒子を考えた場合は，これで良いのだが，問題なのは光子が一個の場合である．普通に（古典力学的に）考えると，光源から出た１個の粒子は，どこかの経路を取り，レンズを通った後で，平行光のいずれかの位置のどこかに一つ存在している．なくした鍵も消滅してしまった訳ではなく，結局はどこかに一つ存在しているのと同じである．ところが，実際は，平行光のどこかに存在している訳ではなく，どこにも同じように同時に存在している，というのだ．（これが分身の術の由縁である．）

それでは，光を波と考えて，一つの光子が，さらに細かく分かれて，原子の大きさ当り，$1/10^{21}$ 個に分かれたらと思うのだが，光の持つエネルギーや運動量は，一光子以下に分けられないことが，実験事実として知られており，一つの粒子であることには変わりはない．この広がっているけれども一個である，不思議な粒子を量子と呼び，この粒子の振る舞いを記述した学問を量子力学と言うは，ご存じのことと思う．これをどう考えるかについては，”観測理論”と呼ばれて様々な解釈があり，未だ確定している訳ではないのだが，無難な線でコペンハーゲン解釈で述べると，

１．一個の光子は，位置と時間の関数である複素数（波動関数）として空間（時間）的に広がっおり，その振幅の二乗は，その位置での存在確率を表す．よって，任意の時間での波動関数の空間積分は１である．

２．観測（例えば光がスクリーンに当たることにより，光の位置を知られる）されると波動関数はある実在する一粒子に収束する．

ということになる．つまり，実在が量子である”あの世（観測以前の世界）”と粒子である”この世（観測した瞬間の世界）”の二つの面を持つことになる．

量子コンピューターにおける計算過程は，観測しない”あの世”の状態で，波動関数のままおこなわれるため，この解釈問題はある意味では無視して通り過ぎることができる．そのため，レンズで光を広げるように分身が容易であり，以下それぞれの位置にある値（状態）が対応すると考えれば，一つの粒子は，たくさんの値が重ね合さった状態であり，まさに超並列を具現化する．

一般に量子力学では，この重ね合わさった波動関数をベクトルで表現する（式（**））．100 の状態を重ね合わせたとすると，100 の成分をもつベクトルで表される．このベクトルは，状態を表す波の振幅を表し，各座標の基底ベクトルをそれぞれの状態とすると，各成分の振幅の二乗は，それぞれの状態の存在確率を表す．つまり，$\psi=a_1\phi_1+a_2\phi_2+a_3\phi_3+a_4\phi_4+\ldots+a_{98}\phi_{98}+a_{99}\phi_{99}+a_{100}\phi_{100}$ とすると，ϕ_1 の状態を取る確率（ρ_1）は，$\rho_1=|a_1|^2$，ϕ_i(i=1～100)の状態を取る確率（ρ_i）は，$\rho_i=|a_i|^2$ となる．当然，全体の存在確率は変わらないので 1 であり，$\Sigma|a_i|^2=1$ となる．

4-2．波動関数の操作

こうして並列化した（広げた）波動関数を任意のアルゴリズムの中で操作できなければ，計算はできない．つまり，波動関数の変換が必要になる．一般に，ある１つの入力を操作して別な１つの出力を得る方法を”関数”と呼ぶが，ここでの関数は，たくさんの状態が重なりあった一つの波動関数を操作し，やはり一つの波動関数を得るもので，従来の関数の意味とはちょっと違う．つまり，従来の関数に波動関数を代入することはできないから，別な工夫がいる．

広がった（状態が重なりあった）波動関数を変換して別な波動関数にするには，調度，光を空間ごとに異なる屈折率を持つフィルターを通すのに似ている．その他多くのレンズや位相板，プリズムなどの光学素子が，光を吸収することなく位相や空間密度を変化させるが，これも光の操作法の具体例である．光は，広がった波動関数のまま，変化し形を変える．

波動関数をベクトル化したように，量子力学における波動関数の操作は，行列 A で表される（式（**））．

$$\psi' = A\psi$$

ただし，どんなに波動関数が変化しても，吸収のない場合，絶対値の２乗の和（空間積分）が，１であることは変わらず，このことから A のユニタリー性が現れる．つまり，

$$\rho = \psi'^{*}\psi' = (A\psi)^{*}(A\psi) = \psi^{*}A^{*}A\psi = \psi^{*}\psi = \rho$$

が，成り立つことから，波動関数を変換する行列は，$A^{*}A=\mathrm{I}$(単位行列)の条件を満たす必要がある．これを満たす行列を，数学用語でユニタリー行列といい，

$$A^{*}A = I = A^{-1}A$$

より，$A^{*}=A^{-1}$ となる．*を付ける操作を”共役”と呼ぶが，これは，行列を転置（行と列を入れ換える）して，複素共役をとる（p=a+ib のとき p^{*}=a-ib とする）ことによって得られる．つまり，行列 A は，その i 行 j 列の成分 a_{ij} について，複素共役を取り（a_{ij}^{*}），これを新たに j 行 i 列の成分とした行列 B をつくると，この B は A の逆行列になっていることになる（$B=A^{-1}$）．

もうちょっと具体的に言うと，2x2 の行列 A について考えると，その成分を以下のように表した場合，

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

A^{*} は，次のように表され，

$$A^{*} = \begin{pmatrix} a^{*} & c^{*} \\ b^{*} & d^{*} \end{pmatrix}$$

これが，A の逆行列と等しいことから（$A^{*}=A^{-1}$），

$$A^{*} = \begin{pmatrix} a^{*} & c^{*} \\ b^{*} & d^{*} \end{pmatrix} = \frac{1}{ad-bc}\begin{pmatrix} a & -c \\ -b & d \end{pmatrix}$$

となり，これを満たす行列がユニタリー性を満足する．

波動関数を変換する操作は，このエルミート行列 A で表され，決して任意の変換が可能ではないことにご留意いただきたい．よくよく考えると，ベクトルの大きさ（原点からの矢印の長さ）を変えない変換には，原点周りの回転と原点を通る面に対しての鏡映（面対称に移すこと）が挙げられるが，行列の成分が実数の場合，エルミート変換は，この回転と鏡映の組み合わせに限られることが分かっている．波動関数を操作するイメージは，この原点周りのベクトルの回転や鏡映であり，この変換によって得たい解の方向へ波動関数を導くことになる．解が，ψ_{50} であった場合，変換によってψをψ_{50}にまで導き，ここで観測をすることになる（図5）．

$$\psi = a_1\psi_1 + a_2\psi_2 + a_3\psi_3 + a_4\psi_4 + \cdots + a_{99}\psi_{99} + a_{100}\psi_{100}$$

-> $\psi=a_{50}\psi_{50}$

ここで，a_{50}=1 であることから，観測の結果，求めたい値であるψ_{50}を得ることができる．この得たい解に収束させる変換方法が量子アルゴリズムの全てであり，因数分解について解を求める方法を見つけたのがショアーである．

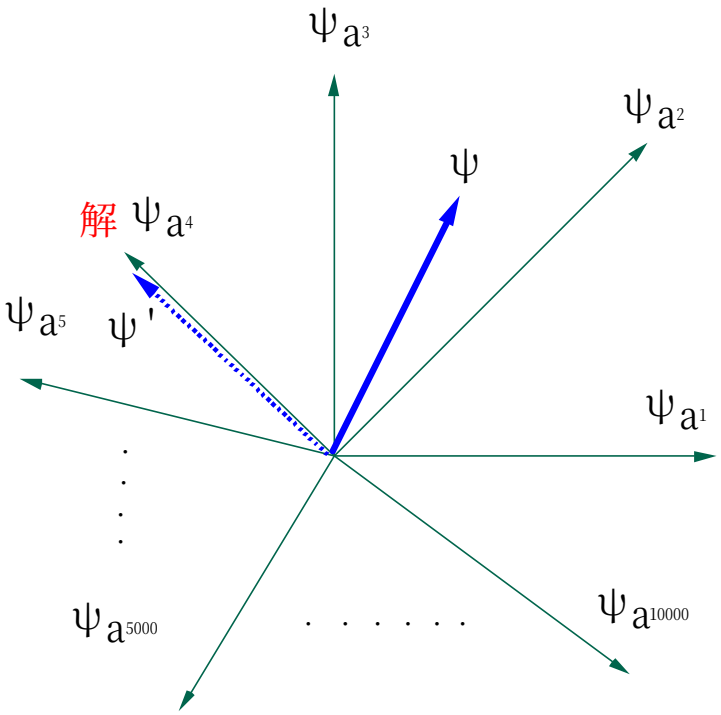
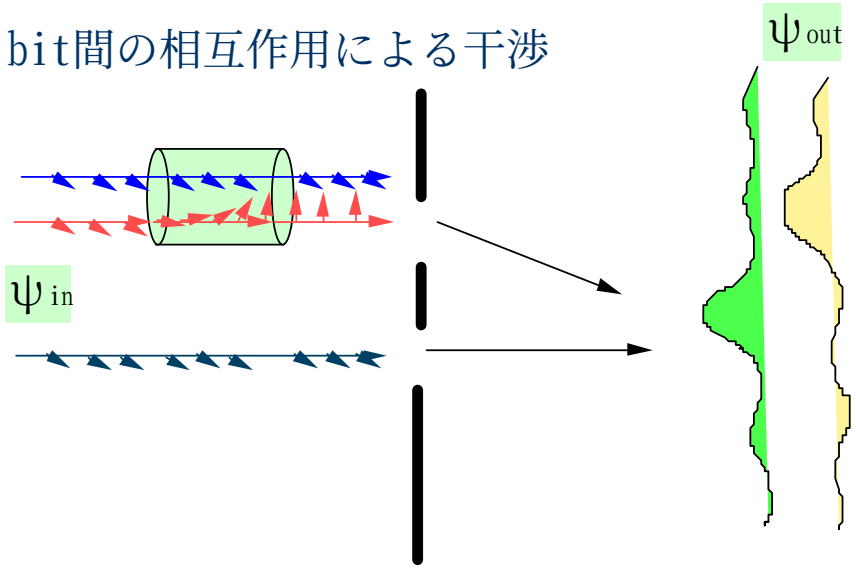


