連載講座

量子情報処理パラダイム
1. 量子計算の基礎

今井　浩

1. 量子情報処理の講座開始にあたって

量子コンピュータとか，量子暗号という言葉を最近目にされたかもしれない．たとえば，2001年12月の新聞では，MIT, IBM研究者が世界ではじめて15の素因数分解3×5を量子コンピュータで計算した，という記事があった．これは小学生でもできることなのだが，このように量子コンピュータが注目されて，小規模でも実際に実現されると記事になるのは，理論としては1990年代半ばに量子コンピュータができれば整数の素因数分解が多項式時間で解けることがShor [5]により示されたからだ．

昔なら素因数分解が早く解けてもそんなに嬉しいことはなかったかもしれない．しかし，今やインターネットの時代で，インターネットショッピングなど電子決済，電子政府実現のための認証・プライバシー保持などを支える情報基盤技術として公開鍵暗号系が使われており，広く使われているRSA暗号などそれが暗号たりうる安全性を有するというのは「大きな整数を素因数分解することは難しい」という計算量仮定と呼ばれるものに基づいてであるからだ．今ならたとえ国をあげてスパコンを全部使っても10進数百桁の整数を素因数分解することは現実的時間内ではできないわけだが，量子コンピュータができるとそれが簡単にできてしまって，ようは量子コンピュータをもつ人は暗号を破ることができるようになるのだ．

さらに，Shorの結果は離散対数系の公開鍵暗号の安全性が崩れることも示しており，現在のほとんどの公開鍵暗号システムの安全性が量子コンピュータの出現によって壊れることになる．上述のようにもはや社会基盤となったセキュリティのシステムが崩壊するというのは，社会に対する衝撃となりうる．

一方，量子コンピュータさらにはそれを含む量子情報処理全般は，セキュリティに関して根本的に異なる新技術も提供してくれる．量子暗号は，量子状態そのものを通信することにより，物理原理に基づいた安全性を保持することを目指しており，今の公開鍵暗号の基づく計算量仮定より確固たるものに基礎をおいていて，これまでとまったく違った形でのセキュアな通信システムを提供しようとしている．その基づく物理原理とは，量子状態は観測すると波束の収縮が起こって状態そのものが変わってしまうことなどである．

量子暗号は実験レベルでは実現されていることもあり，数年内にも実際に使える技術になる可能性がある．量子コンピュータの実現は，なかなか難しそうではあるものの，今このようなインパクトの大きさと，また量子力学が20世紀の生み出した物理学で量子情報処理で使うのはまさしくその基礎部分であるということで，基礎研究としても精力的に研究されている．情報処理方式についても，将来の暗号もこの狭義の量子暗号だけでなく，たとえば量子コンピュータが出現しても安全な新世代の量子公開鍵暗号の提案などもある．

このように，量子コンピュータや量子通信を軸とする量子情報処理は，近い将来，社会に影響をもたらしうるポテンシャルをもっている．一見したところでは，オペレーションズ・リサーチの分野からは遠く見えるかもしれない．しかし，量子計算・量子情報は確固とした土台の上に築かれている問題である．たとえば，量子状態は一般に複素行列でエルミート・非負定値・トレース1の行列で表される．このことだけからも，量子計算・情報での基礎的問題に，半定値計画問題が現れることは容易に想像頂けるだろう．また，量子力学でもある意味これまでフルに使われていなかった数理的側面を活用するのが量子計算・情報であり，実は

いまい　ひろし　東京大学情報理工学系研究科
〒113-0033 東京都文京区本郷7-3-1
ERATO今井量子計算機構プロジェクト, JST
〒113-0033 同文京区本郷5-28-3 本郷ホワイトビル

OR研究者にはとっつきやすいのである．さらに，今のコンピュータがORの問題を解決するのに使われてきただけでなく，コンピュータ自身の発展のためにコンピュータ科学がORへの新しい問題をどんどん提供してきたのと同じ役割を，上の半定値計画など含め量子コンピュータが供することが期待される．

そこで，5回にわたっての新情報処理パラダイムとしての量子コンピューティングの講座を，編集委員会のご助力のもと，企画した．順番に，

1. 量子計算の基礎，今井浩
2. 量子暗号，富田章久 (NEC 基礎研究所)
3. 量子情報理論，松本啓史 (ERATO, JST)
4. トポロジーと量子計算，八森正泰・由良文孝 (ERATO, JST)
5. 量子計算と最適化，今井浩

