量子コンピュータの基礎と物理との接点

東京大学 大学院工学系研究科 附属光量子科学研究センター
藤井啓祐

2017 年 6 月 8 日

1 はじめに

このテキストでは，量子力学の復習から進めて，量子情報及び量子計算の基礎事項について丁寧に説明している．そのかわり，講義の時には，必ずしも詳細な計算や証明については触れない．各自，テキストをもとに自分で計算してみて，量子情報による記述に慣れていただきたい（もちろん講義以外の時間を利用して質問にくることは大歓迎である）．一方，紙面の関係から，トポロジカル秩序やマヨラナ粒子を用いたトポロジカル量子計算等についてはテキストに含めることができなかった．講義のときに丁寧に説明することにする．

量子情報では，特定の物理系にできるだけ依存することなく，複雑な量子系における現象を普遍的に記述することを目指している．そうすることで，計算理論や情報理論などの情報科学的手法を大いに利用し緻密な議論を展開することができる．また，このテキストでも説明する万能性の議論から，任意の量子系のダイナミクスを量子コンピュータで効率よく模倣することができる．このため，量子コンピュータの挙動や限界を理解することによって，より深い物理の理解に繋がるであろう．例えば最近では，量子コンピュータを雑音から守るために作り出された量子誤り訂正理論が，トポロジカル秩序やブラックホールの理解に使われている．今後も，このような例はますます増えていくのではないかと期待される．また，実際に量子コンピュータが実現されることによって，それがたとえ小規模であったとしても，可解模型や古典コンピュータによる数値計算だけでは捉えきれない複雑性の極限にある物理に関する新たな知見を得るための強力な実験的手段となるであろう．また，量子物質設計や量子化学計算などのように潜在的に「量子」の言語で定義された問題を解く上で量子コンピュータが役に立つことは言うまでもなく，今後，機械学習などの一見量子とは関係のない分野においても量子コンピュータがその実現の困難性を引いても余りあるような貢献をする可能性もある．

一方，情報や計算といった概念は，通常の物理系学部の学生はあまり触れてこなかったと思う．よって，一通り慣れてしまうまでは，議論の展開が殺伐としていて（それが良いところでもあるのだが）物理とのつながりが感じにくく思われるかもしれない．最近では，小さいサイズではあるが万能性がある真の量子コンピュータ（IBM quantum experience）がウェブ上で公開されており，誰でも（今のところ）無料で利用することができる．このテキストに書かれていることを自分でサーバー上の量子コンピュータを使って確認してみるのもよいであろう．

今回は，量子デバイスの物理には踏み込む余裕はないが，量子コンピュータの理論は，それを支える量子デバイスの物理や実験技術の蓄積に支えられている（従来のコンピュータが固体物理学や半導体技術の蓄積によって支えられているように）．量子コンピュータを実現するためには，超伝導量子ビットに代表されるような量子情報デバイスの物理をよりよく理解し，それを制御するための技術も重要な鍵となってくる．実験に興味がある意欲的な学生は，量子情報デバイスの物理にも挑戦してもらいたい．

2 量子力学の復習から量子情報へ

本節では，量子力学の復習を兼ねて，量子情報でよく使われる表記方法や，時間発展（量子操作），測定，密度演算子などの取り扱いについて説明する．すでに知っている人は，本節を飛ばして次節から読み進めてもらいたい．

2.1 量子状態:ヒルベルト空間

量子状態は内積[*1]が定義された完備[*2]な複素線型空間である**複素ヒルベルト空間** $\mathcal{H}$ の元 $|\psi\rangle \in \mathcal{H}$ によって記述される．有限次元複素ヒルベルト空間の場合であれば，$|\psi\rangle$ を複素列ベクトル $|\psi\rangle = (c_1, ..., c_d)^T$ だと思って差し支えない．双対空間[*3] $\mathcal{H}^*$ 上の元を $\langle\psi|$ と書くことにし，内積を $\langle\psi|\phi\rangle$ と書くことにする．双対空間上の元は，有限次元複素ベクトル空間の場合，複素行ベクトル $\langle\psi| = (c_1^*, ..., c_d^*)$ だと思って問題ない．このように，ヒルベルト空間，及びその双対空間上の元を $|\cdots\rangle$（**ケット**）や $\langle\cdots|$（**ブラ**）を用いて記述することを**ディラックのブラケット表記**という．A をヒルベルト空間 $\mathcal{H}$ から $\mathcal{H}$ への線型演算子としよう．$|\psi\rangle \in \mathcal{H}$ を A で写した元 $|\psi'\rangle = A|\psi\rangle$ に対応する双対空間上の元は $\langle\psi'| \in \mathcal{H}^*$ になるが，$\langle\psi'| = \langle\psi|A^\dagger$ を満たすような演算子 $A^\dagger$ を A の**随伴演算子**と呼び $\dagger$ のマークを用いて書く．つまり，双対空間上での A の作用に対応するものをもとの空間で書いたものが $A^\dagger$ と言える[*4]．$|\psi\rangle$ に対応する双対空間上の元に対しても $\langle\psi| = (|\psi\rangle)^\dagger$ のように書いたりすることもある．有限次元複素ベクトル空間では，随伴 † は転置および複素共役をとること，つまり**エルミート共役**に等しい．

2.2 Schrödinger 方程式と波動関数との関係

量子力学の授業で習った波動関数との関係を見ておこう．量子系の状態の時間発展を記述する Schrödinger 方程式は，

$$i\hbar\frac{\partial}{\partial t}\psi(x,t) = H\psi(x,t) \tag{1}$$

で与えられ，$\psi(x,t)$ は波動関数（適当な境界条件によって規格化できるものとする），ハミルトニアン H はエネルギーに対応する演算子（波動関数に微分演算子や掛け算演算子として作用する）である．時刻 t に位置 x に粒子を見出す確率密度は $|\Psi(x,t)|^2 = \Psi^*(x,t)\Psi(x,t)$（ボルン則）で与えられる．Schrödinger 方程式は，波動関数を空間と時間で分離し，空間部分のエネルギー固有関数

$$H\psi_k(x) = E_k\psi_k(x) \tag{2}$$

を求めることによって解くことができる．E_k は k 番目のエネルギー固有関数の固有値である．境界条件がうまく与えられており，$\psi_k(x)$ が規格化できる，すなわち $\int dx|\psi_k(x)|^2$ が収束するような場合のみ考えることにする．以降，$\psi_k(x)$ は規格化されたものとする．このエネルギー固有関数の時間発展は，

$$i\hbar\frac{\partial}{\partial t}\psi_k(x) = E_k\psi_k(x) \tag{3}$$

[*1] 内積とは，線型空間の任意の 2 つの元 $|\psi\rangle$ と $|\phi\rangle$ と複素数 $(|\psi\rangle, |\phi\rangle) \in \mathbb{C}$ に対応させたものである．

[*2] 完備性とは，コーシー列 $\||\psi\rangle_n - |\phi\rangle_m\| \to 0$ が空間の元 $|\psi\rangle$ に収束する $\||\psi\rangle_n - |\psi\rangle\| \to 0$ ということである．有限次元複素線型空間であれば，複素数の完備性から線型空間の完備性が保証される．

[*3] ヒルベルト空間 V の元 v に作用し複素数を返すような汎関数 $f : V \to \mathbb{C}$ について考える．汎関数 f と g に対して $f + g$ やスカラー倍 αf も定義できるので，汎関数の集合も線型空間になっており，これを線型空間 V の双対空間 V^* と呼ぶ．ことのき Riesz の定理より，ある汎関数 f は必ずヒルベルト空間 V のある元 v と内積 $(v, \cdot)$ を用いて，$f(v') = (v, v')$ という形で一意的に表されるため，そのような汎関数を f_v と書くことにする．V の元 v をケット $|v\rangle$，双対空間 V^* の元 f_v をブラ $\langle v|$ と表記するのがディラックのブラケット表記である．

[*4] $f_{Av}(v') = f_v(A^\dagger v')$

をとけば良いので，$\psi_k(x,t) = e^{-iE_k t/\hbar}\psi_k(x)$ となる．波動方程式では，解の重ね合わせも解として許されるため，エネルギー固有関数の重ね合わせ $\Psi(x,t) = \sum_k c_k\psi_k(x,t) = \sum_k c_k e^{-iE_k t/\hbar}\psi_k(x)$（$c_k \in \mathbb{C}$）が Schrödinger 方程式の一般解となる．ある 2 つの解の和（重ね合わせ）やスカラー倍が定義できるので，波動関数は線型空間を構成していることがわかる．さらに，2 つの解 $\Psi(x,t)$ と $\Phi(x,t)$ を空間的に積分 $\int dx\Psi^*(x,t)\Phi(x,t)$ することによって複素数を得ることができるので，内積を定義することもできる．また，適当な境界条件によって規格化できるということは，この内積から得られるノルム $\|\Psi(x,t)\|^2$ が収束するような関数からなる空間，L^2 空間を考えていることになり，完備性も示すことができる．つまり，Schrödinger 方程式の解からなる集合は，複素ヒルベルト空間を構成していることがわかる．興味のあるエネルギースケールなどの制約から，有限のエネルギー固有状態（$k = 1, 2, ..., d$）だけに興味がある状況を考えよう．この場合，任意の量子状態は，

$$\Psi(x,t) = \sum_{k=1}^{d} c_k\psi_k(x,t) \tag{4}$$

とかける．$\psi_k(x,t)$ をヒルベルト空間の元として $|\psi_k\rangle$（$k = 1, ..., d$）と書くことにする．ハミルトニアンはエネルギー固有状態を用いて，$H = \sum_{k=1}^{d} E_k |\psi_k\rangle\langle\psi_k|$ とかけ $H^\dagger = H$ すなわち，自己随伴（有限次元の場合はエルミート）演算子になっている．このため 2 つのエネルギー固有状態 $|\psi_k\rangle$ と $|\psi_j\rangle$ に対して，$\langle\psi_k| H |\psi_j\rangle = E_k \langle\psi_k|\psi_j\rangle = E_j \langle\psi_k|\psi_j\rangle$ になることから，$E_j \neq E_k$ の場合は 2 つの固有状態は直交 $\langle\psi_k|\psi_j\rangle = 0$ する．また，$E_j = E_k$ の場合に縮退している場合でも，2 つの直交しない固有状態 $|\psi_k\rangle$ と $|\psi_j\rangle$ から，$|\psi_j\rangle = \langle\psi_k|\psi_j\rangle |\psi_k\rangle + \sqrt{1 - |\langle\psi_k|\psi_j\rangle|^2}\,|\psi_k^\perp\rangle$ とすることによって新たに $|\psi_k^\perp\rangle$ を定義する（Gram-Schmidt の直交化）ことによって直交した状態を得ることができる．これらの正規直交基底 $\{|\psi_k\rangle\}$ を用いて波動関数 $|\Psi(x,t)\rangle$ を列ベクトル表示することによって，波動関数と複素列ベクトルが対応することになる．

2.3 時間発展:ユニタリー演算子

Schrödinger 方程式をブラケット表示で書き直してみよう：

$$i\hbar\frac{\partial}{\partial t}|\psi(x,t)\rangle = H|\psi(x,t)\rangle\,. \tag{5}$$

時刻 $t = 0$ の状態 $|\psi(x,0)\rangle$（波動関数）が与えられているとして，Schrödinger 方程式を形式的に解くと，

$$|\psi(x,t)\rangle = e^{-iHt/\hbar}|\psi(x,0)\rangle\,, \tag{6}$$

が得られる．H はエルミート演算子だったので，$e^{-iHt/\hbar}$ はユニタリー演算子（$U^\dagger U = I_d$ [*5]を満たす）になる．このように，量子系の時間発展は，複素ヒルベルト空間上で作用するユニタリー演算子 U によって記述される．

2.4 量子測定:射影演算子

物理における状態とは，そもそも対象とする物理系から実験的に得られる物理量の値やその統計性に関する予言を与えるために必要となるものであった．量子系における測定は，射影演算子 $\{P_i\}_{i=1}^d$ を選び，それに基づいた射影測定を行うことになる．射影演算子とは $P_iP_j = \delta_{ij}P_i$ と $\sum_{i=1}^d P_i = I_d$ を満たすエルミート演算子の集合のことである．例えば，正規直交基底 $\{|i\rangle\}_{i=1}^d$ を 1 つ選び，$P_i = |i\rangle\langle i|$ とすれば射影演算子が得られる．状態 $|\psi\rangle$ に対して，射影演算子 $\{P_i\}$ による射影測定を行ったときに，測定結果 i を得る確率 p_i は，

$$p_i = \|P_i|\psi\rangle\|^2 = \langle\psi| P_i |\psi\rangle \tag{7}$$

[*5] I_d を d 次元空間の恒等演算子とした．

で与えられる．射影演算子の性質から $\sum_i p_i = 1$ になっている．時間発展はユニタリー演算子（内積を保存する）であるため，初期状態が規格化されていれば，常に確率は保存される．古典状態とは異なり，量子状態は確定した 1 つの状態 $|\psi\rangle$ であっても，測定の仕方によってその結果は確率的に与えられることになる．測定結果 i を得た後の状態は $P_i|\psi\rangle/\sqrt{p_i}$ となる．ここまでで，量子系における状態・時間発展・測定の記述が与えられたことになる．

全く同じ量子状態 $|\psi\rangle$ がたくさん与えられ，何度も繰り返し測定するような状況を考えよう．測定結果 i が得られた時の物理量（確率変数）を a_i とする．例えば，エネルギーに関する射影測定 $\{|\psi_k\rangle\langle\psi_k|\}_{k=1}^d$ の場合はエネルギー固有値 E_k になる．このとき，物理量の平均値はエルミート演算子 $A = \sum_{i=1}^d a_i P_i$ を用いて

$$\langle A\rangle \equiv \sum_{i=1}^{d} a_i p_i = \langle\psi| A |\psi\rangle , \tag{8}$$

と計算できる．逆にエルミート演算子であれば，射影演算子 P_i を用いてスペクトル分解 $A = \sum_{i=1}^d a_i P_i$ でき，物理量 A の射影測定や物理量 A の平均値を計算することができるため，A は可観測量と呼ばれる．

2.5 複合系:テンソル積

2 つの量子系 1,2 から成る複合系について考えよう．複合系も全体としては何らかの量子系になっているので複合系の量子状態はあるヒルベルト空間 $\mathcal{H}_{1,2}$ の元として書くことができるであろう．このような状態の例としては，量子系 1 の状態 $|\psi\rangle_1 \in \mathcal{H}_1$ と，量子系 2 の状態 $|\phi\rangle_2 \in \mathcal{H}_2$ との直積状態 $(|\psi\rangle_1, |\phi\rangle_2)$ が含まれているだろう．複合系の線型性から 2 つの直積状態 $(|\psi\rangle_1, |\phi\rangle_2)$ と $(|\psi'\rangle_1, |\phi'\rangle_2)$ の線型和も複合系 $\mathcal{H}_{1,2}$ に含まれることになる．このようにして，$\mathcal{H}_1$ と $\mathcal{H}_2$ の元の直積状態によって張られる線型空間のことをテンソル積空間 $\mathcal{H}_{1,2} = \mathcal{H}_1 \otimes \mathcal{H}_2$ と呼ぶ．直積状態は，$(|\psi\rangle_1, |\phi\rangle_2)$ の代わりに $|\psi\rangle_1 \otimes |\phi\rangle_2$ や，特に混乱しない場合は $|\psi\rangle_1 |\phi\rangle_2$ と書く．テンソル積空間の基底としては，$\mathcal{H}_1$ と $\mathcal{H}_2$ の基底をそれぞれ $\{|i\rangle_1\}_{i=1}^d$ と $\{|j\rangle_2\}_{j=1}^{d'}$ として，それらの直積状態 $\{|i\rangle_1|j\rangle_2\}_{i=1}^{d}{}_{j=1}^{d'}$ を採用することができる．したがって $\mathcal{H}_{1,2}$ の次元は dd' となる．テンソル積の計算には以下のルール（双線型性）が適用される．

$$(|\psi\rangle + |\psi'\rangle) \otimes |\phi\rangle = |\psi\rangle \otimes |\phi\rangle + |\psi'\rangle \otimes |\phi\rangle , \tag{9}$$
$$|\psi\rangle \otimes (|\phi\rangle + |\phi'\rangle) = |\psi\rangle \otimes |\phi\rangle + |\psi\rangle \otimes |\phi'\rangle , \tag{10}$$
$$\alpha(|\psi\rangle \otimes |\phi\rangle) = (\alpha |\psi\rangle \otimes |\phi\rangle) = (|\psi\rangle \otimes \alpha |\phi\rangle). \tag{11}$$

