

量子エンタングルメントによる量子情報処理

鄭 琳琳 松枝 秀明

高知大学理学研究科数理情報科学専攻

概要

量子コンピュータにおける計算 (量子コンピューティング) の高速性のために、エンタングルメント状態は重要な役割を演じている。また、エンタングルメント状態は量子通信 (量子テレポーテーションや量子暗号など) を行うために必要不可欠な物理的なリソースである。現在までに、2量子ビットのエンタングルメント状態は深く研究され、明確に理解されている。しかし、量子ビットの数が増えると量子状態は複雑になって、エンタングルメントの判定が困難になる。本研究においては、「 k -subsystem total semi-separability (TSS)」と「 k -subsystem partial semi-separability (PSS)」と呼ばれる二つの判定基準を使って、多粒子系エンタングルメント状態の判定と分類を行った。

1 はじめに

1.1 量子コンピュータの原理と意義

量子ビットは、量子コンピュータにおける情報の基本単位であり、 $|0\rangle$ 、 $|1\rangle$ という2つの状態以外に、 $|0\rangle$ と $|1\rangle$ を重ね合わせた状態も保持することができる。量子コンピュータが従来のコンピュータより桁違いに高速な計算ができる理由の1つが、この重ね合わせ状態を利用することである。一般に、 n 個量子ビットの重ね合わせ状態を用いると、 $\underbrace{|00\dots 00\rangle}_n$ から $\underbrace{|11\dots 11\rangle}_n$ まで、全部で 2^n 個の状態を一度に表現することができる。古典コンピュータが 2^n 回の計算で実行することを、量子コンピュータは、たったの1回で実行することができる。つまり、量子コンピュータは、重ね合わせ状態を利用して、超並列計算を行うことができる超高速コンピュータである。

この超並列計算ができる量子コンピュータは、従来のコンピュータが、現実的な時間で解くことができない因数分解を、数分で解いてしまう。このこと

は、1994年にショアが発見した量子アルゴリズムによって証明された。現在、インターネットが情報通信に使っている公開鍵暗号は、大きな数の因数分解を利用している。従来のコンピュータでは、大きな数の因数分解は事実上計算不可能といわれ、この事実が公開鍵暗号の安全性を保証している。しかし、ショアのアルゴリズムを量子コンピュータ上で動かすと、数分間で因数分解を実行することができる。これは、現在のセキュリティに対してとても大きなインパクトを与えた。

1.2 エンタングルメントを判定する意義

量子レジスタの状態は各々の量子ビットが分けられるかどうかで、分離可能な状態か分離不可能な状態かに分類できる。分離不可能な絡み合い状態はエンタングルメント状態と呼ばれる。現在までに、2量子ビットのエンタングルメント状態は明確に理解されている。しかし、量子ビットの数が増えると量子状態は複雑になって、エンタングルメントの判定が困難になる。本研究においては、「 k -subsystem total semi-separability (TSS)」と「 k -subsystem partial semi-separability (PSS)」

と呼ばれる二つの判定基準 [5] を使って、多粒子系エンタングルメント状態の判定と分類を行った。

2 エンタングルメントの相関理論

2.1 量子ビットと重ね合わせ状態

2.1.1 古典ビットと量子ビット

従来のコンピュータは、すべての情報を「0」か「1」で表現している。この情報を担うのがビット(古典ビット)と呼ばれるもので、物理的にはトランジスタのオン・オフ、メモリセル中の電荷の有無、ハードディスク中の磁性体の磁化方向などの状態を用いて表されている。ビットはある瞬間に「0」また「1」のどちらかの状態を取ることである。

量子コンピュータではビットの代わりに量子ビット(qubit)というものをを用いる。量子ビットは、上向きスピンと下向きスピンの2量子状態を持つ量子系で表すことができる。しかし、量子系は上向きスピンと下向きスピンの重ね合わせ状態も表現できる。その重ね合わせ状態は、1つの量子ビットの場合で説明すると、ある瞬間に同時に上向きスピンと下向きスピンを持ち合わせているような状態である。光子の分極の方向や励起原子の離散的エネルギー準位など、任意の2状態量子系は量子ビットを表すことができる。

数学的に、量子系の状態はヒルベルト空間上の1つの列ベクトル(状態ベクトル)で記述できる。状態ベクトルは通常 $|\psi\rangle$ (ケット・ベクトル)と呼ばれる特殊な括弧表示を用いて書かれる。このケットという言葉はディラック(Paul Dirac)によって考案された。列ベクトルと複素共役なベクトルはブラ・ベクトルと呼ばれ、 $\langle |$ と表記する行ベクトルである。数式で列ベクトルと行ベクトルの関係を表すと $\langle \psi | = (|\psi\rangle)^\dagger$ になる。行ベクトルと列ベクトルの積は、Dirac が $\langle \psi | \psi \rangle$ と書いた [3]。その表記を使って、量子ビットの状態は $|0\rangle$ 、 $|1\rangle$ と表すことができる。重ね合わせ状態は、 $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ になる。 α, β は複素数であり、確率振幅である。ただし、 $|\alpha|^2 + |\beta|^2 = 1$ 。 $|\alpha|^2$ は $|0\rangle$ 状態の存在確率で、 $|\beta|^2$ は $|1\rangle$ 状態の存在確率である。

