

# 量子情報とその幾何学

澤山晋太郎

# 目次

1	はじめに	3
2	量子情報理論	4
2.1	量子情報で使う量子力学	5
2.2	量子テレポーテーション	10
2.3	量子計算機(グローバーのアルゴリズム)	12
2.4	計算の複雑さ	15
3	エンタングルメント	18
3.1	発見と定義	19
3.2	エンタングルメントの測度	20
3.3	エンタングルメントしている必要条件と十分条件	24
3.4	エンタングルメントの構造	27
3.4.1	大域的ユニタリ変換における構造	27
3.4.2	エンタングルメント抽出における構造	29
4	量子状態の幾何学	31
4.1	1-qubit の幾何学	31
4.2	2-qubit の幾何学	35
4.2.1	状態とセパラブル領域の視覚化	35
4.2.2	セパラブル領域の体積	42
5	まとめ	42
A	基底空間が正四面体になることの証明	43
B	ファイバーに沿ったときの状態の変化の証明	45

## 1 はじめに

量子情報理論は量子計算 [1],[2],[3] や、量子テレポーテーション [4] などを含む新しい理論である。とりわけショアによって 1994 年に素因数分解を多項式時間で解いてしまうアルゴリズム [3] が発見され、それがこの研究分野を大きく前進させることとなった。それまでの古典的な (もちろん現在のスーパーコンピュータもこれに含まれる) 計算機では素因数分解は与えられた数の桁数に応じて指数関数的時間が掛かってしまっていた。具体的に、例を挙げるならば、十数桁の素因数分解では現在のコンピュータでは宇宙年齢を超えるほど掛かる時間も量子計算機を使えばたったの数年単位でできてしまうことになる。このことは現在の情報伝達の暗号を素因数分解によっておこなっている現状としては驚きをもって受け入れられることになった。また、量子テレポーテーションでは空間的に離れた領域間での量子状態の伝達が可能となった。

これらの発見に伴って量子力学の基礎理論 [5] をより深く理解しようとする研究が進み、他方、量子力学を使った暗号や通信理論など、古典情報理論を量子論で置き換えるという活動も起こった。特に、量子テレポーテーションの特徴であるエンタングルメント (量子纏れ合い) という概念が具体的に研究されるようになった。エンタングルメントは量子力学固有の現象であり、古典理論にアナロジーを持たないことが魅力の一つであり、また、応用面から見ても有意義なものである。エンタングルメントは量子テレポーテーションから、量子暗号 [6]、量子並列計算機 [7] など多様な応用面を持っている。量子情報理論が始まってから最近まで、量子計算の指数関数的スピードアップそのものにも重要な役割を果たしているという考え方もあったが、今日ではそれに対して否定的な考えが強まっている。

第 2 章では量子情報理論の応用的側面を見る。まず、2.1 で量子情報理論の枠組みを一通り記述する。次に 2.2 で量子情報理論の大きな要である量子テレポーテーションについて概説する。次に、2.3 で量子計算が実際にどのようななされるかを見る。量子計算自体の概念は 1985 年にドイチ [2] によって提案されたが、具体的なアルゴリズムはショア 1994 年の [3] から始まる。実はドイチ・ジョザおよびサイモンのアルゴリズムのほうが先だが、興味深いものとしてはショアがはじめてである。ここではグローバーによって考案された検索のアルゴリズム [8] を記述する。最後に 2.4 で計算の複雑さ [9] について概説する。ここでは量子計算によって生み出された新しい計算量のクラス [10] を説明する。

第 3 章では量子情報において重要な役割を果たすエンタングルメントについて概説する。まず、3.1 でエンタングルメントがアインシュタインーパドフスキーローゼンによって発見されたことを示し、その頭文字をとった EPR 実験 [11] について述べる。次にエンタングルメントの定義を述べその意味を明らかにする。3.2 ではエンタングルメントの測度 [12] について述べる。こ

れはエンタングルメントが強いかどうかを測定するものとして利用される。3.3 ではペレスとホロデッキによって与えられた状態がエンタングルしているかどうかの判定条件 [13][14] を記述する。これはまだ任意の状態の必要十分条件ではないが、限られた系においては必要十分条件として利用できる。3.4 で、エンタングルメントの状態空間における構造を見る。3.4.1 では局所化するときにはじめてエンタングルメントが発生するのに対して大域的なユニタリ変換は実質的に禁止もしくは不可能だとされているのに対し、数学的な側面からあえて大域的ユニタリ変換を行ったときのエンタングルメントの測度の変化を記述する。3.4.2 ではエンタングル抽出 [6] というエンタングルメントの測度を増大させる方法についてまず述べ、エンタングルメントを増大できる境界について述べる。

第4章では私が行った研究について述べる。初めに4.1 で現在完全に分かっているスピン  $\frac{1}{2}$  系での量子状態の幾何について概説し、その幾何学的イメージの持つ大切さについて述べる。4.2 は二つの最近の量子情報幾何に関するトピックを述べる。まず第一に、4.2.1 ではスピン  $\frac{1}{2}$  の粒子が二つあったときの(これを 2-qubit という)系の幾何学をみる。この系を調べるのには理由がある。それはエンタングルメントが発生する最小の次元だからである。この仕事はまだ完全ではないが、四次元の断面を描くことに成功した。それまでは二次元断面のピクチャーしかなく、不十分であったが、これで 2-qubit の状態空間およびエンタングル境界の大体のイメージをつかむことができる。4.2.2 ではエンタングルしていない領域、すなわち分離可能 (セパラブル) 領域の体積変化を全状態空間との比率として求めた。ここでは純粋なセパラブル状態に近づくにしたがってエンタングル状態の比率が増加するという直感に反した結果が得られた。

最後に5で今まで私が行ってきた研究についてまとめ、客観的に評価することによって次に研究すべきことがらを言及する。

## 2 量子情報理論

量子情報理論では量子力学の基礎理論と情報理論が融合したものである。この章ではあえて情報理論にはあまり深く立ち入らずに、量子力学の基礎知識だけで完結するように努めた。量子力学の基礎理論も、量子情報で使うものは普通の量子力学の教科書には深く書いてないので、初めにそれを概説する。その次に量子情報の要である量子テレポーテーションと量子計算の一例を概説する。最後に、これは情報理論的になってしまうが計算の複雑さについて述べる。

## 2.1 量子情報で使う量子力学

量子情報理論では主として有限次元のヒルベルト空間のみを扱う。 $n$ 次元のヒルベルト空間は複素  $n \times n$  行列と同様に扱っていい [16]。スペクトルは以後全てこの行列の固有値として扱っていいことを示している。

状態は純粋状態の一般化として密度行列によって記述される。密度行列は  $\rho$  によって記述され、その定義は以下のとおりである。

$$\rho \equiv \sum_i p_i |\psi_i\rangle\langle\psi_i| \quad (1)$$

ここで  $|\psi_i\rangle$  は純粋状態で、 $p_i \geq 0$  はその純粋状態が入っている確率をあらわす。もちろん  $\sum_i p_i = 1$  である。つまり密度行列とは純粋状態の重ね合わせである。これはまた式 (2)(3) のようにに再定義してもよい。

$$\text{Tr}\rho = 1 \quad (2)$$

$$\rho^\dagger = \rho \geq 0 \quad (3)$$

ここで演算子  $A$  の期待値は

$$\langle A \rangle = \sum_i p_i \langle \psi_i | A | \psi_i \rangle \quad (4)$$

より、

$$\langle A \rangle = \text{Tr}(\rho A) \quad (5)$$

となることがわかる。つまり密度行列さえ知っていれば、あらゆる演算子の期待値を求めることが可能であり、密度行列に状態の全ての情報が入っていることになる。

密度行列の性質としては次のものがある。まず上に述べたようにエルミートであり、Trace は 1 である。また、正定値行列である。これはどんな  $|u\rangle$  に対しても、

$$\langle u | \rho | u \rangle \geq 0 \quad (6)$$

を意味する。また、エルミートなので対角化可能であり、固有値は常に非負の数である。また、対角化するようなユニタリ行列が常に存在する。また、密度行列の二乗の対角和は 1 以下である。

$$\text{Tr}\rho^2 \leq 1 \quad (7)$$

これは以下の不等式から明らかであろう。

$$\sum_j \rho_{jj} \leq \left( \sum_j \rho_{jj} \right)^2 = 1 \quad (8)$$

次に観測 (measurement) の公理を示す。

観測の公理: 量子測定は集合  $\{M_m\}$  によって記述される。これらは measurement operator と呼ばれ、状態空間に作用する。指数  $m$  は観測で得られる結果を示している。もしも状態空間が  $|\psi\rangle$  だとすると結果  $m$  が得られる確率は

$$p(m) = \langle \psi | M_m^\dagger M_m | \psi \rangle \quad (9)$$

であり、その観測後の状態は

$$\frac{M_m |\psi\rangle}{\sqrt{\langle \psi | M_m^\dagger M_m | \psi \rangle}} \quad (10)$$

である。measurement operator は完備性を持っている。つまり

$$\sum_m M_m^\dagger M_m = I \quad (11)$$

ここで言う完備性は確率の和が1であるという要請から来ている。

$$1 = \sum_m p(m) = \sum_m \langle \psi | M_m^\dagger M_m | \psi \rangle \quad (12)$$

ここで一般の状態空間である密度行列に観測の概念を入れるために POVM (Positive Operator Valued Measure) [1] という概念を導入する。POVM とは以下の operator の集合である。

$$E_m = M_m^\dagger M_m \quad (13)$$

この operator を導入すると、確率だけを求めることが容易になる。なぜなら、初めの状態を  $|\psi_i\rangle$  とし、それから  $m$  という結果が出る条件付確率は、

$$p(m|i) = \text{tr}(\langle \psi_i | M_m^\dagger M_m | \psi_i \rangle) = \text{tr}(M_m^\dagger M_m |\psi_i\rangle \langle \psi_i|) \quad (14)$$

であり、それを足し合わせたもの

$$\begin{aligned} p(m) &= \sum_i p(m|i) p_i \\ &= \sum_i p_i \text{tr}(M_m^\dagger M_m |\psi_i\rangle \langle \psi_i|) \\ &= \text{tr}(E_m \rho) \end{aligned} \quad (15)$$

となるからである。

ここでもう一度量子力学の公理をまとめてみる。

公理 1 : 量子状態は密度行列  $\rho$  で表され、その満たすべき条件は、(2) および (3) である。

公理 2 : 密度行列の時間変化はリウビル方程式によって与えられる。つまり、

$$\frac{\partial \rho}{\partial t} = -\frac{i}{\hbar} [\mathcal{H}, \rho] \quad (16)$$

公理 3: 観測は  $E_m$  の集合である POVM(13) によってあらわされ、観測結果  $m$  があらわれる確率は

$$p(m) = \text{tr}(E_m \rho) \quad (17)$$

であらわされる。

次に量子操作 (quantum operation) について述べる。量子操作とは、量子状態をあるゲートに通すことであり、量子状態はユニタリ変化以外の変化を行うこととなる。量子操作を通して量子状態は次のように変化する。

$$\rho' = \mathcal{E}(\rho) \quad (18)$$

$$= \sum_k E_k \rho E_k^\dagger \quad (19)$$

ここでの  $E_k$  は POVM とは違うことに注意されたい。POVM はあくまでも測定の実演である。また、量子操作の中でより物理的なものは CP マップと呼ばれるオペレーションの集合で、これは量子操作を任意のヒルベルト空間に拡張したときにも正であるようなオペレーションである。量子操作の変化は次のように解釈できる。つまり、 $\rho$  は環境と接していて、環境と状態のユニタリ変化が起こるわけだが、我々は状態しか見ていない。そのため非物理的なユニタリ変化でない変化が見える。これを式で表せば、

$$\mathcal{E}(\rho) = \sum_k \langle e_k | U [\rho \otimes |e_0\rangle\langle e_0|] U^\dagger | e_k \rangle \quad (20)$$

であり、

$$E_k = \langle e_k | U | e_0 \rangle \quad (21)$$

である。ここで  $|e_l\rangle$  は環境の正規直行基底である。環境の初期状態は  $|e_0\rangle\langle e_0|$  とした。ここでも  $\text{tr} \mathcal{E}(\rho) = 1$  より  $E_k$  における完備性が導かれる。

$$1 = \text{tr}(\mathcal{E}(\rho)) \quad (22)$$

$$= \text{tr}\left(\sum_k E_k \rho E_k^\dagger\right) \quad (23)$$

$$= \text{tr}\left(\sum_k E_k^\dagger E_k \rho\right) \quad (24)$$

より、

$$\sum_k E_k^\dagger E_k = I \quad (25)$$

である。量子操作は情報理論的側面からゲートやチャンネルとよばれ、図 1 のように示されることが多い。また、量子操作を強調するときには図 2 のように書かれる。とくに量子情報理論において重要となるのは、アダマール (Hadamard) ゲートとコントロールドノット (Controlled-not) ゲートである。これからはスピン  $\frac{1}{2}$  の系のみ (もちろん多粒子系も) を考えることにする。コ

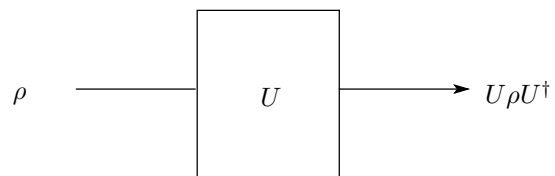


図 1: ユニタリゲート

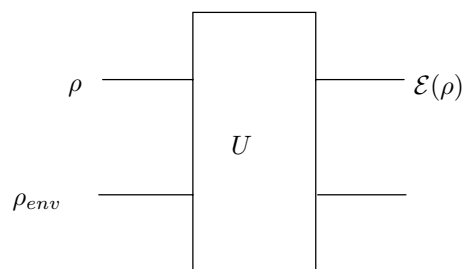


図 2: 一般の量子操作

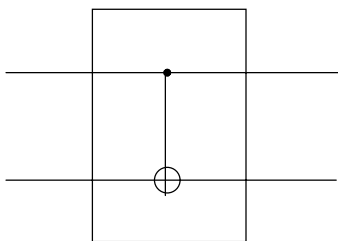


図 3: コントロールドノットゲート



ントロールドノットゲートは図 3 のようにかかれ、●はその状態に制御されていることを示している。ここで、ゲートの一覧を記述する。

$$\text{Hadamard} \quad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad (26)$$

$$\text{Pauli} - X \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad (27)$$

$$\text{Pauli} - Y \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad (28)$$

$$\text{Pauli} - Z \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad (29)$$

$$\text{Phase} \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \quad (30)$$

