量子アルゴリズム

本稿は量子アルゴリズムの入門として，量子情報理論の教科書

石坂智ほか，2024，量子情報科学入門 第 2 版，共立出版株式会社，東京

の第 3 章までをまとめたノートである．(教科書は量子計算のトピックとして第 3 章までを独立に読めるよう配慮されている．) ただし本稿では演習問題をはじめとして，教科書の内容を多少，取捨選択してある．さらに本稿には筆者の誤りや勘違いが潜んでいるかもしれないことをあらかじめ断っておく．言うまでもなく，原著を当たるに越したことはない．

なお本稿の他にも理論物理の各種ノートを以下のページで公開している．特に本書を読む上で役立ち得る教科書として，J.J. サクライ『現代の量子力学 (上)』 [1] のノートも置いてある．その 3.4 節には密度演算子と混合アンサンブルの，3.9 節にはスピン相関の測定と Bell の不等式に関する簡潔な説明もある．関連して文献 [2] の 5.6 節 (のノート) では，量子論の関係的解釈が説明されている．さらに古典系の文脈でゆらぎの熱力学と情報熱力学を説明した，沙川貴大『非平衡統計力学』 [3] のノートも置いてある．

http://everything-arises-from-the-principle-of-physics.com/

目次

第 0 章　量子情報科学への招待

0.1　古典情報科学から量子情報科学へ

現在のあらゆる情報処理は，半導体や光ファイバーなどの何らかの物理的素子の組合せで行われている．従来の情報科学では，量子効果が素子の入出力に現れないよう，素子の中で封じ込めることをデバイス技術のサイドに求めてきた (**古典情報科学**)．他方でシステム全体の効率を上げるために，素子の入出力に量子効果 (状態の量子的な重合せ) を許容し，その組合せを情報科学のサイドで扱うアプローチが**量子情報科学**である．

例えば光ファイバーによる古典通信では図 1 (a) のように，光子を伝送する光ファイバーだけでなく，情報 (入力アルファベットと呼ぶ) を光子に置き換える変調器の選択や，受信側での光子受信機の構成までをデバイス技術のサイドで行う．このとき入力アルファベットに応じた出力アルファベットの確率分布が決まる．すると情報科学のサイドでは古典通信路の内部構造には一切関知せずに，入出力を古典的に記述できる．

これを量子論の枠組みに拡張する方法は一意的ではない．例えば図 1 (b) のように光通信を量子通信路と捉えると，入力は伝送したいメッセージを量子的な光信号に変換する量子符号化に，出力は量子的信号をメッセージに変換する量子復号化に拡張される．量子通信路を用いれば古典的なメッセージだけでなく，量子状態そのものを伝送することもできる．これはしばしば量子誤り訂正と呼ばれ，図 1 (b) に示した設定とは異なることに注意する．他方で図 1 (c) のように入力側では依然として古典的なメッセージを送る，古典-量子通信路としての取り扱いも考え得る．これは量子通信路を用いて古典的メッセージを伝送する符号化の基礎として重要である (第 7 章)．

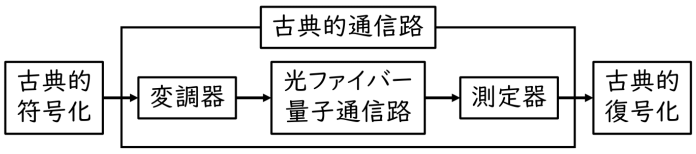
0.2　量子情報科学のさらなる進展

量子情報科学では量子計算や量子暗号など，従来不可能であったタイプの情報処理を扱うことが可能となる．

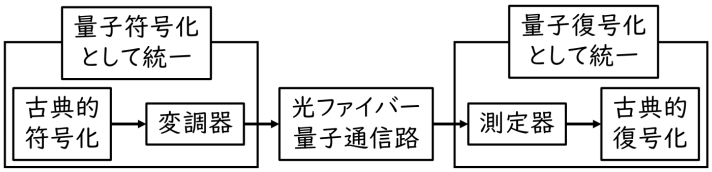
例えば現在用いられている多くの暗号は，その解読に必要な計算量の多さを安全性の根拠としており，一般には暗号を解くことが可能となる全ての情報は初めから盗聴者に漏れている．他方で量子暗号では，量子力学の性質から必然的に盗聴者がアクセスできる情報が制限されることで，情報理論的安全性が保証される．

また量子計算では量子効果を用いたアルゴリズムを導入することにより，特定の問題に対して劇的に計算速度を向上させることができる．まず挙げられるのは，素因数分解を多項式時間で解く Shor のアルゴリズムである．これを実行できる量子計算機が実現すると，現在よく用いられている RSA 暗号は容易に破られることになるため，Shor のアルゴリズムは衝撃をもって受け入れられた．ところで，よく量子計算の計算パワーの源は重合せ状態による並列計算にあると言われる．ただし最後の測定では 1 つの計算結果しか見ることができないため，量子計算がその計算パワーを発揮するには，正解を与える状態の確率振幅を増幅することも鍵となる．3.2 節で説明する Grover のアルゴリズムはその好例である．

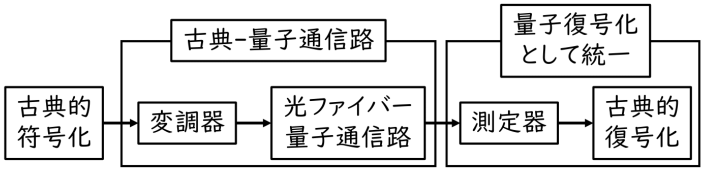
なお量子情報科学には理論分野に限っても，単純に量子計算や量子通信という応用だけでなく，量子論を量子情報科学の視点で見直す量子論基礎の分野，量子力学系のエンタングルメントを扱うエンタングルメント理論分野などがある．



(a) 光通信の古典通信での取り扱い



(b) 光通信の量子通信路に注目した取り扱い



(c) 光通信の古典-量子通信路に注目した取り扱い

図 1　光通信を例にした古典通信／量子通信

0.3　量子情報科学から物理学へのフィードバック

情報科学の視点から見ると，従来の標準的な量子力学のテキストは過度に物理現象に対する解釈に重きを置いており，情報処理を実現するシステムとして量子力学系を扱うには，余計な記述が多すぎる．そこで本書の第 1 章と第 4 章では，状態の準備や (物理量の) 測定といった「操作」に基づき，単に入出力関係の確率分布を記述する最小限の枠組みとして，量子力学を定式化する．

note　ただし物理学の営みはそのような単なるプラグマティズムに収まらず，またそれ故に予言能力を持つ学問として成功してきたと考えられることも，本稿筆者としてはここで強調しておきたい[*1]．

このような量子情報科学的な見方は，物理学の内部の問題にも大きな成果を残してきた：

- エンタングルメントの定量化 (第 6 章)
  - 局所操作と古典通信の概念の導入
  - 符号化の考え方
  - 情報量 (エントロピーなど) を扱う技術 (第 5 章)
- 測定過程の記述 (ユニタリな発展として記述できない)

[*1] 関連して本文 p.100 脚注 62 には次のようにある：物理学者の Mermin は，最も標準的な量子力学の「コペンハーゲン解釈」を揶揄して「黙って計算せよ！ という解釈 (Shut up and calculate interpretation)」と呼んでいる．(この言葉の起源に関しては，例えば N. D. Mermin, Phys. Today **57**, 10 (2004) を参照).

さらに第 8 章で扱う量子誤り訂正は，従来物理で問題になっていたデコヒーレンスに対する 1 つのアプローチにもなり得る．

0.4　量子情報処理の実現へ

数ある量子情報処理技術の中で最も実用化に近いと言われているのは，量子暗号システムである．量子暗号通信は現状の技術の組合せで実現可能であることが，理論的に保証されているからである．実際，量子通信路の前後で量子誤り訂正としての符号化・復号化を行えば，ノイズ (したがってデコヒーレンス) のある状況でも量子暗号の安全性を保証できる．そしてこのプロセスは，古典的な誤り訂正と秘匿性増強の組合せに置き換えることができ，それらは順に伝送に用いる基底 (ビット基底) と双対な基底 (位相基底) での誤り訂正に対応する．

現在，日本国内では総務省・情報通信研究機構 (NICT) を中心として，国内電機メーカーの力を集結し，量子暗号システムの実用化に向けた大規模なプロジェクトが進みつつある．また量子暗号技術の進展に伴い，次いで量子計算技術も実用化に近付くと期待される．

note　もっとも気候変動問題や経済格差に代表される資本主義による危機を前にして，量子情報科学の技術的な応用を優先させる感覚は率直に言って，私 (本稿筆者) には理解できない．

0.5　本書の構成

第 1 章では対象を量子ビットに限って，量子論を簡潔に定式化する．ここでの基礎知識だけで，量子計算を扱った第 3 章までの内容は理解できる．第 2 章では量子計算の基礎と量子回路について述べる (量子計算に興味のない読者も後の章のために読むことを勧める)．第 3 章では代表的な量子アルゴリズムとして，Deutsch-Jozsa のアルゴリズム，Grover のアルゴリズム，Shor のアルゴリズムを詳しく説明する．

第 4 章の前半では，改めて伝統的な量子力学を一般的・公理的に定式化する．後半ではノイズがある場合を含む量子情報処理に適用できる枠組みを紹介する．第 5 章ではエントロピーをはじめとする，量子系における様々な情報量と，その数学的性質を説明する．これら 2 つの章の内容は，後の章で不可欠である．

続いて教科書 p.12 から引用する：

> 第 6 章では，量子エンタングルメントについて扱う．量子テレポーテーション, 超稠密符号, 量子データ圧縮などのエンタングルメントに関連した量子情報処理について述べる．そして, 量子情報処理の鍵となる概念である局所操作 + 古典通信 (LOCC) に触れ，これをベースに, 量子エンタングルメントの変換について扱う．この変換を通じて，量子エンタングルメントがいかに定量化されるのかを説明する．上記の理論は，2 者間の純粋状態の場合は完成されていると言えるが，混合状態の場合については，より難しい扱いが必要となる．この章の最後では，2 者間の混合状態の場合についても扱う．
>
> 第 7 章では，量子通信路符号化について扱う．ここで扱う量子通信の問題では，古典的な情報を量子通信路を用いて伝送する場合を扱う．通信路符号化は，統計的仮説検定と深く関連していることが知られており，最初に，量子仮説検定について扱う．量子仮説検定の知識を用いて，量子通信路符号化を扱う．
>
> 第 8 章では，量子誤り訂正と量子暗号について扱う．量子誤り訂正では，量子状態を量子通信路を用いて伝送する問題を扱う．この点で，第 7 章で扱った問題と根本的に異なることに注意されたい．前半

では，代数的な古典符号について詳しく説明する．その後に，それをベースに量子誤り訂正符号を扱う．後半では，量子誤り訂正符号をベースに，量子通信路を用いた古典的な情報の秘匿通信を扱う．そして，この知識をベースに量子暗号の安全性について最後に触れる．

これらの章の議論で共通する特徴は，ブロックサイズが無限大の極限で，問題を特徴付ける量がエントロピーなどの情報量に集約される点である．これは問題のサイズが大きい多体系に共通の機構を反映していると推察される．

第 1 章　量子ビット系の量子力学

1.1　はじめに

「量子情報科学」は情報の担い手として量子系を利用する情報科学であり，

- 超高速な計算機 (第 2,3 章)
- テレポーテーション (第 6 章)
- 絶対盗聴されない暗号 (第 8 章)

などの新しい情報処理が対象として挙げられる．

情報理論への応用を念頭に置く場合，

> 与えられた状態にある量子系に対して，ある物理量を測定したとき，ある測定値が得られる確率

を記述する体系として量子力学を定式化し[*2]，その上で状態の時間発展の法則および合成系の記述を学べば充分である．ここで量子力学もあくまで，通常の確率の概念 (確率の正値性や期待値の定義など) を適用できる，操作主義的によく定義された一種の確率論であることを強調しておきたい．

本章では単純でありながら実用的である**量子ビット系** (qubit system) を例に，必要な数学を導入する[*3]．厳密で一般的な量子力学の枠組みは，第 4 章で改めて再論する．

1.2　準備

1.2.1　概念の準備：物理系，状態，物理量の測定

- **物理系** ····· 対象とする集まり
  - **量子 (力学) 系** ····· 量子力学的効果が現れる物理系
    例：原子系，電子系，光子系，電子のスピン，光子の偏極など
  - **合成系** ····· 複数の物理系から成る系
- **物理量** ····· 系の状態を表す (**測定**可能な) 量
  粒子の位置，運動量，エネルギー，(スピン) 角運動量など
- **状態** ····· 操作主義的には「あらゆる物理量の測定を行ったときの測定値の確率分布を定めるもの」
  - **量子状態** ····· 量子系の状態

1.2.2　表記法の準備：Dirac の表記法 I

本項では複素 Euclid 空間 $\mathbb{C}^d$ に対して，**Dirac の表記法**を導入する[*4]．

- **ケット (・ベクトル)** $|\psi\rangle$ は (列) ベクトル $(a_1, \cdots, a_d)^T \in \mathbb{C}^d$ (T は転置) を表す．

[*2] このような観点は Copenhagen (**コペンハーゲン**) **解釈**と整合的である．
[*3] 前提とする予備知識は複素 Euclid 空間 (Euclid 内積付きの複素列ベクトル空間) と行列の基礎だけである．
[*4] この表記法は数学をはじめとする，物理以外の分野では評判が悪いという．

［ベクトルとある基底に関するその成分表示を同一視して [1, pp.25–29]］例えば

$$|\psi\rangle = \begin{pmatrix} 1 \\ 2+i \end{pmatrix}$$

と書いて良い［$\vec{r} = (x, y)^T$ と書くのと同じである］.

- 特に零ベクトルは 0 で表す (ノンゼロのベクトル $|0\rangle$ との混同に注意).
- この記法には古典的なビット列 0100101 に対応する量子状態を，
  単に $|0100101\rangle$ と書けるという利点がある.

- **ブラ** (**・ベクトル**)

$$\langle\psi| \equiv (\overline{a_1}, \cdots, \overline{a_d}) \qquad (\text{バーは複素共役})$$

はケット $|\psi\rangle = (a_1, \cdots, a_d)^T$ に複素共役な行ベクトル (上式右辺で定義される) を表す.

ブラ (bra) とケット (ket) の名前の由来は，それらが括弧 (bracket) $\langle\ \rangle$ の左右の部分にあたることである.

- $|\psi\rangle = (a_1, \cdots, a_d)^T$ と $|\phi\rangle = (b_1, \cdots, b_d)^T$ に対して，積

$$\langle\psi|\phi\rangle = (\overline{a_1}, \cdots, \overline{a_d}) \begin{pmatrix} b_1 \\ \vdots \\ b_d \end{pmatrix} = \sum_{i=1}^{d} \overline{a_i} b_i$$

を定義する．このとき直ちに

(a) $\langle\psi|\psi\rangle = \sum_i |a_i|^2 \geq 0$ (等号成立は $|\psi\rangle = 0$ のとき)

(b) $\overline{\langle\phi|\psi\rangle} = \langle\psi|\phi\rangle$

(c) 線形性 $\langle\psi|a\phi_1 + b\phi_2\rangle = a\langle\psi|\phi_1\rangle + b\langle\psi|\phi_2\rangle$ $(a, b \in \mathbb{C})$ ［ただし $|a\phi_1 + b\phi_2\rangle \equiv a|\phi_1\rangle + b|\phi_2\rangle$］

が成り立つので，$\langle\psi|\phi\rangle$ は **Euclid 内積**を定義している (付録 A.2.2).

- ベクトル $|\psi\rangle$ の大きさ，ないし**ノルム**は $\|\psi\| \equiv \sqrt{\langle\psi|\psi\rangle}$ で定義される.
- 正規直交系 $\{|\psi_i\rangle\}_{i=1}^m$ は $\langle\psi_i|\psi_j\rangle = \delta_{ij}$ で定義される (δ_{ij} は Kronecker のデルタ).

- ［**外積**］

$$|\phi\rangle\langle\psi| = \begin{pmatrix} b_1 \\ \vdots \\ b_d \end{pmatrix} (\overline{a_1}, \cdots, \overline{a_d}) = \begin{pmatrix} b_1\overline{a_1} & \cdots & b_1\overline{a_d} \\ \vdots & \ddots & \vdots \\ b_d\overline{a_1} & \cdots & b_d\overline{a_d} \end{pmatrix} \tag{1.8}$$

は行列である．あるいはケット $|\xi\rangle = (c_1, \cdots, c_d)^T$ に作用して，新しいケット

$$|\phi\rangle\langle\psi|\xi\rangle = \begin{pmatrix} b_1\overline{a_1} & \cdots & b_1\overline{a_d} \\ \vdots & \ddots & \vdots \\ b_d\overline{a_1} & \cdots & b_d\overline{a_d} \end{pmatrix} \begin{pmatrix} c_1 \\ \vdots \\ c_d \end{pmatrix} = \begin{pmatrix} \sum_i (\overline{a_i} c_i) b_1 \\ \vdots \\ \sum_i (\overline{a_i} c_i) b_d \end{pmatrix} = \langle\psi|\xi\rangle |\phi\rangle$$

を作る演算子である．上式において行列の結合則 $(AB)C = A(BC)$ はブラ・ケットの結合則に引き継がれていることが見て取れる．ここから $|\phi\rangle\langle\psi|\xi\rangle$ を，最左辺と最右辺のいずれの意味にも解釈して良いことが保証される.

1.3 量子ビット系

量子ビット系 (qubit system)，あるいは単に**量子ビット**は，空間の与えられた軸に沿う電子のスピンの向き (上向き/下向き) のように，**2 つの根源事象** (root events) から成る量子系である．(量子) 情報科学の文脈で

は，2 つの測定値を「0」と「1」で表せば充分である．

1.3.1　量子ビット系の状態と基底測定

(Q-1) 量子ビットの状態は $\mathbb{C}^2$ の単位ベクトルで表される　特に古典ビット「0」と「1」に対応する量子状態を，それぞれ

$$|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}, \qquad |1\rangle = \begin{pmatrix}0\\1\end{pmatrix} \tag{1.13}$$

で表せる．一般的な状態は $|a|^2 + |b|^2 = 1$ を満たす複素数 a, b を用いて，これらの**重合せ**

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle \tag{1.14}$$

で表される．このように状態ベクトルの和もまた状態となることを**重合せの原理**という．

note　$|0\rangle$ と $|1\rangle$ が $\langle 0|0\rangle = \langle 1|1\rangle = 1$ を満たす単位ベクトルになっていることに注意すると，$|\psi\rangle$ もまた

$$\langle\psi|\psi\rangle = |a|^2 + |b|^2 = 1$$

より単位ベクトルであることが分かる．なお以下の確率規則 Q-3 で見るように，状態 $|\psi\rangle$ が測定値 0 と 1 を得る確率はそれぞれ

$$\langle 0|\psi\rangle^2 = |a|^2, \qquad \langle 1|\psi\rangle^2 = |b|^2$$

なので，$|\psi\rangle$ が単位ベクトルであることは確率の規格化を保証している．

なお状態には位相因子 $c = e^{i\phi}$ (実数 ϕ は位相) を掛ける任意性がある．すなわち $|\psi\rangle$ と $|\psi'\rangle = c\,|\psi\rangle$ は同じ状態を表す．［ここで c は状態のノルムを変えないことに注意せよ．］

(Q-2) 量子ビットの測定は $\mathbb{C}^2$ の正規直交基底 $\{|\phi_0\rangle, |\phi_1\rangle\}$ で表される　［物理量 (観測量) の固有状態として］正規直交基底が得られる測定を，**基底測定**という．上式 (1.13) は量子ビットの正規直交基底の 1 例であり，**計算基底**と呼ばれる．また他の正規直交基底として，

$$|\xi_0\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \qquad |\xi_1\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{1.15}$$

(しばしば順に $|+\rangle, |-\rangle$ とも表記する) や，

$$|\eta_0\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle + i\,|1\rangle), \qquad |\eta_1\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle - i\,|1\rangle) \tag{1.16}$$

が挙げられる．

note　$|0\rangle, |1\rangle$ をそれぞれ順にスピン 1/2 の $+z$ 向きと $-z$ 向きの状態と解釈すると，
式 (1.15) はスピン $\pm x$ 向き，式 (1.16) はスピン $\pm y$ 向きの状態に他ならない [1, p.36].