2.1.2 重ね合わせの原理および重ね合わせの意義

一度に1つの許される状態にしか存在しないのではなく、同時にすべての許される状態が混ぜ合わされて存在するという量子系の性質は、重ね合わせの原理として知られている [3]。古典論的にはこのようなことは不可能である。この重ね合わせ状態にある量子ビットを n 個集めると、

$$|\psi\rangle = \sum_{i=0}^{2^n-1} \omega_i |\phi_i\rangle \quad (1)$$

になる。重み係数 ω_i は複素数であり、確率振幅と呼ばれる。 $\sum_{i=0}^{2^n-1} |\omega_i|^2 = 1$ で、 $|\omega_i|^2$ は基底状態 $|\phi_i\rangle$ の存在確率である。

量子コンピュータでは、このような重ね合わせ状態を入力として用いることにより、同時に表現された 2^n 個の値に対して一度に並列して処理を進めることができる。図 2.1 に表しているように、従来のコンピュータがデータ入力を 2^n ステップで行うのに対し、量子コンピュータは、それを1ステップで実行することができる。

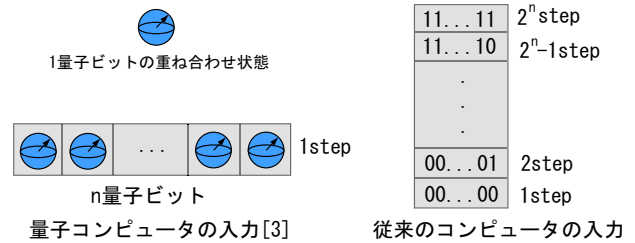


図 2.1 データの入力

2.2 波動関数

ミクロな粒子の3次元空間での運動を表す波動関数(wave function) ψ は、座標ベクトル $\mathbf{r} = (x, y, z)$ と時間 t の関数として $\psi(\mathbf{r}, t)$ と表される。波動関数 ψ は確率振幅と呼ばれる場合もあり、その絶対値の2乗

$$|\psi(\mathbf{r}, t)|^2 = \psi^*(\mathbf{r}, t)\psi(\mathbf{r}, t) \quad (2)$$

は、全空間で積分が1に規格化されているとき、ある時間 t 、ある位置 \mathbf{r} における粒子の確率密度を与える。また、波動関数 ψ は、 $|\psi\rangle$ という記号でも表される。波動関数は規格化条件

$$\langle \psi | \psi \rangle = 1 \quad (3)$$

を満たす。

2.2.1 時間に依存する波動関数

波動関数 ψ の時間変化を決定する運動方程式は、シュレディンガー方程式 (Schrödinger equation) と呼ばれ、以下の式で与えられる [1]。

$$i\hbar \frac{\partial}{\partial t} \psi(\mathbf{r}, t) = \hat{H}\psi(\mathbf{r}, t) \quad (4)$$

ここで、 \hat{H} はハミルトニアンと呼ばれ、運動エネルギーとポテンシャルエネルギーの和で表現される。ハミルトニアンが時間に依存しない場合は、

$$\frac{d\psi(t)}{dt} = \lim_{\Delta t \rightarrow 0} \frac{\psi(t + \Delta t) - \psi(t)}{\Delta t} \quad (5)$$

に注目すると、(4) から微小な時間 Δt に対して、波動関数の時間変化は

$$\psi(t + \Delta t) = \left(1 - \frac{i\hat{H}\Delta t}{\hbar}\right) \psi(t) \quad (6)$$

と表すことができる。ここで、波動関数の時間発展を表すオペレータ $U(\Delta t)$ を

$$U(\Delta t)\psi(t) = \psi(t + \Delta t) \quad (7)$$

と定義すると、

$$U(\Delta t) = \left(1 - \frac{i\hat{H}\Delta t}{\hbar}\right) \quad (8)$$

と求まり、ハミルトニアン \hat{H} はエルミート演算子で $\hat{H}^\dagger = \hat{H}$ であるから $U(\Delta t)$ は Δt の一次のオーダーで

$$U(\Delta t)U^\dagger(\Delta t) = \left(1 - \frac{i\hat{H}\Delta t}{\hbar}\right) \left(1 + \frac{i\hat{H}\Delta t}{\hbar}\right) \cong 1 \quad (9)$$