図5　ユニタリー変換で解を得る

通常の光の実験におけるこの種の変換は干渉と呼ばれており，分身の術も，解への収束もこの干渉によって得られる（図 6）．広がった光をスクリーンに映すまでに，どのような光学素子（この中には，現状において，最先端技術である制御 NOT の変換も含め手）を配置するのかが，具体的量子コンピューターの問題となる．量子系の配置を考える量子アルゴリズムについては，本文では述べないが，別の機会に概説を披露したい．



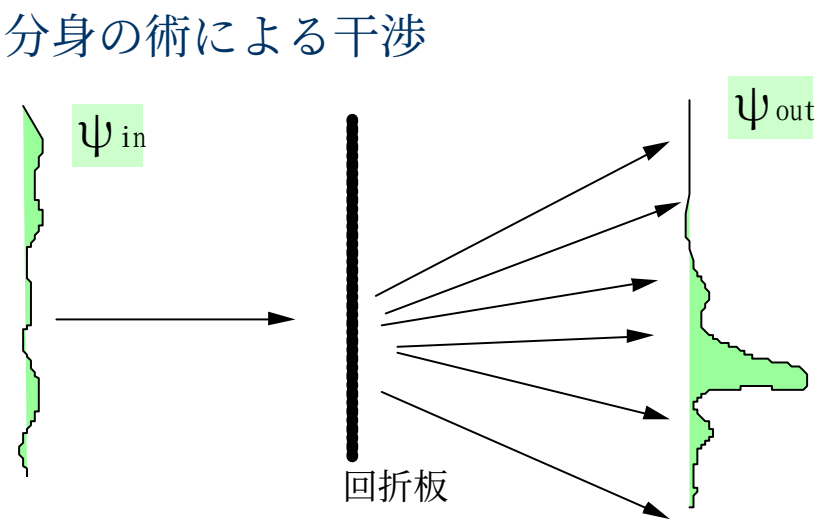


図6 量子コンピューターの操作とは？

5．量子コンピューターとは何か？ ― 何が従来の計算機と違うのか？―

本章では，量子コンピューターの詳しい説明に入る前に，量子コンピューターと，従来のコンピューターとの振るまいの違いについて議論したい．実は，従来のコンピューターを動かすアルゴリズムには，確定論的アルゴリズムと確率論的アルゴリズムがあるのだが，その点についても明らかにしたい．

5-1．迷路の中の宝探し

日本の民話 ”舌切り雀 ” では，物語の最後に，雀からの贈りものとして，大きなつづらと，小さなつづらを差し出される．後の方をとった ” 良いおばあさん ” は，中から宝物がザクザク出てきてお金持ちになったし，先の方を取った ” 強欲いじわるばあさん ” は，中からおばけが出てきて，ひどい目にあう．そんな例をあげるまでもなく，人生にはたくさんの選択（職業，学校，結婚相手，ランチのメニュー，etc.）があり，A か B かの決定を迫られる．選んだ後では後悔はきかない．

今，宝物の入った部屋が一つあり，何とかこれにたどり着きたいとする．現在いる場所の目の前には，左右にドアが二つあり，いずれかのドアの先に，この宝物の入った部屋がある．確率は 1/2 であり，運がよければお金持ちだが，そうでない扉に入った場合は後戻りができない．この選択でうまくいけば，一生遊んで暮らせるだけのお金が手に入るとしたら，挑戦する価値は十分にあるだろう．

しかし，そんなうまいもうけ話しはないもので，ドアの向こうには，また二つの左右にドアがあった場合はどうだろう．そしてその先にも，その先にもドアがあり，その度に，左右どちらかの入り口を選択しなければならないとする．そして，これらの選択を全てうまくした時にのみ，宝の部屋にたどりつけるなら，宝を手にする確率は急激に減少する．宝物にたどり着くまでのドアの階層の数が 8 である場合，最終的な部屋の数は，2^8=256 個で，宝物を手にする確率 (p) は p=1/256=0.4%以下になる．またドアの階層が 16 ある場合は，p=1/65536 0.001%となる．さらに階層が 100 ある場合は，最終段階での部屋数は 2^{100} 10^{30} となり，宝物を手にする確率は，全宇宙の星の中から，地球を見つけるよりも難しくなる．これでは，百回ドアを開ければ宝物が待っているかもしれないと誘われたところで，望み薄であり，宝探しをする元気もでない．余談だが，そうして考えてみると，今までの人生で選択してきたことの数の多さを考えれば，どれだけ違った選択をした自分があったかと思うと気が遠くなる．

5-2．古典的世界での宝探し

こうした状況で，どういった宝探しの行動がとれるかというと，古典力学下での世界では，自分も粒子的実

在であり，一度に一つの扉しか選択できないことから，

１．右端から順番にしらみ潰しにドアを開けて，一つ一つの部屋を探る，か，

２．それぞれのドアのところで，コインを投げて，表がでた場合は右，裏の場合は左というように，その場まかせに進む，但し，一度通った道は決して選ばない（なぜなら，既に宝がないことは分かっているから），

のいずれかの方法が考えられるだろう．

宝の隠し場所がまったくランダムであった場合には，１，２の方法とも，宝を見つける効率の良さは変わらない．100 扉の階層があった場合には，100 回ドアを開けて奥までたどり着くのに１分を要したと考えて，宝が見つかるまでに必要な時間の期待値は，全体の部屋数の半分について試した時だから，1 分x2^{99}=5x10^{29} 分

1x10^{28}時間　1x10^{24}年，つまり１兆年の　１兆倍かかってしまうことになる．今の宇宙の寿命が，150 億年だから，その約 10 兆倍ということになる．

順番に探そうとする相手の行動を見て，それとは反対の位置に宝物が隠された場合，１の方法では，永久に答えが見つかりそうもない．一方，２の方法では，どこに隠されようとも，最初から宝物が見つかる可能性がない訳でもない（ものすごく小さな確率ではあるが…）．一方，宝を見つける確実な法則（宝の地図）を手にしていれば，１の方法では，すぐに見つかるだろうが，２の方法では地図も無駄になる．１の方法は，経路があらかじめ決まっている決定論的アルゴリズムであり，２の方法は，経路は確率的に決まる非決定論的アルゴリズムである．両者ともにアルゴリズムに従うのか粒子的実在であるため，古典的操作であることには違いない．筆者の専門である材料の分野におけるシミュレーション法でいうと，前者の例は，分子動力学であり，後者の例としては，モンテカルロ法があげられる．ある目的においては，確率論的方法は，決定論的方法よりもはるかに早く答えを得ることが出来るが，詳しくは，コラムを参照されたい．

ちなみに従来の古典コンピューターで高速計算をする方法として，並列計算機が知られているが，これは自分の他に，アルバイトを雇って宝探しをするのに似ている．よって，例え，1 万人のアルバイトを雇って仕事を分担しても，掛かる時間が人数分だけ少なくなるに過ぎない．つまり，1x10^{24}年が，1x10^{20}年になるだけで，時間の掛かる効率の悪い方法であることが分かる．これだけの時間，多くのアルバイトを雇ったことを考えると，給料に掛かるお金が，宝の価値を上まわってしまうことにもなりかねない．事実，並列計算機は，高速だが高額で，その値段の割には，現在 10 万円以下で買える家庭用のパソコンの何万倍も仕事量を期待できる訳ではない．

今回例に上げた宝探しの問題は，チェスや囲碁，将棋のようなゲームや多くの人の配置を考える人事の問題，画像から特定の像を見つけだす問題，迷路問題，巡回サラリーマン問題，さらには任意のポテンシャル中の最小値の決定問題など，日常にいくらでも転がっている．このように場合の数が指数関数的に増加する問題では，通常の古典コンピューターは無力であり，この点に現在の機械の限界があり，人と”もの”とを大きく分け隔てている．