コントロールドノットゲートはスピン系 1 の状態が  $|0\rangle$  のときはもう片方のスピンはそのままにしてスピン系 1 の状態が  $|1\rangle$  のときスピン系 2 の状態を反転させる操作である。具体的に、

$$|00\rangle \rightarrow |00\rangle, |01\rangle \rightarrow |00\rangle, |10\rangle \rightarrow |11\rangle, |11\rangle \rightarrow |10\rangle \quad (31)$$

であり、この大域的ユニタリ変換は

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad (32)$$

と表される。このようにコントロールさせることは今までにあげた量子操作にもあてはまり、例えばコントロールド Pauli-X 操作などを作ることができる。

以下、量子情報に必要な数学的知識をまとめる。

### Polar decomposition

$A$  をベクトル空間  $V$  の線形演算子とする。この時、ユニタリ演算子  $U$  と正のオペレーター  $J, K$  が存在し、

$$A = UJ = KU \quad (33)$$

とかける。ここで  $J, K$  は唯一つの正のオペレーターであり、 $J = \sqrt{A^\dagger A}$ ,  $K = \sqrt{AA^\dagger}$  である。

### Singular value decomposition

$A$  を正方行列とする。このときユニタリ行列  $U, V$  と対角行列  $D$  が存在し、その成分は非負の数である。そして、

$$A = UDV \quad (34)$$

とかける。 $D$  の対角要素は singular value と呼ばれる。

シュミット分解 [17]

$|\phi\rangle$  を AB の合成系の純粋状態とする。そのとき A に対しての正規直行基底  $|i_A\rangle$  と B に対しての正規直行基底  $|i_B\rangle$  が次のように存在する。

$$|\phi\rangle = \sum_i \lambda_i |i_A\rangle |i_B\rangle \quad (35)$$

ここで  $\lambda_i$  は非負の数であり、 $\sum_i \lambda_i^2 = 1$  である。これはシュミット係数と呼ばれる。

ホンノイマンエントロピー [18]

$$S(\rho) = -\text{tr}(\rho \log \rho) \quad (36)$$

これは量子状態がいかにランダムかを測定する量である。これはシャノンエントロピーの拡張であり、 $\rho$  が対角の時はシャノンエントロピーと一致する。この形は加法性の要求からである。

相互エントロピー [19]

$$S(\rho||\sigma) = -\text{tr}(\rho \log \rho) - \text{tr}(\rho \log \sigma) \quad (37)$$

で定義される。この量は  $\rho$  が  $\sigma$  に対してどのくらい近いかを測る量である。また、この量は常に正か 0 以上ということが示されている。

$$S(\rho||\sigma) \geq 0 \quad (38)$$

## 2.2 量子テレポーテーション

量子テレポーテーション [4] とは、二人の離れた二点間において量子状態の伝送をするオペレーションである。これからしばしば現れる概念として、局所化のことを説明する必要がある。局所化とは 2 粒子状態で局所ユニタリ変換しか行ってはならないという制限を課すことを意味する。この概念は EPR の論文 [11] において初めて導入された。ここではまず EPR 実験について概説し、その次に Bell によって導入された状態に言及し、その後で量子テレポーテーションのオペレーションについて概説する。

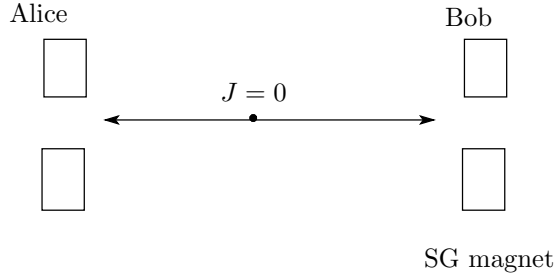


図 4: EPR Experiment

EPR 実験とは、スピン 0 の状態を座標軸原点においてスピン  $\pm\frac{1}{2}$  に崩壊させる思考実験である (図 39)。当初は EPR の三人は崩壊後の粒子の座標と運動量を測定する実験だったが、後にボームはスピンを測る実験として記述した。この実験で得られる状態は次式のシングレット状態である。

$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \quad (39)$$

この実験で特徴的なことは、スピンを測る二人のペアのうち一人がスピン up を測定したとすると、もう片方は必ずスピン down を測定することになることである。これは一見因果律を破るように思える。そしてこの因果律の破れの見せかけは Bell によってエンタングルメントという概念に到達した。よく知られた Bell の不等式 [20] の破れはエンタングルメントが強いほど破れる。そして、Bell はその不等式を最大に破り、式 (39) と直交する正規直行基底を次のように定めた、

$$\begin{aligned} |\Phi_{\pm}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle) \\ |\Psi_{\pm}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) \end{aligned} \quad (40)$$

量子テレポーテーションはまさに上述した状態をもちいて行う。通信を行う人物は Alice と Bob だとし、伝送したい状態は

$$|\psi\rangle = a|0\rangle + b|1\rangle \quad (41)$$

であり、Alice の側が持っているとする。ここで Alice は  $a$  と  $b$  の値を知らないとする。二人のペアは初めから  $\Psi_+$  を持っている (share している) とする。すると全量子状態は、直積で書け、

$$|\Psi_{AB}\rangle = (a|0\rangle + b|1\rangle)(|00\rangle + |11\rangle)/\sqrt{2} \quad (42)$$

である。ここで Bell の基底を用いてこの式を展開すると、

$$\begin{aligned} |\Psi_{AB}\rangle &= (a|000\rangle + a|011\rangle + b|100\rangle + b|111\rangle)/\sqrt{2} \\ &= \frac{1}{2} [|\Psi_+\rangle(a|0\rangle + b|1\rangle) + |\Psi_-\rangle(a|0\rangle - b|1\rangle) \\ &\quad + |\Phi_+\rangle(a|1\rangle + b|0\rangle) + |\Phi_-\rangle(a|1\rangle - b|0\rangle)] \end{aligned} \quad (43)$$

量子テレポーテーションの手順は以下のとおりである。1. Alice は Projective measurement を Bell の基底について行う。ここで得られる結果は式 40 の四つのうちのいずれかで、確率はランダムである。2. ではもし Alice は  $|\Phi_+\rangle$  を得たとする。すると初めの状態は

$$|\Phi_+\rangle(a|1\rangle + b|0\rangle) \quad (44)$$

に射影される。3. Bob は Alice からどの量子状態を観測したかの古典情報を得て、それに見合ったオペレーションを行う。例えば  $|\Phi_+\rangle$  を得たという答えを聞いたら、NOT オペレーションつまり  $|0\rangle \rightarrow |1\rangle, |1\rangle \rightarrow |0\rangle$  というユニタリオペレーションを行う。すると、Bob には  $a|0\rangle + b|1\rangle$  という初めに Alice が伝送したかった状態を得ることになる。

ここでこのような完全な伝送は初めに  $|\Psi_+\rangle$  という、後述する最もエンタングルした状態をシェアしていたために可能となった。エンタングルメントの定義は後で述べるが、今は Bell の不等式を最大に破る状態が最もエンタングルしていると考えればよい。これがエンタングルメントが重要であることを示す大きな要因である。また、このテレポーテーションは因果律を破るかのように見えるが、それは見かけ上のことである。このオペレーションで重要なもう一つの要因は古典情報の伝達にある。Alice がどの状態を得たかを Bob に伝えなければこの操作は完了しない。よって、古典情報の伝達は因果律の範囲に入るので、量子テレポーテーションは因果律を破っていない情報伝達であることが分かる。

もし仮に初めにシェアしていた状態が最もエンタングルした状態でなければこの伝達は完全な精度で行われない。そこでエンタングルメントの測度を考える必要が出てくるのである。

## 2.3 量子計算機 (グローバーのアルゴリズム)

グローバーアルゴリズム [8] とは  $N$  個のデータからそのうちの一つを検索する検索のアルゴリズムである。まず、量子計算に必要な概念であるオラクルを定義しなければならない。オラクルとはある種のブラックボックスで、具体的にどのような操作を行うかを無視することに始まる。基本的にその操作はユニタリ操作である。例えば次のように作用する。

$$O|x\rangle|q\rangle \rightarrow |x\rangle|q \oplus f(x)\rangle \quad (45)$$

ここで  $\oplus$  は mod2 の和をあらわしている。また、 $|x\rangle$  はレジスターと呼ばれ、 $|q\rangle$  はオラクル qubit と呼ばれる。検索のアルゴリズムでは初めにオラクル qubit を  $|0\rangle$  にしておいて、 $x = x_0$  のときだけ  $f(x) = 1$  とすればよい。ここで  $x_0$  が今見つけたい量子状態だとしている。この検索アルゴリズムは  $N$  個のうちから  $M$  個を検索するアルゴリズムにも容易に拡張できる。また、オラ

クル qubit を  $(|0\rangle - |1\rangle)/\sqrt{2}$  にすることによって、

$$O|x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \rightarrow (-1)^{f(x)}|x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \quad (46)$$

という形にすることもできる。この形では結局、

$$O|x\rangle \rightarrow (-1)^{f(x)}|x\rangle \quad (47)$$

という操作が行われたことになる。

まず、 $|0\rangle^{\otimes n}$  という状態が用意されていて、その中から  $x_0$  番目の状態を取り出す。初めにアダマールゲートを通して、状態を次のように変化させる。

$$|\phi\rangle = \frac{1}{N^{1/2}} \sum_{x=0}^{N-1} |x\rangle \quad (48)$$

量子検索アルゴリズムはグローバ操作の連続的施行によってなされる。グローバ操作とは以下の一連の操作である。

- (1) オラクル  $O$  を実行する。
- (2) アダマール変換  $H^{\otimes n}$  を実行する。
- (3) 条件付位相変換を行う。つまり、

$$|x\rangle \rightarrow -(-1)^{\delta_{x0}}|x\rangle \quad (49)$$

- (4) アダマール変換  $H^{\otimes n}$  を実行する。

ここで (3) は  $2|0\rangle\langle 0| - I$  と置き換えられるので (2) から (4) の操作は

$$H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n} = 2|\phi\rangle\langle\phi| - I \quad (50)$$

となるのでグローバ操作は、

$$G = (2|\phi\rangle\langle\phi| - I)O \quad (51)$$

となっていることが分かる。

今度はこれを幾何学的に見てみよう。 $M$  この状態を検索して取り出すオペレーションを考える。まず、状態を二つに分けて考える。

$$|\alpha\rangle \equiv \frac{1}{N-M} \sum_{x \notin \text{solution}} |x\rangle \quad (52)$$

$$|\beta\rangle \equiv \frac{1}{M} \sum_{x \in \text{solution}} |x\rangle \quad (53)$$

すると初めの状態は、

$$|\phi\rangle = \sqrt{\frac{N-M}{N}}|\alpha\rangle + \sqrt{\frac{M}{N}}|\beta\rangle \quad (54)$$

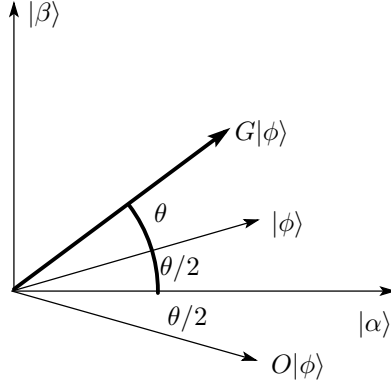


図 5: Grover 操作

となる。ここで、 $\cos \theta/2 = \sqrt{(N-M)/N}$  とおけば、

$$|\phi\rangle = \cos \theta/2 |\alpha\rangle + \sin \theta/2 |\beta\rangle \quad (55)$$

となる。ここで一回のグローバー操作によって状態は次のように変化する。

$$G|\phi\rangle = \cos \frac{3\theta}{2} |\alpha\rangle + \sin \frac{3\theta}{2} |\beta\rangle \quad (56)$$

これを図に表したのが図 5 である。さらにこの操作を何度も行ってやることによって、

$$G^k |\phi\rangle = \cos \left( \frac{2k+1}{2} \theta \right) |\alpha\rangle + \sin \left( \frac{2k+1}{2} \theta \right) |\beta\rangle \quad (57)$$

が得られる。ここで  $|\beta\rangle$  の確率振幅を最大にするような  $k$  の時に観測してやれば、解である  $|\beta\rangle$  を取り出せることができる。 $G$  が必要になる回数は  $O(\sqrt{N/M})$  である。

以上をまとめると次のようになる。

インプット: ブラックボックスのオラクルがあり、 $O|x\rangle|q\rangle = |x\rangle|q \oplus f(x)\rangle$  である。ここで  $f(x) = 0, \text{ for all } 0 \leq x < 2^n$  であり、これは  $x_0$  を除き、 $f(x_0) = 1$  である。アウトプット:  $x_0$  ランタイム:  $O(\sqrt{2^n})$  のオペレーションを必要とする。成功する確率は  $O(1)$  である。操作:

$$\begin{aligned} 1 & \quad |0\rangle^{\otimes n} |0\rangle \\ 2 & \quad \rightarrow \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \left[ \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] \\ 3 & \quad \rightarrow [(2|\phi\rangle\langle\phi| - I)O]^{\otimes R} \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \left[ \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] \\ & \approx |x_0\rangle \left[ \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] \\ 4 & \quad \rightarrow x_0 \end{aligned}$$

ここで  $R \approx \pi\sqrt{2^n}/4$  である。古典検索アルゴリズムが  $O(N)$  かかったことに  
対して量子コンピュータでは  $O(\sqrt{N})$  にかかるのである。この計算の複雑さにつ  
いては次章で説明する。また、グローバールゴリズムは最適であることも指  
摘されている。