となり、ユニタリ演算子である。時間変化を $t + \Delta t \rightarrow t'$ と書き換えて

$$U(\Delta t) = u(t', t) \quad (10)$$

と表す。ここで $t' - t = \Delta t$ は微小な時間変化である。時間発展の演算子により、波動関数 ψ を $t_0 \rightarrow t = t_0 + \Delta t \rightarrow t' = t + \Delta t$ と時間発展させると

$$\begin{aligned} \psi(t') &= U(t', t)\psi(t) = U(t', t)U(t, t_0)\psi(t_0) \\ &= U(t', t_0)\psi(t_0) \end{aligned} \quad (11)$$

から

$$U(t', t_0) = U(t', t)U(t, t_0) \quad (12)$$

と、 $U(t', t_0)$ は微小な時間発展の演算子の積として表される。さらに、

$$U(t', t_0) = \left(1 - \frac{i\hat{H}}{\hbar}\Delta t\right) U(t, t_0) \quad (13)$$

から

$$\frac{U(t', t_0) - U(t, t_0)}{\Delta t} = -\frac{i\hat{H}}{\hbar}U(t, t_0) \quad (14)$$

となり、 $\Delta t \rightarrow 0$ の極限で

$$\frac{1}{U(t, t_0)} \frac{dU(t, t_0)}{dt} = -\frac{i\hat{H}}{\hbar} \quad (15)$$

と表される。この両辺を積分すると

$$U(t, t_0) = e^{-\frac{i}{\hbar}\hat{H}(t-t_0)} \quad (16)$$

が求められる。ここで $U(t_0, t_0) = 1$ の規格化条件を用いた。 t_1 から t_2 への有限な時間変化もこのユニタリ演算子 (16) を用いて

$$\psi(\mathbf{r}, t_2) = U(t_2, t_1)\psi(\mathbf{r}, t_1) \quad (17)$$

と表すことができる。

2.2.2 時間に依存しない波動関数

ハミルトニアン \hat{H} が時間に依存しないとき、 ψ を時間に依存しない部分 $\phi(\mathbf{r})$ と時間に依存する部分 $f(t)$ の積

$$\psi(\mathbf{r}, t) = \phi(\mathbf{r})f(t) \quad (18)$$

と表すと、シュレディンガー方程式 (4) から

$$i\hbar\phi(\mathbf{r})\frac{\partial f(t)}{\partial t} = \hat{H}\phi(\mathbf{r})f(t) \quad (19)$$

となる。(19) を $\psi(\mathbf{r}, t)$ で割ると

$$i\hbar\frac{1}{f(t)}\frac{\partial f(t)}{\partial t} = \frac{1}{\phi(\mathbf{r})}\hat{H}\phi(\mathbf{r}) \equiv E \quad (20)$$

となり、時間に依存する部分と位置に依存する部分が分離できて、あらゆる時間と位置で両者が一致するのは (20) 式が定数であるときのみである。この定数を E とおくと、 $f(t)$ は積分できて

$$f(t) = e^{-i\frac{E}{\hbar}t} \quad (21)$$

と求めることができる。一方、位置に依存する $\phi(\mathbf{r})$ に対しては

$$\hat{H}\phi(\mathbf{r}) = E\phi(\mathbf{r}) \quad (22)$$

となり、 E はハミルトニアン \hat{H} の固有値であり、 $\phi(\mathbf{r})$ は固有状態を表していることがわかる。シュレディンガー方程式 (4) の解は、ハミルトニアンが時間に依存しないとき、

$$\psi(\mathbf{r}, t) = \phi(\mathbf{r})e^{-\frac{iEt}{\hbar}} \quad (23)$$

波動関数は空間部分と時間部分に分離できる。(23) から見ると、系は時間 t 変数より位相因子 $e^{-\frac{iEt}{\hbar}}$ しか変わらない、全く同じ状態である。つまり、系が 1 つのエネルギー固有状態にあれば、系が閉じている限りは、同じ状態にとどまり続ける。即ち、エネルギー固有状態は、定常状態 (steady state) である。

図 2.2 で示しているように、波動関数が有限な領域に局在するとき、時間に依存する場合、波動関数は時間 t 、位置 r における粒子の確率振幅を表している。波動関数が時間に依存しない場合、例えば、時間変数 t がある時間 t_0 であるとき、波動関数は各々の基底状態の確率振幅を表している。

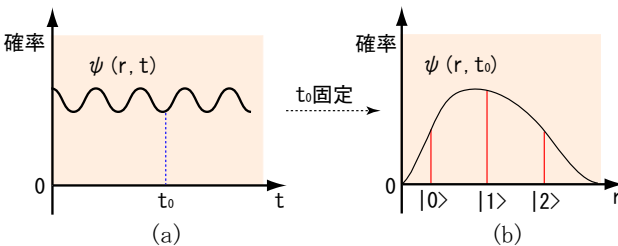


図 2.2 波動関数の表現
(a) 時間に依存する場合
(b) 時間に依存しない場合

2.3 エンタングルメントの定義

エンタングルメントの発見は、1935 年にアインシュタインらにより問題提起された「EPR パラドックス」である。エンタングルメント (entanglement) 状態は複数の量子ビット間に形成される量子力学特有の絡み合い状態である。この状態は「非局所性」と「分離不可能」な性質を持っている。「非局所性」は個々の量子ビットが相互作用し、量子ビットが空間的に離れても量子力学的な一体性を保つ、