確かに，コンピューターの演算速度は，人の比ではなく，何万倍，何億倍も速い．そして時間と共に更に速くなってきている．しかし，考える道筋は地道であり，一つずつこなしていくよりは他に手はない．従って，場合の数が指数関数的に発散するある種の問題には，その高速性も太刀打ちできない．一方，演算スピードが遅いはずの人は，この種の問題にも，短時間で最良に近い答えを出すことが出来る．人とコンピューターを分けるもの，これについての答えはまだなく，コンピューターにおける研究分野における最大の難問の一つである．本報告の話題の中心である量子コンピューターは，必ずしも解ではないにしても，そういった問いに何らかの回答例を与えてはくれるだろう．

５-３．量子的世界での宝探し

この困難を極める宝探しも，量子の世界ではちょっと違う．粒子的実在も量子の世界では波動関数という波の振幅である．前節でも述べたように，波動関数は分身の術を持ち，容易に超並列を実現出来る．現実に qu-bit

をたくさん並べることは，現状では困難だが，理屈上では，波動関数はどこまでも小さく分かれることが出来る．

例えば，後でも述べるが，光の偏光を量子状態として利用した場合，光学異方性を持つプリズムを通った光は後で，二つの偏光の重ね合わせ状態となる．回折格子を利用した場合には，（この場合は偏光ではないが）もっと多くの状態に一度に分身する．今，宝探しのそれぞれのドアの前で，二つに分身して，左右それぞれの部屋を選択したとする．100 層あるこのドアの列で分身を繰り返すと，一つの光子は，2^{100} 10^{30}個の異なる状態の重ね合わせとなる．そしてここがミソなのだが，これだけの数に分解するのに，たったの 100 ステップしか要していない．一つ一つの場合をしらみ潰しに調べていては，気も遠くなるような時間を要していたことが，同じ数だけの分身が登場すれば，いっぺんに問題解決しそうではないか！古典アルゴリズムの場合と同じように考えると，解を得るまでに 1 分しか要しないことになる．10^{24}年と 1 分，しかも階層の数を増やせばこの差はますます大きくなり，量子アルゴリズムの意味することが，従来の古典コンピューターの並列とは威力が桁外れにスゴイことが分かるだろう．”超”並列の”超”の由縁は，この辺にあるのだろう．

ここで，このままではそうは問屋が下ろさない．取らぬタヌキの皮算用である．確かに，分裂した波動関数の一つの状態は，無事，宝までたどり着くだろう．ところが残りの 2^{100}-1 個の状態は，空の部屋に着いてしまう．つまり単に分裂したままでは，波動関数の大半は，空の部屋にたどり着く場合を示す．よって，この波動関数を観測した場合，宝の部屋に光子を発見するのは，古典的確率アルゴリズム同様，10^{30}分の 1 となる．これではわざわざ波動関数を用いる意味がない．

つまり，量子アルゴリズムにおいて，計算の高速性を可能にするには，分身の術だけでは十分ではない．何らかの方法で，解（宝物のある部屋）近くで，波動関数の振幅を増大させなければならない．そのためには分身した（広がった）波動関数をフィルターに入れて，干渉の結果，答え近くに振幅のピークを作らなくてはならない．

それでは，どのように波動関数を操作するか？実はこれが量子アルゴリズムそのものであり，求める解により，それぞれの操作を考案する必要がある．現在のところ大きくは３つのアイディアが発表されているのみであるが，量子コンピューターを構成する qu-bit の理解と従来までの光学や電子における量子現象のアナロジーから，次なるアルゴリズムの出現が期待できる．量子コンピューターのハードウェアーが，膨大な資金を必要とする国家プロジェクトであるのに対し，量子アルゴリズムは，紙と鉛筆で出来る個人研究の領域であり，このためより斬新なアイディアが求められている．我々，地方大学が，少なくとも物理的に可能なテーマはソフト的な分野であり，どう波動関数を操作して見せるかであろう．

コラム１． 決定論的アルゴリズムと確率論的アルゴリズム

確率論的アルゴリズム（ランダムに調べる）が，決定論的アルゴリズム（順番に調べる）よりも，優秀である場合は，選挙における得票数を推定する場合を考えれば分かる．今，有権者数十万人の選挙において，A 候補者と B 候補者のどちらが当選しそうかを予想したい．一つの村から一件ずつ順番に調べる場合（確定論的方法）と色々な村や街からランダムに調べる場合（確率論的方法）を考える．一般に選挙予測は，一部の調査結果から全体の傾向を探るものであり，調査数が少ないほど，調査精度が正確であるほど，良い調査法であると言える．

ここで重要なのは，支持者の分布で，A 候補者の支持者も B 候補者の支持者もまったくのランダムであった場合，両者の方法に差は見られない．一方，それぞれの村や街によって支持者層の分布が異なる場合，順番に調べる方法では，なかなか全体の傾向を知ることはできない．例えば 1000 人の村全員が A 候補者支持であった場合，1000 人調べてもその他の土地の情報は得られない．それに対し，ランダムに調べる場合には，支持者の分布に影響を受けることはないのは，直感的に分かるであろう．実際，選挙の調査会社は，ランダム無作為に調査を行っている．この方法の良い点は，調査結果の誤差も見積もれ

る点にあるのだが，詳しくは統計の本を調べて欲しい．

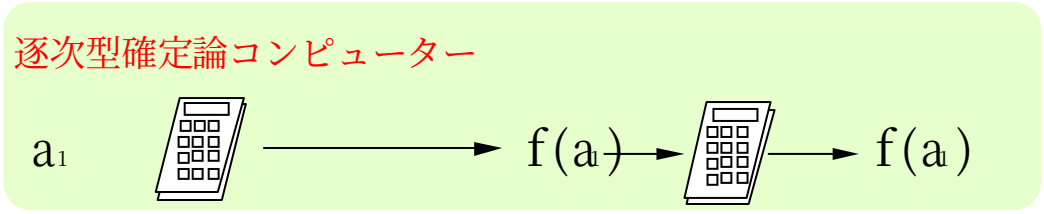
6．量子コンピューターとは何か？　-量子コンピューターのイメージ-

6．1　並列コンピューターと超並列コンピューター

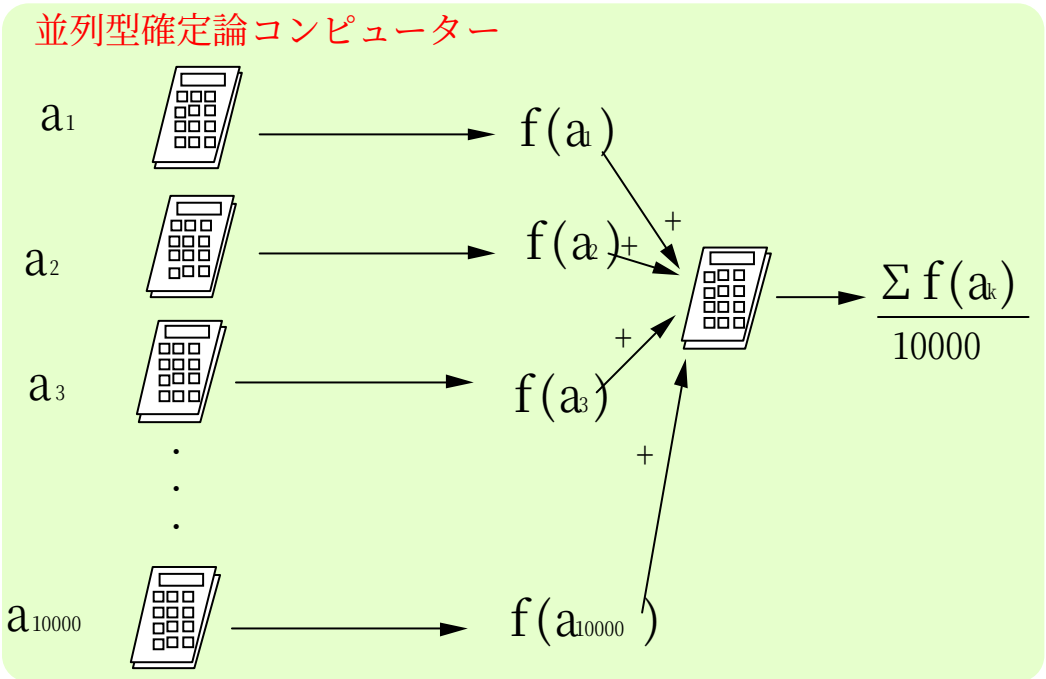
量子コンピューターとは何かと聞かれて，筆者はしばしば，従来のコンピューター（本解説では，古典コンピューターと呼ぶ）と量子コンピューターとの違いを挙げる．従来のコンピューターといっても，イメージは様々なので，ここでは，最も古い古典コンピューターのひとつである”電卓”を例に挙げる．

今，教師Aが，数学の試験をおこなったとする．成績の出来不出来は問題の難しさとも関連するため，クラスの平均得点を得ることは，非常に重要な作業になる．学生数が40人のクラスであれば，ものの1分で学生全員の得点を合計し，それを人数で割って平均得点を得ることが出来る．一回の計算に1秒を要したとすれば40秒強の時間が掛かったことになる．十分有限な数での計算が日常の我々の考察範囲である．