このように量子計算機は今までの古典計算機の計算測度を上回るアルゴリ  
ズムが存在する。これらのアルゴリズムの発見によって量子情報の研究は盛  
んになった。

## 2.4 計算の複雑さ

計算の複雑さとは、ある計算を行うのに必要な時間 (オラクルの回数) や  
どれだけビットを用いなければならないかを分類したものである。ここでは  
まず初めに古典計算における計算の複雑さについて概説し、その後で量子計  
算機における計算の複雑さについて概説する。

まず、古典計算機における計算の複雑さを説明するためには、チューリン  
グマシン [21] の説明をする必要がある。チューリングマシンはテープ、ヘッ  
ドと有限制御部から構成されている。テープは現在のコンピュータの記憶装  
置 (メモリ) に相当し、ヘッドはメモリへの読み書き装置に相当する。また、  
有限制御部は中央処理装置 (CPU) に対応する。テープは同じ大きさの区間に  
区切られていて、右方向に無限に伸びている。テープの区間には左から順番  
に  $0, 1, 2, \dots$  と番号がつけられているものとする。

ヘッドは各時点において、テープの 1 つの区間に対して記号の読み出しや、  
書き込みを行うことができ、テープ上を 1 区間ずつ左右に移動するか、ある  
いは静止していることができる。テープの 1 区間には、あらかじめ指定され  
た有限種類の記号のうち 1 つを書き込むことができる。このテープ上で使用  
できる記号の有限集合のことを、テープ・アルファベットという。また、各  
区間には空白記号を書き込むことができる。空白記号は  $B$  で表される。右方  
向に無限に伸びるテープ上の有限個を除く全ての区間には空白記号が書き込  
まれていると仮定する。

各時点における有限制御部の状態と、その時点でヘッドが呼んでいる記号  
の組に対して、機械の次の 1 ステップの動作、すなわち次の状態への遷移、  
テープへの書き込み、ヘッドの移動の仕方がプログラムとして指定される。  
このようなプログラムは状態遷移関数として与えられる。例えば、状態遷移  
関数として以下のものを考えてみる。

$$\delta(q_0, 0) = (q_0, 0, R)$$

$$\delta(q_0, 1) = (q_0, 1, R)$$

$$\delta(q_0, B) = (q_1, 0, L)$$

ここで  $\delta(p, a) = (q, b, d)$  は、有限制御部の状態が  $p$  で、ヘッドが読み込んだ記号が  $a$  ならば、状態を  $q$  に変え、テープ上の現在ヘッドがある区間に記号  $b$  を書き込み、 $d$  の値が  $R, L, N$  のうちどれかにしたがってヘッドを、右へ 1 区間移動する、左へ 1 区間移動する、または移動させないことを意味している。また、 $q_1$  のような状態を最終状態と呼ぶ。

チューリングマシンとは以下の条件をみたす 7 つの組  $(Q, \Sigma, \Gamma, \delta, q_0, B, F)$  として定義される。

1.  $Q$  は状態の空でない有限集合
2.  $\Gamma$  はテープ記号の有限集合 (テープアルファベットという)
3.  $B \in \Gamma$  は空白記号
4.  $\Sigma \subseteq \Gamma - \{B\}$  は入力記号の有限集合 (入力アルファベットという)
5.  $q_0 \in Q$  は初期状態
6.  $F \subseteq Q$  は最終状態の有限集合 (最終状態に入ったときにはチューリングマシンは停止するものとする)
7.  $\delta: Q \times \Gamma \rightarrow Q \times \Gamma \times \{R, L, N\}$  は状態遷移関数である

このチューリングマシンのことを決定性チューリングマシンとも呼ぶ。ここでさらに非決定性チューリングマシンも定義する。非決定性チューリングマシンはチューリングマシンの定義の条件 7 が以下のものに置き換わったものである。

7.  $\delta: Q \times \Gamma \rightarrow \mathcal{P}(Q \times \Gamma \times \{R, L, N\})$

ここで  $\mathcal{P}(S)$  は  $S$  の部分集合全体からなる集合 (べき集合) をあらわしている。そのほかに多テープチューリングマシンや可逆チューリングマシン、などがあるがここでは詳細にはふれない。多テープチューリングマシンはテープが  $k$  個からなるチューリングマシンで、 $k$ -TM と書く。

では計算可能性について簡単に説明する。1931 年にゲーデルによって「数学的命題の中には真とも偽とも証明できないものが存在する」という不完全性定理が証明された。そのなかで帰納的関数という関数のクラスを定義した。帰納的関数にはその値を計算するためのアルゴリズムが必ず存在する。チャーチは計算可能な関数について次のような提唱をした。それは「計算可能な関数とは帰納的関数のこととしよう」というものであり、計算論のほとんど全ての研究者に受け入れられている。

ここで万能チューリングマシンの定義を述べる。万能チューリングマシンとは、任意のチューリングマシン  $M$  と任意の入力記号列  $x$  が与えられたときに、 $x$  に対する  $M$  の動作を模倣することができるチューリングマシンである。

また、3 項組  $(p, a_1 a_2 \cdots a_m, i)$  を様相という。ここで  $p \in Q$  であり、 $a_1 a_2 \cdots a_m \in \Gamma^*, 0 \leq i \leq m-1$  とする。 $\Gamma^*$  は  $\Gamma$  に属する記号からなる長さ 0 以上の記号列全体の集合を表す。 $i$  はヘッドがテープの第  $i$  区間にあることを示す。チューリングマシン  $M$  が入力  $x$  を受理するとは、初期様相  $\alpha_0 = (q_0, x, 0)$  から始まる  $M$  の計算過程に最終様相  $\alpha_n = (q_f, y, i)$  が存在することを言う。 $M$  に



よって受理される記号列全体の集合を  $M$  が受理する言語といい  $L(M)$  と記す。決定性、または非決定性  $k$ -TM  $M$  が  $T(n)$  時間内で動作するとは、長さ  $n$  のすべての入力記号列  $\omega$  に対し、 $\omega$  に関する  $M$  の計算が  $T(n)$  ステップ以内に停止するときをいう。また、決定性、または非決定性  $k$ -TM  $M$  が  $S(n)$  領域内で動作するとは、長さ  $n$  のすべての入力記号列  $\omega$  に対し、 $\omega$  に関する  $M$  の計算で、各作業用テープにおいて最大  $S(n)$  個の区間が使用されるときをいう。

計算量クラスは以下のように定義される。

$\text{DTIME}(T(n))$

$=\{L: \text{ある決定性 } k\text{-TM が } L \text{ を } O(T(n)) \text{ 時間内に受理する}\}$

$\text{NTIME}(T(n))$

$=\{L: \text{ある非決定性 } k\text{-TM が } L \text{ を } O(T(n)) \text{ 時間内に受理する}\}$

$\text{DSpace}(S(n))$

$=\{L: \text{ある決定性 } k\text{-TM が } L \text{ を } O(S(n)) \text{ 領域内で受理する}\}$

$\text{NSpace}(S(n))$

$=\{L: \text{ある非決定性 } k\text{-TM が } L \text{ を } O(S(n)) \text{ 領域内で受理する}\}$

重要な計算量クラスは以下のようなものである。

$\text{DL} = \text{DSpace}(\log n)$ : 対数領域計算可能な問題のクラス。すなわち入力サイズを  $n$  とするとき、決定性  $k$ -TM で高々  $\log n$  個の区間を使って計算できる問題のクラス。

$\text{NL} = \text{NSpace}(\log n)$ : 非決定性対数領域計算可能な問題のクラス。すなわち入力サイズを  $n$  とするとき、非決定性  $k$ -TM で高々  $\log n$  個の区間を使って計算できる問題のクラス。

$\text{P} = \bigcup_k \text{DTIME}(n^k)$ : 多項式時間計算可能な問題のクラス。すなわち、決定性  $k$ -TM で、入力サイズ  $n$  の多項式時間で計算できる問題のクラス。

$\text{NP} = \bigcup_k \text{NTIME}(n^k)$ : 非決定性多項式時間計算可能な問題のクラス。すなわち、非決定性  $k$ -TM で、入力サイズ  $n$  の多項式時間で計算できる問題のクラス。

$\text{PSPACE} = \bigcup_k \text{DSpace}(n^k) = \bigcup_k \text{NSpace}(n^k)$ : 多項式領域計算可能な問題のクラス。すなわち、決定性  $k$ -TM または非決定性  $k$ -TM で、入力サイズ  $n$  の多項式領域で計算できる問題のクラス。

$\text{EXPTIME} = \bigcup_k \text{DTIME}(2^{n^k})$ : 指数時間計算可能な問題のクラス。すなわち決定性  $k$ -TM で、入力サイズ  $n$  の指数時間で計算できる問題のクラス。

これらの計算量クラスに対しては、以下の包含関係が成り立つことは明らかであろう。

$$\text{DL} \subseteq \text{NL} \subseteq \text{P} \subseteq \text{NP} \subseteq \text{PSPACE} \subseteq \text{EXPTIME} \quad (58)$$

古典情報理論には難問として  $\text{P} = \text{NP}?$  問題が存在する。が、ここでは立ち入らない。量子チューリングマシンは確率的チューリングマシンのある種の拡張であるが、以下のような相違点をもつ

1. 機械の線形重ね合わせ状態内の振幅や、機械の時間発展作用素である行列の成分としては、正の実数ばかりでなく複素数も許される。

2. QTM 場合には、観測が行われた際に各様相が得られる確率は、重ね合わせないの各様相の振幅そのものではなく、振幅の絶対値の 2 乗である。すなわち PTM のように線形重ね合わせ内の成分の和が常に 1 になるのではなく、QTM では線形重ね合わせのユークリッド距離 (振幅の絶対値の 2 乗の総和) が常に 1 になる。したがって、QTM の定義は QTM の時間発展が重ね合わせのユークリッド距離を保存するようになさなければならない。

定義 量子チューリングマシン (以下 QTM) は 3 項組  $M = (\Sigma, Q, \delta)$  によって定義される。ただし、 $\Sigma$  は空白記号  $B$  を含むテープの有限集合であり、 $Q$  は初期状態  $q_0$  と最終状態  $q_f \neq q_0$  を含む状態の有限集合である。また、 $\delta$  は以下のような型の量子状態遷移関数である。

$$\delta : Q \times \Sigma \rightarrow \tilde{C}^{\Sigma \times Q \times \{L, R\}} \quad (59)$$

ここで  $\tilde{C}$  は、その桁数  $n$  の多項式時間内に、その実部と虚部を  $2^{-n}$  以内の精度で計算する DTM が存在するような、複素数  $\alpha \in \mathbb{C}$  の集合とする。

では量子コンピュータにおける計算量クラスを定義する。まず古典的コンピュータにおいて BPP を定義する。これは古典的コンピュータにおいて、効率的に計算可能な言語のクラスである。確率 1 で全ての記号列  $x \in \mathcal{L}$  を受理するとき、QTM  $M$  は正確に  $\mathcal{L}$  を受理するという。

BQP:QTM において効率的に計算可能な言語のクラス。

EQP:ある多項式時間 QTM によって正確に受理される言語のクラス。

EQTime( $T(n)$ ):長さ  $n$  の入力に対する実行時間が  $T(n)$  で限定されるような、ある QTM によって正確に受理される言語のクラス。

BQP(再定義):ある多項式時間 QTM によって確率  $\frac{2}{3}$  で受理される言語のクラス。

BQTime( $T(n)$ ):長さ  $n$  の入力時間が  $T(n)$  で限定されるような、ある QTM によって確率  $\frac{2}{3}$  で受理される言語のクラス。

明らかに  $\text{EQP} \subset \text{BQP}$  であり、ベネットの結果より、 $\text{P} \subset \text{EQP}$ ,  $\text{BPP} \subset \text{BQP}$  である。また以下の証明も存在する。  $\text{BQP} \subseteq \text{PSPACE}$

### 3 エンタングルメント

エンタングルメントはすでに見たように、量子テレポーテーションで重要な役割を演じる。それだけではなく、量子暗号や、並列量子計算機においても重要な役割を演じることが分かっている。この章では、エンタングルメントの発見と定義から、エンタングルメントの測度の定義を述べ、エンタングルしているかどうかの必要十分条件を述べる。さらにエンタングルメントの構造として、大域的ユニタリ変換をした場合にエンタングルメントの測度

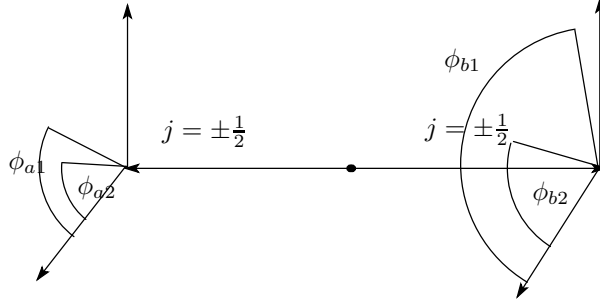


図 6: Bell の実験

がどう変わるのかということ述べる。また、もう一つの構造として、初めにエンタングルメントの測度を増加させるエンタングルメント抽出について述べ、エンタングルしているのにもかかわらず、これ以上エンタングルできない境界の存在についても述べ、それをもってエンタングルメントの構造として論ずる。

### 3.1 発見と定義

エンタングルメントは EPR[11] の三人によって発見され、ベル [20] によってその存在が確立された。まず、図 6 のような実験装置を考える。ここで  $\phi_{ai}, \phi_{bi}, i = 1, 2$  はシュテルンゲルラッハマグネットの向きを表していて、初めスピン 0 だった粒子が崩壊してスピン  $\pm\frac{1}{2}$  になることを意味している。ここで得られる結果は  $\pm 1$  なのでそれを  $\pm 1$  とすれば、測定結果は  $a_1, a_2, b_1, b_2$  であり、 $\pm 1$  をとる。 $a_1$  が  $+1$  だったら  $b_1$  は必ず  $-1$  の結果を得るはずである。これらのことより、

$$a_1 b_1 + a_1 b_2 + a_2 b_1 - a_2 b_2 = \pm 2 \quad (60)$$

であり、この平均を取ったものは、

$$\langle a_1 b_1 \rangle + \langle a_1 b_2 \rangle + \langle a_2 b_1 \rangle - \langle a_2 b_2 \rangle \leq \pm 2 \quad (61)$$