このような性質を非局所性と言う。「分離不可能」とは、ビット間に量子力学特有の相関関係 (量子相関) が存在することであり、個々の量子ビットの状態の積で表現できない性質である。

2.3.1 古典相関と量子相関の関係

先述したように、エンタングルしている量子ビット間に量子相関が存在し、これは一般の相関関係 (古典相関) と区別される。古典相関は、2 つ以上の要素間に存在する関係である。例えば夫婦が一人ずつ東京と大阪に旅行したとすると、大阪に行った人が女性と分かったとき、東京に行ったのは男性と瞬時に分かる。この相関は、人がどちらに行くかを決めた時点で、すでに決まっていた。これは初めから決まっていたことを今知ったというだけのことであり、大阪の人が何かを制御してその影響を同時に東京に伝えることはできない。

量子相関 (quantum correlation) は個々の量子ビット間に存在する量子力学的な相関関係である。例えば、粒子 A と B のスピンの向き (上: $|0\rangle$, 下: $|1\rangle$) を測るという実験を行うとする。まず、エンタングルメント状態を用意する。このとき、エンタングルしている粒子間には量子相関が存在し、A が上向きなら B は必ず上向き、A が下向きなら B は必ず下向きになる。これを数式で表すと $|0_A0_B\rangle, |1_A1_B\rangle$ になる。従って、粒子 A と B のエンタングルメント状態は $|\psi\rangle = \frac{1}{\sqrt{2}}(|0_A0_B\rangle + |1_A1_B\rangle)$ になる。エンタングルメント状態は観測される前は、 $|0_A0_B\rangle$ あるいは $|1_A1_B\rangle$ に定まっていなかった状態で、 $|0_A0_B\rangle$ と $|1_A1_B\rangle$ という重ね合わせになっている。観測したとき、A が $|0_A\rangle$ 状態なら、その情報を同時に B へ伝え、B は同時に $|0_B\rangle$ 状態に決まる。あるいは、A が $|1_A\rangle$ 状態と分かった瞬間に、B は同時に $|1_B\rangle$ 状態と決まる。量子相関とは、観測されたとき決定される状態の間に存在する相関関係である。

2.3.2 エンタングルメントと量子相関の関係

複数の量子ビット間に量子相関が存在し、かつ分離できない重ね合わせ状態はエンタングルメント状態である。エンタングルメントは量子相関と同じと思われているが、両者には異なる点がある。エンタングルメント状態には必ず量子相関が存在す

るが、量子相関が存在してもエンタングルメントと
 言えない状態がある。例えば、量子ビット A と B
 の関係が $|\psi\rangle = \frac{1}{\sqrt{2}}(|0_A0_B\rangle + |1_A1_B\rangle)$ とき、この
 状態はテンソル積で分離できない。つまりエンタ
 ングルメント状態であり、量子相関が存在する。こ
 のエンタングルメント状態を観測する。

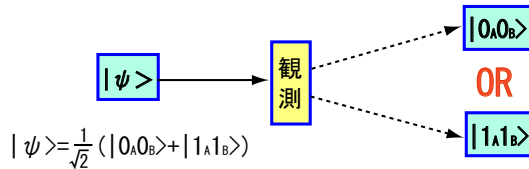


図 2.3 エンタングルメントと量子相関の関係

図 2.3 のように、この状態を観測した後、 $|0_A0_B\rangle$
 あるいは $|1_A1_B\rangle$ の状態になる。 $|0_A0_B\rangle$ あるいは
 $|1_A1_B\rangle$ 状態には量子相関が存在するが、もはやエ
 ンタングルメント状態ではない。

2.3.3 エンタングルメントと重ね合わせの関係

エンタングルメントと重ね合わせは量子系に特
 有の状態であるが、類似点と相違点がある。ここ
 では具体的に、量子ビット A と量子ビット B を含
 む 2 粒子の状態を使って、エンタングルメントと
 重ね合わせの関係を説明する。仮に今、 $\alpha|0_A0_B\rangle +$
 $\beta|0_A1_B\rangle$ という状態がある。これは $|0_A0_B\rangle$ とい
 う状態と $|0_A1_B\rangle$ という状態の重ね合わせ状態を
 表している。しかしよく見るとこの重ね合わせ状
 態では、量子ビット A は常に $|0_A\rangle$ 状態であり、
 $\alpha|0_A0_B\rangle + \beta|0_A1_B\rangle = |0_A\rangle(\alpha|0_B\rangle + \beta|1_B\rangle)$ と書
 き直すことができる。(ちなみに、このとき量子
 ビット B は $\alpha|0_B\rangle + |1_B\rangle$ という重ね合わせ状態を
 とっていることになる)。つまり、2 つの量子ビッ
 トの状態を分離できる。したがって、この状態はエ
 ンタングルメント状態ではない。