$\{|i\rangle_1\}_{i=1}^d$ と $\{|j\rangle_2\}_{j=1}^{d'}$ を基底として列ベクトル表示した状態 $|\psi\rangle_1 = (a_1, ..., a_d)^T$ と $|\phi\rangle_2 = (b_1, ..., b_{d'})^T$ のテンソル積状態，$|\psi\rangle_1 \otimes |\phi\rangle_2$ を基底 $\{|i\rangle_1|j\rangle_2\}_{i=1}^{d}{}_{j=1}^{d'}$ に対してベクトル表示すると，

$$|\psi\rangle_1 \otimes |\phi\rangle_1 = \begin{pmatrix} a_1 \\ \vdots \\ a_d \end{pmatrix} \otimes \begin{pmatrix} b_1 \\ \vdots \\ b_{d'} \end{pmatrix} = \begin{pmatrix} a_1 b_1 \\ a_1 b_2 \\ \vdots \\ a_1 b_{d'} \\ \vdots \\ a_d b_{d'} \end{pmatrix} \tag{12}$$

となる．このように d 次元ベクトルと d' 次元ベクトルから dd' 次元ベクトルを構成することを**クロネッカー積**と呼ぶ．$\mathcal{H}_{1,2}$ 上の状態は必ずしも $|\psi\rangle_1 \otimes |\phi\rangle_2$ と書けるとは限らない．特に，$|\psi\rangle_1 \otimes |\phi\rangle_2$ と書ける場合を**直積状態**と呼び，そのようにかけない状態を**エンタングル状態**と呼ぶ．

$\mathcal{H}_1$ と $\mathcal{H}_2$ 上の演算子 A と B のテンソル積演算子 $A \otimes B$ の $\mathcal{H}_{1,2}$ 上での作用は，

$$(A \otimes B)|\psi\rangle_1 \otimes |\phi\rangle_2 = (A|\psi\rangle_1) \otimes (B|\phi\rangle_2) \tag{13}$$

で定義される．テンソル積演算子も双線型性

$$(A+A')\otimes(B+B')=A\otimes B+A\otimes B'+A'\otimes B+A'\otimes B' \tag{14}$$

が成り立つ．したがって，$A=\sum_{i,i'}a_{i'i}|i'\rangle\langle i|$ と $B=\sum_{j,j'}b_{j'j}|j'\rangle\langle j|$ として $a_{i'i}$ と $b_{j'j}$ を成分として行列表示すると，テンソル積演算子は

$$(A\otimes B)=\sum_{i,i',j,j'}a_{i'i}b_{j'j}(|i'\rangle\otimes|j'\rangle)(\langle i|\otimes\langle j|) \tag{15}$$

で与えられることになるので，２つの行列のクロネッカー積は

$$A\otimes B=\begin{pmatrix}a_{11}&\cdots&a_{1d}\\ \vdots&\ddots&\vdots\\ a_{d1}&\cdots&a_{dd}\end{pmatrix}\otimes\begin{pmatrix}b_{11}&\cdots&b_{1d'}\\ \vdots&\ddots&\vdots\\ b_{d'1}&\cdots&b_{d'd'}\end{pmatrix} \tag{16}$$

$$=\begin{pmatrix}a_{11}B&\cdots&a_{1d}B\\ \vdots&\ddots&\vdots\\ a_{d1}B&\cdots&a_{dd}B\end{pmatrix}=\begin{pmatrix}a_{11}b_{11}&\cdots&a_{11}b_{1d'}&\cdots&a_{1d}b_{1d'}\\ \vdots&\ddots&\vdots&&\vdots\\ a_{11}b_{d'1}&\cdots&a_{11}b_{d'd'}&\cdots&a_{1d}b_{d'd'}\\ \vdots&&&\ddots&\vdots\\ a_{d1}b_{d'1}&\cdots&a_{d1}b_{d'd'}&\cdots&a_{dd}b_{d'd'}\end{pmatrix}. \tag{17}$$

2.6 密度演算子，一般量子操作，一般化測定

これまで確率 1 で 1 つの定まった量子状態 $|\psi\rangle$ が与えられるような状況を考えてきた．これを拡張して，確率的に異なる量子状態が与えられるような状況を考えよう．このためには，密度演算子 $\rho=|\psi\rangle\langle\psi|$ を用いて状態を記述すると便利である（状態とは測定に係る統計性を予言するためのものであったのでその目的が果たせれば何でもよい）．射影演算子 $\{P_k\}$ による射影測定は，

$$p_k=\langle\psi|P_k|\psi\rangle=\langle\psi|(\sum_{i=1}^{d}|i\rangle\langle i|)P_k|\psi\rangle=\sum_{i=1}^{d}\langle i|P_k|\psi\rangle\langle\psi||i\rangle \tag{18}$$

$$=\mathrm{Tr}[P_k|\psi\rangle\langle\psi|] \tag{19}$$

のように，トレース $\mathrm{Tr}[\cdots]=\sum_{i=1}^{d}\langle i|\cdots|i\rangle$ を用いて計算することができる．ただし正規直交基底 $\{|i\rangle\}_{i=1}^{d}$ の完全性 $\sum_i|i\rangle\langle i|=I_d$ を用いた．トレース Tr は正規直交基底の選び方に依存せず決まり，また，$\mathrm{Tr}[ABC]=\mathrm{Tr}[CAB]$ を満たす．

さて，確率 $\{q_j\}$ で異なる量子状態 $\{|\psi_j\rangle\}$ が与えられ，射影測定 $\{P_i\}$ を行う状況を考えよう．確率の結合法則を認めると，測定結果 i を得る確率は，

$$p_i=\sum_j q_j\mathrm{Tr}[P_i|\psi_j\rangle\langle\psi_j|]=\mathrm{Tr}[P_i\sum_j q_j|\psi_j\rangle\langle\psi_j|] \tag{20}$$

となる．よって密度演算子として $\rho\equiv\sum_j q_j|\psi_j\rangle\langle\psi_j|$ を採用しておけば，このような古典的な確率的混合状態に対する射影測定の確率分布は $p_i=\mathrm{Tr}[P_i\rho]$ によって与えられる．

密度演算子 ρ の性質を確認しておこう．$\sum_i p_i=1$ になるために，$\mathrm{Tr}[\rho]=1$ が要求される．また，定義から密度演算子はエルミート演算子 $\rho=\rho^\dagger$ である．$\rho=\sum_j q_j|\psi_j\rangle\langle\psi_j|$ のような分解ができることから任意の $|v\rangle$ に対して，$\langle v|\rho|v\rangle\geq 0$，つまり，半正定値（positive-semidefinite）[*6]演算子となっている．特に ρ がランク 1 の場合，つまり $\rho=|\psi\rangle\langle\psi|$ と書ける場合に**純粋状態**と呼ばれる．$\mathrm{Tr}[\rho^2]$ は**純粋度**と呼ばれ，$\mathrm{Tr}[\rho^2]=1$ となる時だけが純粋状態である．密度演算子 ρ に対するユニタリー時間発展は $\rho\to U\rho U^\dagger$. によって記述される．

[*6] 任意の $|v\rangle$ に対して $\langle v|A|v\rangle\geq 0$ となる演算子 A を半正定値演算子という．すべての固有値が ≥ 0 となる演算子としてもよい．

そもそも，なぜ密度演算子を導入する必要があるのだろうか？確率的に量子状態を送りつけてくる装置も含めて”コヒーレント”に複合系の量子状態を純粋状態 $\sum_j \sqrt{q_j}|j\rangle|\psi_j\rangle$ として記述しておけば，古典的な確率混合を排除できるはずである．しかし，しばしば，複合系も含めて（宇宙全体の純粋状態を）書くと面倒になることがある．量子状態を送りつけてくる装置にアクセスできないという状況では，部分系だけを混合状態として密度演算子として書くことによって簡潔に状態が記述できることがよくある．

例えば，量子系 1,2 の複合系の状態 $\rho_{1,2} = |\Psi\rangle\langle\Psi|_{1,2}$ があるとする．この時，量子系 2 からの情報を一切受け取らずに量子系 1 のみで射影測定 $\{P_k\}$ を行った時の確率は，

$$p_k = \mathrm{Tr}\left[(P_k \otimes I_{d'})|\Psi\rangle\langle\Psi|_{1,2}\right] \tag{21}$$

になる．複合系でのトレースは $\sum_{ij}\langle i|_1\langle j|_2\cdots|i\rangle_1|j\rangle_2$ で与えられるが，先に量子系 2 上でのトレースを複合系の状態に対してとってやる

$$\rho_1 \equiv \mathrm{Tr}_2[\rho_{1,2}] = \sum_{j=1}^{d'}(I_d \otimes \langle j|_2)\rho_{1,2}(I_d \otimes |j\rangle_2) \tag{22}$$

ことによって，

$$p_k = \mathrm{Tr}_1\left[P_k\rho_1\right]. \tag{23}$$

このように部分系に関するトレースをとることを**部分トレース**と呼び，部分トレースをとった密度演算子 ρ_1 のことを**縮約密度演算子** (reduced density operator) と呼ぶ．先の例 $\sum_j \sqrt{q_j}|j\rangle|\psi_j\rangle$ の場合，装置にアクセスできないもとでは装置系に対して部分トレースをとると，縮約密度演算子として混合状態 $\sum_j q_j|\psi_j\rangle\langle\psi_j|$ が得られる．このように，宇宙全体の状態がたとえ純粋状態であったとしても，我々が興味をもつ部分系だけで閉じた議論をするときには，その系は古典的な混合状態として密度演算子を用いて記述されることになる．逆に，任意の密度演算子は，スペクトル分解することによって直交する状態 $\{|\psi_j\rangle\}$ を用いて $\rho = \sum_j q_j|\psi_j\rangle\langle\psi_j|$ と書けるので，何らかの補助系を付け加えて，それらの複合系上で純粋状態 $\sum_j \sqrt{q_j}|\psi_j\rangle|j\rangle$ として記述することもできる．これを**純粋化** (purification) と呼ぶ．同様に，複合系を付け加えた複合系でのユニタリー時間発展や射影測定を部分系のみで記述することによって，部分系だけで閉じた形で量子操作や量子測定を一般化することができる．

密度演算子に対する物理的に許されたもっとも一般的な量子操作について考える．物理的に許される密度演算子 ρ はトレースが 1 である半正定値演算子であった．量子操作においても確率が保存されるとすると，トレースを保存し，かつ半正定値性を保つ写像が物理的に許される量子操作といえそうだ．しかし，それではまだ不十分である．先の議論のように，密度演算子を扱う場合は，補助系を追加されるような状況を含めたい．このため，密度演算子そのものの正定値性だけでなく，任意の補助系を追加してその複合系の状態を考えても正定値性が保たれていなければならないという強い要請が必要になる．これを満たすものが CPTP 写像（completely-positive trace preserving map）である．$\mathcal{L}(\mathcal{H})$ を $\mathcal{H}$ 上で作用する演算子からなる空間とすると，CPTP 写像 $\mathcal{E} : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H})$ は，

$$\mathcal{E}(\rho+\sigma) = \mathcal{E}(\rho) + \mathcal{E}(\sigma), \quad \text{(線型性)} \tag{24}$$

$$\mathrm{Tr}[\mathcal{E}(\rho)] = 1 \ \text{(ただし } \mathrm{Tr}[\rho] = 1), \quad \text{(trace preserving)} \tag{25}$$

$$\mathcal{E} \otimes \mathcal{I}(\tilde{\rho}) \geq 0 \quad \text{(complete positivity)} \tag{26}$$

を満たすものである．$\mathcal{I}$ は追加した補助系上の恒等操作，$\tilde{\rho}$ は補助系も含めた複合系の密度演算子，≥ 0 は半正定値性を意味する．物理的な操作になるためには完全正値性が必要である具体例を見ておこう．密度演算子の転置

$\mathcal{T}(\rho)=\rho^T$ をとるような操作を考える．$\rho=\sum_{ij} r_{ij}|i\rangle\langle j|$ とすると，$\mathcal{T}(\rho)=\sum_{ij} r_{ji}|i\rangle\langle j|$ となる．一方，

$$\langle v|\rho|v\rangle=\sum_{ij} r_{ij}\langle v|i\rangle\langle j|v\rangle=\sum_{ij} r_{ji}\langle v|j\rangle\langle i|v\rangle \tag{27}$$

$$=\left(\sum_{ij} r_{ji}\langle v|i\rangle\langle j|v\rangle\right)^*=(\langle v|\mathcal{T}(\rho)|v\rangle)^* \tag{28}$$

となるので $\rho\geq 0$ から，$\mathcal{T}(\rho)\geq 0$ も言える．よって転置をとる操作は正値性を満たすことになる．複合系でのエンタングル状態

$$|\Phi^+\rangle\equiv\frac{|0\rangle_1|0\rangle_2+|1\rangle_1|1\rangle_2}{\sqrt{2}} \tag{29}$$

に対して 1 系だけに転置をとる操作 $\mathcal{T}\otimes\mathcal{I}$ を考える．密度演算子は，

$$|\Phi^+\rangle\langle\Phi^+|=\frac{1}{2}\begin{pmatrix}1&0&0&1\\0&0&0&0\\0&0&0&0\\1&0&0&1\end{pmatrix} \tag{30}$$

なので，系 1 の転置は，

$$\mathcal{T}\otimes\mathcal{I}(|\Psi^+\rangle\langle\Phi^+|)=\frac{1}{2}\begin{pmatrix}1&0&0&0\\0&0&1&0\\0&1&0&0\\0&0&0&1\end{pmatrix}, \tag{31}$$

となり，負の固有値を持つため半正定値演算子にはならない．エンタングルした状態の一方に量子操作を施した結果物理的ではない状態が得られるような量子操作は認めたくない．よって，着目している系の正定値性を保つだけではなく，補助系を追加した複合系においても正定値性が保たれる，CPTP 写像が物理的に許された量子操作を表すことになる．CPTP 写像 $\mathcal{E}$ は必ず，$\sum_k E_k^\dagger E_k=I$ を満たす Kraus 演算子 E_k を用いて，

$$\mathcal{E}\rho=\sum_k E_k\rho E_k^\dagger \tag{32}$$

と書くことができる（Kraus 表現）．また，このような CPTP 写像は，補助系 (a) と着目している系 (s) の複合系上のユニタリー時間発展 $U_{\rm s,a}$ に対して，補助系をトレースアウトすることによって得られる:

$$\mathcal{E}\rho=\mathrm{Tr}_{\rm a}[U_{\rm s,a}\rho\otimes|e\rangle\langle e|_{\rm a}U_{\rm s,a}^\dagger]=\sum_k E_k\rho E_k^\dagger, \tag{33}$$