となるはずである。この式をベルの不等式という。

一方量子力学より、 $a_1 b_1$  の平均は、

$$E(a_1, b_1) = P_{++}(a_1, b_1) + P_{--}(a_1, b_1) - P_{+-}(a_1, b_1) - P_{-+}(a_1, b_1) \quad (62)$$

である。ここで  $P_{++}(a_1, b_1)$  は  $a_1, b_1$  方向に  $++$  という観測を得る確率である。これは量子力学より計算でき、

$$\begin{aligned} E(a_1, b_1) &= -\vec{a}_1 \cdot \vec{b}_1 \\ &= \langle \psi | (\vec{a}_1 \cdot \vec{\sigma})(\vec{b}_1 \cdot \vec{\sigma}) | \psi \rangle \end{aligned} \quad (63)$$

となる。ここで  $\sigma$  はパウリ行列である。さて、ベルの不等式に対応する量子力学の式は、

$$E(a_1, b_1) + E(a_1, b_2) + E(a_2, b_1) - E(a_2, b_2) \quad (64)$$

であるが、ここで例えば

$$\begin{aligned} \vec{a}_1 &= \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \\ 0 \end{pmatrix} & \vec{a}_2 &= \begin{pmatrix} -\frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \\ 0 \end{pmatrix} \\ \vec{b}_1 &= \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} & \vec{b}_2 &= \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \end{aligned} \quad (65)$$

とすれば、式 (65) は  $2\sqrt{2}$  という値を持つ、これがベルの不等式の破れである。ではなぜこのようなことが起こったのか、それはベルの不等式を導くときにある仮定をおいたからである。1つは実在性である。これは実験の値は  $\pm 1$  しかとらないという仮定である。2つめに局所性である。これは一方が他方の観測に影響を与えないとしたことである。ベルの不等式の破れはこの二つが間違っていることを示している。もちろん今の場合は電磁氣的相互作用は無視している。それにもかかわらず、遠く離れた二つの量子状態は局所的でない。非局所的である。この非局所性をエンタングルメントという。例えばこの実験では、

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \quad (66)$$

という状態が生成されるのだが、これは明らかに片一方の観測によってもう片方の観測は左右される。

ここで改めてエンタングルメントの定義を述べる。状態  $\rho_{AB}$  がエンタングルしているとは、

$$\rho_{AB} = \sum_i p_i \sigma_{Ai} \otimes \sigma_{Bi} \quad (67)$$

と書けない時である。ここで  $p_i$  は  $\sum_i p_i = 1$  という制限を受けている。逆にこうかけるときには状態  $\rho_{AB}$  は分離可能（セパラブル）であるという。ここではヒルベルト空間は  $A$  と  $B$  に分けて考えられるとしている。このヒルベルト空間の局所視がエンタングルメントが発生する前提条件である。

### 3.2 エンタングルメントの測度

エンタングルメントが強いほど量子テレポーテーションは正確に行われると考えられる。そこで、その正確性を測るためにエンタングルメントに測度 [12] を導入する必要がある。初めはベルの不等式の破れの度合いがエンタ

ングルメント度を測るものとされていた、しかし、Gisin によってエンタングルしている状態でもベルの不等式を破らないものが発見された [22]。それによってエンタングルメント度を測る為の基準を設ける必要がまずある。

基準 1 どんなセパラル状態に対してもエンタングルメントの測度はゼロである、つまり、

$$E(\sigma) = 0 \quad (68)$$

ここで注意すべきところはこの逆は要請していないことである。つまりもし  $E(\sigma) = 0$  なら  $\sigma$  はセパラルであるとは言っていない。これは基準 1 から明らかなことだ。

基準 2 任意の状態  $\sigma$  に対して、次の形のどんな局所ユニタリ変換 ( $U_A \otimes U_B$ ) に対してもエンタングルメントの測度は変わらない。つまり、

$$E(\sigma) = E(U_A \otimes U_B \sigma U_A^\dagger \otimes U_B^\dagger) \quad (69)$$

これは局所ユニタリ変換による局所基底の取り方にはエンタングルメント度は不変であることを言っている。

基準 3 局所オペレーション、古典情報のやりとり、はエンタングルメント度を増大させない。つまり、もしも、 $\sigma$  が確率  $p_i$  で状態  $\sigma_i$  の平均で表せるとき、

$$E(\sigma) \geq \sum p_i E(\sigma_i) \quad (70)$$

である。ここで  $\sigma_i = A_i \otimes B_i \sigma A_i^\dagger \otimes B_i^\dagger / p_i$  で、 $p_i = \text{Tr}(A_i \otimes B_i \sigma A_i^\dagger \otimes B_i^\dagger)$  である。古典情報のやり取りとは  $A_i$  と  $B_i$  に相関があってもいいことを言っている。 $A_i \otimes B_i$  は局所的なオペレーションであることを示している。局所的なオペレーションと古典情報のやり取りを LOCC と呼ぶ。これは Local Operations and Classical Communication の略である。基準 2 は基準 3 の特殊な場合だと考えられる。これは古典情報のやり取りを含めたあらゆる局所オペレーションはエンタングルメントを増大させないという、エンタングルメントがグローバルな性質を持つべきだということからきている。

基準 4 純粋状態のエンタングルメントの測度は reduced von Neumann entropy に等しい。つまり、

$$E(\sigma) = S(\text{tr}_A \rho) = S(\text{tr}_B \rho) \quad (71)$$

これは純粋状態においてエンタングルメント度に additivity を保障するものである。また、二項から三項への等式はシュミット分解できるためである。

さらに課したい条件として、additivity と連続性がある。additivity は

$$E(\sigma \otimes \rho) = E(\sigma) + E(\rho) \quad (72)$$

であるが、これを弱めた条件、weakly additive

$$E(\sigma \otimes \sigma) = 2E(\sigma) \quad (73)$$

であってもよい。連続性はもし  $\rho$  が  $\sigma$  と十分近ければ、 $E(\rho)$  と  $E(\sigma)$  は近い値をもつということである。基準 4 は weakly additive と連続性の帰結であることが Popescu と Rohrlich(1997)[23]、Vidal(2000)[24] によって示されている。

ではこのような基準を満たすエンタングルメントの測度にはどのようなものがあるのだろうか。ここでは 3 つの測度を定義する。

**Entanglement of formation**[6]

エンタングルメントを用意するにはコストがかかる。そこでエンタングルメントを作る最小のコストで測度を定義することが考えられる。それが Entanglement of formation である。定義は、

$$E(\rho) = \min_{p_i, |\Phi_i\rangle} \sum p_i S(|\Phi_i\rangle) \quad (74)$$

である。ここで  $|\Phi_i\rangle$  は純粋状態であり、 $\min$  はあらゆる状態の分割に対して行っている。 $S(|\Phi_i\rangle)$  は純粋状態のフォンノイマンエントロピーである。

$$S(|\Phi_i\rangle) = -\text{Tr}|\Phi_i\rangle\langle\Phi_i|\log(|\Phi_i\rangle\langle\Phi_i|) \quad (75)$$

Entanglement of formation は一般次元の時には解析解は知られていないが、2 qubit の時には知られている [25]。まず、concurrence  $C(\rho)$  を導入する。まず、

$$R(\rho) = \sqrt{\sqrt{\rho}\tilde{\rho}\sqrt{\rho}} \quad (76)$$

の行列を作る。ここで  $\tilde{\rho} = \sigma_y \otimes \sigma_y \rho^* \sigma_y \otimes \sigma_y$  である。この行列の固有値を大きい順に  $\lambda_1, \dots, \lambda_4$  とする。ここで、concurrence を以下のように定義する。

$$C(\rho) = \max\{0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4\} \quad (77)$$

この時、Entanglement of formation は、

$$E(\rho) = h\left(\frac{1 + \sqrt{1 - C^2}}{2}\right) \quad (78)$$

である。ここで  $h$  は、

$$h(x) = -x \log_2 x - (1 - x) \log_2 (1 - x) \quad (79)$$

である。さらに 2-qubit の場合には分割の仕方も 4 つで十分だということが知られている [25]。

**Entanglement of distillation**[26]

まず、この測度を定義するにはエンタングルメントを抽出する方法のクラスを定義しなくてはならない。ヒルベルト空間は 2 つからなるとして  $V_A \otimes V_B$  とする。

(1) 局所オペレーション。これは次の形のオペレーションである。

$$S_A \otimes S_B \quad (80)$$

ここで  $S_A$  は  $V_A$  に対して非測オペレーション (観測を含まないオペレーション) であり  $S_B$  は  $V_B$  に対して非測オペレーションである。

(2)1 局所オペレーション (局所オペレーションと一方向の古典情報のやりとり)。これは任意の  $S_A$  によってもたらされる

$$S_A \otimes 1 \quad (81)$$

というオペレーションである。ここで古典情報は A から B に伝送されるものとする。ここで注意すべきところは、局所オペレーションではオペレーションが非測だったのに対して、1 局所オペレーションではオペレーションが任意ということである。

(3)2 局所オペレーション。これは次のオペレーションによって形成されるクラスである。

$$S_A \otimes 1 \quad (82)$$

$$1 \otimes S_B \quad (83)$$

このオペレーションは A と B に対して連続的に行うことも可能である。

(4)Separable オペレーションこれはオペレーション  $S$  の部分オペレーション  $S_i$  がセパラブルであるようなオペレーションのクラスである。つまり、

$$S_i(\rho) = \sum_j (A_j \otimes B_j) \rho (A_j \otimes B_j)^\dagger \quad (84)$$

と書けるときである。ここで  $A_j, B_j$  は  $V_A, V_B$  にそれぞれ作用するオペレーションである。

(5)Positive-partial-transpose(PPT) オペレーション。これはそれぞれの部分オペレーションが完全に正の部分転置を持つオペレーションである。部分転置とは  $\Gamma$  で表され、

$$\langle \mu_i \nu_j | \rho^\Gamma | \omega_k \chi_l \rangle = \langle \mu_i \chi_l | \rho | \omega_k \nu_i \rangle \quad (85)$$

という変換である。完全に正とはもしこのヒルベルト空間を任意に拡張してもその行列の固有値が正であることを言っている。つまり超演算子、

$$S_i^\Gamma : \rho \rightarrow S_i(\rho^\Gamma)^\Gamma \quad (86)$$

が完全に正であるクラスである。

次にフィデリティというものを定義する。まず、最もエンタングルした状態の一つとして、

$$\Psi^+(V) = \frac{1}{\sqrt{\dim V}} \sum_i |ii\rangle \quad (87)$$

を定義する。そして、フィデリティを次のように定義する。

$$F(\rho) = \Psi^+(V) \rho \Psi^+(V)^\dagger \quad (88)$$

これらのクラスにおいてエンタングル抽出 (エンタングルメントを高める操作) したときの Entanglement of distillation を定義することができる。

定義  $\rho$  の  $C$ -distillable entanglement とは最大値  $D_C(\rho)$  である。それはどのようなものかという、入力  $(V_A \otimes V_B)^{\otimes n_i}$  に対して、クラス  $C$  から一連のオペレーション  $\mathcal{T}$  をして、出力として  $V_{ij} \otimes V_{ij}$  が得られるとする。  $i \rightarrow \infty$  に対して  $n_i \rightarrow \infty$  とする。このとき

$$\frac{1}{n_i} \sum_j p_{ij} \log_2 \dim V_{ij} \rightarrow D_C(\rho) \quad (89)$$

でかつ、

$$\frac{1}{n_i} \sum_j p_{ij} (1 - F_{ij}) \log_2 \dim V_{ij} \rightarrow 0 \quad (90)$$

となるようなものである。これに対して解析解は知られていない。

Relative entropy of entanglement[27]

これは次のように定義される。

$$E(\rho) = \min_{\sigma \in \mathcal{D}} S(\rho || \sigma) \quad (91)$$

ここで

$$S(\rho || \sigma) = -\text{tr} \rho \log \rho - \text{tr} \rho \log \sigma \quad (92)$$

であり、量子相互エントロピーと呼ばれる。この量は必ず正であることが証明されている。 $\mathcal{D}$  はセパラブル領域全体を示している。

ここで定義した3つのエンタングルメントの測度には次の不等式が成り立っている。

$$E_D \leq E_R \leq E_F \quad (93)$$

### 3.3 エンタングルメントしている必要条件と十分条件

この章ではエンタングルしている必要十分条件について述べる。一般次元の場合には必要十分条件は確立されていないが (必要条件だけならペレスによって与えられた [13])、特殊な場合、 $2 \times 2$  と  $2 \times 3$  の時には必要十分条件が存在する [14]。その定理を述べるための準備として、まず定理 1 から始める。

定理 1 任意の分離不可能状態  $\tilde{\rho} \in \mathcal{A}_1 \otimes \mathcal{A}_2$  に対して、エルミート演算子  $\tilde{A}$  が存在し、

$$\text{Tr}(\tilde{A}\tilde{\rho}) < 0, \quad \text{Tr}(\tilde{A}\sigma) \geq 0 \quad (94)$$

ここで  $\sigma$  はあらゆる分離可能状態である。

証明、分離可能状態の定義から、それは  $\mathcal{A}_1 \otimes \mathcal{A}_2$  で凸で閉集合であるそれゆえ、Harn-Banach[28] の定理が使える。ここでこの定理とは、もし、バナッ



