量子計算量理論入門

西村　治道[1]

2023 年 10 月 21 日

[1]名古屋大学大学院情報学研究科数理情報学専攻

目 次

第1章　ブラケット記法と量子計算でおなじみの行列

量子力学ではベクトルや行列の表記にブラケット記法（Dirac 記法）と呼ばれる独特の記法を使います．以下では，とくに断らない限り有限次元複素内積空間のみ扱います．また i は，とくに断らない限り虚数単位を表すものとします．

行列やベクトルの転置共役は † という上添え字記号を用います．例えば行列 A の転置共役は $A^\dagger$ と表します．単位行列は I で表します．

1.1　ベクトル

複素列ベクトル空間の要素は，$\boldsymbol{v}$ などの線形代数で使われる記法の代わりに，$|\psi\rangle$ という記法（ケット記法）を使います．j 番目の要素が 1 でそれ以外が 0 ですような列ベクトルは，$|j\rangle$ と表します．これにより，n 次元複素内積空間の任意の列ベクトル

$$|\psi\rangle = \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} \tag{1.1}$$

は

$$|\psi\rangle = a_0|0\rangle + a_1|1\rangle + \cdots + a_{n-1}|n-1\rangle$$

と表せます．なお，インデックス j は状況によっては 1 から始まることもありますし，2 進表示であること，さらには「$n = 2$ のときに最初のインデックスが a で 2 番目が b」など文字であることもあります．以下では後の便宜のために，$|j\rangle$ のインデックス j は，とくに断らない限り 0 から始まるものとします（つまり，n 次元の場合，$j = 0, 1, \ldots, n-1$ とします）．

列ベクトル $|\psi\rangle$ の転置共役である行ベクトルは，$\langle\psi|$（ブラ記法）と表されます．つまり，式 (1.1) の列ベクトルに対して

$$\langle\psi| = \begin{pmatrix} a_0^* & a_1^* & \cdots & a_{n-1}^* \end{pmatrix} \tag{1.2}$$

であり，

$$\langle\psi| = a_1^*\langle 0| + a_2^*\langle 1| + \cdots + a_n^*\langle n-1|$$

となります．

$|\phi\rangle$ と $|\psi\rangle$ の内積は，$\langle\phi|\psi\rangle$ と表されます（$\langle\phi||\psi\rangle$ の略記です）．

例 1.1.

$$|\phi\rangle = \begin{pmatrix} 1 \\ 2i \end{pmatrix} = |0\rangle + 2i|1\rangle, \qquad |\psi\rangle = \begin{pmatrix} 4i \\ 2 \end{pmatrix} = 4i|0\rangle + 2|1\rangle$$

のとき，その内積は

$$\langle\phi|\psi\rangle = \begin{pmatrix} 1 & -2i \end{pmatrix} \begin{pmatrix} 4i \\ 2 \end{pmatrix} = 0$$

となります．これはまた

$$\langle j|k\rangle = \delta_{jk} = \begin{cases} 1 & (j = k) \\ 0 & (j \neq k) \end{cases} \tag{1.3}$$

に注意すると，

$$\begin{aligned}\langle\phi|\psi\rangle &= (\langle 0| - 2i\langle 1|)(4i|0\rangle + 2|1\rangle) = 4i\langle 0|0\rangle + 2\langle 0|1\rangle - 8i^2\langle 1|0\rangle - 4i\langle 1|1\rangle \\ &= 4i + 0 + 0 - 4i = 0\end{aligned}$$

とも計算できます．

1.2　行列

n 次元列ベクトル $|j\rangle$ と n 次元行ベクトル $\langle k|$ の積 $|j\rangle\langle k|$ は (j,k) 成分のみ 1 で他がすべて 0 の n 次（正方）行列になることに注意すると，n 次行列 $A = (a_{jk})$ はブラケット記法を使って

$$A = \sum_{jk} a_{jk}|j\rangle\langle k| \tag{1.4}$$

と表されます．再び $\langle j|k\rangle = \delta_{jk}$ に注意すると

$$\langle j|A|k\rangle = a_{jk}$$

となります．つまり，$\langle j|A|k\rangle$ は A の (j,k) 成分を表すことになります．また，列ベクトル $A|\psi\rangle$ や行ベクトル $\langle\phi|A$ の計算も同様に計算できます．

例 1.2.

$$A = \begin{pmatrix} 3 & -1 \\ 0 & 1 \end{pmatrix}$$

はブラケット表記では

$$A = 3|0\rangle\langle 0| - 1|0\rangle\langle 1| + |1\rangle\langle 1|$$

と表せます．このとき，A の $(0,1)$ 成分は

$$\langle 0|A|1\rangle = 3\langle 0|0\rangle\langle 0|1\rangle - 1\langle 0|0\rangle\langle 1|1\rangle + \langle 0|1\rangle\langle 1|1\rangle = -1$$

と計算されます．また

$$|\psi\rangle = \begin{pmatrix} 2 \\ 1 \end{pmatrix} = 2|0\rangle + |1\rangle$$

に対して A を作用させると

$$\begin{aligned} A|\psi\rangle &= 6|0\rangle\langle 0|0\rangle - 2|0\rangle\langle 1|0\rangle + 2|1\rangle\langle 1|0\rangle + 3|0\rangle\langle 0|1\rangle - |0\rangle\langle 1|1\rangle + |1\rangle\langle 1|1\rangle \\ &= 6|0\rangle - |0\rangle + |1\rangle = 5|0\rangle + |1\rangle \end{aligned}$$

と計算できます．

例 1.3. n 次単位行列 I は

$$I = \sum_{j=1}^{n} |j\rangle\langle j|$$

と表現できます．

n 次元行列 A の**トレース (trace)** とは A の対角成分の和のことであり，$\mathrm{tr}(A)$ と表します．ブラケット記法では

$$\mathrm{tr}(A) = \sum_{j=1}^{n} \langle j|A|j\rangle$$

となります．

1.3 エルミート行列，ユニタリ行列，射影

正方行列 U が

$$UU^\dagger = U^\dagger U = I$$

をみたすとき，U は**ユニタリ (unitary)** 行列といいます．ユニタリ行列は，ベクトル間の内積（それゆえベクトルの長さ）を保存する行列です．実際，任意の二つのベクトル $|\phi\rangle, |\psi\rangle$ に対して，ユニタリ行列 U をかけた後の $U|\phi\rangle$ と $U|\psi\rangle$ の内積は

$$(U|\phi\rangle)^\dagger(U|\psi\rangle) = \langle\phi|U^\dagger U|\psi\rangle = \langle\phi|I|\psi\rangle = \langle\phi|\psi\rangle$$

となり，$|\phi\rangle$ と $|\psi\rangle$ の内積に等しいです．とくに

$$\|U|\psi\rangle\|^2 = (U|\psi\rangle)^\dagger(U|\psi\rangle) = \langle\psi|U^\dagger U|\psi\rangle = \langle\psi|\psi\rangle = \||\psi\rangle\|^2$$

となって，ベクトルの長さが保存されています．また，

$$\langle j|U^\dagger U|k\rangle = \langle j|k\rangle = \delta_{jk}$$

であることから，ベクトルの集合 $\{U|j\rangle\}$ は正規直交基底であることがわかります．つまり，ユニタリ行列 U は標準基底 $\{|j\rangle\}$ を別の正規直交基底 $\{U|j\rangle\}$ に変換する行列と考えられます．また，$U|j\rangle$ が U の第 j 列ベクトルであることを鑑みると，U の列ベクトルは長さ 1 で互いに直交するものであることがわかります．そして，これは U がユニタリ行列であることの必要十分条件です．

命題 1.1. n 次元行列 U において，以下は互いに必要十分である．

1. U はユニタリ行列である．
2. U の列ベクトルの集合 $\{U|j\rangle\}$ は正規直交基底である．
3. U の行ベクトルの集合 $\{\langle j|U\}$ は正規直交基底である．

例 1.4. 任意の実数 θ に対して，

$$U(\theta) = \begin{pmatrix} \cos\theta & i\sin\theta \\ i\sin\theta & \cos\theta \end{pmatrix}$$

はユニタリ行列です．実際，

$$U(\theta)^\dagger U(\theta) = \begin{pmatrix} \cos\theta & -i\sin\theta \\ -i\sin\theta & \cos\theta \end{pmatrix}\begin{pmatrix} \cos\theta & i\sin\theta \\ i\sin\theta & \cos\theta \end{pmatrix} = 0$$

となります．また，2 つの列ベクトル

$$U(\theta)|0\rangle = \begin{pmatrix} \cos\theta \\ -i\sin\theta \end{pmatrix}$$

および

$$U(\theta)|1\rangle = \begin{pmatrix} -i\sin\theta \\ \cos\theta \end{pmatrix}$$

は，内積を計算すると 0 になるので確かに直交しています．

問 1.1. ユニタリ行列の固有値は $e^{i\theta}$（θ は実数）の形になることを示しなさい.

問 1.2. n 次複素内積空間における任意の正規直交基底 $\{|\psi_j\rangle\}$ に対して，

$$\sum_{j=1}^{n} |\psi_j\rangle\langle\psi_j| = I \tag{1.5}$$

（**完備関係式 (completeness relation)**）が成り立つことを示しなさい. また，任意の n 次行列 A に対して，

$$\mathrm{tr}(A) = \sum_{j=1}^{n} \langle\psi_j|A|\psi_j\rangle$$

が成り立つことも示しなさい.

正方行列 A が

$$AA^\dagger = A^\dagger A$$

をみたすとき，A は**正規行列 (normal matrix)** であるといいます．正規行列については，対角化に関する以下の定理が知られています.

定理 1.2 (**スペクトル分解定理**)**.** A が正規行列のとき，あるユニタリ行列 U が存在して

$$U^\dagger A U = \sum_j \lambda_j |j\rangle\langle j|$$

と対角化できる．ただし，λ_j は A の固有値である.（右辺は j 番目の対角成分が λ_j の対角行列であることに注意.）

定理 1.2 は，正規直交基底 $\{|\psi_j\rangle\}$ $(= \{U|j\rangle\})$ が存在して

$$A = \sum_j \lambda_j |\psi_j\rangle\langle\psi_j| \tag{1.6}$$

（A の**スペクトル分解**と呼ばれる）と書けるとも言い直せます．$|\psi_j\rangle$ は A の固有値 λ_j に対する固有ベクトルになります.

n 次行列 A が

$$A^\dagger = A$$

をみたすとき，A は**エルミート (Hermite) 行列**といいます．任意のエルミート行列 A は実数値を固有値として持ち，正規行列であるため，スペクトル分解定理より，ある正規直交基底 $\{|\psi_j\rangle\}$ と対応する実固有値 λ_j を使って式 (1.6) の形にできます.

例 1.5. エルミート行列

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1|$$

は対角行列なので，右辺の表現がすでにスペクトル分解になっています．

例 1.6. エルミート行列

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

の固有値は $+1, -1$ であり，対応する固有ベクトルは $|+\rangle := \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|-\rangle := \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ なので，そのスペクトル分解は

$$X = |+\rangle\langle +| - |-\rangle\langle -|$$

です．

ユニタリ行列も正規行列なので，問 1.1 より

$$\sum_j e^{i\theta_j} |\psi_j\rangle\langle\psi_j|$$

の形にスペクトル分解できます．

問 1.3. エルミート行列およびユニタリ行列が正規行列であることを示しなさい．

問 1.4. 2 次行列

$$\begin{pmatrix} 1 & -i \\ i & 1 \end{pmatrix}$$

のスペクトル分解を求めなさい．

固有値が $0, 1$ のみのエルミート行列を**射影行列**（あるいは**射影**）と呼びます．n 次元複素内積空間の正規直交基底 $\{|\psi_j\rangle\}$ の部分集合 $\{|\psi_{j_1}\rangle, \ldots, |\psi_{j_m}\rangle\}$ から決まるエルミート行列

$$A = |\psi_{j_1}\rangle\langle\psi_{j_1}| + \cdots + |\psi_{j_m}\rangle\langle\psi_{j_m}|$$

は射影行列です．とくに，任意の単位ベクトル $|\psi\rangle$ に対し，ランク 1 のエルミート行列 $|\psi\rangle\langle\psi|$ は射影行列です．実際，任意の n 次元ベクトル $|\phi\rangle$ に $|\psi\rangle\langle\psi|$ を作用させると

$$(|\psi\rangle\langle\psi|)|\phi\rangle = (\langle\psi|\phi\rangle)|\psi\rangle$$

となって，作用後のベクトルは文字通り $|\psi\rangle$ を軸とする直線上に射影されています．

射影行列 A は次の形で特徴付けられます．

定理 1.3. 正方行列 A が射影行列であることと，以下の 2 条件が成り立つことは，必要十分である．

1. $A^2 = A$
2. $A^\dagger = A$

固有値が 0 以上のエルミート行列は，**半正定値行列 (semi-definite positive matrix)** と呼ばれています．半正定値行列 A は，任意のベクトル $|\psi\rangle$ について

$$\langle\psi|A|\psi\rangle \geq 0 \tag{1.7}$$

をみたします．任意の $|\psi\rangle$ に対して式 (1.7) が成り立つことは

$$A \geq 0$$

と表されます．

問 1.5. 半正定値行列 A は，任意のベクトル $|\psi\rangle$ について式 (1.7) をみたすことを示しなさい．(ヒント：スペクトル分解)

また，エルミート行列 A, B が

$$A - B \geq 0$$

をみたすとき，

$$A \geq B$$

と表されます．とくに

$$kI - A \geq 0$$

である場合（すなわち，A の固有値が k 以下である場合），

$$A \leq k$$

と表されます．例えば，

$$0 \leq A \leq 1$$

は，A が 0 以上 1 以下の固有値を持つエルミート行列であることを意味しています．

第2章　量子情報の基礎

量子コンピュータは微細粒子などのミクロ系が従うとされる量子力学を基礎原理としています．以下では，量子コンピュータによる計算（量子計算）の数理を展開するために必要な量子力学の基礎を説明します．なお，量子計算の分野では，我々が日常的に使っているコンピュータや計算や情報などにしばしば「古典」という接頭語をつけて呼ぶことがあります[1]．

2.1　量子ビット，量子状態

古典コンピュータにおける情報の基本単位はビットで，値として 0 および 1 を取ることができます．一方，量子コンピュータにおける情報の基本単位は**量子ビット**（quantum bit，略して **qubit** と呼ばれます）で，0 と 1 の中間的な状態も取ることができます（**重ね合わせの原理**）．数学的には，2 次元複素内積空間の単位ベクトルとして表されます．0 および 1 に対応する状態として，

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

を対応させ，一般の量子ビットの状態は

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \tag{2.1}$$

が対応します．ただし，α, β は $|\alpha|^2 + |\beta|^2 = 1$ をみたす複素数です．

一般に，量子状態は（無限次元でない限り）n 次元複素内積空間の単位ベクトルとして

$$|\psi\rangle = \sum_{j=0}^{n-1} \alpha_j |j\rangle \tag{2.2}$$

のように表されます．ただし，$|j\rangle$ は j 番目の成分が 1，それ以外の成分が 0 の n 次単位ベクトルであり，α_j は $\sum_{j=0}^{n-1} |\alpha_j|^2 = 1$ をみたす複素数です．

[1] 従来の計算やアルゴリズムが古典力学（ニュートン力学）に従っていることによります．

量子ビットの状態は $n = 2$ の場合です．係数 α_j は**振幅 (amplitude)**，あるいは確率振幅と呼ばれます．

2.1.1　量子ビット，量子状態の測定

式 (2.2) で表される量子状態 $|\psi\rangle$ から人間が情報を得るには，測定を行う必要があります．最も基本的な測定は**標準基底 $\{|j\rangle\}$ による測定**と呼ばれる測定です．$|\psi\rangle$ にその測定を施すと，確率 $|\alpha_j|^2$ で測定値 j が得られることになります．そして測定後の量子状態は，得られた測定値 j に対応する状態 $|j\rangle$ に変化します．

例 2.1. 量子ビットの状態

$$|\psi_1\rangle = \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle \tag{2.3}$$

を標準基底 $\{|0\rangle, |1\rangle\}$（量子計算では**計算基底**と呼ばれる）による測定を行うと，

- 確率 $\frac{1}{4}$ で測定値 0 を得て測定後の状態が $|0\rangle$ になるか，
- 確率 $\frac{3}{4}$ $(= |\frac{\sqrt{3}}{2}|^2)$ で測定値 1 を得て測定後の状態が $|1\rangle$ になるか

が起こります．

問 2.1. 量子ビットの状態

$$|\varphi\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$$

に対して，計算基底による測定を行うとどうなるでしょうか？

注意 2.1. 式 (2.3) の状態に $e^{i\theta}$（$\theta \in [0, 2\pi)$ は任意）をつけた状態 $e^{i\theta}|\psi_1\rangle$ を計算基底で測定しても，$|\psi_1\rangle$ と同じ測定値の確率分布が得られます．

実際には $e^{i\theta}|\psi_1\rangle$ と $|\psi_1\rangle$ は，計算基底による測定だけでなく，(この後紹介するような）どんな測定に対しても識別が不可能（すなわち測定を表す数学的操作から得られる確率分布が同一）であることが示せます．そのため数学的表現は少し違っても**量子状態としては同一のもの**を表します．$e^{i\theta}$ は**位相因子 (phase factor)** と呼ばれます．このような表現の非一意性は，後に紹介する密度行列の表現を使うと解消されます．

標準基底による測定は，数学的には射影によって記述されます．実際，式 (2.2) の状態を標準基底で測定すると，測定値 j が確率 $|\alpha_j|^2$ で得られ

て測定後の状態は $|j\rangle$ になります．これは標準基底 $\{|j\rangle\}$ への射影を，射影の長さの 2 乗で決まる確率

$$|\alpha_j|^2 = |\langle j|\psi\rangle|^2 \ (= \|(|j\rangle\langle j|)|\psi\rangle\|^2)$$

に応じて行った後で得られたベクトル

$$\alpha_j|j\rangle$$

を正規化して

$$\frac{\alpha_j|j\rangle}{|\alpha_j|} \simeq |j\rangle$$

を得るという操作といえます．ここで $\simeq$ は量子状態としての同一視を表します．

2.1.2 量子ビットの幾何的描像

量子ビットの状態を表す式 (2.1) において，振幅 α, β が実数の場合は，図 2.1 のように 2 次元平面上の単位円の点 (α, β) に対応するベクトルで表現できます．ただし，図のベクトルと原点対称の位置にあるベクトル $-|\psi\rangle$ も注意 2.1 により同一の状態を表すことに注意する必要があります．

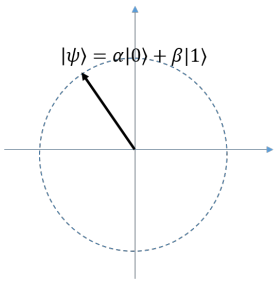

図 2.1: 実数を振幅に持つ量子ビットの描像

一般の場合，α, β は複素数なので，

$$\alpha = r_\alpha e^{i\theta_\alpha}, \quad \beta = r_\beta e^{i\theta_\beta}$$

と極座標表示できます．実数 r_α, r_β は $r_\alpha^2 + r_\alpha^2 = 1$ をみたすので，

$$r_\alpha = \cos(\theta/2), \quad r_\beta = \sin(\theta/2)$$

と表現できます．注意 2.1 より $r_\beta \geq 0$ としてもよいので，θ の範囲は $0 \leq \theta \leq \pi$ としてよいです．このとき，式（2.1）は

$$e^{i\theta_\alpha}\cos(\theta/2)|0\rangle + e^{i\theta_\beta}\sin(\theta/2)|1\rangle = e^{i\theta_\alpha}(\cos(\theta/2)|0\rangle + e^{i\gamma}\sin(\theta/2)|1\rangle)$$

（ただし，$\gamma = \theta_\beta - \theta_\alpha$ と置き直しました）となります．再び注意 2.1 より，これは

$$|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\gamma}\sin(\theta/2)|1\rangle \tag{2.4}$$

（$0 \le \theta \le \pi$，$0 \le \gamma < 2\pi$）という状態と同一視できます（式 (2.1) の $|\psi\rangle$ とは位相因子分の数学的表現の差がありますが，同一の記号で $|\psi\rangle$ と表しています）．よって一般の場合の量子状態は，図 2.2 のように実 3 次元空間上の単位球上の点 $(\cos\gamma\sin\theta, \sin\gamma\sin\theta, \cos\theta)$ に対応するベクトルで表現できます．この単位球は **Bloch 球**と呼ばれています．

例 2.2.

$$|\varphi\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{i}{\sqrt{2}}|1\rangle$$

は，式 (2.4) において $\theta = \pi/2$, $\gamma = 3\pi/2$ として得られるものです．よって，この状態は Bloch 球の点 $(0, 1, 0)$ に対応します．

問 2.2. $|0\rangle$, $|1\rangle$, $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ は，それぞれ Bloch 球においてどの点に対応するでしょうか？

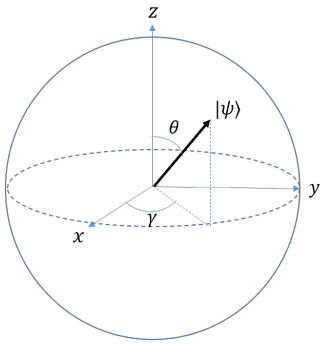

図 2.2: 一般の量子ビットの描像 (Bloch 球)

2.1.3　量子ビット，量子状態の時間発展

測定以外に量子状態を変化させる操作として，**時間発展 (time evolution)** があります．数学的には，時間発展はユニタリ行列で表現されます．式 (2.2) で表される量子状態 $|\psi\rangle$ がユニタリ行列 U で表現される時間発展を受けるとき，時間発展後の状態は $U|\psi\rangle$ となります．時間発展後の状態 $U|\psi\rangle$ が単位ベクトルであることは，ユニタリ行列が長さを保存することから保証されます．量子計算においてはこのようなユニタリ行列を**量子ゲート**と呼びます．

例 2.3.

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

は**NOT ゲート**と呼ばれるユニタリ行列です．式 (2.1) の量子ビットの状態に時間発展 X を施した後の状態は

$$X|\psi\rangle = \alpha X|0\rangle + \beta X|1\rangle = \alpha|1\rangle + \beta|0\rangle$$

となります．とくに，$|0\rangle$ は $|1\rangle$，$|1\rangle$ は $|0\rangle$ に変化するので NOT ゲートと呼ばれますが，物理では σ_x という Pauli 行列に対応するため，X **ゲート**とも呼ばれます．

例 2.4.

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

は**Hadamard ゲート**と呼ばれるユニタリ行列です．例えば，量子ビットの状態 $|0\rangle$ に時間発展 H を施した後の状態は

$$H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

となって，$|0\rangle$ と $|1\rangle$ が一様に重なった状態を作ることができます．

問 2.3. X および H がユニタリ行列であることを示しなさい．

問 2.4. 任意の量子ビット状態 $|\psi\rangle$ に対して，H で時間発展させた後，再び H で時間発展させるとどうなるのか考えなさい．

例 2.5.