(Q-3) 状態 $|\psi\rangle$ にある量子ビットに対して測定 $\{|\phi_0\rangle, |\phi_1\rangle\}$ を行ったとき，測定値 $i = 0, 1$ が得られる確率は $\Pr(i) = |\langle\phi_i|\psi\rangle|^2$ で与えられる　正規直交基底 $\{|\phi_i\rangle\}\,(i = 0, 1)$ を用いて状態を $|\psi\rangle = \sum_{i=0,1} x_i\,|\phi_i\rangle$ と展開したとき，展開係数は $\{|\phi_i\rangle\}$ の規格直交性より $x_i = \langle\phi_i|\psi\rangle$ と定まる．［これは測定値 i の確率振幅 (その絶対値の 2 乗が確率 $\Pr(i)$ を与える量) に他ならない．］よって状態の展開は

$$|\psi\rangle = \sum_{i=0,1} |\phi_i\rangle\,\langle\phi_i|\psi\rangle$$

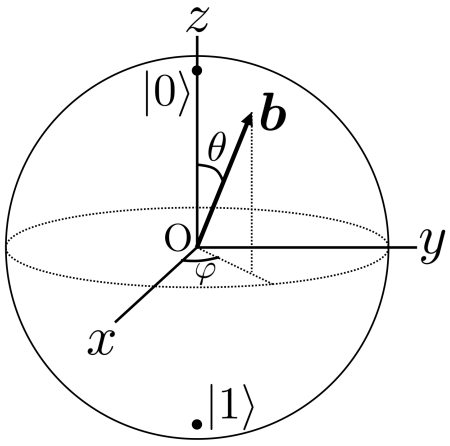


図 2　Bloch 球と Bloch ベクトル $\boldsymbol{b}$

と書ける．［ここから状態を $\{|\phi_i\rangle\}$ で展開できる条件として，有用な恒等式 $\sum_i |\phi_i\rangle\langle\phi_i| = \mathbb{I}$ が見出される [1, pp.24–25].］するとベクトルのノルム

$$\|\psi\|^2 = \sum_i |x_i|^2 = \sum_i \Pr(i)$$

が 1 であることは，確率の規格化を意味することが分かる．

Bloch (ブロッホ) ベクトル　量子ビットの任意の状態は

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle \qquad (0 \le \theta \le \pi,\, 0 \le \varphi \le 2\pi) \tag{1.21}$$

の形に表せる．

理由　一般的な状態 (1.14) において $|a|^2 + |b|^2 = 1$ なので，

$$(0 \le)|a| = \cos\frac{\theta}{2}, \qquad (0 \le)|b| = \sin\frac{\theta}{2} \qquad (0 \le \theta \le \pi)$$

とおける．次いで $|\psi\rangle$ 全体の位相の自由度を利用すると，2 つの係数 a, b のうち一方を実に選べる．そこで $a = \cos\frac{\theta}{2}$ としたときの b の位相を $\varphi\,(0 \le \varphi \le 2\pi)$ とすると上式 (1.21) を得る．

そこで上式 (1.21) の θ と φ をそれぞれ天頂角と方位角に持つ，単位球 (**Bloch 球**) 上の位置ベクトル (**Bloch ベクトル**)

$$\boldsymbol{b} = (\sin\theta\cos\varphi, \sin\theta\sin\varphi, \cos\theta)^T \in \mathbb{R}^3 \qquad (\text{図 } 2)$$

に状態 (1.21) を対応付けて，状態を視覚的に把握することができる．特に $|0\rangle$ は Bloch 球の北極 ($\theta = 0$) に，$|1\rangle$ は Bloch 球の南極 ($\theta = \pi$) に対応する．

note　$|0\rangle, |1\rangle$ をそれぞれスピン $\pm z$ 向きの状態 $|+\rangle, |-\rangle$ に読み替えると，式 (1.21) は (全体の位相の違いを除いて) 文献 [1, pp.225–226] で求めた，スピン $\boldsymbol{b}$ 向きの固有状態に他ならない．

1.3.2　量子ビット系の時間発展

(Q-4) 自然な状態変化　初期時刻の量子状態 $|\psi\rangle$ から終時刻の量子状態 $|\psi'\rangle$ への時間発展は，**ユニタリ (ー) 発展 (変換)**

$$|\psi'\rangle = U|\psi\rangle$$

で与えられる．ここに U は性質 $UU^\dagger = U^\dagger U = \mathbb{I}$ (ただし $U^\dagger$ は U の随伴行列 (転置行列の複素共役)，$\mathbb{I}$ は単位行列) で定義されるユニタリ行列である．例えば Schrödinger 発展では H をハミルトニアンとして，時間発展の演算子 $U = \exp(-iHt/\hbar)$ が対応する (4.3.2 項) ［これは H が時間に陽に依らない場合の表式である [1, pp.96–98]］．ユニタリ性は確率の保存を保証する：

$$\langle\psi'|\psi'\rangle = \langle\psi|U^\dagger U|\psi\rangle = \langle\psi|\psi\rangle\,(=1). \tag{1.26}$$

ユニタリ行列の重要な例として **Pauli 行列**

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{1.27}$$

が挙げられる．これらを代わりに $(\sigma_1, \sigma_2, \sigma_3)$ や X, Y, Z で表すこともある．

note　物理的にはこれらはスピン $\hbar/2$ を単位として測ったスピン角運動量演算子

$$\frac{S_x}{\hbar/2} = (|+\rangle\langle -|) + (|-\rangle\langle +|), \qquad \frac{S_y}{\hbar/2} = -i(|+\rangle\langle -|) + i(|-\rangle\langle +|), \qquad \frac{S_z}{\hbar/2} = (|+\rangle\langle +|) - (|-\rangle\langle -|)$$

の，スピン $\pm z$ 向きの状態 $|\pm\rangle$ に関する行列表示に他ならない [1, p.29,p.36,p.222]．すなわち

$$\frac{\hbar}{2}(\sigma_i)_{a',a''} = \langle a'|S_i|a''\rangle\,. \qquad (a', a'' = \pm\text{は行列要素のラベル})$$

Pauli 行列は［角運動量の］交換関係と，反交換関係

$$[\sigma_i, \sigma_j] \equiv \sigma_i\sigma_j - \sigma_j\sigma_i = 2i\epsilon_{ijk}\sigma_k, \qquad \{\sigma_i, \sigma_j\} \equiv \sigma_i\sigma_j + \sigma_j\sigma_i = 2\delta_{ij}\mathbb{I}$$

を満たす．ここに ϵ_{ijk} は $\epsilon_{123} = +1$ で定義される Levi–Civita 記号であり，また繰り返された (ダミー) 添字 k について和をとる．具体的には第 1 式は $[\sigma_x, \sigma_y] = 2i\sigma_z$, etc. であり，第 2 式は ${\sigma_i}^2 = \mathbb{I}$ (i で和をとらない) を含意する．2 式を辺々足すと，［積 $\sigma_i\sigma_j$ の対称部分と反対称部分への分解として］恒等式

$$\sigma_i\sigma_j = \delta_{ij}\mathbb{I} + i\epsilon_{ijk}\sigma_k$$

を得る．

ここで方向単位ベクトル $\boldsymbol{n} = (n_1, n_2, n_3)(\in \mathbb{R}^3)$ に対して［$\boldsymbol{\sigma} \equiv (\sigma_1, \sigma_2, \sigma_3)$ との“内積”］

$$\sigma_{\boldsymbol{n}} \equiv \sum_{i=1,2,3} n_i\sigma_i = \begin{pmatrix} n_3 & n_1 - in_2 \\ n_1 + in_2 & -n_3 \end{pmatrix}$$

を定義しておく．特に $\boldsymbol{n} = (1, 0, 1)/\sqrt{2}$ に対応する行列

$$H \equiv \frac{1}{\sqrt{2}}(\sigma_x + \sigma_z) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{1.29}$$

は **Hadamard (アダマール) 行列**と呼ばれ，量子計算において重要な役割を演じる．

なお文献 [1, pp.223–224] (のノート) では既に，恒等式

$${\sigma_{\boldsymbol{n}}}^2 = \mathbb{I} \tag{1.35}$$

を示し，次いでこれを用いて，回転行列

$$R_{\boldsymbol{n}}(\theta) = \exp\left(-i\frac{\theta}{2}\sigma_{\boldsymbol{n}}\right) \tag{1.37}$$

(回転演算子 $\exp(-i\boldsymbol{S}\cdot\boldsymbol{n}\theta/\hbar)$ の行列表示，4.4.6 項も見よ) を定義する Taylor 展開が

$$R_{\boldsymbol{n}}(\theta) = \cos\left(\frac{\theta}{2}\right)\mathbb{I} - i\sin\left(\frac{\theta}{2}\right)\sigma_{\boldsymbol{n}} \tag{1.31}$$

を与えることを確認した．

note：教科書 p.31 演習問題 4 について　指数が交換する場合には“指数法則”

$$R_{\boldsymbol{n}}(\theta)^{\dagger}R_{\boldsymbol{n}}(\theta) = \exp\left(i\frac{\theta}{2}\sigma_{\boldsymbol{n}}\right)\exp\left(-i\frac{\theta}{2}\sigma_{\boldsymbol{n}}\right) = \mathbb{I}$$

が成り立つので[*5]，Hermite 行列を生成子に持つ指数 (1.37) はユニタリである．

(Q-5) 状態 $|\psi\rangle$ の系に対して基底 $\{|\phi_0\rangle, |\phi_1\rangle\}$ による測定を行い測定値 $i(=0,1)$ が得られたとき，状態は $|\psi\rangle \mapsto |\phi_i\rangle$ と変化する　これは決定論的なユニタリ発展とは異なる，非連続的でランダムな状態変化であり，測定に伴う状態の攪乱と解釈できる．［規則 (Q-3) は測定により系が状態 $|\phi_i\rangle$ に“飛び移る”確率を与えると言える [1, pp.30–31].］

1.3.3　量子ビット系の合成系——多量子ビット系

n 個の量子ビットの合成系は n-**量子ビット系**と呼ばれ，その状態は 2^n 次元複素ベクトル空間 $\mathbb{C}^{2^n}$ のベクトルで表される．このような**多量子ビット系**に対しても規則 (Q-1) から (Q-5) を (直接一般化して) 適用できる．

ここで合成系の状態・測定と，個々の量子ビット系の状態・測定の関係を記述する手法として，テンソル積を導入する．例えば状態

$$|\psi\rangle = (a_0, a_1)^T, \qquad |\phi\rangle = (b_0, b_1)^T, \qquad |\xi\rangle = (c_0, c_1)^T$$

にある 2 つ，または 3 つの量子ビットから成る合成系の状態は，それぞれ**テンソル積**

$$|\psi\otimes\phi\rangle \equiv |\psi\rangle\otimes|\phi\rangle \equiv \begin{pmatrix} a_0b_0 \\ a_0b_1 \\ a_1b_0 \\ a_1b_1 \end{pmatrix} = \begin{pmatrix} a_0\begin{pmatrix} b_0 \\ b_1 \end{pmatrix} \\ a_1\begin{pmatrix} b_0 \\ b_1 \end{pmatrix} \end{pmatrix} \in \mathbb{C}^4, \tag{1.38}$$

$$|\psi\otimes\phi\otimes\xi\rangle \equiv |\psi\rangle\otimes|\phi\rangle\otimes|\xi\rangle \equiv \begin{pmatrix} a_0b_0c_0 \\ a_0b_0c_1 \\ a_0b_1c_0 \\ a_0b_1c_1 \\ a_1b_0c_0 \\ a_1b_0c_1 \\ a_1b_1c_0 \\ a_1b_1c_1 \end{pmatrix} = \begin{pmatrix} a_0\begin{pmatrix} b_0\begin{pmatrix} c_0 \\ c_1 \end{pmatrix} \\ b_1\begin{pmatrix} c_0 \\ c_1 \end{pmatrix} \end{pmatrix} \\ a_1\begin{pmatrix} b_0\begin{pmatrix} c_0 \\ c_1 \end{pmatrix} \\ b_1\begin{pmatrix} c_0 \\ c_1 \end{pmatrix} \end{pmatrix} \end{pmatrix} \in \mathbb{C}^8$$

で与えられる．この定義は一般の n-量子ビット系の状態を表すテンソル積にも直接拡張される．またテンソル積の構造を考える限り，対応してベクトル空間も

$$\mathbb{C}^{2^n} = \overbrace{\mathbb{C}^2\otimes\cdots\otimes\mathbb{C}^2}^{n\text{ 個}}, \qquad \text{あるいは} \qquad \mathbb{C}^{2^n} = (\mathbb{C}^2)^{\otimes n}$$

のように表される．

[*5] 第 1 の等号で $\sigma_{\boldsymbol{n}}$ の Hermite 性を考慮した．Pauli 行列は Hermite でありユニタリーでもある．

その定義により，テンソル積は以下の性質を満たす［本稿次項で補足］[*6].

- 分配則 (多重線形性)

$$\left(\sum_{i_1=1}^{m_1} a_{i_1}^{(1)} |\psi_{i_1}^{(1)}\rangle\right) \otimes \left(\sum_{i_2=1}^{m_2} a_{i_2}^{(2)} |\psi_{i_2}^{(2)}\rangle\right) \otimes \cdots \otimes \left(\sum_{i_n=1}^{m_n} a_{i_n}^{(n)} |\psi_{i_n}^{(n)}\rangle\right)$$
$$= \sum_{i_1=1}^{m_1} \sum_{i_2=1}^{m_2} \cdots \sum_{i_n=1}^{m_n} a_{i_1}^{(1)} a_{i_2}^{(2)} \cdots a_{i_n}^{(n)} |\psi_{i_1}^{(1)}\rangle \otimes |\psi_{i_2}^{(2)}\rangle \otimes \cdots \otimes |\psi_{i_n}^{(n)}\rangle \,. \tag{1.45}$$

- ノルム

$$\langle \psi_1 \otimes \psi_2 \otimes \cdots \otimes \psi_n | \psi_1' \otimes \psi_2' \otimes \cdots \otimes \psi_n' \rangle = \langle \psi_1 | \psi_1' \rangle \langle \psi_2 | \psi_2' \rangle \cdots \langle \psi_n | \psi_n' \rangle \,. \tag{1.46}$$

ここから単位ベクトル $|\psi_1\rangle, |\psi_2\rangle, \cdots$ のテンソル積も規格化された単位ベクトルとなる.

合成系の状態が必ずしも**積状態**

$$|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$$

の形に書けるとは限らない．実際，例えば 2-量子ビット系に対して，［計算基底 (1.13) の］テンソル積

$$|0\rangle \otimes |0\rangle = (1,0,0,0)^T, \qquad |1\rangle \otimes |1\rangle = (0,0,0,1)^T$$

の重合せ

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle) = \frac{1}{\sqrt{2}}(1,0,0,1)^T \tag{1.43}$$

［係数 $1/\sqrt{2}$ は規格化定数］は積状態 (1.38) の形に書けない.

背理法による確認　仮に 2 式 (1.38),(1.43) を等置すると,

- 第 2 成分より $a_0 = 0$ または $b_1 = 0$.
  ところが $a_0 = 0$ は (第 1 成分) $= 1 \neq 0$ に，$b_1 = 0$ は (第 4 成分) $= 1 \neq 0$ に矛盾する.
- 第 3 成分より $a_1 = 0$ または $b_0 = 0$.
  ところが $a_1 = 0$ は (第 4 成分) $= 1 \neq 0$ に，$b_0 = 0$ は (第 1 成分) $= 1 \neq 0$ に矛盾する.

積状態でない状態は一般に**エンタングル状態** (entangled state)(あるいは**量子もつれ状態，量子絡み合い状態**) と呼ばれる (第 6 章).

次に合成系と部分系に対する測定の関係の議論に移ろう．まず各部分系 $\mu = 1, \cdots, n$ の正規直交基底 $\{|\phi_{i_\mu}^{(\mu)}\rangle\}_{i_\mu=0,1}$ に対して，そのテンソル積 $\{|\phi_{i_1}^{(1)}\rangle \otimes \cdots \otimes |\phi_{i_n}^{(n)}\rangle\}_{i_1,\cdots,i_n=0,1}$ もまた $(\mathbb{C}^2)^{\otimes n}$ の正規直交基底となることに注意する：

$$\langle \phi_{i_1}^{(1)} \otimes \cdots \otimes \phi_{i_n}^{(n)} | \phi_{j_1}^{(1)} \otimes \cdots \otimes \phi_{j_n}^{(n)} \rangle = \langle \phi_{i_1}^{(1)} | \phi_{j_1}^{(1)} \rangle \cdots \langle \phi_{i_n}^{(n)} | \phi_{j_n}^{(n)} \rangle = \delta_{i_1 j_1} \cdots \delta_{i_n j_n}.$$

特に，全ての量子ビット系 μ に計算基底 $|i_\mu = 0,1\rangle$ を用いた場合の基底は，しばしば単に

$$|i_1\rangle \otimes \cdots \otimes |i_n\rangle \equiv |i_1 \cdots i_n\rangle$$

と略記され，n-量子ビット系の**計算基底**と呼ばれる．例えば 2-量子ビット系の計算基底は，式 (1.38) を用いて成分計算すると

$$|00\rangle = (1,0,0,0)^T, \qquad |01\rangle = (0,1,0,0)^T, \qquad |10\rangle = (0,0,1,0)^T, \qquad |11\rangle = (0,0,0,1)^T.$$

[*6] 正確にはテンソル積はそのベクトル表現ではなく，むしろ性質 (1.45–46) で定義される (付録 A.5).

さて，各量子ビット系 $\mu = 1, \cdots, n$ において基底測定 $\{|\phi_{i_\mu}^{(\mu)}\rangle\}_{i_\mu=0,1}$ を行うことは，**合成系上では各基底のテンソル積**

$$|\phi_{i_1}^{(1)} \otimes \cdots \otimes \phi_{i_n}^{(n)}\rangle \tag{1}$$

$(i_1, \cdots, i_n = 0, 1)$ **の基底による測定**に対応する．一般の状態 $|\psi\rangle$ にある合成系に対してこの測定を行い，測定値の組 $(i_1, \cdots, i_n)$ を得る同時確率は

$$\Pr(i_1, \cdots, i_n) = |\langle \phi_{i_1}^{(1)} \otimes \cdots \otimes \phi_{i_n}^{(n)} | \psi \rangle|^2 \tag{1.47}$$

で与えられる．基底 (1) の正規直交性より，上式 (1.47) 右辺における確率振幅は，状態 $|\psi\rangle$ の基底 (1) に関する展開係数 $x_{i_1,\cdots,i_n}$ に他ならない．また測定によって系の状態は $|\psi\rangle$ から式 (1) に飛び移る．

例　2-ビット系のエンタングル状態 (1.43) に対して計算基底 $\{|i_1 i_2\rangle\}$ による測定を行い，測定値の組 $i_1, i_2 = 0, 1$ を得る確率 $\Pr(i_1 i_2)$ は

$$\Pr(00) = \frac{1}{2}, \qquad \Pr(01) = 0, \qquad \Pr(10) = 0, \qquad \Pr(11) = \frac{1}{2}.$$

このとき 2 つのビット系は，一方の測定値が 0 (または 1) ならば，他方の測定値は確実に 0 (または 1) になるという意味で，完全相関している．

他方で同じエンタングル状態 (1.43) において，第 1 の量子ビットには基底測定 (1.15) を，第 2 の量子ビットには基底測定 (1.16) を行う場合，内積の性質 (1.46) より確率振幅は

$$\langle \xi_0 \otimes \eta_0 | \psi \rangle = \frac{1}{\sqrt{2}}(\langle \xi_0|0\rangle \langle \eta_0|0\rangle + \langle \xi_0|1\rangle \langle \eta_0|1\rangle) = \frac{1}{2\sqrt{2}}(1+i),$$

同様に　$\langle \xi_0 \otimes \eta_1 | \psi \rangle = \frac{1}{2\sqrt{2}}(1-i), \qquad \langle \xi_1 \otimes \eta_0 | \psi \rangle = \frac{1}{2\sqrt{2}}(1-i), \qquad \langle \xi_1 \otimes \eta_1 | \psi \rangle = \frac{1}{2\sqrt{2}}(1+i)$

と計算できる．よって 2 つの測定値の相関確率は，完全にランダムな分布

$$\Pr(00) = \Pr(01) = \Pr(10) = \Pr(11) = \frac{1}{4}$$

となる．

さらに n-量子ビット系の**一部**の部分系のみを測定する場合を考える．一般性を失うことなく，測定する量子ビット系を $(\mathbb{C}^2)^{\otimes n} = \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2$ における最初の $m (\leq n)$ 個に選べる[*7]．また基底を $|\phi_i\rangle \to |i\rangle$ (必ずしも計算基底に限らない) と略記する．このとき状態 $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$ の下で測定値の組 $(i_1, \cdots, i_m)$ を得る確率は，仮想的に残りの系も併せて測定を行った場合の確率を考え，次いで和をとることで余分な系に関する分布を無視して得られる**周辺分布** (marginal distribution)

$$\Pr(i_1, \cdots, i_m) = \sum_{j_{m+1}, \cdots, j_n = 0,1} |\langle i_1 \cdots i_m j_{m+1} \cdots j_n | \psi \rangle|^2 \tag{1.55}$$

で与えられる．ここで $x_{j_1 \cdots j_n}$ を展開係数として，全体系と部分系のベクトル

$$|\psi\rangle = \sum_{j_{m+1}, \cdots, j_n = 0,1} x_{j_1 \cdots j_n} |j_1 \cdots j_n\rangle \in (\mathbb{C}^2)^{\otimes n}, \qquad |\phi\rangle \in (\mathbb{C}^2)^{\otimes m}$$

[*7] あるいは注目する m 個の系が任意の箇所にある場合にも，以下の議論は容易に修正できる．

の**部分内積** (partial inner product)

$$\langle\phi|\psi\rangle = \sum_{j_{m+1},\cdots,j_n=0,1} x_{j_1\cdots j_n} \langle\phi|j_1\cdots j_m\rangle\, |j_{m+1}\cdots j_n\rangle \in (\mathbb{C}^2)^{\otimes n-m} \tag{1.52}$$

を定義しよう．これは ($m < n$ のとき)，左辺の見かけに反してベクトルであることに注意する．すると上式 (1.55) は，確率の表式 (1.47) を一般化した形

$$\Pr(i_1,\cdots,i_m) = \| \langle i_1\cdots i_m|\psi\rangle \|^2 \tag{1.56}$$

に書ける．[これは少なくとも見かけ上は，仮想的な測定に関する表現をあからさまに含まない.]