この時，$\{|k\rangle_a\}$ を補助系の正規直交基底として，Kraus 演算子は，$E_k=(I_{\rm s}\otimes\langle k|_{\rm a})U_{\rm s,a}(I_{\rm s}\otimes|e\rangle_{\rm a})$ と書き表される．CPTP 写像や量子操作というとユニタリー時間発展とは本質的に異なる難しいことをしているように感じるかもしれないが，宇宙全体でみたときには単なる純粋状態に対するユニタリー時間発展に対応するものを，（必ずしも宇宙全体を操作したり観測したりすることはできないし，そもそも宇宙全体をわざわざ記述することも面倒なので）興味のある着目した系だけで閉じた都合の良い形で書いているだけのことである．

同様に，着目する系（s）と補助系（a）から成る複合系において，s 系と a 系の初期状態をそれぞれ $\rho_{\rm s}$ と $|e\rangle\langle e|_{\rm a}$ とし複合系のユニタリー時間発展を $U_{\rm s,a}$ とし，補助系において射影測定 $\{|k\rangle\langle k|_{\rm a}\}$ をすることにする．測定結果 k を得る確率は，

$$p_k=\mathrm{Tr}_{\rm s,a}[I_{\rm s}\otimes|k\rangle\langle k|_{\rm a}U_{\rm s,a}\left(\rho_{\rm s}\otimes|e\rangle\langle e|_{\rm a}\right)U_{\rm s,a}^\dagger] \tag{34}$$

$$=\mathrm{Tr}_{\rm s}[E_k^\dagger E_k\rho_{\rm s}] \tag{35}$$

となる．つまり，$E_k = I_{\rm s} \otimes \langle k|_{\rm a} U_{\rm s,a} I_{\rm s} \otimes |e\rangle_{\rm s}$ として定義した演算子 $M_k \equiv E_k^\dagger E_k$ を射影演算子の代わりすることによって，着目する系だけで閉じた形，

$$p_k = {\rm Tr}_{\rm s}[M_k \rho_s] \tag{36}$$

で書くことができる．定義から $M_k \geq 0$ かつ $\sum_k M_k = I_s$ となっており，p_k は確かに確率になっている（複合系の射影測定を行っていることから自明である）．測定結果 k が得られたときの測定後の状態は，

$$E_k \rho E_k^\dagger / {\rm Tr}[E_k \rho E_k^\dagger] \tag{37}$$

となっている．このようにして，一般に $M_k \geq 0$ かつ $\sum_k M_k = I$ となる演算子の集合 $\{M_k\}$ を **POVM 演算子**（positive operator valued measure）と呼び，**一般化測定（POVM 測定）**，

$$p_k = {\rm Tr}[M_k \rho] \tag{38}$$

が定義される．測定後の状態はあるユニタリー演算子 U_k を用いて定義した測定演算子 $E_k \equiv U_k \sqrt{M_k}$ [*7] によって

$$E_k \rho E_k^\dagger / {\rm Tr}[E_k \rho E_k^\dagger] \tag{39}$$

で与えられる．以上のように，純粋状態，ユニタリー時間発展，射影測定を複合系において行い，着目する系だけにおいて記述することによって，密度演算子，CPTP 演算子，POVM 測定が得られた．

3 量子ビット

3.1 Bloch 球

量子力学系（有限次元）の一般的な取り扱いについて一通り説明したので，本題である量子コンピュータの話をすすめていく．古典の情報の世界における情報の最小単位はビットという 0 と 1 の 2 値をもつ変数である．同様に，量子の世界の情報の最小単位は，2 次元複素ヒルベルト空間上の状態，**量子ビット**によって記述される．量子ビットは，直交する 2 つの状態（量子計算に使う基準となる基底として，**計算基底**と呼ぶことにする）$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ と $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, の線型和として

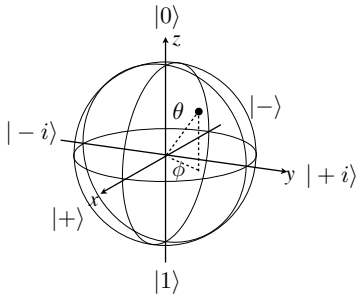
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{40}$$

と一般的に書くことができる．ここで，α と β は，$|\alpha|^2 + |\beta|^2 = 1$ を満たす複素数とした．$|0\rangle$ と $|1\rangle$ の直交する 2 状態としては，原子の 2 つのエネルギー状態，光子の直交する偏光状態，電子・核スピンなど，直交する 2 つの量子状態であればなんでも良い．これらの複素数は，$\theta \in [0, 2\pi)$ と $\phi \in [0, \pi/2)$ を用いて

$$\alpha = \cos\frac{\theta}{2}, \quad \beta = e^{i\phi} \sin\frac{\theta}{2}, \tag{41}$$

と書くことができる．ここで，量子状態全体に作用する位相 $e^{i\gamma}|\psi\rangle$ は測定確率には一切寄与しないので無視していることに注意する．これら θ と ϕ を用いて量子ビットの状態を半径 1 の球面（**Bloch 球**）上に表示することができる．

[*7] エルミート（自己随伴）演算子 A の関数 $f(A)$ は，演算子 A の固有値 $\{a_i\}$ と固有空間への射影演算子 $\{P_i\}$ を用いたスペクトル分解 $A = \sum_i a_i P_i$ を利用して，$f(A) = \sum_i f(a_i) P_i$ として定義される．特に，$\sqrt{A} = \sum_i \sqrt{a_i} P_i$ と定義される．



3.2 パウリ演算子

量子計算に必要となる量子ビットに対する演算子を定義していこう．もっとも重要な演算子は**パウリ演算子**である：

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix},\ Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{42}$$

X, Y, Z を $\sigma_1, \sigma_2, \sigma_3$ と書くこともあるが，量子情報では X, Y, Z と書くと便利なことが多いので，このように書くことにする．$X^2 = Y^2 = Z^2 = I$, $XZ = -ZX$（どの 2 つも互いに反交換する），$Y = iXZ$ などの関係式はよく使うので覚えておこう．量子ビットを定義した基底は $|0\rangle$ と $|1\rangle$ パウリ Z 演算子の固有状態 $Z|0\rangle = |0\rangle$, $Z|1\rangle = -|1\rangle$ となっている．計算基底 $\{|0\rangle, |1\rangle\}$ に対するパウリ X 演算子の作用は，

$$|1\rangle = X|0\rangle, \quad |0\rangle = X|1\rangle. \tag{43}$$

のように量子ビットを反転させる作用となる．パウリ X 演算子の固有状態として，$|0\rangle$ と $|1\rangle$ の重ね合わせ状態，

$$|+\rangle \equiv \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \quad |-\rangle \equiv \frac{|0\rangle - |1\rangle}{\sqrt{2}}, \tag{44}$$

を定義しておこう．同様に，パウリ Y 演算子の固有状態として

$$|+i\rangle \equiv \frac{|0\rangle + i|1\rangle}{\sqrt{2}}, \quad |-i\rangle \equiv \frac{|0\rangle - i|1\rangle}{\sqrt{2}}, \tag{45}$$

を定義しておく．これらパウリ X, Y, Z 演算子の固有状態からなる基底をそれぞれ X, Y, Z 基底と呼ぶことにする．これらパウリ演算子の固有状態は，Bloch 球上の x, y, z 軸上に存在する．Bloch 球上の座標は，パウリ演算子を用いて

$$(r_x, r_y, r_z) = (\mathrm{Tr}[X\rho], \mathrm{Tr}[Y\rho], \mathrm{Tr}[Z\rho]), \tag{46}$$

として与えることもできる．この場合，純粋状態だけではなく，1 量子ビットの任意の混合状態の場合も記述することが可能である．純粋度は $\mathrm{Tr}[\rho^2] = r_x^2 + r_y^2 + r_z^2$ となることから，純粋状態は半径 1 の球面上，混合状態はその内部に対応することになる．確率 $|0\rangle$, $|1\rangle$ の確率 $1/2$ での混合状態 $\frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)$ は Bloch 球の原点に対応する．古典ビットや，その確率的混合は，Bloch 球では z 軸上の状態に対応する一方，一般の量子状態は半径 1 の球面上及びその内部を状態としてとれることから，古典情報よりも一般的な情報を表現できることがわかる．

3.3 アダマール・位相演算子

次に重要な 1 量子ビット演算子はアダマール演算子 H と位相演算子 S である：

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}.$$

これらの演算子は，あるパウリ基底を他のパウリ基底へと変換する．例えば，$H:\{|0\rangle,|1\rangle\}\leftrightarrow\{|+\rangle,|-\rangle\}$，$S:\{|+\rangle,|-\rangle\}\leftrightarrow\{|+i\rangle,|-i\rangle\}$．これは，これらの演算子をパウリ演算子に対して共役作用[*8]させたとき他のパウリ演算子が得られることに対応する:

$$X=HZH,\quad Y=SXS^{\dagger}. \tag{47}$$

アダマール演算子 H の Bloch 球上での作用は，x 軸と z 軸の入れ替えに対応している．位相演算子 S の作用は，z 軸を中心に $\pi/2$ 回転していることになる．このように，共役作用のもとでパウリ演算子を再びパウリ演算子に写す演算子を Clifford 演算子[*9]とよぶ．

3.4 1 量子ビットの任意の回転

アダマール演算子や位相演算子を繰り返し作用させても任意の 1 量子ビットのユニタリー演算子を構成することはできない．1 量子ビットのユニタリー演算子 U は一般に

$$U=\begin{pmatrix} u_{11} & u_{12}\\ u_{21} & u_{22}\end{pmatrix} \tag{48}$$

の 4 つの複素数によって記述され，$U^{\dagger}U=I$ より，

$$|u_{11}|^2+|u_{21}|^2=1,\quad u_{12}^{*}u_{11}+u_{22}^{*}u_{21}=0,\quad |u_{22}|^2+|u_{12}|^2=1 \tag{49}$$

を満たすことになる．これを満たす複素数は必ず，

$$u_{11}=e^{i\alpha}e^{-i(\beta+\delta)2}\cos(\gamma/2),\quad u_{21}=e^{i\alpha}e^{i(\beta-\delta)/2}\sin(\gamma/2), \tag{50}$$

$$u_{12}=-e^{i\alpha}e^{-i(\beta-\delta)/2}\sin(\gamma/2),\quad u_{22}=e^{i\alpha}e^{i(\beta-\delta)/2}\cos(\gamma/2), \tag{51}$$

と書き表すことができる．このことから，

$$U=e^{i\alpha}e^{-i(\beta/2)Z}e^{-i(\gamma/2)Y}e^{-i(\delta/2)Z} \tag{52}$$

のように分解できることになる．ここで，$e^{-i(\theta/2)A}=\cos(\theta/2)I-i\sin(\theta/2)A$（$A=X,Y,Z$）は，Bloch 球上でそれぞれ x, y, z 軸を中心に θ 回転させる操作に対応する．よって，任意の 1 量子ビットユニタリー演算子は全体の位相 $e^{i\alpha}$ を除いて，2 つの直交する軸を中心とした回転に分解することができる（**オイラー分解**）．

一般に Bloch 球上での (r_x,r_y,r_z) 方向（$|r_x|^2+|r_y|^2+|r_z|^2=1$）を中心とした θ 回転は，

$$e^{-i(\theta/2)(r_xX+r_yY+r_zZ)} \tag{53}$$

となる．これは，以下の事実から示すことができる．まず，Bloch 球上の点 $(1,0,0)$ を (r_x,r_y,r_z) に写すユニタリー演算子を U とした時，点 $(1,0,0)$ が $|+\rangle$ に対応することを使うと，

$$(r_x,r_y,r_z)=(\mathrm{Tr}[U|+\rangle\langle+|U^{\dagger}X],\mathrm{Tr}[U|+\rangle\langle+|U^{\dagger}Y],\mathrm{Tr}[U|+\rangle\langle+|U^{\dagger}Z]) \tag{54}$$

を満たしていることになる．σ_i（$i=0,1,2,3$）をパウリ演算子（I,X,Y,Z）として，$\mathrm{Tr}[\sigma_i\sigma_j]=2\delta_{ij}$ となることから，

$$U|+\rangle\langle+|U^{\dagger}=U\frac{I+X}{2}U^{\dagger}=\frac{I+r_xX+r_yY+r_zZ}{2} \tag{55}$$

$$\Leftrightarrow UXU^{\dagger}=r_xX+r_yY+r_zZ, \tag{56}$$

[*8] 演算子 A の演算子 B に対する共役作用とは，$ABA^{\dagger}$ によって定義される．

[*9] パウリ演算子から生成される群をパウリ群とすると，Clifford 演算子はパウリ群を共役作用のもとで不変にする，つまり，パウリ群を正規部分群としてもつ演算子である．このような演算子は群を成し，Clifford 群と呼ばれる．

となる．$(1,0,0)$ 軸に対する θ 回転は $e^{-i(\theta/2)X}$ なので，(r_x,r_y,r_z) 軸に対する θ 回転は $Ue^{-i(\theta/2)X}U^\dagger = e^{-i(\theta/2)(r_xX+r_yY+r_zZ)}$ と書けることがわかる．

3.5 ユニタリー演算子の近似と計算の精度

1 量子ビットの任意のユニタリー演算子を実現するためには，特定の軸周りに任意の角度で回転させる必要があった．量子コンピュータを構成する上では，有限個の量子演算から任意の量子計算，つまり万能量子計算を構成したい．厳密な意味で 1 量子ビットのユニタリー演算子を実現するためには，無限個の量子演算を必要とすることになるが，実際には厳密なユニタリー演算を実現する必要はなく，十分良い精度 ϵ で任意のユニタリー演算子を近似できれば良い．例えば，演算子 1-ノルム（もしくはトレースノルム）$\|\cdot\|_1$ [*10]を用いて，理想的なユニタリー演算子 $\{U_i\}_{i=1}^N$ に対して，$\left\|\tilde{U}_i - U_i\right\|_1 \le \epsilon$ を満たすような $\{\tilde{U}_i\}_{i=1}^N$ が実現されたとしよう．これらユニタリー演算子の積 $U \equiv \prod_{i=1}^N U_i$ と $\tilde{U} \equiv \prod_{i=1}^N \tilde{U}_i$ の誤差は，演算子 1-ノルムの性質（ユニタリー不変性及び三角不等式）を使うと

$$\left\|\tilde{U} - U\right\|_1 = \left\|\prod_{i=1}^N \tilde{U}_i - U_N \prod_{i=1}^{N-1} \tilde{U}_i + U_N \prod_{i=1}^{N-1} \tilde{U}_i - \prod_{i=1}^N U_i\right\|_1 \tag{57}$$

$$\vdots \tag{58}$$

$$= \left\|\sum_{k=1}^N \left[\left(\prod_{i=k+1}^N U_i\right)(\tilde{U}_k - U_k)\left(\prod_{i=1}^{k-1}\tilde{U}_i\right)\right]\right\|_1 \tag{59}$$

$$\le \sum_{k=1}^N \left\|\left[\left(\prod_{i=k+1}^N U_i\right)(\tilde{U}_k - U_k)\left(\prod_{i=1}^{k-1}\tilde{U}_i\right)\right]\right\|_1 \tag{60}$$

$$= \sum_{k=1}^N \left\|\left[(\tilde{U}_k - U_k)\right]\right\|_1 \le N\epsilon \tag{61}$$

となる．これら近似的なユニタリー演算子を作用させたのち射影測定を行ったときの確率分布 $\{\tilde{p}_k\}$ と理想的な場合 $\{p_k\}$ との誤差は l_1-ノルム（確率分布の全変動距離, total variation distance）を用いて

$$\|\tilde{p}_k - p_k\|_1 = \sum_k |\tilde{p}_k - p_k| = \sum_k |\mathrm{Tr}[P_k W]| = \sum_k \left|\sum_j w_j \langle w_j|P_k|w_j\rangle\right| \tag{62}$$

$$\le \sum_{k,j} |w_j|\,|\langle w_j|P_k|w_j\rangle| \le \sum_j |w_j| = \|W\|_1 \tag{63}$$