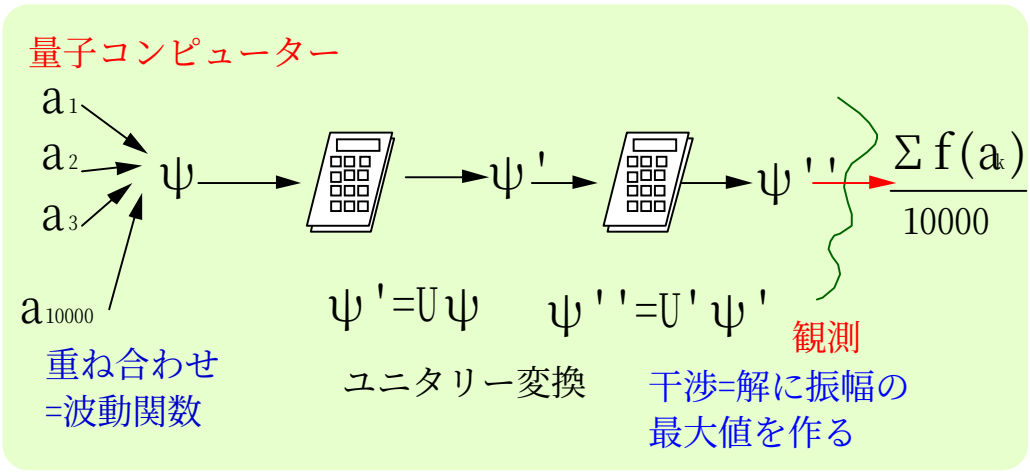
一方，全国一斉に行われる大学受験の共通テストでの得点 の平均を考えたとしよう．受験者はざっと40万人であり，一人で計算すれば，同じ時間で計算が続けられたとしても，100時間の労力を要する．これが世界全体に広がるテストとすれば，100億人に対し，約10000時間近くの労力が掛 かり，寝ずに約1年の仕事が要求される．近頃は，電卓などではなく，最速のWindowsに搭載されたExcelで計算する場合が多く，このような心配は無用かもしれない．しかしこの場合も，入力は何らかの方法で逐次的におこなわれており，時間に対する本質的な要請は変わりはない．現在，100MHzのコンピューターを駆使すれば，単時間で済むかも知れないが，計算数に比例して所要時間が増加することは免れない（図7(a)）．



(a)



(b)



(c)

図7. 電卓，並列電卓，超並列電卓(量子コンピューター電卓)による平均値の計算

一方，古典コンピューターには違いないが，近頃はやりの並列コンピューターで計算した場合，例えば，10台の機械を並列に運転したとすると，時間は 1/10 に短縮されたにすぎない．つまり，努力はそれ程報われない．世に言う並列コンピューティングはその程度に過ぎない（図7(b)）．
一方，平均値を一回で算出する方法がある．電卓でいえば一つの値を代入するだけで，全ての合計が得られるようなものである．そのためには，入れる値は，全てのデーターを重ね合わせた波動関数にする必要があり，よって波動関数を波動関数のまま計算する量子コンピューターが必要となる（図7(c)）．

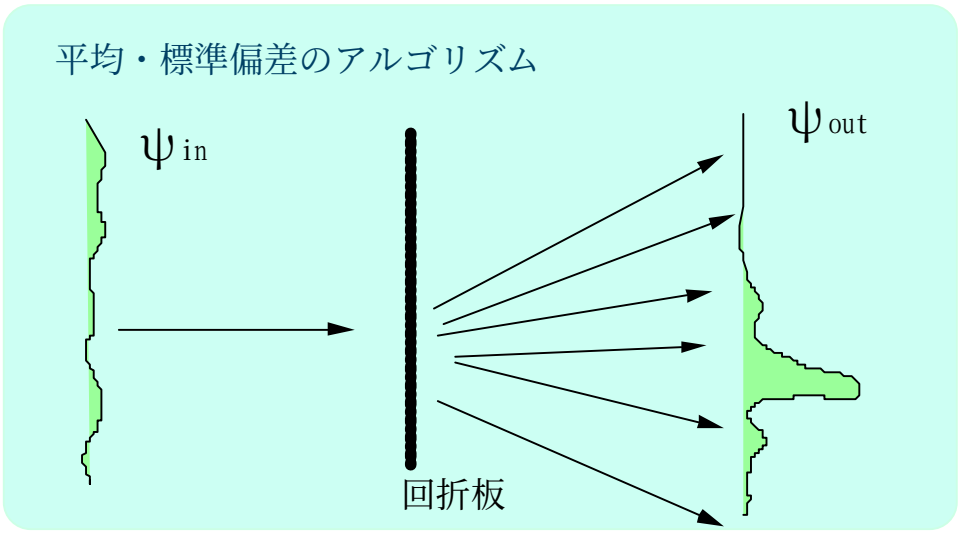


図8 回折板を通る光子による平均値，標準偏差のアルゴリズム

それでは，そのような計算は実際，可能であるのか？実は，量子粒子による単純な平均の例は，身近にあり，例えば，透明板に筋を付けた回折格子を通る光がそうである．光の波動関数は例の分身の術で回折格子全体に広げることができ，それぞれの場合の数がいかに増えようとも一回で光は総ての場合をつくす．広がった光の波動関数は，たとえ１個の光子であっても，全ての格子と相互作用する．広がった光は，それぞれの回折格子を通った後，各格子の間隔と回折方向に対応した位相遅れをもつ光へと分身する．つまり最初にそれぞれの回折格子一つ一つ分身した光子は，再び各々方向に分身することになる．そして最後に回折格子から離れたスクリーンには全体の格子からスクリーンのある点に向かって飛んできた光が再び重ね合わされる．

ここでは詳しくは述べないが，これこそは二段フーリエ変換であり，スクリーンの光子の存在確率（もしくは，光の強度）は回折点の間隔のフーリエ変換となっている．表れた１次回折点と０次回折点の距離 d は，丁度，回折格子のそれぞれの間隔の平均 x の逆数になっており，（$x=1/d$）一次回折点の一回の観測から，データーの平均が得られることになる（図８）．

フーリエ変換は，後から述べるような 2qu-bit からなる量子コンピューターにおいては，制御 NOT を実現せざる得ず，実現が難しい操作となるが，レンズや回折格子からなる光学回路においては，位相回転からのみなる単純なアルゴリズムで成り立つ変換であり，いとも簡単に，超並列計算ができてしまった．ウソのような話しだが，これでも立派な量子計算ではある．（汎用性がない分，量子コンピューター とは言い難い．足し算や引き算しかできないそろばんをコンピューターと呼ばないのと同じである．）

６．２　粒子的コンピューターと波動的コンピューター

前章では，別れ道の多い中での宝探しについて古典コンピューターと量子コンピューターの場合について議論してきた．この時は，量子計算が場合の数が爆発的に増える場合について極めて有効である点を強調してきた．実は，前節の平均を求める計算について考えると量子計算がそれ以上の働きをしている事が見て取れる．スクリーンに現れる回折点の光は，一つの回折格子を通った光子がたまたまそこにたどり着いた訳ではない．多くの回折格子を同時に通った光が，スクリーン上で重ね合った結果が現れる．これは，従来のコンピューターが時刻毎に決まった位置を通る粒子的な振る舞いをしているのとは対照に，同じ時刻にも複数の場所に広がっており，その後も各地点から球面波状に広がりながら伝わっていく波動的な振る舞いをするコンピューターであると言える．

波動は，重なるものの量が複素数であるため，振幅の大きさとともに位相といった方向性の情報を持ち，波動関数の重ね合わせとは，ベクトルの合成を意味することとなる．時には逆方向のベクトルを足し合わせるため，足し合った結果は必ずしも増加するとは限らない．

古典的な粒子の場合，その因果律を成り立たせる原因は，過去の一つの状態であり，原因から結果まで一つの流れを一個一個，個別に取り出すことが可能であった．つまり，一個一個，解析的に状況を分解し調べあげることが可能であった．ところが量子粒子の場合，スクリーンに現れた粒子の原因となる過去の状態は，回折格子の全体に広がっている．現在の一点と過去の一点を結んだだけの単純な因果律は成り立たず，これを解析的に切って取り出すことも不可能となる．

つまり量子計算は，単純に多くの場合を同時に処理できるだけの並列計算機とは大きく異なり，古典的因果律では成り立ちえない量子的因果律に則った，特殊な計算を実現させるとまさに超並列計算機であるといえる．筆者が不思議だと思うのは，こういった複数の事象が同時に影響しあう場合は，日常生活にたくさん経験されることである．それにも関わらず，また一方で，個人主義や解析的分析手法など個々の事象を区別して理解する古典的考えも根強い．この辺については，コラムで考察したい．

コラム２．　物理的理解の社会科学への影響

まさに驚くべきことだが，社会科学の多くは，自然科学をモデルとして成り立っている．個人といった概念も市民革命を迎える前の西欧啓蒙主義の中で，古典力学の粒子に人を見立てて産まれたものらしい．さしずめ経済学は，経済人というお金ポテンシャルのみによって動く粒子の多体系の振る舞いといったところだろうか．様々なパラメーターも線形化された空間の中で相互の独立・従属を扱われるにすぎない．