を予定している．是非，この講座が，OR的センスを量子情報科学にもたらす端緒になれば！

2. 量子力学基礎 — 量子計算・情報で必要な数理の準備

まず講座の第1回目では，一見とっつきにくい量子計算・量子情報が実はORワーカには身近なものであることを，その基礎を解説することによって示したい．具体的には，本稿では量子計算・情報の基礎部分を線形代数で解説する．

量子計算というからには量子力学が必要である．物理・電子工学などの大学教育では，量子力学という確立された講義があり，それを全部理解しないと量子計算の研究はできないというのでは，なかなか量子計算への情報分野からの新規参入者は限られてしまう．しかし，実際に量子計算・情報で使う最初の部分は，大学入門の線形代数とその周辺を理解しているとほぼわかる事柄である．なんにせよ，この解説では量子力学講義で常に出てくるハミルトニアンやSchrödinger方程式は出てこず，複素ベクトル空間の線形代数で話が進む．

量子力学を記述するには，一般にHilbert空間と線形作用素を用いるが，本稿では有限次元に限って話を進めるので，すべて複素ベクトル空間と行列で話を進めることができ，実際にそうしていく．無限次元の場合の取り扱いは，また別途議論が必要となる．

量子力学の入門で多くの方は，量子状態を表現する際の量子力学独特のブラケット表記，すなわち縦ベクトルのケットベクトル$|\phi\rangle$，その共役転置のブラベクトル$\langle\phi|$を覚えてらっしゃるかもしれないが，本節ではまずは通常のベクトル記法を用い，また数理計画・最適化に造詣の深い方には理解しやすい行列表現を用いていく．次節の量子ビットの話のところから，一部ブラケット表記も用いる．

2.1 密度行列とPOVM測定

量子状態は，対応する次元dをもってきて，次の条件を満す$d \times d$複素行列ρで数理的に表現できる: (1) $\rho = \rho^*$, (2) $\rho \geq 0$, (3) $\mathrm{Tr}\,\rho = 1$. ここで*は共役転置を表し，ρ^*とはρの転置行列で，各要素について複素共役をとったものである．$\rho \geq 0$は，ρが非負定値であることをいい，$\mathrm{Tr}\,\rho$はρのトレースであり，対角要素の総和である．すなわち，量子状態とはエルミート，非負定値でトレースが1の複素行列で表現される．このような条件を満す行列を，密度行列という．

密度行列ρの固有値$\lambda_1 \geq \ldots \geq \lambda_d$は，エルミートなので実数であり，非負定値であることから非負，また条件(3)より総和が1である:

$$\sum_{i=1}^{d} \lambda_i = 1, \quad \lambda_i \geq 0$$

ρはエルミートであるので，λ_iの正規化された固有ベクトル$\boldsymbol{v}_i$を(固有値に重複のある場合うまく)とって正規直交基底が構成でき，次のように対角化できる:

$$\rho = \sum_{i=1}^{d} \lambda_i \boldsymbol{v}_i \boldsymbol{v}_i^*, \quad \boldsymbol{v}_i^* \boldsymbol{v}_j = 0 \ (i \neq j).$$

ρのランクが1であるとき，0でない固有値は最大固有値の$\lambda_1 = 1$となる．このとき，対応する量子状態を純粋状態 (pure state) と呼ぶ．純粋状態は，$\lambda_1 = 1$の正規化された固有ベクトル$\boldsymbol{v}_1$によって完全に表現でき，これがブラケット記法で量子状態をケットベクトルで表したものに対応する．

ρのランクが2以上のとき，対応する量子状態を混合状態 (mixed state) と呼ぶ．混合状態は，純粋状態$\boldsymbol{v}_i \boldsymbol{v}_i^*$が確率$\lambda_i$で混合された状態とみなせる．

量子状態から何らかの情報を得るには，測定をしないといけない．ここでも，本稿では得られる情報は有限でm個の事象であるとしよう (測度論的な扱いは他に譲る)．すると，測定の数理モデルとして，k個のエルミート非負定値行列M_iの集合$\{M_1, \ldots, M_m\}$で，