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

は**位相反転ゲート**，あるいは Z **ゲート**（やはり σ_z という Pauli 行列の一つ）と呼ばれるユニタリ行列です．式 (2.1) の量子ビットの状態に時間発展 Z を施した後の状態は

$$Z|\psi\rangle = \alpha|0\rangle - \beta|1\rangle$$

と $|1\rangle$ 側の係数の符号が変化します（位相が反転すると言います）．もしこれを計算基底で測定すれば，確率 $|\alpha|^2$ で 0，確率 $|\beta|^2$ で 1 を測定値として得るため，$|\psi\rangle$ を測定したときと変わらず，Z をかけた意味がないように感じるかもしれません．しかし，このような位相の反転は確かに状態を

変化させており，とくに，例 1.6 における $|+\rangle$ および $|-\rangle$ という二つの直交する状態は，

$$Z|+\rangle = Z(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle) = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle = |-\rangle$$

および

$$Z|-\rangle = Z(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle) = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle = |+\rangle$$

となって，Z によって互いに移りあうことがわかります．

問 2.5. $\theta \in [0, 2\pi)$ に対して，

$$|\varphi_\theta\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta}|1\rangle)$$

は時間発展 Z によってどのような状態に変化するでしょうか?また，Bloch 球においてはどのような変化をしているでしょうか？

時間発展と計算基底での測定を組み合わせると，異なる正規直交基底 $\{|\phi_j\rangle\}$ への射影に対応する測定を行うこともできます．つまり，$|\psi\rangle$ を基底 $\{|\phi_j\rangle\}$ を使って

$$|\psi\rangle = \sum_j \alpha'_j |\phi_j\rangle$$

と展開したときに，確率 $|\alpha'_j|^2 = |\langle\phi_j|\psi\rangle|^2$ で測定値 ϕ_j（あるいは j と解釈）が得られて測定後の状態は $|\phi_j\rangle$ になるような測定です．実際，$\{|\phi_j\rangle\}$ から標準基底 $\{|j\rangle\}$ への基底変換に対応するユニタリ行列（$U|\phi_j\rangle = |j\rangle$ で定義される行列 U）を施してから計算基底で測定すればそのような測定と同じ測定値の確率分布が得られます．また，測定後の状態も，測定後に得られている基底状態に $U^\dagger$ を施すことで再現できることになります．

このような異なる正規直交基底での測定は，以下の量子ランダムアクセス符号で見るように，量子ビットから適切な情報を引き出すうえでしばしば有効です．

2.1.4　量子ランダムアクセス符号

1 量子ビットが古典のビットにはない優位性を引き起こす例として，量子ランダムアクセス符号 [2] を紹介します．ランダムアクセス符号とは次のような 2 者間プロトコルです．

定義 2.1 (ランダムアクセス符号). Alice は入力として長さ m のビット列 $x = x_1x_2\cdots x_m$ が与えられ，Bob は入力として添字 $j \in \{1, 2, \ldots, m\}$ が与えられます．お互い相手の入力は知りません（Alice は j を知らないし，Bob は x を知りません）．このとき，Alice が Bob に 1 ビット（1 量子ビット）を送ることで，Bob が常に（どんな x と j であっても）確率 p 以上で x_j を得ることができるような，Alice による m ビットから 1 ビット（1 量子ビット）への符号化を，$(m, 1, p)$ **古典ランダムアクセス符号（量子ランダムアクセス符号）**といいます．

$(2, 1, p)$ 古典ランダムアクセス符号は $p = 1/2$ しか達成できません．つまり，x_j をあてずっぽうで答えることしかできないということです．Alice は Bob の添字が 1 か 2 かわからないまま 1 ビットを送らないといけないので，$j = 1$ のときでも $j = 2$ のときでも $1/2$ を超える確率で x_j を当てることは考えてみれば難しいし，実際不可能であることが証明されています（証明は [2] を参照してください）．

一方，$(2, 1, p)$ 量子ランダムアクセス符号では以下のような符号化で

$$p = \cos^2(\pi/8) = \frac{1}{2} + \frac{1}{2\sqrt{2}} \approx 0.85$$

という高い確率を達成することができます．ただし，$|\varphi(x_1x_2)\rangle$ は Alice が x_1x_2 を持つときに Bob に送る量子ビットの状態です．

$$\begin{aligned}
|\varphi(00)\rangle &= \cos(\pi/8)|0\rangle + \sin(\pi/8)|1\rangle,\\
|\varphi(10)\rangle &= \cos(3\pi/8)|0\rangle + \sin(3\pi/8)|1\rangle,\\
|\varphi(01)\rangle &= \cos(-\pi/8)|0\rangle + \sin(-\pi/8)|1\rangle,\\
|\varphi(11)\rangle &= \cos(5\pi/8)|0\rangle + \sin(5\pi/8)|1\rangle.
\end{aligned}$$

Bob は x_j を復号するために $j = 1$ のとき計算基底で測定します．$j = 2$ のときは正規直交基底 $\{|+\rangle, |-\rangle\}$ で測定し，測定値 $+$ は 0，$-$ は 1 と解釈します．この様子は図 2.3 のように 2 次元実平面上で表現されます．Alice の送ったベクトル $|\varphi(x_1x_2)\rangle$ は，Bob の選んだ測定をなす二つの基底ベクトルのうち，測定値として x_j を出す方のベクトルにより近くなっていることが確認できます．例えば $x = 01$ の場合，Alice は $|\varphi(01)\rangle$ を Bob に送ります．$j = 1$ の場合，Bob は計算基底 $\{|0\rangle, |1\rangle\}$ で測定しますがこのとき $|\varphi(01)\rangle$ は $|0\rangle$ により近く，$|\langle 0|\varphi(01)\rangle|^2 = \cos^2(\pi/8)$ の確率で $x_1 = 0$ を得られます．一方 $j = 2$ の場合，Bob は基底 $\{|+\rangle, |-\rangle\}$ で測定しますがこのとき $|\varphi(01)\rangle$ は $|-\rangle$ により近く，やはり $|\langle -|\varphi(01)\rangle|^2 = \cos^2(\pi/8)$ の確率で $x_2 = 1$ が得られることになります．

注意 2.2. 上記の量子の優位性は，Bob が知りたい 1 ビットを得ることを目的とするランダムアクセス符号の設定に特有のものです．1 量子ビット

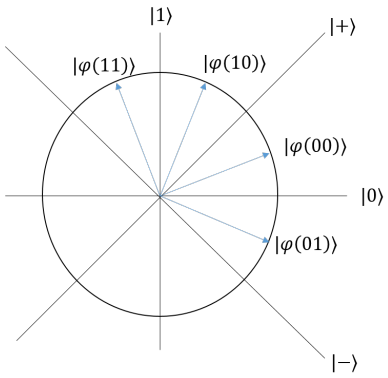

図 2.3: $(2, 1, \cos^2(\pi/8))$ 量子ランダムアクセス符号

が送れるからといって，Alice の 2 ビットの情報を Bob が同時に得られるわけではありません[2]．実際，上記の量子ランダムアクセス符号でも，Bob が片方のビットを得るために測定した後の量子ビットは，もはや $|\varphi(x)\rangle$ とは異なる状態に変化しているために，もう一方のビットの情報は全く得られなくなってしまうのです．つまり，同じ量子ビットの状態に対する計算基底 $\{|0\rangle, |1\rangle\}$ と基底 $\{|+\rangle, |-\rangle\}$ の情報は，**同時測定不可能**ということです．

2.1.5　量子鍵配送

量子ビットが古典ビットと異なる点の一つとして，量子ビットが複製（コピー）できないことがあります．より正確には，未知の量子ビット $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ （ここで未知なのは α および β）を複製して $|\psi\rangle$ を二つ作ることはできないということです．この事実は**量子状態の非複製可能定理 (no-cloning theorem)** と呼ばれています（証明は後述）．

この事実と 2 種類の異なる基底での測定の同時測定不可能性を利用することで，情報理論的に安全な暗号鍵の配送を可能になることが知られています（このような情報理論的に安全な暗号鍵配送は古典情報では不可能です）．ここで暗号鍵配送とは，第 3 者にとってランダムなビット列を 2 者間で共有する方法のことです．量子鍵配送として最もよく知られているのが Bennett と Brassard によって 1984 年に発見されたものであり，BB84 鍵配送プロトコルと呼ばれています．

BB84 鍵配送プロトコル

秘密鍵を共有したい 2 人を Alice, Bob とします

[2]そのようなことは不可能であることも知られています（Holevo の定理）．

1. Alice は，ランダムなビット列を選択したのち，各ビットについてランダムに $+$ か $\times$ かを選択して

- $+$ なら 0 を $|0\rangle$，1 を $|1\rangle$ として Bob へ送信します.
- $\times$ なら 0 を $|0'\rangle := |+\rangle$，1 を $|1'\rangle := |-\rangle$ として Bob へ送信します.

2. Bob は，各ビットについてランダムに $+$ か $\times$ かを選択して

- $+$ なら Alice からの量子ビットを $+$ 基底 $\{|0\rangle, |1\rangle\}$ で測定します.
- $\times$ なら Alice からの量子ビットを $\times$ 基底 $\{|0'\rangle, |1'\rangle\}$ で測定します.

3. Alice と Bob は，各ビットについて $+$ と $\times$ のどっちを選択したかを（電話などで）教えあいます．その結果，選択が一致しなかったビットは捨てます.

4. Alice は，残ったビットの中で半分のビットをランダムに選択して，選択したビットがどれかという情報と，それらのビットの値（0 か 1 か）を Bob に教えます.

5. Bob は，4. で Alice が選択したビットの値が 2. で行った測定の結果と一致しているかどうか（ただし Bob の測定値 $0'$ は 0，測定値 $1'$ は 1 と解釈）をチェックし，一つでも一致していないものがあれば「盗聴者がいる」と認定します.

6. 「盗聴者がいる」と認定されなかった場合，3. で捨てられなかったビットで，かつ 4. で Alice が値をばらさなかったビット達を共有鍵とします.

N を Alice がステップ 1. で用意するランダムビット列の長さとします．まず盗聴者がいないときを考えます．$N = 16$ の場合の例が図 2.4 です．Alice と Bob が選択する基底が一致すれば，ビットの情報は Alice から Bob に正しく伝わることになります．図 2.4 では，$1, 3, 4, 7, 8, 11, 12, 14$ 番目のビットが Alice から Bob に正しく伝わります．ステップ 3. で Alice, Bob が捨てなかったビット（$+$，$\times$ が一致したもの）は，約半分（$= N/2$ ビット）です．これらのうち，ステップ 4. でチェックのため Alice が値を教えるビットは，平均 $N/4$ ビットです．図 2.4 では，$1, 3, 4, 7, 8, 11, 12, 14$ 番目のビットのうち，$1, 4, 8, 14$ 番目のビットがチェックに使用されます．そして，残る平均 $N/4$ ビットが共有鍵となります．図 2.4 では，$3, 7, 11, 12$ 番目のビットからなるビット列 1001 が共有鍵となります.

次に盗聴者 Eve がいる場合を考えます．簡単のため，Eve は Alice が送る量子ビットを，$+$ 基底か $\times$ 基底で当てずっぽうに測定して情報を盗も

Bit	0	1	1	0	1	0	0	0	0	1	0	1	1	0	1	1
A	+	×	+	×	×	+	+	×	+	×	×	+	+	+	×	+
状態	0	1′	1	0′	1′	0	0	0′	0	1′	0′	1	1	0	1′	1
B	+	+	+	×	+	×	+	×	×	+	×	+	×	+	+	×
測	0	0	1	0′	1	0′	0	0′	1′	1	0′	1	0′	0	0	1′

3.		捨			捨	捨			捨	捨			捨		捨	捨
4.	選			選				選						選		
5.	O			O				O						O		
6.			1				0				0	1				

図 2.4: BB84 プロトコル（盗聴者なし）

うとすることにします[3]．$N = 16$ の場合の例が図 2.5 です．ステップ 4. でチェックのために Alice が値を教える K ビット (平均 $N/4$ ビット) のそれぞれは，やはり Alice と Bob で基底（$+$, $\times$）が一致しています．図 2.5 では，$1, 4, 7, 14$ 番目のビットです．ところが，Eve はその一致した基底を知らないので，$1/2$ の確率で

(E) 間違った基底を選択

します．図 2.5 では，$4, 14$ 番目のビットで Eve は間違った基底を選んでしまいました．さらに，間違った基底を選択したという条件 (E) のもとでは，対応するビットは Eve の測定により状態が変化します．例えば，Alice が $+$ 基底から $|0\rangle$ を用意したのに，Eve が $\times$ 基底で測定したとします．すると

$$|0\rangle = \frac{1}{\sqrt{2}}(|0'\rangle + |1'\rangle)$$

より $1/2$ の確率で $|0'\rangle$，$1/2$ の確率で $|1'\rangle$ になってしまいます．これを Bob が $+$ 基底で測定すると

$$|0'\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |1'\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

より，どちらにせよ Bob は $1/2$ の確率で 0 を得て $1/2$ の確率で 1 を得ます．Alice が $+$ 基底から $|1\rangle$ を用意するなどの他の場合も同様です．つまり，条件 (E) のもとでは確率 $1/2$ で

(F)Bob の測定値が Alice のビットと一致しない

[3]実際の安全性証明はもっと一般的な Eve の攻撃とともに通信路で生じるエラーも含めて解析を行う必要があります．

ことになります．図 2.5 では，14 番目のビットで Bob の測定値と Alice のビットは一致していません．ゆえに，4. でチェックのために Alice が値を教える K ビットのそれぞれは，

$$\Pr[E] \times \Pr[F|E] = \frac{1}{4}$$

の確率で Bob の測定値が Alice のビットと異なることになります．以上により，盗聴者 Eve が発見されない確率は，

$$\left(1 - \frac{1}{4}\right)^K$$

となり，N に関して指数的に小さな確率になるというわけです．

Bit	0	1	1	0	1	0	0	0	0	1	0	1	1	0	1	1
A	+	×	+	×	×	+	+	×	+	×	×	+	+	+	×	+
状態	0	1′	1	0′	1′	0	0	0′	0	1′	0′	1	1	0	1′	1
E	+	×	+	+	+	×	+	×	×	×	+	×	+	×	+	×
状態	0	1′	1	0	1	1′	0	0′	0′	1′	0	0′	1	0′	0	0′
B	+	+	+	×	+	×	+	×	×	+	×	+	×	+	+	×
測	0	0	1	0′	1	1′	0	0′	0′	1	1′	1	0′	1	0	0′
3.		捨			捨	捨			捨	捨			捨		捨	捨
4.	選			選				選						選		
5.	O			O				O						×		

図 2.5: BB84 プロトコル（盗聴者あり）

2.2 複数の量子ビット

ビット列の量子版である量子ビット列を紹介します．そのためには，複数の量子状態をどう数学的に表現するかが必要となります．複数の量子状態からなる量子状態とその変化は，テンソル積の概念を使って表現できます．

2.2.1 テンソル積

二項演算 $\otimes$ は，**テンソル積**と呼ばれるベクトル同士の双線形演算で，l 次元ベクトルと m 次元ベクトルから lm 次元のベクトルを，以下のように

作り出します.

$$\begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{l-1} \end{pmatrix} \otimes \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{m-1} \end{pmatrix} := \begin{pmatrix} a_0 b_0 \\ a_0 b_1 \\ \vdots \\ a_0 b_{m-1} \\ a_1 b_0 \\ a_1 b_1 \\ \vdots \\ a_{l-1} b_{m-1} \end{pmatrix}. \tag{2.5}$$

これをケット記法で表すと

$$\left(\sum_{j=0}^{l-1} a_j |j\rangle \right) \otimes \left(\sum_{k=0}^{m-1} b_k |k\rangle \right) := \sum_{j=0}^{l-1} \sum_{k=0}^{m-1} a_j b_k |jm+k\rangle$$

となりますが，式 (2.5) より，$|j\rangle \otimes |k\rangle = |jm+k\rangle$ なので

$$\left(\sum_{j=0}^{l-1} a_j |j\rangle \right) \otimes \left(\sum_{k=0}^{m-1} b_k |k\rangle \right) = \sum_{j=0}^{l-1} \sum_{k=0}^{m-1} a_j b_k |j\rangle \otimes |k\rangle \tag{2.6}$$

となって，テンソル積の双線形性がより明示的になります．$|\psi\rangle \otimes |\phi\rangle$ は $|\psi\rangle|\phi\rangle$，$|\psi, \phi\rangle$，更に誤解がない限りは（後に量子ビット列でそうするように）$|\psi\phi\rangle$ と略することもあります．$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$ と $|\phi\rangle = |\phi_1\rangle \otimes |\phi_2\rangle$（$|\psi_1\rangle$ と $|\phi_1\rangle$，$|\psi_2\rangle$ と $|\phi_2\rangle$ の次元はそれぞれ同じ）の内積は，

$$\langle\psi|\phi\rangle = (\langle\psi_1|\phi_1\rangle)(\langle\psi_2|\phi_2\rangle)$$

と計算されます．また，テンソル積は結合法則が成り立つので，三つ以上のベクトルのテンソル積も

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

のように，テンソル積の順序を表す括弧なしで書かれます．とくに，全ての $j \in \{1, 2, \ldots, m\}$ について $|\psi_j\rangle = |\phi\rangle$ のときは，

$$|\phi\rangle^{\otimes n}$$

と書かれることもあります.

問 2.6. 2 次元ベクトル $|\psi\rangle = 2|0\rangle + |1\rangle$ および 3 次元ベクトル $|\varphi\rangle = |0\rangle - |2\rangle$ に対して，$|\psi\rangle \otimes |\varphi\rangle$ および $|\varphi\rangle \otimes |\psi\rangle$ を求めなさい．さらに，$|\psi\rangle^{\otimes 3}$ を求めなさい.

正規直交基底 $\{|j\rangle\}$ で張られる複素内積空間 $\mathcal{H}_1$ と別の正規直交基底 $\{|k\rangle\}$ で張られる複素内積空間 $\mathcal{H}_2$ に対し，$\{|j\rangle \otimes |k\rangle\}$ で張られる複素内積空間は，$\mathcal{H}_1 \otimes \mathcal{H}_2$ と表します．また

$$\underbrace{\mathcal{H} \otimes \mathcal{H} \otimes \cdots \otimes \mathcal{H}}_{n\text{ 個}}$$

は $\mathcal{H}^{\otimes n}$ と略します．

正規直交基底 $\{|j\rangle\}$ で張られる l 次元複素内積空間 $\mathcal{H}_1$ と，その上で作用する行列 $A = \sum_{j',j} a_{j',j}|j'\rangle\langle j|$ および正規直交基底 $\{|k\rangle\}$ で張られる複素内積空間 $\mathcal{H}_2$ とその上で作用する行列 $B = \sum_{k',k} b_{k',k}|k'\rangle\langle k|$ に対し，lm 次元複素内積空間 $\mathcal{H}_1 \otimes \mathcal{H}_2$ 上の行列 $A \otimes B$ は

$$(A \otimes B)(|j\rangle \otimes |k\rangle) := (A|j\rangle) \otimes (B|k\rangle) \tag{2.7}$$

と定義されます．このことから

$$A \otimes B = \sum_{j',k',j,k} a_{j',j} b_{k',k} |j', k'\rangle\langle j, k| \tag{2.8}$$

と表現できることも容易に確認できます．

さらに行列のテンソル積の概念は自然に正方行列でない行列にも拡張できます．とくに，行または列の個数が 1 の場合，行列はベクトルとみなせるので，$A \otimes |\psi\rangle$ や $\langle\psi| \otimes A$ のような行列とベクトルのテンソル積に対しても同様の定義が拡張できます．

例 2.6. $\{|0\rangle, |1\rangle\}$ で張られる 2 次元内積空間上の行列

$$A = \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}$$

とベクトル $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ に対して，

$$\begin{aligned} A \otimes |\psi\rangle &= (|0\rangle\langle 0| + 2|0\rangle\langle 1| + 3|1\rangle\langle 1|) \otimes (\alpha|0\rangle + \beta|1\rangle) \\ &= \alpha|00\rangle\langle 0| + \beta|01\rangle\langle 0| + 2\alpha|00\rangle\langle 1| + 2\beta|01\rangle\langle 1| + 3\alpha|10\rangle\langle 1| + 3\beta|11\rangle\langle 1| \end{aligned}$$

となります．よって，標準基底での行列表示では

$$A \otimes |\psi\rangle = \begin{pmatrix} \alpha & 2\alpha \\ \beta & 2\beta \\ 0 & 3\alpha \\ 0 & 3\beta \end{pmatrix}$$

となります．

問 2.7.

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

について，$A \otimes B$ および $B \otimes A$ を計算しなさい．

テンソル積同士の積については，以下の事実が成立します．

命題 2.1. $m_1 \times n_1$ 行列 A_1，$m_2 \times n_2$ 行列 B_1，$n_1 \times l_1$ 行列 A_2，$n_2 \times l_2$ 行列 B_2 に対して，

$$(A_1 \otimes B_1)(A_2 \otimes B_2) = (A_1 A_2) \otimes (B_1 B_2).$$

また，$\mathcal{H}_1^{\otimes n}$ 上の行列 $\underbrace{A \otimes A \otimes \cdots \otimes A}_{n \text{ 個}}$ は $A^{\otimes n}$ と略します．

問 2.8. 問 2.7 の A, B に対して，

$$(A \otimes B)^2 = A^2 \otimes B^2$$

であることを確認しなさい．また，$A^{\otimes 2}$ を求めなさい．

2.2.2　テンソル積と複数の量子ビットからなる量子状態

$\mathcal{H}$ を $\{|0\rangle, |1\rangle\}$ で張られる 2 次元複素内積空間とします．このとき，n 個の量子ビットの状態（n 量子ビット状態）は，2^n 次元複素内積空間 $\mathcal{H}^{\otimes n}$ の単位ベクトルとして表されます．つまり，n 個の量子ビット（n 量子ビット）が取りえる状態は，長さ n のビット列 $x \in \{0,1\}^n$ に対応するベクトル $|x\rangle$ の線形結合で表される単位ベクトル

$$|\psi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle \tag{2.9}$$

（ただし，$\sum_{x \in \{0,1\}^n} |\alpha_x|^2 = 1$）で表現されます．ここで x_j を x の第 j ビットとするとき，$|x\rangle$ は

$$|x\rangle = |x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_n\rangle \tag{2.10}$$

を表します．$\{|x\rangle : \ x \in \{0,1\}^n\}$ は $\mathcal{H}^{\otimes n}$ の正規直交基底となっています．式 (2.9) で表される状態 $|\psi\rangle$ は 2^n 個という（量子ビットの個数 n に対して）指数的な個数のビット列の重ね合わせ状態であり，これらに量子力学で認められた操作を一挙に施せるところに量子計算の高速化の一因があります．

例 2.7 (1 量子ビット状態のテンソル積)**.** 二つの 1 量子ビット状態 $|\phi\rangle = a|0\rangle + b|1\rangle$ と $|\psi\rangle = c|0\rangle + d|1\rangle$ からなる 2 量子ビット状態は，テンソル積の双線形性を使うと

$$\begin{aligned}|\phi\rangle \otimes |\psi\rangle &= (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle) \\ &= ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle\end{aligned}$$

となります.

例 2.8 (エンタングルした量子状態)**.** 一般に 2 量子ビットの状態は，二つの 1 量子ビット状態のテンソル積として書けるわけではありません．例えば

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

は EPR 対[4]と呼ばれる 2 量子ビット状態ですが，どんな係数 $\alpha, \beta, \gamma, \delta$ に対しても

$$|\Phi^+\rangle \neq (\alpha|0\rangle + \beta|1\rangle)(\gamma|0\rangle + \delta|1\rangle) \tag{2.11}$$

となることが簡単な計算で確かめられます．このとき，最初の量子ビットと 2 番目の量子ビットは，**エンタングルしている**と呼ばれます．より一般に，n 量子ビット状態 $|\psi\rangle$ が k 量子ビット状態 $|\psi_1\rangle$ と $(n-k)$ 量子ビット状態 $|\psi_2\rangle$ のテンソル積として書けない（つまり $|\psi\rangle = |\psi_1\rangle|\psi_2\rangle$ と書けない）とき，最初の k 個の量子ビットと残りの $(n-k)$ 個の量子ビットはエンタングルしていると呼ばれます．このような**エンタングルメント**と呼ばれる現象は，後に見るように量子力学特有の相関を表していて，重ね合わせの原理と並んで量子計算の計算能力の源とされています.

問 2.9. どんな係数 $\alpha, \beta, \gamma, \delta$ に対しても，式 (2.11) が成り立つことを確かめなさい.

2.2.3 複数の量子ビットの時間発展および測定

複数の量子ビットに認められた操作としては，1 量子ビットの場合と同じく時間発展と測定があります．時間発展は原理的には 2^n 次ユニタリ行列 U を施すことで表現されますので，時間発展によって状態 $|\psi\rangle$ は $U|\psi\rangle$ に変化します.

しかし，計算量理論的な観点で考えると，どんな 2^n 次ユニタリ行列も一発で施せるというのは適当ではありません．そこで通常は，定数個の量子ビットだけを時間発展させるようなユニタリ行列（**基本ゲート**と呼ばれ

[4]EPR は Einstein, Podolsky, Rosen の頭文字です.