最近，量子理論をモデルに社会現象を取り扱おうとする試みがなされている．異なる要因から得られる状態を重ね合わせたまま考慮し，それぞれの要因をつながった全体として捉える．ゲーム理論にしても，相手の出方が自分の行動に影響し，またそれが相手の行動に影響を与える．とかく人間社会

の行動の多くは，独立事象として捉えられない点が多い．イギリスの D.ゾーハーは，量子論による社会現象の理解を押し進める先鋒隊であり，近年注目されている．

また，さらに，それが様々な社会問題を露呈しつつある人間の意識に自然とつながった生命としての東洋的な観点を思い起こさせてくれるきっかけとなることを望みたい．とすれば，今の古典力学的モデルを意識して生きる人間は，自然とも回りの人間とも切り離されて，さぞかし孤独だろう．

６．３　古典的波動コンピューターと量子コンピューター

前節では，粒子的な古典コンピューターと波動的な波動コンピューターの違いについて述べてきた．粒子性と波動性の違いは空間的な存在形式の違いのためか歴然としていた．一方，前回，コラムでも取り上げたように波動コンピューターとしては，光コンピューターが存在し，そこでも量子アルゴリズムとしてのゲートによる普遍化が，量子コンピューターをより進んだ概念としていることを説明した．しかし，古典的波動コンピューターである光コンピューターと量子コンピューターの違いを述べるには，これだけでは十分ではないので，粒子と波動の描像が出たところでもう少し，この点についても説明を加えたい．

量子が波動と大きく異なる点は，その粒子性である．つまり古典的波動はどこまでいっても，分解可能であるが，量子は，それ以上分解のできない最小の単位を持つ．そしてそれは，観測の際，得られる結果が確率となって現れることにつながってくる．古典的波動はどこまで行っても連続であり，一点に収束することはない．後から述べるショアーのアルゴリズムでは，広げた波動関数を，一部の観測によって絞りこむプロセスを折りこんでいる．古典的波動を絞りこむには絞りを入れることになるが，これでは絞りを入れるたびに振幅が減少していってしまう．

一方，観測による波動関数の収縮には，振幅のロスがない．これも観測による波動関数の結果であると言えよう．そして特に粒子的であるために，得られる結果が確率的になる点は，これによるアルゴリズムが古典的確率コンピューターにも似た複数回の試行の中から解にたどり着くといった演繹的アルゴリズムを構築する必要のない帰納的計算を可能にする．

この他にも，光コンピューターにはない機構として，制御 NOT 等による波動関数間のエンタングル化ができる点が大きな違いとして現れる．一般の古典波動は，線形であり，波動同士は独立に振る舞う．波動がエンタングル的な振る舞いをするには，フェルミ粒子的特質を波動関数に盛りこむ必要があり，実際の量子コンピューターでも苦労している点と言えよう．

６．４　量子コンピューターを構成する qu-bit

古典コンピューターは，2 進法における 0 もしくは 1 で表わされ，ON-OFF のスイッチとして振る舞う．このスイッチを並べ，アルゴリズムに従って，スイッチを動かすことにより計算が進むのである．一方，量子コンピューターは，波動のような複素数の振幅を持つこと，そして粒子的な最小単位を持つことを前２節では述べてきた．これはつまり振幅の絶対値が 1 である複素数である複素平面上の単位円 が 1 量子を表わす単位となることを意味する．この 1 量子を量子コンピューターでは，波動関数ψとして表わし，1qu-bit と呼ぶ．ψは回転する昔のテレビチャンネルのようなスイッチとして振る舞う．（あまりにも古い例えなので，アナログ時計の針と言った方が良いかもしれない）1 qu-bit が 12 時の方向に向いている時，ψ=|1>，3 時の方向に向いている時をψ=|0> とすると，6 時の方向はψ=-|1>，9 時の方向はψ=-|0>となる．一般に，|0>となす角がθの場合，ψ=cosθ|0>+sinθ|1>となる．もちろんθは位相である．

今，bit と qu-bit の意味を明確にするために，それぞれのイメージを例を挙げて説明したい．まず古典コンピューターの bit だが，これはコインの裏の時と表の時に相当する（図 9）．例えば前者だと 0 で，後者だと 1 を意味する．古典コンピューターとは，常にこれらの位置がいずれかに定まっている状態にあり，裏か表かに確定したコインが列をなして並んでいる．常に各状況は確定的であり，計算するとは，これらの表裏をある規

則にしたがって変化させることにある.

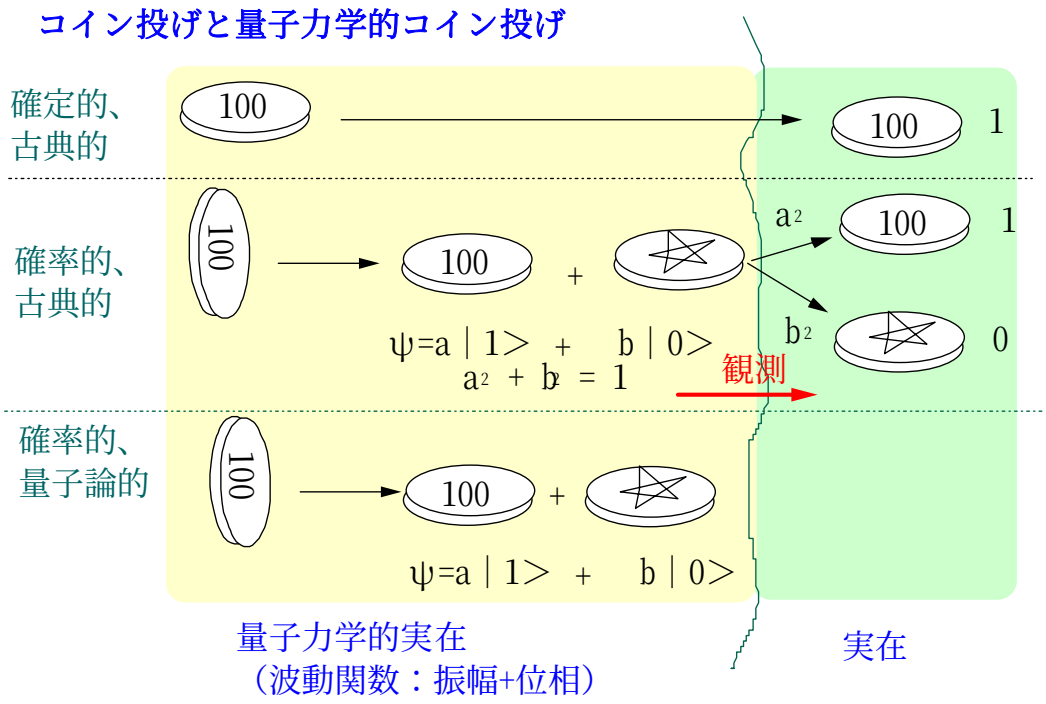


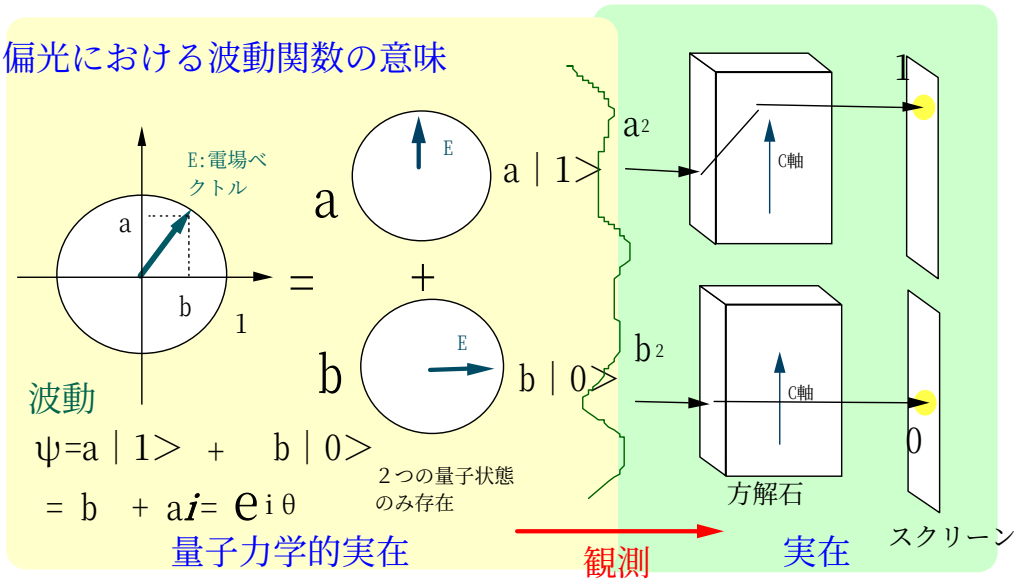
図9　古典的コイン投げと量子的コイン投げ

いま，計算中のコンピューターの箱を開けて中身のメモリーの様子をつぶさに観察できたとする．すると，何十億と並んだメモリーが0か1の状態にあり，刻々と計算手順（アルゴリズム）に従って状態を変化させている様子が観察されるに違いない．もちろんある時間で止めた時，全てのメモリーは確定的に定まっている．