八空間  $W_1, W_2$  が凸で閉集合でそのうち一つがコンパクトであるならば、連続関数  $f$  と  $\alpha \in R$  がすべての  $w_1 \in W_1, w_2 \in W_2$  において存在し、

$$f(w_1) < \alpha \leq f(w_2) \quad (95)$$

というものである。この理論はバナッハ空間の閉じた凸集合は連続関数を含む不等式で完全に記述できることを示している。

一つの要素の集合はコンパクトであることに注目すると、実空間  $\tilde{A}$  上に関数  $g$  が存在していることが分かる。それは全ての分離可能状態  $\sigma$  にたいして、

$$g(\tilde{\rho}) < \beta \leq g(\sigma) \quad (96)$$

である。どんなヒルベルト空間上の線形な連続関数もその空間のベクトルで表せられることはよく知られた事実である。 $\tilde{A}$  はヒルベルト空間なので、 $g$  はあるエルミート演算子  $A$  に表される。

$$g(\rho) = \text{Tr}(\rho A) \quad (97)$$

いま  $I$  を恒等演算子とすれば、どんな状態  $\rho, \sigma$  に対しても、 $\text{Tr}(\beta I \rho) = \text{Tr}(\beta I \sigma) = \beta$  なので

$$\tilde{A} = A - \beta I \quad (98)$$

ならよい。この定理を完全に証明するには次の定理が必要である。

定理 2 状態  $\rho \in \mathcal{A}_1 \otimes \mathcal{A}_2$  が分離可能であるための必要十分条件は、

$$\text{Tr}(A\rho) \geq 0 \quad (99)$$

である。ここで  $A$  は  $\text{Tr}(AP \otimes Q) \geq 0$  を満たすあらゆる演算子であり、 $P$  と  $Q$  は  $\mathcal{H}_1$  と  $\mathcal{H}_2$  の射影演算子である。

証明、もし  $\rho$  が分離可能状態ならば、式 (99) は明らかに満たされる。その逆を言うために、 $\rho$  は式 (99) を満たし、分離不可能状態とする。そのとき、分離不可能性より、定理 1 よりあるエルミート演算子  $A$  を見つけてきて、 $\text{Tr}(A\rho) < 0$  しかし分離可能状態  $\sigma$  には  $\text{Tr}(A\sigma) \geq 0$  となることが分かる。これは矛盾である。言い換えれば、分離可能状態は直積の射影演算子  $P \otimes Q$  なのだから  $\text{Tr}(A\rho) < 0$  となることはない。

では、上の定理をポジティブマップの言葉へ拡張する。そのためにポジティブマップ ( $\mathcal{L}$ ) と演算子の間にある位相同型を使う。つまり、

$$\mathcal{L}(\mathcal{A}_1, \mathcal{A}_2) \ni \Lambda \rightarrow S(\Lambda) = \sum_i E_i^\dagger \otimes \Lambda(E_i) \in \mathcal{A}_1 \otimes \mathcal{A}_2 \quad (100)$$

ここで  $E_i$  は  $\mathcal{A}_1$  の直行基底である。ここで変換  $\Lambda \in \mathcal{L}(\mathcal{A}_1, \mathcal{A}_2)$  が正であるための必要十分条件は  $S(\Lambda)$  がエルミートで任意の射影演算子  $P \in \mathcal{A}_1, Q \in \mathcal{A}_2$  に対して、 $\text{Tr}(S(\Lambda)P \otimes Q) \geq 0$  となることである。いま、 $\mathcal{A}_1$  の基底を  $\mathcal{H}_1$  で与

えられた基底  $\{e_l\}$  とし、 $P_{ij}e_l = \delta_{jl}e_i$  で与えられる演算子の集合  $\{P_{ij}\}_{i,j=1}^{\dim \mathcal{H}_1}$  とする。すると式 (99) は次の式と等価である。

$$\text{Tr}[(I \otimes \Lambda) \sum_{ij} P_{ji} \otimes P_{ij} \rho] \geq 0 \quad (101)$$

または

$$\text{Tr}[(I \otimes \Lambda T) \sum_{ij} P_{ji} \otimes T P_{ij} \rho] \geq 0 \quad (102)$$

ここで  $T : \mathcal{A}_1 \rightarrow \mathcal{A}_1$  は  $T P_{ij} = P_{ji}$  で与えられる。つまり基底の変換である。もちろん  $T$  は正であり、 $T^2 = I$  である。そのとき、任意の正の射影  $\tilde{\Lambda} : \mathcal{A}_1 \rightarrow \mathcal{A}_1$  は  $T\Lambda$  の形をしている。今、 $P_0 = (1/d) \sum_{ij} P_{ji} \otimes P_{ji}$  ( $d = \dim \mathcal{H}_1$ ) とおけば、式 (102) はヒルベルト空間  $\mathcal{A}_1 \otimes \mathcal{A}_2$  の内積を使って、

$$\langle \rho, (I \otimes \Lambda P_0)^\dagger \rangle \geq 0 \quad (103)$$

と書き直せる。しかし正の射影はエルミート性を保存する。よって  $I \otimes \Lambda$  もしかりである。よって、

$$\langle \rho, I \otimes \Lambda P_0 \rangle \geq 0 \quad (104)$$

となる。これは次の式とも等価である。

$$\langle I \otimes \Lambda \rho, P_0 \rangle = \text{Tr}[P_0(I \otimes \Lambda \rho)] \quad (105)$$

ここで任意の  $\Lambda : \mathcal{A}_2 \rightarrow \mathcal{A}_\infty$  においてこれは成り立つ。今、状態が分離可能なら演算子  $I \otimes \Lambda \rho$  は正の  $\Lambda$  に対して明らかに正である。逆に、 $I \otimes \Lambda \rho$  が任意の  $\Lambda$  に対して正であるならば、 $P_0$  は射影演算子であるから条件式 (105) は満たされ、状態は分離可能である。このようにして定理 3 が導かれた

定理 3  $\rho$  をヒルベルト空間  $\mathcal{H}_1 \otimes \mathcal{H}_2$  上の状態とする。この時、 $\rho$  が分離可能であるための必要十分条件は、どんな正の射影  $\Lambda : \mathcal{A}_2 \rightarrow \mathcal{A}_1$  に対しても演算子  $I \otimes \Lambda \rho$  が正であることである。

このことより、 $2 \times 2$  と  $2 \times 3$  については以下の定理が言える。

定理 4 ヒルベルト空間  $C^2 \otimes C^2$  または  $C^2 \otimes C^3$  上の状態  $\rho$  が分離可能であるための必要十分条件は部分転置が正のオペレーターであることである。ここで部分転置  $\rho^{T_2}$  は

$$\rho^{T_2} = I \otimes T \rho \quad (106)$$

であたえられる。

証明、もし  $\rho$  が分離可能ならば  $\rho^{T_2}$  はもちろん正である。この逆を言うためには、Stromer と Woronowicz[29][30] の結果を用いる。つまり、彼らは  $\mathcal{H}_1 = \mathcal{H}_2 = C^2$  もしくは  $\mathcal{H}_1 = C^3, \mathcal{H}_2 = C^2$  の時には正のマップ  $\Lambda : \mathcal{A}_1 \rightarrow \mathcal{A}_2$  は次の形をしている、

$$\Lambda = \Lambda_1^{CP} + \Lambda_2^{CP} T \quad (107)$$

ここで  $\Lambda_i^{CP}$  は完全に正のマップである。このマップの完全に正の性質より、 $\Lambda_i = I \otimes \Lambda_i^{CP}$  も正である。もし  $\rho^{T_2}$  が正であるならば、 $\Lambda_1 \rho + \Lambda_2 \rho^{T_2}$  も正である。よって定理 3 より、 $\rho$  は分離可能である。

このようにして、 $2 \times 2$  と  $3 \times 2$  の場合には部分転置した行列が正であることが状態が分離可能な必要十分条件であることが示された。

### 3.4 エンタングルメントの構造

この節では、エンタングルメントの構造を大域的ユニタリ変換によってどこまでエンタングルメントの測度を増やせるのかという観点と、エンタングルメント抽出について述べ、それによってエンタングルメントを増やせる境界について述べる。これらはエンタングルメントの構造を調べる上で重要である。

#### 3.4.1 大域的ユニタリ変換における構造

ここでは以下の定理 [31] を証明する。

定理 1  $\rho$  の固有値分解を、

$$\rho = \Phi \Lambda \Phi^\dagger \quad (108)$$

とする。ここで固有値  $\lambda_i$  は増大する向きにとってある。エンタングルメントオブフォーメーションは次の形の大域的ユニタリ変換を施したときに最大値をとる。

$$U = (U_1 \otimes U_2) \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1/\sqrt{2} & 0 & 1/\sqrt{2} & 0 \\ 1/\sqrt{2} & 0 & -1/\sqrt{2} & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} D_\phi \Phi^\dagger \quad (109)$$

ここで  $U_1, U_2$  は局所ユニタリ演算子で、 $D_\phi$  は直行行列である。エンタングルメントフォーメーションはこの  $\rho' = U \rho U^\dagger$  に対して、

$$E_F(\rho') = f(\max(0, \lambda_1 - \lambda_3 - 2\sqrt{\lambda_2 \lambda_4})) \quad (110)$$

となる。ここで、

$$f(C(\rho)) = H\left(\frac{1 + \sqrt{1 - C^2}}{2}\right) \quad (111)$$

$$H(x) = -x \log x - (1 - x) \log(1 - x) \quad (112)$$

である。

証明、エンタングルメントフォーメーションの最大値を求めることは、コンカーレンス  $C$  の最大値を求めることと同じである。したがって問題は、

$$C_{max} = \max_{U \in U(4)} (0, \sigma_1 - \sigma_2 - \sigma_3 - \sigma_4) \quad (113)$$

に帰着される。ここで  $\sigma_i$  は次の行列の特異値 (Singular value) である。

$$Q = \Lambda^{1/2} \Phi^T U^T S U \Phi \Lambda^{1/2} \quad (114)$$

ここで  $\Phi, U, S$  はユニタリである。そのとき次の不等式が成り立つ。

$$C_{max} \leq \max_{V \in U(4)} (0, \sigma_1 - \sigma_2 - \sigma_3 - \sigma_4) \quad (115)$$

ここでの  $\sigma_i$  は  $\Lambda^{1/2} V \Lambda^{1/2}$  の特異値である。この不等式は  $V$  が  $\Phi^T U^T S U \Phi$  とかけるときに等号がなりたち、そのとき最大である。この条件を満たす必要十分条件は、 $V$  が対称行列のときである ( $V = V^T$ )。  $S$  は対称行列でユニタリなので、次のように積に書ける  $S = S_1^T S_1$  これは高木ファクトリゼーション [32] と呼ばれ、一意ではない。直行行列の分だけ任意性を持っている。具体的な  $S_1$  の形は、

$$S_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & 1 & 1 & 0 \\ -1 & 0 & 0 & 1 \\ 0 & -i & i & 0 \\ i & 0 & 0 & i \end{pmatrix} \quad (116)$$

である。もし  $V$  が対称行列ならば、 $V$  もまた、 $V_1^T V_1$  とファクトライズできる。  $U$  が

$$U = S_1^\dagger O V_1 \Phi^\dagger \quad (117)$$

の形ならば、 $V = V_1^T V_1$  とかけることがわかる。さらに証明を進めるために、特異値に関する不等式を導いておかなければならない、[33]

**Lemma 1**  $A \in M_{n,r}(C), B \in M_{r,m}(C)$  のとき、

$$\sum_{i=1}^k \sigma_i(AB) \leq \sum_{i=1}^k \sigma_i(A) \sigma_i(B) \quad (118)$$

ここで  $k = 1, \dots, q = \min\{n, r, m\}$

さらにここで Wang と Xi の結果を使う [34]。

**Lemma 2**  $A \in M_n(C), B \in M_{n,m}(C), 1 \leq i_1 \dots i_k \leq n$  とする。このとき

$$\sum_{t=1}^k \sigma_{i_t}(AB) \geq \sum_{t=1}^k \sigma_{i_t}(A) \sigma_{n-t+1}(B) \quad (119)$$

ここで  $n = 4$  としてやり、これら二つの不等式に代入する。まず  $k = 1$  と初めの不等式でし、 $k = 3, i_1 = 2, i_2 = 3, i_3 = 4$  と二番目の不等式です。両辺を引くと、

$$\begin{aligned} & \sigma_1(AB) - (\sigma_2(AB) + \sigma_3(AB) + \sigma_4(AB)) \leq \\ & \sigma_1(A) \sigma_1(B) - \sigma_2(A) \sigma_4(B) - \sigma_3(A) \sigma_3(B) - \sigma_4(A) \sigma_2(B) \end{aligned} \quad (120)$$

ここでさらに、 $A = \Lambda^{1/2}, B = V\Lambda^{1/2}$  としてやることにより、 $\sigma_i(A) = \sigma_i(B) = \sqrt{\lambda_i}$  となり上の式は、

$$(\sigma_1 - (\sigma_2 + \sigma_3 + \sigma_4))(\Lambda^{1/2}V\Lambda^{1/2}) \leq \lambda_1 - (2\sqrt{\lambda_2\lambda_4} + \lambda_3) \quad (121)$$

この不等式は  $V$  が順序の入れ替えの演算子のとき等号が成り立つことがわかる。つまり、

$$V = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \quad (122)$$

したがって、今以下のことが証明された。

$$\max_{V \in U(4)} (\sigma_1 - (\sigma_2 + \sigma_3 + \sigma_4))(\Lambda^{1/2}V\Lambda^{1/2}) = \lambda_1 - (2\sqrt{\lambda_2\lambda_4} + \lambda_3) \quad (123)$$

$V$  は実際に対称行列であった、したがって高木ファクトリゼーションが行える  $V = V_1^T V_1$ 。このようなものとして、

$$V_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1/\sqrt{2} & 0 & 1/\sqrt{2} \\ 0 & 0 & 1 & 0 \\ 0 & i/\sqrt{2} & 0 & -i/\sqrt{2} \end{pmatrix} \quad (124)$$

がある。したがって最適な  $U$  は、 $U = S_1^\dagger O V_1 D_\phi^{1/2} \Phi^\dagger$  という形で与えられる。 $O$  は任意の直行行列である。つぎに以下の事実をつかう。

$$SU(2) \otimes SU(2) \cong SO(4) \quad (125)$$

この事実から  $S_1(U_1 \otimes U_2)S_1^\dagger$  は直行で、 $SO(4)$  の成分であることが分かる。また逆に、どんな  $SO(4)$  の成分  $Q$  も  $Q = S_1(U_1 \otimes U_2)S_1^\dagger$  で表せることができる。したがって結論として、任意の  $O \in O(4)$  と対角の  $D_\phi$  には  $U_1, U_2 \in SU(2)$  が存在し、 $U = S_1^\dagger O V_1 D_\phi \Phi^\dagger = (U_1 \otimes U_2)S_1^\dagger V_1 D_\phi \Phi^\dagger$  となることがいえる。ここで簡単な計算より、エンタングルメントフォーメーションは以下のユニタリ演算子を作用させたときに最大になることが分かる。

$$(U_1 \otimes U_2) \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1/\sqrt{2} & 0 & 1/\sqrt{2} & 0 \\ 1/\sqrt{2} & 0 & -1/\sqrt{2} & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} D_\phi \Phi^\dagger \quad (126)$$