上式 (1.56) の導出　部分内積の定義式 (1.52) は $|\phi\rangle = |i_1\cdots i_m\rangle$ に対して

$$\langle i_1\cdots i_m|\psi\rangle = \sum_{j_{m+1},\cdots,j_n=0,1} x_{i_1\cdots i_m j_{m+1}\cdots j_n} |j_{m+1}\cdots j_n\rangle$$

を与えるので，

$$\begin{aligned}\| \langle i_1\cdots i_m|\psi\rangle \|^2 &= \sum_{j_{m+1},\cdots,j_n=0,1} |x_{i_1\cdots i_m j_{m+1}\cdots j_n}|^2 = \sum_{j_{m+1},\cdots,j_n=0,1} | \langle i_1\cdots i_m j_{m+1}\cdots j_n|\psi\rangle |^2 \\ &= \Pr(i_1,\cdots,i_m) : (1.56). \qquad (\because \text{式 } (1.55))\end{aligned}$$

測定後の部分系の状態は得られた測定結果に対応する基底ベクトル $|i_1\cdots i_m\rangle$ に変化し，測定されていない残り $(n-m)$ 個の量子ビット系の状態は部分内積 $\langle i_1\cdots i_m|\psi\rangle$ に比例する．すなわち全体系の状態は

$$|\psi\rangle \;\mapsto\; |i_1\cdots i_m\rangle \otimes \frac{1}{\| \langle i_1\cdots i_m|\psi\rangle \|} \langle i_1\cdots i_m|\psi\rangle \tag{1.57}$$

と変化し，ここで分母のノルムは適切な規格化因子となっている．

最後に本節の議論を形式的にまとめておく．

(Q-6)　n 個の量子ビットの合成系には，$\mathbb{C}^2$ を n 重テンソル積空間 $(\mathbb{C}^2)^{\otimes n}$ に置き換えた上で規則 (Q-1) から (Q-5) を適用できる．また各部分系と全体の合成系との関係は，(上記の意味で) テンソル積演算 $\otimes$ を通じて与えられる．

1.3.3 項について

■テンソル積の多重線形性 (1.45) について　$n = 3$ の場合には，次にように確認できる．

$$|\psi_i\rangle = \begin{pmatrix} a_0^{(i)} \\ a_1^{(i)} \end{pmatrix}, \qquad |\phi_j\rangle = \begin{pmatrix} b_0^{(j)} \\ b_1^{(j)} \end{pmatrix}, \qquad |\xi_k\rangle = \begin{pmatrix} c_0^{(k)} \\ c_1^{(k)} \end{pmatrix}, \qquad (i = 1,\cdots,l;\ j = 1,\cdots,m;\ k = 1,\cdots,n)$$

とおくと，

$$\begin{aligned}\left(\sum_{i=1}^{l} a_i |\psi_i\rangle\right) \otimes \left(\sum_{j=1}^{m} b_j |\phi_j\rangle\right) \otimes \left(\sum_{k=1}^{n} c_k |\xi_k\rangle\right) &= \begin{pmatrix} \left(\sum_i a_i a_0^{(i)}\right)\left(\sum_j b_j b_0^{(j)}\right)\left(\sum_k c_k c_0^{(k)}\right) \\ \left(\sum_i a_i a_0^{(i)}\right)\left(\sum_j b_j b_0^{(j)}\right)\left(\sum_k c_k c_1^{(k)}\right) \\ \vdots \\ \left(\sum_i a_i a_1^{(i)}\right)\left(\sum_j b_j b_1^{(j)}\right)\left(\sum_k c_k c_1^{(k)}\right) \end{pmatrix} = \sum_{i,j,k} a_i b_j c_k \begin{pmatrix} a_0^{(i)} b_0^{(j)} c_0^{(k)} \\ a_0^{(i)} b_0^{(j)} c_1^{(k)} \\ \vdots \\ a_1^{(i)} b_1^{(j)} c_1^{(k)} \end{pmatrix} \\ &= \sum_{i,j,k} a_i b_j c_k\, |\psi_i\rangle \otimes |\phi_j\rangle \otimes |\xi_k\rangle\,.\end{aligned}$$

■テンソル積のノルム (1.46) の確認

$$|\psi_i\rangle = \begin{pmatrix} a_0^{(i)} \\ a_1^{(i)} \end{pmatrix},\ |\psi_i'\rangle = \begin{pmatrix} b_0^{(i)} \\ b_1^{(i)} \end{pmatrix},\quad \therefore |\psi_1 \otimes \cdots \otimes \psi_n\rangle = \begin{pmatrix} a_0^{(1)} \cdots a_0^{(n-1)} a_0^{(n)} \\ a_0^{(1)} \cdots a_0^{(n-1)} a_1^{(n)} \\ \vdots \\ a_1^{(1)} \cdots a_1^{(n-1)} a_1^{(n)} \end{pmatrix},\ |\psi_1' \otimes \cdots \otimes \psi_n'\rangle = \begin{pmatrix} b_0^{(1)} \cdots b_0^{(n-1)} b_0^{(n)} \\ b_0^{(1)} \cdots b_0^{(n-1)} b_1^{(n)} \\ \vdots \\ b_1^{(1)} \cdots b_1^{(n-1)} b_1^{(n)} \end{pmatrix}$$

とおくと，式 (1.46) の左辺は

$$\langle \psi_1 \otimes \cdots \otimes \psi_n | \psi_1' \otimes \cdots \otimes \psi_n' \rangle = \overline{(a_0^{(1)} \cdots a_0^{(n)})}(b_0^{(1)} \cdots b_0^{(n)}) + \cdots + \overline{(a_1^{(1)} \cdots a_1^{(n)})}(b_1^{(1)} \cdots b_1^{(n)})$$

と書ける．ここで上式右辺の各項において $\overline{a^{(i)}}$ と $b^{(i)}$ の下付き添字の値 $0, 1$ は常に共通であり，右辺は 2^n 通りの可能な下付き添字の組合せにわたる和から成る．よってこれは式 (1.46) 右辺

$$\prod_{i=1}^{n} \langle \psi_i | \psi_i' \rangle = \prod_{i=1}^{n} \left(\overline{a_0^{(i)}} b_0^{(i)} + \overline{a_1^{(i)}} b_1^{(i)} \right)$$

を展開した結果に一致している．

第 2 章　量子計算基礎

2.1　「計算」とは何か？

抽象的には，**計算**とは単純な基本演算の組合せにより入力された情報を変形し，その結果を出力する操作である．例えば素数判定問題では，与えられた自然数 x［≥ 3］を 2 以上 x 未満の整数で順に割り，ある数で割り切れれば x は合成数，いずれの数でも割り切れなければ x は素数と判定できる．この方法は以下の一連の手続きとして明示できる．

素数判定アルゴリズム (primality test)

入力　自然数 $x \in \mathbb{N}$［以下は $x = 1, 2$ には適用できないと考えられる］

出力　x が素数ならば 1，合成数ならば 0

(i)　$y = 2$ とする．

(ii)　x を y で割った余りが 0 ならば 0 を出力して終了する．そうでなければステップ (iii) へ進む．

(iii)　y の値を 1 増価させる．

(iv)　$y = x$ ならば 1 を出力して終了する．そうでなければステップ (ii) へ戻る．

このように条件分岐や加算，剰余算などの単純な基本演算の組合せで計算を実現する手続きを一般に**アルゴリズム**と呼ぶ．実際には数理科学的にアルゴリズムを定式化するには，数学的な計算機のモデルを定義し，基本演算を厳密に定める必要がある．2.3 節では計算機のモデルの具体例として，**回路**モデルを取り上げる．

実践的・工学的にはアルゴリズムの効率の良さにも興味が持たれる．効率の良さの指標は一般に**計算量** (complexity) と呼ばれる．例えば時間計算量とは粗く言うと，計算に必要十分な基本演算の回数のことであり，単に計算量と言う場合には時間計算量のことを指す場合が多い．

プラグマティックには特に，非常に長い入力に対する計算時間のオーダーに興味が持たれる (オーダーの厳密な定義は 2.2 節)．そこで上記の素数判定アルゴリズムの計算時間として，簡単のために割り算の回数だけを調べよう．入力 x が $n(\gg 1)$ ビット列の 2 進数であるとき，すなわち $x \in \{0, 1, 2, \cdots, 2^{n-1}\}$ のとき，割り算の回数のオーダーはたかだか $O(2^n)$ となる．

ここでアルゴリズムの改良を考える．$\sqrt{x}$ を超えない最大の整数を $\lfloor \sqrt{x} \rfloor$ で表すと，x が合成数であれば必ず $\lfloor \sqrt{x} \rfloor$ 以下に因数が現れる．

note：**理由**　合成数は少なくとも 2 つの自然数 a と b を因数として $x = a \cdot b$ と表せる．ただし $1 < a \leq b < x$．ここで仮に $a > \sqrt{x}$ かつ $b > \sqrt{x}$ とすると $a \cdot b > x$ となって $a \cdot b = x$ に反するので，因数 a と b の少なくとも一方，小さい方 a は $\lfloor \sqrt{x} \rfloor$ 以下である．

よって割る数は $\lfloor \sqrt{x} \rfloor$ まで調べれば充分であり，このとき割り算の回数はたかだか $O(2^{n/2})$ に減らせる．

いかなるアルゴリズムを用いてもその問題を解くのに最低限，必要となる時間計算量の下限の存在を示すこともまた有用である．素数判定問題に対しては，現在知られている最良の時間計算量の下限は n である[*8]．また素数判定問題に対する現在最良のアルゴリズムの時間計算量はおよそ $O(n^6)$ であり[*9]，これが最適である

[*8] T. Tao, *Journal of the Australian Mathematical Society,* **91**, 3:405–413 (2012).

[*9] Jr. H. W. Lenstra, C. Pomerance, Primality testing with Gaussian periods, *J. Eur. Math. Soc.,* **21**, 4:1229–1269 (2019).

かは不明である．

2.2 情報科学で必須となる数学記号・記法

- **床関数** (floor function) $\lfloor x \rfloor \equiv \max\{n \in \mathbb{Z} | n \leq x\}$ は x 以下の最大の整数である (2.1 節で導入済み)．
  天井関数 (ceiling function) $\lceil x \rceil \equiv \min\{n \in \mathbb{Z} | x \leq n\}$ は x 以上の最小の整数である．
- **対数** log は断りのない限り，2 を底とする．また $(\log x)^n$ を $\log^n x$ と書く．
- **定義：オーダー記法**　関数 $f, g : \mathbb{N} \to \mathbb{N}$ を考える．
  ある正の実数 C が存在して，十分大きな任意の $n \in \mathbb{N}$ に対して $f(n) \leq Cg(n)$ が成立する，すなわち

$$\limsup_{n\to\infty} \frac{f(n)}{g(n)} \leq C$$

  ならば，$f(n) \in O(g(n))$ あるいは $f(n) = O(g(n))$ と書く．
  ある正の実数 D が存在して，十分大きな任意の $n \in \mathbb{N}$ に対して $f(n) \geq Dg(n)$ が成立する，すなわち

$$\liminf_{n\to\infty} \frac{f(n)}{g(n)} \leq D$$

  ならば，$f(n) \in \Omega(g(n))$ あるいは $f(n) = \Omega(g(n))$ と書く．
  記号 O, Ω はそれぞれ関数の大雑把な上界と下界を与える．
  ［少なくとも第 3 章までは，直観的な理解で良い[*10]．］
- 集合 $\mathcal{X}$ の要素の数 (**集合のサイズ**) を $|\mathcal{X}|$ で表す．
- ビット列において隣接する n 個の 0 の並びを 0^n で表す．

2.3 古典回路モデル

アルゴリズムを定式化する代表的な計算モデルとして，回路モデルが挙げられる．量子力学の原理を取り入れた**量子計算**における回路モデルと区別して，通常の計算機上で実現される**古典計算**の回路モデルを特に**古典回路**モデルと呼ぶ．今一つの代表的な計算モデルに Turing 機械があるものの，これに関しては定義と取り扱いがやや煩雑となるため，ここでは取り上げない．

古典回路は表 1 のように，入力に対してあらかじめ決まった出力を持つ素子を基本素子とし，それらを組合せて構成できる．演算の優先順位は $\neg > \wedge > \vee$ である．

表 1　古典回路の基本素子［0 を偽，1 を真と読み替えれば良い］

$\wedge$ 素子 (AND)

入力	出力
00	0
01	0
10	0
11	1

$\vee$ 素子 (OR)

入力	出力
00	0
01	1
10	1
11	1

$\neg$ 素子 (NOT)

入力	出力
1	0
0	1

[*10] オーダーに関する教科書 p.50 の演習問題 9 はやや人工的・数学的なパズルの感がある．

古典回路モデルは n ビット列から 1 ビットへの関数 $\{0,1\}^n \to \{0,1\}$ を計算しており，これを**論理関数** (Boolean function) と呼ぶ．また論理関数を実現する回路モデルは，その計算資源が少ない方が実用的である．計算資源の指標として「回路に使用する基本素子の数」を用いることができる．そこで以下の定義が動機付けられる．

定義　論理関数 $f : \{0,1\}^n \to \{0,1\}$ の**回路計算量** (circuit complexity) $\mathcal{C}(f)$ とは，f を正しく計算する回路 C の素子数 $|C|$ が最小となる回路の素子数

$$\mathcal{C}(f) \equiv \min\{\, |C| \,|\forall x \in \{0,1\}^n, C(x) = f(x)\}$$

である．

以下の議論のためには，古典計算であれ量子計算であれ，論理関数 f を計算する素子数の小さな回路があれば，計算モデルに依らずに f を計算する効率の良いアルゴリズムがある，という程度の認識で十分である．

ここで例として，n ビット列 x の入力に含まれる 1 の数が奇数ならば 1 を，偶数ならば 0 を出力する**偶奇判定問題** (parity problem) を考える．$n = 2$ の場合 $x = x_1x_2$ であり，ビット $x_1, x_2 \in \{0,1\}$ に対して出力 $x_1 \oplus x_2$ が表 2 のように定義される排他的論理和 $\oplus$ が，偶奇判定問題の正しい出力 $\mathrm{PARITY}(x)$ を与えている．［本稿の表 2 では入出力の列の間に予備計算の欄を補っておいた．ここから見て取れるように］排他的論理和は基本素子の組合せ

$$x_1 \oplus x_2 = \oplus(x_1, x_2) = (x_1 \wedge \neg x_2) \vee (\neg x_1 \wedge x_2)$$

で実現できる．これを回路として描けば図 3 のようになる．

note　次に $n = 3$ の場合，2 つのビット列 x_1 と x_2x_3 の一方のみが奇数個の 1 を含む (ことが真である) 場合に，$x_1x_2x_3$ は奇数個の 1 を含むので，再び排他的論理和を用いて

$$\mathrm{PARITY}(x_1x_2x_3) = x_1 \oplus (x_2 \oplus x_3) \equiv x_1 \oplus x_2 \oplus x_3$$

とできる．この論法は繰り返し適用でき，再帰的に $x_1 \oplus x_2 \oplus x_3 \oplus \cdots$ を定義できる：

$n = 3, 4, \cdots$ に対して

$$\begin{aligned}
\mathrm{PARITY}(x_1x_2x_3x_4) =& (x_1 \oplus x_2) \oplus (x_3 \oplus x_4) \equiv x_1 \oplus x_2 \oplus x_3 \oplus x_4, \\
\mathrm{PARITY}(x_1x_2x_3x_4x_5) =& (x_1 \oplus x_2) \oplus (x_3 \oplus x_4 \oplus x_5) \equiv x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5, \\
&\vdots
\end{aligned}$$

であり，対応する回路に要する素子の総数は $O(n)$ となる．

より一般に任意の関数は基本素子を組合せた回路で計算でき，その回路計算量の上限は次の定理で与えられる．

定理　任意の $n \in \mathbb{N}$ に対して，任意の論理関数 $f : \{0,1\}^n \to \{0,1\}$ の回路計算量はたかだか $5 \cdot 2^{n-1} - 4$ である．

証明　n に関する数学的帰納法で証明する．

$n = 1$ のとき入力は 1 ビットの $x = 0, 1$ であり，その 2 値の各々に対して出力 $f(x)$ もまた 2 値 $0, 1$ なので，4 通りの関数

$$f(x) = 0, \qquad f(x) = 1, \qquad f(x) = x, \qquad f(x) = \neg x$$

表 2　排他的論理和 $\oplus$

x_1	x_2	$\neg x_1$	$\neg x_2$	$x_1 \wedge \neg x_2$	$\neg x_1 \wedge x_2$	$x_1 \oplus x_2$
0	0	1	1	0	0	0
0	1	1	0	0	1	1
1	0	0	1	1	0	1
1	1	0	0	0	0	0

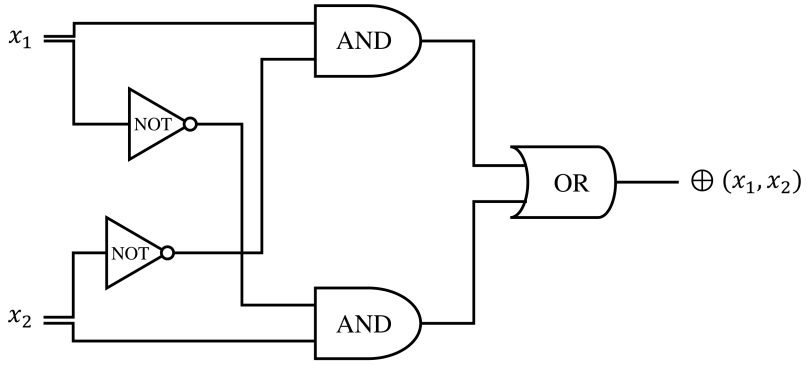


図 3　排他的論理和 $\oplus$

があり得る．最初の 2 つは定数関数であり，$f(x) = \neg x$ の場合にのみ 1 つの素子 $\neg$ が必要となるので，命題は $n = 1$ で成り立っている．
次にある n で命題が成り立つと仮定して，恒等式

$$f(x_1, \cdots, x_n, x_{n+1}) = (\neg x_{n+1} \wedge f(x_1, \cdots, x_n, 0)) \vee (x_{n+1} \wedge f(x_1, \cdots, x_n, 1)) \tag{2.3}$$

に着眼しよう．
note：式 (2.3) について　(教科書の指示に従い) $x_n = 0, 1$ を代入すると，上式 (2.3) はそれぞれ

$$\begin{aligned} f(x_1, \cdots, x_n, 0) =& (1 \wedge f(x_1, \cdots, x_n, 0)) \vee (0 \wedge f(x_1, \cdots, x_n, 1)), \\ f(x_1, \cdots, x_n, 1) =& (0 \wedge f(x_1, \cdots, x_n, 0)) \vee (1 \wedge f(x_1, \cdots, x_n, 1)) \end{aligned}$$

を与える．y を 0 または 1 のいずれかとして，右辺において恒等的に

$$0 \wedge f(x_1, \cdots, x_n, y) = 0, \quad 1 \wedge f(x_1, \cdots, x_n, y) = f(x_1, \cdots, x_n, 0), \quad 0 \vee f(x_1, \cdots, x_n, y) = f(x_1, \cdots, x_n, y)$$

と簡略化されることに注意すると，上式が成り立っていることが分かる．なお $n = 1$ の場合から始め，このように論理関数を逐次的に構成できることは，任意の論理回路が基本素子を組合せた回路で計算できることの証明にもなっている．
式 (2.3) の右辺は合計 4 つの素子 ($\wedge$ が 2 つ，$\vee$ が 1 つ，$\neg$ が 1 つ) と，仮定により各々がたかだか $5 \cdot 2^{n-1} - 4$ 個の素子で計算できる 2 つの関数から成っているので，その回路計算量はたかだか

$$2 \cdot (5 \cdot 2^{n-1} - 4) + 4 = 5 \cdot 2^n - 4.$$

よって $n \to n + 1$ と置き換えた命題も成り立つので，示された．

他方で具体的な関数の回路計算量の下限を証明することは一般に極めて困難である．実際，有名な未解決問

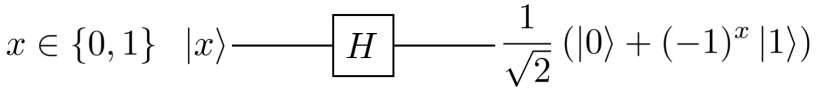


図 4　Hadamard 変換

題である NP≠P 予想[*11]は，ある種の問題の時間計算量の下限を証明する問題である．しかしながら天下りに述べると，小さな回路では計算できない難しい関数の存在を示す，以下の定理が成り立つことが知られている．

定理　十分大きな任意の $n \in \mathbb{N}$ に対して，ある n 入力 1 出力の論理関数 $f : \{0,1\}^n \to \{0,1\}$ が存在して，その f の回路計算量は少なくとも $2^n/2n$ である．［指数の因子があるため，n の多項式の回路計算量を持つアルゴリズムよりも効率が圧倒的に悪い．］

2.4　量子回路モデル

古典計算において古典ビットを操作する古典回路のように，量子計算において量子ビットを操作する計算モデルとして，ここでは**量子回路**モデルを説明する．量子計算は量子ビットを量子ビットへと変換し，そのアルゴリズムにおいて許される操作は測定とユニタリ変換のみである．以下では計算基底による基底測定を単に測定と呼ぶ．

単位行列 $\mathbb{I}$ と Pauli 行列 (1.27) を Dirac の表記法で

$$\mathbb{I} = |0\rangle\langle 0| + |1\rangle\langle 1|, \qquad \sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|, \qquad \sigma_y = -i|0\rangle\langle 1| + i|1\rangle\langle 0|, \qquad \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$$

と書いておく．すると直ちに，σ_x, σ_z の量子ビットへの作用は

$$\sigma_x|0\rangle = |1\rangle, \qquad \sigma_x|1\rangle = |0\rangle, \qquad \sigma_z(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle - \beta|1\rangle$$

となることが分かる．

- すなわち σ_x は古典計算における $\neg$ 素子と同じ**ビット反転** (bit flip) の操作を行う．
- またこの σ_z の作用は**位相反転** (phase flip) と呼ばれる．

さらに **Hadamard 変換** (1.29) もユニタリであり，基底 (1.15):$|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ を用いて

$$H = |+\rangle\langle 0| + |-\rangle\langle 1| \tag{2.4}$$

と表せる［本稿次節で確認］．ここから量子ビットへの作用

$$H|0\rangle = |+\rangle, \qquad H|1\rangle = |-\rangle$$

が見て取れる．［スピン 1/2 の系の文脈では，H は $\pm z$ 向きのスピンを $\pm x$ 向きに移行させる．］Hadamard 変換のように入出力長があらかじめ決められたユニタリ行列を**量子素子** (quantum gate) と呼ぶ．Hadamard 行列に対応する量子素子は図 4 のような回路図で表せる．

[*11] Clay Mathematics Institute, *Millennium Prize Problems: NP versus P Problem*, `http://www.claymath.org/millennium/P_vs_NP/`.
J. Carlson, A. Jaffe, A. Wiles, *The Millennium Prize Problems*, AMS (2006).