る）が認められています．例えば，$|\psi\rangle$ の j 番目の量子ビットに H を施すという操作，つまり，

$$\underbrace{I \otimes I \otimes \cdots \otimes I \otimes \overbrace{H}^{j\text{ 番目}} \otimes I \otimes \cdots \otimes I}_{n\text{ 個}}$$

（I は 2 次単位行列）を行うと，式 (2.9) の状態は

$$\sum_{x \in \{0,1\}^n} \alpha_x |x_1\rangle \otimes \cdots \otimes |x_{j-1}\rangle \otimes (H|x_j\rangle) \otimes |x_{j+1}\rangle \otimes \cdots \otimes |x_n\rangle$$

という状態に変化します．

問 2.10. $a|000\rangle + b|111\rangle$ の 2 番目の量子ビットに H を施した後の状態を求めなさい．

同様に，j 番目と k 番目の量子ビットに（j 番目を最初の量子ビット，k 番目を 2 番目の量子ビットとして）作用する行列 U を考えると，式（2.9）における各ベクトル $|x\rangle$ 中の $|x_j\rangle$ および $|x_k\rangle$ のテンソル積 $|x_j\rangle|x_k\rangle$ が $U(|x_j\rangle|x_k\rangle)$ に置き換えられた状態に変化することになります．

例 2.9. CNOT ゲート $C\text{-}X$ は 2 量子ビットに作用するユニタリ行列で $|x_1x_2\rangle$ を $|x_1\rangle|x_1 \oplus x_2\rangle$ に変化させます（ここで $\oplus$ は排他的論理和です）．標準基底での行列表示は，

$$C\text{-}X = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

です．x_1 を条件として x_2 を反転するか否かが決められるため，最初の量子ビットは条件量子ビット (controlled qubit)，2 番目の量子ビットは標的量子ビット (target qubit) と呼ばれます．図 2.6 の左辺ないし右辺のように表現されることが多く，黒丸がついた側が条件量子ビットを表します．例えば，

$$\frac{1}{\sqrt{2}}(|010\rangle + |011\rangle)$$

の第 2 量子ビットを標的量子ビット，第 3 量子ビットを条件量子ビットとして，CNOT ゲートを施すと

$$\frac{1}{\sqrt{2}}(|010\rangle + |001\rangle)$$

に変化します．

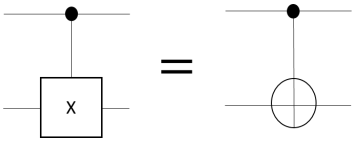

図 2.6: CNOT ゲート

問 2.11.

$$\frac{1}{\sqrt{3}}(|100\rangle + |010\rangle - |111\rangle)$$

の第 1 量子ビットを条件量子ビット，第 3 量子ビットを標的量子ビットとして CNOT を施した後の状態を求めなさい．

基本的な測定は，各量子ビットを計算基底 $\{|0\rangle, |1\rangle\}$ で測定するものです．式 (2.9) の状態を計算基底で測定することは，正規直交基底 $\{|x\rangle : x \in \{0,1\}^n\}$ への射影に対応する測定を意味します．つまり，確率 $|\alpha_x|^2$ で測定値 x が得られて測定後の状態は $|x\rangle$ になります．

例 2.10. 2 量子ビット状態

$$|\varphi\rangle = (\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes (\beta_0|0\rangle + \beta_1|1\rangle) \tag{2.12}$$

を計算基底で測定すると，

$$|\varphi\rangle = \alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle$$

なので，以下のように変化します．

- 確率 $|\alpha_0\beta_0|^2$ で，測定値 00 を得て，測定後の状態は $|00\rangle$ になる
- 確率 $|\alpha_0\beta_1|^2$ で，測定値 01 を得て，測定後の状態は $|01\rangle$ になる
- 確率 $|\alpha_1\beta_0|^2$ で，測定値 10 を得て，測定後の状態は $|10\rangle$ になる
- 確率 $|\alpha_1\beta_1|^2$ で，測定値 11 を得て，測定後の状態は $|11\rangle$ になる

これは，式 (2.12) の各量子ビットを計算基底で測定したときの各確率の積 $|\alpha_j|^2|\beta_k|^2$ で，対応する測定値 jk を得て測定後の状態が $|jk\rangle$ になることを示しています．これは最初の量子ビットと 2 番目の量子ビットがテンソル積で書かれていて，相関がないことによる測定の独立性によるものです．

より一般に，任意の正規直交基底 $\{|\phi_x\rangle : x \in \{0,1\}^n\}$ への射影に対応する測定による確率分布を得ることは，1 量子ビットの場合と同様に，$\{|\phi_x\rangle : x \in \{0,1\}^n\}$ から $\{|x\rangle : x \in \{0,1\}^n\}$ への基底変換に対応するユニタリ行列 U を行ってから，計算基底で測定することで原理的に実現可能です．ただし，計算量的な効率を鑑みると，U が多項式個の基本ゲートで表現できることが必要となるため，実際には限られたものしか効率的に実現できません．

2.2.4　量子状態の非複製不可能定理の証明

ここで，未知の量子ビット $|\psi\rangle = a|0\rangle + b|1\rangle$ が複製できないことの証明を与えます．

もしそのような複製が可能とすると，ある 2^{m+1} 次ユニタリ行列 U と補助の m 量子ビット状態 $|\phi_0\rangle$ が存在して，どんな $|\psi\rangle, |\psi'\rangle$ についても

$$U(|\psi\rangle|\phi_0\rangle) = |\psi\rangle|\psi\rangle|g(\psi)\rangle \tag{2.13}$$

および

$$U(|\psi'\rangle|\phi_0\rangle) = |\psi'\rangle|\psi'\rangle|g(\psi')\rangle \tag{2.14}$$

となるべきです（$|g(\psi)\rangle, |g(\psi)\rangle$ はなんらかの $(m-1)$ 量子ビット状態）．ところが，$0 < |\langle\psi|\psi'\rangle| < 1$ なる $|\psi\rangle, |\psi'\rangle$ を考えると式 (2.13) および (2.14) の左辺の内積の絶対値は

$$|(U|\psi\rangle|\phi_0\rangle)^\dagger (U|\psi'\rangle|\phi_0\rangle)| = |\langle\psi|\psi'\rangle|$$

なのに対して，右辺の絶対値の内積は

$$\begin{aligned} |(|\psi\rangle|\psi\rangle|g(\psi)\rangle)^\dagger (|\psi'\rangle|\psi'\rangle|g(\psi')\rangle| &= |\langle\psi|\psi'\rangle|^2 |\langle g(\psi)|g(\psi')\rangle|^2 \\ &\leq |\langle\psi|\psi'\rangle|^2 \\ &< |\langle\psi|\psi'\rangle| \end{aligned}$$

となるので，等式 (2.13) および (2.14) に矛盾します．

2.2.5　量子状態の部分測定

複数の量子ビットからなる状態においては，量子ビットを**部分的に測定**することも可能です．例えば，n 個の量子ビットのうち，最初の k 個の量子ビットを計算基底で測定することを考えます．このときどんな変化が起こるかを表現するには，式 (2.9) の状態を最初の k 個の量子ビットの値毎にまとめるとよいです．実際，式 (2.9) は

$$|\psi\rangle = \sum_{y\in\{0,1\}^k, z\in\{0,1\}^{n-k}} \alpha_{yz}|y\rangle \otimes |z\rangle = \sum_{y\in\{0,1\}^k} |y\rangle \otimes |\psi_y\rangle$$

（ただし，$|\psi_y\rangle = \sum_{z\in\{0,1\}^{n-k}} \alpha_{yz}|z\rangle$）と書き直すことができます．このとき，$|\psi\rangle$ の最初の k 量子ビットを計算基底で測定すると，確率 $\||\psi_y\rangle\|^2$ で測定値 y を得て，測定後の状態は

$$|y\rangle \otimes \frac{|\psi_y\rangle}{\||\psi_y\rangle\|}$$

になります ($\||\psi_y\rangle\|$ で割るのは測定後の状態が単位ベクトルになるための正規化です)．

例 2.11 (3 量子ビット状態における部分測定の例)**.**

$$|\psi\rangle = \frac{1}{\sqrt{3}}|000\rangle + \frac{1}{\sqrt{3}}|011\rangle + \frac{1}{\sqrt{3}}|111\rangle$$

の最初の 1 量子ビットを計算基底で測定することを考えます．このとき，

$$|\psi\rangle = |0\rangle \otimes \left(\frac{1}{\sqrt{3}}|00\rangle + \frac{1}{\sqrt{3}}|11\rangle\right) + |1\rangle \otimes \frac{1}{\sqrt{3}}|11\rangle$$

と書き直せるので，測定により確率 $\|\frac{1}{\sqrt{3}}|00\rangle + \frac{1}{\sqrt{3}}|11\rangle\|^2 = 2/3$ で測定値 0 を得て測定後の状態が

$$|0\rangle \otimes \frac{\left(\frac{1}{\sqrt{3}}|00\rangle + \frac{1}{\sqrt{3}}|11\rangle\right)}{\sqrt{2/3}} = |0\rangle \otimes \left(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle\right)$$

となるか，確率 $\|\frac{1}{\sqrt{3}}|11\rangle\|^2 = 1/3$ で測定値 1 を得て測定後の状態が

$$|1\rangle \otimes \frac{\frac{1}{\sqrt{3}}|11\rangle}{\sqrt{1/3}} = |1\rangle \otimes |11\rangle$$

$(= |111\rangle)$ となります.

問 2.12.

$$|\psi\rangle = \frac{1}{3}(|001\rangle + 2|010\rangle - 2|100\rangle)$$

の最初の量子ビットを計算基底で測定したとき，$|\psi\rangle$ はどのように変化するのかを述べなさい.

より一般に，最初の k 量子ビットを正規直交基底 $\{|\phi_y\rangle : y \in \{0,1\}^k\}$ で測定する場合，式 (2.9) は

$$|\psi\rangle = \sum_{y\in\{0,1\}^k} |\phi_y\rangle|\psi_y\rangle$$

の形に書き直すことができて，測定によって確率 $\||\psi_y\rangle\|^2$ で測定値 ϕ_y（または y と解釈）を得て測定後の状態は

$$|\phi_y\rangle \otimes \frac{|\psi_y\rangle}{\||\psi_y\rangle\|}$$

になります.

問 2.13. 2 量子ビット状態

$$|\psi\rangle = a|+\rangle|+\rangle + b|-\rangle|-\rangle$$

の最初の量子ビットを $\{|+\rangle, |-\rangle\}$ で測定したときに $+$ を測定する確率と $+$ を測定した後の状態を求めなさい．また，最初の量子ビットを計算基底で測定したときに 0 を得る確率と 0 を得た後の状態を求めなさい.

2.2.6　CHSH ゲーム

エンタングルメントは，測定による状態変化の観点から見ると，ある種の相関があることを示すものといえます．実際，2 量子ビット状態が $|\phi\rangle \otimes |\psi\rangle$ と書かれているときは，第 1 量子ビットの測定は（上記で与えた測定の定義からわかるように）第 2 量子ビットになんら影響を与えませんが，EPR 対 $|\Phi^+\rangle$ の第 1 量子ビットを計算基底で測定すると，確率 1/2 で 0 あるいは 1 が測定されて，測定後の状態は 0 を得たときは $|00\rangle$，1 を得たときは $|11\rangle$ となって第 2 量子ビットの状態も変化させてしまいます．

もっと驚くことに，$|\Phi^+\rangle$ は任意の実ベクトルによる正規直交基底 $\{|\phi_0\rangle, |\phi_1\rangle\}$ に対して

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}|\phi_0\rangle|\phi_0\rangle + \frac{1}{\sqrt{2}}|\phi_1\rangle|\phi_1\rangle \tag{2.15}$$

と表現され，それ故に $|\Phi^+\rangle$ の第 1 量子ビットを正規直交基底 $\{|\phi_0\rangle, |\phi_1\rangle\}$ で測定すると，測定後に第 1 量子ビットと同じ状態が第 2 量子ビットにも出現することになります．

問 2.14. 式 (2.15) を証明しなさい．また，$\{|\phi_0\rangle, |\phi_1\rangle\}$ が複素ベクトルによる正規直交系の場合に式 (2.15) はどうなるかを検討しなさい．

上記の擬似的テレパシーとも呼べるようなエンタングルメントの特質を利用したゲームとして，よく知られるのが CHSH ゲームです[5]．これは Alice，Bob，検証者の 3 名による次のようなゲームです．

定義 2.2. [CHSH ゲーム] ゲームは Alice と Bob の組対検証者で行われます．Alice と Bob はゲームの開始前はどんなことをしてもよいのですが，ゲームが始まったら通信が許されません．検証者が $x \in \{0, 1\}$ を Alice，$y \in \{0, 1\}$ を Bob に一様ランダムに送ることでゲームは始まります．Alice は $a \in \{0, 1\}$ を検証者に送り，Bob は $b \in \{0, 1\}$ を検証者に送ります．

$$x \wedge y = a \oplus b$$

が成立すれば Alice と Bob の組が勝ちで，成立しなければ検証者の勝ちです．ここで $\wedge$ は論理積を表します．

古典的な戦略でこのゲームに Alice と Bob の組が勝てる確率は，0.75 であることが知られています．一方で，Alice と Bob が量子的な戦略を取れる場合は，次のようにしてより良い勝率 $\cos^2(\pi/8) \approx 0.85$ を達成できます．

CHSH ゲームに対する量子プロトコル

[5] CHSH は Clauser, Horne, Shimony, Holt という 4 名の物理学者の頭文字です．

1. Alice と Bob はゲームの開始前に $|\Phi^+\rangle$ を共有します（第 1 量子ビットは Alice が所有し，第 2 量子ビットは Bob が所有します）．この共有は Alice が $|\Phi^+\rangle$ を準備して，その第 2 量子ビットを Bob に送る（ゲーム開始前なので量子ビットの送信も許されます）ことで実現されます．

2. Alice は正規直交基底

$$\{|\phi_0\rangle := |\varphi(0x)\rangle, |\phi_1\rangle := |\varphi(1\overline{x})\rangle\}$$

（$\overline{x}$ はビット値 x を反転したビット値）で測定して，その測定値を $a \in \{0,1\}$ とします（ϕ_a を a と解釈）．ただし，$|\varphi(x_1x_2)\rangle$ は図 2.3 の量子ランダムアクセス符号です．Bob は $y=0$ のときは計算基底で測定し，$y=1$ のときは正規直交基底 $\{|+\rangle, |-\rangle\}$ で測定して，その測定値を $b \in \{0,1\}$ とします（$+$ を 0，$-$ を 1 と解釈します）．

以下では $c = a \oplus x$ とおきます．式 (2.15) より Alice の測定値が a であるときの Bob の状態は

$$|\varphi(ac)\rangle$$

となります．$b = a \oplus (x \wedge y)$ となれば Alice と Bob は勝てることに注意すると，$y=0$ のときは $b=a$ となれば彼らは勝つことになります．Bob は量子ランダムアクセス符号 $|\varphi(ac)\rangle$ を持っていて，計算基底で測定（ac の第 1 ビット目 a を復号する測定）するので確率 $\cos^2(\pi/8)$ で $b=a$ を得ることになります．同様に，$y=1$ のときは $b = a \oplus x$ となれば彼らは勝つことになりますが，今度は $\{|+\rangle, |-\rangle\}$ で測定（ac の第 2 ビット目 $c = a \oplus x$ を復号する測定）するので，やはり確率 $\cos^2(\pi/8)$ で $b = a \oplus x$ を得ることになります．

CHSH ゲームにおいて古典の最高勝率 0.75 を達成する方法は，Alice と Bob が何も考えず $a=b=0$ を送ることです．つまり，古典においては Alice と Bob は開始前にどんな相関を用意してもこのゲームにおいては無意味です．一方で，量子においては上記で見たように，EPR 対が量子ランダムアクセス符号の状態に関する Alice から Bob への擬似的テレパシーを可能にするため，古典を上回る勝率を達成できるのです．

2.2.7 量子テレポーテーション

部分測定の興味深い応用例として量子テレポーテーションがあります．量子テレポーテーションは最も基本的な量子情報処理の一つであり，様々な形でより複雑な量子情報処理の構築に役立っています．

設定 Alice は量子ビット $|\psi\rangle = a|0\rangle + b|1\rangle$ を持っています．Alice も Bob も $|\psi\rangle$ について未知です（a, b を知りません）．ただし，Alice と Bob は事前に EPR ペア $|\Phi^+\rangle$ を共有しています．
目的 Alice と Bob が量子通信（つまり量子状態を送ること）を行わず，Alice から Bob への 2 ビットの古典通信だけで，$|\psi\rangle$ を Alice から Bob に移動させることです．

量子テレポーテーションのプロトコルは以下のようです．ただし，以下で $A1$ は Alice が持つ $|\psi\rangle$ に対応する量子ビット，$A2$ は Alice が持つ $|\Phi^+\rangle$ の片割れに対応する量子ビット，B は Bob が持つ $|\Phi^+\rangle$ の片割れに対応する量子ビットとします．

量子テレポーテーションプロトコル

1. Alice は $A1, A2$ を **Bell 基底**と呼ばれる以下の正規直交基底

$$|\Phi^+\rangle = \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad |\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$
$$|\Psi^+\rangle = \tfrac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \quad |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

で測定します．測定値 $\Phi^+, \Phi^-, \Psi^+, \Psi^-$ を $00, 01, 10, 11$ と解釈した後，得られた 2 ビットを Bob に送ります．

2. Bob は B に次の操作を行います．

- 00 を受け取ったときは何もしない．
- 01 を受け取ったときは Z を施す．
- 10 を受け取ったときは X を施す．
- 11 を受け取ったときは Z を施してからさらに X を施す．

ポイントは Alice と Bob の量子ビット状態 $|\psi\rangle|\Phi^+\rangle$ が

$$\begin{aligned}|\psi\rangle|\Phi^+\rangle = \frac{1}{2}\big(&|\Phi^+\rangle(a|0\rangle + b|1\rangle) + |\Phi^-\rangle(a|0\rangle - b|1\rangle) \\ &+|\Psi^+\rangle(a|1\rangle + b|0\rangle) + |\Psi^-\rangle(a|1\rangle - b|0\rangle)\big)\end{aligned} \tag{2.16}$$

と書き直せるところにあります．そのため，Alice の Bell 基底による測定は Bob の状態を

$$a|x\rangle + (-1)^y b|1-x\rangle$$

に射影し，Bob は「誤り」$xy \in \{0,1\}^2$ を Alice からの 2 ビットで修正できることになります．

問 2.15. 式 (2.16) が成り立つことを確認しなさい．

2.3 観測量

これまでの射影を使った測定によると，正規直交系 $\{|\psi_j\rangle\}$ での測定によって状態 $|\phi\rangle$ を測定したとき，$|\langle\psi_j|\phi\rangle|^2$ の確率で測定値 ψ_j が得られて，測定後の状態は $|\psi_j\rangle$ となります．一方で，ψ_j はしばしば実数 $f(\psi_j)$ への読み替えを行ってきました．このような読み替えを含めた測定は，エルミート作用素

$$A = \sum_j f(\psi_j)|\psi_j\rangle\langle\psi_j|$$

に対応すると考えられます．このとき，A は**観測量 (observable)** と呼ばれ，読み替えを含めた測定は「$|\psi\rangle$ を観測量 A で測定する」と表現します．観測量の概念を使うことで測定値の期待値が

$$\langle A\rangle := \langle\psi|A|\psi\rangle$$

と表せます．

例 2.12. ユニタリ行列として紹介した Z はエルミート行列でもあり，例 1.5 および例 1.6 で紹介したように

$$Z = |0\rangle\langle 0| - |1\rangle\langle 1|$$

というスペクトル分解を持っています．つまり Z は観測量でもあり，計算基底 $\{|0\rangle, |1\rangle\}$ で測定して，$b \in \{0, 1\}$ が得られたら $(-1)^b$ を測定値とするという観測量に対応しています．このとき，状態 $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ を観測量 Z で測定したときの測定値の期待値は

$$\langle Z\rangle = \langle\psi|Z|\psi\rangle = |\alpha|^2 - |\beta|^2$$

となります．

同様に，

$$X = |+\rangle\langle +| - |-\rangle\langle -|$$

は，正規直交基底 $\{|+\rangle, |-\rangle\}$ で測定して，$+$ が得られたら $+1$, $-$ が得られたら -1 を測定値とする観測量に対応しています．このため，$\{|0\rangle, |1\rangle\}$ で測定することは（主に物理出身の研究者により）「Z 基底で測る」，$\{|+\rangle, |-\rangle\}$ で測定することは「X 基底で測る」と呼ばれることもあります．

Pauli 行列 σ_y として Z, X とともに出てくる観測量が

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

です．$|+'\rangle := \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$ および $|-'\rangle := \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$ としたとき，Y は

$$Y = |+'\rangle\langle+'| - |-'\rangle\langle-'|$$

とスペクトル分解できます．

問 2.16. 状態

$$|\psi_\theta\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta}|1\rangle)$$

（θ は実数）の観測量 Y で測定したときの測定値の期待値を求めなさい．

さらに二つ以上の観測量 $A_1, \ldots, A_m$ が互いに交換可能，つまり同じ正規直交系 $\{|\psi_j\rangle\}$ を使ってスペクトル分解可能（同時対角化可能）である場合は，$A_1, \ldots, A_m$ の測定順序によってそれらの測定値が変化することはありません．これは $A_1, \ldots, A_m$ が同時測定可能であることを意味します．

例 2.13. 観測量 X と A

$$A = \begin{pmatrix} 3 & -1 \\ -1 & 3 \end{pmatrix}$$

は，$AX = XA$ をみたすので交換可能です．よって，A で測定してから X で測定しても，X で測定してから A で測定してもそれらの測定値は不変です．実際，A も X と同じ正規直交基底 $\{|+\rangle, |-\rangle\}$ で

$$A = 2|+\rangle\langle+| + 4|-\rangle\langle-|$$

とスペクトル分解できます．任意の量子ビット状態 $|\psi\rangle$ は正規直交基底 $\{|+\rangle, |-\rangle\}$ で

$$|\psi\rangle = \alpha|+\rangle + \beta|-\rangle \tag{2.17}$$

と表せるので，A で測定してから X で測定したとき，測定値は以下のようになります．

- 確率 $|\alpha|^2$ で A の測定値が 2 で X の測定値は 1.[6]
- 確率 $|\beta|^2$ で A の測定値 4 で X の測定値は -1.

一方，X で測定してから A で測定したとき，測定値は以下のようになり，全く同じです．

- 確率 $|\alpha|^2$ で X の測定値は 1 で A の測定値が 2.[7]
- 確率 $|\beta|^2$ で X の測定値は -1 で A の測定値は 4.