### 3.4.2 エンタングルメント抽出における構造

ここではまずエンタングルメント抽出の具体的な方法について述べ、それからバウンドエンタングルメント [35][36] について概説する。まず、エ

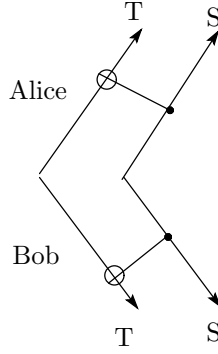


図 7: BXOR オペレーション

エンタングルメント抽出の一般論はすでに 3.2 で、Entanglement of distillation のところで述べた。ここでは 2-qubit の場合に具体的にどのようにエンタングルメントを抽出するかを述べる [4][15]。まず、 $\rho$  は状態であり、混合状態であってもかまわないとする。ここで以下のオペレーションを行ってやる。

$$\int U \otimes U^* \rho (U \otimes U^*)^\dagger dU \quad (127)$$

こうすることによって、状態はワナー状態、

$$W_F = F|\Psi_-\rangle\langle\Psi_-| + \frac{1-F}{3}(|\Psi_+\rangle\langle\Psi_+| + |\Phi_+\rangle\langle\Phi_+| + |\Phi_-\rangle\langle\Phi_-|) \quad (128)$$

に変化する。ここで  $F$  はフィデリティと呼ばれる量であり、 $F \equiv \text{Tr}(\rho|\Psi_-\rangle\langle\Psi_-|)$  である。ここで  $|\Psi_\pm\rangle, |\Phi\rangle$  は量子テレポーテーションの章ででてきたベルの直行基底である。初めに  $\rho^{\otimes n}$  という状態を用意してやってから上の変換を施す。次に図 7 という BXOR [4] というオペレーションをする。ここでは状態をアリスサイドとボブサイドにわけ、二つの状態において制御 NOT 演算をする。このオペレーションによりベルの直行基底はそれぞれ入れ替わる。その変換の仕方は [4] に表として載っている。ここでターゲット T の観測値が同じならば状態を残しておき、違う値の時には捨てることにする。このようにして、フィデリティは

$$F \rightarrow \frac{F^2 + \frac{1}{9}(1-F)^2}{F^2 + \frac{2}{3}F(1-F) + \frac{5}{9}(1-F)^2} \quad (129)$$

と変化する。この関数は  $F = 0.5$  以上でそれより大きい値をもつ。したがってフィデリティが 0.5 以下ではエンタングルメントを最大に持っていくことはできず、0.5 以上ではこの操作を繰り返すことによってエンタングルメントを最大に持っていくことができる。エンタングルメントの測度を高めることができ、純粋状態へ持っていけないとき、bound エンタングル状態という。2 × 2 の状態と、2 × 3 の状態は bound エンタングル状態はないことが示されている。また、高次元では、PPT(Positive partial transposition)、つま

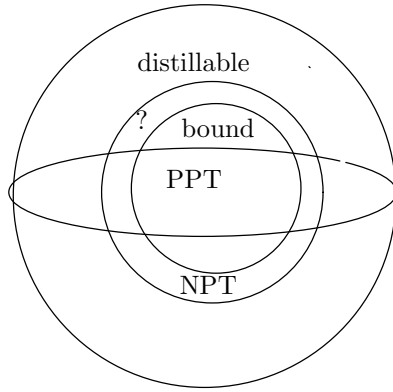


図 8: エンタングル抽出におけるヒルベルト空間の構造。?の領域は bound か undistillable の領域である。

り、部分転置を行ってやった行列が正であるときにはそれは bound エンタングル状態ではないことも示されている。また、bound エンタングル状態は NPT(Negative partial transposition) 状態に入っていることも示されている [36]。これを図に描けば、次のようになる。だがこの図からではセパラブル境界がわからないことは一つの問題であり、現在もセパラブル境界を絵に描くための必要十分条件を探しているのが現実である。

## 4 量子状態の幾何学

この章では、状態空間の幾何学について言及する。幾何学といっても視覚化からメトリックを使った微分幾何までであるが、ここでは視覚化することを目指す。次の節では 1-qubit の幾何学を扱う。この場合の大域的構造は完全な形で求まっている。しかもこの状態を絵に書くことは大きなメリットがある。それは、さまざまなオペレーションにたいして状態がどのように変化するかを一目で分かるためである。次の節ではそれと同じことを 2-qubit( $2 \times 2$ ) 状態に対しておこなう。2-qubit はエンタングルメントが発生する最も低次元の状態である。この幾何学を研究することはエンタングル境界という状態空間にある大域的構造を明らかにすることも視野に入れている。

### 4.1 1-qubit の幾何学

1-qubit の幾何は完全に分かっており、それはブロッホ球である (図??)。この表面は純粋状態を表していて、内部は混合状態である。この球全体が状態を表している。例えば、ユニタリ変換による回転はこの球の回転に相当す

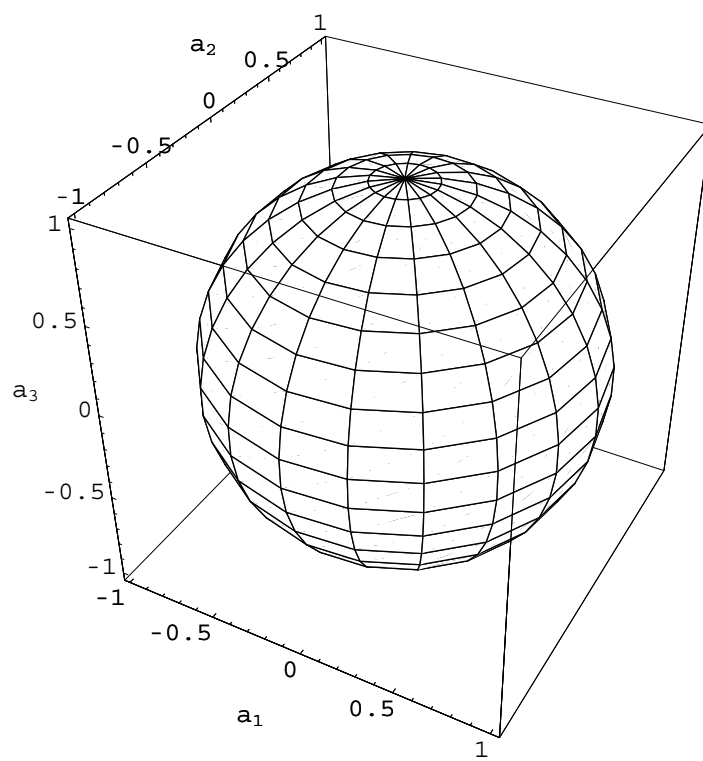


図 9: ブロッホ球



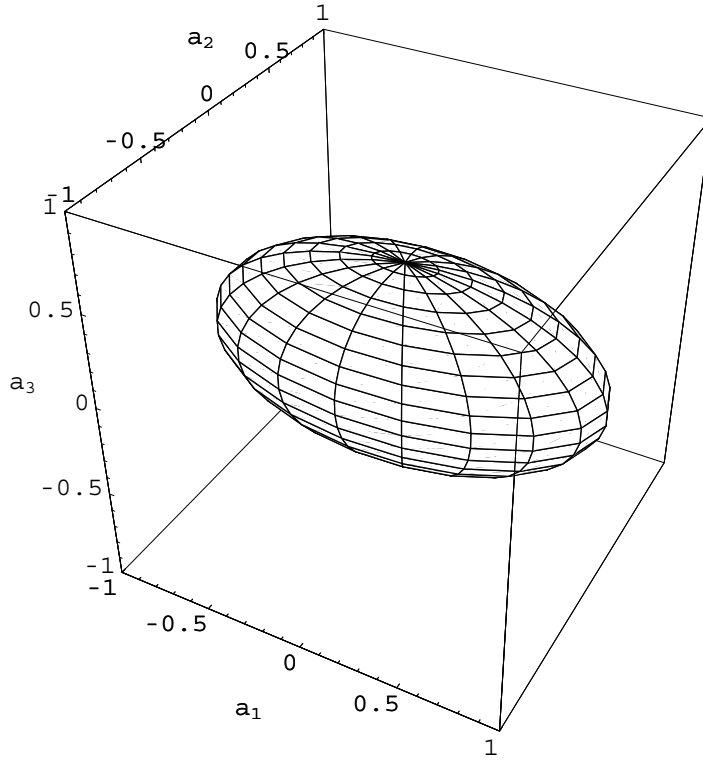


図 10: ビットフリップチャンネルを通った後の状態

る。この絵は、状態が、

$$\rho = \frac{1}{2}(1 + \vec{a} \cdot \vec{\sigma}) \quad (130)$$

とパラメトライズできることからきている。ここで状態であるためには、 $\text{Tr} \rho = 1$  であり、これは変数の取り方より自動的に満たされている。また、 $\text{Tr} \rho^2 \leq 1$  よりこの球が描ける。この方法は木村の方法と同値であり、状態空間を完全に書き表している。ここでこの幾何を用いるメリットは次のような量子操作を行うときに顕著である。ここでは二つの例を用いて説明する。まず一つ目はビットフリップチャンネルである。これは  $|0\rangle$  を  $p$  の確率で  $|1\rangle$  にし、 $|1\rangle$  を  $1-p$  の確率で  $|0\rangle$  にする量子ゲートである。量子操作の行列で書けば、

$$E_0 = \sqrt{p} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad (131)$$

$$E_1 = \sqrt{1-p} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad (132)$$

である。この時、量子状態は、図 10 のように変化する。ここで分かるように、ビットフリップチャンネルを通過すると、球が楕円になる。もともと純粋状態だったところは半径 1 以下のところにあり、すでに混合状態となる。こ

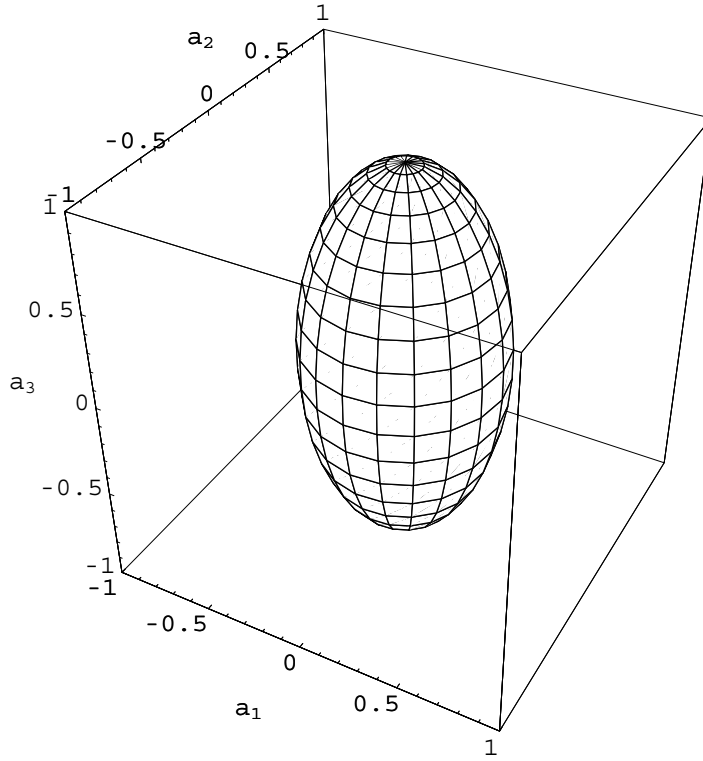


図 11: フェイズフリップチャンネルを通った後の状態

では  $p = 0.5$  の場合を描いたが、 $p$  が大きくなるにつれて、このゆがみ具合はさらに大きくなり、最後には線になる。次に、フェイズフリップチャンネルを通過した場合の状態の変化を見る。今度は確率  $p$  で  $|0\rangle$  の符号が、 $1-p$  で  $|1\rangle$  の符号が逆転するゲートである。ここでも量子操作の表示で書くと、

$$E_0 = \sqrt{p} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad (133)$$

$$E_1 = \sqrt{1-p} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad (134)$$

となる。これによって引き起こされた状態の変化は図 11 のようである。ここでもビットフリップの場合と同様に球が変形することが見て取れる。

このように、状態をブロッホ球として視覚化した場合、さまざまな量子操作によって状態がどのように変化するかを全体的に見ることができることが、視覚化の利点である。

## 4.2 2-qubit の幾何学

ここでは2キュービットの状態の幾何を見る。この状態を見る理由はエンタングルメントが初めて登場する最小の次元だからである。

### 4.2.1 状態とセパラブル領域の視覚化

まず初めに2キュービットの状態のパラメトリゼーションを次のように定義する。

$$\rho = \frac{1}{4} \left( 1 + \sum_i a_i \sigma_i \otimes 1 + \sum_j b_j 1 \otimes \sigma_j + \sum_{ij} c_{ij} \sigma_i \otimes \sigma_j \right) \quad (135)$$

このようにパラメトライズした理由は、まず  $\text{Tr} \rho = 1$  を自明に満たしているところであり、また、 $a_i, b_j$  が局所情報を表しているからである。 $c_{ij}$  は局所情報でない二つの状態の相関を表している。これらの基底  $\sigma_\mu \otimes \sigma_\nu$ ,  $(\mu, \nu = 0, \dots, 4)$  でかつ、 $\sigma_0 = 1$  は互いに直行している。なおここで  $\sigma_i, i = 1, 2, 3$  はパウリ行列である。状態の形は木村の方法 [38] によって決められる。それは

$$\sum_{j=0}^N (-1)^j \alpha_j x^{N-j} = \det(x - \rho) \quad (136)$$

となる係数  $\alpha_j$  が全て0以上という条件である。2キュービットの場合には具体的に、

$$\begin{aligned} 1! \alpha_1 &= 1 \\ 2! \alpha_2 &= 1 - \text{Tr} \rho^2 \\ 3! \alpha_3 &= 1 - 3 \text{Tr} \rho^2 + 2 \text{Tr} \rho^3 \\ 4! \alpha_4 &= 1 - 6 \text{Tr} \rho^2 + 8 \text{Tr} \rho^3 + 3 (\text{Tr} \rho^2)^2 - 6 \text{Tr} \rho^4 \end{aligned} \quad (137)$$