ただし，$W \equiv \tilde{U}|\psi\rangle\langle\psi|\tilde{U}^\dagger - U|\psi\rangle\langle\psi|U^\dagger$ とし（$W = W^\dagger$），$|w_j\rangle$ を W の固有値 $w_i \in \mathbb{R}$ の固有ベクトルとした．一方，

$$\|W\|_1 = \left\|\tilde{U}|\psi\rangle\langle\psi|\tilde{U}^\dagger - U|\psi\rangle\langle\psi|U^\dagger\right\|_1 \tag{64}$$

$$= \left\|(\tilde{U} - U)|\psi\rangle\langle\psi|\tilde{U}^\dagger - U|\psi\rangle\langle\psi|(U^\dagger - \tilde{U}^\dagger)\right\|_1 \tag{65}$$

$$\le \left\|(\tilde{U} - U)|\psi\rangle\langle\psi|\tilde{U}^\dagger\right\|_1 + \left\|U|\psi\rangle\langle\psi|(U^\dagger - \tilde{U}^\dagger)\right\|_1 \tag{66}$$

$$= 2\left\|(\tilde{U} - U)|\psi\rangle\langle\psi|\tilde{U}^\dagger\right\|_1 \tag{67}$$

$$\le 2\left\|(\tilde{U} - U)\right\|_1 \left\||\psi\rangle\langle\psi|\tilde{U}^\dagger\right\|_1 = 2N\epsilon. \tag{68}$$

[*10] 演算子 1-ノルム（1-norm）は，$\mathrm{Tr}\sqrt{AA^\dagger}$．もしくは A を特異値分解し，すべての特異値（$\sqrt{AA^\dagger}$ の固有値）の和をとったものである．$\|A\|_1 = \left\|A^\dagger\right\|_1$ 及び，任意のユニタリー演算子に対して $\|A\|_1 = \|AU\|_1 = \|UA\|_1$ を満たす．また，劣加法性 $\|A+B\|_1 \le \|A\|_1 + \|B\|_1$ 及び，劣乗法性 $\|AB\|_1 \le \|A\|_1\,\|B\|_1$ を満たす．

よって，近似的な確率分布は l_1 ノルムの意味で誤差 $2N\epsilon$ の範囲内にいる．つまり，1 つのユニタリー演算の誤差 ϵ をユニタリ演算子の総数 N よりも十分小さくすることができれば，十分精度の高い出力が得られることになる．

3.6 Solovay-Kitaev アルゴリズム

アダマール演算子や位相演算子は，Bloch 球上での軸の入れ替えや $\pi/2$ 回転に対応していたため，これらの演算子の積で任意のユニタリー演算子を構成することはできない．1 量子ビットユニタリ演算子を任意の精度 ϵ で近似するためには，これらの他に $\pi/8$ 演算子

$$T = e^{-i(\pi/8)Z} \tag{69}$$

が必要となる．$\pi/8$ 回転は π の有理数倍になるので，この演算子（及び，H と S）の積から任意の 1 量子ビットユニタリー演算子を構成できないような気もするが，実は $THTH$ がある方向についての π の無理数倍の角度の回転になっていることが以下の議論からわかる．まず，

$$V \equiv THTH = e^{-i(\pi/8)Z}e^{-i(\pi/8)X} = \frac{1}{2\sqrt{2}}\left[(\sqrt{2}+1)I - iX - iZ - i(\sqrt{2}-1)Y\right], \tag{70}$$

$$V^\dagger = \frac{1}{2\sqrt{2}}\left[(\sqrt{2}+1)I + iX + iZ + i(\sqrt{2}-1)Y\right], \tag{71}$$

とすると，

$$VXV^\dagger = \frac{\sqrt{2}}{2}(X+Y) \tag{72}$$

$$VYV^\dagger = \frac{1}{2}(-X+Y+\sqrt{2}Z) \tag{73}$$

$$VZV^\dagger = \frac{1}{2}(X-Y+\sqrt{2}Z) \tag{74}$$

になるため，$\frac{X+(-1+\sqrt{2})Y+Z}{\sqrt{5-2\sqrt{2}}}$ は V の共役作用のもとで不変であることがわかる．$(1,-1+\sqrt{2},1)$ 方向と直交する方向として Bloch 球上の点 $(1/\sqrt{2},0,-1/\sqrt{2})$ 方向を選び，V によって回転させると，点 $(\frac{2-\sqrt{2}}{4},\frac{2+\sqrt{2}}{4},-\frac{1}{2})$ が得られる．よって回転角は内積の公式から，

$$\theta = \arccos\left(\frac{2\sqrt{2}-1}{4}\right) \tag{75}$$

を満たす角度となる．この回転角は π の無理数倍になっており，V を繰り返し作用させることによってこの軸方向の回転に対しては稠密（任意の角度の回転を近似できる）になっている．また，同様の議論から，HVH は $(1,1-\sqrt{2},1)$ 方向を中心とした π の無理数倍の回転になっている．2 つの異なる軸に対して，任意の角度の回転を近似することができるので，これらを繰り返すことによって任意の 1 量子ビットユニタリー演算子を近似することができる．よって，$\{H,T\}$ の 2 つの 1 量子ビット演算から任意の 1 量子ビットユニタリー演算が近似的に構成できることがわかった．Solovay-Kitaev の定理より，演算子ノルムの意味で誤差 ϵ の近似に必要な $\{H,T\}$ の個数は，$\log(1/\epsilon)$ の多項式で十分であることが知られている（例えば [1] もしくは [2] 参照）．前述の議論から，$1/\epsilon$ は 1 量子ビット演算の個数に対して高々多項式的にしか増えないので，非常に効率よく理想的な 1 量子ビット演算を近似することができる．

4 万能量子計算

万能量子計算とは，n 量子ビットの任意のユニタリー演算を近似的に実行できるような量子計算を意味する．我々の世界が量子力学によって記述されていることを考慮すると，万能量子コンピュータは，量子力学のルールで

動きかつあらゆる量子系のダイナミクスを含んだ任意の物理系と互換性があるマシンであるといえる．したがって，万能量子コンピュータにおける時間発展（量子計算）において何らかの制約が明らかになったとき，任意の物理系は（量子力学に従う限り）その制約に従わなければならないことになる．以下では，どのようにして，有限個の量子演算から，n 量子ビットの任意のユニタリー演算が構成されるかを見ていきたい．

4.1 CNOT 演算

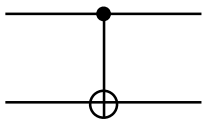
任意の n 量子ビットのユニタリー演算を構成するためには，相互作用を必要とする 2 量子ビット演算が必要になる．2 量子ビット演算の代表的なものが CNOT（controlled-not）演算，

$$\Lambda_{c,t}(X) = |0\rangle\langle 0|_c I_t + |1\rangle\langle 1|_c X_t,$$

である[*11]．c 系（コントロール系）が 1 のときに t 系（ターゲット系）に対してパウリ X 演算子を作用させる．計算基底の入力 $|i\rangle_c|j\rangle_t$ に対して CNOT 演算は排他的論理和（XOR）をターゲット系に出力する，$\Lambda_{c,t}(X)|i\rangle_c|j\rangle_t = |i\rangle_c|i \oplus j\rangle_t$．c 系の入力状態が重ね合わせ状態 $|+\rangle_c|0\rangle_t$ のとき，出力状態は最大エンタングル状態

$$\Lambda_{c,t}(X)|+\rangle_c|0\rangle_t = (|00\rangle + |11\rangle)/\sqrt{2}, \tag{77}$$

になる．CNOT 演算は，コントロール側を黒丸，ターゲット側を白丸にして以下のような回路図で記述する：



古典論理回路にならって，水平な線は量子ビットが通過するワイヤを表しており，左から右へと量子状態が進んでいく．CNOT 演算のダイアグラムを通過したときに ΛX が作用する．

アダマール演算 H と位相演算 S はパウリ演算子をパウリ演算子に写す Clifford 演算であった．CNOT 演算も 2 量子ビットのパウリ演算子からなるパウリ群 $\{\pm 1, \pm i\} \times \{I, X, Y, Z\}^{\otimes 2}$ を共役作用のもとで不変にする．このように，一般に共役作用 $U : G \to UGU^\dagger$ のもとで，n 量子ビットパウリ群 $\{\pm 1, \pm i\} \times \{I, X, Y, Z\}^{\otimes n}$ が不変になるような U を **Clifford 演算子**と呼ぶ．CNOT 演算については，具体的に

$$\Lambda(X)_{c,t} X_c I_t \Lambda(X)^\dagger_{c,t} = X_c X_t, \tag{78}$$
$$\Lambda(X)_{c,t} I_c X_t \Lambda(X)^\dagger_{c,t} = I_c X_t, \tag{79}$$
$$\Lambda(X)_{c,t} Z_c I_t \Lambda(X)^\dagger_{c,t} = Z_c I_t, \tag{80}$$
$$\Lambda(X)_{c,t} I_c Z_t \Lambda(X)^\dagger_{c,t} = Z_c Z_t, \tag{81}$$

となり，Clifford 演算子であることが確認できる．これまで出てきた $\{H, S, \mathrm{CNOT}\}$ の Clifford 演算から，任意の n 量子ビット Clifford 演算を構成することができる．

[*11] k 番目の量子ビットに作用する演算子 A を

$$A_k = \overbrace{I \otimes \cdots \otimes I}^{k-1} \otimes A \otimes \overbrace{I \otimes \cdots I}^{n-k-1}, \tag{76}$$

と書くことにする．

4.2 Clifford 演算と Gottesman-Knill の定理

1 量子ビットの場合，H と S からは任意の 1 量子ビットユニタリー演算を構成することはできなかった．同様に，Clifford 演算 $\{H, S, \mathrm{CNOT}\}$ からは任意の n 量子ビットユニタリー演算子を構成することはできない．それどころか，Z 基底での初期状態準備，Clifford 演算，及び，Z 基底での射影測定から構成される量子計算[*12]は，古典計算機で効率よくシミュレーションすることができてしまう（エンタングルメントした状態はいくらでも生成できるのに！）．このことを理解するために，量子計算を演算子を用いて特徴づけしてみよう．初期状態として初期化された n 量子ビット $|0\rangle^{\otimes n}$ を用意する．この状態は，演算子 $\{Z_i\}_{i=1}^n$ の固有値 $+1$ の固有状態になっている．このように，状態をその固有状態として特徴付ける演算子を**スタビライザー演算子**と呼ぶことにする．ある，n 量子ビット Clifford 演算 U を作用させたのちに得られる状態は，$U|0\rangle^{\otimes n}$ であるが，この状態を固有状態に持つスタビライザー演算子は，

$$U|0\rangle^{\otimes n} = UZ_i|0\rangle^{\otimes n} = UZ_iU^\dagger(U|0\rangle^{\otimes n}) \equiv S_i(U|0\rangle^{\otimes n}), \tag{82}$$

から $\{S_i\}_{i=1}^n$（$S_i \equiv UZ_iU^\dagger$）ということになる．U は今，Clifford 演算に限定しているので，$\{S_i\}$ は互いに交換する，n 量子ビットのパウリ演算子のテンソル積であることがわかる．$\{S_i\}$ の固有状態に対する Z 基底で射影測定した場合の確率分布は，$\{S_i\}$ と Z 演算子の交換関係から効率よく計算することができる（**Gottesman-Knill の定理**，例えば [1] もしくは [2] を参照）．このように，量子状態をその状態を固有状態として持つスタビライザー演算子（から成るスタビライザー群）を用いて記述する形式を**スタビライザー形式**と呼ぶ．Gottesman-Knill の定理は，Clifford 演算だけから構成された量子回路が古典シミュレーションできてしまうことを意味するが，同時に，高くエンタングルした複雑な量子状態であっても効率よく記述できる場合があることも意味する．実際，量子誤り訂正符号や測定型量子計算のリソース状態など，量子情報において重要になる多体エンタングル状態の多くは，スタビライザー形式で効率よく記述することができる（例えば，[3] 参照）．

4.3 制御ユニタリー演算

話を万能量子計算に戻そう．実は，すでに導入した任意の 1 量子ビットユニタリー演算を近似できる $\{H, T\}$ と CNOT の 3 種類のユニタリー演算から任意のユニタリー演算を構成することができる．その構成方法はやや込み入っているので，1 つ 1 つ段階を踏んで構成していこう．まず，必要になるのが，制御 U 演算

$$\Lambda_{c,t}(U) = |0\rangle\langle 0|_c I_t + |1\rangle\langle 1|_c U_t, \tag{83}$$

である．コントロール系が $|0\rangle$ の場合は何もせず，$|1\rangle$ の場合はユニタリー演算 U をターゲット系に作用させる．CNOT 演算の一般化だと思えばよい．この制御 U 演算を CNOT と 1 量子ビットユニタリー演算から構成する方法を見ていこう．まず，ユニタリー演算 U はオイラー分解より $U = e^{i\alpha}e^{-i\beta Z}e^{-i\gamma X}e^{-i\delta Z}$ と分解できたので，$U = e^{i\alpha}I$ [*13]と $U = e^{-i(\theta/2)A}$（$A = X, Y, Z$）に対して $\Lambda(U)$ が実現できれば良いことになる．まず，$\Lambda(e^{i\alpha}I)$ は，コントロール系の量子ビットの相対位相に他ならないので，コントロール系に $e^{-i(\alpha/2)Z}$ を作用させればよい．次に具体的に，$A = Z$ として，$\Lambda(e^{-i(\theta/2)Z})$ について考えよう．$e^{-i(\theta/2)Z} = e^{-i(\theta/4)Z}Xe^{i(\theta/4)Z}X$ と $I = e^{-i(\theta/4)Z}Ie^{i(\theta/4)Z}I$ を利用すると，

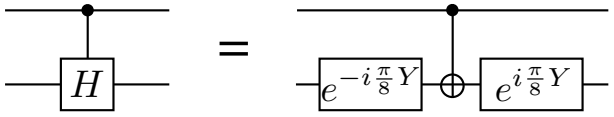
$$\Lambda_{c,t}(e^{-i(\theta/2)Z}) = \Lambda_{c,t}(X)e^{i(\theta/4)Z_t}\Lambda_{c,t}(X)e^{-i(\theta/4)Z_t} \tag{84}$$

[*12] Clifford 演算を用いて基底の変換が行えるので初期状態や測定をパウリ基底で行っても同じことが主張できる

[*13] $e^{i\alpha}$ は全体の位相なので重要でないように思うかもしれないが，制御演算の場合には相対位相になるのできちんと対処しなければならない．

が得られる．ターゲット系に H や S を（共役に）作用させることによって，同様に x 軸や y 軸に関しても回転させることができるので，任意の 1 量子ビットユニタリー演算に対して制御 U 演算が構成できたことになる．

例えば，制御アダマール演算 $\Lambda(H)$ は，$H = e^{i\pi/8Y} X e^{-i\pi/8}$ であることを利用して以下のように実現される：



（回路は左から右に進むが，数式では左から掛けていくので注意すべきである．）

4.4 Toffoli 演算と可逆計算

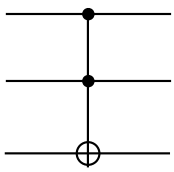
次に，万能性を証明するために重要となるもう一つのユニタリー演算，Toffoli 演算，を導入しておく．Toffoli 演算は，3 量子ビットに作用するユニタリー演算で，

$$\Lambda^2_{c_1,c_2,t}(X) = (I_{c_1} I_{c_2} - |1\rangle\langle 1|_{c_1} |1\rangle\langle 1|_{c_2}) I_t + |1\rangle\langle 1|_{c_1} |1\rangle\langle 1|_{c_2} X_t, \tag{85}$$