和が単位行列になるものを考える．すなわち，

$$M_l = M_l^* \geq 0\ (l = 1,\ldots,m), \quad \sum_{l=1}^{m} M_l = I.$$

そして，密度行列ρの量子状態に対してこの測定を行うと，l番目の事象は確率 $\mathrm{Tr}\ \rho M_l$ で観測される．すなわち，測定から得られる確率変数 X とそのとる値 $\{1,\ldots,m\}$ に対して，

$$\Pr(X = l) = \mathrm{Tr}\ \rho M_l \quad (l = 1,\ldots,m).$$

このような測定系をPOVM (Positive Operator Valued Measure) と呼ぶ．lが測定されたとき，量子状態は元の状態から変化する．これについては，量子状態の変換操作の1つとしてその節で述べる．

ここで，ρ, M_l がエルミート非負定値であることより，$\mathrm{Tr}\rho M_l$ は非負実数であり，かつ

$$\sum_{l=1}^{m} \mathrm{Tr}\ \rho M_l = \mathrm{Tr}\left(\rho \sum_{l=1}^{m} M_l\right) = \mathrm{Tr}\ \rho = 1$$

であるので，確率の条件が満されている．

例 1 (有限離散分布): 有限離散分布を，これまでの枠組みで表してみよう．値 i をとる確率が p_i $(i = 1,\ldots,d)$ であるような有限離散分布 $(\sum_{i=1}^{d} p_i = 1,\ p_i \geq 0)$ に対して，$p_1,\ldots,p_d$ を対角要素とする対角行列 (これを $\rho_p = \mathrm{diag}[p_1,\ldots,p_d]$ で表す) とするとこれは密度行列であり，第i対角要素のみ1で他は0であるような行列 M_i $(i = 1,\ldots,d)$ の集合はPOVMであり ($\mathcal{M}$ と呼ぶ)，このときi番目の事象が測定される確率は $\mathrm{Tr}\ \rho_p M_i = p_i$ となり，元の有限離散分布になっている． □

例 2 (純粋状態の射影測定): 純粋状態で，固有値1に対する正規化固有ベクトルが $\boldsymbol{v} = (v_i) \in \mathbb{C}^d$ であるとき，上と同じPOVM $\mathcal{M}$ を考えると，事象iが測定される確率は $v_i\overline{v_i} = |v_i|^2$ となる．これは最も基本的な測定である．

$\boldsymbol{e}_i$ を第i要素のみ1で他は0として，$\boldsymbol{e}_i$ からなる正規直交座標系を考えたとき，この測定は純粋状態の対応するベクトルの $\boldsymbol{e}_i$ への射影のノルムの2乗が測定確率になる．

そこで，$\mathbb{C}^d$ の任意の正規直交基底 $\boldsymbol{e}'_i$ に対して，$M'_i = \boldsymbol{e}'_i(\boldsymbol{e}'_i)^*$ とするとこれもPOVMになり，これで測定することは$\boldsymbol{v}$の座標をその座標系に変換して，そこで上のような射影操作を行うことに対応する． □

一般に，POVMで $(M_i)^2 = M_i$, $M_iM_j = 0\ (i \neq j)$ の条件が満たされているとき，射影測定という．上のPOVMは射影測定である．射影測定でないPOVMで，最適となるものもある．林，松本 [3] など参照．

2.2 テンソル積と部分トレース

ここまでは次元は一定であった．量子状態を合成してより高い次元の量子状態を構成したり，高い次元の量子状態から部分のみの情報をえて低次元の量子状態を扱う操作について述べる．

行列 $A = (a_{ij}) \in \mathbb{C}^{d_h \times d_h} \equiv \mathcal{H}$ と $B \in \mathbb{C}^{d_k \times d_k} \equiv \mathcal{K}$ に対して，そのテンソル積の行列を

$$A \otimes B = \begin{pmatrix} a_{11}B & \cdots & a_{1d_h}B \\ \vdots & \ddots & \vdots \\ a_{d_h1}B & \cdots & a_{d_hd_h}B \end{pmatrix}$$

と定める．$A \otimes B$ は $d_hd_k \times d_hd_k$ の行列であり，この土台の空間の $\mathbb{C}^{d_hd_k}$ を $\mathcal{H} \otimes \mathcal{K}$ と表す．このテンソル積の定義ではいわゆるKronecker積の行列表現を用いており，生成される行列に関してテンソル積は一般に可換でない．ρ を $\mathcal{H}$ 上の密度行列，σ を $\mathcal{K}$ 上の密度行列としたとき，$\rho \otimes \sigma$ は $\mathcal{H} \otimes \mathcal{K}$ の密度行列になっている (確認されたい)．