それでは、 $\alpha|0_A0_B\rangle + \beta|1_A1_B\rangle$ という状態は重
 ね合わせ状態であることに変わりはないが、今回は
 上のように個々の量子ビットの状態に分離するこ
 とはできない。したがって、これはエンタングルメ
 ント状態である。

つまり、エンタングルメント状態は必ず重ね合
 わせ状態である。しかしながら、重ね合わせ状態
 であるからといって、必ずしもエンタングルメント状態

であるとは限らない。エンタングルメント状態と
 いうのは、量子ビット間に量子相関がはたらいたと
 き、初めて実現される状態である。

2.3.4 重ね合わせと量子相関とエンタングルメントの関係

図 2.4 示しているように、エンタングルメント状
 態は重ね合わせ状態で、量子相関も存在する。量子
 相関が存在することはエンタングルメントである
 ための必要条件になる。重ね合わせはエンタング
 ルメントであるための必要条件である。



図 2.4 重ね合わせと量子相関とエンタングルメン
 トの関係

量子ビット A と B を含む 2 粒子系において、
 $\frac{1}{\sqrt{3}}(|0_A1_B\rangle + |1_A0_B\rangle + |1_A1_B\rangle)$ のような状態は、
 個々の基底状態の重ね合わせになっている。これ
 は量子ビット間に相関関係が存在し、かつ各々の量
 子ビットの状態に分離できない、エンタングルメン
 ト状態である。この 2 粒子系において、量子相関が
 存在する $|1_A1_B\rangle$ のような状態は積状態である。こ
 の積状態は重ね合わせでもエンタングルメントで
 もない。1 粒子系における量子ビット A の重ね合
 わせ状態は $|\psi_A\rangle = \frac{1}{\sqrt{2}}(|0_A\rangle + |1_A\rangle)$ のような状態
 である。この重ね合わせ状態はエンタングルメン
 ト状態ではなく、量子相関関係が存在しない状態
 である。エンタングルメントは複素粒子系における
 量子力学的な絡み合いであり、量子相関は複素粒子
 状態間に存在する量子力学的な相関関係のことで
 ある。

2.4 量子回路

2.4.1 電気回路と量子回路

一般に電気回路は、多数の論理ゲートから構成さ
 れている。通常のコンピュータを実現するのに用
 いられている論理ゲートには、AND, NOT, OR,
 NOR などがある。それぞれの論理ゲートは非常に

単純なものだが、例えば AND と NOT、または OR と NOT の二種類のゲートを用いれば、チューリング機械のどんな動作も模倣する回路を構成することができる。実際、従来のコンピュータはこのような回路から構成されている。一方、量子コンピュータとは、時間に依存したシュレディンガー方程式に従う量子系をコンピュータとして使うものである。入力された量子状態が時間経過して出力側の量子状態になる。シュレディンガー方程式が時間反転可能であるため、量子状態を扱う量子回路は可逆回路でなければならない。つまり、量子回路は可逆ゲートで構成される。可逆ゲートでは、出力から入力再現できるために、出力端子の数は入力端子の数と同じでなければならないことは明らかである。また、量子コンピュータの特徴は、論理値 0 と論理値 1 の重ね合わせがありうるということである [1]。

古典的な論理回路では、AND 等の素子には入力側の配線から入ってきた値が素子の中で処理され、出力側に出ていく。これに対して、量子回路では必ずしも入力側と出力側の位置の区別がない。すなわち、ある入力状態にあるスピンの、磁場等による相互作用により、一定時間の後に出力状態に変わる、という仕組みになっている場合がある (図 2.6)[1]。

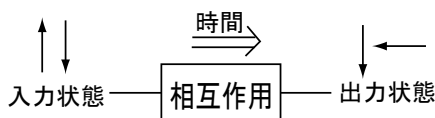


図 2.5 量子ゲートの仕組み

量子論理ゲートにもさまざまなタイプが存在し、世界中で量子回路のシミュレーションの研究が行なわれているが、特にユニタリ変換ゲートと制御 NOT ゲートが有名である。原理的には、この二種類の量子論理ゲートで量子チューリング機械のすべての動作を模倣することができると考えられている。

2.4.2 ユニタリ変換ゲートと制御ユニタリ変換ゲート

量子状態間の遷移行列はユニタリ行列で表すことができる。量子コンピュータにおける n 量子ビット

の各状態の複素振幅の遷移行列は $2^n \times 2^n$ のユニタリ行列で表現することができる。1 量子ビットのユニタリゲートと 2 量子ビットの制御 NOT ゲートの組み合わせは任意のユニタリ変換を実現することができる。1 量子ビットの基底状態は行列で表すと、 $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ 、 $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ 、となる。また、これらの重ね合わせ状態は $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ である。ただし、 α と β は複素数で、 $|\alpha|^2 + |\beta|^2 = 1$ である。