と定義される．2 つのコントロール系があり，両方とも $|1\rangle$ 状態の時のみターゲット系にパウリ X 演算子を作用させる，CNOT 演算の一般化になっている．計算基底の入力状態 $|i_1\rangle_{c_1}|i_2\rangle_{c_2}|j\rangle_t$ に対して，

$$\Lambda^2_{c_1,c_2,t}(X)|i_1\rangle_{c_1}|i_2\rangle_{c_2}|j\rangle_t = |i_1\rangle_{c_1}|i_2\rangle_{c_2}|j \oplus (i_1 \cdot i_2)\rangle_t. \tag{86}$$

ターゲット系に論理積（AND）を出力する．

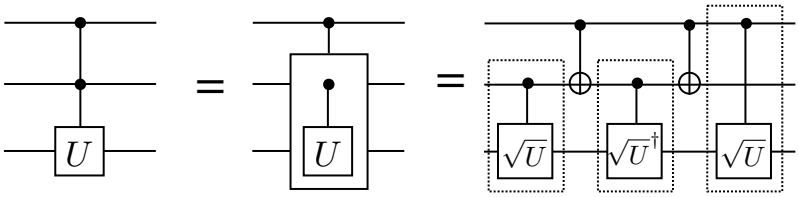


Toffoli 演算も $\{H, T, CNOT\}$ から構成できることを示しておこう．Toffoli 演算は CNOT 演算にコントロール系を追加すれば良いので，$\Lambda(\Lambda(X))$ を実現すればよいことになる．一般に $\Lambda^2(U) = \Lambda(\Lambda(U))$ は，

$$\Lambda_{c,t}(U) = \sqrt{U}_t X_c \Lambda_{c,t}(\sqrt{U}^\dagger) X_c \Lambda_{c,t}(\sqrt{U}) \tag{87}$$

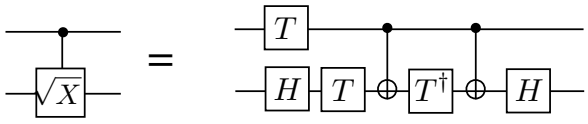
となるので，これをさらに制御化するには，

$$\Lambda^2_{c_1,c_2,t}(U) = \Lambda_{c_1,t}(\sqrt{U}) \Lambda_{c_1,c_2}(X) \Lambda_{c_2,t}(\sqrt{U}^\dagger) \Lambda_{c_1,c_2}(X) \Lambda_{c,t}(\sqrt{U}) \tag{88}$$

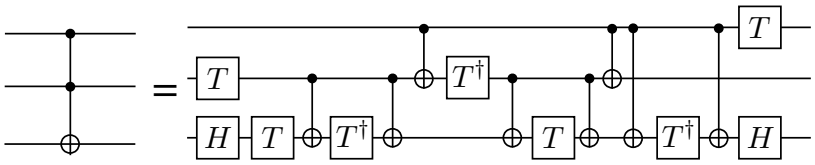


(89)

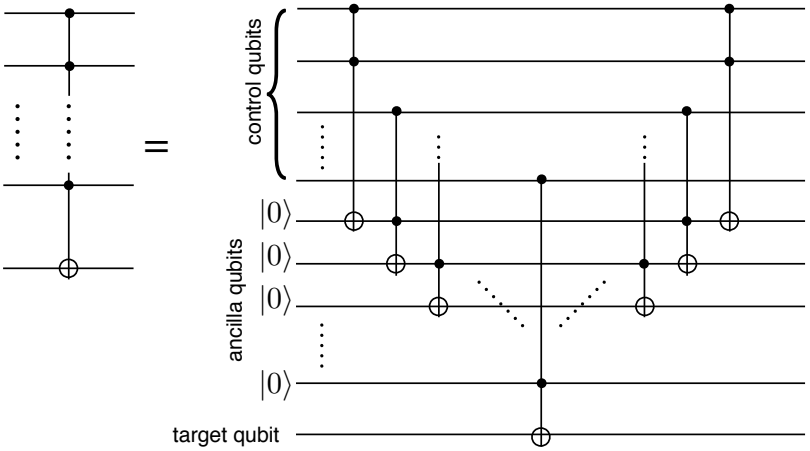
とすれば良いことになる．$U = X$ とすれば Toffoli 演算が構成できる．$\Lambda(\sqrt{X})$ は，先に述べた制御ユニタリー演算の構成を用いて，



のようになり，Toffoli 演算は T 演算を用いて以下のように分解できる．



ひとたび Toffoli 演算が構成されると補助系を用いることによって，以下のようにコントロール系をいくらでも増やすことができる：



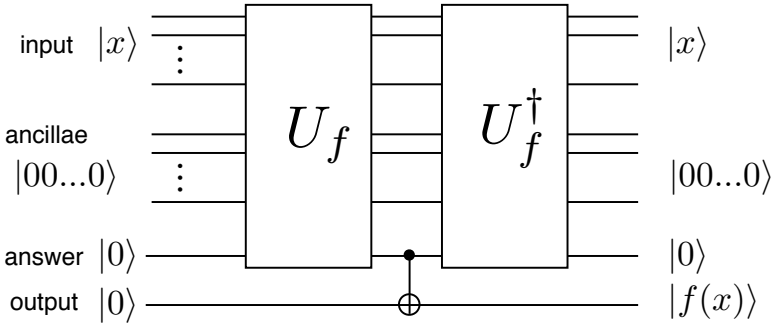
Toffoli 演算は，ターゲット系の入力状態を $|1\rangle$ にしておけば，ターゲット系の出力は古典論理回路における NAND 演算に対応することになる．つまり，Toffoli 演算は，NAND 演算を可逆なユニタリー演算で実現していることになる．任意の論理回路（ブール関数）は NAND 演算から構成でき，古典論理回路において万能性があることが知られていることから，量子計算は古典計算を自明に含むことがわかる．さらに，量子計算はユニタリー演算を用いて計算をするので，可逆に計算ができることになる．実際に，入力 $x \in \{0,1\}^n$ に対するブール関数 $f : \{0,1\}^n \to \{0,1\}$ の出力の可逆計算を構成してみよう．f は NAND 演算から構成できることがわかっているので，f に対応するユニタリー演算 U_f を Toffoli 演算，パウリ X 演算，補助量子ビットを用いて構成できる．$|\cdots\rangle_{\rm input}, |\cdots\rangle_{\rm ancilla}, |\cdots\rangle_{\rm answer}$ をそれぞれ，入力，補助量子ビット，答えを記録する量子ビットとすると，U_f の作用は，

$$U_f|x\rangle_{\rm input}|0...0\rangle_{\rm ancilla}|0\rangle_{\rm answer} = |x\rangle_{\rm input}|g(x)\rangle_{\rm ancilla}|f(x)\rangle_{\rm answer}, \tag{90}$$

となり，出力 $f(x)$ が得られる．しかしながら，計算を可逆にするために，補助量子ビットに計算のゴミ $|g(x)\rangle_{\rm ancilla}$ が残ってしまうことになり，この初期化のためには不可逆な操作が必要になると思うかもしれない．しかし，このゴミは計算結果 $f(x)$ を新たな量子ビットにコピーして保存し（直交状態なのでコピーできる），逆計算

(uncomputation) $U_f^\dagger$ を施すことによって初期状態に戻すことができる:

$$\begin{aligned} & U_f^\dagger \Lambda_{\mathrm{answer,out}}(X) U_f |x\rangle_{\mathrm{input}} |0...0\rangle_{\mathrm{ancilla}} |0\rangle_{\mathrm{answer}} |0\rangle_{\mathrm{out}} \\ &= U_f^\dagger |x\rangle_{\mathrm{input}} |g(x)\rangle_{\mathrm{ancilla}} |f(x)\rangle_{\mathrm{answer}} |f(x)\rangle_{\mathrm{out}} \\ &= |x\rangle_{\mathrm{input}} |0...0\rangle_{\mathrm{ancilla}} |0\rangle_{\mathrm{answer}} |f(x)\rangle_{\mathrm{out}}. \end{aligned} \tag{91}$$



以上のようにして，可逆な操作のみからゴミを残さずに $f(x)$ を計算できることがわかった．この結果は，量子計算が定式化される前の 80 年代に計算の物理的限界（消費エネルギーや発熱問題）を研究する過程で，Toffoli と Fredkin らによって得られた．その後，量子力学を積極的に計算に利用する万能量子計算へと研究が進んでいくことになった．

4.5 万能量子計算

やっと準備が整ったので，$\{H, T, CNOT\}$ から任意の n 量子ビットユニタリー演算子を近似的に構成できることを示しておこう．まず，2^n 次元複素ヒルベルト空間 $\mathcal{H}_n$ に作用する任意の n 量子ビットユニタリー演算子 U は，$m \equiv 2^n$ 次元空間の 2 次元部分空間内のユニタリー演算子（2 準位ユニタリー演算子）に分解できることを示そう．基底を 1 から m までの整数でラベルし直して，$|i\rangle$ と $|j\rangle$（$i, j \in \{1, 2, ..., m\}$）の 2 つの基底に対する 2 準位ユニタリー演算子を T_{ij} としよう．[*14] このとき，$T_{m\,m-1}$ の要素を適切に選ぶことによって，

$$UT_{m\,m-1} = \begin{pmatrix} u_{11} & \cdots & u_{1\,m-1} & u_{1\,m} \\ \vdots & \ddots & \vdots & \vdots \\ u_{m-1\,1} & \cdots & u'_{m-1\,m-1} & u'_{m-1\,m} \\ u_{m\,1} & \cdots & 0 & u'_{m\,m} \end{pmatrix}, \tag{92}$$

と変形することができる．ここで $(U)_{kl} = u_{kl}$ を U の行列要素とした．この操作を繰り返し行うことによって，

$$UT_{m\,m-1}T_{m\,m-2}\cdots T_{m\,1} = \begin{pmatrix} u''_{11} & \cdots & u''_{1\,m-1} & u''_{1\,m} \\ \vdots & \ddots & \vdots & \vdots \\ u''_{m-1\,1} & \cdots & u''_{m-1\,m-1} & u''_{m-1\,m} \\ 0 & \cdots & 0 & u''_{m\,m} \end{pmatrix} \tag{93}$$

のように，m 行目を対角項を除いてすべて 0 にすることができる．また，ユニタリー演算子であることから自動的に $u''_{1\,m} = \cdots = u''_{m-1\,m} = 0$ と $|u''_{mm}| = 1$ がわかる．これらの操作をまとめて，$R_m \equiv T_{m\,m-1}T_{m\,m-2}\cdots T_{m\,1}$，とかくことにする．この操作 R_k を $k = 1, ..., m$ に対して繰り返すことによって，U を対角ユニタリー演算子 D へと変形することができる:

$$U = D(R_m \cdots R_1)^\dagger. \tag{94}$$

[*14] T_{ij} の行列要素を $(T_{ij})_{kl}$ とするとき，$k, l \neq i, j$ のときは $(T_{ij})_{kl} = \delta_{kl}$ であり，$k, l = i, j$ に対応する 4 つの要素が 2×2 ユニタリー演算子を構成する．つまり部分空間 $\{|i\rangle, |j\rangle\}$ の外では恒等演算子として作用することに注意する．

D はもはや対角項しかないので，2 準位ユニタリー演算子（対角な）の積に分解できることは自明である．よって，U を 2 準位ユニタリー演算子の積に分解できた．

最後に，2 準位ユニタリー演算子 T_{ij} が Toffoli 演算と制御 U 演算（および $\{H, T, \mathrm{CNOT}\}$）を用いて実行できることを示そう．Toffoli 演算も制御 U 演算も，$\{H, T, \mathrm{CNOT}\}$ から構成できたので，これを示せば $\{H, T, \mathrm{CNOT}\}$ から任意の n 量子ビットユニタリー演算が構成できることになる．

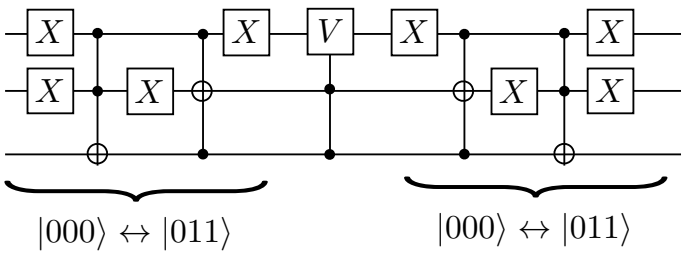
i と j は 1 から m までの整数であったが，これを 2 進数（n ビット列）を用いて書き直したものをそれぞれ $\mathbf{s} = s_1 s_2 ... s_n$ と $\mathbf{t} = t_1 t_2 ... t_n$ とする．このとき，$\mathbf{s}$ からスタートし各ステップごとに 1 つのビットだけを反転させて $\mathbf{t}$ に至るような，ビット列の列 $\{\mathbf{g}_k\}_{k=1}^{d}$，

$$\mathbf{s} = \mathbf{g}_0 \to \mathbf{g}_1 \to \cdots \to \mathbf{g}_d = \mathbf{t} \tag{95}$$

を簡単にみつけることができる．ここで，d を 2 つのビット列 $\mathbf{s}$ と $\mathbf{t}$ の異なるビットの総数（Hamming 距離）とした．

ビット列 $\mathbf{s}$ と $\mathbf{g_1}$ は 1 ビットだけ異なるので，パウリ X 演算や Toffoli 演算を用いて，同じビット列部分をコントロール系にし，ターゲット系を異なるビットにすることによって，$|\mathbf{s}\rangle$ 基底を $|\mathbf{g_1}\rangle$ 基底へと変換するユニタリー演算子を構成することができる．これを繰り返していくと，$|\mathbf{s}\rangle$ を $|\mathbf{g}_{d-1}\rangle$ まで基底の変換を行うことができる．最後に，$|\mathbf{t}\rangle$ と $|\mathbf{g}_{d-1}\rangle$ は 1 ビットだけ異なるので，この基底では 2 準位ユニタリー演算子は，同じビット列をコントロール系とした 1 量子ビット（部分空間）のユニタリー演算子となる．制御ユニタリー演算を用いてこれを実行し，再び元の基底に戻すことによって，$|\mathbf{s}\rangle$ と $|\mathbf{t}\rangle$ の 2 準位ユニタリー演算を構成することができた．

具体例として，3 量子ビット（8 次元空間）の部分空間 $\{|000\rangle, |111\rangle\}$ に作用するユニタリー演算子の実装例を示しておく：



以上をまとめておくと，アダマール演算 H，$\pi/8$ 演算 T を用いて任意の 1 量子ビットユニタリー演算が構成でき，CNOT 演算と 1 量子ビット演算を用いて，制御ユニタリー演算と Toffoli 演算が構成できる．Toffoli 演算があれば，コントロール系を追加することもできた．これらを用いて，任意の 2 準位に関する 2 準位ユニタリー演算が構成でき，それから任意の n 量子ビットユニタリー演算子が構成できた．よって，$\{H, T, \mathrm{CNOT}\}$ の 3 種類の演算があれば万能量子計算が実行できることになる．このような演算集合を，万能演算集合と呼ぶ.