μ を $\mathcal{H} \otimes \mathcal{K}$ の密度行列としたとき，行列全体を $d_k \times d_k$ ブロック行列に分解したとき，対角の $d_k \times d_k$ ブロック行列の和を σ' とすると，それは $\mathcal{K}$ 上の密度行列となっている．この操作を $\mathcal{H}$ をトレースアウトする，または $\mathcal{K}$ の部分トレースをとるという．記法として

$$\sigma' = \mathrm{Tr}_{\mathcal{H}}\ \mu \in \mathcal{K}$$

と表す．上の ρ, σ のテンソル積に関して，

$$\sigma = \mathrm{Tr}_{\mathcal{H}}\ (\rho \otimes \sigma)$$

であり，この意味で部分トレースはテンソル積の逆演算とみなせる．

テンソル積を上では正方行列の間で定義したが，一般の正方でないものの間でも，したがってベクトルの間でも同様に定義できる．

それも用いて上の部分トレース $\mathrm{Tr}_{\mathcal{H}}$ を式で書くと，

$$\mathrm{Tr}_{\mathcal{H}}\ \rho = \sum_{i=1}^{d_h} (\boldsymbol{e}_i^* \otimes I_{\mathcal{K}})\rho(\boldsymbol{e}_i \otimes I_{\mathcal{K}}),$$

ここで，d_h は $\langle$ の次元で，$I_{\mathcal{K}}$ は $\mathcal{K}$ 上の単位行列，$\{\boldsymbol{e}_1,\ldots,\boldsymbol{e}_{d_h}\}$ は $\mathcal{H}$ の任意の正規直交基底である．$\mathrm{Tr}_{\mathcal{K}}$ も定義できるが，テンソル積が一般に可換でないことなど注意が必要である．

もとの量子状態が純粋状態であっても，部分トレースをとると必ずしも純粋状態でないことに注意．

例 3 (テンソル積・部分トレースと有限離散分布): 有限離散分布との対応を見ておこう．簡単のため，2 つのコインに対応する 2 つの 2 次元有限離散分布 (p_1,p_2)，(q_1,q_2) を考える (前者で表が確率 p_1 で，裏が確率 p_2 ででることを表す)．このとき，それぞれを表現する密度行列は，$\rho = \mathrm{diag}[p_1,p_2]$，$\sigma = \mathrm{diag}[q_1,q_2]$ であり，このテンソル積 $\rho\otimes\sigma = \mathrm{diag}[p_1q_1,p_1q_2,p_2q_1,p_2q_2]$ は，この 2 つのコインが独立に投げられたときの有限離散分布を表している．

逆に，4 次元の有限離散分布に対応する $\rho' = \mathrm{diag}[p'_1,p'_2,p'_3,p'_4]$ をこれまでのように $\mathcal{H}\otimes\mathcal{K}$ 上の密度行列とみなし，それに対して $\mathcal{H}$ をトレースアウトすると，部分トレース $\mathrm{Tr}_{\mathcal{H}}\,\rho' = \mathrm{diag}[p'_1+p'_3,p'_2+p'_4]$ となる．これは周辺分布をとることに対応していることを，上のテンソル積の逆演算としても理解することによってみてとられたい．□

2.3 量子状態の変換操作

テンソル積と部分トレースにより，量子状態を合成したり，部分的に扱えたりと操作することができた．ある量子状態を他の量子状態に変換する一般的な操作は (トレース保存) 完全正写像とよばれる (トレース保存という用語は以下では除く)．

完全正写像 (Completely Positive Map)T は，$\mathbb{C}^{d\times d}$ の密度行列 ρ を $\mathbb{C}^{d'\times d'}$ の密度行列 $T(\rho)$ に写像するもので，$d'\times d$ 行列の集合 $\{A_1,\ldots,A_k\}$ で，$\sum_{j=1}^k A_j^*A_j = I$ を満たすものによって定められ，

$$T(\rho) = \sum_{j=1}^{k} A_j\rho A_j^*$$

と変換する．$T(\rho)$ が密度行列になっていることを確かめられたい (テンソル積も部分トレースも完全正写像であることも)．完全正写像 T は，$\{A_1,\ldots,A_k\}$ によって定められるという．