ユニタリ変換ゲート

ユニタリ行列

$$U \equiv \begin{pmatrix} \langle 0|U|0\rangle & \langle 0|U|1\rangle \\ \langle 1|U|0\rangle & \langle 1|U|1\rangle \end{pmatrix} \quad (24)$$

を使えば、出力側の状態ベクトル = $U \times$ 入力側の状態ベクトルと書ける。図 2.6 にはユニタリ変換ゲートの回路記号を表している [1]。

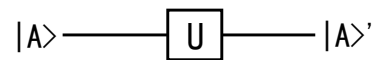


図 2.6 ユニタリ変換ゲート

恒等変換 (単位行列)

$|0\rangle \rightarrow |0\rangle$ 、 $|1\rangle \rightarrow |1\rangle$ で単位行列：

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad (25)$$

で表される。

NOT ゲート

$|0\rangle$ と $|1\rangle$ が入れ替わるので、

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad (26)$$

行列で表すことができる。

$$\begin{aligned} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} |0\rangle &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle \\ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} |1\rangle &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle \end{aligned} \quad (27)$$

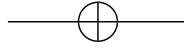


図 2.7 量子 NOT ゲートの回路記号

図 2.7 の入力側から量子ビット A の状態 $|0_A\rangle$ を入力すると、出力側に $|1_A\rangle$ を得ることができる。 $|1_A\rangle$ 状態を入力したら、 $|0\rangle$ 状態を出力する。量子 NOT ゲートの真理値表 (表 1) は以下である。

$ A\rangle$	$ A'\rangle$
0	1
1	0

表 1 量子 NOT ゲートの真理値表

アダマール・ゲート (Hadamard Gate)

下の行列 (28) は、アダマール・ゲートを表している。

$$H \equiv \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad (28)$$

このゲートは重ね合わせ状態を作るときに利用され、2 度作用すると恒等変換になる行列である。

$$\begin{aligned} \hat{H}|0\rangle &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ \hat{H}|1\rangle &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned} \quad (29)$$

下の図 2.8 はアダマール・ゲートの回路記号である。

$$\alpha|0\rangle + \beta|1\rangle \longrightarrow \boxed{H} \longrightarrow \alpha \frac{|0\rangle + |1\rangle}{\sqrt{2}} + \beta \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

図 2.8 アダマール・ゲートの回路記号

制御ユニタリ変換ゲート (Controlled Unitary Gate)

2 量子ビットゲートで、1 量子ビットユニタリ変換を伴う制御ユニタリ変換ゲートは次のように定義される。

$$\begin{aligned} |A\rangle = |0\rangle &\rightarrow |A'\rangle = |A\rangle = |0\rangle, |B'\rangle = |B\rangle \\ |A\rangle = |1\rangle &\rightarrow |A'\rangle = |A\rangle = |1\rangle, |B'\rangle = U|B\rangle \end{aligned}$$

行列で表すと以下ようになる。

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \langle 0|U|0\rangle & \langle 0|U|1\rangle \\ 0 & 0 & \langle 1|U|0\rangle & \langle 1|U|1\rangle \end{pmatrix} \quad (30)$$

下の図 2.9 は制御ユニタリ変換ゲートの回路記号を表している。

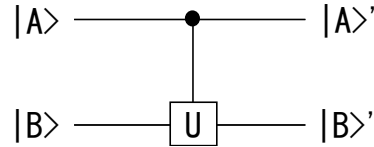


図 2.9 制御ユニタリ変換ゲートの回路記号

特に、U が NOT ゲートするとき、制御 NOT ゲートと呼ばれる。

制御 NOT ゲート (Controlled Not Gate)

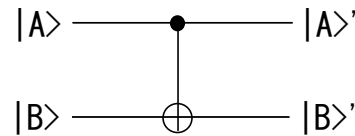


図 2.10 制御 NOT ゲート

制御 NOT ゲート (CNOT) とは 2 入力 2 出力のゲートである。回路図 2.11 において、上のビット $|A\rangle$ が制御ビット、下のビット $|B\rangle$ が標的ビットと呼ばれる。制御ビット A の状態はそのまま出力し、 $|A'\rangle = |A\rangle$ である。出力側の $|B'\rangle$ について、制御ビット A が $|0\rangle$ のとき、標的ビットにそのまま出力し、制御ビット A が $|1\rangle$ のとき、標的ビットを反転させる。数式で表すと、 $|B'\rangle = |A\rangle \oplus |B\rangle$ となる。CNOT ゲートはエンタングルメント状態を作るために必要なゲートである。CNOT ゲートは行列で表現すると以下の行列になる。