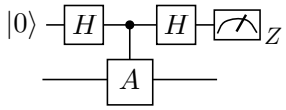
5 量子アルゴリズム

ここでは，量子コンピュータが古典コンピュータに対してどういった優位性があるのかを，アダマールテストという量子アルゴリズムを通じて説明する．アダマールテストの発展系として，量子アルゴリズムとして非常に重要な位相推定アルゴリズム，及び素因数分解アルゴリズムを理解することができる．

5.1 間接測定

光子検出器のように，測定後量子状態を破壊してしまう場合がしばしばある．このような場合において，測定後に射影された状態を残すためには，補助系を用いて間接測定を行う必要がある．A を固有値が ± 1 のエルミート

演算子としよう．演算子 A の間接測定は，制御 A 演算 $\Lambda(A)$ を用いて:

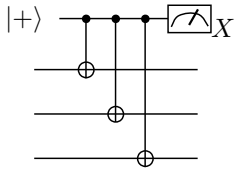


のように構成することができる．左端に書かれた状態 $|0\rangle$ は補助系の入力状態を意味し，黒丸に繋がれた箱 U は補助系をコントロール系とする制御 U 演算 $\Lambda(U)$ を表している．右端のメータが書かれた箱は Z 基底での射影測定を意味している．この量子回路が A の間接測定になっていることは，直接計算することによって被測定系の測定後の状態が補助系の測定結果 $s \in \{0,1\}$ に依存して，

$$\frac{I+(-1)^s A}{2}|\psi\rangle / \sqrt{\mathrm{Tr}[(I+(-1)^s A)/2|\psi\rangle\langle\psi|]}, \tag{96}$$

となることからも理解できるし，被測定系における POVM 演算子が $\frac{I_t+(-1)^s A_t}{2}$ で与えられることからも理解できる．

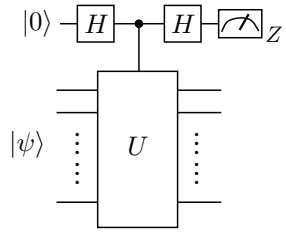
例えば，3 体の演算子 $X_1X_2X_3$ の間接測定は以下のように構成される．



このような多体パウリ演算子の間接測定は量子誤り訂正におけるスタビライザー演算子の測定に頻繁に使われることになる．

5.2 アダマールテスト

一般に，任意の n 量子ビットユニタリー演算子 U に対してアダマールテストを補助量子ビットと制御 U 演算を用いて以下のように定義する：



入力状態を $|\psi\rangle$ とすると，測定前の状態は，

$$\frac{1}{\sqrt{2}}\left[|+\rangle|\psi\rangle + |-\rangle(U|\psi\rangle)\right] \tag{97}$$

なので，測定結果 0 を得る確率は，

$$p_0 = \frac{1}{4}\left\|(I+U)|\psi\rangle\right\|, \quad p_1 = \frac{1}{4}\left\|(I-U)|\psi\rangle\right\|, \tag{98}$$

となる．補助系における測定結果 $0,1$ を得る確率は簡単な計算から，

$$p_0 = \frac{1}{2}\left(1+\mathrm{Re}\langle\psi|U|\psi\rangle\right), \quad p_1 = \frac{1}{2}\left(1-\mathrm{Re}\langle\psi|U|\psi\rangle\right). \tag{99}$$

となることがわかる．補助系に位相演算 S を付け加えると，実部 Re を虚部 Im に置き換えたものが得られる．従って，アダマールテストを何回も繰り返すことによって，ユニタリー演算子 U の行列要素

$$\langle\psi|U|\psi\rangle \tag{100}$$

を推定することができる．アダマールテストを M 回繰り返し，測定結果 0 が M_0 回得られたとすると，Chernoff-Hoeffding 限界から

$$\mathrm{Prob}\left(\left|\frac{M_0}{M}-p_0\right|>\epsilon\right)<2e^{-2\epsilon^2 M}, \tag{101}$$

となり，$M=\mathrm{poly}(1/\epsilon)$ のサンプル数で誤差 ϵ の近似ができることになる．

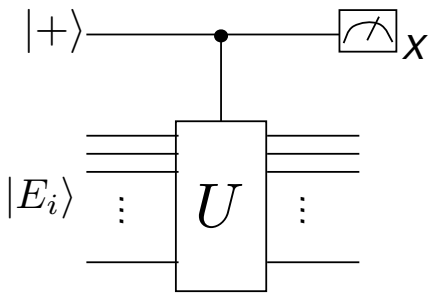
入力状態 $|\psi\rangle$ を U の固有状態 $|\lambda\rangle$（$U|\lambda\rangle=e^{i\lambda}|\lambda\rangle$）とすると，アダマールテストから固有値 $e^{i\lambda}$ を推定することができる．一般の状態 $|\psi\rangle$ を入力した場合は，測定後の状態に作用する演算子は $(I\pm U)$ の定数倍なので，ユニタリー演算子の固有状態 $|\lambda\rangle$ はこの測定において不変である．従って，測定後の状態を再び入力としてアダマールテストを繰り返す極限を考えると次第に特定の固有状態へと確率的に収束し，$e^{i\lambda}$ が推定できることになるので，アダマールテストを繰り返した極限では，U の固有状態 $\{|\lambda\rangle\}$ に関する間接的な射影測定になっている．

n 量子ビットのユニタリ演算子 U の行列要素を計算することくらい古典コンピュータでも簡単にできると思うかもしれない．しかし，U は $2^n\times 2^n$ 行列なので，例えば，$n=50$（たった 50 量子ビットからなる系）であったとしても，行列の要素の数は $2^{50}\sim 10^{15}$ になり，倍精度の複素数 1 つに対して 128 ビットのメモリーが必要になるので，U の行列要素の計算には 100 ペタビットのメモリーが必要になる．もちろん U は，局所的なユニタリー演算子の積から構成されるので，このサイズの行列の積をひたすら計算する必要がある．量子系はテンソル積構造をもつため，量子系において部分系にユニタリー操作をする場合でも（量子デバイス上ではその部分系のみに操作をすればいいのであるが），古典コンピュータ上では $2^n\times 2^n$ の行列積の処理をする必要があることにも注意したい．量子コンピュータを用いてアダマールテスト行った場合は，行列要素の近似になるが，おなじ近似精度を要求しても古典コンピュータの場合は（特定の都合の良い構造がない限り），愚直に指数的なサイズの行列を操作するしかないのだ．ここに，量子コンピュータの古典に対する優位性が端的に現れている．

アダマールテストを用いた量子アルゴリズムの例としては，ユニタリー演算 U としてブレイド群のユニタリ表現をとれば，その行列要素と組紐不変多項式であるジョーンズ多項式との数学的対応から，ジョーンズ多項式を近似する量子アルゴリズムを構成することができる．U としてハミルトニアンダイナミクス e^{-iHt} を採れば，量子多体系の実時間発展を意のままに追うこともできる．前述の議論から入力状態 $|\psi\rangle$ のエネルギーに関する射影測定を行うこともできる．アダマールテストでは，何回も繰り返して度数分布を作る必要があったが，測定に用いる補助系をもう少しうまく工夫した位相推定アルゴリズムを用いることによって，固有値をより精度よく求めることができる．素因数分解アルゴリズムは，特殊な U に対して位相推定を行い，固有値を精度よく求めることによって構成される．

5.3 位相推定

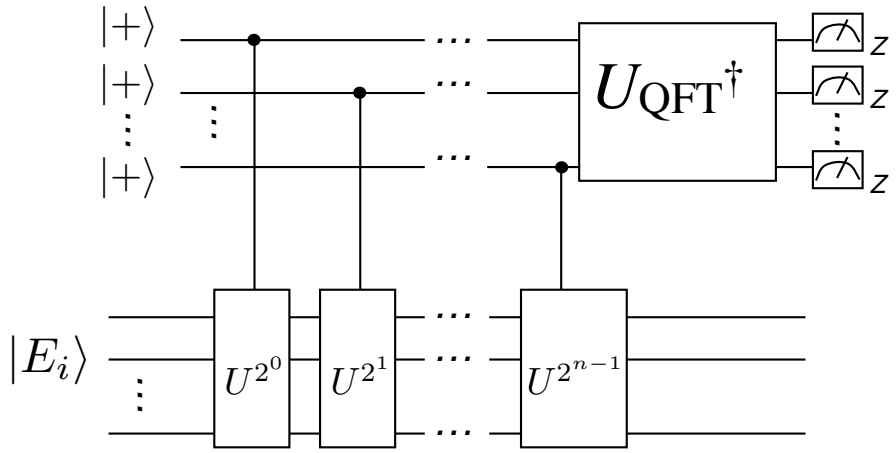
ユニタリー演算子 U の固有状態 $|E\rangle$ が与えられていれば，その固有値 $e^{i\phi}$ をアダマールテストを用いて推定することができた．



残念ながらアダマールテストでは，固有値 $e^{i\phi}$ の指数にある位相 ϕ を指数精度（多項式桁まで）求めることはできない．しかし，うまく補助系を構成した Kitaev による位相推定アルゴリズムを用いれば，ϕ を指数精度で推定できる場合がある．位相 $e^{i\phi}$ を 2 進小数を使って $e^{2\pi i 0.j_1 j_2 ... j_n}$（$j_k \in \{0,1\}$）と書くことにする．2 進小数の定義は，

$$0.j_1 j_2 ... j_n = \sum_{k=1}^{n} j_k (1/2)^k. \tag{102}$$

である．アダマールテストと異なり位相推定アルゴリズムでは，n 量子ビットの補助系を用いてビット列 $j_1, ..., j_n$ を以下のような回路で求めることになる：



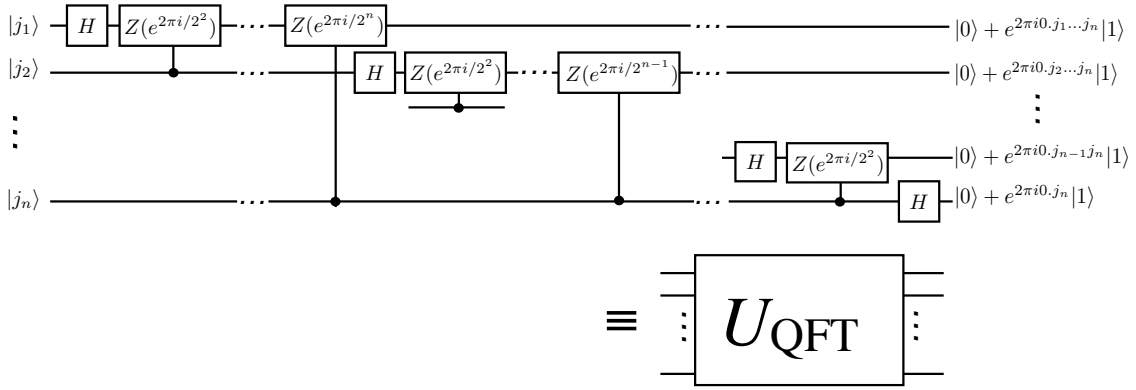
ここで，U_{QFT} は量子フーリエ変換であり，後に説明する．n 個の補助量子ビットを $|+\rangle$ にし，それぞれを制御量子ビットとして $\Lambda(U^{2^k})$（$k = 0, ..., n-1$）を作用させる．U^{2^k} の固有状態が入力すると，補助量子ビットが $|1\rangle$ 状態のときだけ固有値 $(e^{2\pi i 0.j_1 j_2 ... j_n})^{2^k} = e^{2\pi i 0.j_{k+1} ... j_n}$ が位相として乗る（phase kickback）ことになる．よって，量子フーリエ変換前の補助系の量子状態は，

$$\frac{|0\rangle + e^{2\pi i 0.j_1 ... j_n}|1\rangle}{\sqrt{2}} \frac{|0\rangle + e^{2\pi i 0.j_2 ... j_n}|1\rangle}{\sqrt{2}} \cdots \frac{|0\rangle + e^{2\pi i 0.j_{k+1} ... j_n}|1\rangle}{\sqrt{2}} \cdots \frac{|0\rangle + e^{2\pi i 0.j_n}|1\rangle}{\sqrt{2}} \tag{103}$$

となる．最終的な目標は，この状態を $|j_1\rangle|j_2\rangle \cdots |j_n\rangle$ に変換し，計算基底の測定から $j_1, ..., j_n$ の情報を得ることである．量子フーリエ変換の作用は，

$$U_{\mathrm{QFT}}|j_1 j_2 ... j_n\rangle = \frac{|0\rangle + e^{2\pi i 0.j_1 j_2 ... j_n}|1\rangle}{\sqrt{2}} \frac{|0\rangle + e^{2\pi i 0.j_2 ... j_n}|1\rangle}{\sqrt{2}} ... \frac{|0\rangle + e^{2\pi i 0.j_n}|1\rangle}{\sqrt{2}} \tag{104}$$

で定義されるので，逆量子フーリエ変換がまさに目標のタスクになっている．逆量子フーリエ変換のための量子回路は，



で構成される．ポイントは，制御ユニタリー演算を用いて各補助量子ビットの位相の小数第 1 位にのみビット j_k が出てくるようにし，アダマール変換をしてビット $|j_k\rangle$ を得ている．例えば，$\frac{|0\rangle+e^{2\pi 0.j_n}|1\rangle}{\sqrt{2}} = \frac{|0\rangle+(-1)^{j_n}|1\rangle}{\sqrt{2}}$ より，n 番目の補助量子ビットはアダマール変換をすると $|j_n\rangle$ が得られる．$(n-1)$ 番目の補助量子ビットは，$\frac{|0\rangle+e^{2\pi 0.j_{n-1}j_n}|1\rangle}{\sqrt{2}}$ なので，$|j_n\rangle$ から制御 $e^{2\pi 0.01}$ を作用させると，小数第 2 位がキャンセルされて，$\frac{|0\rangle+e^{2\pi 0.j_{n-1}}|1\rangle}{\sqrt{2}}$ が得られ，アダマール変換から $|j_{n-1}\rangle$ を得る．これを繰り返し行っていくことになる．最後に補助量子ビットを計算基底で測定すれば $j_1, ..., j_n$ が得られる．

位相推定アルゴリズムを用いて効率よく位相を n 桁目まで求めるためには，U^{2^n} を効率よく作用させる必要がある．n が問題のサイズに対して多項式的に増える場合は，U を指数回作用させる必要があると思うかもしれないが，U の古典的記述がうまく与えられているときは，U^{2^n} を多項式個の量子演算から構成できる場合がある．素因数分解アルゴリズムではまさにそのような例が使われている．

5.4 素因数分解アルゴリズム

準備が整ったので，Shor による素因数分解アルゴリズムを紹介しよう．N を素因数分解したい整数だとしよう．N と互いに素な整数 x を見つけてくる．適当に x を選びユークリッドの互除法で共約数が見つかれば素因数分解ができることになるし，見つからなければ互いに素ということになる．以降の議論では表記を簡単にするため，$\{|0\rangle, ..., |N-1\rangle\}$ の基底を用いて書くことにする．x と N を用いてユニタリー演算子

$$U_x = \sum_y |xy \pmod N\rangle\langle y|, \tag{105}$$

を定義する．このユニタリー演算子の場合，

$$U_x^{2^k} = \sum_y |x^{2^k} y \pmod N\rangle\langle y|, \tag{106}$$

なので，冪剰余 $x^{2^k} \bmod N \equiv e$ を先に計算しておけば U を 2^k 回作用させることなく，直接 $U_x^{2^k} = \sum_y |ey \pmod N\rangle\langle y|$ を作用させれば良い．さて，位数 r を $x^r = 1 \bmod N$ を満たす整数と定義すると，固有状態のラベル $0 \le s \le r-1$ を用いて，U_x の固有状態は，

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi i(s/r)k} |x^k \pmod N\rangle. \tag{107}$$

固有値は，

$$U_x|u_s\rangle = e^{2\pi i(s/r)}|u_s\rangle, \tag{108}$$

であることがわかる．位相推定をする入力状態は，$|1\rangle = \sum_{s=0}^{r-1} |u_s\rangle$ になることから，$|1\rangle$ を入力させると，位相推定によって確率的に固有状態 $|u_s\rangle$ が得られる．位相推定アルゴリズムを用いると，s/r を効率よく推定することができ，連分数展開を用いて有理数で書き直すと r の候補が得られる．$|1\rangle$ からランダムに $|u_s\rangle$ を選ぶと高い確率で s と r が互いに素になるので，位数 r を得ることができる．また，得られる位数が高い確率で偶数になることも保証されている．よって $x^r = 1 \pmod N$ を変形して，$(x^{r/2}-1)(x^{r/2}+1) = 0 \pmod N$ に至る．$\big(x^{r/2}-1 \pmod N\big)\big(x^{r/2}+1 \pmod N\big)$ が N で割りきれることになるが，$x^r = 1 \pmod N$ から $x^{r/2} \pmod N < N-1$ なので，$x^{r/2} \pm 1 \pmod N$ が N で割りきれることはない．つまり，$x^{r/2}-1$ もしくは $x^{r/2}+1$ と N との共約数が N の約数になっていることになるので，ユークリッド互除法を用いて N の約数を見つけることができる．