注意：ユニタリ変換の性質

- ユニタリ性

$$\delta_{ij} = U_{ik}(U^\dagger)_{kj} = U_{ik}{U_{jk}}^*, \qquad \delta_{ij} = (U^\dagger)_{ik}U_{kj} = {U_{ki}}^*U_{kj} \qquad (k \text{ で和をとる})$$

より，ユニタリ行列 U の各行および各列は正規直交基底を成す．

- ユニタリ変換はベクトルの大きさを保存するため［式 (1.26)］，正規直交系 $\{|\phi_i\rangle\}$ を別の正規直交系に移す：

$$|\phi_i'\rangle = U|\phi_i\rangle \quad \Rightarrow \quad \langle\phi_i'|\phi_j'\rangle = \langle\phi_i|U^\dagger U|\phi_j\rangle = \langle\phi_i|\phi_j\rangle = \delta_{ij}.$$

- 測定を含まない量子計算はユニタリ変換から成るので逆演算が存在する (他方，測定は非可逆過程)．

$N = 2^n$ 次の正方行列 $U = (U_{ij})$ と $M = 2^m$ 次の正方行列 V のテンソル積は

$$U \otimes V = \begin{pmatrix} U_{11}V & \cdots & U_{1N}V \\ \cdots\cdots\cdots\cdots\cdots\cdots & & \\ U_{N1}V & \cdots & U_{NN}V \end{pmatrix} \tag{2.6}$$

で定義される．このとき

- n-量子ビット列 $|\phi\rangle \in \mathbb{C}^N$ と m-量子ビット列 $|\psi\rangle \in \mathbb{C}^M$ の積状態 $|\phi,\psi\rangle \equiv |\phi\rangle \otimes |\psi\rangle$ への作用は

$$(U \otimes V)|\phi,\psi\rangle = U|\phi\rangle \otimes V|\psi\rangle \tag{2.5}$$

となる．

- 双線形性

$$U \otimes (aV_0 + bV_1) = aU \otimes V_0 + bU \otimes V_1, \qquad (aU_0 + bU_1) \otimes V = aU_0 \otimes V + bU_1 \otimes V$$

が成り立つ．

［これらを本稿次節で一般的に確認する．また以下で重要なこととして，ユニタリ性がテンソル積 $U \otimes V$ に引き継がれることも示す．］

テンソル積を用いて，多量子ビット列に対する重要な量子素子 (ユニタリ行列) を定義する．まず 2-量子ビット列に対して，**制御 NOT 素子** (controlled NOT gate)

$$\begin{aligned} \mathrm{CNOT} &= |0\rangle\langle 0| \otimes \mathbb{I} + |1\rangle\langle 1| \otimes \sigma_x \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \otimes \mathbb{I} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \otimes \sigma_x = \begin{pmatrix} \mathbb{I} & 0 \\ 0 & \sigma_x \end{pmatrix} \end{aligned}$$

を定義する (図 5)．このとき式 (2.5) と本節冒頭の $\sigma_x|y\rangle = |\neg y\rangle$ より

$$\begin{aligned} \mathrm{CNOT}|xy\rangle &= |0\rangle\langle 0|x\rangle \otimes \mathbb{I}|y\rangle + |1\rangle\langle 1|x\rangle \otimes \sigma_x|y\rangle \\ &= \begin{cases} |0\rangle \otimes |y\rangle & (x = 0 \text{ のとき}) \\ |1\rangle \otimes |\neg y\rangle & (x = 1 \text{ のとき}) \end{cases} \end{aligned}$$

となるので，CNOT は 1 ビット目に 1 が入力されているときだけ，2 ビット目に $\neg$ と同じ操作 (0 と 1 の反転) を行うことが分かる (1 ビット目は常にそのまま出力される)．［このとき図 5 のように，2 ビット目の出力は常に排他的論理和 $x \oplus y$ で表されることが，場合分けにより直接確認できる．］このように 1 ビット目が 2 ビット目の出力の制御ビットとなっていることが，制御 NOT という名前の由来である．

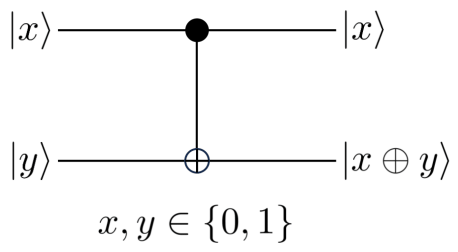


図 5　制御 NOT 素子

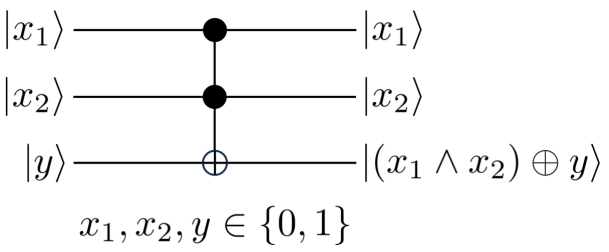


図 6　Toffoli 素子

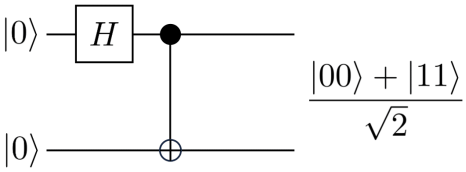


図 7　量子回路の例 (1)

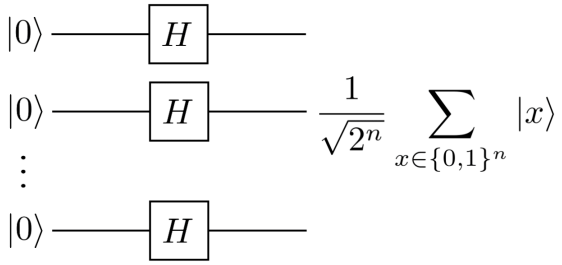


図 8　量子回路の例 (2)

$(k+1)$ ビット入力 $(k+1)$ ビット出力の一般化制御 NOT 素子 GCNOT は，最初の k 個の制御ビットの入力が全て 1 のとき $(k+1)$ 番目のビットを反転し，それ以外は何もしない，すなわち

$$\mathrm{GCNOT}\,|x_1, \cdots, x_k, y\rangle = |x_1, \cdots, x_k, y \oplus (x_1 \wedge \cdots \wedge x_k)\rangle \tag{2.8}$$

と表せる ($k = 1$ で CNOT に帰着)．$k = 2$ に対してこれは **Toffoli 素子**，あるいは制御-制御 NOT 素子 CCNOT と呼ばれ，図 6 の回路図で表される．

次に図 7 の量子回路を考える．ここに任意の量子ビット列 $|xy\rangle$ を入力すると，状態は

$$\begin{aligned} |xy\rangle &\xmapsto{H\otimes\mathbb{I}} H\,|x\rangle \otimes \mathbb{I}\,|y\rangle = \left(\frac{1}{\sqrt{2}}(|0\rangle + (-1)^x\,|1\rangle)\right) \otimes |y\rangle = \left(\frac{1}{\sqrt{2}}(|0y\rangle + (-1)^x\,|1y\rangle)\right) \\ &\xmapsto{\mathrm{CNOT}} \left(\frac{1}{\sqrt{2}}(\mathrm{CNOT}\,|0y\rangle + (-1)^x \mathrm{CNOT}\,|1y\rangle)\right) = \left(\frac{1}{\sqrt{2}}(|0y\rangle + (-1)^x\,|1(\neg y)\rangle)\right) \end{aligned}$$

と変化する．特に入力 $|00\rangle = |0^2\rangle$ に対する出力は $(|00\rangle + |11\rangle)/\sqrt{2}$ である．［これはエンタングル状態 (1.43) である．教科書ではあらかじめ $x = y = 0$ の場合のみを調べている．］

また n 個の Hadamard 変換から成る図 8 の量子回路では，量子ビット列 $|0\cdots0\rangle = |0^n\rangle$ を入力したときの出力は

$$\begin{aligned} H^{\otimes n}\,|0^n\rangle =& H\,|0\rangle \otimes \cdots \otimes H\,|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \cdots \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ =& \frac{1}{\sqrt{2^n}} \underbrace{(|000\cdots\rangle + |010\cdots\rangle + \cdots + |111\cdots\rangle)}_{2^n\text{個}} = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \end{aligned} \tag{2}$$

となる．すなわち 2^n 個の基底の等しい重みによる重合せが得られる．

以下，より詳しい量子回路についての基礎的な事項に踏み込んでいくが，もし量子回路よりも量子アルゴリズムに興味がある読者はここまでの知識で次章の「量子アルゴリズム」に進んでも差し支えない．(教科書 p.60 を引用)

定理：Z–Y 分解　式 (1.37) の $R_{\boldsymbol{n}}(\theta)$ で特に各座標軸の方向単位ベクトル $\boldsymbol{n} = \hat{\boldsymbol{x}}, \hat{\boldsymbol{y}}, \hat{\boldsymbol{z}}$ 周りの回転を表す行列をそれぞれ $R_x(\theta), R_y(\theta), R_z(\theta)$ と書こう．このとき 1 量子ビットの状態に作用するユニタリ行列は，単に R_y, R_z と位相因子の組合せ

$$U = e^{i\varphi} R_z(\alpha) R_y(\beta) R_z(\gamma)$$

で表せる．

これについては教科書の説明を補足しつつまとめる．1 量子ビット系の状態はスピンの Bloch ベクトル向きの固有状態に対応する 2 成分スピノルで表される (1.3.2 項)．このスピノルに作用する回転の表現行列は式 (1.37) で与えられる．回転を軸方向と回転角 $\boldsymbol{n}, \theta$ の代わりに Euler 角 (α, β, γ) で指定すれば，行列 (1.37) は等価的に $R(\alpha, \beta, \gamma)$ と書ける．ここで文献 [1, pp.231–234](のノート) では与えられた Euler 角の回転操作 $\mathcal{D}(\alpha, \beta, \gamma)$ が，(物理系ではなく) **空間に**固定された座標軸の周りの一連の回転操作 $\mathcal{D}_z(\alpha)\mathcal{D}_y(\beta)\mathcal{D}_z(\gamma)$ として再現されることを幾何学的に確認し，その行列表現が

$$\begin{aligned} R(\alpha, \beta, \gamma) =& R_z(\alpha) R_y(\beta) R_x(\gamma) = \exp\left(-\frac{i\sigma_3\alpha}{2}\right) \exp\left(-\frac{i\sigma_2\beta}{2}\right) \exp\left(-\frac{i\sigma_3\gamma}{2}\right) \\ =& \begin{pmatrix} e^{-i(\alpha+\gamma)/2}\cos(\beta/2) & e^{-i(\alpha-\gamma)/2}\sin(\beta/2) \\ e^{i(\alpha-\gamma)/2}\sin(\beta/2) & e^{i(\alpha+\gamma)/2}\cos(\beta/2) \end{pmatrix} \end{aligned}$$

となることを見た．最右辺は SU(2) 行列の一般的な形

$$R = \begin{pmatrix} a & -\bar{b} \\ b & \bar{a} \end{pmatrix}, \qquad |a|^2 + |b|^2 = 1$$

をしており，教科書ではこのことから逆に，SU(2) 行列が必ず $R_z(\alpha)R_y(\beta)R_x(\gamma)$ の形に書けることだけを述べて済ませている．最後に 1 量子ビット系へのユニタリな操作は回転に限らず，U(2) 行列 (2 次のユニタリ行列) であって良い．ところが直積への分解 $\mathrm{U}(2) \simeq \mathrm{U}(1) \times \mathrm{SU}(2)$ により [5, p.80,p.88]，U(2) 行列 U は SU(2) 行列 R と位相因子の違いしかない．実際 $1 = \det(U^\dagger U) = |\det U|^2$ より $\det U = e^{2i\varphi}$ とおける．そこで $U = e^{i\varphi}R$ とおくと

$$e^{2i\varphi} = \det U = (e^{i\varphi})^2 \det R, \ \therefore \det R = 1, \qquad \text{また} \qquad R^\dagger R = U^\dagger U = 1$$

より R は SU(2) 行列である．

以降は半ば天下りに話を進める．さらに任意の長さの量子ビット列のユニタリ変換の量子回路は，1 ビット量子ビットの量子回路と CNOT 素子で構成できることが知られている．

定理　任意の n-量子ビット上のユニタリ行列は 1 ビット入出力量子回路と CNOT 素子を合計 $O(n^2 2^{2n})$ 個使用することで構成することができる[*12]．

[*12] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, H. Weinfurter, *Phys. Rev. A,* **52**, 3457–3467 (1995).
M. A. Nielsen, I. L. Chuang, *Quantum Computation and Quantum Information,* Cambridge University Press (2000).

このように任意のユニタリ行列が構成可能な量子素子集合は**万能** (universal) であると言われる．

古典回路とは対照的に，量子回路にはユニタリ行列が可逆でなければならないという制約がある．すると古典回路では計算可能であった論理関数 $f : \{0,1\}^n \to \{0,1\}$ を量子回路でも計算できるかという疑問が生じる．ところが Toffoli 素子

$$\mathrm{CCNOT}(x_1, x_2, x_3) = (x_1, x_2, (x_1 \wedge x_2) \oplus x_3) \qquad (x_1, x_2, x_3 \in \{0,1\})$$

を組合せると，古典回路の基本素子 $\neg, \wedge, \vee$ を模倣できる．実際

- $\mathrm{CCNOT}(1, 1, x_3) = (1, 1, \neg x_3)$ より第 3 入出力で $\neg$ 素子を実現できる．
- $\mathrm{CCNOT}(x_1, x_2, 0) = (x_1, x_2, x_1 \wedge x_2)$ より［$x = 0, 1$ に対して $x \oplus 0 = x$ を直接確認できる］，入力 x_1, x_2 と第 3 出力の間で $\wedge$ 素子を実現できる．
- De Morgan (ド・モルガン) の法則 $x_1 \vee x_2 = \neg((\neg x_1) \wedge (\neg x_2))$ より，このとき $\vee$ 素子も模倣可能である．

ここから任意の f を計算する量子回路を構成できることが期待される．この直観を反映して，次の定理が成立する．

定理　論理関数 $f : \{0,1\}^n \to \{0,1\}$ を回路サイズ $s(n)$ の論理回路で計算可能な任意の関数とする．このとき

$$U_f \left|x\right\rangle \left|0\right\rangle \left|011\right\rangle \left|0^{l(n)}\right\rangle = \left|x\right\rangle \left|f(x)\right\rangle \left|011\right\rangle \left|G(x)\right\rangle \tag{2.10}$$

を満たす CCNOT 素子のみから成る量子回路 U_f が存在する．ただし，ここでテンソル積の記号 $\otimes$ を省略しており，また

$$G : \{0,1\}^n \to \{0,1\}^{l(n)}, \qquad l(n) = O(s(n) + n)$$

である．

左辺は $|x\rangle$ の他に固定入力ビット列 $|011\rangle$ および計算過程を保存する補助入力ビット列を含んでおり，右辺において計算したい値 $f(x)$ のビット列が得られている．$|G(x)\rangle$ はゴミ情報であり，これは f の計算終了後に，可逆性を壊すことなく $|0^{l(n)}\rangle$ へと初期化できる．

式 (2.10) の定理の系　上式 (2.10) における U_f を 2 つと CNOT を 1 つ使用した量子回路 U'_f が存在して，

$$U'_f \left|x\right\rangle \left|0\right\rangle \left|011\right\rangle \left|0^{l(n)}\right\rangle = \left|x\right\rangle \left|f(x)\right\rangle \left|011\right\rangle \left|0^{l(n)}\right\rangle . \tag{2.11}$$

最後に量子計算においてゴミ情報を除くことの重要性を説明する．式 (2.10) において入出力に対応するのは両辺の最初の 2 ビット列 $\left|x\right\rangle \left|0\right\rangle , \left|x\right\rangle \left|f(x)\right\rangle$ である．そこで入力として特に重合せ $(\left|x\right\rangle \left|0\right\rangle + \left|y\right\rangle \left|0\right\rangle)/\sqrt{2}$ を考えると，式 (2.10) 右辺は

$$\frac{1}{\sqrt{2}}(\left|x\right\rangle \left|f(x)\right\rangle \left|011\right\rangle \left|G(x)\right\rangle + \left|y\right\rangle \left|f(y)\right\rangle \left|011\right\rangle \left|G(y)\right\rangle)$$

となり，ゴミ情報の部分 $\left|G(x)\right\rangle , \left|G(y)\right\rangle$ を分離できない．他方で式 (2.11) の方法を用いた場合には，補助ビット列が式全体から乗法的な形で分離された結果

$$\frac{1}{\sqrt{2}}(\left|x\right\rangle \left|f(x)\right\rangle + \left|y\right\rangle \left|f(y)\right\rangle) \otimes \left|011\right\rangle \left|0 \cdots 0\right\rangle$$

が得られる．しかるに分離不可能なゴミ情報があると，量子的効果が期待通りに活かせない場合がある．そのことを例示するために，以下では $f(0)=f(1)=0$ として一連の操作

$$\text{Hadamard 変換} \quad \to \quad \text{ユニタリ変換} U_f \quad \to \quad \text{Hadamard 変換}$$

を考えよう．$U_f|x\rangle|0\rangle = |x\rangle|f(x)\rangle$ を通じて f がゴミ情報なしで計算できるとき，

$$\begin{aligned}
&|0\rangle|0\rangle \overset{H\otimes\mathbb{I}}{\longmapsto} \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)|0\rangle \overset{U_f}{\longmapsto} \frac{1}{\sqrt{2}}(|0,f(0)\rangle+|1,f(1)\rangle)\\
=&\frac{1}{\sqrt{2}}(|0,0\rangle+|1,0\rangle) \overset{H\otimes\mathbb{I}}{\longmapsto} \frac{1}{\sqrt{2}}\left\{\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)|0\rangle+\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)|0\rangle\right\} = |0\rangle|0\rangle
\end{aligned}$$

となる［2 行目の途中計算を補足した］．よって最後の量子ビット $|f(x)\rangle$ を測定すると，常に 0 が得られる．他方で例えば $U_f|x\rangle|0\rangle|0\rangle = |x\rangle|G_f(x)\rangle|f(x)\rangle$ のようにゴミ情報 $G_f(x)$ が付随する場合，

$$\begin{aligned}
|0\rangle|0\rangle|0\rangle &\overset{H\otimes\mathbb{I}\otimes\mathbb{I}}{\longmapsto} \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)|0\rangle)|0\rangle \overset{U_f}{\longmapsto} \frac{1}{\sqrt{2}}(|0,G_f(0),f(0)\rangle+|1,G_f(1),f(1)\rangle)\\
&\overset{H\otimes\mathbb{I}\otimes\mathbb{I}}{\longmapsto} \frac{1}{\sqrt{2}}(|0\rangle|G_f(0)\rangle|0\rangle+|1\rangle|G_f(0)\rangle|0\rangle+|0\rangle|G_f(1)\rangle|0\rangle-|1\rangle|G_f(1)\rangle|0\rangle).
\end{aligned}$$

するとゴミ情報が分離できない $G_f(0)=G_f(1)$ の場合には，最後の量子ビット $|f(x)\rangle$ の測定で 0 と 1 がそれぞれ確率 1/2 ずつで得られることになってしまう．なお，この例は 3.1 節の Deutsch-Jozsa のアルゴリズムの特別な場合である．

2.4 節について

■Hadamard 行列 (1.29) のユニタリ性と Dirac 表記 (2.4) について　行列 (1.29) に対して直接の成分計算により

$$H^\dagger = H, \qquad H^2 = \mathbb{I}$$

が確かめられるので，H は Pauli 行列と同様に Hermite 性とユニタリー性が成り立つ．また

$$\begin{aligned}
H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} =& \frac{1}{\sqrt{2}}(|0\rangle\langle 0|+|0\rangle\langle 1|+|1\rangle\langle 0|-|1\rangle\langle 1|)\\
=& \left(\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\right)\langle 0|+\left(\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\right)\langle 1| = |+\rangle\langle 0|+|-\rangle\langle 1| : (2.4).
\end{aligned}$$

■テンソル積 (2.6) の作用 (2.5) と双線形性について　行列のテンソル積の定義式 (2.6) は等価的に

$$[U\otimes V]_{ia,jb} = U_{ij}V_{ab} \qquad (i,j=1,\cdots,N;\ a,b=1,\cdots,M)$$

と書ける．実際このとき例えば $N=3, M=2$ とすると，$NM=6$ 次正方行列 $U\otimes V$ の行はラベルの組 ia で，列はラベルの組 jb で指定される．すると図 9 のように 3×3 個のブロックの位置が (i,j) でラベルされ，ブロック内の 2×2 個の成分が (a,b) で指定されることになる．そこで上式に従って各 (i,j) ブロックごとに共通の行列要素 U_{ij} を置き，次いで各ブロックに行列 V のコピーを置くと (U_{ij} との積をとる)，式 (2.6) 右辺が得られる [4, p.29].