[6] A の測定後の状態は確率 $|\alpha|^2$ で $|+\rangle$ になり，$|+\rangle$ において X を測定するので確実に測定値 1 を得ることになります．

[7] X の測定後の状態は確率 $|\alpha|^2$ で $|+\rangle$ になり，$|+\rangle$ において A を測定するので確実に測定値 2 を得ることになります．

2.3.1 Magic-Square ゲーム

CHSH ゲームは量子と古典で勝率に差があるゲームの例を示していますが，量子でも確率 1 で勝てるわけではありません．以下のゲームは古典では確率 1 で勝てないが，量子では確率 1 で勝てるゲームの例です．

定義 2.3. [Magic-Square ゲーム] ゲームは Alice と Bob の組対検証者で行われます．Alice と Bob はゲームの開始前はどんなことをしてもよいのですが，ゲームが始まったら通信は許されません．検証者は（成分が $0,1$ からなる 3×3 行列に対応する）「行番号」$s\in\{1,2,3\}$ を Alice,「列番号」$t\in\{1,2,3\}$ を Bob に一様ランダムに送ることでゲームは始まります．Alice は $a_1a_2a_3\in\{0,1\}^3$ を検証者に送り，Bob は $b_1b_2b_3\in\{0,1\}$ を検証者に送ります．以下の 2 条件がみたされれば Alice と Bob の組が勝ちで，どちらかでもみたされなければ検証者の勝ちです．

1. $a_1\oplus a_2\oplus a_3=0$（$s$ 行の成分のパリティは 0）かつ $b_1\oplus b_2\oplus b_3=1$（$t$ 列の成分のパリティは 1）
2. $a_t=b_s$（Alice と Bob が送ってきた二つの (s,t) 成分は等しい）

古典では Alice と Bob がこのゲームに勝てる確率は $8/9$ です（成分が $0,1$ からなる 3×3 行列で全ての行の成分のパリティが 0 かつ全ての列の成分のパリティが 1 になることはありえない）．

一方で，量子では驚いたことに Alice と Bob に必勝戦略が存在します．以下が量子での必勝戦略です．

Magic-Square ゲームに対する量子プロトコル

1. Alice と Bob はゲームの開始前に

$$|\Psi^-\rangle_{A_1B_1}\otimes|\Psi^-\rangle_{A_2B_2}$$

を共有します（添え字 A_1,B_1,A_2,B_2 は量子ビットの名前です）．ただし，

$$|\Psi^-\rangle:=\frac{1}{\sqrt{2}}(|01\rangle-|10\rangle)$$

であり，A_1,A_2 は Alice が所有し，B_1,B_2 は Bob が所有します．

2. Alice，Bob はそれぞれ A_1A_2，B_1B_2 上で表 2.1 の中で s,t に応じた行列にある三つの観測量をそれぞれ測定します．Alice の j 列（Bob の i 行）に対応する測定値 $(+1$ か $-1)$ が α_j（β_i）なら，$\alpha_j=(-1)^{a_j}$（$\beta_i=(-1)^{b_i}$）となるように a_j（b_i）を取ります．

行 \ 列	$t=1$	$t=2$	$t=3$
$s=1$	$X\otimes X$	$Y\otimes Z$	$Z\otimes Y$
$s=2$	$Y\otimes Y$	$Z\otimes X$	$X\otimes Z$
$s=3$	$Z\otimes Z$	$X\otimes Y$	$Y\otimes X$

表 2.1: (s,t) に応じた観測量

勝利の条件のうち，まずは一つ目の条件がみたされることを確認します．各行の三つの観測量は互いに交換するので同時測定可能です．そのため，それらをどういう順で測定しても観測結果は変わりません．また三つの観測量の積は $I\otimes I$ なので，Alice の測定値の積 $\alpha_1\alpha_2\alpha_3$ は $+1$ です．よって $a_1\oplus a_2\oplus a_3=0$ となります．同様に，各列の三つの観測量も考えられますが，測定値の積は $-I\otimes I$ なので $b_1\oplus b_2\oplus b_3=1$ となります．

次に二つ目の条件がみたされることを確認します．$|\Psi^-\rangle_{A_1B_1}\otimes|\Psi^-\rangle_{A_2B_2}$ を Alice，Bob とも (s,t) 成分に対応する観測量 $P_1\otimes P_2$ を測ったとします．A_1 上の P_1 の測定値に対応するビットを a', A_2 上の P_2 の測定値に対応するビットを a'' とすると $a_t=a'\oplus a''$ です．B_1 上の P_1 の測定値に対応するビットを b', B_2 上の P_2 の測定値に対応するビットを b'' とすると $b_s=b'\oplus b''$ です．また，$|\Psi^-\rangle_{A_1B_1}$ は観測量 $P_1\otimes P_1$ を，$|\Psi^-\rangle_{A_2B_2}$ は観測量 $P_2\otimes P_2$ を測ることになるので

$$(X\otimes X)|\Psi^-\rangle=(Y\otimes Y)|\Psi^-\rangle=(Z\otimes Z)|\Psi^-\rangle=-|\Psi^-\rangle$$

から $a'\oplus b'=1$ かつ $a''\oplus b''=1$ となります．以上より，

$$a_t\oplus b_s=a'\oplus a''\oplus b'\oplus b''=0$$

が得られます．

問 2.17. 表 2.1 の各行の三つの観測量が互いに交換することを以下の事実を使って確認しなさい．

$$XY=-YX=iZ,\quad YZ=-ZY=iX,\quad ZX=-XZ=iY.$$

2.4　混合状態

混合状態 (mixed state) は量子状態の確率分布に対応するものです．

例 2.14. 確率 0.2 で $|+\rangle$，確率 0.3 で $|0\rangle$，確率 0.5 で $|-\rangle$ にあるような量子状態の確率分布は，混合状態

$$\{(0.2,|+\rangle),(0.3,|0\rangle),(0.5,|-\rangle)\}$$

にあるといいます.

より一般には，確率 p_j で状態 $|\psi_j\rangle$ を取るような場合，その状態は混合状態 $\{(p_j, |\psi_j\rangle)\}_j$ にあるといいます.

混合状態は**密度行列 (density matrix)** というエルミート行列で表現できます．混合状態 $\{(p_j, |\psi_j\rangle)\}_j$ は密度行列

$$\sigma = \sum_j p_j |\psi_j\rangle\langle\psi_j| \tag{2.18}$$

で表現されます．とくに量子状態 $|\psi\rangle$ は「確率 1 で $|\psi\rangle$ を取る混合状態」とみなせるので，密度行列で表現すると

$$|\psi\rangle\langle\psi| \tag{2.19}$$

と表されます．$|\psi\rangle$ のような状態（あるいは式 (2.19) で表現されるような混合状態）は，一般の混合状態と区別したいとき，**純粋状態 (pure state)** と呼ばれます.

例 2.15. $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$ のとき，その密度行列は

$$|\psi\rangle\langle\psi| = \frac{1}{2}(|0\rangle + i|1\rangle)(\langle 0| - i\langle 1|) = \frac{1}{2}\begin{pmatrix} 1 & -i \\ i & 1 \end{pmatrix}$$

となります．また，注意 2.1 に記したように $|\psi\rangle$ と $e^{i\theta}|\psi\rangle$ は任意の θ について同じ量子状態を表していますが，数学的表現としては異なります．しかし，密度行列では

$$|\psi\rangle\langle\psi| = (e^{i\theta}|\psi\rangle)(e^{-i\theta}\langle\psi|)$$

となるため，同じ数学的表現になります.

密度行列は以下のように特徴付けられます.

定理 2.2. ρ が密度行列であることと，以下の 2 条件が成り立つことは，必要十分である.

1. $\mathrm{tr}(\rho) = 1$
2. $\rho \geq 0$

時間発展 U により，混合状態 $\{(p_j, |\psi_j\rangle)\}_j$ が $\{(p_j, U|\psi_j\rangle)\}_j$ に変化したとき，対応する密度行列は

$$U\sigma U^\dagger = \sum_j p_j U|\psi_j\rangle\langle\psi_j|U^\dagger$$

です．また正規直交基底 $\{|k\rangle\}$ で混合状態 $\{(p_j, |\psi_j\rangle)\}_j$ を測定すると，測定値 k を得る確率は

$$\sum_j p_j |\langle k|\psi_j\rangle|^2 \tag{2.20}$$

ですが，この確率は密度行列

$$\sigma = \sum_j p_j |\psi_j\rangle\langle\psi_j|$$

を使って

$$\langle k|\sigma|k\rangle \tag{2.21}$$

と書けることが確認できます．

問 2.18. 式 (2.20) と式 (2.21) が等しいことを確認しなさい．

とくに，N 次元正規直交基底 $\{|\psi_j\rangle\}$ の各ベクトルを一様ランダムに選んだ混合状態は**完全混合状態 (totally mixed state)** と呼ばれ，密度行列は

$$\sum_j \frac{1}{N}|\psi_j\rangle\langle\psi_j| = \frac{1}{N}\sum_j |\psi_j\rangle\langle\psi_j| = \frac{1}{N}I$$

となります．上式の最後の等号は完備関係式によります．完全混合状態はその系の状態が一様にランダムであることを示しています．

2.4.1　1 量子ビットの密度行列と量子ワンタイムパッド

1 量子ビットの純粋状態 $|\psi\rangle$ は式 (2.4) で与えられたので，これをもとに $|\psi\rangle\langle\psi|$ を計算して，(2 次複素行列がなす空間の）基底 I, X, Y, Z で展開すると

$$|\psi\rangle\langle\psi| = \frac{1}{2}(I + (\cos\gamma\sin\theta)X + (\sin\gamma\sin\theta)Y + (\cos\theta)Z) \tag{2.22}$$

となります．これによって Bloch 球上の点 $(\cos\gamma\sin\theta, \sin\gamma\sin\theta, \cos\theta)$ は密度行列の表現 (2.22) における X, Y, Z の係数であることがわかります．

また任意の 1 量子ビットの混合状態 ρ は純粋状態を表す密度行列の凸結合であることから，Bloch 球の内部の点 (a, b, c)（ただし，$a^2+b^2+c^2 \leq 1$）に対応します．とくに完全混合状態 $I/2$ は原点 $(0, 0, 0)$ に対応することになります．

上記の事実を使ってワンタイムパッドの 1 量子ビット版を考えることができます．(1 ビットの）ワンタイムパッドとは共有のランダムビット $r \in \{0, 1\}$ をもつ Alice と Bob が Alice から Bob へ 1 ビット b を第 3 者に

知られることなく安全に送る方法です．Alice は $b' := r \oplus b$ を通信路を通じて Bob に送り，Bob は $b' \oplus r = b$ と計算することで b を得ますが，通信路を盗聴する第 3 者は r を知らないので第 3 者にとって b' はランダムビットとなるというものです．

では Alice がもつ量子ビット $\rho = (1/2)(I + aX + bY + cZ)$ を Bob へ第 3 者に知られることなく安全に送るにはどうすればよいでしょうか．この場合，Alice と Bob は 2 ビット $r \in \{0,1\}^2$ を共有していれば以下のプロトコルを実行することができます．

1 量子ビットに対するワンタイムパッド

1. Alice は，共有の 2 ビット r に応じて ρ に以下のユニタリ行列を施してから Bob に量子通信を通じて送信する．

- $r = 00$ のとき I
- $r = 01$ のとき X
- $r = 10$ のとき Y
- $r = 11$ のとき Z

2. 受け取った状態 ρ に対して Bob は，r に応じて Alice と同じユニタリ行列を施す．

上記のプロトコルで Bob が正しい状態 ρ を受け取ることは $I^2 = X^2 = Y^2 = Z^2 = I$ であることから明らかとなります．一方で第 3 者は r を知らないので量子通信路を通る状態は

$$\rho' := \frac{1}{4}(\rho + X\rho X^\dagger + Y\rho Y^\dagger + Z\rho Z^\dagger)$$

となります．実は $\rho' = I/2$ です．ブロッホ球で点 (a,b,c) に対応する状態は

- X によって $(a,-b,-c)$
- Y によって $(-a,b,-c)$
- Z によって $(-a,-b,c)$

に対応する状態に移されることが簡単な計算で確認できます．よって，ρ' は

$$\frac{1}{4}\left[(a,b,c) + (a,-b,-c) + (-a,b,-c) + (-a,-b,c)\right] = (0,0,0)$$

に対応する状態，すなわち完全混合状態 $I/2$ となるわけです．よって第 3 者にとっては量子通信路を通る状態はランダムな 1 量子ビット状態となります．

2.4.2　部分トレースと混合状態

m 次元複素内積空間 $\mathcal{H}_1$ と n 次元複素内積空間 $\mathcal{H}_2$ のテンソル積空間 $\mathcal{H}_1 \otimes \mathcal{H}_2$ 上の行列 A に対して，A のトレースは

$$\mathrm{tr}(A) = \sum_{j=1}^{m}\sum_{k=1}^{n}(\langle j| \otimes \langle k|)A(|j\rangle \otimes |k\rangle)$$

となります．ただし，$\{|j\rangle\}$ は $\mathcal{H}_1$ の正規直交基底，$\{|k\rangle\}$ は $\mathcal{H}_2$ の正規直交基底です．これに対して A の $\mathcal{H}_1$ 上の**部分トレース (partial trace)** とは，

$$\mathrm{tr}_1(A) = \sum_{j=1}^{m}(\langle j| \otimes I)A(|j\rangle \otimes I)$$

で定義されます．

量子状態の部分系は部分トレースを使って表現されます．$\mathcal{H}_A$ と $\mathcal{H}_B$ の合成系 $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ の量子状態が ρ であるとき，部分系 $\mathcal{H}_A$ の量子状態は $\mathcal{H}_B$ 上で部分トレースを取って得られる行列 $\mathrm{tr}_B(\rho)$ で表されます．同様に，部分系 $\mathcal{H}_B$ の量子状態は $\mathcal{H}_A$ 上で部分トレースを取って得られる行列 $\mathrm{tr}_A(\rho)$ で表されます．

$\mathcal{H}$ の状態 ρ が $\mathcal{H}_A$ 上の量子状態 ρ_1 と $\mathcal{H}_B$ 上の量子状態 ρ_2 のテンソル積

$$\rho = \rho_1 \otimes \rho_2$$

であるとき，部分系 $\mathcal{H}_A$ の量子状態は

$$\begin{aligned}\mathrm{tr}_B(\rho) &= \sum_j (I \otimes \langle j|)(\rho_1 \otimes \rho_2)(I \otimes |j\rangle) \\ &= \rho_1 \otimes \left(\sum_j \langle j|\rho_2|j\rangle\right) \\ &= \rho_1 \otimes \mathrm{tr}(\rho_2) \\ &= \rho_1\end{aligned}$$

となります．最後の等式は定理 2.2 によります．トレースが線形な操作であることからより一般的には次の事実が確認できます．

命題 2.3. 合成系 $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ の状態 ρ が

$$\rho = \sum_j p_j \rho_{j,1} \otimes \rho_{j,2} \tag{2.23}$$

の形に書けるとき，部分系 $\mathcal{H}_A$ の状態は $\sum_j p_j \rho_{j,1}$ であり，部分系 $\mathcal{H}_B$ の状態は $\sum_j p_j \rho_{j,2}$ である．

一般に式 (2.23) の形に書けないとき，混合状態 ρ はエンタングルしているといいます．これは純粋状態に対するエンタングルメントの概念の混合状態への拡張になっています．

例 2.16. $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ を密度行列で表現すると

$$|\Phi^+\rangle\langle\Phi^+| = \frac{1}{2}(|00\rangle + |11\rangle)(\langle 00| + \langle 11|)$$

となります．このとき，第 1 量子ビットの量子状態は

$$\mathrm{tr}_2(|\Phi^+\rangle\langle\Phi^+|) = \frac{1}{2}\sum_{b\in\{0,1\}} (I \otimes \langle b|)(|00\rangle + |11\rangle)(\langle 00| + \langle 11|)(I \otimes |b\rangle)$$

$$= \frac{1}{2}\sum_{b\in\{0,1\}} (I \otimes \langle b|)(|00\rangle\langle 00| + |11\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 11|)(I \otimes |b\rangle)$$

となり，さらに

$$(I \otimes \langle 0|)(|ab\rangle\langle cd|)(I \otimes |0\rangle) = \begin{cases} |a\rangle\langle b| & (c = d = 0) \\ 0 & (c = 1 \text{ または } d = 1) \end{cases}$$

となるので,

$$\mathrm{tr}_2(|\Phi^+\rangle\langle\Phi^+|) = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)$$

となります．つまり，$|\Phi^+\rangle$ の第 1 量子ビットの量子状態は，完全混合状態ということになります．

問 2.19.

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

の第 2 量子ビットの量子状態も完全混合状態であることを確認しなさい．

2.5 POVM

これまで測定は正規直交系から決まる射影測定のみを扱ってきましたが，測定をより一般的な形に拡張した数学的表現もあります．POVM とは，そのような一般的な測定による測定結果の確率分布を表す数学的表現です．

定義 2.4 (POVM)**.** 半正定値作用素の集合 $M = \{E_j\}_j$ が **POVM（positive operator valued measure）**であるとは,

$$\sum_j E_j = I \tag{2.24}$$

をみたすことをいう．E_j は測定値 j に対応する（測定値 j に対応する POVM の要素と呼ぶ）．混合状態 ρ に対して，POVM $M = \{E_j\}$ に対応する測定を行うと，測定値 j が得られる確率 $\Pr[M(\rho) = j]$ は

$$\Pr[M(\rho) = j] = \mathrm{tr}(\rho E_j) \tag{2.25}$$

となる.

実際には，POVM の要素 E_j は

$$0 \leq E_j \leq 1 \tag{2.26}$$

をみたします．$E_j \leq 1$ は

$$E_j = I - \sum_{k:k\neq j} E_k \leq I$$

から示せます．とくに 2 値測定を表す POVM は要素が二つなので，式（2.24）より一つの半正定値作用素 E を使って

$$M = \{E_0 = E, E_1 = I - E\}$$

と書けます.

例 2.17. 正規直交基底 $\{|\psi_j\rangle\}$ に対して，$E_j = |\psi_j\rangle\langle\psi_j|$ とすると，E_j は半正定値であり，完備関係式より $\sum_j E_j = I$ をみたすので，$M = \{E_j\}$ は POVM になります．この POVM は正規直交基底 $\{|\psi_j\rangle\}$ での測定を表しています．実際，任意の純粋状態 $|\varphi\rangle$ に POVM M に対応する測定を行うと，測定値 j を得る確率は,

$$\begin{aligned}
\mathrm{tr}((|\varphi\rangle\langle\varphi|)E_j) &= \sum_k \langle k|\varphi\rangle\langle\varphi|E_j|k\rangle \\
&= \sum_k \langle\varphi|E_j|k\rangle\langle k|\varphi\rangle \\
&= \langle\varphi|E_j(\sum_k |k\rangle\langle k|)|\varphi\rangle \\
&= \langle\varphi|E_j|\varphi\rangle \\
&= |\langle\psi_j|\varphi\rangle|^2
\end{aligned}$$

となり，正規直交基底 $\{|\psi_j\rangle\}$ での測定で得られる確率と一致します.

第3章　量子回路

3.1　基本ゲート，量子回路

量子計算で基本ゲートとしてよく使用されるものには，前述のNOTゲート X, 位相反転ゲート Z，Hadamard ゲート H 以外に以下に記すようなものがあります.

- Toffoli ゲート CC-X:　3 量子ビットに作用するユニタリ行列で $|x_1x_2x_3\rangle$ を

$$CC\text{-}X|x_1x_2x_3\rangle := |x_1x_2\rangle|(x_1 \wedge x_2) \oplus x_3\rangle$$

に変化させます．これは $x_1 = x_2 = 1$ のときに限り x_3 が反転されることを意味します．CNOT 同様に，最初の二つの量子ビットは条件量子ビットと呼ばれ，図 3.1 の左図のように表されます（左辺，右辺どちらの記述も使われますが，右辺の方がより標準的に使用されています）.

- $\pi/8$ ゲート T：　1 量子ビットに作用するユニタリ行列で $|b\rangle$ を $(e^{i\pi/4})^b|b\rangle$ に変化させます．つまり，

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

です．これは

$$\begin{pmatrix} e^{-i\pi/8} & 0 \\ 0 & e^{i\pi/8} \end{pmatrix}$$

と時間発展として本質的に等価であるために $\pi/8$ ゲートと呼ばれています.

- 制御ユニタリゲート：より一般の条件量子ビットを持つ量子ゲートとして制御ユニタリゲートという概念が考えられます．ユニタリ行列 U に対して，制御 U ゲート C-U は

$$C\text{-}U(|b\rangle \otimes |\psi\rangle) = |b\rangle \otimes (U^b|\psi\rangle)$$

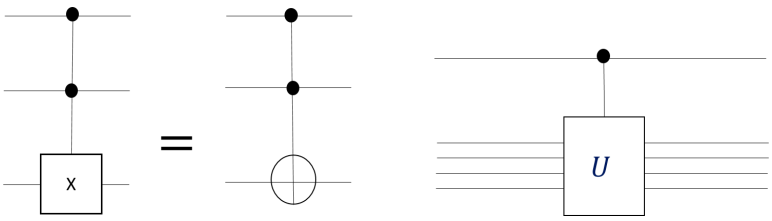

図 3.1: Toffoli ゲート（左図）と制御 U ゲート（右図）

と定義されて（$|\psi\rangle$ は任意のベクトル），図 3.1 の右図のように表されます．つまり，$b = 1$ のときだけ 2 番目以降の量子ビットに U を施すものです．Toffoli ゲート CC-X は制御 C-X とみなせます．制御ユニタリゲートを用いて CC-X から再帰的に定義される一般化 Toffoli ゲートは，ユニタリ行列を基本ゲートに分解するうえでよく利用されます．また，$U = Z$ の場合である制御 Z ゲート（CZ ゲート）C-Z，さらには $U = C$-Z の場合である量子ゲート CC-Z も頻繁に利用される量子ゲートです．

問 3.1. Toffoli ゲートの標準基底での行列表示を与えなさい．

問 3.2. CC-$Z = (I \otimes I \otimes H)CC$-$X(I \otimes I \otimes H)$ を確認しなさい．

基本ゲートとそのゲートが作用する量子ビットの番号の列を**量子回路**と呼び，図 3.2 のように図示されます．各量子ビットに対応するワイヤが横線で表され，時間発展は左から右に進むように描かれています．この図では，まず各量子ビットに H を施した後，1 番目の量子ビットを条件とした C-X を 1 番目と 3 番目の量子ビットに施し，その後で 3 番目の量子ビットを条件とした C-X を 2 番目と 3 番目の量子ビットに施すという量子回路を表すものです．

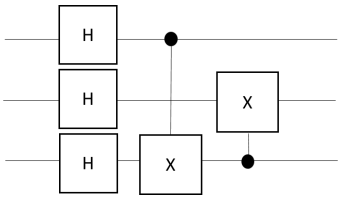

図 3.2: 量子回路の例

また，測定を行う場合，それを表すゲートを別途付け加えて表現することがあります．例えば，図 3.3 は計算の最後で最初と 2 番目の量子ビットを計算基底で測定することを表しています（図のメータのような記号は，計算基底での量子ビットの測定によく使用されます）．

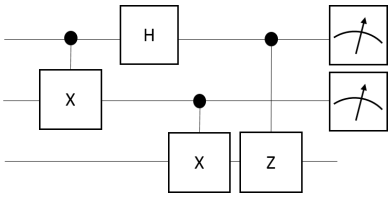

図 3.3: 測定付き量子回路の例

問 3.3. 図 3.3 に入力 $(a|0\rangle + b|1\rangle)|\Phi^+\rangle$ を与えたとき，測定値 $xy \in \{0,1\}^2$ を得る確率を求めなさい.

3.2 古典計算 vs 量子計算

基本的な事実として,「従来の計算（古典計算）は量子計算で効率的に実行可能である」ということを見ておきます.

従来の計算の代表的な計算モデルはブール回路であり，すべてのブール関数が 2 つのゲート AND, NOT だけを使ったブール回路で表現できることは，よく知られた事実です．一方で，Toffoli ゲートはどちらの代わりとしても使えます．実際，Toffoli ゲート $CC\text{-}X$ は，最後の量子ビットを $|0\rangle$ にセットすることで

$$CC\text{-}X(|x_1\rangle|x_2\rangle|0\rangle) = |x_1\rangle|x_2\rangle|x_1 \wedge x_2\rangle$$

となるため,（最初と 2 番目の量子ビットを AND ゲートの入力，最後の量子ビットの出力を AND ゲートの出力とみなすことで）AND ゲートの代わりとなりますし，最初と 2 番目の量子ビットをともに $|1\rangle$ にセットすれば

$$CC\text{-}X(|1\rangle|1\rangle|x_3\rangle) = |1\rangle|1\rangle|\neg x_3\rangle$$

となるため，NOT ゲートの代わりになります.

さらに，古典の乱択アルゴリズム（計算の途中でコインを投げて次の動作を決めてよいアルゴリズム）も $|0\rangle$ を用意して H を書けると

$$H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

となるので，これを測定することで 0 が確率 1/2，1 が確率 1/2 で出現する一様ランダムなコイン投げが模倣できます.

以上より，H と $CC\text{-}X$ を基本的な量子ゲートとして備えた量子回路はすべての古典計算を実行することができます.

3.3　万能量子ゲート集合

前節で述べたように，すべてのブール関数が二つのゲート AND, NOT だけを使ったブール回路で表現できます．この量子回路版として，任意のユニタリ行列が「量子回路として表現できる」ような基本ゲートの集合を**万能ゲート集合 (universal gate set)** と呼びます．ただし,「量子回路として表現できる」の意味には

- 正確に表現できるか，任意の精度で表現できるか
- アンシラ（補助量子ビット）なしで表現できるか，アンシラありで表現できるか

といったバリエーションがあります.

2^n 次元ユニタリ行列 U が万能ゲート集合 $\mathcal{G}$ によってアンシラなしで正確に表現できるとは，$\mathcal{G}$ の要素で構成されたある n 量子ビット量子回路 C が存在して，$U(C) = U$ となることを意味します．ここで $U(C)$ は C によって得られるユニタリ行列を表します．一方，$\mathcal{G}$ によってアンシラありで正確に表現できるとは，$\mathcal{G}$ の要素で構成されたある $(n+m)$ 量子ビット量子回路 C が存在して,

$$U(C)(|\psi\rangle|0^m\rangle) = (U|\psi\rangle) \otimes |0^m\rangle$$

がすべての $|\psi\rangle$ について成り立つことを意味します．ここで $|0^m\rangle$ は，U を実現するために補助として利用されている量子ビットで**アンシラ (ancilla)** と呼ばれています.