5.5 BQP 問題とアダマールテスト

これまでアダマールテストを中心に量子アルゴリズムを構成してきた．アダマールテストは，量子回路の一例なので，アダマールテストで行列要素 $\langle\psi|U|\psi\rangle$ を求めるという問題は，量子コンピュータで解くことができる問題のクラスよりも狭いと感じるかもしれない．しかし，それらは**同等に難しい**ということも示すことができる．まず，量子コンピュータで解くことができる問題を定義しておこう．多くの問題において yes (0)，no (1) の 2 値を返すような問題に帰着することができるので，もっとも単純化された yes か no を判定する問題を考える．例えば，素因数分解の場合は，$1 \le M \le N$ なる整数 N, M に対して，$x \le M$ なる x で N が割り切れるか？という決定問題を考えることができる．yes，no の回答から 2 分探索していくことによって，実質的に因数 x を見つけることができる．その他，ある整数 N が素数かどうかを判定する素数判定問題も決定問題の一種であり，これは古典コンピュータで多項式時間で解けることが知られている．

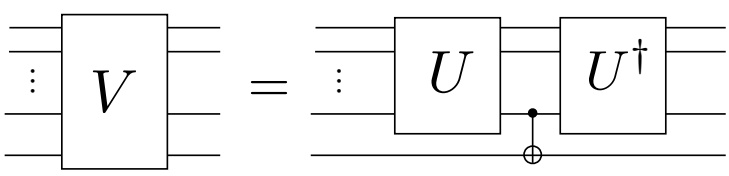
さて，量子コンピュータで解ける決定問題の定義に戻ろう．量子系の場合，出力は一般的に確率的に与えられるので，非常に高い確率で正解できればよいという条件にする．つまり，問題のサイズ n に対して多項式的なサイズの量子回路 U が存在して，答えが yes もしくは no の問題のそれぞれに対して，量子コンピュータの出力が yes を返す確率が，

$$\mathrm{Prob}(\mathrm{yes}|\mathrm{yes}) > 1/2 + \delta, \quad \mathrm{Prob}(\mathrm{yes}|\mathrm{no}) < 1/2 - \delta \tag{109}$$

であれば良いことにする．δ は問題のサイズ n に依存しないパラメータである．また，$0 < \delta < 1/2$ であればその値に依存せずに問題のクラスを定義することができる．なぜならば，多数決を行う量子回路を U の中に組み込んでしまえばいくらでも成功確率を増幅することができるからだ．よって，必要であれば量子回路 U に増幅回路を組み込むことによって，指数的に 1 に近い確率で正解できることになる．このような意味で解ける問題のクラスを BQP（bounded error quantum polynomial time computation）と呼ぶ．

上記の判定問題を解く量子回路の出力は 1 量子ビット測定であるが，可逆計算のときに用いた逆計算を利用することによって，新たにユニタリー演算子 V を

$$V = U^\dagger \Lambda(X)_{c,t} U, \tag{110}$$



(111)

と定義することによって，

$$p_0 = \mathrm{Tr}[P_0 U(|0\rangle\langle 0|)^{\otimes n} U^\dagger] = |\langle 0|^{\otimes n} V |0\rangle^{\otimes n}|^2 = \langle 0|^{\otimes 2n} (V \otimes V^\dagger) |0\rangle^{\otimes 2n} \tag{112}$$

と書ける．従って，判定問題を解く量子回路 U に対応してユニタリー演算子 $\tilde{V} = V \otimes V^\dagger$ が常に存在し，その行列要素 $\langle 0|^{\otimes 2n}(V \otimes V^\dagger)|0\rangle^{\otimes 2n}$ が $1/2+\delta$ よりも大きいか，$1/2-\delta$ よりも小さいかを判定する問題に等しい．つまり，行列要素 $\langle 0|^{\otimes 2n}(V \otimes V^\dagger)|0\rangle^{\otimes 2n}$ が近似できることによってクラス BQP に含まれる問題を全て解くことができる．このように BQP 問題に含まれる問題すべてと同等に難しいとき **BQP 困難**であるという．一方，行列要素の大小の判定問題は万能量子コンピュータを用いてアダマールテストを行えば判定できるので BQP 問題に含まれる．よって，与えられたユニタリー演算子 W に対して $\langle 0|^{\otimes n} W |0\rangle^{\otimes n}$ が $1/2+\delta$ よりも大きいか，$1/2-\delta$ よりも小さいかを判定する問題は **BQP 完全問題**と呼ばれる．**BQP 問題というと物理とはかけ離れた人工的な問題を取り扱っているように感じられるかもしれないが，これはユニタリー演算子の行列要素を良い精度で近似できるか？という問題と互換性があるため，量子多体系の物理において幅広く扱う問題の難しさを自然な形で定式化しているといえる．**

例えば，n 量子ビット系と $(M+1)$ 次元量子系の複合系における以下のようなハミルトニアンを考えよう:

$$H = \sum_{i=0}^{M-1} \left(U_{i+1} \otimes |i+1\rangle\langle i| + U_{i+1}^\dagger \otimes |i\rangle\langle i+1| \right). \tag{113}$$

これは，Feynman が 80 年代に考えたハミルトニアンで，n 量子ビット系は量子計算を実行する作業空間，M 次元量子系は計算のタイムステップに対応するクロック空間になっている．初期状態を $|0\rangle^{\otimes n} \otimes |0\rangle$ として，定常ハミルトニアンによって時間発展させると量子計算がステップ k まで進んだ状態の重ね合わせ状態（history state と呼ばれる）

$$e^{-iHt}(|0\rangle^{\otimes n} \otimes |0\rangle) = \sum_{k=0}^{M-1} C_k(t) \left(\prod_{i=1}^{k} U_i |0\rangle^{\otimes n} \right) \otimes |k\rangle. \tag{114}$$

が得られる．よって，定常ハミルトニアンによるユニタリー演算子の行列要素は，

$$\langle 0|^{\otimes n} \langle M| e^{-iHt} |0\rangle^{\otimes n} |0\rangle = \langle 0|^{\otimes n} C_M(t) \left(\prod_{i=1}^{M} U_i \right) |0\rangle^{\otimes n} \tag{115}$$

となり，BQP 完全問題を埋め込むことができるので,[*15]自然な定常ハミルトニアンのもとでの実時間ダイナミクスの遷移確率振幅にも万能量子計算と同等に複雑な計算が埋め込まれていることになる．Feynman が構成した H は，人工的な模型のように思えるかもしれないが，現在では，ランダムネスのある 2 次元正方格子上に並んだ量子ビット（スピン 1/2 粒子）に対する最近接 2 体相互作用ハミルトニアンにもこのようなダイナミクスを埋め込むことができることが知られている．よって，とある物性研究者が研究対象としているランダムネスを含む量子多体系の実時間ダイナミクスが，計らずしも万能量子コンピュータと同等に複雑な問題を取り扱っているということがありえても不思議ではない．

6 量子デコヒーレンス

一般的に，量子状態は環境系との結合によるデコヒーレンスに弱く，量子性はすぐに失われてしまう．例えば，基底状態と励起状態を量子ビットとして使っている場合，励起状態がエネルギーを放出して基底状態になる縦緩和現象や，エネルギー間隔が外場の影響を受けて揺らぐことによる位相緩和現象などが生じうる．外界との結合（エンタングルメント）によるデコヒーレンスを簡単なモデルで理解してみよう．まず，着目している量子ビット系（s）と環境系（e）からなる複合系を考える．量子ビットの状態は，$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ とする．最初は簡単のために環境系も 1 つの量子ビットから構成されており，初期状態は $|0\rangle_{\rm e}$ にいるとする．この状態が，ハミルトニアン

$$H_{\rm amp} = g(\sigma_{\rm s}^+ \sigma_{\rm e}^- + \sigma_{\rm s}^- \sigma_{\rm e}^+) \tag{116}$$

[*15] $C_M(t)$ を厳密に計算するか，もしくは $\langle 1|\langle 0|^{\otimes n-1}\langle M|e^{-iHt}|0\rangle^{\otimes n}|0\rangle$ との比から判定問題の出力に対応する $p_{0,1}$ が得られる．

のもとで時間発展するとしよう．ここで $\sigma^+ = |1\rangle\langle 0|$， $\sigma^- = |0\rangle\langle 1|$ とした．$|0\rangle$ を低エネルギー状態，$|1\rangle$ を高エネルギー状態としたとき，$\sigma^\pm$ はエネルギーを昇降する演算子になっている．[*16]時間 t における量子状態は，

$$e^{-iH_{\rm amp}t} = e^{-igt(\sigma_{\rm s}^+\sigma_{\rm e}^- + \sigma_{\rm s}^-\sigma_{\rm e}^+)}|\psi\rangle|0\rangle \tag{117}$$

$$= \alpha|00\rangle + \beta[\cos(gt)|10\rangle - i\sin(gt)|01\rangle] \tag{118}$$

となり，量子ビットは環境系とエンタングルしていることがわかる．環境系にはアクセスできないものとして，s 系の縮約密度行列を求めると，

$$\rho_{\rm s} = [\alpha|0\rangle + \beta\cos(gt)|1\rangle]\,[\alpha|0\rangle + \beta\cos(gt)|1\rangle]^\dagger + |\beta|^2\sin^2(gt)|0\rangle\langle 0| \tag{119}$$

$$= \begin{pmatrix} |\alpha|^2 + |\beta|^2\sin^2(gt) & \alpha\beta^*\cos(gt) \\ \alpha^*\beta\cos(gt) & |\beta|^2\cos^2(gt) \end{pmatrix} \tag{120}$$

となり，$|1\rangle$ 状態の振幅が減少する．$|\psi\rangle\langle\psi| \to \rho_{\rm s}$ の写像は，Kraus 演算子を

$$E_1 = \begin{pmatrix} 1 & 0 \\ 0 & \cos(gt) \end{pmatrix}, \quad E_2 = \begin{pmatrix} 0 & \sin(gt) \\ 0 & 0 \end{pmatrix}, \tag{121}$$

として

$$\mathcal{E}_{\rm amp}[t](\rho) = E_1\rho E_1^\dagger + E_2\rho E_2^\dagger \tag{122}$$

で与えられる．

もう一つの例を見てみよう．環境系の初期状態が $|+\rangle$ にあり，相互作用ハミルトニアンが

$$H_{\rm ph} = (g/2)Z_{\rm s}Z_{\rm e} \tag{123}$$

で与えられる状況を考えよう．先の例とは異なり環境系とのエネルギーのやりとりはない．時間 t の複合系の状態は，

$$e^{-iH_{\rm ph}t} = \frac{e^{-igt/2}}{2}(\alpha|00\rangle + \beta|11\rangle) + \frac{e^{igt/2}}{2}(\alpha|01\rangle + \beta|10\rangle) \tag{124}$$

となり，やはり環境系とエンタングルする．e 系をトレースアウトして，s 系の縮約密度演算子を計算すると，

$$\rho_{\rm s} = \begin{pmatrix} |\alpha|^2 & \cos(gt)\alpha\beta^* \\ \cos(gt)\alpha^*\beta & |\beta|^2 \end{pmatrix} \tag{125}$$

となり，非対角項が減少する．$|\psi\rangle\langle\psi| \to \rho_{\rm s}$ の写像 $\mathcal{E}_{\rm ph}[t]$ は，

$$\mathcal{E}_{\rm ph}[t](\rho) = \frac{1+\cos(gt)}{2}\rho + \frac{1-\cos(gt)}{2}Z\rho Z \tag{126}$$

と書くことができ，確率 $\frac{1-\cos(gt)}{2}$ でパウリ演算子 Z が作用すると考えても良い．

ここまでの議論は，1 量子ビットからなる環境系を考えていたので，しばらく時間がたつと系にコヒーレンスが戻ってくることになる．しかし，実際には着目する系を取り巻く環境系は大自由度の系になっていることが多い．したがって，それぞれの結合 g は小さい（常に $gt \ll 1$ が成り立つ）とし，環境系に独立に M（$\gg 1$）個ある量子ビットと結合してしまう状況を考えよう．

最初の例の場合の時間 t に対応する写像は

$$(\mathcal{E}_{\rm amp}[t])^M \quad \rho = \sum_{i_1,\ldots,i_M \in \{1,2\}^{\times M}} \left(\prod_{k=1}^M E_{i_k}\right)\rho\left(\prod_{k=1}^M E_{i_k}\right)^\dagger \tag{127}$$

$$= E_1^M\rho E_1^{\dagger M} + \sum_{k=0}^{M-1}(E_1^k E_2 E_1^{M-k-1})\rho(E_1^k E_2 E_1^{M-k-1})^\dagger, \tag{128}$$

[*16] それぞれの量子ビットのハミルトニアン $H_{\rm s} = -\omega_{\rm s}Z_{\rm s}$ および $H_{\rm e} = -\omega_{\rm e}Z_{\rm e}$ を顕には考えていないが，$\omega_{\rm e} = \omega_{\rm s}$ として相互作用描像を考えていると思えば良い．

と書ける．ここで，$E_2^2 = 0$ を使った．さらに，

$$E_1^M = \begin{pmatrix} 1 & 0 \\ 0 & \cos^M(gt) \end{pmatrix}, \quad E_1^k E_2 E_1^{M-k-1} = \begin{pmatrix} 0 & \sin(gt)\cos^{M-1-k}(gt) \\ 0 & 0 \end{pmatrix} \tag{129}$$

となる．このことから，時間 t の写像の Kraus 演算子は，$\gamma = gM$ として（gM を固定し，$g \to 0$ の極限で），

$$E_1^M = \begin{pmatrix} 1 & 0 \\ 0 & e^{-\gamma t} \end{pmatrix}, \quad E_2 = \begin{pmatrix} 0 & \sqrt{\sum_{k=0}^{M-1} \sin(gt)\cos^{M-k-1}(gt)} \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & \sqrt{1-e^{-\gamma t}} \\ 0 & 0 \end{pmatrix}, \tag{130}$$

で与えられることになる．時間 t に対して指数的に $|1\rangle$ の振幅が減衰する，振幅減衰ノイズになっている．同様に２つめの例に対して計算をすると，

$$(\mathcal{E}_{\rm ph}[t])^M = \frac{1+\cos^M(gt)}{2}\rho + \frac{1-\cos^M(gt)}{2} Z\rho Z \tag{131}$$

$$= \frac{1+e^{-\gamma t}}{2}\rho + \frac{1-e^{-\gamma t}}{2} Z\rho Z \tag{132}$$

となり，減衰定数 $\gamma = gM$ で非対角項が減衰する．これを位相減衰ノイズと呼ぶ．これらのような極限では，もはやコヒーレンスは系には戻ってこない．デコヒーレンスが生じてしまうと，量子情報は失われてしまい，量子コンピュータはうまく動かない．それに対処するための方法が次に説明する量子誤り訂正である．