とかける。この式に上のパラメトライズした状態を代入してやれば状態の形は形式的に分かったことになるのだが、15次元の空間であり、具体的にどのような形をしているかを想像するのは難しい。そこでまず、基底空間を

$$\rho = \frac{1}{4} (1 + p \sigma_1 \otimes \sigma_1 + q \sigma_2 \otimes \sigma_2 + r \sigma_3 \otimes \sigma_3) \quad (138)$$

として、残りの方向をファイバー [39] として捉え、基底空間のファイバーに沿った変化を見ることにした。ここで、ファイバー方向は、

パラメター	ファイバーの基底	
$a_{i\pm}$	$\sigma_i \otimes 1 \pm 1 \otimes \sigma_i$	(139)
$c_{ij\pm}$	$\sigma_i \otimes \sigma_j \pm \sigma_j \otimes \sigma_i$	

とする。ここでの  $a, c$  は式 (135) のそれとは違うことに注意する。ここで  $c_{ij}$  の  $i, j$  は  $i \neq j$  であり、 $i, j = 1, 2, 3$  である。まず、基底空間の幾何だが、こ

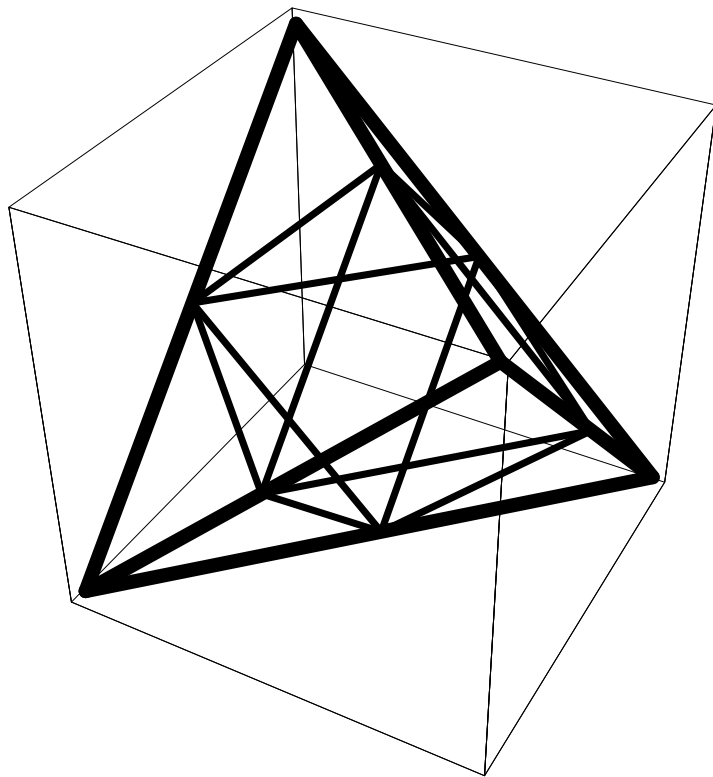


図 12: 基底空間の幾何構造

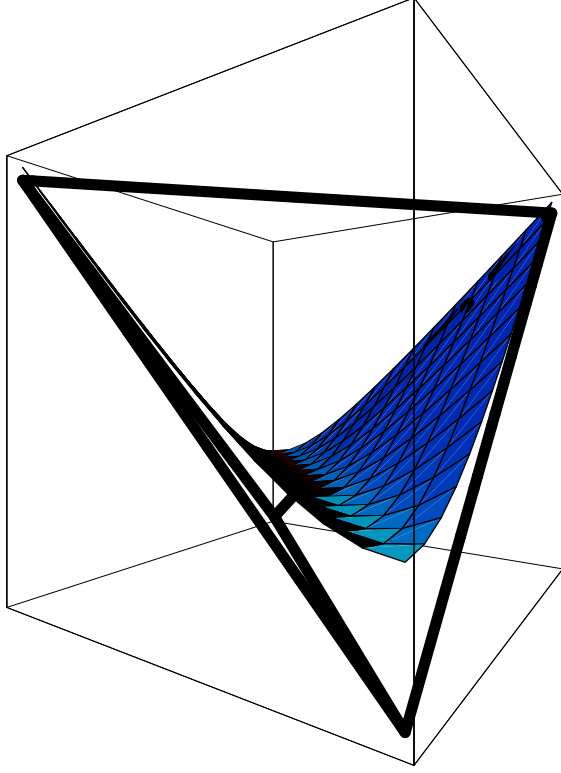


図 13:  $a_{3+}$  方向に沿って動かしたときの基底空間の変化

れは図 12 のようになっている。ここで正四面体の内部が状態空間で、頂点はベルの基底  $|\Psi_{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$   $|\Phi_{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$  になっている。さらに内部の正八面体の中はセパラル状態である (付録 A)。こばの領域がエンタングルメント状態を表している。さて、これをファイバー  $a_{3+}$  の方向に沿って動かしてみたとする。すると基底空間は図 13 のように変化する。ここで状態は

$$\begin{aligned} & 1 - p - q \\ & 1 + p + q \\ & -1 + \sqrt{a_{3+}^2 + (p - q)^2} \end{aligned} \quad (140)$$

ではさまれた領域、つまり曲面の上側と正四面体の屋根の部分にはさまれた領域が状態空間である。ここでは  $a_{3+} = 0.5$  の場合を図にかいたが、 $a_{3+}$  が 2 に近づくにしたがって曲面は上昇し最後は正四面体の上辺の中点になりこれは  $|00\rangle\langle 00|$  の状態になる。ではセパラル境界はどのように変化するのだろうか、それを図に示したのが図 14 である。ここでも  $a_{3+} = 0.5$  である。具体的には

$$1 + p - q$$

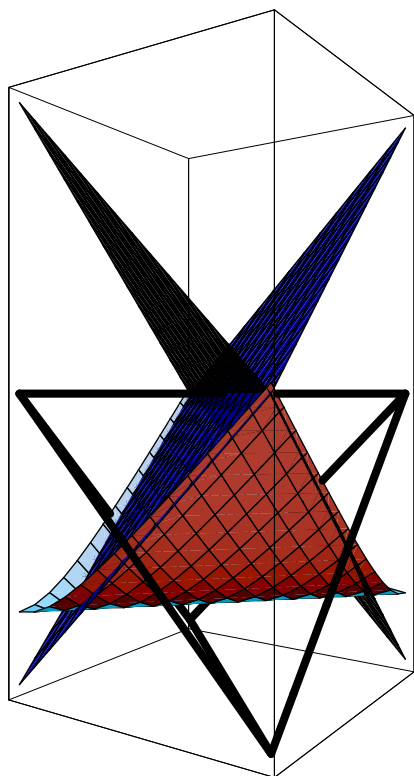


図 14:  $a_{3+}$  方向に沿って動かしたときのセパブル境界の変化

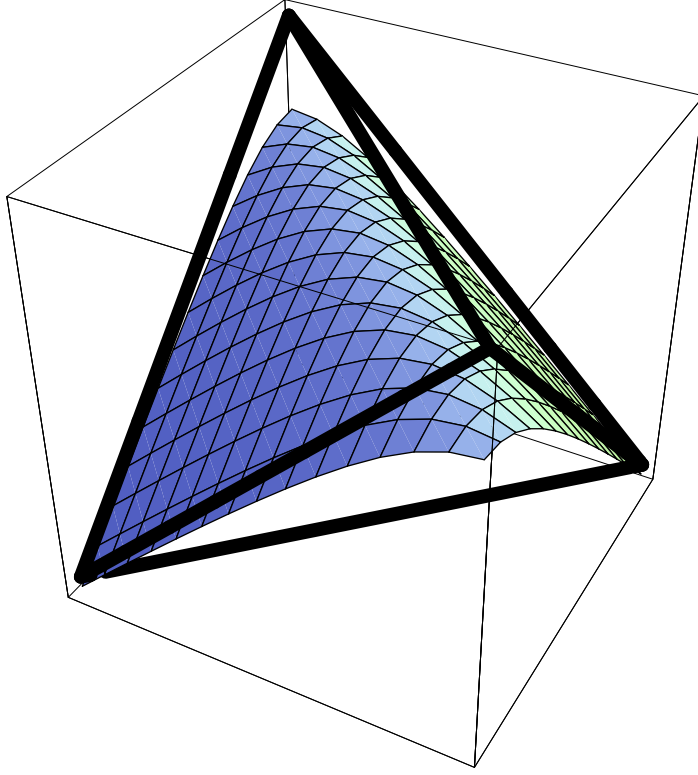


図 15:  $a_{3-}$  方向に沿って動かしたときの状態の変化

$$-1 + \frac{1 - p + q}{\sqrt{a_{3+}^2 + (p + q)^2}} \quad (141)$$

ではさまれた領域である。ここでは正八面体の下部が曲面になって上昇してくるのが分かる。この類の形をタイプ + と呼ぶことにする。この導出は付録 B を参照。次に  $a_{3-}$  に沿って動かしたときの基底空間の変化を表したものが、図 15 である。今度は、

$$1 - \frac{-1 + p - q}{\sqrt{a_{3-}^2 + (p + q)^2}} \quad (142)$$

ではさまれる領域が状態空間である。今度は曲面と正四面体の下側ではさまれる領域が状態空間となっている。ここでも  $a_{3-} = 0.5$  の場合を描いている。セパブル境界の変化は図 16 のようになっている。今度は、

$$1 - \frac{-1 - p - q}{\sqrt{a_{3-}^2 + (p - q)^2}} \quad (143)$$

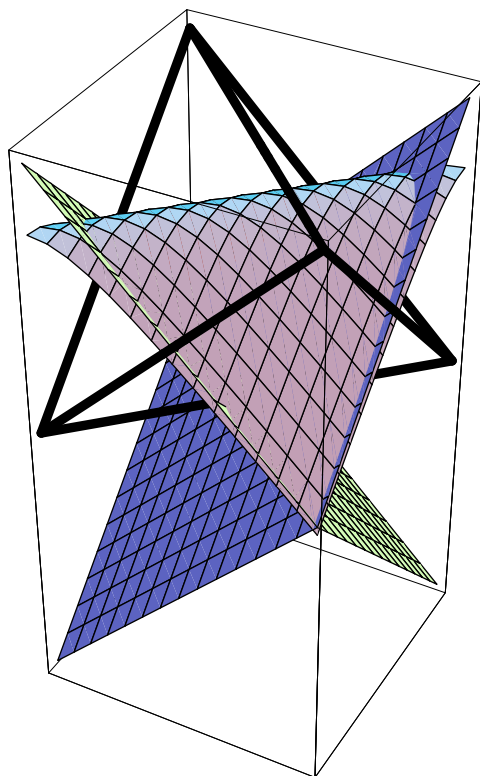


図 16:  $a_{3-}$  方向に沿って動かしたときの状態の変化



ではさまれた領域がセパラル境界である。もちろん状態領域との境界も考慮に入れなくてはならない。以上のことは木村の方法または固有値を求めることによってなされる。セパラル境界に関しては部分転置した行列に木村の方法または固有値を求めることによってなされる。 $a_{3-}$  の場合をケース－と呼ぶことにする。すると他のファイバーに沿った状態の変化は次の表のようになる。

パラメター	タイプ	座標変換
$a_{1\pm}$	$\pm$	$(p, q, r) \rightarrow (q, r, p)$
$a_{2\pm}$	$\pm$	$(p, q, r) \rightarrow (r, p, q)$
$a_{3\pm}$	$\pm$	$(p, q, r)$ not change
$c_{12\pm}$	$\pm$	$(p, q, r)$ not change
$c_{13\pm}$	$\pm$	$(p, q, r) \rightarrow (r, p, q)$
$c_{23\pm}$	$\pm$	$(p, q, r) \rightarrow (q, r, p)$

では元の基底空間にさまざまなオペレーションをしたときに状態空間はどのように変化するだろうか。ここではHadamard ゲート、部分転置、Hadamard+制御 NOT オペレーション、制御 NOT オペレーションの4種類の量子操作をしたときの状態の変化を調べる。まずはHadamard ゲートである。このとき、 $H\sigma_1 H = \sigma_3, H\sigma_2 H = -\sigma_2 H\sigma_3 H = \sigma_1$  より、 $(p, q, r) \rightarrow (r, q, p)$  となる。しかし、正四面体の対称性より状態空間およびセパラル境界は不変である。次に、部分転置を考えてみる。この時には  $\sigma_2 \otimes \sigma_2^\Gamma = -\sigma_2 \otimes \sigma_2$  であり、 $(p, q, r) \rightarrow (p, -q, r)$  と変数が変化する。しかしここでも正四面体の対称性より状態空間、およびセパラル境界は不変である。次に Hadamard+制御 NOT オペレーションを加えたときにどうなるだろうか、この操作は  $|00\rangle$  を最大にエンタングルした状態にするという特別な操作である。制御 NOT オペレーションを  $C$  と書くならば、

$$CH \otimes 1_\rho H \otimes 1C = \frac{1}{4} \begin{pmatrix} 1 & p & q & r \\ p & 1 & -r & -q \\ q & -r & 1 & -p \\ r & -q & -p & 1 \end{pmatrix} \quad (144)$$

となる。状態空間はこのオペレーションがユニタリであることから不変である。またセパラル境界もこの場合は不変である。しかし、この場合はオペレーション後の状態は基底空間にとどまっていない。基底は次式のように変化している。

$$\rho = \frac{1}{4}(1 + p\sigma_3 \otimes \sigma_1 + q\sigma_1 \otimes \sigma_3 - r\sigma_2 \otimes \sigma_2) \quad (145)$$

では最後に、制御 NOT オペレーションを加えたときにどのように状態が変化するかを見る。この場合、

$$C\rho C = \frac{1}{4} \begin{pmatrix} 1+r & 0 & p-q & 0 \\ 0 & 1-r & 0 & p+q \\ p-q & 0 & 1+r & 0 \\ 0 & p+q & 0 & 1-r \end{pmatrix} \quad (146)$$