同じ次元の量子状態間の完全正写像として基本的なものに，ユニタリ変換に対応するものがある．$\mathbb{C}^{d\times d}$ の密度行列 ρ に対して，U を $\mathbb{C}^d$ 上のユニタリ行列 (すなわち，$UU^* = U^*U = I$) として，$\{U\}$ により完全正写像 $T_U(\rho) = U\rho U^*$ が定まる．ρ がベクトル $\boldsymbol{v}$ によって $\rho = \boldsymbol{v}\boldsymbol{v}^*$ と表される純粋状態のとき，$T_U(\rho)$ もベクトル $U\boldsymbol{v}$ により $U\rho U^* = (U\boldsymbol{v})(U=\boldsymbol{v})^*$ と表される純粋状態となる．純粋状態の量子状態の世界では，純粋状態から他の純粋状態へはこの U によるユニタリ変換で写され，これが量子計算の中核となる．ユニタリ変換は可逆であるから，量子計算の中核部は完全に可逆な計算となる．

測定も量子状態を変換する．$\{M_1,\ldots,M_k\}$ で定められる POVM を考える．M_l はエルミート非負定値であるから，エルミート非負定値な行列 $L_l = L_l^* = \sqrt{M}$ を考えることができ，$M_l = L_l^*L_l$ と分解できる．このとき，POVM による測定によって密度行列 ρ は $\sum_{j=1}^k L_j\rho L_j^*$ に変換される．ただし，測定で事象 l が観測された場合，状態は $(1/\mathrm{Tr}\;L_l\rho L_l^*)L_l\rho L_l^*$ に変換される．これを波束の収縮・収束という．もとが純粋状態であっても，POVM 測定によって状態は一般に混合状態になる．

例 4 (射影測定による状態変化): 少なくとも 2 要素が非ゼロのベクトル $\boldsymbol{v}$ で表される純粋状態に対して，射影測定 $\mathcal{M}$ によって測定すると，量子状態は密度行列 $\mathrm{diag}[|v_1|^2,\ldots,|v_d|^2]$ で表される混合状態になる．したがって，量子計算で計算過程で測定を行う前後を同じ枠組みで扱うには密度行列での表現が必須となる．□

例 5 (確率遷移行列の完全正写像としての表現): 前に有限離散分布が量子状態としてどう表されるかをみた．確率分布を変換する操作に，確率過程がある．その 1 ステップは，有限離散分布を横ベクトル $\boldsymbol{p} = (p_1,\ldots,p_d)$ で表して，行和が 1 で要素が非負の確率遷移行列 $Q = (q_{ij})$ を作用させ，$\boldsymbol{p}\mapsto\boldsymbol{p}Q$ とする．

この操作は，完全正写像として書ける．完全正写像での行列の添字は 1 つであったが，ここでは確率遷移行列の要素に対応する 2 つ添え字とし，A_{ij} を ji-要素が $\sqrt{q_{ij}}$ で他は 0 の行列とすると，$\{A_{ij}\mid i,j=1,\ldots,d\}$ で定まる完全正写像はもとの有限離散分布を表す状態 $\rho = \mathrm{diag}[\boldsymbol{p}]$ を $T(\rho) = \mathrm{diag}[\boldsymbol{p}Q]$ とする．□

2.4 量子ビットと部分測定

量子計算では，純粋状態を量子状態の表現として用いる．$\mathbb{C}^2$ の正規化ベクトル $\boldsymbol{v}$ で，1 量子ビットを次のように表す．$\begin{pmatrix}1\\0\end{pmatrix}$ と $\begin{pmatrix}0\\1\end{pmatrix}$ で構成される正規直交座標系を考え，前者を 1 ビットの 0 に，後者を 1 ビットの 1 に対応させる．純粋状態 $\boldsymbol{v} = \begin{pmatrix}v_1\\v_2\end{pmatrix}$ は，座標系に関する射影測定によって確率 $|v_1|^2$ で 0 と，確率 $|v_2|^2$ で 1 と観測される．そのためには，上の基底をそれぞれ $|0\rangle$, $|1\rangle$ と表記し，

$$\boldsymbol{v} = v_1|0\rangle + v_2|1\rangle$$

と表すと以下のように2量子ビットからわかりやすくなる．この$|0\rangle, |1\rangle$をケットベクトルといい，その共役転置を$\langle 0|, \langle 1|$で表し，ブラベクトルという．