7　量子誤り訂正

量子誤り訂正では，量子状態を雑音から保護するために量子情報を大きな次元のヒルベルト空間（多量子ビットからなる空間）の部分空間に埋め込む．このため，効率よく部分空間を記述することが必要となるが，そのための一つの方法であるスタビライザー形式について説明し，それによって定義されるスタビライザー符号を導入する．n 量子ビットからなる 2^n 次元ヒルベルト空間を考えよう．n 量子ビットのパウリ演算子のテンソル積から構成される n 量子ビットパウリ群

$$\{\pm 1, \pm i\} \times \{I, X, Y, Z\}^{\otimes n} \tag{133}$$

の可換部分群でかつ要素に $-I^{\otimes n}$ を含まないものをスタビライザー群 $\mathcal{S}$ を定義する（以降，特に混乱がない場合は恒等演算子を次元に関係なくすべて I と書くことにする）．i 番目の量子ビットに作用する演算子を

$$A_i \equiv I \otimes I \otimes \cdots \otimes A \otimes I \otimes \cdots \otimes I \tag{134}$$

として，例えば $\mathcal{S}_2 = \{I, X_1X_2, Z_1Z_2, -Y_1Y_2\}$ は可換群でありまた $-I$ を含まないため，一つのスタビライザー群である．このようなスタビライザー群を定義するためには，スタビライザー群の独立な要素から成る最大の集合である生成元を定義すればよい．ここで，独立であるとは，ある集合に含まれる要素がその集合に含まれる他の要素の積で表すことができないことを意味する．例えば，前述の例の場合は，$\{X_1X_2, Z_1Z_2\}$ を生成元として選ぶことができ，この要素の積で閉じるようにしてスタビライザー群 $\mathcal{S}_2$ を生成することができる．このとき $\mathcal{S}_2 = \langle\{X_1X_2, Z_1Z_2\}\rangle$ と書くことにする．スタビライザー形式では，状態をあらわに定義するかわりに，スタビライザー群の（要素の），状態に対する作用において安定となる状態，すなわち固有値 $+1$ の固有状態として状態を定義する．例えば，前述のスタビライザー群 $\mathcal{S}_2$ に対するスタビライザー状態は最大エンタングル状態 $(|00\rangle + |11\rangle)/\sqrt{2}$ である．これは，

$$Z_1Z_2 \frac{|0\rangle_1|0\rangle_2 + |1\rangle_1|1\rangle_2}{\sqrt{2}} = \frac{|0\rangle_1|0\rangle_2 + |1\rangle_1|1\rangle_2}{\sqrt{2}} \tag{135}$$

$$X_1X_2 \frac{|0\rangle_1|0\rangle_2 + |1\rangle_1|1\rangle_2}{\sqrt{2}} = \frac{|0\rangle_1|0\rangle_2 + |1\rangle_1|1\rangle_2}{\sqrt{2}} \tag{136}$$

表 1　スタビライザー符号 $\langle Z_1Z_2, Z_2Z_3\rangle$ のに対するビット反転エラーとシンドローム．

$Z_1Z_2 \setminus Z_2Z_3$	$+1$	-1
$+1$	I, $X_1X_2X_3$	X_3, X_1X_2
-1	X_1, X_2X_3	X_2, X_1X_3

であることから確認される．

スタビライザー群には $-I$ が含まれないので，生成元 $\{S_i\}$ の元は $S_i^2 = I$ を満たす．よって固有値は ±1 の 2 通りになることがわかる．1 つの生成元に対して，固有値 $+1$ と -1 の固有空間の 2 通りに分割されるので，生成元の個数を m とすると，2^n 次元のヒルベルト空間を 2^m 個に分割し，2^{n-m} 次元の部分空間内の状態がすべてスタビライザー状態となる．このような部分空間をスタビライザー部分空間と呼ぶことにしよう．スタビライザー符号とは，このようなスタビライザー部分空間に情報を埋め込む量子誤り訂正符号のことである．

一般的な定義の前に，具体的にスタビライザー演算子が $\langle Z_1Z_2, Z_2Z_3\rangle$ で与えられるようなスタビライザー部分空間を考えて，スタビライザー符号を構成してみよう．量子ビットの数 3 に対して生成元の数は 2 であるので，2 次元の部分空間（縮退）が定義される．この部分空間を張る基底を**符号状態（code state）**として**論理量子ビット（logical qubit）**を構成する．この縮退を解くために，スタビライザー演算子と独立でかつスタビライザー演算子と可換な演算子 Z_1 を 1 つ選び，この演算子の ±1 の固有状態 $Z_1|\bar{0}\rangle = |\bar{0}\rangle$ ，$Z_1|\bar{1}\rangle = -|\bar{1}\rangle$ として**論理基底（logical basis）**

$$|\bar{0}\rangle \equiv |000\rangle, |\bar{1}\rangle \equiv |111\rangle \tag{137}$$

を定義する．同様に $X_1X_2X_3$ と選び，基底を特定することもできる．このような，スタビライザー群と可換でありかつスタビライザー群と独立な演算子の作用において，スタビライザー部分空間は不変である．一方，スタビライザー演算子とは異なり，部分空間内部では $X_1X_2X_3|\bar{0}\rangle = |\bar{1}\rangle$ のように非自明に作用する．このような演算子を符号化された論理量子ビットに作用する演算子という意味で，**論理演算子**（logical operator）と呼ぶ．Z_1 と $X_1X_2X_3$ は互いに反可換であり，符号状態 $\alpha|\bar{0}\rangle + \beta|\bar{1}\rangle$ に対するパウリ演算子として振る舞うことがわかる．このような論理演算子の選び方は一意的でないことに注意しておこう．というのも，スタビライザー演算子は符号状態 $|\bar{\psi}\rangle$ に対して，自明に作用する

$$S_i|\bar{\psi}\rangle = |\bar{\psi}\rangle \text{ for all } S_i \in \mathcal{S} \tag{138}$$

ので，L を論理演算子とすると，LS_i（$S_i \in \mathcal{S}$）も同じ作用をする論理演算子ということになる．つまり，論理演算子の作用は，スタビライザー群と交換する演算子に対してスタビライザー群についての同値類をとったものに対応する．

一つ目の量子ビットにビット反転エラー X_1 が発生したとしよう．符号状態 $\alpha|\bar{0}\rangle + \beta|\bar{1}\rangle$ は基底 $\{X_1|\bar{0}\rangle = |100\rangle, X_1|\bar{1}\rangle = |011\rangle\}$ によって貼られる直交空間へと移される．スタビライザー演算子 Z_1Z_2 とビット反転演算子 X_1 は反交換するので，固有値は $+1$ から -1 へと反転する．つまり，スタビライザー演算子の固有値の反転からエラーの発生（正しい部分空間にいるかどうか）に関する情報が得られる．このためエラー発生後のスタビライザー演算子の固有値のことをシンドローム値と呼び，シンドローム値の集合をシンドロームと呼ぶことにする．今考えている 3 量子ビットから成るスタビライザー符号のエラーの種類とシンドロームの対応は 1 のようになる．ビット反転エラーが 1 つの量子ビットにしか発生しない場合は対応表からエラーを識別し，エラーを訂正することができる．しかし，X_2X_3 のように 2 つの量子ビットに同時にエラーが発生してしまった場合は X_1 と区別することができず，異なる符号状態になる論理エラーとなる．この符号は，ビット反転に対する誤り訂正が可能なので，3 量子ビット・ビット反転符号（3-qubit bit-flip code）と呼ぶ．

一般に，$m = n - k$ 個のスタビライザー生成元 $\langle S_1, ...S_m\rangle$ から構成されるスタビライザー符号に対して，スタビライザー演算子と独立でかつ可換な k 個の互いに独立な論理演算子 $\langle \bar{Z}_k\rangle$ を選び，その固有状態として k 個の論理量子ビットを定義することができる．シンドロームはスタビライザー生成元 $\{S_i\}$ の固有値の集合 $\{s_i\}$ によって与えられる．また，それぞれの演算子と反交換する演算子 $\bar{X}_i$ $(i = 1, ..., k)$，つまり，すべての $i, j \in 1, ..., k$ に対して

$$\bar{X}_i\bar{Z}_j = (-1)^{\delta_{ij}}\bar{Z}_i\bar{X}_j, \ \ \bar{X}_i\bar{X}_j = \bar{X}_j\bar{X}_i \tag{139}$$

を満たす演算子 $\bar{X}_i$ が常に存在する．$\{\bar{X}_i, \bar{Z}_i\}$ は符号化された自由度における i 番目の論理量子ビットに作用するパウリ演算子と見なす．

このようにして定義されたスタビライザー符号のエラーに対する耐性を測る指標として**符号距離**（code distance）がある．符号距離は，論理演算子に含まれるパウリ演算子の数を，全ての論理演算子に対した最小化したときの最小値 d として定義される．つまり，演算子 A に含まれる（I 以外の）パウリ演算子の数を $\mathrm{wt}(A)$ として，$\mathcal{L}$ を論理演算子が構成する群とすると，$d \equiv \min_L \mathrm{wt}(L)$ ということになる．例えば，前述の 3 量子ビット符号の場合は符号距離は $d = 1$ である．これは，1 つのパウリ Z エラーが作用してもスタビライザー空間内にとどまり，そのエラーの検出および訂正が出来ないことを意味する．きちんとした量子誤り訂正符号を構成するためには，もうすこし複雑な構造が必要になる．

少々天下り的であるが，以下のようにうまくスタビライザー群の生成元を選ぶことによって $d = 3$ の 5 量子ビット・スタビライザー符号を構成することができる：

$$S_1 = X \otimes Z \otimes Z \otimes X \otimes I, \tag{140}$$
$$S_2 = I \otimes X \otimes Z \otimes Z \otimes X, \tag{141}$$
$$S_3 = X \otimes I \otimes X \otimes Z \otimes Z, \tag{142}$$
$$S_4 = Z \otimes X \otimes I \otimes X \otimes Z, \tag{143}$$

例えば，$X^{\otimes 5}$ や $Z^{\otimes 5}$ が論理演算子になるが，論理演算子に対してスタビライザー演算子の積をとっても論理演算子になることからすべての論理演算子に対して調べると $d = 3$ であることが確認できる．

符号距離 d は，符号空間内の 1 つの符号状態から始めてパウリ演算子を 1 つ 1 つ作用させていき，d 個作用させたときに初めて異なる符号状態になるという意味で，符号空間内の異なる 2 状態間の距離を表している．したがって，ある符号状態に対して $(d-1)/2$ 以下のパウリ演算子がエラーとして発生（パウリエラー）した場合，その状態から最も近い符号状態は一意的にもとの符号状態になる．従って，エラーが発生してしまい，あるシンドローム $\{s_i\}$ によって定義される直交空間に符号状態が移ってしまったとき，その空間から元の符号空間に戻すことができる最小パウリ演算子で回復させることによって，$\lfloor (d-1)/2 \rfloor$ 個までのパウリエラーを訂正することができる．このような復号方法を**最小距離復号**という．前述の 5 量子ビット・スタビライザー符号は $d = 3$ なので 1 つの量子ビットに対するパウリエラーを訂正することができる．つまり，従って，ビット反転エラー（X）に加え，位相反転エラー（Z），ビット・位相反転エラー（Y）のすべてを訂正することができる．

5 量子ビットの空間は 32 次元であり，4 つの生成元によって 16 通りのシンドロームに対応した部分空間に分割される．一方，1 量子ビットのパウリエラーのパターンの総数は各量子ビットに対して 3 種類あるので $3 \times 5 = 15$ 個あり，エラーが全く発生していない 1 つを加え合計 16 通りのエラーパターンがある．16 個の直交する部分空間と 16 通りのエラーパターン（エラー無しを含む）がそれぞれ 1 対 1 対応していることに注意したい．このような性質を満たしうる最小の符号が上記の 5 量子ビット・スタビライザー符号である．

既に述べたように，スタビライザー演算子を適切に選んでおけば，ビット反転が生じる X エラー，位相反転が生じる Z エラー，もしくはその両方である Y エラーが作用した状態は，スタビライザー空間と直交する部分空間へと移され，$t = \lfloor (d-1)/2 \rfloor$ 個以下のエラーであれば訂正が出来るのであった．それでは，一般的な CPTP 写像で与えられるような量子ノイズであった場合はどうなるだろうか．実は，1 量子ビットの CPTP 写像の Kraus 演

算子 E_k は，パウリ演算子を基底として以下のように展開することができる．

$$E_k = \eta_k^I I + \eta_k^X X + \eta_k^Y Y + \eta_k^Z Z. \tag{144}$$

この事実と X, Y, Z の全ての種類のエラーを訂正できることから一般的な量子ノイズであっても訂正可能であることが以下のように示される．$\mathcal{R}$ をパウリエラーに対して回復操作を行う超演算子としてその Kraus 演算子を R_j とすると，スタビライザ符号状態 $|\Psi\rangle$ に対してパウリエラー $A = X, Y, Z$ がうまく訂正されもとの状態に戻るので，以下の式が満たされていることになる：

$$R_j A|\Psi\rangle \propto |\Psi\rangle. \tag{145}$$

(144) 式の分解のそれぞれにこの条件を適用することにより $R_j E_k|\Psi\rangle \propto |\Psi\rangle$ を得るので，

$$\mathcal{R} \circ \mathcal{E}(|\Psi\rangle\langle\Psi|) = |\Psi\rangle\langle\Psi|, \tag{146}$$

となる（ここで $\mathcal{R}$ と $\mathcal{E}$ はともにトレースを保存することを使った）．よって，符号距離 d のスタビライザー符号は Kraus 演算子が非自明に作用する量子ビットの数が高々 d 個であるような任意の量子ノイズを訂正することができることになる．

量子状態は古典ビットと異なり，連続的な自由度（波動関数）をもつ．従って，量子状態に対する量子ノイズは連続的な自由度を微妙に変化させるアナログ的なノイズが生じると考えられ，本来の状態とエラーが生じた状態を区別し訂正を行うことは，古典デジタル情報のそれとは異なり，難しいのではないかと考えられていた．古典の世界においてもアナログ計算機を定義することはできるが，もしアナログノイズを考慮せずに無限精度のアナログ計算機を仮定すると（そのようなマシンを作ることを物理法則が許すとは思えないが）PSPACE という NP 問題を含んだ非常に難しい問題をも効率よく解けてしまうことになる．PSPACE は，従来の古典 Turing 機械（デジタル古典計算機だと思ってよい）においてメモリー空間は多項式的であるが，計算時間は指数的にかけても良い，という非常に難しい問題のクラスである．しかし，このような強力なアナログ計算機が実現していないのは，アナログノイズを克服できないからである（だからといってアナログ計算機が有用ではないということではなく，風洞実験のように，古典デジタル計算機でシミュレーションすることが難しい状況において有用であることは大いにある．また，最近ではアナログデバイスの並列性を利用して最適化問題や機械学習などを実測時間で高速化しようという試みもある）．もし，量子コンピュータが量子力学がもつアナログ性を顕につかって，アナログマシンの意味で計算を加速しているのであれば，その興味はもっと限定されたものになるであろう（もちろん量子シミュレーターなど，アナログ量子計算としても利用価値はある）．しかし，重ね合わせの原理を逆に利用することによって，エラーをパウリエラーとして離散化し訂正することが可能であることは興味深い．つまり，**ある種アナログ的な情報をもつ量子状態に対するアナログエラーは，量子誤り訂正符号という量子多体系におけるエンタングルした構造を導入することによって離散化され，訂正することができることになる．**この意味で，量子誤り訂正によって保護された万能量子計算はデジタル量子計算であるということができる．そして，量子誤り訂正によって誤り耐性のある量子コンピュータを構築できるという事実は，量子コンピュータという計算モデルが物理法則で許された計算の原理的限界を追求する上で適切なモデルであるという理論的保証も与える．

参考文献

[1] Nielsen, M. A., Chuang, I. L. Quantum computation and quantum information. (Cambridge university press 2010).

[2] K. Fujii, *Quantum Computation with Topological Codes -From Qubit to Topological Fault-Tolerance-*, SpringerBriefs in Mathematical Physics (Springer-Verlag 2015).

[3] 小柴 健史, 藤井 啓祐, 森前 智行,「観測に基づく量子計算」（コロナ社 2017）.