任意のユニタリ行列を正確に量子回路として表現するには，一般に無限種類の基本ゲートを必要とします．例えば，C-X と 1 量子ビットに対する量子ゲートの集合 $\{R(\theta) : \theta \in [0, 2\pi)\}$ （$R(\theta)$ は角度 θ の回転行列を表す）からなる集合 $\mathcal{G}_{exact}$ は万能ゲート集合ですが，$R(\theta)$ は連続パラメータ θ を含みます．この万能ゲート集合については次の事実が知られています（回路サイズが量子ビット数の指数になってしまうことは一般には避けられません）.

定理 3.1. 任意の 2^n 次ユニタリ行列は，$\mathcal{G}_{exact}$ からなるサイズ $O(n^3 4^n)$ の量子回路によってアンシラなしで実現可能である.

一方で，有限種類の基本ゲートからなる万能ゲート集合を考えたければ，近似で我慢するしかありません．その場合，求める精度に対して，どの程度の回路サイズが必要になるかが重要になります．定理 3.1 より連続パラメータをもつ 1 量子ビットゲートの集合 $\{R(\theta) : \theta \in [0, 2\pi)\}$ が効率よく近似できれば良く，それを保証するのが以下の Solovay-Kitaev の定理です.

定理 3.2 (Solovay-Kitaev)**.** 任意の 1 量子ビットユニタリ行列は，有限種類の 1 量子ビットゲートを $O(\log^c(1/\varepsilon))$ 個使用することで，精度 ε で近似できる[1]．ここで c は定数.

与えられた任意の精度で近似できるような有限種類の基本ゲート集合からなる万能ゲート集合としては,

- $\{H, CC\text{-}X\}$
- $\{H, C\text{-}X, T\}$

が代表的です．微妙なことに，H と C-X だけでできた量子回路は古典的に模倣可能です (Gottesman-Knill の定理)．誤り訂正などを含めて実際に量子回路を実装するための理論では，3 量子ビットにまたがる Toffoli ゲートは望ましくないことから，$\{H, C\text{-}X, T\}$ がよく利用されています．一方，量子計算量理論の研究では，$\{H, CC\text{-}X\}$ の方が複素数が出てこないことなどから，簡素で扱いやすいためよく使用されます．さらに，$\{H, CC\text{-}X\}$ は Toffoli ゲートを含んでいるため，前節で述べた古典計算の量子計算による模倣を正確に実行できます.

3.4 量子回路の一様性

古典回路の場合と同様に，量子回路も単一では一定のサイズの入力しか取り扱えないため，Turing 機械のように任意の入力長を取り扱うには，各入力長 n に応じて異なる量子回路 Q_n を対応させて，量子回路の族 $\mathcal{Q} = \{Q_n\}$ を考えることになります．このとき，$\mathcal{Q}$ が有限の万能ゲート集合 $\mathcal{G}$ のもとで**一様 (uniform)** であるとは，$\mathcal{G}$ からなる量子回路 Q_n が n に関する多項式時間で計算可能であることを意味します.

さらに，量子計算では入力 x に対して量子回路 Q_x を対応させた量子回路族 $\{Q_x\}$ を考えることもよくあります．この場合，$\mathcal{Q} = \{Q_x\}$ が有限の万能ゲート集合 $\mathcal{G}$ のもとで一様であるとは，量子回路 Q_x が $|x|$（x の長さ）に関する多項式時間で計算可能であることを意味します.

二つの一様性の概念は，多項式時間計算可能性の意味で等価であることが確認できます．状況に応じて双方のどちらか都合のよい方が使われています.

[1] ユニタリ行列 U に対して，$\|U - U'\| \leq \varepsilon$ となるユニタリ行列 U' が存在するとき，U' は U を精度 ε で近似するという.

3.5　よく使用される量子回路

以下ではよく使用される量子回路を幾つか紹介します．最初の二つはユニタリ行列を実現する量子回路です．残りのはなんらかの量子的なタスクを実現する量子回路であり，その目的に沿って作られた量子アルゴリズムともいえます．

3.5.1　量子ワイヤの交換

最初の例（図 3.4）は，量子回路のワイヤを交換することに対応する量子回路です．これは 2 量子ビット状態 $|\psi\rangle|\phi\rangle$ を $|\phi\rangle|\psi\rangle$ に移すユニタリ行列に対応します．実際，$a, b \in \{0, 1\}$ とするとき，

$$\begin{aligned} |a\rangle|b\rangle &\Rightarrow |a\rangle|a \oplus b\rangle \quad (\text{最初の CNOT}) \\ &\Rightarrow |a \oplus (a \oplus b)\rangle|a \oplus b\rangle = |b\rangle|a \oplus b\rangle \quad (\text{2 番目の CNOT}) \\ &\Rightarrow |b\rangle|a \oplus b \oplus b\rangle = |b\rangle|a\rangle \quad (\text{3 番目の CNOT}) \end{aligned}$$

となり，$|\psi\rangle = |a\rangle$, $|\phi\rangle = |b\rangle$ のとき，確かにそうなっていることが確認できました．

問 3.4. $|\psi\rangle$, $|\phi\rangle$ が一般の 1 量子ビットである場合について確認しなさい．

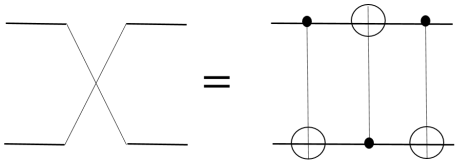

図 3.4: 量子ワイヤの交換

3.5.2　量子 Fourier 変換

次の例は，量子 Fourier 変換と呼ばれる基底変換を行う量子回路です．$\mathcal{H}_{2^n}$ を $\{|0\rangle, |1\rangle, \ldots, |2^n - 1\rangle\}$ で張られる複素内積空間とするとき，$\mathcal{H}_{2^n}$ 上の Fourier 基底とは，2^n 個のベクトル

$$|\widehat{j}\rangle := \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{\frac{(2\pi i)jk}{2^n}} |k\rangle \quad (j = 0, 1, \ldots, 2^n - 1) \tag{3.1}$$

からなる $\mathcal{H}_{2^n}$ の正規直交基底です．

問 3.5. 式 (3.1) が正規直交基底になっていることを確認しなさい.

量子 Fourier 変換（Quantum Fourier Transfom, 略して QFT）とは, 計算基底 $\{|j\rangle\}$ から Fourier 基底 $\{|\widehat{j}\rangle\}$ への基底変換です. 量子回路では $O(n^2)$ 個の基本ゲートで実現可能です. ただし, 量子回路での実現において, $|j\rangle$ は n 量子ビット状態 $|\mathrm{bin}(j)\rangle$ （ここで $\mathrm{bin}(j)$ は j の n ビットでの 2 進表現）で表現されます. 図 3.5 は $n = 4$ の場合であり, 量子ゲート R_k は

$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^k}} \end{pmatrix}$$

です. 最後にワイヤの順序を逆順にしています. この量子 Fourier 変換の回路族は入力長 n に関しての量子一様回路族です. 一般の場合がどのような回路になるかは予想できるでしょう.（その正当性は例えば [20] を参照してください.）

量子状態 (3.1) を 2^n 次元ベクトルで古典的に表現したものが通常の Fourier 基底ですが, その場合対応する Fourier 変換は $2^n \times 2^n$ 行列で表現されるため, その実現には, 比較的効率の良い高速 Fourier 変換でさえ, $O(n2^n)$ 個の（古典の）基本ゲートを必要とします. 量子 Fourier 変換は, Shor のアルゴリズムを始めとする様々な量子アルゴリズムの基盤技術の一つとなっています.

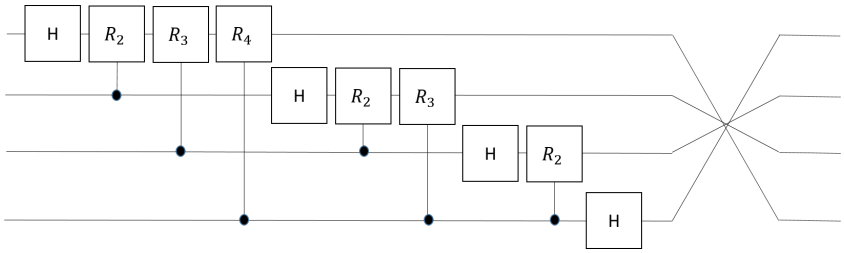

図 3.5: 量子 Fourier 変換の量子回路

3.5.3 Hadamard テスト

次の例は Hadamard テストと呼ばれる量子回路（図 3.6）です. U や入力状態は用途によって変わりえます.

Hadamard テスト：入力を m 量子ビット状態 $|\psi\rangle$ とするとき, 以下のステップを行います.

H1. 1 量子ビットからなるレジスタ A と m 量子ビットからなるレジスタ B を

$$|0\rangle_A \otimes |\psi\rangle_B$$

のように準備します（添え字 A, B はそれぞれ単一ないし複数の量子ビットからなるレジスタ名を表します）.

H2. レジスタ A に H を適用します．その結果は,

$$\frac{1}{\sqrt{2}}(|0\rangle_A + |1\rangle_A) \otimes |\psi\rangle_B$$

となります.

H3. レジスタ A を条件量子ビットとして制御 U を適用します．その結果は,

$$\frac{1}{\sqrt{2}}(|0\rangle_A|\psi\rangle_B + |1\rangle_A(U|\psi\rangle_B))$$

となります.

H4. レジスタ A に H を適用します．その結果は,

$$\begin{aligned}&\frac{1}{2}((|0\rangle_A + |1\rangle_A)|\psi\rangle_B + (|0\rangle_A - |1\rangle_A)(U|\psi\rangle_B))\\ &= \frac{1}{2}(|0\rangle_A(|\psi\rangle_B + U|\psi\rangle_B) + |1\rangle_A(|\psi\rangle_B - U|\psi\rangle_B))\end{aligned}$$

となります.

H5. レジスタ A を計算基底で測定します．その結果が 0 なら受理，1 なら拒否します．このとき，0 を得る確率は

$$\frac{1}{4}\||\psi\rangle_B + U|\psi\rangle_B\|^2 = \frac{1}{4}(2 + \langle\psi|U|\psi\rangle + \langle\psi|U^\dagger|\psi\rangle) \tag{3.2}$$

となります.

例えば $|\psi\rangle$ が U の固有値 $e^{i\theta}$ に対応する固有値なら式（3.2）は

$$\frac{1}{4}(2 + e^{i\theta} + e^{-i\theta}) = \frac{1}{2}(1 + \cos\theta)$$

となり，位相 θ の推定に利用できます.

3.5.4　SWAP テスト

次の例（図 3.7）は，二つの m 量子ビット状態 $|\psi\rangle, |\phi\rangle$ が等しいか否かを判定するための量子回路で，SWAP テストと呼ばれています．図 3.7 は $m = 2$ の例を表しています．一般には以下のような手続きで行われます.

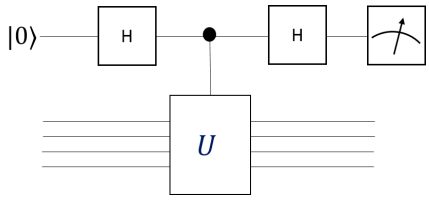

図 3.6: Hadamard テストの量子回路

SWAP テスト

S1. 余分に $|0\rangle$ を用意して，状態 $|0\rangle_A|\psi\rangle_B|\phi\rangle_C$ を準備します．

S2. レジスタ A に H を施します．

S3. A の値が 1 なら B と C（の各 m 個の量子ワイヤ）を交換します．すると状態は

$$\frac{1}{\sqrt{2}}(|0\rangle_A|\psi\rangle_B|\phi\rangle_C + |1\rangle_A|\phi\rangle_B|\psi\rangle_C)$$

になります．

S4. A に H を施します．すると状態は

$$\frac{1}{2}|0\rangle(|\psi\rangle|\phi\rangle + |\phi\rangle|\psi\rangle) + \frac{1}{2}|1\rangle(|\psi\rangle|\phi\rangle - |\phi\rangle|\psi\rangle)$$

になります．

S5. A を計算基底で測定して 0 なら YES，1 なら NO を出力します．

このとき，YES を出力する確率は

$$\Pr[\text{出力} = \text{YES}] = \frac{1}{2} + \frac{1}{2}|\langle\psi|\phi\rangle|^2 \tag{3.3}$$

となります．よって，$|\psi\rangle = |\phi\rangle$ のときは常に YES を出力し，$|\psi\rangle$ と $|\phi\rangle$ が離れる（内積が 0 に近づく）ほど NO を出力するようになります．

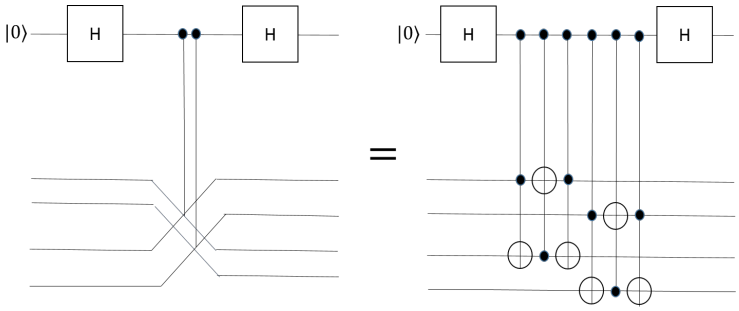

図 3.7: SWAP テストの量子回路

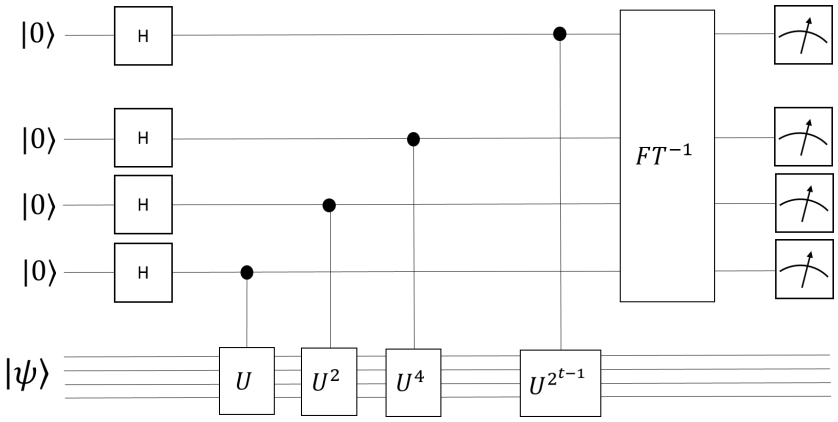

図 3.8: 位相推定の量子回路

問 3.6. 式 (3.3) を示しなさい.

問 3.7. レジスタ B に混合状態 ρ，レジスタ C に混合状態 σ を入れたときに YES を出力する確率は

$$\frac{1}{2}+\frac{1}{2}\mathrm{tr}(\rho\sigma)$$

となることを示しなさい（ヒント：まずは ρ,σ を純粋状態で展開してください）.

3.5.5　位相推定

次の例として位相推定の量子回路（図 3.8）を紹介します（解析はやはり [20] を参照してください）．これはユニタリ行列 U の固有状態 $|\psi\rangle$ に対する固有値 $e^{(2\pi i)\theta}$ の位相 θ を推定する量子回路です（その意味で Hadamard テストの発展版といえます）．図 3.8 において，FT^{-1} は量子 Fourier 変換の逆変換です．制御 U^{2^j}（$j=0,1,\ldots,t-1$）の条件量子ビットの個数 t を増やすことで θ の近似精度をあげることができて，

$$t=n+\lceil\log(2+\frac{1}{2\varepsilon})\rceil$$

（$\lceil x\rceil$ は x 以上となる最小の整数）とすれば，θ の 2 進表示における小数点以下 n ビットを，確率 $1-\varepsilon$ 以上で正しく出力できることが知られています．位相推定は，素因数分解を行う Kitaev の量子アルゴリズムを始めとして，比較的初期から利用されています技術ですが，線形方程式を解く Harrow-Hassidim-Lloyd の量子アルゴリズムを始めとした量子アルゴリズムなどでの利用によってますます重要度が増しています.

第4章　量子アルゴリズム

量子アルゴリズムは，平たく言えば量子回路を使って問題を解くためのレシピです.

4.1　最も代表的な量子アルゴリズム

最も有名な量子アルゴリズムは，1994 年に Peter Shor によって発明された **Shor のアルゴリズム**です．Shor のアルゴリズムは以下の問題を解きます.

問題 4.1 (Integer Factoring (整数の素因数分解))**.**

入力 正の整数 N

出力 N の素因数分解

定理 4.1 (Shor のアルゴリズム)**.** Integer Factoring を 2/3 以上の成功確率で解く多項式時間[1]量子アルゴリズムが存在する.

Integer Factoring は，現在の古典コンピュータで入力長（$\fallingdotseq N$ の桁数）の多項式時間で解けることが知られておらず，その困難性は RSA 暗号としてインターネット上での安全な通信を支えています．一方，Shor の量子アルゴリズムは,「量子コンピュータが実現すれば RSA 暗号は安全でなくなる」ことを意味しています．Shor の量子アルゴリズムとその発展形である隠れ部分群問題に対する量子アルゴリズムは，様々な公開鍵暗号系を支える代数的問題を多項式時間で解くことができます.

Shor のアルゴリズムは，実際には Integer Factoring の代わりに，以下の位数発見問題を解いています（位数発見問題が解ければ，その解をもとにして，古典の乱択アルゴリズムで Integer Factoring を解くことができます）.

問題 4.2 (Order Finding (位数発見問題))**.**

入力 互いに素な正の整数 a, N（ただし，$a < N$）

[1]入力長（$\fallingdotseq N$ の桁数）の多項式なので $O((\log N)^c)$ 時間であることに注意（c は入力によらない定数）.

出力 $f_{a,N}(x) := a^x \pmod N$ としたとき，$f_{a,N}(r) = 1$ なる最小の正の整数 r（r は N を法とする a の位数と呼ばれます）

例えば $N = 15$, $a = 2$ の場合，

$$f_{2,15}(1) = 2, \quad f_{2,15}(2) = 4, \quad f_{2,15}(3) = 8, \quad f_{2,15}(4) = 1$$

となり位数は 4 です．さて，この関数 $f_{2,15}(x)$ は周期 4 の周期関数です．実際，

$$f_{2,15}(4k + b) = f_{2,15}(b)$$

が任意の自然数 k と $b \in \{1, 2, 3, 4\}$ に対して成り立っています．このような周期関数の周期を取り出すのは，量子アルゴリズムが得意とするところです．

次に有名な量子アルゴリズムは，1996 年に Lov Grover によって発見された **Grover のアルゴリズム**です．

問題 4.3 (Unordered Search)**.**

入力 関数 $f : \{1, 2, \ldots, N\} \to \{0, 1\}$．ただし，$f$ はオラクル（ブラックボックス）として与えられます．

出力 $f(j) = 1$ なる「解」j．そのような解が存在しないときは「存在しない」と出力．

Unordered Search では f を計算するサブルーチンが与えられていて，質問として x を入れれば $f(x)$ が返ってきます．計算時間の代わりに質問の回数が計算の複雑さを表す指標になります．例えば $f(x) = 1$ となる x が 1 個しかない場合，解を見つけるには古典では平均 $N/2$ 回質問しないといけないことが予想されると思います．一方で，量子だと平方的に質問回数を減らすことが可能です．

定理 4.2 (Grover のアルゴリズム)**.** Unordered Search を成功確率 2/3 以上で解くためには，古典のアルゴリズムでは最悪で $\Omega(N)$ 回の f への質問を要するが，量子アルゴリズムでは $O(\sqrt{N})$ 回の質問でよい．

NP 探索問題は Unordered Search の形に抽象化できるため，Grover のアルゴリズムは，NP 探索問題をしらみつぶしで解くことに比べて，平方的な時間計算量の削減を可能にします．一方で，この問題に対しては量子アルゴリズムの限界も同時期に示されていて，$\Omega(\sqrt{N})$ 回の質問が必要です．このことは，NP 探索問題に対する多項式時間量子アルゴリズムが存在しないことの状況証拠となっています．

以下では，より簡素である Deutsch-Jozsa のアルゴリズムと，Simon のアルゴリズム，そして解の個数が既知の場合における Grover のアルゴリズムについて詳しく紹介します．位相発見アルゴリズムは概略のみ記します．詳細はこの分野の代表的教科書である Nielsen-Chuang [20] や，その他の教科書（例えば [10, 17, 3, 16]）を参照してください．

4.2 準備

以下では，n ビット列 $x = x_1x_2\cdots x_n$ と $y = y_1\cdots x_n$ に対する演算として XOR（$\oplus$）とドット積（$\cdot$）を用います．$x \oplus y$ は各ビットごとに XOR(排他的論理和) を取って得られたビット列です．

例 4.1. $x = 1011$ と $y = 1101$ の XOR は $x \oplus y = 0110$ です．

n ビット列 $x = x_1x_2\cdots x_n$ および $y = y_1y_2\cdots y_n$ に対して，

$$\begin{aligned} x \cdot y &:= x_1y_1 \oplus x_2y_2 \oplus \cdots \oplus x_ny_n \\ &= x_1y_1 + x_2y_2 + \cdots + x_ny_n \pmod 2 \end{aligned} \tag{4.1}$$

と定義します．$x \cdot y$ は x と y のドット積（あるいはスカラー積）と呼ばれます．

例 4.2. $x = 1011$ と $y = 1101$ のドット積は，

$$x \cdot y = 1 \oplus 0 \oplus 0 \oplus 1 = 0$$

です．

n ビット列を $\mathbb{F}_2^n$ 上のベクトルと同一視すると，$x \oplus y$ はベクトルの和に対応し，$x \cdot y$ はベクトルの内積に対応します．以下の補題はこの対応を念頭に置けば必然です．

補題 4.3 (分配則)**.** $x, y, z \in \{0,1\}^n$ に対して，

$$(x \oplus y) \cdot z = x \cdot z \oplus y \cdot z.$$

問 4.1. 補題 4.3 を証明しなさい．

以下の補題は，ブール関数の解析においてよく使用される事実です．

補題 4.4. 任意の n ビット列 x, z について，

$$\sum_{x \in \{0,1\}^n} (-1)^{x \cdot z} = \begin{cases} 2^n & (z = 0^n) \\ 0 & (z \neq 0^n). \end{cases}$$

問 4.2. 補題 4.4 を証明しなさい.

次に，Hadamard ゲート H を古典ビット列 $x = x_1x_2\cdots x_n$ に対応する n 量子ビット状態（計算基底状態）

$$|x\rangle = |x_1x_2\cdots x_n\rangle = |x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_n\rangle \tag{4.2}$$

の各量子ビットに適用したときに，どのような状態に変化するかを見ておきます．まず，$n = 1$ の場合ですが,

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

なので，これら 2 つの式を 1 つの式として，$x \in \{0,1\}$ に対して

$$H|x\rangle = \frac{1}{\sqrt{2}} \sum_{y\in\{0,1\}} (-1)^{xy}|y\rangle \tag{4.3}$$

と書けます．これとテンソル積およびドット積の性質を利用して，一般の n の式を導きます．式 (4.2) の各量子ビット $|x_j\rangle$ に H を施すと，式 (4.3) より

$$H|x_j\rangle = \frac{1}{\sqrt{2}} \sum_{y_j\in\{0,1\}} (-1)^{x_jy_j}|y_j\rangle$$

になるので，$|x\rangle$ の各量子ビットに H を施した状態は

$$\begin{aligned}
H^{\otimes n}|x\rangle &= (H|x_1\rangle) \otimes (H|x_2\rangle) \otimes \cdots \otimes (H|x_n\rangle) \\
&= \frac{1}{\sqrt{2}} \sum_{y_1\in\{0,1\}} (-1)^{x_1y_1}|y_1\rangle \otimes \cdots \otimes \frac{1}{\sqrt{2}} \sum_{y_n\in\{0,1\}} (-1)^{x_ny_n}|y_n\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{y_1,\ldots,y_n\in\{0,1\}} (-1)^{x_1y_1+\cdots+x_ny_n}|y_1\rangle \otimes \cdots \otimes |y_n\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} (-1)^{x\cdot y}|y\rangle
\end{aligned} \tag{4.4}$$

となります．とくに,

$$H^{\otimes n}|0^n\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle \tag{4.5}$$

は，すべての n ビット列に対応する状態を一様に重ね合わせた状態として，非常によく使用されます.