一方，古典コンピューターを確率的（但し古典的）に扱う場合は，コインを投げて裏か表か確率的に決める場合に相当する．投げるまでは，コインの裏，表は定まっておらず，丁度，垂直に立っている状態であるとも言える．但し毎回コインが振られると，表か裏かに決まりその結果が後の展開に影響を与える．つまり後の状況に因果的につながっているのは，一つの状態だけである．その点が古典的であると言える．

この古典的確率コンピューターの箱を開けて覗いて見たとすると，任意の時間における何十億とある各bitは，やはり0か1かに確定している．ただし次にどの状態に移っているかについては，確率的にさいころを振って決めている．丁度，双六のようなものだろうか？振る前と振った後では位置は確定しているが，その関係は確率的なものでしかない．

一方，qu-bitは，古典的なコインでは表わせられず，例えば，光の最小単位である光子の偏光によって表わされる（図10）．量子コンピューターは，この光子一つが作るqu-bitが何個も並んでできたメモリーから成るコンピューターである．偏光は光の電場ベクトルであり，横波であるため，進行方向とは垂直な面内に2次元の自由度を持つ．この平面内での偏光状態の向きがbitの位相にあたる．光子は斜め方向の偏光を持つ場合，これは縦方向の偏光と横方向の偏光の重ね合わせ状態となっているが，各時刻でこの状態は重ね合わされたままに進展していく．よってそのbitの状態は，0や1と確定している訳ではなく，いずれの可能性も残したまま計算が進んでいく（図11）．



波動関数は、波（振幅と位相を持つ）　　重ね合わせ状態　　位相が消える 0 か 1か

振幅の絶対値の２乗は存在確率　$|\psi|^2=\psi^*\psi=a^2+b^2=1$

図 10　光子の偏光における量子的コイン投げ

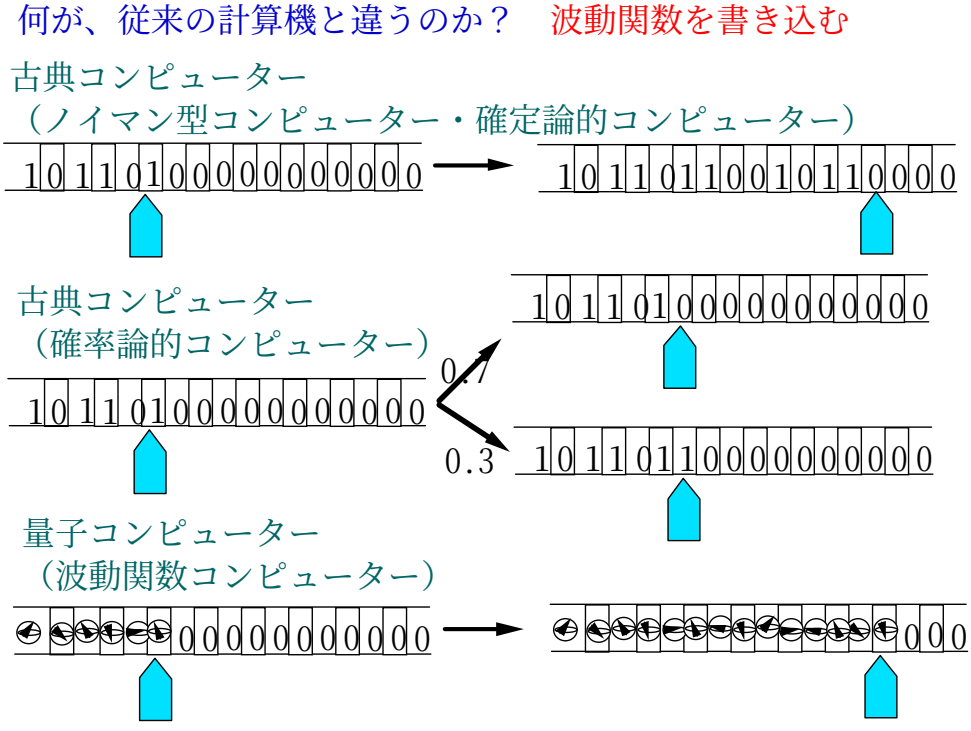


図 11　古典コンピューターと量子コンピューター

ここでもし，量子コンピューターの箱を開けて各 bit の状態を覗いたとしたらどうだろう．0 と 1 の重ね合わせ状態が観察されるのであろうか？ところがここで観測の問題が生じる．観測とは，0 であるか 1 であるかといった状態を見極めることであり，観測の結果が 0 と 1 の重ね合わせのままであることはできない．よって

観測した後に計算機の状態が変化してしまい，計算を続けることはできない厄介な代物なのである．量子コンピューターは計算結果が出るまで基本的には何人とも触ることは許されない．もっとも後から示すように計算途中でエラー訂正を行うことはできるが，これは観測のうちに入らない．部屋を覗いてしまっては鶴は恩返しが出来なくなってしまう．

コラム３．　光子の観測方法

それでは実際に光子の状態を観測する方法にはどんなものがあるのだろうか？光子の状態を観測するには，方かい石等，光学一軸結晶の光学異方面に光を入射させれば良い．偏光が０状態か１状態かによって伝播経路は異なることとなり，上か下かのいずれかに観測されることになる．方かい石の後に置いたスクリーン上の写真乾パンに塗られた塩化銀粒子と反応する光子は，１個だけであり，スクリーンに現れた後に重ね合っていることはできない．

なぜ，観測すると一つで，観測する前は重ね合っていて良いのか，これらの問題は，量子論 の観測問題という未解決問題とも関連しており，現在も完全な理解が得られている訳ではないため，こうであるという事実だけ述べるに留める．

６．５　qu-bit の重ね合わせが作る NP 空間

１つの qu-bit は２つの状態の重ね合わせである．３つの qu-bit は 2^3=8 つの状態を表現することが可能となる（図 12）．qu-bit の作る空間はひとつひとつの qu-bit が作る空間の直積空間を作り出す．よって，n 個の qu-bit の表わしうる空間の場合の数は，2^n といった爆発的に大きな数を表わすことが可能となる．それも n 個の qu-bit しか使わずにである（図 13）．

$$
\begin{aligned}
|\psi\rangle &= (\omega^{(1)}_0 |0\rangle + \omega^{(1)}_1 |1\rangle) \otimes (\omega^{(2)}_0 |0\rangle + \omega^{(2)}_1 |1\rangle) \otimes (\omega^{(3)}_0 |0\rangle + \omega^{(3)}_1 |1\rangle) \\
&= \omega^{(1)}_0 \omega^{(2)}_0 \omega^{(3)}_0 |000\rangle + \omega^{(1)}_0 \omega^{(2)}_0 \omega^{(3)}_1 |001\rangle \\
&\quad + \omega^{(1)}_0 \omega^{(2)}_1 \omega^{(3)}_0 |010\rangle + \omega^{(1)}_0 \omega^{(2)}_1 \omega^{(3)}_1 |011\rangle \\
&\quad + \omega^{(1)}_1 \omega^{(2)}_0 \omega^{(3)}_0 |100\rangle + \omega^{(1)}_1 \omega^{(2)}_0 \omega^{(3)}_1 |101\rangle \\
&\quad + \omega^{(1)}_1 \omega^{(2)}_1 \omega^{(3)}_0 |110\rangle + \omega^{(1)}_1 \omega^{(2)}_1 \omega^{(3)}_1 |111\rangle \\
&= \omega_{000} |000\rangle + \omega_{001} |001\rangle + \omega_{010} |010\rangle + \omega_{011} |011\rangle \\
&\quad + \omega_{100} |100\rangle + \omega_{101} |101\rangle + \omega_{110} |110\rangle + \omega_{111} |111\rangle
\end{aligned}
$$

$$
|ijk\rangle = |i\rangle \otimes |j\rangle \otimes |k\rangle
$$

図 12　3 qu-bit のつくる 2^3 個の直積空間

そして，ここからが重要なのだが，qu-bit が作る重ねあわされた空間が従来の古典コンピューターでは作れない指数関数的な場合の数を包含する状態を可能にする．この重ね合わせが実現する数の発散は，古典コンピューターの速度や並列化が進んだとしても，この発散する場合の数には追い付けない程の爆発的な数の増加である．これを理解するには，多項式関数（Polynomial function）と非多項式関数（Non-polynomial function）である指数関数の様子をイメージすれば良い．

量子コンピューターが持つ究極的な可能性は，この点に尽きるといっても過言ではないだろう．（量子テレポテーションなどは，もっと別な価値を表わしているのかもしれないけれど…）そしてこの点において，一般の古典コンピューターが到達できない問題に新たな可能性を示唆してくれるものと考えている．その一つは，人工知能問題への応用である．現代のコンピューターは，bit 数の上からは，既に単純な生命の脳と同じくらいのメモリー数を持つに至っている．しかしながら，生命の意識を模倣できるコンピューターには，未だ成功

していない.

筆者は，この問題の解決は，ひょっとすると量子コンピューターやDNAコンピューターといった今までのコンピューターにはない原理で動くシステムが必要ではないかと考えている．この点については，量子応用での来年度の研究計画に上がっており，その例としての報告が次回できるかもしれない.