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad (31)$$

2 量子ビットにおける任意の量子状態を、この回路に入力した場合の出力状態を以下の真理値表 (表 2) に示している。

$ A\rangle$	$ B\rangle$	$ A'\rangle$	$ B'\rangle$
$ 0\rangle$	$ 0\rangle$	$ 0\rangle$	$ 0\rangle$
$ 0\rangle$	$ 1\rangle$	$ 0\rangle$	$ 1\rangle$
$ 1\rangle$	$ 0\rangle$	$ 1\rangle$	$ 1\rangle$
$ 1\rangle$	$ 1\rangle$	$ 1\rangle$	$ 0\rangle$

表 2 制御 NOT ゲートの真理値表

2.4.3 エンタングルメントの生成回路

2量子ビット・エンタングルメント生成回路

アダマール・ゲートは1量子ビットの重ね合わせ状態を生成することができる。制御 NOT ゲートについて、制御ビットが $|1\rangle$ 状態のとき、標的ビットの状態を反転させる。この2つのゲートの組み合わせることで、エンタングルメント生成回路を構成することができる。

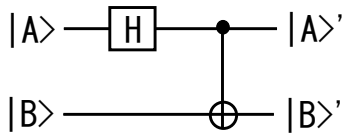


図 2.11 2量子ビットのエンタングルメント生成回路

図 2.11 で表しているように、まず、制御ビット $|A\rangle$ にアダマール・ゲートが作用することで、重ね合せ状態が生成される。そして、制御が量子状態の重ね合わせで行われるため、制御ビットと標的ビットが互いに絡みあった状態になる。この生成回路を行列で表すと、

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{pmatrix} \quad (32)$$

となる。制御ビット A と標的ビット B のすべての入力状態に対して、出力状態は以下の真理値表 (表 3) で示している。

$ A\rangle$	$ B\rangle$	$ AB'\rangle$
$ 0\rangle$	$ 0\rangle$	$\frac{1}{\sqrt{2}}(0_A0_B\rangle + 1_A1_B\rangle)$
$ 0\rangle$	$ 1\rangle$	$\frac{1}{\sqrt{2}}(0_A1_B\rangle + 1_A0_B\rangle)$
$ 1\rangle$	$ 0\rangle$	$\frac{1}{\sqrt{2}}(0_A0_B\rangle - 1_A1_B\rangle)$
$ 1\rangle$	$ 1\rangle$	$\frac{1}{\sqrt{2}}(0_A1_B\rangle - 1_A0_B\rangle)$

表 3 真理値表

3量子ビット・エンタングルメント生成回路

アダマール・ゲートと制御 NOT ゲートの組み合わせ回路は3量子ビットのエンタングルメント状態を作ることも可能である。図 2.12 は3量子ビットのエンタングルメント生成回路である。

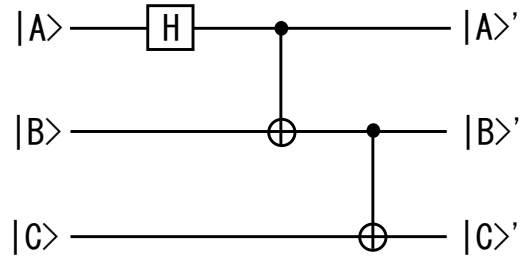


図 2.12 3量子ビットのエンタングルメント生成回路

この生成回路は行列で表すと、

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \end{pmatrix} \quad (33)$$

となる。入力側に $|A\rangle$, $|B\rangle$, $|C\rangle$ のすべての状態 $|0_A0_B0_C\rangle \dots |1_A1_B1_C\rangle$ を入力したときの出力状態を、以下の真理値表 (表 4) に示す。

$ A\rangle$	$ B\rangle$	$ C\rangle$	$ ABC'\rangle$
$ 0\rangle$	$ 0\rangle$	$ 0\rangle$	$\frac{1}{\sqrt{2}}(0_A0_B0_C\rangle + 1_A1_B1_C\rangle)$
$ 0\rangle$	$ 0\rangle$	$ 1\rangle$	$\frac{1}{\sqrt{2}}(0_A0_B1_C\rangle + 1_A1_B0_C\rangle)$
$ 0\rangle$	$ 1\rangle$	$ 0\rangle$	$\frac{1}{\sqrt{2}}(0_A1_B1_C\rangle + 1_A0_B0_C\rangle)$
$ 0\rangle$	$ 1\rangle$	$ 1\rangle$	$\frac{1}{\sqrt{2}}(0_A1_B0_C\rangle + 1_A0_B1_C\rangle)$
$ 1\rangle$	$ 0\rangle$	$ 0\rangle$	$\frac{1}{\sqrt{2}}(0_A0_B0_C\rangle - 1_A1_B1_C\rangle)$
$ 1\rangle$	$ 0\rangle$	$ 1\rangle$	$\frac{1}{\sqrt{2}}(0_A0_B1_C\rangle - 1_A1_B0_C\rangle)$
$ 1\rangle$	$ 1\rangle$	$ 0\rangle$	$\frac{1}{\sqrt{2}}(0_A1_B1_C\rangle - 1_A0_B0_C\rangle)$
$ 1\rangle$	$ 1\rangle$	$ 1\rangle$	$\frac{1}{\sqrt{2}}(0_A1_B0_C\rangle - 1_A0_B1_C\rangle)$