4.3 Deutsch-Jozsa の量子アルゴリズム

Deutsch-Jozsa のアルゴリズム (1992) は，入力がスケーラブルな問題に対する最初の量子アルゴリズムです.

問題 4.4 (DJ)**.**

入力 関数 $f : \{0,1\}^n \to \{0,1\}$．ただし，$f$ はオラクルとして与えられます.

約束 f は次の (a),(b) のいずれかをみたします：

(a) constant：すべての $x \in \{0,1\}^n$ について $f(x)$ は等しい.

(b) balance：2^{n-1} 個の $x \in \{0,1\}^n$ について $f(x) = 1$ で残りは $f(x) = 0$.

出力 f が (a) なら YES，(b) なら NO.

この問題を古典のアルゴリズムで**誤りなく解く**ことを考えます（問 4.5 にあるように，**誤りを認めれば**少ない質問回数で解けます）．2^n 個の $f(x)$ のうち半分を質問しても，それらの答えがすべて同じ値なら依然 (a) か (b) かわかりません．よって，古典のアルゴリズムで DJ を正しく解くには，少なくとも $2^{n-1}+1$ 回の質問が必要です．一方，量子アルゴリズムでは，以下のように非常に少ない質問回数で誤りなく解くことができます.

定理 4.5 (Deutsch-Jozsa のアルゴリズム)**.** DJ を誤りなく（確率 1 で）解くためには，古典のアルゴリズムでは最悪で $2^{n-1}+1$ 回の f への質問を要するが，量子アルゴリズムでは 2 回の質問でよい.

Deutsch-Jozsa のアルゴリズムは以下のようになります．量子回路の図は，図 4.1 のようになります．図の中の U_f は，オラクルへの質問を表す $(n+1)$ 量子ビット上の時間発展であり，

$$U_f|x\rangle|b\rangle = |x\rangle|b \oplus f(x)\rangle \tag{4.6}$$

（ただし，$x \in \{0,1\}^n$ および $b \in \{0,1\}$ です．二つ目のレジスタに $f(x)$ を書きこんでいることを表しています）と定義されます.

問 4.3. U_f がユニタリ行列であることを示しなさい.

Deutsch-Jozsa のアルゴリズム $\mathcal{A}_{\mathrm{DJ}}$

1. $n+1$ 個の量子ビットを状態 $|0^n\rangle_A|0\rangle_B$ に準備します.
2. レジスタ A の各量子ビットに H を施します．式 (4.5) より量子状態は

$$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle_A|0\rangle_B$$

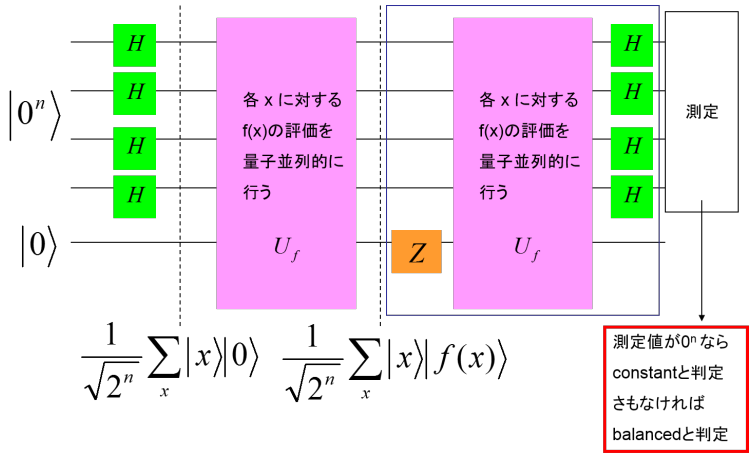

図 4.1: Deutsch-Jozsa のアルゴリズム

になります.

3. A に格納された x をオラクルに質問して，その答えを B に書き込みます．式 (4.6) より量子状態は

$$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle_A |f(x)\rangle_B$$

になります.

4. B に量子ゲート Z を施します．すると量子状態は

$$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} |x\rangle_A |f(x)\rangle_B$$

になります（$b \in \{0,1\}$ に対して，$Z|b\rangle = (-1)^b|b\rangle$ となることに注意）.

5. 再び A に格納された x をオラクルに質問して，その答えを B に書き込みます．式 (4.6) より量子状態は

$$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} |x\rangle_A |0\rangle_B$$

になります.

6. レジスタ A の各量子ビットに H を施します．式 (4.4) より量子状態は

$$\frac{1}{2^n} \sum_{x\in\{0,1\}^n} \sum_{z\in\{0,1\}^n} (-1)^{f(x)} (-1)^{x\cdot z} |z\rangle_A |0\rangle_B \tag{4.7}$$

になります.

7. レジスタ A の各量子ビットを計算基底で測定します．測定値が 0^n なら YES（=constant），そうでなければ NO（=balance）と判定します.

上記の量子アルゴリズムにおいて，質問回数は 2 回です．ステップ 7. における測定値は，入力 f が constant のとき必ず 0^n になり，balance のときは必ず $\neq 0^n$ であるため，アルゴリズムの正当性が保証されます．

実際，式 (4.7) における $|0^n\rangle$ の係数は

$$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)}(-1)^{x\cdot 0^n} = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} \tag{4.8}$$

なので，f が constant のときは，

- 1（すべての x について $f(x) = 0$）か，
- -1（すべての x について $f(x) = 1$）

です．つまり，$z = 0^n$ を測定する確率は 1 ということになります．一方で，f が balance のときは，やはり式 (4.8) より $|0^n\rangle$ の係数は 0，つまり $z = 0^n$ を測定する確率は 0 ということになります．よって，アルゴリズムの正当性が保証されました．

さらに以下のようにして，phase kick-back と呼ばれる小技を使うことで，Deutsch-Jozsa のアルゴリズムは，質問回数が 1 回で十分なように改良できます．

Deutsch-Jozsa のアルゴリズム (phase-kick back による改良版) $\mathcal{A}_{\mathrm{DJ2}}$

1. $n+1$ 個の量子ビットを状態 $|0^n\rangle_A|-\rangle_B$ に準備します．
2. レジスタ A の各量子ビットに H を施します．すると量子状態は

$$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle_A|-\rangle_B$$

になります．

3. A に格納された x をオラクルに質問して，その答えを B に書き込みます．すると量子状態は

$$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)}|x\rangle_A|-\rangle_B \tag{4.9}$$

になります (phase kick-back[2]) ．つまり，レジスタ A には $\mathcal{A}_{\mathrm{DJ}}$ のステップ 5 が終わった後の状態が得られます．

4. $\mathcal{A}_{\mathrm{DJ}}$ のステップ 6, 7 を行います．

[2] レジスタ B への操作で生じた位相係数 $(-1)^{f(x)}$ の効果がレジスタ A に跳ね返ることからこのように呼ばれます．

実際，式（4.9）は次のように確認することができます．ステップ 3. によって量子状態は

$$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle_A \frac{1}{\sqrt{2}}(|f(x)\rangle_B - |f(x)\oplus 1\rangle_B) \tag{4.10}$$

となります．ここで，

$$|f(x)\rangle - |f(x)\oplus 1\rangle = (-1)^{f(x)}(|0\rangle - |1\rangle) \tag{4.11}$$

となることが $f(x)=0$ の場合と $f(x)=1$ の場合に場合分けして確認できるため，式（4.10）は

$$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle_A \frac{1}{\sqrt{2}}(-1)^{f(x)}(|0\rangle_B - |1\rangle_B) = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)}|x\rangle_A|-\rangle_B$$

となって，式（4.9）が確認できました．

問 4.4. 式 (4.11) を確認しなさい．

問 4.5. 問題 DJ を解く（古典の）乱択アルゴリズムを構成し，アルゴリズムの正当性を示しなさい．成功確率 99/100 以上を達成するためには何回の質問が必要か検討しなさい．

問 4.6. 以下の問題 PARITY を $\lceil N/2\rceil$ 回の質問で誤りなく解くような量子アルゴリズムを構成し，アルゴリズムの正当性を示しなさい．

問題 4.5 (PARITY)**.**

入力 関数 $f:\{1,2,\ldots,N\}\to\{0,1\}$．ただし，$f$ はオラクルとして与えられる．

出力 $f(j)=1$ となる j の個数が偶数なら YES，奇数なら NO.

4.4　Grover のアルゴリズム（解の個数が既知の場合）

Grover のアルゴリズムが解く問題は，問題 4.3 の Unordered Search でした．実は定理 4.2 は，より正確には解の個数に応じて以下のように改良した形で記述できます．

定理 4.6 (Grover のアルゴリズム (解の個数のパラメータを含む場合))**.** Unordered Search を成功確率 2/3 以上で解くためには，古典のアルゴリズムでは最悪で $\Omega(N/K)$ 回の f への質問を要するが，量子アルゴリズム

では $O(\sqrt{N/K})$ 回の質問でよい．ただし，K は $f(j)=1$ となるような解 $j \in \{1,2,\ldots,N\}$ の個数，つまり

$$K := \{j \in \{1,2,\ldots,N\} \mid f(j)=1\}$$

を表す．

以下では簡単のため，K が既知である場合を考えます．Grover のアルゴリズムの記述は以下のようになります．

Grover のアルゴリズム（解の個数 K が既知の場合） $\mathcal{A}_{\text{grover-known}}$：以下，$n := \lceil \log N \rceil$ とします．

1. $(n+1)$ 個の量子ビットを使って状態 $|0^n\rangle_A|-\rangle_B$ を準備します．
2. 均等な重ね合わせ状態

$$|\psi\rangle := \frac{1}{\sqrt{N}} \sum_{j=1}^{N} |j\rangle \tag{4.12}$$

をレジスタ A に得るために，

$$U|0^n\rangle = |\psi\rangle$$

をみたすようなユニタリ変換 U を施します[3]．すると量子状態は

$$\frac{1}{\sqrt{N}} \sum_{j=1}^{N} |j\rangle_A|-\rangle_B \tag{4.13}$$

になります．

3. 以下のサブルーチン 3.1–3.2 を $m = O(\sqrt{N/K})$ 回繰り返します．

3.1. A に格納された j をオラクルに質問して，その答えを B に書き込みます．

3.2. 「平均に関する折り返し」と呼ばれるユニタリ変換

$$R(|\psi\rangle) := 2|\psi\rangle\langle\psi| - I$$

を A 上で行います．

4. レジスタ A の値を計算基底で測定して，測定値を得ます．その測定値が解か否かを確認するために，もう 1 回オラクルに質問します．実際に解であれば，その測定値を出力します．解でなければ「?」を出力します．

[3] $N = 2^n$ の場合，U は Deutsch-Jozsa のアルゴリズムのように各量子ビットに H を施すことで実現できます．N が 2 べきでない場合に U を実行する方法は幾つかありますが，ここでは触れないことにします．

問 4.7. $R(|\psi\rangle)$ がユニタリであることを示しなさい.

問 4.8. $R(|\psi\rangle)$ の固有値と固有ベクトルを求めなさい.

Grover のアルゴリズムの解析に移りましょう．まずは質問回数ですが，ステップ 3 のサブルーチン 3.1 を 1 回実行するたびに質問を 1 回行うので，ステップ 3 で質問を $m = O(\sqrt{N/K})$ 回行うことになります．他ではステップ 4 で確認の質問を 1 回行うだけなので，総質問回数は $m+1 = O(\sqrt{N/K})$ であり，定理 4.2 の通りの質問回数が得られました.

次にアルゴリズムの正当性を解析します．実は Grover のアルゴリズムの挙動は，2 次元平面上のベクトルの変化によって視覚的に理解することができます．Grover のアルゴリズムの挙動は，解の集合 $S = \{j \mid f(j) = 1\}$ の要素の均等重ね合わせ

$$|S\rangle := \frac{1}{\sqrt{K}} \sum_{j \in S} |j\rangle$$

と，解でない要素の集合 $\overline{S} = \{j \mid f(j) = 0\}$ （S の補集合）の要素の均等重ね合わせ

$$|\overline{S}\rangle := \frac{1}{\sqrt{N-K}} \sum_{j \in \overline{S}} |j\rangle$$

で張られる 2 次元部分空間上のベクトルの回転として，解析することができるのです.

簡単のため，$N = 4$，$K = 1$ の場合を考えてみましょう．以下，$K = 1$ の場合の唯一解を j_0 とします.

ステップ 2. の後の状態（式 (4.13)）は

$$\begin{aligned} |\psi\rangle_A|-\rangle_B &= \left(\sqrt{\frac{N-K}{N}} |\overline{S}\rangle_A + \sqrt{\frac{K}{N}} |S\rangle_A \right) |-\rangle_B \\ &= \left(\frac{\sqrt{3}}{2} |\overline{S}\rangle_A + \frac{1}{2} |S\rangle_A \right) |-\rangle_B \end{aligned}$$

と表現できます．このとき，x 軸を $|\overline{S}\rangle$，y 軸を $|S\rangle = |j_0\rangle$ と考えた 2 次元空間 $\mathcal{H}_S$ では，x 軸から 30 度回転した位置にレジスタ A の量子状態を表すベクトル $|\psi\rangle$ がいると考えられます（図 4.2 の左図）．ステップ 3.1 の後，phase kick-back により

$$|\psi'\rangle_A|-\rangle_B = \left(\frac{\sqrt{3}}{2} |\overline{S}\rangle_A - \frac{1}{2} |S\rangle_A \right) |-\rangle_B \tag{4.14}$$

と変化します．このとき，レジスタ A の量子状態を表すベクトル $|\psi'\rangle$ は x 軸から -30 度回転した位置に移動します（図 4.2 の中図）．これはステッ

プ 3.1 の操作が，x 軸に関する折り返しであると考えられることを意味しています．

ここで，ステップ 3.2 の平均に関する折り返し $R(|\psi\rangle)$ が，今考えている 2 次元空間 $\mathcal{H}_S$ でどのような役割を果たすかを考えます．$R(|\psi\rangle)$ はその名の通り，「平均ベクトル[4]」$|\psi\rangle$ に関する折り返し変換になっているのです．実際，$|\psi^\perp\rangle$ を $\mathcal{H}_S$ 上で $|\psi\rangle$ に直交する単位ベクトルとすると，

$$R(|\psi\rangle)|\psi\rangle = |\psi\rangle, \quad R(|\psi\rangle)|\psi^\perp\rangle = -|\psi^\perp\rangle$$

です．それゆえ，$\mathcal{H}_S$ 上の任意のベクトルは

$$a|\psi\rangle + b|\psi^\perp\rangle$$

の形で書けることから，$R(|\psi\rangle)$ によって

$$a|\psi\rangle - b|\psi^\perp\rangle$$

に移されることになります．そして，式 (4.14) は $|\psi\rangle$ から見て -60 度回転した単位ベクトルなので，$R(|\psi\rangle)$ の適用によって逆に $|\psi\rangle$ から見て 60 度回転した単位ベクトルに移されることになります（図 4.2 の右図）．$|\psi\rangle$ は x 軸から 30 度回転した単位ベクトルでしたので，得られるベクトルは x 軸から 90 度回転した解 $|j_0\rangle$ を得ることになります．つまり，$N = 4$, $K = 1$ の場合は，唯一解を確率 1 で，サブルーチン 3,1–3.2 を 1 回実行するだけで（つまりオラクルへの質問回数 1 回で），解を得ることになりました．

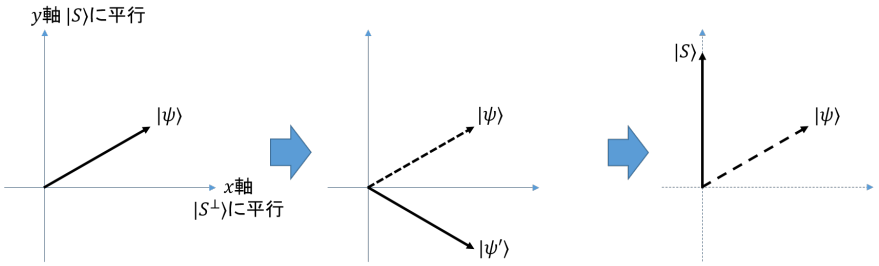

図 4.2: Grover のアルゴリズム ($N = 4, k = 1$ の場合)

一般の N と k の場合も，この拡張で考えることができます．状態 $|\psi\rangle$（式 (4.12)）は，x 軸の正の方向を向く単位ベクトルを

$$\sin\theta = \sqrt{\frac{K}{N}} \tag{4.15}$$

[4] $|\psi\rangle$ は式 (4.12) が表すように解の候補 $|1\rangle, \cdots, |N\rangle$ を均等に重ね合わせたベクトルなので，平均的なベクトルと考えられます．

となる θ だけ回転した単位ベクトルとして，

$$|\psi\rangle = \cos\theta|\overline{S}\rangle_A + \sin\theta|S\rangle_A$$

と書けます．このとき，以下の補題が成立します．

補題 4.7. サブルーチン 3.1–3.2 を 1 回適用することで，レジスタ A の状態ベクトルは 2θ 回転される．

よって，サブルーチンを t 回（オラクルへの質問回数も t 回）行うことで得られる量子状態は

$$\cos((2t+1)\theta)|\overline{S}\rangle_A + \sin((2t+1)\theta)|S\rangle_A$$

になります．$\sin((2t+1)\theta) \approx 1$ のとき，つまり $(2t+1)\theta \approx \pi/2$ のとき，解をほぼ確率 1 で得ることになります．式 (4.15) より $\theta \approx \sqrt{\frac{K}{N}}$ なので，Grover のアルゴリズムは，

$$t \approx \frac{\pi}{2\theta} = \Theta(\sqrt{\frac{N}{K}})$$

のときに高確率で解を出力することが分かります．

問 4.9. 補題 4.7 を証明しなさい．

なお，アルゴリズム $\mathcal{A}_{\text{grover-known}}$ をサブルーチンとした古典のアルゴリズムによって，たとえ解の個数 K が未知の場合でも，$O(\sqrt{N/K})$ 回の質問で Unordered Search を高確率で解くことができます（例えば文献 [10] を参照してください）．

4.4.1　Grover のアルゴリズムの応用

Grover のアルゴリズムの応用としてよく利用されるのが，**量子振幅増幅 (Quantum Amplitude Amplification)** と呼ばれる次の定理です．

定理 4.8 (量子振幅増幅)**.** 基本ゲート数 t の量子アルゴリズムがある問題の解を成功率 p 以上で発見できるとき，成功率 2/3 以上で同じ解を発見する基本ゲート数 $O(t/\sqrt{p})$ の量子アルゴリズムが存在する．

例えば，有名な NP 問題である 3SAT を考えましょう．

問題 4.6 (3SAT)**.**

入力 各節が 3 つのリテラル（変数かその否定）からなる和積形論理式（3CNF 論理式）$F = F(x_1, x_2, \ldots, x_n)$（例えば

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

は入力の一例）

出力 F が充足可能なら YES，そうでなければ NO（例で挙げた $G(x_1, x_2)$ は $G(0, 0) = 1$ より出力は YES）

3SAT は全探索，つまり変数への全ての割当 $(x_1, x_2, \ldots, x_n) \in \{0, 1\}^n$ をチェックすれば解けますが，その計算時間は $2^n q(n)$ になります（$q(n)$ は各割当に対して F を評価する時間を表し，n の多項式で抑えられます）．しかし，全探索を行う代わりに，定理 4.2 の Grover のアルゴリズムを使うと，$F(x_1, x_2, \ldots, x_n) = 1$ となるような割り当てを探すのは，量子コンピュータでは $O(\sqrt{2^n})$ 回の F の評価で可能であるため，

$$O(2^{n/2}\mathrm{poly}(n)) = O(1.415^n \mathrm{poly}(n))$$

（$\mathrm{poly}(n)$ は多項式オーダーを表す）の計算時間で 3SAT を（高い成功確率で）解くことができるようになります．

一方で，古典のアルゴリズムでは全探索より良いアルゴリズムが知られています．代表的なものは Schöing のランダムウォークを用いた 3SAT に対する乱択アルゴリズムです（詳細は文献 [18] など）．このアルゴリズムは入力 F の出力が YES の場合，多項式時間で $F(x_1, x_2, \ldots, x_n) = 1$ となる割当を $p = (\frac{3}{4})^n$ の確率で発見できることが知られています．よって，解が発見されるまでアルゴリズムを $\frac{100}{p} = O((\frac{4}{3})^n)$ 回繰り返せば，

$$1 - (1 - p)^{\frac{100}{p}} \approx 1 - \left(\frac{1}{e}\right)^{100} \tag{4.16}$$

（$e = 2.717\cdots$ は自然対数の底）という高確率で，$F(x_1, x_2, \ldots, x_n) = 1$ となる割当が見つけられることになります．つまり，古典で

$$O\left(\left(\frac{4}{3}\right)^n \mathrm{poly}(n)\right) = O(1.334^n \mathrm{poly}(n))$$

時間のアルゴリズムが知られているというわけです．

しかし，定理 4.8 を使うと，そのように工夫された古典アルゴリズムを取り込んで，さらに高速化ができることになります．既に述べたように，古典の計算は量子ゲート H および $CC\text{-}X$ を使って量子アルゴリズムで実行することができました．そこで成功率 $p = (\frac{3}{4})^n$ で充足解を発見する（n は入力 3SAT 論理式のブール変数の個数）多項式時間古典アルゴリズムを

実行する量子サブルーチンを $\mathcal{Q}$ としたうえで，成功率を式 (4.16) と同じくらいまで増幅するのに定理 4.8 を使うと

$$O\left(\frac{1}{\sqrt{p}}\right) = O\left(\left(\frac{4}{3}\right)^{n/2}\right) = O(1.155^n)$$

回 $\mathcal{Q}$ を実行すればよいことになるのです．つまり，量子コンピュータを使えば 3SAT は

$$O\left(\left(\frac{4}{3}\right)^{n/2}\mathrm{poly}(n)\right) = O(1.155^n\mathrm{poly}(n))$$

時間で解けることになるというわけです．これは現在知られている最速の古典アルゴリズムよりも高速です．

4.5　Simon のアルゴリズム

Simon のアルゴリズム (1994) は，古典の乱択アルゴリズムより指数的に優れた計算量を持つ最初の量子アルゴリズムです．このアルゴリズムは Shor のアルゴリズムのヒントとなったものであり，Shor のアルゴリズムのエッセンスを感じることができます．さらに，様々な秘密鍵暗号システムの暗号文を従来のアルゴリズムより高速に解読するための量子アルゴリズムを構成する上での基本要素となっています．

問題 4.7 (SIMON)**.**

入力 関数 $f : \{0,1\}^n \to \{0,1\}^n$．ただし，$f$ はオラクルとして与えられる．

約束 f は 2 対 1 関数で，$f(x \oplus s) = f(x)$ なる $s \in \{0,1\}^n$（ただし，$s \neq 0^n$）が存在する．

出力 s.

定理 4.9 (Simon のアルゴリズム)**.** SIMON を成功確率 2/3 以上で解くためには，古典の乱択アルゴリズムでは最悪で $\Omega(\sqrt{2^n})$ 回の f への質問を要するが，量子アルゴリズムでは $O(n)$ 回の質問でよい．

古典の下界については例えば [26] を参照してください．量子アルゴリズムは以下の通りです．量子回路の図は図 4.3 のようになります．図の中の O_f はオラクルへの質問を表すユニタリ行列であり，

$$O_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$$

と定義されます．

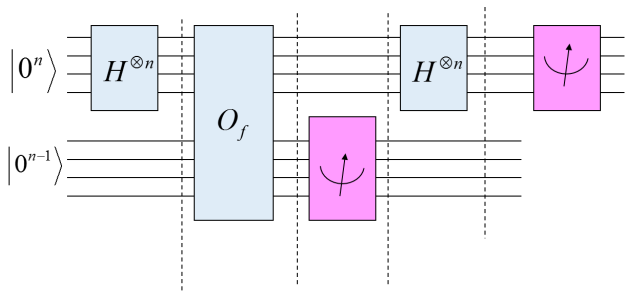

図 4.3: Simon のアルゴリズム

Simon のアルゴリズム $\mathcal{A}_{\mathrm{simon}}$

1. 以下のサブルーチン 1.1–1.5 を $m = O(n)$ 回繰り返します.