n量子ビットは，$\mathbb{C}^2$をn個テンソル積して得られる$\mathbb{C}^{2^n} = \mathbb{C}^N$ $(N = 2^n)$空間の純粋状態$\boldsymbol{v}$である．ブラケット記法で，$|0\rangle \otimes |0\rangle = |00\rangle$, $|1\rangle \otimes |0\rangle \otimes |1\rangle = |101\rangle$などと記すこととする．すると，$n$量子ビットは，$|0\cdots 0\rangle$から$|1\cdots 1\rangle$までの$2^n$パタンの0,1列に対応する正規直交基底で表される$2^n$次元空間でのノルム1のベクトルであり，射影測定によってi番目の事象が第i座標値v_iについて$|v_i|^2$の確率で観測される．

$n = 2$の場合を考えよう．$\mathbb{C}^{2\times 2}$において，

$$|00\rangle = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}, |01\rangle = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}, |10\rangle = \begin{pmatrix}0\\0\\1\\0\end{pmatrix}, |11\rangle = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$

となっている．

$$\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle) = \begin{pmatrix}1/\sqrt{2}\\1/\sqrt{2}\\0\\0\end{pmatrix} = |0\rangle \otimes \left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right)$$

のように1量子ビットのテンソル積に分解できる場合があるのに対して，

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \begin{pmatrix}1/\sqrt{2}\\0\\0\\1/\sqrt{2}\end{pmatrix}$$

はどのようにしても1量子ビットのテンソル積に分解することができない．このように分解できない状態をエンタングルしている(entangled)という．

これらの例で全体でなく部分の1量子ビットのみを測定することができることをみておこう．$M_1 = \mathrm{diag}[1,0,1,0]$, $M_2 = \mathrm{diag}[0,1,0,1]$からなる$\{M_1, M_2\}$で与えられるPOVMで測定してみると，$\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)$の場合は確率1/2で1量子ビット目について0が測定され，状態が$|00\rangle$に収縮し，確率1/2で1量子ビット目について0が測定され，状態が$|01\rangle$に収縮する．一方，$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$の場合は，確率1/2で1量子ビット目について0が測定され，$|00\rangle$に収縮し，確率1/2で1量子ビット目について1が測定され，$|11\rangle$に収縮する．分離可能な方では測定した値からは収縮した情報がどちらであるかわからないので，状態は結局$\mathrm{diag}[1/2,1/2,0,0]$という密度行列をもつ混合状態となる．それに対して，このようにエンタングルしている場合は，測定値がわかっていれば，収縮した状態もユニークに特定できる．これは通信の手段，計算の単位操作として使えるもので，このエンタングルしていること(エンタングルメント)は量子計算・量子情報で重要な役割を果たす．注意として，空間的に離れた量子系がエンタングルしていると，片方の測定結果が他方の状態に瞬時に影響しているが，このことを通信の手段として用いる場合でも，他に古典的通信路も必要なため，光速を超えて情報を送ることはできない．

3. 量子計算

量子力学に対してニュートン力学を古典力学と呼ぶのと同じように，量子計算に対して今の計算のモデルを古典計算と呼ぼう．もちろん，古典がつまらないなどというのではなく，ここまでの成功を収めたことを評しての表現である．

古典計算を回路モデルで述べると，入力に対してAND, OR, NOTという回路素子をネットワークで結んで回路とし，入力から出力へ演算していくことが古典計算である．そのとき，回路の素子数が計算時間に対応する．AND, OR, NOTという回路素子で任意の論理関数を回路構成できることが肝要である．

量子計算を回路で扱うとき，どういう回路素子で汎用計算ができ，かつ妥当な単位計算時間を与えるものとして有用かというのが量子計算を定義するときに重要だ．まず，1量子ビットに対する操作としては，前出のユニタリ変換を1量子ビットの場合に限って，1量子ビットから1量子ビットへのユニタリ変換を考える．これだけだと1量子ビットだけしか操作できないので，2量子ビットの間の操作が必要で，代表的なものが次の制御NOTである．2量子ビット$\boldsymbol{v} \in \mathbb{C}^4$について，前出の座標系で表したとき，

$$C_{\mathrm{NOT}} = \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}$$

を用いて$C_{\mathrm{NOT}}\boldsymbol{v}$を出力する素子を制御NOT素子という．基底ベクトルがどう変換されるかを書くと，

$$|00\rangle \mapsto |00\rangle,\ |01\rangle \mapsto |01\rangle,\ |10\rangle \mapsto |01\rangle,\ |11\rangle \mapsto |10\rangle$$