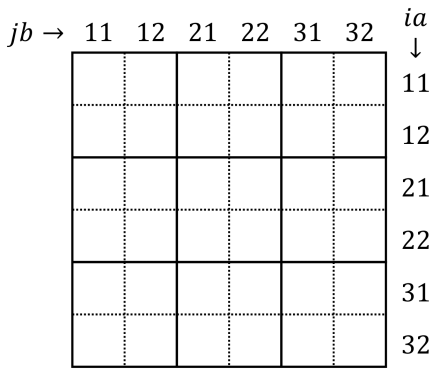


図 9　行列のテンソル積の構造

対応して積状態

$$|\phi,\psi\rangle = \begin{pmatrix} \phi_1 \begin{pmatrix} \psi_1 \\ \vdots \\ \psi_M \end{pmatrix} \\ \vdots \\ \phi_N \begin{pmatrix} \psi_1 \\ \vdots \\ \psi_M \end{pmatrix} \end{pmatrix}$$

のベクトル成分 $|\phi,\psi\rangle_{ia} = \phi_i\psi_a$ も添字の組

$$ia = 11,\cdots,1M,21,\cdots,2M,\cdots,N1,\cdots,NM$$

で順にラベルすると便利である．このとき式 (2.5) は

$$\sum_{j,b}[U\otimes V]_{ia,jb}\,|\phi,\psi\rangle_{jb} = \sum_{j,b}(U_{ij}V_{ab})(\phi_j\psi_b) = \left(\sum_j U_{ij}\phi_j\right)\left(\sum_b V_{ab}\psi_b\right)$$

と確かめられる．

また双線形性は

$$\left[\left(\sum_\mu c_\mu U^{(\mu)}\right)\otimes\left(\sum_\nu d_\nu V^{(\nu)}\right)\right]_{ia,jb} = \left(\sum_\mu c_\mu U^{(\mu)}\right)_{ij}\left(\sum_\nu d_\nu V^{(\nu)}\right)_{ab} = \left(\sum_\mu c_\mu U^{(\mu)}_{ij}\right)\left(\sum_\nu d_\nu V^{(\nu)}_{ab}\right)$$
$$= \sum_{\mu,\nu} c_\mu d_\nu U^{(\mu)}_{ij}V^{(\nu)}_{ab} = \sum_{\mu,\nu} c_\mu d_\nu [U^{(\mu)}\otimes V^{(\nu)}]_{ia,jb}$$

と確かめられる．

さらに U,V のユニタリ性がテンソル積 $U\otimes V$ に引き継がれることを示す．まず

$$\sum_{j,b}[(U\otimes V)^\dagger]_{ia,jb}[U\otimes V]_{jb,kc} = \sum_{j,b}[U\otimes V]_{jb,ia}{}^*[U\otimes V]_{jb,kc} = \sum_{j,b}(U_{ji}V_{ba})^*(U_{jk}V_{bc})$$
$$= \left(\sum_j U_{ji}{}^*U_{jk}\right)\left(\sum_b V_{ba}{}^*V_{bc}\right) = \left(\sum_j (U^\dagger)_{ij}U_{jk}\right)\left(\sum_b (V^\dagger)_{ab}V_{bc}\right) = \delta_{ik}\delta_{ac} = \delta_{ia,kc}$$

より，$(U\otimes V)^\dagger(U\otimes V) = \mathbb{I}$．同様に $(U\otimes V)(U\otimes V)^\dagger = \mathbb{I}$.

第 3 章　量子アルゴリズム

［量子アルゴリズムは量子ビット列に対する恒等式の手品のようである.］

3.1　Deutsch-Jozsa のアルゴリズム

本節で説明する **Deutsch-Jozsa のアルゴリズム**[*13]は，与えられた関数 $f : \{0,1\}^n \to \{0,1\}$ が定数関数とバランス関数のいずれかを判定する人工的な問題を対象にしており，応用的ではないものの教育的である．ここで

- 定数関数とは，全ての $x \in \{0,1\}$ に対して常に $f(x) = 0$,
  もしくは常に $f(x) = 1$ となる関数 f である．
- バランス関数とは $f(x)$ の値が，2^n 通りの $x \in \{0,1\}^n$ のちょうど半分に対して 0,
  残り半分に対して 1 である，すなわち

$$|\{x \in \{0,1\}^n | f(x) = 0\}| = 2^n/2$$

  となる関数 f である［左辺 $|\cdots|$ は集合 $\{\cdots\}$ の要素数 (2.2 節)］.

定数関数／バランス関数判定問題

入力　関数 $f : \{0,1\}^n \to \{0,1\}$

出力　f が定数関数ならば 0，バランス関数ならば 1

関数 f は質問 x に対する値 $f(x)$ を通じてのみ，その情報を得ることができるブラックボックス——**オラクル** (oracle，日本語で「神託」の意) ——として与えられているとする．オラクルに対する計算量の指標としては，**質問計算量** (query complexity) が挙げられる．これは［判定問題を解決するための］質問の回数である．

例えば入力に対して一意に出力が決定する古典計算 (決定性計算) では，どのようなアルゴリズムに対しても［上記の判定問題を］正しく判定するには，$2^{n-1}+1$ 回の質問が必要なバランス関数 f が存在することが分かる．これに対し量子計算を用いた Deutsch-Jozsa のアルゴリズムでは，たった 1 回の質問で確率 1 で正しく判定できる．

注意　量子計算では量子ビットから古典情報を測定により確率的に取り出し，一般には誤った答を出力する確率はゼロでない．しかしながら後述の Grover のアルゴリズムや Shor のアルゴリズムでは，そのような確率は十分小さい上に，これらの問題では得られた答が正しいかを容易に確認できる．

Deutsch-Jozsa のアルゴリズムを導入する準備として，状況設定を行う．まず量子回路からオラクルに質問するためには，オラクル自体が素子として量子回路に組み込まれている必要がある．そこで n-量子ビットと 1-量子ビットから成る 2 つの量子ビット列に，

$$U_f |x\rangle |b\rangle = |x\rangle |b \oplus f(x)\rangle \qquad (x \in \{0,1\}^n,\, b \in \{0,1\}) \tag{3.1}$$

のように作用する 2^{n+1} 次ユニタリ行列 U_f としてオラクルが実現しているとする．これは式 (2.11) の方法を用いてゴミ情報を残さないように実装した f を計算する量子回路と見なすことができ，U_f を 1 つ使用することがオラクルに 1 回質問することに対応する．

[*13] D. Deutsch, R, Jozsa, *Proc. of the Royal Society of London A,* **439**, 553–558 (1992).

これを踏まえて，Deutsch-Jozsa のアルゴリズムを実現する量子回路を以下に示す．ただし回路には初期量子ビット列として $|0^{n+1}\rangle = |0^n\rangle\,|0\rangle$ を入力する．

Deutsch-Jozsa のアルゴリズム

- (i) $(n+1)$ ビット目のみに Pauli 行列 σ_x を作用させる．
- (ii) $(n+1)$ ビット全体に Hadamard 変換 H を作用させる．
- (iii) $(n+1)$ ビット全体に U_f を作用させる．
- (iv) 最初の n ビットに Hadamard 変換 H を作用させる．
- (v) 最初の n ビットを基底測定で測定して得られた古典 n ビット列が $0\cdots0$ ならば 0 (定数関数) と判定，それ以外ならば 1 (バランス関数) と判定する．

この回路は U_f を，したがってオラクルへの質問を 1 回含んでいる．

このアルゴリズムがどのように機能するかを調べよう．ステップ (i)–(iii) で量子ビット列は

$$
\begin{aligned}
|0^n\rangle\,|0\rangle &\overset{(i)}{\longmapsto} |0^n\rangle\,|1\rangle \overset{(ii)}{\longmapsto} \frac{1}{\sqrt{2N}} \sum_{x\in\{0,1\}^n} |x\rangle\,(|0\rangle - |1\rangle) \qquad (2.4\text{ 節の式 (2)},\ N \equiv 2^n) \\
&\overset{(iii)}{\longmapsto} \frac{1}{\sqrt{2N}} \sum_{x\in\{0,1\}^n} |x\rangle\,(|0\oplus f(x)\rangle - |1\oplus f(x)\rangle) \\
&= \left(\frac{1}{\sqrt{N}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)}\,|x\rangle\right)\left(\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right) \qquad (3.2)
\end{aligned}
$$

と変化する．［最後の等号を本稿次節で確認する．最右辺分母の $\sqrt{2}$ はもとより $(n+1)$ ビット目の因子である．］(iii) の過程では $|x\rangle$ の振幅が $f(x)=0$ のとき変化せず，$f(x)=1$ のとき逆符号になっている (**位相キックバック**)．次いで (iv) にて再び $H^{\otimes n}$ を作用させると，最初の n-量子ビット列において

$$
H^{\otimes n}\,|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} (-1)^{\langle x,y\rangle}\,|y\rangle \qquad (3.3)
$$

と変化する［本稿次節で確認］．ここで x, y の i 番目のビット x_i, y_i に対して $\langle x,y\rangle = \sum_{i=1}^n x_i y_i \bmod 2$ を定義した．よって最初の n-量子ビット列は

$$
\frac{1}{\sqrt{N}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)}\,|x\rangle \overset{(iv)}{\longmapsto} \frac{1}{N} \sum_{x,y\in\{0,1\}^n} (-1)^{f(x)}(-1)^{\langle x,y\rangle}\,|y\rangle
$$

となる．この状態に測定 (v) を行うと，$|0^n\rangle$ を得る確率振幅は $|y\rangle = |0^n\rangle$ の係数なので，確率は

$$
\Pr(0^n) = \left|\frac{1}{N} \sum_{x\in\{0,1\}^n} (-1)^{f(x)}\right|^2 .
$$

これは f が定数関数のとき 1，バランス関数のとき 0 となることが見て取れる．よって判定方法 (v) は上手くいく．こうして初めに予告したように Deutsch-Jozsa のアルゴリズムは，定数関数／バランス関数判定問題を U_f の使用回数 1 かつ確率 1 で正しく解ける．

結果を解釈するにあたり，(iii) の後の状態 (3.2) において最後の 1-量子ビットは f に依存せず分離されているため，最初の n-量子ビット

$$
|\phi_f\rangle \equiv \frac{1}{\sqrt{N}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)}\,|x\rangle
$$

だけに着目できることに注意しよう．定数関数 f とバランス関数 g に対しては

$$\langle\phi_f|\phi_g\rangle = \frac{1}{N}\sum_{x,y}(-1)^{f(x)+g(y)}\langle x|y\rangle = \frac{1}{N}\sum_{x}(-1)^{f(x)+g(x)} = 0 \tag{3}$$

となるので［最後の等号を本稿次節で確認］，$|\phi_f\rangle$ と $|\phi_g\rangle$ は直交する．すると Deutsch-Jozsa のアルゴリズムでは与えられた関数を識別する問題を，直交する量子状態 $|\phi_f\rangle, |\phi_g\rangle$ を見分ける問題に帰着させていると言える，実際，問題を量子状態識別問題に帰着している量子アルゴリズムは数多くあり，3.3 節の Shor のアルゴリズムも量子計算を本質的に利用している部分は量子状態識別である．この観点からは以下の 2 点が重要となる．

1. 入力から直交する (あるいは直交に近い) 状態を生成する効率の良い量子回路が構成可能であること．
2. 生成された状態を識別する測定が効率の良い量子回路で構成可能であること．

3.1 節について

■式 (3.2) 最後の等号の確認　$f(x) = 0, 1$ に対して恒等式 $|0 \oplus f(x)\rangle = |f(x)\rangle, |1 \oplus f(x)\rangle = |\neg f(x)\rangle$ が直接の場合分けにより確かめられる．よって

$$\begin{aligned}|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle = |f(x)\rangle - |\neg f(x)\rangle &= \begin{cases}|0\rangle - |1\rangle & (f(x) = 0 \text{ のとき}) \\ |1\rangle - |0\rangle & (f(x) = 1 \text{ のとき})\end{cases} \\ &= (-1)^{f(x)}(|0\rangle - |1\rangle)\end{aligned}$$

とまとめられる．

■補題 (3.3) の確認　任意の $x \in \{0,1\}^n$ に対する式 (3.3) の証明は，教科書 p.70 の演習問題 13 となっている．式 (3.3) において

$$\langle x, y\rangle = \sum_{i=1}^{n} x_i y_i \mod 2$$

は (-1) の指数なので，2 の倍数を加える自由度がある．そこで右辺は 2 で割った余りとなっている．等価的にこの定義式は 2 を法とする合同式と見て良い．

$n = 1$ のとき式 (3.3) は

$$H|x\rangle = \frac{1}{\sqrt{2}}\sum_{y\in\{0,1\}}(-1)^{\langle x,y\rangle}|y\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x|1\rangle) \qquad (\because \langle x, 0\rangle \equiv 0, \langle x, 1\rangle \equiv x)$$

となる．最右辺は実際に $H|x\rangle$ の適正な表式となっている (2.4 節の図 4)．

もうしばらく式 (3.3) の含意を具体的に調べよう．$n = 2$ のときには

$$y = y_1y_2 = 00, 01, 10, 11 \quad \Rightarrow \quad \langle xy\rangle \equiv 0, x_2, x_1, x_1 + x_2 \qquad (\text{それぞれ順に})$$

なので，式 (3.3) は

$$H^{\otimes 2}|x\rangle = \frac{1}{\sqrt{2^2}}\sum_{y\in\{0,1\}^2}(-1)^{\langle x,y\rangle}|y\rangle = \frac{1}{\sqrt{2^2}}\left(|00\rangle + (-1)^{x_2}|01\rangle + (-1)^{x_1}|10\rangle + (-1)^{x_1+x_2}|11\rangle\right)$$

を与える．これは

$$H^{\otimes 2}|x\rangle = (H|x_1\rangle)(H|x_2\rangle) = \frac{1}{\sqrt{2^2}}\left(|0\rangle + (-1)^{x_1}|1\rangle\right)\left(|0\rangle + (-1)^{x_2}|1\rangle\right)$$

と比較すると，確かに成り立っていることが分かる．

ここで任意の n に対して式 (3.3) が成り立つことを，数学的帰納法にて示そう．

$$x = x_1 \cdots x_n, \qquad y = y_1 \cdots y_n, \qquad x' = x x_{n+1} = x_1 \cdots x_{n+1}, \qquad y' = y y_{n+1} = y_1 \cdots y_{n+1}$$

と書き，ある n (および $n = 1$) で式 (3.3) が成り立つと仮定すると，

$$\begin{aligned} H^{\otimes(n+1)}|x'\rangle =& (H^{\otimes n}|x\rangle)(H|x_{n+1}\rangle) = \left(\frac{1}{\sqrt{2^n}}\sum_{y\in\{0,1\}^n}(-1)^{\langle x,y\rangle}|y\rangle\right)\left(\frac{1}{\sqrt{2}}\sum_{y_{n+1}\in\{0,1\}}(-1)^{\langle x_{n+1},y_{n+1}\rangle}|y_{n+1}\rangle\right) \\ =& \left(\frac{1}{\sqrt{2^{n+1}}}\sum_{y'\in\{0,1\}^{n+1}}(-1)^{\langle x',y'\rangle}|y'\rangle\right) \qquad (\because \langle x,y\rangle + \langle x_{n+1},y_{n+1}\rangle \equiv \langle x',y'\rangle) \end{aligned}$$

を得る．よって式 (3.3) で $n \to n+1$ と置き換えた関係も成り立つので，示された．

■式 (3) 最後の等号の確認　$g(x) = 0, 1$ となる $2^n/2$ 通りずつの x をそれぞれ x', x'' で表すと，定数関数 $f(x)$ の一定値を c として

$$\sum_x (-1)^{f(x)+g(x)} = (-1)^c\left(\sum_{x'}(-1)^{g(x')} + \sum_{x''}(-1)^{g(x'')}\right) = (-1)^c 2^{n-1}(1-1) = 0.$$

3.2　Grover のアルゴリズム

関数 $f : \{0,1\}^n \to \{0,1\}$ の $f(x_0) = 1$ となる x_0 を充足解 (以下，単に解) という．本節で取り上げる **Grover のアルゴリズム**[*14]は著名かつ汎用的な量子アルゴリズムであり，解 x_0 を見つけるという一般的な探索問題に適用できる．

Grover の探索問題

入力　関数 $f : \{0,1\}^n \to \{0,1\}$，ただし $f(x_0) = 1$ となる解 $x_0 \in \{0,1\}^n$ はただ 1 つ存在する．

出力　$f(x_0) = 1$ を満たす解 $x_0 \in \{0,1\}^n$

前節と同様に関数 f はオラクルとして与えられており，式 (3.1) を満たす量子素子 U_f として実現されているとする．

再び $N \equiv 2^n$ とおくと，古典的な決定性計算［3.1 節］では任意の f に対して正しく x_0 を得るには，明らかに $(N-1)$ 回質問する必要がある．ところが Grover のアルゴリズムは f への $O(\sqrt{N})$ 回だけの質問で，確率 $1-(1/N)$ 以上 (したがって $N \gg 1$ でほぼ 1) で正しく x_0 を出力できる．

Grover のアルゴリズムのアイデアを発見的に導入しよう．まずは入力 $|0^n\rangle|0\rangle$ に対する次の量子回路を考える．

(1) 最初の n ビットの入力に Hadamard 変換 H を作用させる．

[*14] Lov K. Grover, *Proc. of the 28th ACM Symposium on Theory of Computing,* 212–218 (1996).

(2) $(n+1)$ ビット全体に U_f を作用させる．

このとき式 (2)，式 (3.1) より

$$|0^n\rangle|0\rangle \overset{(1)}{\longmapsto} \frac{1}{\sqrt{N}}\sum_{x\in\{0,1\}^n}|x\rangle|0\rangle \overset{(2)}{\longmapsto} \frac{1}{\sqrt{N}}\sum_{x\in\{0,1\}^n}|x\rangle|f(x)\rangle$$

となるので，出力状態を測定すると $(x, f(x))$ の組が完全にランダムに得られる．$(x_0, 1)$ が得られる確率振幅は $1/\sqrt{N}$，確率は $1/N$ であり，このままでは量子計算の利点は何もない．

そこで次の回路を考える．

(1) $(n+1)$ ビット目だけに Pauli 行列 σ_x を作用させる．
(2) $(n+1)$ ビットのそれぞれに Hadamard 変換 H を作用させる．
(3) $(n+1)$ ビット全体に U_f を作用させる．
(4) N 次ユニタリ行列

$$D_N = ((D_N)_{ij}), \qquad \text{対角成分 } [D_N]_{ii} = -1 + \frac{2}{N}, \qquad \text{非対角成分 } [D_N]_{ij} = \frac{2}{N} \tag{3.4}$$

［ユニタリ性を本稿次項で確認］として定義される拡散行列 D_N を最初の n ビットに作用させる．

すると

$$\begin{aligned}
|0^n\rangle|0\rangle &\overset{(1)}{\longmapsto} |0^n\rangle|1\rangle \overset{(2)}{\longmapsto} \frac{1}{\sqrt{N}}\sum_{x\in\{0,1\}^n}|x\rangle\otimes\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle) \qquad (\because \text{式 (2)})\\
&\overset{(3)}{\longmapsto} \frac{1}{\sqrt{N}}\sum_{x\in\{0,1\}^n}|x\rangle\otimes\frac{1}{\sqrt{2}}(|0\oplus f(x)\rangle-|1\oplus f(x)\rangle) \qquad (\because \text{式 (3.1)})\\
&= \frac{1}{\sqrt{N}}\sum_{x\in\{0,1\}^n}(-1)^{f(x)}|x\rangle\otimes\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle) \qquad (\text{式 (3.2) と同様})\\
&= \frac{1}{\sqrt{N}}\left(-|x_0\rangle+\sum_{x\neq x_0}|x\rangle\right)\otimes\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\\
&\overset{(4)}{\longmapsto} \left(\frac{3-(4/N)}{\sqrt{N}}|x_0\rangle+\sum_{x\neq x_0}\frac{1-(4/N)}{\sqrt{N}}|x\rangle\right)\otimes\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)
\end{aligned} \tag{4}$$

となる［最後の変形 (4) を本稿次項で確認］．

ステップ (3) で $f(x)=1$ を満たす $|x\rangle$ の位相がキックバックされており，さらに拡散行列 D_N を作用させて得られる最終的な状態では，測定により x_0 が得られる確率は $(3-(4/N)^2)/N$ となっていることが見て取れる．したがって我々は依然として U_f を 1 つしか用いていないにも関わらず，成功確率は先ほどの $1/N$ と比べて 9 倍程度上昇していることになる．この結果の解釈は次項で行う．

いずれにせよ Grover のアルゴリズムは以下のように，この成功確率を増幅させる回路を繰り返すことで構成される．ただし初期量子ビット列は $|0^n\rangle|1\rangle$ とし［上記のステップ (1) 後に対応］，また θ を $\sin\theta = \sqrt{1/N}$ で定義する．［$0 \le \theta \le \pi/2$ であることを 3.2.1 項で暗に用いる．3.2.2 項の θ_t も同様.］

Grover のアルゴリズム

(i)　$(n+1)$ ビット全体に Hadamard 変換 H を作用させる．

(ii)　ステップ (iii) と (iv) を $\lfloor \pi/(4\theta) \rfloor$ 回繰り返す.