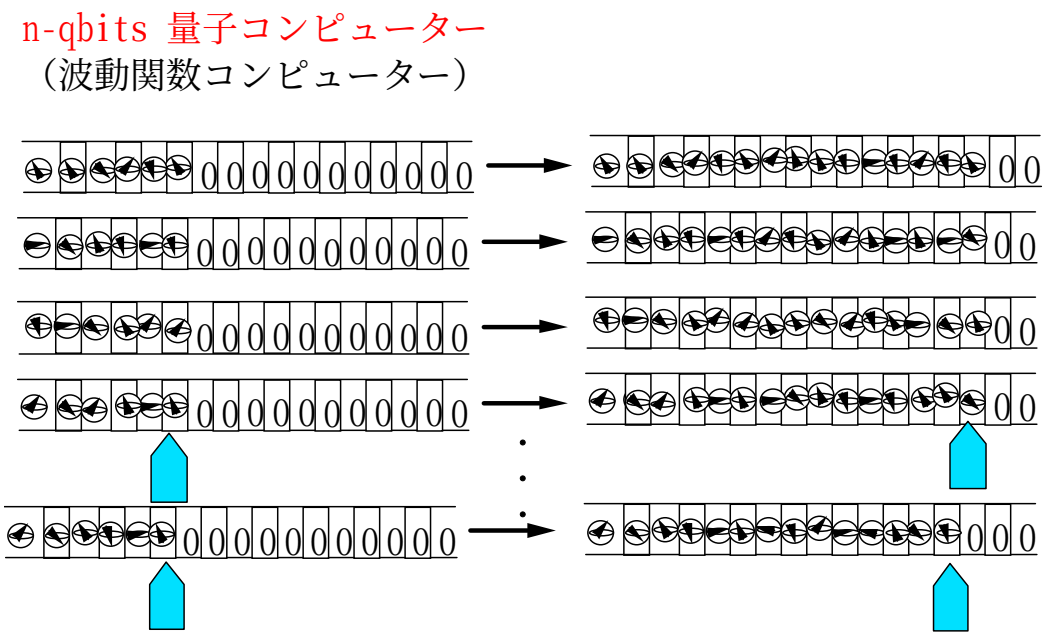


図13　n qu-bit のつくる量子チューリング機械

7　量子コンピューターにおける操作

7．1　古典コンピューターにおける演算

今までの章で，qu-bit が並んだメモリーからなる量子コンピューター のイメージが得られたと思う．これらのメモリーをどのように操作して，計算を行うかが次ぎなる問題となる．本書は，一般のコンピューターの説明をするものではない．また私本人も，情報科学の専門ではないので，この点は，簡略して説明する．詳細な議論は，情報科学の本を読んでもらいたい.

コンピューターの演算は，チューリングによってメモリーとそれを操作するヘッドの動きとして理解される．ヘッドとメモリーの状態からどのような操作を行うかを定めたものがプログラム（”前もって定める”という意味）であり，これによりメモリー上の演算が次々と進む．基本的な演算には，ADD，OR，NOR，NANDなどの論理演算と和差積商の算術演算からなるが，これらは基本的に2bitから1bitを計算するNANDゲートの組み合わせで作成できることが証明されている.

つまりNANDゲートにメモリーの結果をつなげて，計算が進んでいく．この回路内の信号は，0または1の状態で確定しており，信号の変化も回路が確定していることで決定論的である．ここでは詳しくは述べないが，複雑な算術演算も複雑なプログラムも，結局はNANDゲー トを組み合わせた流れである.

7．2　量子コンピューターにおけるqu-bit間の演算

それでは，量子コンピューターにおける操作とは何か？古典コンピューターの操作では，0，1のいずれかにデーターを変化させていく過程であったが，量子コンピューターでは，bit の位相の変化を意味する．bit の位相の変化によって，波動関数の絶対値は変化しないことからこの操作を可能にする演算は，ユニタリー変換であることが分かる．ユニタリー演算の定義は，変換されたベクトルの絶対値が変化しないことである.

ユニタリー変換とは，0，1の状態をそれぞれ意味するベクトル(1,0)，(0,1)を変換する行列で表わされることは，前回で説明した通りである．1bitのコンピューターにおけるユニタリー演算は，2x2の行列で表わされ，ユニタリー変換の定義から，求めた条件は，前回示した．一方，2bitや3bitの演算では，変換されるqu-bitの直積空間における成分が2^nで増加することから，それぞれ4つと8つとなり，これを変換するユニタリー行列は，それぞれ4X4と8X8となる．位相が特別な0とπ/2の場合，古典コンピューターの演算と同じになり，量子演算が古典演算よりも広い拡張概念であることが分かる．

量子コンピューターの曙を作ったドイッチェの業績は，このユニタリー変換をある特定のゲートの組み合わせで汎用に（ユニバーサルに）表現できることを証明したことにある．そのゲートとは二つあり，一つは位相回転ゲート（U_1），もう一つは，制御NOTゲート（U_2）である．これにより，この二つのゲートを可能とすれば，任意の量子アルゴリズムを組み立てることができる．任意のアルゴリズムを組み立てる手法を開発した点に量子科学の情報論への拡張があったといえる．

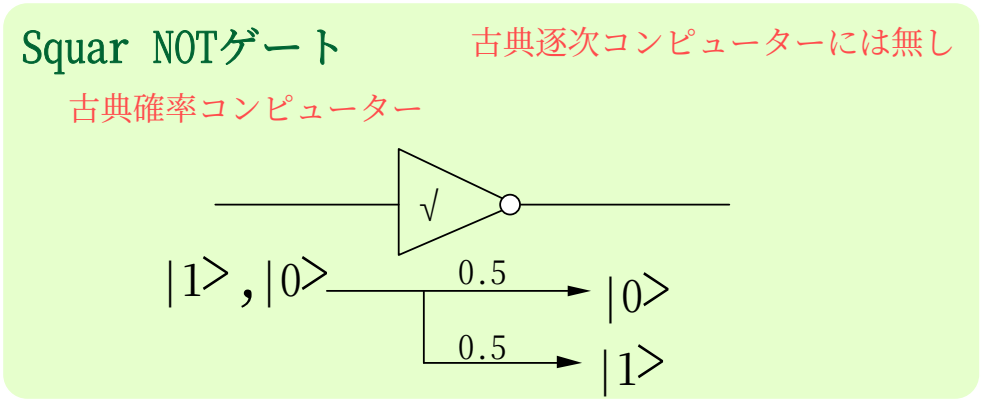
7．3　位相回転ゲートとは？

それでは，位相回転ゲートとは何であろうか．1の状態は，回転ゲートにより，θだけ位相が回転し，ψ=cosθ|1>+sinθ|0>となる．その概略図を図14に示す．θ=π/4のとき，|1>は，|1>と|0>の重ね合わせとなる．n qu-bitのそれぞれにθ=π/4の位相回転をほどこすことにより，一つの状態は，2^n個の状態へと分身する．光の分野でそれを簡単に言うと，偏光回転素子や位相板のことを指す．1qu-bitの偏光の向きや位相の位置を変化させる素子であり，一般の光学素子にも多用されている．光について言えば，別にどうと言うことはない当たり前の操作と言えよう．

7．4　制御NOTゲートとは？

一方，制御NOTゲートは，2qu-bit間の変換であり，一つの波動関数が別の波動関数に影響を及ぼさなければならない．一般に光子のようなボーズ粒子は，独立性が高く光子同士が影響を及ぼすことはあまり見られない．むしろ電子のようなフェルミ粒子の方が互いに影響を及ぼし易い．

一方，量子計算においては，各bitは制御NOTを施すまでは，独立を保たなければならず，波動関数がすぐに変化するqu-bitは，メモリーに適さない．そのため，これまで提案されているqu-bitは，光子や核スピンといった独立性の高い量子粒子を用いる場合が多い．量子粒子間の相互作用は，これらの粒子を結ぶ別のフェルミ粒子である電子等の働きを通して達成される．例えば，特定の分子における原子間の価電子が二つの核スピンを結び付ける．この間接的な量子粒子間の相互作用を得ることが，一般的には難しく，そのため現在においては，より多くのbit間の制御NOT回路を作製することが，量子コンピューターの実現化における一つの研究課題となっている．