1.1. $2n$ 個の量子ビットを状態 $|0^n\rangle_A|0^n\rangle_B$ に準備します.

1.2. レジスタ A の各量子ビットに H を施します．すると量子状態は

$$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle_A|0^n\rangle_B$$

になります.

1.3. A に格納された x をオラクルに質問して，その答えを B に書き込みます．このとき量子状態は,

$$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle_A|f(x)\rangle_B$$

になります.

1.4. B を計算基底で測定します．その値が $z \in \{0,1\}^n$ のとき，得られる量子状態は

$$\frac{1}{\sqrt{2}}(|x_z\rangle_A + |x_z \oplus s\rangle_A)$$

になります．ただし，x_z は $f(x_z) = z$ なる n ビット列です.

1.5. レジスタ A の各量子ビットに H を施します．式 (4.4) によって量子状態は,

$$\frac{1}{\sqrt{2^{n+1}}} \sum_{y\in\{0,1\}^n} ((-1)^{x_z\cdot y} + (-1)^{(x_z\oplus s)\cdot y})|y\rangle_A$$

になります．これは補題 4.3 によって,

$$\frac{1}{\sqrt{2^{n+1}}} \sum_{y\in\{0,1\}^n} ((-1)^{x_z\cdot y}(1 + (-1)^{s\cdot y}))|y\rangle_A \tag{4.17}$$

と書き換えられます.

1.6. レジスタ A を計算基底で測定して，サブルーチンの出力を得ます. このとき，得られる測定値 y は，式 (4.17) より

$$y \cdot s = 0 \tag{4.18}$$

をみたします.

2. i 回目のサブルーチンの出力を $x(i) \in \{0,1\}^n$ とするとき,（$\{0,1\}^n$ を $\mathbb{F}_2^n$ と同一視して）w に関する連立一次方程式

$$\begin{cases} x(1) \cdot w = 0 \\ x(2) \cdot w = 0 \\ \vdots \\ x(m) \cdot w = 0 \end{cases}$$

を解きます.（自明な 0^n 以外の）解が一意に得られたなら，その値をアルゴリズムの出力とします．そうでない場合は「?」を出力します.

問 4.10. 式 (4.18) が成り立つ理由を説明しなさい.

問 4.11.（$\mathbb{F}_2$ 上の）連立一次方程式が

$$\begin{cases} (1110) \cdot w = 0 \\ (1101) \cdot w = 0 \\ (1001) \cdot w = 0 \end{cases}$$

（ただし，$w = w_1w_2w_3w_4$）のとき，解を求めなさい.

問 4.11 の三つの $\mathbb{F}_2$ 上の 4 次元ベクトル $(1110), (1101), (1001)$ は一次独立なので，解空間は $4 - 3 = 1$ 次元，つまり唯一の非自明解が決まります．同様に，Simon のアルゴリズムで得られた n 次元ベクトル $x(1), x(2), \ldots, x(m)$ が $n-1$ 個の一次独立なベクトルを含めば，一意解である s が見つけられることになります．方程式 (4.18) をみたす 2^{n-1} 個のベクトルのうち，$n-1$ 個の一次独立なベクトルを見つけるまでにかかる繰り返し回数は，次のような解析で評価できます.

- 1 回目は $1 - \frac{1}{2^{n-1}}$ の確率で 1 次独立なベクトル v_1 を得る（ゼロベクトル 0^n さえ引かなければよい）
- 2 回目は $1 - \frac{2}{2^{n-1}}$ の確率で 1 次独立なベクトル v_2 を得る（0^n と v_1 以外であればよい）
- 3 回目は $1 - \frac{2^2}{2^{n-1}}$ の確率で 1 次独立なベクトル v_3 を得る（v_1 と v_2 で張られる空間に属する 2^2 個のベクトル以外であればよい）

- ⋯

最後の 1 個を見つけるときには，$1-\frac{2^{n-2}}{2^{n-1}}=1/2$ まで新しい一次独立なベクトルを見つける確率は下がります．しかし，それでも 2 回に 1 回はうまくいくので，$m=O(n)$ としておけば十分であることが想像できるかと思います．

4.6 量子計算に古典アルゴリズムを組み込むには

ここまで紹介した量子アルゴリズムは，オラクルへの質問によって，オラクルに対応する関数のある情報（例えば Unordered Search なら $f(j)=1$ となる j）を明らかにするものでした．一方で，量子アルゴリズムをオラクルのない通常の問題（例えば 3SAT などの NP 完全問題）に適用する場合は，オラクルへの質問に対応する部分（関数評価）の古典計算を，Toffoli ゲートなどを使って量子計算で実行することが求められます．

例えば，SAT 論理式 $F(x)$（ただし，$x\in\{0,1\}^n$）が充足可能かどうかを，Grover のアルゴリズムで解きたいとします．そのためには，まず均等重ね合わせ

$$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle_A|0\rangle_B$$

を作って，各 x についてオラクルの答に対応する $F(x)$ を（ブール回路などにより）古典的に計算して，状態

$$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle_A|F(x)\rangle_B$$

を得たいところです．ところが，古典計算では $F(x)$ という計算結果以外の情報が（計算途中のメモのように）通常一緒に付いてきます．つまり，$F(x)$ の古典計算を Toffoli ゲートからなる量子回路で模倣すると

$$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle_A|F(x)\rangle_B|g(x)\rangle_G$$

となって，各 x について余計な情報 $g(x)$（garbage と呼ばれる）が付いてくることになります．このような余計な情報は，一般に量子計算を邪魔するため，除去する必要があります．古典計算なら単に消去することが可能ですが，この「単に消去」という計算は可逆計算ではありません（つまり出力から入力に戻すことができません）．一方，量子計算は時間発展がユニタリであるため（途中で測定を行わない限り）可逆計算であることが要請されます．そのため量子計算では,「単に消去」という計算は,（測定で量子重ね合わせを壊さない限り）実行できないのです．

この余計な情報 $|g(x)\rangle$ の除去は，古典の可逆計算の分野で，Bennett が提案した以下の手続きによって行うことができます．ここで古典の可逆計算とは，量子計算の言葉でいえば

- ユニタリ行列が各行各列に 1 が一つづつある直交行列に限られ，
- 状態ベクトルが計算基底だけを対象とする

計算と考えることができます（Toffoli ゲートによる計算は可逆計算であることに注意）.

Bennett の可逆計算手続き

1. $F(x)$ を計算する古典アルゴリズムを模倣する Toffoli ゲートからなる量子回路の時間発展 U，つまり

   $$U(|x\rangle_A|0\rangle_B|0\rangle_G) = |x\rangle_A|F(x)\rangle_B|g(x)\rangle_G$$

   のような直交行列 U を用いて，

   $$|x\rangle_A|F(x)\rangle_B|g(x)\rangle_G|0\rangle_C$$

   という状態を作ります.

2. CNOT ゲートでレジスタ B にある古典情報を C にコピーします.

   $$|x\rangle_A|F(x)\rangle_B|g(x)\rangle_G|F(x)\rangle_C$$

3. レジスタ A, C, G に U^{-1} に対応する量子回路を実行することで

   $$|x\rangle_A|F(x)\rangle_B|0\rangle_G|0\rangle_C$$

   を得ます.

この手続きによって garbage を除去できるために，古典計算は量子計算のサブルーチンとして取り込むことが可能となっています.

4.7　位数発見アルゴリズムの概略

位数発見アルゴリズムの回路図は，Simon のアルゴリズムと非常に似ていて，図 4.4 のようになります.

Shor の位数発見アルゴリズム $\mathcal{A}_{\mathrm{OrderFind}}$

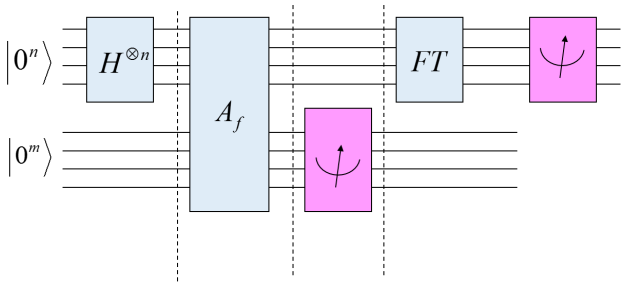

図 4.4: 位数発見アルゴリズム

1. $n+m$ 個の量子ビットを状態 $|0^n\rangle_A|0^m\rangle_B$ に準備します．ただし，n は $N^2 \leq 2^n < 2N^2$ をみたす整数で，$m = \lceil \log N \rceil$ です．

2. レジスタ A の各量子ビットに H を施します．すると量子状態は

$$\frac{1}{\sqrt{2^n}} \sum_{\in\{0,1\}^n} |x\rangle_A|0^m\rangle_B$$

になります．

3. A に格納した x に対して，

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

を計算し，その答えを B に書き込みます．図 4.4 の A_f は対応するユニタリ行列

$$A_f(|x\rangle|y\rangle) = |x\rangle|y + a^x \pmod N\rangle$$

です（なおこのユニタリ行列 A_f は 4.6 章の技術を使って余分な情報を消去して実行されます）．すると量子状態は

$$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle_A|a^x \pmod N\rangle_B$$

になります．

4. B を計算基底で測定します．その値が $z \in \{0, 1, \ldots, N-1\}$ のとき，得られる量子状態は

$$\frac{1}{\sqrt{2^n}} \sum_{x:a^x=z \pmod N} |x\rangle_A$$

になります．実際には f の周期性から

$$z = a^k \bmod N \tag{4.19}$$

（$0 \leq k \leq r-1$）となっています．

5. レジスタ A に量子フーリエ変換 FT を施します．すると量子状態は

$$\frac{1}{2^n}\sum_{x:a^x=z \pmod N}\sum_{y=0}^{2^n-1}\exp\left(\frac{2\pi ixy}{2^n}\right)|y\rangle_A$$

になります．これは式（4.19）を代入して

$$\frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x:a^x=a^k \pmod N}\exp\left(\frac{2\pi ixy}{2^n}\right)|y\rangle_A \tag{4.20}$$

と書き換えられます．

6. レジスタ A を測定します．このとき，y が得られる確率は

$$\Pr[y]=\frac{1}{2^{2n}}\left|\sum_{x:a^x=a^k \pmod N}\exp\left(\frac{2\pi ixy}{2^n}\right)\right|^2 \tag{4.21}$$

ですが，$x=lr+k$（l はある整数）と書けることから

$$\Pr[y]=\frac{1}{2^{2n}}\left|\sum_l\exp\left(\frac{2\pi i(lr+k)y}{2^n}\right)\right|^2=\frac{1}{2^{2n}}\left|\sum_l\exp\left(\frac{2\pi il(ry)}{2^n}\right)\right|^2 \tag{4.22}$$

と書きなおせます．このとき，式 (4.22) の右辺が大きい値になるのは，$\frac{ry}{2^n}$ が整数に近いとき，つまり，ある整数 l' について，

$$\left|\frac{y}{2^n}-\frac{l'}{r}\right|\approx 0 \tag{4.23}$$

の形になるときであることを，示すことができます．[5]

まとめると，ステップ 6. で測定される y は，高確率で式 (4.23) をみたすものとなります．式 (4.23) をみたすとき，l' と r が互いに素であれば，y から r を見つける多項式時間古典アルゴリズム（連分数展開）が知られています．さらに，l' と r が互いに素な y を得る確率もある程度以上なことが示せるため，上記の量子アルゴリズムは，求めたい位数 r を高確率で求めることができるというわけです．

4.8　量子シミュレーション

Feynman が量子コンピュータのアイデアを提唱したのは，量子力学系のシミュレーションへの応用でした．量子力学系のシミュレーションのた

[5] 直感的には，$\sum_l \exp\left(\frac{2\pi il(ry)}{2^n}\right)$ は，複素平面上で単位ベクトル $\exp\left(\frac{2\pi il(ry)}{2^n}\right)$ を $l=0,1,\ldots$ について足していくので，$\frac{ry}{2^n}$ が整数に近くないと単位ベクトルが原点を中心に回って足されていくので，ほぼ 0 になってしまうのです．

めの量子アルゴリズムは，計算問題を効率的に解くということを目的とする量子アルゴリズムと異なりますが，様々な量子アルゴリズムへの応用を持つため，重要な量子アルゴリズムの一つとなっています．

一般に量子力学系の時刻 t における状態 $|\psi(t)\rangle$ は，Schrödinger 方程式

$$i\frac{d}{dt}|\psi(t)\rangle = H|\psi(t)\rangle \tag{4.24}$$

（Planck 定数は省略）の解です．H はハミルトニアンと呼ばれるエルミート行列（物理系のエネルギーに対応する観測量）で，ここでは時間に依存しないとします．このとき，式 (4.24) の解は

$$|\psi(t)\rangle = e^{-itH}|\psi(0)\rangle$$

となります．ここで e^{-itH} は，H のスペクトル分解が

$$H = \sum_k a_k|\psi_k\rangle\langle\psi_k|$$

のとき，

$$e^{-itH} = \sum_k e^{-ita_k}|\psi_k\rangle\langle\psi_k|$$

と定義されるユニタリ行列です．よって，e^{-itH} を効率的に実行する量子回路があれば，どんな量子力学系でも量子回路で効率的に模倣可能ということになります．一般のハミルトニアンに対しては，そのような量子回路の効率的構成は難しいですが，実際の物理系で頻出するスパースなハミルトニアンについては，効率的な量子アルゴリズムが示されていて，スパース性や近似精度などの各種パラメータについての改良も進められています．基本となる幾つかの量子アルゴリズムは，[7] や [26] で紹介されています．

4.9 その他の量子アルゴリズム

上記で紹介した量子アルゴリズムは，より複雑な量子アルゴリズムのサブルーチンとして，古典のアルゴリズムなどと組み合わせて使用されています．例えば，Grover のアルゴリズムと動的計画法を組み合わせることで，TSP(Traveling Salesman Problem) など，幾つかの NP 困難な問題の古典アルゴリズムに対する高速化を行う量子アルゴリズムが提案されています [1].

さらに量子ウォーク，Harrow-Hassidim-Lloyd の線形方程式を解く量子アルゴリズム（HHL），量子シミュレーションを行うアルゴリズムなど，多種多様な量子アルゴリズムが登場しており，さらにそれらを土台にし

てより複雑な量子アルゴリズムが構築されています．Jordan が運営する Quantum Algorithm Zoo [13] では，それらの多くが紹介されています．[9] は量子アルゴリズムの基本技術や応用がまとめられたサーベイです．

主要な量子アルゴリズムの説明は，[7] や [26] などの講義ノートで学習できます．

4.10　通信を含む計算問題に対する量子プロトコル

入力が複数のパーティに分割されているときに何らかのタスクを実行するという設定は，データが大規模化した今日では非常に重要です．そのような設定の中で最も簡素な設定の一つが，以下の同時通信計算量モデル (Simultaneous Message Passing model: 略して SMP モデル) です．

SMP モデル
設定 A は入力 $x \in \{0,1\}^n$，B は入力 $y \in \{0,1\}^n$ を持ちます．R は入力を持たず．A および B は R にメッセージを送ることができるとします．
目的 A,B はなるべく短いメッセージで R に $f(x,y)$ か否かを判定させたいとします．ここで関数 f は A,B,R すべてにとって既知です．
計算量 A,B が R に送るメッセージ長の和（ビット数の和）のみ考慮します．関数 f の通信計算量 (communication complexity) とは，SMP モデルにおける $f(x,y)$ を計算させるための A,B,R のすべてのアルゴリズム（通信プロトコルと呼ばれる）において，最小を達成するような通信プロトコルにおける計算量を指します．

この設定で代表的な関数の一つが，等価性判定関数 $EQ : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ です．EQ は

$$EQ(x,y) = \begin{cases} 1 & (x = y) \\ 0 & (x \neq y) \end{cases}$$

と定義されます．Buhrman ら [6] は 2001 年に SMP モデルの量子版を考えました．量子版では A および B が R に送るメッセージは量子ビット列となり，量子ビット列の長さの和が代わりに計算量の尺度になります．Buhrman らは，従来の古典通信プロトコルより指数的にメッセージ長が短くなるような等価性判定関数に対する量子通信プロトコルを発見しました．

定理 4.10. EQ の通信計算量について，以下のギャップが得られる．

1. 古典のメッセージのみで EQ を成功確率 2/3 以上で解くための通信計算量は $\Omega(\sqrt{n})$.

2. 量子のメッセージ（量子ビット列）を使って EQ を成功確率 2/3 以上で解くための通信計算量は $O(\log n)$.

古典の下界については原論文 [4] を参照してください．量子プロトコルは以下のようです.

量子指紋プロトコル $\mathcal{P}_{\text{fingerprint}}$

q を $3n \leq q \leq 6n$ をみたす素数とします．$\mathbb{F} := \mathbb{F}_q$ は要素数 q の有限体を表すとします．n ビット列 $x = x_1 \cdots x_n$ に対して，多項式 $p_x(z)$ を

$$p_x(z) := \sum_{i=1}^{n} x_i z^{i-1}$$

とします．このとき，以下の 1.—2. を実行します.

1. A は量子状態[6]

$$|\phi_x\rangle = \frac{1}{\sqrt{q}} \sum_{z \in \mathbb{F}} |z\rangle |p_x(z)\rangle,$$

B は量子状態

$$|\phi_y\rangle = \frac{1}{\sqrt{q}} \sum_{z \in \mathbb{F}} |z\rangle |p_y(z)\rangle$$

を R に送ります.

2. R は $|\phi_x\rangle = |\phi_y\rangle$ か否かを SWAP テストでチェックします．SWAP テストが YES を出力すれば「A と B の入力は同じ」と判定し，NO を出力すれば「A と B の入力は異なる」と判定します.

$\mathcal{P}_{\text{fingerprint}}$ の解析ですが，まず必要な通信量は z も $p_x(z)$（あるいは $p_y(z)$）も $\mathbb{F}$ の要素であり，それらを表すのに $\lceil \log q \rceil$ ビットが必要であることから，高々

$$2\lceil \log q \rceil \times 2 = 4\lceil \log q \rceil \times 2 = O(\log n)$$

個の量子ビットの通信で十分です.

正当性は $x = y$ の場合とそうでない場合に分けて考えます．$x = y$ の場合は $|\psi_x\rangle = |\psi_y\rangle$ なので，$\langle \psi_x | \psi_y \rangle = 1$ であり，式 (3.3) によって常に YES を出力しますので，常に「A と B の入力は同じ」と判定することになります.

次に $x \neq y$ の場合を考えます．z の多項式

$$s_{x,y}(z) := p_x(z) - p_y(z)$$

[6] このような量子状態は量子指紋 (quantum fingerprinting) と呼ばれています.

は恒等的に0ではなく，また次数はnなので，$s_{x,y}(z)=0$となるようなzの個数は高々n個です．よって，

$$\Pr_{z\in\mathbb{F}}[p_x(z)=p_y(z)]=\Pr_{z\in\mathbb{F}}[s_{x,y}(z)=0]\leq\frac{n}{|\mathbb{F}|}=\frac{n}{q}\leq\frac{1}{3}$$

となります．このとき，

$$\langle w|w'\rangle=\begin{cases}1 & (w=w'\text{の場合}),\\ 0 & (\text{そうでない場合})\end{cases}$$

なので，

$$\begin{aligned}|\langle\phi_x|\phi_y\rangle| &= \frac{1}{q}\left|\sum_{z,z'\in\mathbb{F}}\langle z|z'\rangle\langle p_x(z')|p_y(z)\rangle\right|\\ &= \frac{1}{q}\sum_{z\in\mathbb{F}}\langle p_x(z)|p_y(z)\rangle\\ &= \Pr_{z\in\mathbb{F}}[p_x(z)=p_y(z)]\\ &\leq \frac{1}{3}\end{aligned}$$

となり，式 (3.3) より「A と B の入力は同じ」と判定する確率は，高々

$$\frac{1}{2}\left(1+\left(\frac{1}{3}\right)^2\right)=\frac{5}{9}$$

となります．

以上より，$\mathcal{P}_{\text{fingerprint}}$は，$x=y$のときは常に「A と B の入力は同じ」と判定し，$x\neq y$のときは高々5/9の確率で「A と B の入力が同じ」と判定します．よって，$\mathcal{P}_{\text{fingerprint}}$を（並列処理で）2回繰り返すことで$x=y$のときは常に「A と B の入力は同じ」と判定し，$x\neq y$のときは，高々1/3の確率で「A と B の入力が同じ」（つまり2/3以上の確率で「A と B の入力が異なる」）と出力するような通信量$O(\log n)$の量子プロトコルが構築できました．

より一般の量子通信計算量については，[26] が初学者には適当な文献の一つです．また，[5] は量子力学の非局所性との関係から通信計算量を紹介したサーベイです．

分散計算の量子版についてはまだそれほど多くの結果が世に出ていません．既存の成果は例えば文献 [24, 12, 14] およびそこで引用されている文献を参照するとよいでしょう．

第5章　量子計算量クラス

本章ではP, NP, 対話型証明といった古典の計算量クラスの量子版である量子計算量クラスを取り上げ，主だった結果の幾つかを紹介します（より詳細な紹介および以下で述べる結果の参考文献は，[19, 21, 25] を参照してください）.

以下で考える計算問題は答えがYESかNOの問題ですが，（Deutsch-Jozsaや Simonの問題と同様に）必ずしも考えうるすべての入力に対して答えを要求するわけではありません．このような問題は約束問題 (promise problem) と呼ばれますが，以下では単に問題と呼びます．形式的には，2進列全体 $\{0,1\}^*$ の部分集合 $A_{\rm yes}, A_{\rm no}$ が $A_{\rm yes} \cap A_{\rm no} = \emptyset$ をみたすとき，$A = (A_{\rm yes}, A_{\rm no})$ を**（約束）問題**と呼びます．とくに $A_{\rm yes} \cup A_{\rm no} = \{0,1\}^*$ のとき，$A_{\rm yes}$ は**言語**と呼ばれます.

5.1　古典計算量クラス

まず古典の計算量クラスを確認しておきます．Pは多項式時間決定性Turing機械（平たく言えば多項式時間アルゴリズム）で解ける問題の全体（以下，クラスという）であり，PSPACEは多項式空間Turing機械（入力長の多項式で抑えられる量のメモリを使用するアルゴリズム）で解ける問題のクラスです．形式的な定義は以下のようになります.

定義 5.1. $A = (A_{\rm yes}, A_{\rm no})$ がPに属する (PSPACEに属する) とは，ある多項式時間（多項式空間）決定性Turing機械 M が存在して，任意の入力 x について以下の条件をみたす.

- $x \in A_{\rm yes}$ のとき，$M(x) = \text{accept}$.[1]
- $x \in A_{\rm no}$ のとき，$M(x) = \text{reject}$.

NPは多項式時間非決定性Turing機械で解ける問題のクラスです．あるいは，NPは以下のような「入力がYESであるとき，YESであることが効率的に検証可能な問題」と定義することもできます.

[1] $M(\cdot)$ は $\cdot$ を入力としたときの M の出力を表しています.

定義 5.2. $A = (A_{\text{yes}}, A_{\text{no}})$ が NP に属するとは，ある多項式時間決定性 Turing 機械 M が存在して，任意の入力 x について以下の条件をみたす（p は多項式）.

完全性 (completeness) $x \in A_{\text{yes}}$ のとき，ある $w \in \{0,1\}^{p(|x|)}$（**証拠 (certificate,witness)**）が存在して，$M(x,w) = \text{accept}$.

健全性 (soundness) $x \in A_{\text{no}}$ のとき，すべての $w \in \{0,1\}^{p(|x|)}$ に対して，$M(x,w) = \text{reject}$.

通常の古典アルゴリズムは動作が決定的ですが，次の動作を決めるのにランダムなコインを投げて決めることを認めたアルゴリズムが乱択アルゴリズムです．これに対応する Turing 機械は確率 Turing 機械とよばれ，Turing 機械における次の動作がやはり確率 1/2 で分岐することを認めたものです．BPP は，平たく言えば，多項式時間乱択アルゴリズムで任意の約束をみたす入力 $x \in A_{\text{yes}} \cup A_{\text{no}}$ に対して，確率 2/3 以上で正しい答えを出力することのできる問題のクラスです．確率 2/3 は便宜上のものであって，多数決により 2/3 を $1-1/2^n$ まで上げたり，逆に $1/2+1/\text{poly}(n)$（n は入力長で $\text{poly}(n)$ は常に正の値を取る任意の多項式）に下げたりしても，問題のクラスは不変です（BPP は bounded-error probabilistic polynomial-time の略）．PP は，多項式時間確率 Turing 機械によって，1/2 より大きな確率で正しい答えを出すことのできる問題のクラスです．正解率は 1/2 に指数的に近い可能性もあるため，多数決で十分に誤り確率を低減させるには指数回の繰り返しを必要とします.