(iii)　$(n+1)$ ビット全体に U_f を作用させる.

(iv)　最初の n ビットに拡散行列 D_N を作用させる.

(v)　最初の n ビットを計算基底で測定して得られた古典 n ビット列を出力する.

$\sin\theta \leq \theta$ より U_f の使用回数は $\lfloor \pi/(4\theta) \rfloor \leq \lfloor (\pi/4)\sqrt{N} \rfloor$ である. また成功確率について次の定理が成り立つ (証明は次項).

定理　Grover のアルゴリズムは U_f の使用回数 $\lfloor (\pi/4)\sqrt{N} \rfloor$ で, $f(x_0) = 0$ を満たす x_0 を確率

$$1 - \frac{1}{N} \tag{5}$$

以上で正しく出力する.

3.2 節の冒頭 (3.2.1 項の直前まで) について

■拡散行列 (3.4) のユニタリ性の確認　${D_N}^\dagger = D_N$ であり, そこで

$$({D_N}^2)_{ij} = \sum_k (D_N)_{ik}(D_N)_{kj}$$

における和を $k = i, j$ とそれ以外の項に分けると

$$i \neq j \text{ のとき} \quad ({D_N}^2)_{ij} = (N-2)\left(\frac{2}{N}\right)^2 + 2 \cdot \frac{2}{N}\left(-1 + \frac{2}{N}\right) = 0,$$
$$i = j \text{ のとき} \quad (D_N)_{ii} = (N-1)\left(\frac{2}{N}\right)^2 + \left(-1 + \frac{2}{N}\right)^2 = 1$$

となるので, D_N はユニタリ行列である.

等価的に D_N の任意の 2 つの行 (または列) の内積をとって, D_N は各行 (または各列) が正規直交系を成す直交行列であることを確かめても良い. ところが内積の成分計算は上式と全く同じである.

■式 (4) 最後における D_N の作用の確認　$|x\rangle$ のベクトル表現

$$(\langle 000\cdots|x\rangle, \langle 010\cdots|x\rangle, \cdots, \langle 111\cdots|x\rangle)^T$$

はビット列 $x \in \{0,1\}^n$ に対応する成分が 1, その他の成分がゼロであるような $N = 2^n$ 次元の基底ベクトルである. 特にベクトル $|x_0\rangle$ は i_0 番目にゼロでない成分 1 を持つとする. すると

$$|v\rangle = -|x_0\rangle + \sum_{x(\neq x_0)} |x\rangle$$

は第 i_0 成分が -1, その他の成分が 1 のベクトルである. よって

$$\begin{aligned}(D_N|v\rangle)_i &= \sum_j (D_N)_{ij}|v\rangle_j = \left(-1 + \frac{2}{N}\right)|v\rangle_i + \sum_{j(\neq i)} \frac{2}{N}|v\rangle_j \\ &= \begin{cases} \left(-1 + \frac{2}{N}\right)(-1) + (N-1)\frac{2}{N}\cdot 1 = 3 - \frac{4}{N} & (i = i_0 \text{のとき}) \\ \left(-1 + \frac{2}{N}\right)\cdot 1 + \frac{2}{N}(-1) + (N-2)\frac{2}{N}\cdot 1 = 1 - \frac{4}{N} & (i \neq i_0 \text{のとき}) \end{cases}\end{aligned}$$

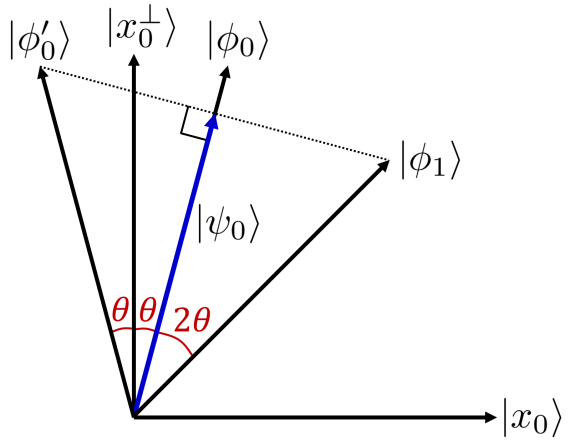


図 10　Grover のアルゴリズムの幾何学的解釈

であり，これらは $D_N|v\rangle$ の基底 $|x_0\rangle, |x \neq x_0\rangle$ に関する展開係数なので，

$$D_N|v\rangle = \left(3 - \frac{4}{N}\right)|x_0\rangle + \sum_{x(\neq x_0)} \left(1 - \frac{4}{N}\right)|x\rangle$$

が成り立つ．

3.2.1　アルゴリズムの解析

ステップ (iii) と (iv) の繰り返しにおいて最初の n-量子ビット列は分離可能であり，それは 2 つの直交する単位ベクトル

$$|x_0\rangle \text{（「解」の基底）}, \qquad |x_0^\perp\rangle \equiv \frac{1}{\sqrt{N-1}} \sum_{x \neq x_0} |x\rangle \text{（「非解」の基底）}$$

で張られる 2 次元部分線形空間上の，したがって 1-量子ビット上の操作として解釈できる (**量子ビット化**)．我々の目標はなるべく $|x_0\rangle$ に近い n-量子ビット系の状態を得ることである．

この観点から繰り返し部分の 1 回目を再考しよう．Hadamard 変換の作用 (i) の下で n-量子ビット部分は

$$|\phi_0\rangle = H^{\otimes n}|0^n\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle = \frac{1}{\sqrt{N}}|x_0\rangle + \sqrt{\frac{N-1}{N}}|x_0^\perp\rangle \tag{6}$$

となる．［式 (4) を見よ．上式 (6) 最右辺より $|\phi_0\rangle$ もまた単にベクトルである ($H^{\otimes n}$ のユニタリ性から期待されるように)．］次いで U_f の作用の下で n-量子ビットは，$|x_0\rangle$ の符号だけが反転した

$$|\phi_0'\rangle = -\frac{1}{\sqrt{N}}|x_0\rangle + \sqrt{\frac{N-1}{N}}|x_0^\perp\rangle$$

になる［再び式 (4) を見よ］．これは変換 $V_f = \mathbb{I} - 2|x_0\rangle\langle x_0|$ を用いて $|\phi_0'\rangle = V_f|\phi_0\rangle$ と書ける．幾何学的には変換 V_f は図 10 のような，$|x_0^\perp\rangle$ を軸とする鏡映である．

さらに拡散行列 D_N の作用 (iv) も幾何学的に解釈するために，

$$D_N = H^{\otimes n}(-\mathbb{I} + 2|0^n\rangle\langle 0^n|)H^{\otimes n} = -\mathbb{I} + 2H^{\otimes n}|0^n\rangle\langle 0^n|H^{\otimes n} = \qquad -\mathbb{I} + 2|\phi_0\rangle\langle\phi_0|$$

と書けることに注意する．ただし第 2 の等号は H がユニタリかつ Hermite なので，自分自身を逆行列に持つことによる．［1 行目の表式は 3.2.3 項で用いる．］

上式最右辺の確認 (教科書 p.77 の演習問題 14)　$|x\rangle$ はある成分 (i_x 番目とする) のみがゼロでない成分 1 を持つ基底ベクトルである．また第 i 成分にゼロでない成分 1 を持つ基底ベクトルを $|i\rangle$ で表す．すると上式右辺の行列要素は

$$\langle i|(-\mathbb{I}+2\,|\phi_0\rangle\,\langle\phi_0|)|j\rangle = -\,\langle i|j\rangle + \frac{2}{N}\sum_{x,y}\langle i|x\rangle\,\langle y|j\rangle = -\delta_{ij} + \frac{2}{N}\sum_{x,y}\delta_{ii_x}\delta_{i_yj} = -\delta_{ij} + \frac{2}{N}$$

となる．ただし最後の等号では $i_x = i$ かつ $i_y = j$ となるただ 1 つの項のみが和に寄与することに注意した．これは拡散行列 (3.4) の行列要素に一致している．

よって n-量子ビットの状態は

$$|\phi_1\rangle = D_N\,|\phi_0'\rangle = (-\mathbb{I}+2\,|\phi_0\rangle\,\langle\phi_0|)\,|\phi_0'\rangle = -\,|\phi_0'\rangle + 2\,|\phi_0\rangle\,\langle\phi_0|\phi_0'\rangle$$

になる．これは図 10 のように，$|\phi_0\rangle$ を軸として $|\phi_0'\rangle$ と線対称な位置にある．実際，図 10 に示した $|\phi_0'\rangle$ の［方向単位ベクトル］$|\phi_0\rangle$ への正射影ベクトルは $|\psi_0\rangle = |\phi_0\rangle\,\langle\phi_0|\phi_0'\rangle$ であり，したがって $|\phi_0'\rangle$ の軸 $|\phi_0\rangle$ に関する鏡映は

$$|\phi_0'\rangle + 2(|\psi_0\rangle - |\phi_0'\rangle) = -\,|\phi_0'\rangle + 2\,|\phi_0\rangle\,\langle\phi_0|\phi_0'\rangle$$

と表される．ところで $\sin\theta = 1/\sqrt{N}, \therefore \cos\theta = \sqrt{(N-1)/N}$ に注意すると，ベクトル (6) は

$$|\phi_0\rangle = \sin\theta\,|x_0\rangle + \cos\theta\,|x_0^\perp\rangle \tag{7}$$

と書ける．すなわち我々の定義した θ は $|\phi_0\rangle$ と $|x_0^\perp\rangle$ の成す角という意味を持つ．このとき変換後のベクトル $|\phi_1\rangle$ が $|x_0^\perp\rangle$ と成す角は図 10 のように，もとの $|\phi_0\rangle$ と比べて 2θ だけ増加し，解の基底 $|x_0\rangle$ に近づく．

さて，(iii) と (iv) の繰り返し部分を k 回適用した後の n-量子ビット列の状態は

$$|\phi_k\rangle = \alpha_k\,|x_0\rangle + \beta_k\,|x_0^\perp\rangle \tag{8}$$

と表せる．この状態に対しても U_f の作用 (iii) は軸 $|x_0^\perp\rangle$ に関する鏡映 V_f となる［本稿次項で確認］．さらに拡散行列 D_N の作用 (iv) は再び $|\phi_0\rangle$ を軸としてベクトルを鏡映する．すると操作を繰り返すたびに状態は $|x_0\rangle$ に近づいてゆくことが，幾何学的に期待される．実際，操作の繰り返しごとに $|\phi_k\rangle$ の $|x_0^\perp\rangle$ との成す角は 2θ ずつ増えてゆく，すなわち上式 (8) の展開係数は

$$\alpha_k = \sin((2k+1)\theta), \qquad \beta_k = \cos((2k+1)\theta) \tag{9}$$

と表される．

補題 (9) の証明　数学的帰納法にて証明する．教科書の計算をいくらか捕捉しつつまとめる．まず $k=0$ のとき，式 (7) より上式 (9) は成り立っている．

次にある $k \geq 0$ (および $k=0$) で式 (9) が成り立つと仮定する．

$$|\phi_0\rangle = \alpha_0\,|x_0\rangle + \beta_0\,|x_0^\perp\rangle\,, \quad \therefore D_N = -\mathbb{I}+2\,|\phi_0\rangle\,\langle\phi_0| = -\mathbb{I}+\{{\alpha_0}^2\,|x_0\rangle\,\langle x_0| + \alpha_0\beta_0(|x_0\rangle\,\langle x_0^\perp| + |x_0^\perp\rangle\,\langle x_0|) + {\beta_0}^2\,|x_0^\perp\rangle\,\langle x_0^\perp|\}$$

であり，これを $|\phi_k'\rangle = V_f\,|\phi_k\rangle = -\alpha_k\,|x_0\rangle + \beta_k\,|x_0^\perp\rangle$ に作用させると，

$$\begin{aligned}|\phi_{k+1}\rangle = D_N\,|\phi_k'\rangle &= -\,(-\alpha_k\,|x_0\rangle + \beta_k\,|x_0^\perp\rangle) + 2(-\alpha_k{\alpha_0}^2\,|x_0\rangle - \alpha_k\alpha_0\beta_0\,|x_0^\perp\rangle + \beta_k\alpha_0\beta_0\,|x_0\rangle + \beta_k{\beta_0}^2\,|x_0^\perp\rangle) \\ &= (\alpha_k(1-2{\alpha_0}^2) + 2\beta_k\alpha_0\beta_0)\,|x_0\rangle + (\beta_k(-1+2{\beta_0}^2) - 2\alpha_k\alpha_0\beta_0)\,|x_0^\perp\rangle\end{aligned}$$

が得られる．ここで仮定を用いると

$$1-2{\alpha_0}^2 = 1-2\sin^2\theta = \cos 2\theta, \quad -1+2{\beta_0}^2 = -1+2\sin^2\theta = \cos 2\theta, \quad 2\alpha_0\beta_0 = 2\sin\theta\cos\theta = \sin 2\theta$$

であり，加法定理とより

$$\alpha_{k+1} \equiv (|x_0\rangle \text{の係数}) = \sin(2((k+1)+1)\theta), \qquad \beta_{k+1} \equiv (|x_0^\perp\rangle \text{の係数}) = \cos(2((k+1)+1)\theta)$$

とまとめられる．よって式 (9) で $k \to k+1$ と置き換えた関係も成り立つので，示された．

$|\phi_k\rangle$ と $|x_0^\perp\rangle$ の成す角が 2θ ずつ増えていくのであれば，$|\phi_k\rangle$ がある程度 $|x_0\rangle$ に近づいたところで繰り返しの操作を打ち切るのが理想的である．実際，成功確率 $\sin^2((2k+1)\theta)$ は k が大きすぎると，かえって低くなってしまう．そこで繰り返しの回数 (したがって U_f の使用回数) を $k = \lfloor \pi/(4\theta) \rfloor$ とすると，成功確率は式 (5) の定理で与えられる．

証明　$\pi/(4\theta)$ の小数部分 δ を用いて $k = \lfloor \pi/(4\theta) \rfloor = \pi/(4\theta) - \delta$ と表すと，

$$\cos^2((2k+1)\theta) = \cos^2\left(\frac{\pi}{2} + (-2\delta+1)\theta\right) = \sin^2((-2\delta+1)\theta) \leq \sin^2\theta = \frac{1}{N}.$$

ただし第 3 の (不) 等号では小数部分が $0 \leq \delta < 1$ ［なので $-1 < -2\delta + 1 \leq 1$］であることに注意した．よって成功確率は $\sin^2((2k+1)\theta) = 1 - \cos^2((2k+1)\theta) \geq 1 - (1/N)$ である．

［粗く言うと $\lfloor \pi/(4\theta) \rfloor$ は時計回りに $\pi/2$ だけ回転するときの，角度 2θ ずつの回転の回数である．］

3.2.1 項について

■U_f の作用が常に鏡映 $|\phi'_k\rangle = V_f|\phi_k\rangle$ であることの確認　k 回の繰り返し操作後の状態 (8) に対して，全体系の状態は

$$|\phi_k\rangle \otimes \left(\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right) = \frac{1}{\sqrt{2}}\left\{\alpha_k(|x_0\rangle|0\rangle - |x_0\rangle|1\rangle) + \sum_{x\neq x_0}\frac{\beta_k}{\sqrt{N-1}}(|x\rangle|0\rangle - |x\rangle|1\rangle)\right\}$$

である．これに対して式 (4) ないし式 (3.2) と同様の計算を繰り返すと，U_f を作用させた状態は

$$\begin{aligned}
&\frac{1}{\sqrt{2}}\left\{\alpha_k(|x_0\rangle|0\rangle - |x_0\rangle|1\rangle) + \sum_{x\neq x_0}\frac{\beta_k}{\sqrt{N-1}}(|x\rangle|0\rangle - |x\rangle|1\rangle)\right\}\\
=&\frac{1}{\sqrt{2}}\left\{\alpha_k|x_0\rangle(|0\oplus f(x_0)\rangle - |1\oplus f(x_0)\rangle) + \sum_{x\neq x_0}\frac{\beta_k}{\sqrt{N-1}}|x\rangle(|0\oplus f(x)\rangle - |1\oplus f(x)\rangle)\right\}\\
=&\frac{1}{\sqrt{2}}\left\{\alpha_k|x_0\rangle(-1)^{f(x_0)}(|0\rangle - |1\rangle) + \sum_{x\neq x_0}\frac{\beta_k}{\sqrt{N-1}}|x\rangle(-1)^{f(x)}(|0\rangle - |1\rangle)\right\}\\
=&(-\alpha_k|x_0\rangle + \beta_k|x_0^\perp\rangle)\otimes\left(\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right)
\end{aligned}$$

と求まる．n-量子ビット列の部分は，$|x_0\rangle$ の項だけ符号が反転した状態

$$|\phi'_k\rangle = -\alpha_k|x_0\rangle + \beta_k|x_0^\perp\rangle = V_f|\phi_k\rangle$$

に置き換わっていることが見て取れる．

3.2.2　一般化：解が複数ある場合

より一般に $f(x_0) = 1$ を満たす，ブラックボックス関数 $f : \{0,1\}^n \to \{0,1\}$ の解 x_0 が複数 (t 個とする) ある場合に，そのうちの 1 つ (いずれでも良い) を見つける問題を考える．

$N = 2^n$ 個の x からランダムに選んだ 1 つの x が解である確率は t/N なので，k 個の x を一様かつ独立に選んだときに解が 1 つも含まれない確率は

$$\left(1 - \frac{t}{N}\right)^k \leq 1 - k\frac{t}{N} + \frac{k(k-1)}{2}\left(\frac{t}{N}\right)^2$$

である．［興味のある $t/N \ll 1$ の場合には右辺に対する 3 次の補正項が負なので，上式が成り立つと期待される．］そこで $k = N/t$ とおくと［(上式右辺) $= \frac{1}{2}\left(\frac{t}{N}\right) \leq \frac{1}{2}$ より］，解を選ぶ確率は 1/2 以上となる．したがって古典計算の場合では N/t 回程度の質問で答が定数確率で得られる．

他方で (iii) と (iv) の繰り返し回数が k の Grover のアルゴリズムを適用すれば，パラメータ θ の代わりに $\sin\theta_t = \sqrt{t/N}$ で決まる θ_t を定義すると，解 x_0 の 1 つを得る確率は

$$\sin^2((2k+1)\theta_t) \tag{10}$$

となる［本稿次項で確認］．ここから前項と同様に考えると，直ちに次の定理が得られる．

定理　繰り返し回数 (したがって U_f の使用回数) $R_t \equiv \lfloor \pi/(4\theta_t) \rfloor = O(\sqrt{N/t})$ の Grover のアルゴリズムは，t 個の解 x_0 のうちの 1 つを確率 $1-(t/N)$ で得ることができる．

解が複数の場合にもやはり，繰り返し回数が多すぎると成功確率 (10) はかえって低くなってしまうことが分かる．適切な回数 R_t は解の個数 t に応じて決めねばならない．

ところが解の個数 t は必ずしも，あらかじめ分かっているとは限らない．そこで t が既知でない場合には，繰り返し回数 $r = 1, 2, 4, 8, \cdots$ の Grover のアルゴリズムを順次実行するという改良を考える．すると，いずれ適正な R_t に近い繰り返し回数に達し，このとき定数確率で解が得られる．U_f の使用回数も含め，具体的には次の定理が成り立つ．

定理　解の数 t が未知の場合の Grover のアルゴリズムは，U_f の使用回数 $2\sqrt{N/t}$ 以下で (したがって R_t の 2 倍程度で)，解のうちの 1 つを確率 1/2 以上で見つけることができる．［もっともオーダーの評価としては，回数の数係数 2 は重要でない．］

証明　l を $\pi/(8\theta_t) \leq 2^l \leq \pi/(4\theta_t)$ を満たす値とすると，繰り返し回数 $r = 2^l$ の Grover のアルゴリズムで解が見つかる確率は式 (10) より，

$$\sin^2((2\cdot 2^l+1)\theta_t) \geq \sin^2\left(\frac{\pi}{4}+\theta_t\right) = 1-\cos^2\left(\frac{\pi}{4}+\theta_t\right).$$

ここで

$$\cos^2\left(\frac{\pi}{4}+\theta_t\right) = \frac{1}{2}\left\{1+\cos 2\left(\frac{\pi}{4}+\theta_t\right)\right\} = \frac{1}{2}(1-\sin 2\theta_t) \leq \frac{1}{2}$$

なので，解を得る確率は 1/2 以上である．また繰り返し回数 $r = 2^l$ のアルゴリズムで解を見つけるまでの U_f の使用回数は

$$1+2+4+8+\cdots+2^l = 2^{l+1}-1 < 2^{l+1} \leq \frac{\pi}{2\theta_t} \leq \frac{\pi}{2\sin\theta_t} = \frac{\pi}{2}\sqrt{\frac{N}{t}} < 2\sqrt{\frac{N}{t}}.$$