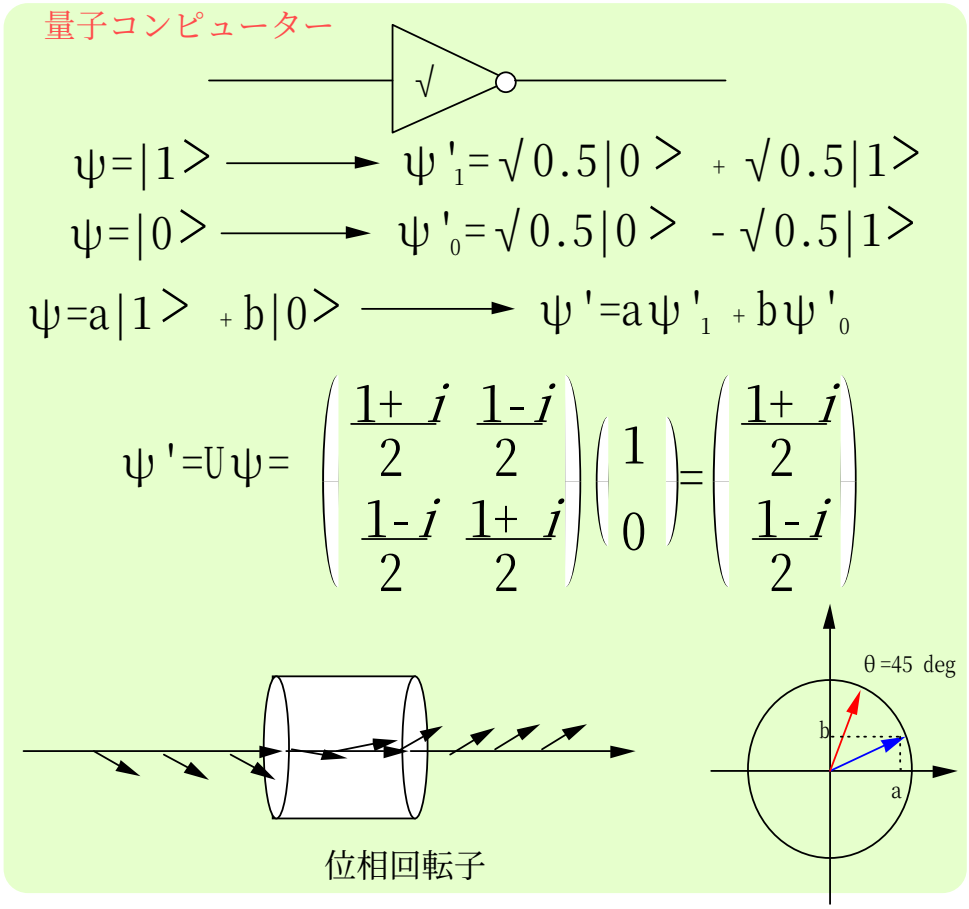
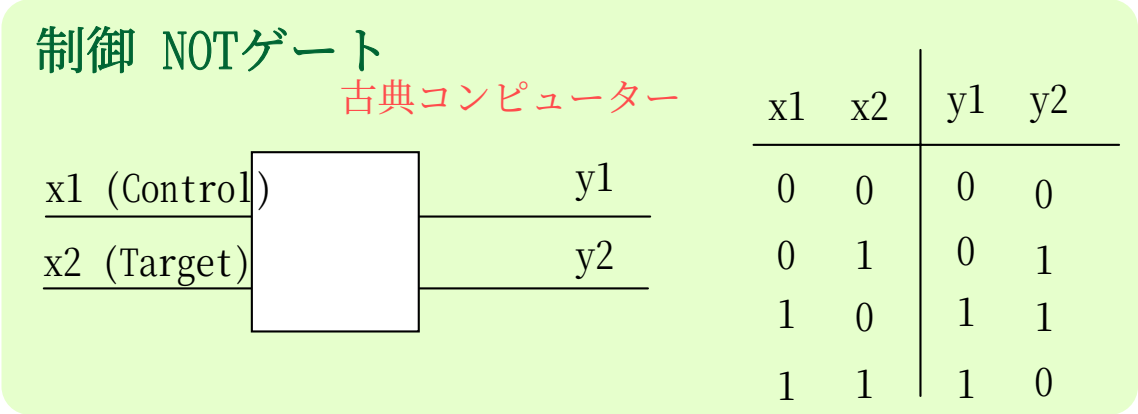


図 14　古典的位相回転ゲートと量子的位相回転ゲート（Square Not ゲート）

こうして得られた相互作用により（むしろ一方的な制御により）ある波動関数（制御 bit）の状態に依存した別の波動関数（ターゲット bit）の変換を作用させる．この変換は，制御 bit が 0 の場合，ターゲット bit を変化させず制御 bit が 1 の場合，ターゲット bit の|1>を|0>に，また|0>を|1>に変換させる NOT ゲートとして働く．このとき制御 bit はどの場合も変化しない．こうして表わされるゲートを制御 NOT ゲートと呼ぶ．量子回路を表わす記号として制御側とターゲット側を図 15 のようにして表わす．



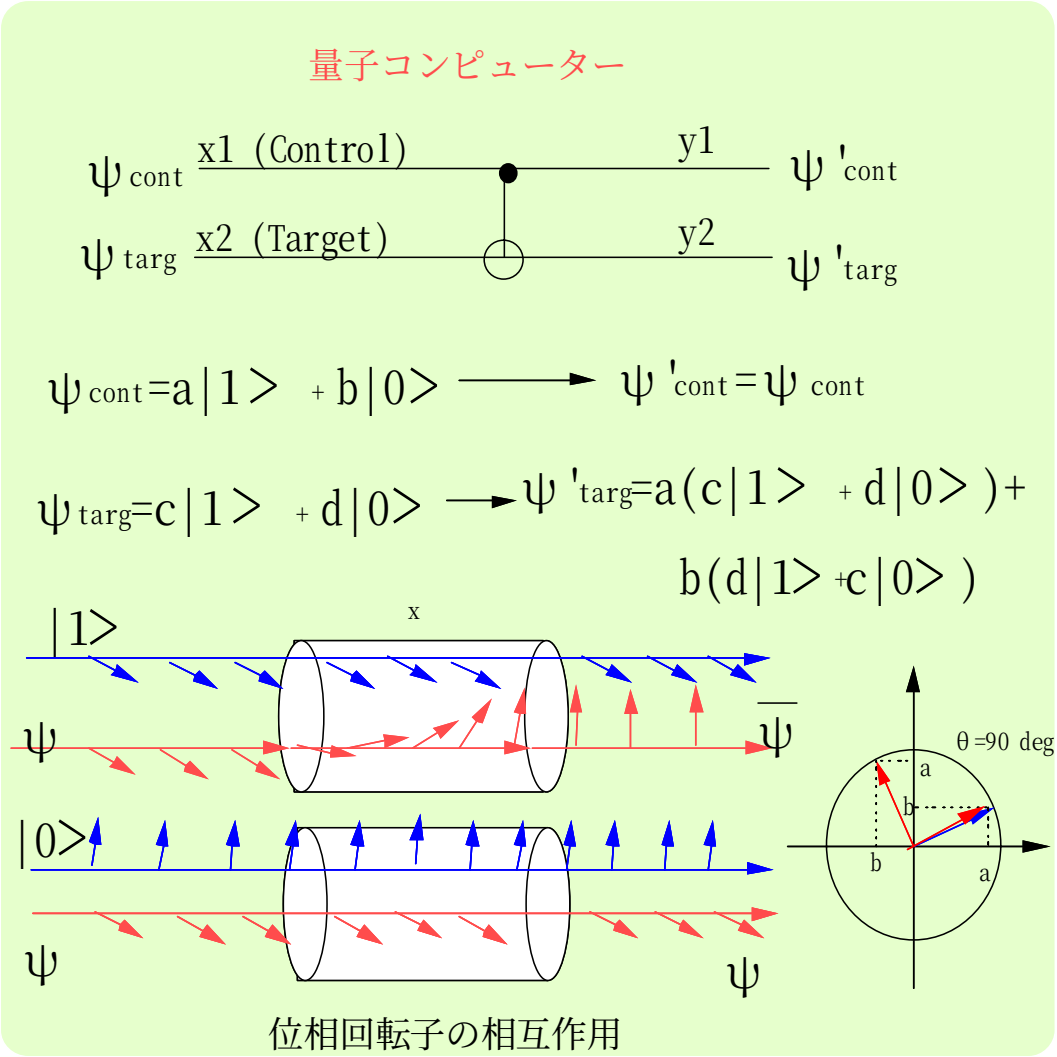


図 15　古典的制御 Not ゲートと量子的制御 Not ゲート

また制御 bit が|1>と|0>の重ね合わせであった場合，例えば，ψ=cos θ |1> + sin θ |0>とするとターゲット bit|0>は，ψ_t=cos θ |1> + sin θ |0>と変化することになる．この制御 NOT 回路による波動関数間の振る舞いには，これ以上に特筆すべき点が多く，ある意味，量子情報による量子論の発展を形作る源泉であるといっても過言ではない．

最後に，本文章は，2000 年度にまとめた量子応用研究会の報告書をベースに書き直したものであり，幾分情報は古くはなっているものの，初学者向けに何らかのお役に立てれば幸いである．

参考文献

[1]　西野哲朗，量子コンピュータ入門，情報科学セミナー，東京電機大学出版局　(1997)．
[2]　上坂吉則，量子コンピュータの基礎数理，コロナ社 (2000)．
[3]　大矢雅則，量子コンピュータの数理，パリティ物理学コース，丸善　(1999)．
[4]　コリン・P．ウィリアムズ，スコット・H．クリアウォ－タ，量子コンピューティング　ー量子コンピュータの実現へ向けてー，シュプリンガ－・フェアラーク東京　(2000)．
[5]　ジョン・ホーガン，科学の終焉，徳間書店　(1997)．