となる．すなわち，最初の量子ビットが0のときはなにもせず，1のときは他方の量子ビットの0,1を反転(NOT)する．

量子計算では，n ビットの入力が与えられたとき，あらかじめ途中で作業用に使う量子ビットも最初から用意して全体で$n'(\geq n)$量子ビットからはじめ，上の1量子ビットに対するユニタリ変換と2量子ビットに対する制御NOTを適用して，最後に測定を行って計算結果を得て計算終了となる．ここで，上のユニタリ変換・制御NOTの説明は当該量子ビットに対するものだけであったが，この計算過程では常にn'量子ビットで操作するので，該当以外の量子ビットのところはそのままということで単位行列を対応させ，全体のn'量子ビットに対するユニタリ行列をそれらをテンソル積とする．たとえば，1量子ビット目に2次元ユニタリ行列Uをかける場合，全体は$U\otimes(\otimes_{i=2}^{n'}I_2)$ (I_2は2次元単位行列)というユニタリ行列をかけることに，$(n'-1), n'$量子ビット目に制御NOTをかける場合，全体は$(\otimes_{i=1}^{n'-2}I_2)\otimes C_{\mathrm{NOT}}$というユニタリ行列をかけることになる．この2つをうまく掛け合わせることで，任意の$2^{n'}$次元のユニタリ行列が表現できることがわかっている．

今一度，量子計算をまとめると，

量子計算:

1. nビットの入力に対して，作業ビットも加えn'量子ビットの初期状態を構成;
2. 1量子ビットに対するユニタリ変換，2量子ビットに対する制御NOT変換という単位演算操作を順次適用;
3. 測定を行い，計算結果の情報を得て終了.

となる．このとき，計算時間は単位演算操作を適用した回数と定義する．

もちろん，この定義ではまだ不備がある．1量子ビットに対する単位演算として任意のユニタリ変換を使っているが，そのようなものは無数にあり，古典回路でAND, OR, NOTと定数個の単位操作を用いていたのと違う．その前にも，これでは連続数を扱うモデルになっているので，古典計算ですべてを0, 1の離散で表す世界と違う．これらの点については，まず連続数を有限離散の数で近似し，その際，指定された精度での近似をきちんと保証すること，また2次元ユニタリ変換が定数個の基本的なユニタリ変換を組合せて所望精度で近似表現できることによって解決する．

他の大きな問題に，途中で測定を許したモデルや最後の測定に関する詳細など，色々な問題があるが，それらについては専門の解説書に譲るとする．

4. おわりに

量子計算の代表的アルゴリズムであるShorの多項式時間の素因数分解アルゴリズムについては，この稿では触れられなかった．一部，その本質部分に言及すると，n量子ビット上での2^n次元空間のFourier変換が量子計算で多項式時間で行えることを道具に，素因数分解を周期発見問題に帰着してFourier変換を適用するというものである．

他の代表的な量子アルゴリズムに，Groverの量子探索アルゴリズム・量子サンプリングがある[1]．これは，基本的に探索問題の計算時間を，量子の性質を使って元の平方根分のオーダにスピードアップするものである．また，本稿で明示して触れられなかった量子計算で重要な性質として，複製不可能定理(量子状態の複製を完全に作ることはできない)，量子重ね合わせによる量子並列計算(本稿で説明したテンソル積で作られた状態にユニタリ変換をかけることは，一度に並列計算していることに対応する)などがある．

量子計算の教科書としては，Gruska [2]は情報科学や最適化の研究者にとっては，包括的で量子計算が述べられ，物理的イメージの獲得も一度にできてよいと思われる．Nielsen, Chuang [4]は，量子情報まで含めて書かれたもので，広く読まれるようになっている．

参考文献

[1] L. K. Grover, A Fast Quantum Mechanical Algorithm for Database Search, *Proceedings of the 28th ACM Symposium on Theory of Computing*, 1996, pp.212–219.

[2] J. Gruska, *Quantum Computing*, McGraw-Hill, 1999.

[3] 林正人, 松本啓史, 量子系における統計的推測の最近の展開, 応用数理, Vol.11, No.3 (2001), pp.27–48.

[4] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2000.

[5] P. W. Shor, Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, *SIAM Journal on Computing*, Vol.26, No.5 (1997), pp.1484–1509.