参考：教科書 p.81 の演習問題 16　関数 $f(x)$ が $f(x_0)=1$ となる解 x_0 を 1 つだけ持つか，あるいは $f(x)=0$ の定数関数である場合を考える．前者の場合，Grover のアルゴリズムを用いれば質問回数 $O(\sqrt{N})$ で解が高確率で得られる．そこで実際に解が得られれば，確率 1 で f は前者の (非自明な) 関数と判定できる．他方で質問回数 $O(\sqrt{N})$ の時点で解が見つからなければ，f は高確率で後者の定数関数と判定できる．

3.2.2 項について

■補題 (10) の証明　教科書 p.79 の演習問題 15 となっており，3.2.1 項の議論を直接拡張すれば良い．まず正規直交基底を

$$|x_0\rangle = \frac{1}{\sqrt{t}}\sum_{\text{解 } x}|x\rangle, \qquad |x_0^\perp\rangle = \frac{1}{\sqrt{N-t}}\sum_{\text{非解 } x}|x\rangle$$

で再定義すると，Hadamard 変換の作用 (i) の下で n-量子ビットの状態は

$$|\phi_0\rangle \equiv \frac{1}{\sqrt{N}} \sum_x |x\rangle = \sqrt{\frac{t}{N}}\,|x_0\rangle + \sqrt{\frac{N-t}{N}}\,|x_0^\perp\rangle = \sin\theta_t\,|x_0\rangle + \cos\theta_t\,|x_0^\perp\rangle$$

になる (よって θ_t は $|x_0^\perp\rangle$ との成す角)．次に (iii) と (iv) を k 回だけ繰り返した後の状態を

$$|\phi_k\rangle = \alpha_k\,|x_0\rangle + \beta_k\,|x_0^\perp\rangle$$

とおくと前項と同様にして，U_f の作用 (iii) により状態は

$$|\phi_k\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \stackrel{(iii)}{\longmapsto} |\phi_k'\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

と変化することが確かめられる．ここに

$$|\phi_k'\rangle \equiv -\alpha_k\,|x_0\rangle + \beta_k\,|x_0^\perp\rangle$$

は再び，$|\phi_k\rangle$ を軸 $|x_0^\perp\rangle$ に関して線対称に折り返したベクトルである．また表式 $|\phi_0\rangle = \frac{1}{\sqrt{N}}\sum_x |x\rangle$ に，したがって $D_N = -\mathbb{I} + 2\,|\phi_0\rangle\langle\phi_0|$ と書けることに変わりはないので，拡散行列の作用 (iv) は依然として $|\phi_0\rangle$ に関する鏡映と解釈できる．よって幾何学的解釈から，k 回の操作を繰り返した後の状態は $|\phi_0\rangle$ を角度 $2\theta_t \times k$ だけ時計回りに回転したベクトル

$$|\phi_k\rangle = \sin((2k+1)\theta_t)\,|x_0\rangle + \cos((2k+1)\theta_t)\,|x_0^\perp\rangle$$

になる．改めて $|x_0\rangle = \frac{1}{\sqrt{t}}\sum_{\text{解 }x} |x\rangle$ に注意すると，この状態において特定の解 x を得る確率は

$$\frac{1}{t}\sin^2((2k+1)\theta_t).$$

t 個の解のいずれかを得る確率は，その t 倍 (10) で与えられる．$t = 1$ とおくと，前項の議論が再現される．

3.2.3 振幅増幅法

Grover のアルゴリズムをさらに一般化した量子アルゴリズムとして，**振幅増幅法** (amplitude amplification)[*15]を紹介する．

何らかの探索問題の正解を小さな成功確率 p で見つけられる，乱択アルゴリズム A を考える．ここで乱択計算とは「0 と 1 が等確率で現れる一様ランダムなビットの列を利用する古典計算であり，入力と利用したランダムビット列によって出力が決定する計算」(p.68) である．また乱択アルゴリズム A を実行して得られる解候補 s の，正解 $(B(s) = 1)$ と不正解 $(B(s) = 0)$ を効率的に判定できる決定性アルゴリズム B があるとする．例えば与えられた合成数 N の約数を探索する問題に対しては，N を解候補 s で割り切れるかを確認するアルゴリズム B を採れば良い．A で得た解候補の正しさを B で検証する作業を k 回繰り返したとき，一度も正解が得られない確率は $(1-p)^k$ なので，［前項の冒頭と同様に］正解を (p に依らない) 定数確率で得るには回数 $k = O(1/p)$ 程度の繰り返しが必要である．ところが振幅増幅法を用いると，この繰り返し回数は $O(1/\sqrt{p})$ で済む．

[*15] G. Brassard, P. Hϕyer, M. Mosca, A. Tapp, in *Quantum Computation and Information, Contemporary Mathematics,* **305**, 53–74, S. J. Lomonaco, Jr., H. E. Brandt ed., AMS (2002).

解候補を表すビット列の長さを n，A が計算に利用する補助ビット列の長さを m とすると，A, B はそれぞれユニタリ変換

$$U_A \left|0^n\right\rangle \left|0^m\right\rangle = \sum_{\substack{s\in\{0,1\}^n \\ a\in\{0,1\}^m}} \gamma_{s,a} \left|s\right\rangle \left|a\right\rangle, \qquad U_B \left|s\right\rangle = (-1)^{B(s)} \left|s\right\rangle$$

として実現できる．ここに

$$\text{確率の規格化} \ \sum_{s,a} |\gamma_{s,a}|^2 = 1, \qquad \text{成功確率} \ \sum_{s:B(s)=1,a} |\gamma_{s,a}|^2 = p.$$

また U_B の作用は正解と不正解に応じた位相キックバックであり，補助ビット列は分離できるので省略した．

ここで Grover のアルゴリズムとの対応を考える．最初に Hadamard 変換で全ての解候補の重合せ $H^{\otimes n}\left|0^n\right\rangle = \frac{1}{\sqrt{N}} \sum_x \left|x\right\rangle$ を生成することは，解候補を一様ランダムに選ぶことに対応する．次いで Grover のアルゴリズムは

$$\begin{aligned} &\text{軸 } \left|x_0^\perp\right\rangle \text{に関する折り返し} \qquad V_f = \mathbb{I} - 2\left|x_0\right\rangle\left\langle x_0\right|, \\ &\text{軸 } \left|\phi_0\right\rangle = H^{\otimes n}\left|0^n\right\rangle \text{に関する折り返し} \qquad D_N = -\mathbb{I} + 2H^{\otimes n}\left|0^n\right\rangle\left\langle 0^n\right| H^{\otimes n} \end{aligned}$$

を適当な回数 k だけ繰り返した状態

$$\{(-\mathbb{I} + 2H^{\otimes n}\left|0^n\right\rangle\left\langle 0^n\right| H^{\otimes n})(\mathbb{I} - 2\left|x_0\right\rangle\left\langle x_0\right|)\}^k H^{\otimes n}\left|0^n\right\rangle$$

を生成して，正解 $\left|x_0\right\rangle$ の振幅を増幅していた．そこで

$$\begin{aligned} &\text{正解の振幅の符号反転 } V_f \quad \to \quad U_B, \\ &\left|\phi_0\right\rangle = H^{\otimes n}\left|0^n\right\rangle \text{に関する折り返し} \quad \to \quad \left|\phi_0\right\rangle \equiv U_A\left|0^n, 0^m\right\rangle \text{に関する折り返し} \end{aligned}$$

と一般化できる．このときアルゴリズムにより正解の振幅の増幅した状態は

$$\left|\phi_k\right\rangle \equiv \{(-\mathbb{I} + 2U_A\left|0^n, 0^m\right\rangle\left\langle 0^n, 0^m\right| U_A^\dagger) U_B \otimes \mathbb{I}\}^k U_A\left|0^n, 0^m\right\rangle \tag{11}$$

と書ける．また $\left|x_0\right\rangle, \left|x_0^\perp\right\rangle$ に対応する 2 つの直交する状態

$$\begin{aligned} \left|\phi_{\text{good}}\right\rangle &\equiv \left(\sum_{s:B(s)=1,a} |\gamma_{s,a}|^2\right)^{-1/2} \sum_{s:B(s)=1,a} \gamma_{s,a}\left|s\right\rangle\left|a\right\rangle, \\ \left|\phi_{\text{bad}}\right\rangle &\equiv \left(\sum_{s:B(s)=0,a} |\gamma_{s,a}|^2\right)^{-1/2} \sum_{s:B(s)=0,a} \gamma_{s,a}\left|s\right\rangle\left|a\right\rangle \end{aligned}$$

を導入して

$$\left|\phi_k\right\rangle = \alpha_k\left|\phi_{\text{good}}\right\rangle + \beta_k\left|\phi_{\text{bad}}\right\rangle \qquad (\text{ただし } |\alpha_0|^2 = p,\ |\beta_0|^2 = 1-p)$$

と書く．すると Grover のアルゴリズムの解析の一般化により，$\sin\theta = \sqrt{p}$ なる θ に対して

$$|\alpha_k|^2 = \sin^2((2k+1)\theta), \qquad |\beta_k|^2 = \cos^2((2k+1)\theta)$$

であり，したがって繰り返し回数 $k = O(1/\sqrt{p})$ で成功確率が定数以上になることが分かる．

最後に U_A, U_B が効率的な量子回路であれば，上式 (11) における繰り返し変換，とりわけ $U_A\left|0^n, 0^m\right\rangle$ に関する折り返し

$$-\mathbb{I} + 2U_A\left|0^n, 0^m\right\rangle\left\langle 0^n, 0^m\right| U_A^\dagger = U_A(-\mathbb{I} + 2\left|0^n, 0^m\right\rangle\left\langle 0^n, 0^m\right|) U_A^\dagger$$

も効率的な量子回路として実現可能であることを証明する．まず右辺において $U_A^\dagger$ は，U_A の入出力を入れ替えた量子回路で実現できる．また変換 $(-\mathbb{I}+2\left|0^n,0^m\right\rangle\left\langle 0^n,0^m\right|)$ は入力が $\left|0^n,0^m\right\rangle$ のときには何もせず，それ以外のときに振幅の符号を反転する回路である．これを実現するには Pauli 行列 σ_x と式 (2.8) の GCNOT を用いて，

$$(\sigma_x^{\otimes n+m+1})\mathrm{GCNOT}(\sigma_x^{\otimes n+m}\otimes\mathbb{I})$$

を構成するところから始める良い．

note　実際，この量子回路で状態は

$$\begin{aligned}\left|0^n,0^m\right\rangle\otimes\left|x=0,1\right\rangle &\xmapsto{\sigma_x^{\otimes n+m}\otimes\mathbb{I}}\left|1^n,1^m\right\rangle\otimes\left|x=0,1\right\rangle\xmapsto{\mathrm{GCNOT}}\left|1^n,1^m\right\rangle\otimes\left|x=1,0\right\rangle\\ &\xmapsto{\sigma_x^{\otimes n+m+1}}\left|0^n,0^m\right\rangle\otimes\left|x=0,1\right\rangle,\\ \left|\ \text{その他}\ \right\rangle\otimes\left|x=0,1\right\rangle &\xmapsto{\sigma_x^{\otimes n+m}\otimes\mathbb{I}}\left|\neg^{\otimes n}(\text{その他})\right\rangle\otimes\left|x=0,1\right\rangle\xmapsto{\mathrm{GCNOT}}\left|\neg^{\otimes n}(\text{その他})\right\rangle\otimes\left|x=0,1\right\rangle\\ &\xmapsto{\sigma_x^{\otimes n+m+1}}\left|\ \text{その他}\ \right\rangle\otimes\left|x=1,0\right\rangle\end{aligned}$$

と変化し，$(n+m)$ 量子ビットが $\left|0^n,0^m\right\rangle$ か否かは $(n+m+1)$ ビット目の変化の有無に反映される．そこで，これに応じて

$(n+m+1)$ ビット目に位相キックバックを適用すれば，量子回路 $(-\mathbb{I}+2\left|0^n,0^m\right\rangle\left\langle 0^n,0^m\right|)$ を効率的に実現できる．

3.3　Shor のアルゴリズム

現実にインターネット上などで広く利用されている暗号プロトコルが依拠している，素因数分解問題および離散対数問題を，**Shor のアルゴリズム**[*16]は非常に少ない計算量で解くことが可能である．このため現在の古典計算機と同程度の規模の計算が可能な現実的な量子計算機が実現した場合，これらの暗号プロトコルは簡単に破られてしまう．

3.3.1　周期発見問題に対する量子アルゴリズム

Shor のアルゴリズムの中心的なアイデアは，以下の**周期発見問題** (period-finding problem) を解く量子アルゴリズムに集約される．$N\in\mathbb{N}$ に対して $\mathbb{Z}_N\equiv\{0,\cdots,N-1\}$ を定義する．

周期発見問題

入力　$\mathbb{Z}_N$ 上の関数 f，ただし $N\in\mathbb{N}$ はある $s\in\mathbb{N}$ で割り切れ，

$$f(a)=f(a+s\bmod N)=f(a+2s\bmod N)=f(a+3s\bmod N)=\cdots$$

を満たし，$f(a),\cdots,f(a+s-1\bmod N)$ は全て異なる値をとる．

出力　f に隠されている周期 s

note　$a\bmod N$ は a を N で割った余りを表す．例えば $N=16,s=4$ とすると上の条件は

$$\begin{aligned}&f(0)=f(4)=f(8)=f(12),\qquad f(1)=f(5)=f(9)=f(13),\\ &f(2)=f(6)=f(10)=f(14),\qquad f(3)=f(7)=f(11)=f(15)\end{aligned}$$

[*16] P. W. Shor, *SIAM Journal on Computing,* **26**, 1484–1509 (1997).

を意味するので，$f(x)$ は数列として $\{f(0), f(1), f(2), f(3)\}$ を繰り返す．しかも $f(0), \cdots, f(3)$ の値は相異なるから，$f(x)$ は周期 $s = 4$ の周期関数である．

例えば $f(0), f(1), f(2), \cdots$ を順に計算し，$f(0) = f(s)$ を満たす s として周期を見つけることができる．しかしこの単純な古典アルゴリズムでは，最悪 $N/2$ 回程度 f を計算する必要がある．この回数は N の二進数での表現長 $n \equiv \lceil \log N \rceil$ の指数である．

note　二進数表記で n 桁の数 N は

$$\underbrace{10\cdots0}_{n\text{ 桁}}(2) = 2^{n-1} \le N \le \underbrace{11\cdots1}_{n\text{ 桁}}(2) = 2^n - 1 < 2^n, \tag{12}$$
$$\therefore n - 1 \le N < n, \qquad \therefore \log N < n \le \log N + 1$$

を満たすので，$n = \lceil \log N \rceil$ と表せる．

そこで n の多項式程度の回数で s を求める量子アルゴリズムを考える．我々は 2 つの量子ビット列を用い，ここでは古典ビット列を

$$|01\rangle \ \to\ |1\rangle\,, \qquad |11\rangle \ \to\ |3\rangle$$

のように二進数と見て自然数で表す．

周期発見量子アルゴリズム

(i)　1 つ目の量子ビット列に以下の同じ振幅の重合せ状態を生成する．

$$\frac{1}{\sqrt{N}} \sum_{a \in \mathbb{Z}_N} |a\rangle\,|0\rangle\,.$$

(ii)　1 つ目の量子ビット列を入力とした f の出力を 2 つ目の量子ビット列に書き込む．

$$\frac{1}{\sqrt{N}} \sum_{a \in \mathbb{Z}_N} |a\rangle\,|f(a)\rangle\,.$$

(iii)　2 つ目の量子ビット列を計算基底で測定する．測定値 z が得られたとすると，量子メモリの状態は

$$\frac{1}{\sqrt{N/s}} \sum_{a:f(a)=z} |a\rangle\,|z\rangle \tag{13}$$

となる (和は $f(a) = z$ となる N/s 個の a にわたる，以下で確認)．

(iv)　1 つ目の量子ビット列に**量子 Fourier 変換** (以下の式 (3.7)) を作用させ，その後，1 つ目の量子ビット列を計算基底で測定する．この結果として N/s の倍数の 1 つが得られる．

(v)　(i) から (iv) を適切な回数繰り返し，得られた N/s の倍数から s を得る．

以下，各ステップについて順に説明する．

ステップ (i) の状態を生成するために，手始めに Hadamard 変換

$$\underbrace{|0\cdots0\rangle}_{n\text{ ビット}}|0\rangle \xmapsto{H^{\otimes n}\otimes\mathbb{I}} \frac{1}{\sqrt{2^n}} \sum_{a\in\{0,1\}^n} |a\rangle\,|0\rangle$$

を行う．ここで n 桁のビット列 a を二進数と見る．［このとき上式 (12) より $2^{n-1} \le a < 2^n$ であり，同様に］$2^{n-1} \le N < 2^n$ である．さて，我々が得たいのは $a \in \mathbb{Z}_N$ にわたる和なので，$a \ge N$ の項を除く必要がある．

そこで関数

$$t(a) = \begin{cases} 0 & (a \geq N) \\ 1 & (\text{その他}) \end{cases}$$

を定義し，その値を最後の量子ビットに入れて

$$\frac{1}{\sqrt{2^n}} \sum_{a \in \{0,1\}^n} |a\rangle \, |t(a)\rangle \tag{14}$$

とする．この状態で $t(a) = 1$ が得られれば全体系の状態は

$$\frac{1}{\sqrt{N}} \sum_{a=0}^{N} |a\rangle \, |1\rangle \tag{15}$$

に移るので［本稿次項で確認］，最後の量子ビット $|1\rangle$ を捨てると (i) の r-量子ビット状態が得られる．$t(a) = 0$ を得る確率は $1/2$ 以下であり，その場合は最初の Hadamard 変換からやり直す．この試行を k 回繰り返せば，所望の状態が確率 $1 - (1/2^k)$ 以上で得られる．

ステップ (ii) では式 (2.11) の方法で，ゴミ情報を残さずに f を計算する量子回路を用いることができる．

ステップ (iii) では，合成量子ビット系の部分測定に関する 1.3.3 項の一般公式を利用できる．まず (ii) の状態 $|\psi\rangle$ と部分系の状態 $|z\rangle$ に対して，部分内積 (1.52) は

$$\langle z|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{a \in \mathbb{Z}_N} |a\rangle \, \langle z|f(a)\rangle = \frac{1}{\sqrt{N}} \sum_{a:f(a)=z} |a\rangle$$

と評価できる．最右辺の和は $f(a) = z$ を満たす N/s 個の a にわたる．すると測定値 z を得る確率 (1.56) と測定後の状態 (1.57) はそれぞれ，

$$\| \langle z|\psi\rangle \|^2 = \sum_{a:f(a)=z} \frac{1}{N} = \frac{N}{s}\frac{1}{N} = \frac{1}{s}, \quad \left(\frac{1}{\| \langle z|\psi\rangle \|} \langle z|\psi\rangle \right) |z\rangle = \frac{1}{\sqrt{N/s}} \sum_{a:f(a)=z} |a\rangle \, |z\rangle : (13). \tag{3.5–6}$$

次にステップ (iv) の量子 Fourier 変換を説明する．これは多くの量子アルゴリズムで重要な役割を演じる．$\mathbb{Z}_N$ 上の量子 Fourier 変換 F は任意の $a \in \mathbb{Z}_N$ に対して

$$F \, |a\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \omega_N^{ak} \, |k\rangle \tag{3.7}$$

で定義される．ただし $\omega_N \equiv \exp(2\pi i/N)$ ［であり，ω_N^{ak} はその ak 乗］である．この変換はユニタリ行列で与えられる［本稿次項で確認］．

さて，(iii) の測定で得られた値 z に対し，$z = f(a)$ を満たす a の値を

$$a = a_0, a_0 + s, a_0 + 2s, \cdots, a_0 + ((N/s) - 1)s \tag{16}$$

とおく［N/s は数列 $\{f(a)\}$ に含まれる周期の個数］．このとき測定後の状態 (13) に量子 Fourier 変換 F を作用させると，

$$\begin{aligned}
F\left(\frac{1}{\sqrt{N/s}}\sum_{a:f(a)=z}|a\rangle\right) =& \frac{1}{\sqrt{N/s}}\sum_{a:f(a)=z}\frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}\omega_N^{ak}|k\rangle \\
=& \frac{\sqrt{s}}{N}\sum_{k=0}^{N-1}\left(\omega_N^{a_0k}+\omega_N^{(a_0+s)k}+\omega_N^{(a_0+2s)k}+\cdots+\omega_N^{(a_0+((N/s)-1)s)k}\right) \\
& (a \text{ の値 (16) で和をとった}) \\
=& \frac{\sqrt{s}}{N}\sum_{k=0}^{N-1}\omega_N^{a_0k}\sum_{l=0}^{(N/s)-1}\omega_{N/s}^{lk}|k\rangle \qquad \text{［本稿次項で確認］} \\
=& \frac{\sqrt{s}}{N}\sum_{k=0}^{N-1}\omega_N^{a_0k}S_{N/s}(k)|k\rangle \qquad \left(S_{N/s}(k)\equiv\sum_{l=0}^{(N/s)-1}\omega_{N/s}^{lk}\right) \qquad (17)
\end{aligned}$$