となる。この場合もユニタリ変化のため状態空間の形は変わらない。しかし、今度の場合は状態空間全体がセパラブルになる。この場合の状態は次のように基底が変わっている。

$$\rho = \frac{1}{4}(1 + p\sigma_1 \otimes 1 - q\sigma_1 \otimes \sigma_3 + r1 \otimes \sigma_3) \quad (147)$$

#### 4.2.2 セパラブル領域の体積

この節では局所情報が分かったときにどれだけセパラブルな状態が得られるかについて述べる。パラメータのとり方は前節でとったとり方と同じとする。まずここではそのパラメトリゼーションでランダムに生成される状態を作るマシンを仮定し、局所的に情報が分かったとする。つまり、 $a_i, b_j$  が分かったとする。この時、そのパラメータでのユークリッド体積を求めることにする。使うのは木村の方法である。木村の方法によってパラメータの取りえる範囲が与えられる。それが状態であるための必要十分条件である。また、部分転置してやった状態に対しても同じことをすることによってセパラブルな状態の必要十分条件であるパラメータの範囲が決まる。ここでは状態であるためのパラメータのとりえる範囲の中からランダムに変数を作り、それがセパラブルの領域に入っているかどうかを調べるモンテカルロシミュレーションを行った。ここでは簡単のため、 $a_3 = b_3$  で  $a_1 = a_2 = b_1 = b_2 = 0$  とおいたときを考える。これは局所ユニタリ変換で常にもっていける形である。さらに局所ユニタリ変換では  $c_{ij}$  のうち2つを0にすることができる。得られた結果は図 17 である。ここで顕著なことは、終状態が  $|00\rangle$  という純粋なセパラブル状態なのに対して、そのセパラブルな体積の比率は0に近づくということである。この計算結果はモンテカルロでの積分変数全てで行ったわけではないのでまだ不完全ながら、セパラブルである条件は「かつ」であるから、この傾向は正しいものといえる。

## 5 まとめ

ここで見てきたように量子状態の幾何構造は1キュービットの場合にしか完全に分かっていない。2キュービットの場合にはある特定のファイバーに沿った形の変化しか分かっていない。この分野の完成は2キュービットの量

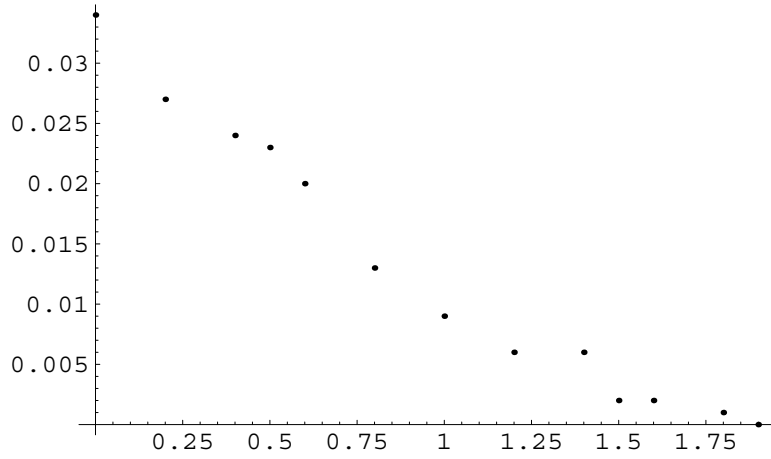


図 17: セパラブル領域の体積の比率の変化

子状態のあらゆる断面を書くことである。しかし、それには数学的困難が付きまとう。なぜなら木村の方法にしる、固有値を求める方法にしる、それは4次の多変数多項式をとくことに他ならない。4次の方程式の解は形式的に知られているが、その解が実数であるかどうかを判定するにはより高次の多項式を解かなくてはならない。今のところ5次以上の多項式の形式解は知られていない。そのため断面を描くことも数学的に困難である。これを解決する方法として線形でないパラメトリゼーションを施す方法が考えられる。どれがいいパラメトリゼーションなのかその基準はまだ提示されていない。物理的、情報理論的なものがいいと思われるが、それはまだ未知の分野である。

また、今回はセパラブル領域の体積の比率を求める際にユークリッド体積を用いたが、これも議論の余地がある。物理的に意味のある体積はハールメジャーと対角成分に対する任意のメジャーを取ってくるほうが自然だ。さらに今回は  $a = b$  の場合しか調べていないが、 $a \neq b$  の場合も調べるべきである。

これからの課題として、純粋状態が  $S^{15}$  にどのように埋め込まれているのかも考える必要がある。そして、便利なパラメトリゼーションを考えることによって、一般相対性理論で言うところのペンローズダイアグラムに相当するものがかけるかもしれない。これらが今後の課題である。

## A 基底空間が正四面体になることの証明

基底空間は、

$$\rho = \frac{1}{4}(1 + p\sigma_1 \otimes \sigma_1 + q\sigma_2 \otimes \sigma_2 + r\sigma_3 \otimes \sigma_3) \quad (148)$$

である。これを行列表示にすると、

$$\rho = \frac{1}{4} \begin{pmatrix} 1+r & 0 & 0 & p-q \\ 0 & 1-r & p+q & 0 \\ 0 & p+q & 1-r & 0 \\ p-q & 0 & 0 & 1+r \end{pmatrix} \quad (149)$$

となる。この固有値は、

$$\begin{aligned} & \frac{1}{4}(1-p-q-r) \\ & \frac{1}{4}(1+p+q-r) \\ & \frac{1}{4}(1+p-q+r) \\ & \frac{1}{4}(1-p+q+r) \end{aligned} \quad (150)$$

である。これを  $r$  について解くと、 $r = 1-p-q, 1+p+q, -1-p+q, -1+p-q$  となる。固有値が正であるという条件より、この面内で囲まれた領域が状態空間となる ( $r \leq 1-p-q, r \leq 1+p+q, r \geq -1-p+q, r \geq -1+p-q$ )。今の場合、 $(p, q, r) = (1, 1, -1), (1, -1, 1), (-1, 1, 1), (-1, -1, -1)$  が頂点であるから、これは正四面体である。部分転置を行ったときの行列は、

$$\rho = \frac{1}{4} \begin{pmatrix} 1+r & 0 & 0 & p+q \\ 0 & 1-r & p-q & 0 \\ 0 & p-q & 1-r & 0 \\ p+q & 0 & 0 & 1+r \end{pmatrix} \quad (151)$$

であり、この固有値は、

$$\begin{aligned} & \frac{1}{4}(1+p-q-r) \\ & \frac{1}{4}(1-p+q-r) \\ & \frac{1}{4}(1-p-q+r) \\ & \frac{1}{4}(1+p+q+r) \end{aligned} \quad (152)$$

となる。これが正であるという条件より、 $r \leq 1-p+q, r \leq 1+p-q, r \geq -1+p+q, r \geq -1-p-q$  ではさまれた領域が分離可能状態（セパラル状態）となる。これを図示すれば、正四面体の中に正八面体が描ける。よって、図 12 が描けることになる。

## B ファイバーに沿ったときの状態の変化の証明

今、 $a_{3+}$  に沿った状態の変化だけを考える。他のファイバーに沿ったときも同様の計算をすればよい。状態は、

$$\rho = \frac{1}{4}(1 + a_{3+}(1 \otimes \sigma_3 + \sigma_3 \otimes 1) + p\sigma_1 \otimes \sigma_1 + q\sigma_2 \otimes \sigma_2 + r\sigma_3 \otimes \sigma_3) \quad (153)$$

である。この行列表示は、

$$\rho = \frac{1}{4} \begin{pmatrix} 1+a+r & 0 & 0 & p-q \\ 0 & 1-r & p+q & 0 \\ 0 & p+q & 1-r & 0 \\ p-q & 0 & 0 & 1-a+r \end{pmatrix} \quad (154)$$

となり、その固有値は、

$$\begin{aligned} & \frac{1}{4}(1-p-q-r) \\ & \frac{1}{4}(1+p+q-r) \\ & \frac{1}{4}(1-\sqrt{a_{3+}^2 + (p-q)^2} + r) \\ & \frac{1}{4}(1+\sqrt{a_{3+}^2 + (p-q)^2} + r) \end{aligned} \quad (155)$$

となる。これらが正であるという条件より、 $r \leq 1-p-q, r \leq 1+p+q, r \geq -1 + \sqrt{a_{3+}^2 + (p-q)^2}, r \geq -1 - \sqrt{a_{3+}^2 + (p-q)^2}$  が導かれる。ここで最後の不等式は常に満たされるので無視してよい。これらの条件によって、図?? が描かれる。ここで正四面体の屋根の部分は条件が変わっていないことに注意する。次にこの状態の部分転置を行ってやったときの行列は、

$$\rho = \frac{1}{4} \begin{pmatrix} 1+a+r & 0 & 0 & p+q \\ 0 & 1-r & p-q & 0 \\ 0 & p-q & 1-r & 0 \\ p+q & 0 & 0 & 1-a+r \end{pmatrix} \quad (156)$$

となる。この固有値は、

$$\begin{aligned} & \frac{1}{4}(1+p-q-r) \\ & \frac{1}{4}(1-p+q-r) \\ & \frac{1}{4}(1-\sqrt{a_{3+}^2 + (p+q)^2} + r) \\ & \frac{1}{4}(1+\sqrt{a_{3+}^2 + (p+q)^2} + r) \end{aligned} \quad (157)$$

となり、固有値が正であるような領域、つまり分離可能状態は、 $r \leq 1+p-q, r \leq 1-p+q, r \geq -1 + \sqrt{a_{3+}^2 + (p+q)^2}, r \geq 1 + \sqrt{a_{3+}^2 + (p+q)^2}$  では

さまれる領域になる。これを図示したものが、図 14 である。ここでも正八面体の屋根の部分は変わっていない。正八面体の下部が曲がり、上昇するのである。

## 参考文献

- [1] Nielsen and Chuang, "Quantum Computation and Quantum Information" Cambridge University Press, (2000).
- [2] D.Deutsch,*Proc. R. Soc. Lond.*,**A 400** 97 (1985)
- [3] P.W.Shor, "Algorithms for Quantum Computation: Discrete Log and Factoring" *Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science*,(1994)
- [4] C.H.Bennett, G.Brassard, C.Crepeau, R.Jozsa, A.Peres, and K.Wotters *Phys. Rev. Lett* **70** 1895 (1993)
- [5] A.Peres, "Quantum Theory: Concepts and Methods" ,Kluwer Academic Publishers (1995)
- [6] C.H.Bennett and G.Brassard,"Quantum cryptography public key distribution and coin tossing" *Int. conf Computers, System & signal Processing* Bangalore, India 175 (1984)
- [7] A.Ekert and R.Jozsa,*Reviews of Modern Physics*,**68**, 733 (1996)
- [8] L.Grover; e-print quant-ph/9605043
- [9] C.H.Papadimitriou, "Computational Complexity" Addison Wesley Longman (1994)
- [10] 西野哲朗、"量子コンピュータの理論"、培風館 (2002)
- [11] A.Einstein, B.Podolsky and N.Rosen *Phys. Rev* **47** 777 (1935)
- [12] V.Vedral e-print quant-ph/0102094
- [13] A.Peres *Phys. Rev. Lett.* **77** 1413 (1996)
- [14] M.Horodecki, P.Horodecki, R.Horodecki *Phys. Lett.* **A 223** 1 (1996)
- [15] C.H.Bennett, D.P.DiVincenzo, J.A.Smolin and W.K.Wotters *Phys. Rev.* **A 54** 3824 (1996)
- [16] 江沢洋、新井朝雄 "量子力学の数学的構造"、" 朝倉書房 (1999)

- [17] E.Schmidt *Math. annalen* **63** 433 (1907)
- [18] von Neumann "Mathematische Grundlagen der Quantenmechanic" Springer, Berlin (1932)
- [19] H.Umegaki *Kodai Math. Sem. Rep.* **14** 59 (1962)
- [20] J.S.Bell, "Speakable and Unspeakable in Quantum Mechanics" Cambridge Univ. Press (1987)
- [21] 守屋悦朗 "チューリングマシンと計算量の理論" 培風館 (1997)
- [22] N.Gisin *Phys. Lett A* **210** 151 (1996)
- [23] S.Popescu and D.Rohrlich *Phys. Rev. A* **56** R3319 (1997)
- [24] G.Vidal *J. Mod. Opt* **47** 355 (2000)
- [25] W.K.Wotters *Phys. Rev. Lett* **80** 2245 (1998)
- [26] E.M.Rains *Phys. Rev. A* **60** 173 (1999)
- [27] V.Vedral, M.B.Plenio K.Jacobs and P.L.Knight *Phys. Rev. A* **56** 4452 (1997)
- [28] F.Riesz and B.Sz.-Nagy "Functional Analysis" Dover (1952)
- [29] E.Stromer *Acta. Math* **110** 233 (1963)
- [30] S.L.Woronowicz *Rep. Math. Phys.* **10** 165 (1976)
- [31] F.Verstraete, K.Audenaert, T.D.Bie, B.D.Moor e-print quant-ph/0011110
- [32] R.Horn and C.Johnson "Matrix Analysis" Cambridge University Press (1985)
- [33] R.Horn and C.Johnson "Topics in Matrix Analysis" Cambridge University Press (1991)
- [34] B.-Y.Wang and B.-Y.Xi *Lin. Alg. Appl.* **264** 109 (1997)
- [35] M.Horodecki, P.Horocecki, R.Horodecki *Phys. Rev. Lett* **80** 5239 (1998)
- [36] D.DiVincenzo, P.W.Shor, J.A.Smolin B.M.Terhal and A.V.Thapliyal *Phys. Rev A* **61** 062312 (2000)
- [37] C.H.Bennett, G.Brassard, S.Popescu, B.Schumacher, J.A.Smolin, and W.K.Wootters *Phys. Rev. Lett* **76** 722 (1996)

- [38] G.Kimura *Phys. Lett. A* **339** (2003)
- [39] Kobayashi and Nomizu "Foundations of Differential Geometry Volume  
" John Wiley (1963)