以上の計算量クラスには，以下の包含関係が知られています．二つ目は定義から自明です．NP $\subseteq$ PP は，非決定性 Turing 機械と確率 Turing 機械をベースにした PP の定義を考えれば自明であり，PP $\subseteq$ PSPACE は，確率 Turing 機械の計算木を各計算パスごとに模倣していって受理と拒否の計算パスの数の多数決を取れば示せます.

- P $\subseteq$ NP $\subseteq$ PP $\subseteq$ PSPACE
- P $\subseteq$ BPP $\subseteq$ PP

5.2 P の量子版：BQP

量子アルゴリズムによって多項式時間で解ける問題のクラスは，BQP(bounded-error quantum polynomial-time) と呼ばれています．これは大まかには P の量子版ですが，名前の通り厳密には BPP の量子版です．つまり，BQP は多項式時間量子アルゴリズム（H と Toffoli ゲートか

らなる万能ゲート集合のもとでの一様量子回路族）で任意の約束をみたす入力 $x \in A_{\text{yes}} \cup A_{\text{no}}$ に対して，確率 2/3 以上で正しい答えを出力することのできる問題のクラスです（成功確率 2/3 は BPP 同様に便宜上のものです）．3.3 章で述べた通り，乱択アルゴリズムは一様量子回路族で模倣可能なため，BQP は自然に BPP を含みます．Simon のアルゴリズムや Shor のアルゴリズムは，BQP が BPP より真に大きいことの証左を与える結果（BQP と BPP を分かつオラクル付き問題の存在）とみることができます．さらに BQP は，NP や NP の論理構造の拡張で得られたクラス PH（多項式階層）にさえ含まれないことを示唆する結果 [22] もあります（一方で，BPP は多項式階層に含まれることが知られています）．周期性のような特定の構造を持った問題ならば，古典計算量理論では比較的複雑度が高いと位置づけられる問題でも，量子アルゴリズムなら多項式時間で解けることがあるということです．

一方で，BQP が BPP に比べて非常に広い範囲の問題を含むクラスなのかというと，一般にはそうとは考えられていません．例えば，NP 完全問題は量子アルゴリズムをもってしても多項式時間で解けない（つまり NP $\not\subseteq$ BQP）だろうと考えられていますし，NP 完全でなくても，グラフ同型性判定問題や最短格子ベクトル問題なども（量子アルゴリズムの構築に関する精力的な研究の末）BQP には属さないであろうと考えられています．

BQP の限界を示す古典計算量クラスへの包含関係としては，まず BQP が PP に包含されていることが知られています．さらに，Aaronson は，PP が以下の事後選択 (postselection) の概念を用いた仮想量子計算で，多項式時間で計算可能な問題のクラス PostBQP と一致することを示しています（これによって，BQP が PP に含まれることの自然な解釈が与えられたと考えられます）．

定義 5.3. $A = (A_{\text{yes}}, A_{\text{no}})$ が PostBQP に属するとは，多項式時間量子アルゴリズム（一様量子回路族）M が存在して，任意の入力 x について以下の条件をみたすことをいう．なお M の出力ビットは最初の量子ビット（事後選択ビット）と異なるものとする．

1. $\Pr[M \text{ の最初の量子ビットを測定値が } 1] \geq 1/2^{\text{poly}(|x|)}$.
2. $x \in A_{\text{yes}}$ のとき，

   $\Pr[M \text{ の出力量子ビットの値が } 1 | M \text{ の事後選択ビットの値が } 1] \geq 2/3$.
3. $x \in A_{\text{no}}$ のとき，

   $\Pr[M \text{ の出力量子ビットの値が } 0 | M \text{ の事後選択ビットの値が } 1] \geq 2/3$.

PostBQP は 2019 年の Google チームによる実験で有名になった「量子超越性」というトピック（量子計算が出す確率分布が古典で効率的に模倣できないことを実証する試み）の理論的側面を支えるうえで重要な役割を果たしています.

BQP はよりマニアックには AWPP という PP のサブクラスにも含まれることが知られていて，現時点ではそれが最良の限界です（なお，AWPP は NP を含まないというオラクル付き問題による成果があります）.

5.3　NP の量子版：QMA

NP の量子版，つまり「入力が YES であるとき，YES であることが効率的に量子アルゴリズムで検証可能な問題」は，NP の定義に倣って次のように定義されています．検証アルゴリズムのみならず証拠も量子的に変更されていることに注意すべきです．なお，成功確率は 2/3 以上になっているように，これも厳密には，NP の乱択版である MA というクラスの量子版です（MA は魔法使い Merlin と Arthur 王の M と A です．Merlin が証拠を作り出せる計算能力無限のもので，Arthur が多項式時間の能力しか持たない検証者という設定です）.

定義 5.4. $A = (A_{\text{yes}}, A_{\text{no}})$ が QMA に属するとは，ある多項式時間量子アルゴリズム (検証者)V が存在して，任意の入力 x について以下の条件をみたす（p は多項式）.

完全性 (completeness) $x \in A_{\text{yes}}$ のとき，ある $p(|x|)$ 量子ビット状態 $|\varphi\rangle$（証拠 (witness)）が存在して

$$\Pr_V[V(x, |\varphi\rangle) = \text{accept}] \geq 2/3.$$

健全性 (soundness) $x \in A_{\text{no}}$ のとき，すべて $p(|x|)$ 量子ビット状態 $|\varphi\rangle$ に対して

$$\Pr_V[V(x, |\varphi\rangle) = \text{reject}] \geq 2/3.$$

QMA 特有の問題として知られているのが，次の代数的問題です.

問題 5.1 (GNM(Group Non-Membership))**.**

入力 有限群 G の要素 $h_1, \ldots, h_k, g$．ただし，G はオラクルとして与えられる（つまり，二つの元 $g_1, g_2 \in G$ に対する積 $g_1 g_2$ や g_1 の逆元 g_1^{-1} は，オラクル G への質問で得られる）.

出力 $g \notin H = \langle h_1, h_2, \ldots, h_k \rangle$ なら YES，そうでなければ NO.

実際，検証者は証拠として

$$|H\rangle := \frac{1}{\sqrt{|H|}} \sum_{h\in H} |h\rangle$$

を受け取れば，$g \in H$ のときは

$$|gH\rangle := \frac{1}{\sqrt{|H|}} \sum_{h\in H} |gh\rangle$$

が $|H\rangle$ と等しく，$g \notin H$ のときは

$$|gH\rangle \perp |H\rangle$$

となります．そのため，この二つのどちらなのかを，Hadamard テストにより高確率でチェックできます（もちろん，いつも $|H\rangle$ を受け取るとは限らないので，その場合の解析が必要ですが）．

また，NP 完全問題に対応する QMA 完全問題としては，以下の問題が代表的です．

問題 5.2 (k-LH(Local Hamiltonian))**.**

入力 n 個の量子ビットに作用するエルミート行列（ハミルトニアン）の集合 $S = \{H_1, H_2, \ldots, H_r\}$ および実数 α, β で以下をみたすもの

- 各 H_j（$j \in [r]$）は $0 \le H_j \le 1$ をみたし，k 個の量子ビットにしか非自明な作用をしない
- $\beta - \alpha \ge 1/\mathrm{poly}(n)$

出力 $H_S = \sum_{i\in S} H_i$ の最小固有値（最低エネルギーに対応）が α 以下なら YES，β 以上なら NO.

これは NP 問題 SAT（より正確には MAX-SAT）の量子版と考えられます．

例 5.1. 2SAT 式

$$F(x_1, x_2, x_3) = (\neg x_1 \vee x_2) \wedge (x_1 \vee x_3) \wedge (\neg x_2 \vee \neg x_3) \wedge (\neg x_1 \vee \neg x_3)$$

は，次のようなハミルトニアンの集合を対応させれば，自然に 2-LH の入力としてみることができます．

$$\begin{aligned}
H_1 &= |10\rangle\langle 10|_{12} := |100\rangle\langle 100| + |101\rangle\langle 101| \\
H_2 &= |00\rangle\langle 00|_{13} := |000\rangle\langle 000| + |010\rangle\langle 010| \\
H_3 &= |11\rangle\langle 11|_{23} := |011\rangle\langle 011| + |111\rangle\langle 111| \\
H_4 &= |11\rangle\langle 11|_{13} := |101\rangle\langle 101| + |111\rangle\langle 111|
\end{aligned}$$

$F(x_1, x_2, x_3)$ の四つの節が四つの H_j に対応しています．例えば，最初の節 $\neg x_1 \vee x_2$ は，$x_1 = 1$ かつ $x_2 = 0$ のとき充足されないので，割当を表す量子状態として $|10b\rangle$（$b \in \{0, 1\}$）が来たときに，正の固有値（ペナルティーとして与えられるエネルギーに対応）を与えるように，H_1 を対応させています．

k-LH が QMA に属することを保証する検証プロトコルは，次のようになります．

k-LH に対する QMA プロトコル：

レジスタ R 上に証拠の候補が $|\psi\rangle_R$ と与えられたとします．

1. レジスタ A に均等重ね合わせ状態

$$\frac{1}{\sqrt{r}} \sum_{j=1}^{r} |j\rangle_A$$

を準備します．

2. レジスタ A の中身が j のとき，R 上で POVM $\{H_j, I - H_j\}$ を実行します（この POVM は，H_j が $k = O(1)$ 個の量子ビットにしか非自明な作用をしないことから，定数個の量子ゲートからなる量子回路によって実行できます）．POVM 要素 H_j に対応する測定値を得たとき，受理します．

このとき，検証者が受理する確率は，

$$\Pr[\text{accept}] = \frac{1}{r} \sum_{j=1}^{r} \langle\psi|H_j|\psi\rangle = \frac{1}{r} \langle\psi|H|\psi\rangle \tag{5.1}$$

となります．よって YES 入力の場合，ある状態 $|\phi\rangle$ が存在して

$$\Pr[\text{accept}] \leq \frac{\alpha}{r}$$

となり，NO 入力の場合，すべての状態 $|\psi\rangle$ に対して

$$\Pr[\text{accept}] \geq \frac{\beta}{r}$$

となります．

一方で，k-LH が QMA 困難であることは，Cook-Levin の定理（SAT が NP 困難であることを示す定理）を量子化することで示されます．なお，k-LH は（MAX2SAT が NP 完全であるように）$k = 2$ に対して QMA 完全であることが示されています．

QMA と古典計算量クラスの包含関係としては，QMA $\subseteq$ PP が知られています．さらに，QMA は PP の部分クラス $\mathrm{A_0PP}$ （このクラスは SBQP という量子計算量クラスで特徴づけされています）にも含まれていて，それが現在の（古典計算量クラスへの包含に関する）最良の結果です．

5.4 量子対話型証明

対話型証明 (Interactive Proof) は，NP を通信プロトコルとしてみたときの NP の拡張概念です．NP は，計算能力無限のパーティ（証明者）からの情報（証拠）をもとに，多項式時間の能力を持つパーティ（検証者）が入力が YES か否かを検証する一方向通信のプロトコルとみなせます．この一方向通信を双方向通信（対話プロトコル）に拡張したのが対話型証明です．

定義 5.5. $A = (A_{\text{yes}}, A_{\text{no}})$ が IP に属するとは，証明者と検証者 V の対話プロトコルが存在して，以下の条件をみたす．

完全性 (completeness) $x \in A_{\text{yes}}$ のとき，V が 2/3 以上の確率で受理する（accept を出力する）ような証明者の対話プロトコルにおける戦略が存在する．

健全性 (soundness) $x \in A_{\text{no}}$ のとき，証明者がどんな戦略を取っても V が 2/3 以上の確率で拒否する（reject を出力する）

このような対話が検証能力を飛躍的にアップさせることは，IP = PSPACE という定理（例えば [3] を参照してください）が保証しています．ただし，PSPACE 問題を検証する対話型証明プロトコルは，多項式回の通信を必要としています．

量子対話型証明は，上記の対話型証明における次の点を量子的にしたものです．

- V は多項式時間量子アルゴリズムに変更
- 通信は量子通信に変更（つまり量子状態を送ることができる）

このような変更を行って得られたクラス（量子対話型証明で検証可能な問題のクラス）が QIP です．また，QIP(k) は QIP の部分クラスで，k 回の通信で検証可能な量子対話型証明をもつ問題のクラスです．図 5.1 は，QIP(3) に対する量子対話型証明を，量子回路の形で表現したものです．QIP(3) プロトコルの場合，

1 **回目の通信：証明者から検証者** 証明者は自分のメモリに対応する量子ビットと通信用の量子ビットにユニタリ行列 P_1 をかける．

2 **回目の通信：検証者から証明者** 検証者は自分のメモリに対応する量子ビットと通信用の量子ビットにユニタリ行列 V_1 をかける．

3 **回目の通信：証明者から検証者** 証明者は自分のメモリに対応する量子ビットと通信用の量子ビットにユニタリ行列 P_2 をかける．

検証者の判定 検証者は自分のメモリに対応する量子ビットと通信用の量子ビットにユニタリ行列 V_2 をかけて量子ビットの測定を行うことで受理か拒否かを判定する.

という形になります. V_1, V_2 は検証者によって実行されるので, 一様な多項式サイズの量子回路でなければなりません. 一方で, 証明者は能力無限なので, P_1, P_2 は任意のユニタリ行列が認められています.

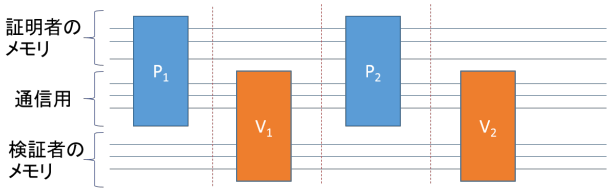

図 5.1: 量子対話型証明の量子回路による表現

量子対話型証明で検証可能な問題の例は, 以下の問題です.

問題 5.3 (QSD(Quantum State Distinguishability))**.**

入力 m 量子ビット量子回路 C_0, C_1

出力 $D(\rho_0, \rho_1) \geq a$ なら YES, $D(\rho_0, \rho_1) \leq b$ なら NO. ただし, $\rho_j := C_j(|0^m\rangle\langle 0^m|)$ (C_j が生成する量子状態) であり, a, b は $a^2 > b$ をみたす定数, $D(\rho_0, \rho_1)$ は (混合) 状態 ρ_1 と ρ_2 の (トレース距離と呼ばれる) 距離を表しています.

この問題は, 以下のような QIP(2) プロトコルで検証可能です.

QSD に対する QIP(2) プロトコル

1. 検証者はランダムに $b \in \{0, 1\}$ を選択して, $\zeta_b = (\rho_b)^{\otimes k}$ を証明者に送る (k は十分大きな多項式).
2. 証明者は $c \in \{0, 1\}$ を送る.
3. $c = b$ ならば検証者は受理. さもなければ拒否.

十分大きな k に対して, ζ_b は次の性質をみたします.

- YES 入力の場合, $D(\zeta_0, \zeta_1) \approx 1$ (量子状態 ζ_0 と ζ_1 は情報理論的にほぼ識別可能)
- NO 入力の場合, $D(\zeta_0, \zeta_1) \approx 0$ (ζ_0 と ζ_1 は情報理論的にほぼ識別不可能)

よって，YES 入力のときには，無限の能力を持つ証明者は ζ_0 か ζ_1 のどちらを検証者が送ってきたかがほぼわかるので，ほぼ確率 1 で検証者を受理させることができます．一方，NO 入力のときには，ζ_0 と ζ_1 はほぼ同じ状態であり，証明者をもってしてもほぼ識別不可能なので，検証者がどちらを送ってきたかを，ほぼ確率 1/2 でしか当てることはできません．つまり，ほぼ 1/2 の確率で検証者は拒否することができることになります．

QIP の検証能力に関しては，以下の二つが代表的な成果です．二つ目の成果は，古典の対話型証明では起こりえない[2]と考えられていて，量子対話型証明特有のものです．

- QIP = IP．つまり，量子対話型証明で検証可能な問題のクラスは，古典の対話型証明と変わらない．
- QIP = QIP(3)．つまり，QIP に属する全ての問題は，高々3 回の通信で検証可能．

5.5 多証明者量子対話型証明

対話型証明プロトコルにおいて，検証者が複数の証明者と対話することができれば，検証能力は上がるでしょうか? 複数の証明者は，プロトコルが始まる前（問題の入力を受け取る前）に通信して情報共有等をしてもよいのですが，いざ検証プロトコルが始まったら通信できないものとします．このような状況で検証可能な問題のクラスは，MIP(Multi-prover Interactive Proof の略) と名づけられています．このクラスについて，次の定理が知られています．

定理 5.1 (Babai-Fortnow-Lund 1991)**.** MIP = NEXP.

ここで NEXP は NP の指数時間版であり，PSPACE よりはるかに大きなクラスと考えられています．つまり，対話型証明において，複数の証明者と通信することは，単一の証明者と通信するよりも検証能力の意味で有益というわけです．

では，その量子版はどうでしょうか？ここで量子版を考えるとき，次のような点が量子的になりうることに注意すべきです．

1. 検証者のアルゴリズムを量子アルゴリズムに変更
2. 検証者と各証明者の通信を量子通信に変更

[2]古典の対話型証明によって，定数回の通信で検証可能な問題のクラスは，PSPACE（=IP）より低いクラスである PH に含まれることが知られています．

3. プロトコルが始まる前に証明者が共有する情報を量子情報に変更

3. のみ量子的にした場合のクラスは，MIP* と呼ばれています．MIP* は，通常の対話型証明において,「証明者たちは能力無限なんだから，前もって量子情報を共有する能力もありえるよね」という着想のもとで提案されました．

MIP* の検証能力の理解が一筋縄ではいかない点は，MIP* ⊆ MIP のみならず，MIP ⊆ MIP* という一見自明に見える関係も実は非自明という点にあります．実際，[8] では，2.3.1 章で紹介した Magic-Square ゲームを 3SAT に帰着することで，3SAT の充足可能性を検証する古典の多証明者対話型証明が，証明者が量子状態を使えるとすると，うまく検証できなくなることを示しています．

この問題は，その問題提起から約 10 年の歳月を経て，伊藤と Vidick [11] によって解決されました．

定理 5.2 (Ito-Vidick 2012)**.** NEXP ⊆ MIP*

一方で，1., 2., 3. のすべてを量子的にした場合のクラスは，QMIP*（あるいは QMIP）と呼ばれています．Reichard ら [23] は，このクラスが MIP* と等しいことを証明しました．

定理 5.3 (Reichard-Unger-Vazirani 2013)**.** QMIP* = MIP*

この結果には，2.2.6 章で紹介した CHSH ゲームが持つ硬直性（rigidity）という性質（つまり，CHSH ゲームに最適確率 $\cos^2 \frac{\pi}{8} \approx 0.85$ で勝利するには，本質的に 2.2.6 章で紹介した方法しかないこと）が，量子テレポーテーションを利用した量子計算とともに巧みに使用されています．

一方で，MIP* がどれくらい大きな計算量クラスなのかについては，2010 年代半ばになって研究が進み，最終的には計算不可能な問題まで含むほど大きなクラスになることが示されました [15]（RE は帰納的枚挙可能な言語のクラスです）．この結果は，量子計算におけるエンタングルメントの効果が，予想外に強力になりうることを示しているといえます．

定理 5.4 (Ji-Natarajan-Vidick-Whight-Yuen 2020)**.** MIP* = RE

関連図書

[1] Andris Ambainis, Kaspars Balodis, Jānis Iraids, Martins Kokainis, Krišjānis, Prūsis, and Jevgēnijs Vihrovs, Quantum speedups for exponential-time dynamic programming algorithms, in *Proceedings of the 30th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA2019)*, pp. 1783–1793 (2019).

[2] Andris Ambainis, Ashwin Nayak, Amnon Ta-Shma, and Umesh Vazirani, Dense quantum coding and quantum finite automata, *Journal of the ACM* **49**, pp. 496–511 (2002).

[3] Sanjeev Arora and Boaz Barak, *Computational Complexity*, Cambridge University Press (2009).

[4] László Babai and Peter G. Kimmel, Randomized simultaneous messages: solution of a problem of Yao in communication complexity, in *Proceedings of the 12th Annual IEEE Conference on Computational Complexity (CCC1997)*, pp. 239–246 (1997).

[5] Harry Buhrman, Richard Cleve, Serge Massar, and Ronald de Wolf. Nonlocality and communication complexity. *Review of Modern Physics* **82**, pp. 665–698 (2010).

[6] Harry Buhrman, Richard Cleve, John Watrous, and Ronald de Wolf. Quantum fingerprinting. *Physical Review Letters* **87**, 167902 (2001).

[7] Andrew Childs, Lecture Notes on Quantum Algorithms, May 2017, http://www.cs.umd.edu/˜amchilds/qa/qa.pdf

[8] Richard Cleve, Peter Høyer, Benjamin Toner, and John Watrous, Consequence and limits of nonlocal strategies, in *Proceedings of the 19th IEEE Conference on Computational Complexity (CCC2004)*, pp. 236–249 (2004).

[9] Alexander M. Dalzell, Sam McArdle, Mario Berta, Przemyslaw Bienias, Chi-Fang Chen, András Gilyén, Connor T. Hann, Michael J. Kastoryano, Emil T, Khabiboulline, Aleksander Kubica, Grant Salton, Samson Wang, and Fernando G. S. L. Brandão, Quantum algorithms: A survey of applications and end-to-end complexities, arXiv: 2310.03011 (2023)

[10] 石坂智，小川朋宏，河内亮周，木村元，林正人，量子情報科学入門，共立出版 (2015).

[11] Tsuyoshi Ito and Thomas Vidick. A multi-prover interactive proof for NEXP sound against entangled provers, in *Proceedings of the 53rd Annual IEEE Symposium on Foundations of Computer Science (FOCS2012)*, pp. 243–252 (2012).

[12] Taisuke Izumi, François Le Gall, and Fredric Magniez. Quantum distributed algorithm for triangle finding in the CONGEST model, arXiv:1908.11488 (2019).

[13] Stephen P. Jordan, Quantum Algorithms zoo, https://quantumalgorithmzoo.org/

[14] François Le Gall, Masayuki Miyamoto, and Harumichi Nishimura, Distributed quantum interactive proofs, arXiv:2210.01390 (2022).

[15] Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen. $\mathrm{MIP}^* = \mathrm{RE}$. arXiv:2001.04383 (2020).

[16] A. Yu. Kitaev, A. H. Shen, and M. N. Vyalyi. *Classical and Quantum Computation*, Graduate Studies in Mathematics Volume 47, American Mathematical Society (2002).

[17] David N. Mermin, *Quantum Computer Science*, Cambridge University Press (2007). （和訳：木村元訳，量子コンピュータ科学の基礎，丸善 (2009).）

[18] Michael Mitzenmacher and Eli Upfal, *Probability and Computing: Randomized Algorithms and Probabilistic Analysis*, Cambridge University Press (2005). (和訳：小柴健史・河内亮周共訳，確率と計算 —乱択アルゴリズムと確率的解析—，共立出版 (2009).)

[19] 森前智行，量子計算理論，森北出版 (2017).

[20] Michael A. Nielsen and Isaac L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press (2000). (和訳：木村達也訳，量子コンピュータと量子通信（3 分冊），オーム社 (2005).)

[21] 西村治道，基礎から学ぶ量子計算，オーム社（2022）.

[22] Ran Raz and Avishay Tal, Oracle separation of BQP and PH, in *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing (STOC2019)*, pp. 13–23 (2019).

[23] Ben W. Reichard, Falk Unger, and Umesh V. Vazirani, Classical command of quantum systems.*Nature* **496**, pp. 456–460 (2013).

[24] Seiichiro Tani, A fast exact quantum algorithm for solitude verification, *Quantum Information and Computation* **17**(1-2), pp. 15–40 (2017).

[25] Thomas Vidick and John Watrous, Quantum Proofs, *Foundations and Trends in Theoretical Computer Science* **11**(1-2), pp. 1–215 (2015).

[26] Ronald de Wolf, Quantum Computing: Lecture Notes, arXiv:1907.09415 (2019).