となる．最右辺のように，一般に任意の $N,k\in\mathbb{N}$ に対して $S_N(k)=\sum_{l=0}^{N-1}\omega_N^{lk}$ を定義すると，

$$S_N(k)=\begin{cases}N & (k \text{ が } N \text{ の倍数のとき})\\ 0 & (\text{それ以外のとき})\end{cases} \qquad (18)$$

が成り立つ［本稿次節で確認］．すると上式 (17) の最右辺において，$S_{N/s}(k)$ は k が N/s の倍数 $k=(N/s)j$ のときのみ，ゼロでない寄与 N/s を持つ．［ここで $0\le k\le N-1$ より $0\le j\le s-1$ となることに注意する．］よって

$$F\left(\frac{1}{\sqrt{N/s}}\sum_{a:f(a)=z}|a\rangle\right)=\frac{1}{\sqrt{s}}\sum_{j=0}^{s-1}\omega_N^{a_0j(N/s)}|j(N/s)\rangle\,.$$

各 $\omega_N^{a_0j(N/s)}$ は単なる位相因子なので，この状態で量子ビット列を測定すると，N/s の倍数

$$0,N/s,2(N/s),\cdots,(s-1)(N/s)$$

のいずれかが確率 $1/s$ で得られる．

得られた 2 つの倍数を

$$m_1=k_1(N/s),\qquad m_2=k_2(N/s)\qquad (k_1,k_2=0,\cdots,s-1)$$

とする．このとき m_1,m_2,N が既知であり，s,k_1,k_2 は未知である．k_1 と k_2 が互いに素ならば，m_1 と m_2 の最大公約数が N/s となる．そこで Euclid の互除法で N/s を求めれば，s が得られる．

k_1 と k_2 が互いに素にならない確率は

$$\Pr\{\cup_{p:\text{素数}}k_1\text{と }k_2\text{が }p\text{ の倍数 }\}\le\sum_{p:\text{素数}}\Pr\{k_1\text{と }k_2\text{が }p\text{ の倍数 }\}\le\sum_{p:\text{素数}}\frac{1}{p^2}<\sum_{n\ge2}\frac{1}{n^2}<0.65 \qquad (19)$$

となる［本稿次項で補足］．よって $2k$ 個のサンプルからは確率 $1-0.65^k$ 以上で s が得られる．

- 天下りに述べると，f の計算が n の多項式 $n^{O(1)}$ 程度の個数の素子で実現できれば，
  この量子アルゴリズムは $n^{O(1)}$ 個の素子で高い確率で周期 s を求められる．
- N が s で割り切れない場合の取り扱いついては，

– P. W. Shor, *SIAM Journal on Computing,* **26**, 1484–1509 (1997)
– M. A. Nielsen, I. L. Chuang, *Quantum Computation and Quantum Information,* Cambridge University Press (2000) の第 5 章

を見よ．

最後に肝心の解釈として最終段落を引用する：

> 3.1 節でも説明したようにこの量子アルゴリズムも一種の量子状態識別である．実際，ステップ (iii) の量子状態（の確率的混同）は周期 s によって決まっており，与えられた量子状態がどの s から来た状態かがわかれば十分である．この場合，その識別が量子 Fourier 変換から効率良く行うことが可能なのである．

3.3.1 項について

■$t(a)=1$ の測定後の状態が式 (15) で与えられることの確認　合成量子ビット系の部分測定に関する 1.3.3 項の一般公式を利用する．測定前の状態 $|\psi\rangle =$ (式 (14)) と部分系の状態 $|t(a)=1\rangle$ に対して，部分内積 (1.52) は

$$\langle 1|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{a\in\{0,1\}^n} |a\rangle \langle 1|t(a)\rangle = \frac{1}{\sqrt{2^n}} \sum_{a=0}^{N-1} |a\rangle$$

と評価できる．すると $t(a)=1$ を得る確率 (1.56) と測定後の状態 (1.57) はそれぞれ，

$$\| \langle 1|\psi\rangle \|^2 = \sum_{a=0}^{N-1} \frac{1}{\sqrt{2^n}} = \frac{N}{\sqrt{2^n}}, \qquad \left(\frac{1}{\| \langle 1|\psi\rangle \|} \langle 1|\psi\rangle \right) |1\rangle = \left(\frac{1}{\sqrt{N/\cancel{2^n}}} \frac{1}{\cancel{\sqrt{2^n}}} \sum_{a=0}^{N-1} |a\rangle \right) |1\rangle : (15).$$

■量子 Fourier 変換 (3.7) のユニタリ性の確認 (教科書 p.88 の演習問題 17)　行列要素は定義式 (3.7) より

$$F_{kl} = \langle k|F|l\rangle = \frac{1}{\sqrt{N}} \sum_{m=0}^{N-1} \omega_N^{lm} \langle k|m\rangle = \frac{1}{\sqrt{N}} \omega_N^{lk} = \frac{1}{\sqrt{N}} \exp\left(\frac{2\pi i}{N} lk\right) = F_{lk}.$$

この行列 $F=(F_{kl})$ は

$$(F^\dagger F)_{kl} = \frac{1}{N} \sum_{m=0}^{N-1} \exp\left\{ \frac{2\pi i}{N}(l-k)m \right\} = \delta_{kl}, \qquad (FF^\dagger)_{kl} = \frac{1}{N} \sum_{m=0}^{N-1} \exp\left\{ \frac{2\pi i}{N}(k-l)m \right\} = \delta_{kl}$$

を満たすので，ユニタリである．2 式の第 2 の等号はよく知られた関係であり，直観的には $k\neq l$ のとき複素平面上の N 方向の単位ベクトルの和がゼロになることとして理解できる．厳密には以下の演習問題 18 の論法を適用して説明できる．

■式 (17) 第 3 の等号の確認

$$\sum_{k=0}^{N-1} \omega_N^{a_0 k} \sum_{l=0}^{(N/s)-1} \omega_{N/s}^{lk} = \sum_{k=0}^{N-1} \sum_{l=0}^{(N/s)-1} \exp\left(\frac{2\pi i}{N} a_0 k\right) \exp\left(\frac{2\pi i}{N/s} lk\right) = \sum_{k=0}^{N-1} \sum_{l=0}^{(N/s)-1} \exp\left(\frac{2\pi i}{N} k(a_0+sl)\right)$$
$$= \sum_{k=0}^{N-1} \sum_{l=0}^{(N/s)-1} \omega_N^{k(a_0+sl)}$$

とすると，1 行前の表式に戻ることができる．

■$S_N(k)$ の公式 (18) の確認 (教科書 p.88 の演習問題 18)

$$S_N(k) = \sum_{l=0}^{N-1} \omega_N^{lk} = \sum_{l=0}^{N-1} \exp\left(\frac{2\pi i}{N} lk\right)$$

より，k が N の倍数のとき $S_N(k) = N$ となることは直ちに見て取れる．次に

$$(\omega_N^k - 1)S_N(k) = (\omega_N^k - 1)(\omega_N^{k(N-1)} + \omega_N^{k(N-2)} + \cdots + \omega_N^k + \omega_N^0) = \omega_N^{kN} - \omega_N^0 = 1 - 1 = 0$$

が恒等的に成り立つことに注目する．すると k が N の倍数でないとき $\omega_N^k = \exp\left(\frac{2\pi i}{N}k\right) \neq 1$ なので，$S_N(k) = 0$.

■不等式 (19) について　第 1 の不等号は

- k_1 と k_2 が 2 の倍数，または 3 の倍数，または 5 の倍数，……である確率 (最左辺)
- k_1 と k_2 が 2 の倍数の確率，3 の倍数の確率，5 の倍数の確率，……の和 (第 2 辺)

に対する，いわゆる Boole の不等式である．

第 2 の不等号について，p の倍数は p 回に 1 回ずつ現れるので，整数の並びから任意に選んだ整数が p の倍数である確率は $1/p$ である．ところが $k = k_1, k_2$ は 0 以上 $(s-1)$ 以下なので，それぞれが p の倍数となる確率は $1/p$ 以下である．(一般には次の p の倍数が現れる前に $(s-1)$ に達する．)

「最後の不等式は $\sum_{n\in\mathbb{N}} n^{-2} = \pi^2/6$ から得られる」(p.90, l.3) ことについて，初等的には Fourier 級数展開

$$\frac{x^2}{4} = \frac{\pi^2}{12} + \sum_{n=1}^{\infty} \frac{(-1)^n}{n^2} \cos nx \qquad (-\pi \leq x \leq \pi)$$

に $x = \pi$ を代入して

$$\zeta(2) \equiv \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$$

を得る [6, p.212].

3.3.2　素因数分解問題に対する量子アルゴリズム

周期発見問題に対する量子アルゴリズムを，素因数分解問題に応用しよう．

素因数分解問題 (factorization problem)

入力　n ビット長の自然数 N，ただし素数 p, q に対し $N = pq$.

出力　$N = pq$ を満たす素数 p, q

ただし N が偶数の場合は明らかに 2 を素因数に持つので，以下では N が奇数 (したがって p, q は奇素数) の場合だけを考える．[また $N = 3^2 \cdot 5^3 \cdot 7$ のような場合も考えない．]

$N \leq 2^n - 1$ より，しらみ潰しで素因数を調べると n の指数関数的な計算時間が必要であり，現在のところ多項式時間アルゴリズムは知られていない．しかしながら古典計算においても，素因数分解問題をある程度，効率良く解くことができる．手始めにその手順を以下に示す．ただし 2 整数 a, b の最大公約数を $\mathrm{GCD}(a, b)$ で表す．

(*i*) $x \in \{1, \cdots, N-1\}$ を一様ランダムに選ぶ．

(*ii*) GCD(x, N) を計算する．その値が 1 でなければ GCD(x, N) を出力して終了する．

(*iii*) $x^r \equiv 1 \bmod N$ となる最小の r を求める．

(*vi*) r が偶数かつ $x^{r/2} \not\equiv -1 \bmod N$ ならば，GCD$(x^{r/2}+1, N)$ と GCD$(x^{r/2}-1, N)$ が N を割り切るか検証し，割り切るならばそれを出力して終了する．そうでなければ (*i*) からやり直す．

説明 まず (*i*) で選んだ x が N と互いに素でない，すなわち GCD$(x, N) \neq 1$ であれば，GCD(x, N) を素因数として出力すれば良い (ステップ (*ii*))．［例えば $N = 15, x = 9$ に対して GCD$(x, N) = 3$ は N の素因数である．もう一方の素因数は $15/3 = 5$.］

次に GCD$(x, N) = 1$ の場合に進もう．x に応じて $x^r \equiv 1 \bmod N$ を満たす最小の r が決まる．［例えば $N = 15, x = 4$ のとき $r = 2$.］ここで r を偶数とすると，$r/2$ は整数であり

$$(x^{r/2}+1)(x^{r/2}-1) = x^r - 1 \equiv 0 \mod N$$

が成り立つ．

note これは $x^{r/2} \pm 1$ の積が N の倍数であることを意味するものの，必ずしも $x^{r/2} \pm 1$ は N の倍数とならない．実際，再び $N = 15, x = 4, r = 2$ を考えると $x^{r/2}+1 = 5 \not\equiv 0, x^{r/2}-1 = 3 \not\equiv 0$．また一般に $x^{r/2}-1 \equiv 0$ と仮定すると，$x^{r'} \equiv 1$ なる $r' = r/2 < r$ が存在することになり，r の最小性に反する．よって $x^{r/2} \not\equiv 1$ である，すなわち $x^{r/2}-1$ は N の倍数ではない．その上で

$x^{r/2} \not\equiv -1 \bmod N$ ならば GCD$(x^{r/2}+1, N)$ と GCD$(x^{r/2}-1, N)$ の双方が N の非自明な因数になる．

天下りに述べると，ランダムに選んだ x に対して r が偶数かつ $x^{r/2} \not\equiv -1 \bmod N$ となる確率は $1/2$ 以上であることが示せる．なお GCD を効率良く求めるには，単に Euclid の互除法を用いれば良い．

さて，量子計算を利用できるのはステップ (*iii*) である：r を求める問題はべき剰余関数

$$f(a) = x^a \mod N$$

の周期発見問題に帰着するため，Shor のアルゴリズムを適用できる．実際，例えば $N = 15 = 3 \cdot 5$, $x = 2$ ［したがって GCD$(x, N) = 1$］のとき，［N を法として $x^0 = 1, x^1 = 2, x^2 = 4, x^3 = 8, x^4 = 16 \equiv 1$ なので］$f(x)$ は

$$f(0) = 1, \qquad f(1) = 2, \qquad f(2) = 4, \qquad f(3) = 8$$

を繰り返し，周期 $s = 4$ の周期関数となる．すると $1 = f(0) = f(s) = f(2s) = \cdots$ なので，この周期 s が求める r の値に他ならない．

Shor のアルゴリズムは $f(a)$ の値を評価するステップを含んでいる［3.3.1 項］．そこで最後に効率良く $f(a)$ を計算する方法を概説する．二進法で

$$a = a_1 \cdots a_n \qquad \text{i.e.} \qquad a = a_1 2^{n-1} + \cdots + a_n 2^0 = \sum_{i=1}^{n} a_i 2^{n-i}$$

(ただし $a_i = 0, 1$) と書くと，

$$x^a = \prod_{i=1}^{n} x^{a_i 2^{n-i}} = \prod_{i:a_i=1} x^{2^{n-i}}.$$

よってせいぜい n 個の値

$$x^1 \bmod N, \qquad x^2 \bmod N, \qquad x^4 \bmod N, \qquad x^8 \bmod N, \qquad \cdots \qquad x^{2^{n-1}} \bmod N$$

が分かっていれば，直ちに $f(a)$ が求まる．これら n 個の値は，$x = x \bmod N$ から始めて $(n-1)$ 回の掛け算と剰余演算を行えば求められる．

3.3.3 離散対数問題に対する量子アルゴリズム

特別な離散対数問題に対して，Shor のアルゴリズムを適用するアイデアを例示的に説明する．

離散対数問題 (discrete logarithm problem)

入力 素数 p と

$$\{g^0 \bmod p, g^1 \bmod p, \cdots, g^{p-2} \bmod p\} = \{1, 2, \cdots, p-1\} \tag{20}$$

かつ $1 < g < p$ を満たす自然数 g，$0 < y < p$ を満たす自然数 y

出力 $y \equiv g^x \bmod p$ かつ $0 \leq x < p$ を満たす自然数 x

例えば $p = 5, y = 2, g = 3$ は入力の条件を満たしている．とりわけ上式 (20) は，5 を法として

$$3^0 \equiv 1, \qquad 3^1 \equiv 3, \qquad 3^2 \equiv 4, \qquad 3^3 \equiv 2 \tag{21}$$

となることから直接確かめられる．このとき問題は

$$2 \equiv 3^x \mod 5 \qquad \text{かつ} \qquad 0 \leq x < 5$$

を満たす自然数 x を求めることとなる［離散対数問題という名前も頷ける］．5 つの値 $x = 0, 1, 2, 3, 4$ に対して 3^x の値を順に調べると，上式 (21) と $3^4 \equiv 1$ より，答として $x = 3$ を得る．

一般に p の入力長を n とすれば，p 個の $x = 0, \cdots, p-1$ からしらみ潰しに答を探すと，最悪 $O(2^n)$ の計算量が必要になりかねない．今のところ知られている改良された古典計算のいずれも，やはり計算量は指数関数的である．他方，以下のように離散対数問題を周期発見問題に帰着させると，Shor のアルゴリズムを用いて n の多項式程度の素子で問題を解くことができる．

$$\mathbb{Z}_p = \{0, \cdots, p-1\}\ [3.3.1\text{ 項}], \qquad \mathbb{Z}_p^* = \{y \in \mathbb{Z}_p | y \text{ と } p \text{ の最大公約数が } 1\} = \mathbb{Z}_p$$

($\mathbb{Z}_p^*$ の第 2 の等号で素数 p を仮定した) と，$y \in \mathbb{Z}_{p-1}$ に対して $y \cdot y^{-1} \equiv 1 \bmod p$ を満たす元 $y^{-1} \in \mathbb{Z}_{p-1}$ を定義し，関数

$$f : \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1} \to \mathbb{Z}_p^* : (a, b) \mapsto f(a, b) = g^a \cdot (y^{-1})^b \bmod p \tag{3.8}$$

を考える［p で割った余りは確かに $f(a, b) \in \mathbb{Z}_p^*$］．再び $p = 5, y = 2, g = 3$ の場合を考えると $a, b \in \{0, \cdots, 3\}$，$f(a, b) \in \{0, \cdots, 4\}$ であり，また $2 \cdot 2^{-1} \equiv 1 \bmod 5$ を満たす元 $2^{-1} \in \{0, \cdots, 3\}$ は $2^{-1} = 3$ に定まる．すると関数 (3.8) は

$$f(a, b) = 3^a 3^b \mod 5,$$

あるいは明示的には

$$\begin{aligned}
&f(0,0) = f(3,1) = f(2,2) = f(1,3) = 1,\\
&f(1,0) = f(0,1) = f(3,2) = f(2,3) = 3,\\
&f(2,0) = f(1,1) = f(0,2) = f(3,3) = 4,\\
&f(3,0) = f(2,1) = f(1,2) = f(0,3) = 2
\end{aligned}$$

となる．ここから f は

$$f(a, b) = f(a + 3 \bmod 4, b + 1 \bmod 4)$$

を満たし，隠れた周期 $(x, 1) = (3, 1)$ を持つことが見て取れる．

一般に関数 (3.8) はこの意味で隠れた周期 $(x,1)$ を持つ．そこで答 x を得るには，周期 $(x,1)$ を求めれば良い．2 次元の周期 $(x,1)$ を Shor のアルゴリズムで求めるには，量子 Fourier 変換として $\mathbb{Z}_{p-1}\times\mathbb{Z}_{p-1}$ 上のそれ

$$F\left|a\right\rangle\left|b\right\rangle=\frac{1}{\sqrt{(p-1)^2}}\sum_{k,l\in\mathbb{Z}_{p-1}}\omega_{p-1}^{ak+bl}\left|k\right\rangle\left|l\right\rangle$$

を用いれば良い．

3.4 その他の量子アルゴリズム

- 量子ウォーク (ランダムウォークの量子拡張) を利用したアルゴリズム
  - A. Ambainis, *SIAM Journal on Computing,* **37**, 210–239 (2007).
  - A. M. Childs, R. Cleve, E. Deotto, E. Farhi, S. Gutmann, D. A. Spielman, *Proc. of the 35th Annual ACM Symposium on Theory of Computing,* 59–68 (2003).
  - M. Szegegy, *Proc. of the 45th IEEE Symposium on Foundations of Computer Science.* 32–41 (2004).
- HHL アルゴリズム
  巨大で疎な連立一次方程式の解を表す量子状態を高速で生成するアルゴリズムであり，
  量子機械学習の基礎として広く利用
  - A. W. Harrow, A. Hassidim, S. Lloyd, *Phys. Rev. Lett.,* **103**, 150502 (2009).
- さらに発展的な内容を含んだ，量子アルゴリズムの包括的な解説論文
  - D. Bacon, W. van Dam, *Communications of the ACM,* **53**, 84–93 (2010).
  - A. Montanaro, *npj Quantum Inf.,* **2**, 15023 (2016).
- Shor のアルゴリズムの発展形とそれが対象とする代数的な問題の解説論文
  - A. M. Childs, W. van Dam, *Rev. Mod. Phys.,* **82**, 1 (2010).
- これまで提案された多くの量子アルゴリズムを
  簡潔にまとめたウェブサイト“Quantum Algorithm Zoo”
  - S. Jordan, `https://quantumalgorithmzoo.org/`
- **量子特異値変換** (quantum singular value transform)
  種々の量子アルゴリズムの「大統一」を示唆か

    複素行列 A に対して，適切なユニタリ行列 U,V と成分が非負の実数 $\sigma_1,\cdots,\sigma_n$ である対角行列 Σ をとって $A=U\Sigma V^\dagger$ と分解できることが知られている．これを A の特異値分解と呼び，また Σ の対角成分 $\sigma_1,\cdots,\sigma_n$ を A の特異値と呼ぶ．大雑把に言うと量子特異値変換は与えられた行列 A の特異値をある条件を満たす所望の多項式 P で変換した行列 $P(A)=UP(\Sigma)V^\dagger$ で与えられる変換（ただし $P(\Sigma)$ は対角成分に $P(\sigma_1),\cdots,P(\sigma_n)$ を持つ対角行列）を量子アルゴリズムとして効率良く実現する方法である．(教科書 pp.95–96)
  - A. Gilyén, Y. Su, G.H. Low, N. Wiebe, *Proc. of the 51st ACM Symposium on Theory of Computing,* 193–204 (2019).
  - J. M. Martyn, Z. M. Rossi, A. K. Tan, I. L. Chuang, *PRX Quantum,* **2**, 040203 (2021).

参考文献

[1] J.J.Sakurai，2017，現代の量子力学 (上)(桜井明夫訳)，株式会社吉岡書店，京都.

[2] Rovelli, C. (2010) *Quantum Gravity.* Cambridge University Press, Cambridge.

[3] 沙川貴大，2022，非平衡統計力学——ゆらぎの熱力学から情報熱力学まで——，共立出版株式会社，東京.

[4] H. ジョージァイ，2010，物理学におけるリー代数——アイソスピンから統一理論へ—— (原著第 2 版) (九後汰一郎訳)，株式会社吉岡書店，京都.

[5] 佐藤光，2019，群と物理，丸善出版株式会社，東京.

[6] 矢野健太郎，石原繁，2013，基礎解析学 (改訂版)，株式会社裳華房，東京.