表 4. 3量子ビットのエンタングルメント生成回路の真理値表

一般に、アダマール・ゲートと $(n-1)$ 個の制御 NOT ゲートを組み合わせることで、 n 量子ビットのエンタングルメント状態を生成することができる (図 2.14)。

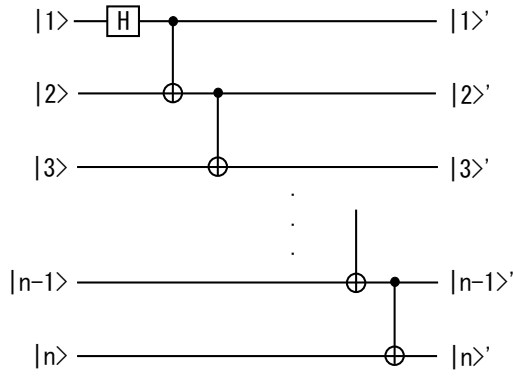


図 2.14 n 量子ビットのエンタングルメント生成回路

3 純粋状態と混合状態

3.1 純粋状態と混合状態の定義

量子状態には「純粋状態」と「混合状態」が存在する。どんな物理量を測っても他の二つ以上の状態に関する測定値を混合したような確率分布が得られる状態が混合状態 (mixed state) であり、そうではない状態が純粋状態 (pure state) である。数式を用いて定義を繰り返しておく。一般に、用意された状態 $|\psi\rangle$ について、どんな物理量 A を測っても、その測定値の確率分布 $P_\psi(a)$ が、別の n ($n > 2$) 個の状態 $|\psi_0\rangle, |\psi_1\rangle, \dots, |\psi_{n-1}\rangle$ における測定値の確率分布 $P_{\psi_0}(a), P_{\psi_1}(a), \dots, P_{\psi_{n-1}}(a)$ の「重みをつけた平均値」に等しいとき、すなわち

$$P_\psi(a) = \sum_{j=0}^{n-1} \lambda_j P_{\psi_j}(a)$$

for all a ($0 \leq \lambda_j \leq 1, \sum_{j=0}^{n-1} \lambda_j = 1$) (34)

を満たす n 個の異なる状態 $|\psi_0\rangle, |\psi_1\rangle, \dots, |\psi_{n-1}\rangle$ と定数 λ_j ($0 \leq j \leq n-1$) が存在するとき、混合状態 (mixed state) という [2]。他方、純粋状態は、混合状態の理想極限 ($\lambda \rightarrow 1$) とも見なせる。純粋状態と混合状態の関係は下の図 3.1 に示している。

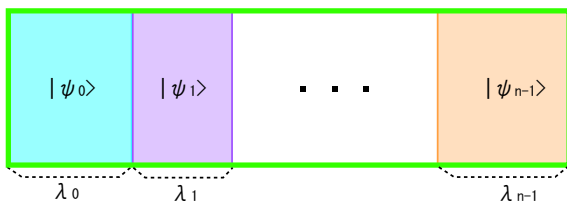


図 3.1 純粋状態と混合状態の関係

3.2 密度演算子と密度行列 — 純粋状態と混合状態の行列表現

3.2.1 密度演算子

量子力学で、混合状態や純粋状態を扱うとき、密度演算子 $\hat{\rho}$ を用いる場合がある。純粋状態の密度演算子 $\hat{\rho}_1$ は、波動関数 $|\psi\rangle$ を使って表すことができる。

$$\hat{\rho}_1 = |\psi\rangle\langle\psi| \quad (35)$$

混合状態の場合、 $|\psi_j\rangle$ ($j \geq 2$) を完全系とし、

$$\hat{\rho}_2 = \sum_j \lambda_j |\psi_j\rangle\langle\psi_j| \quad (36)$$

$\hat{\rho}_2$ はその状態の密度演算子である。ただし、 λ_j が状態 $|\psi_j\rangle$ の統計的確率であり、その総和は $\sum_j \lambda_j = 1$ である。

3.2.2 密度行列

密度演算子のハイゼンベルク行列力学的な表現は密度行列と言う、記号は ρ である。用意された状態の基底を具体的に決めると密度行列が書け、異なる基底を決めれば異なる密度行列が書ける。

以下は粒子 A, B を含む 2 粒子系の純粋状態に対して、異なる基底から得た異なる密度行列の例である。

基底 1 :

$$\begin{aligned} |0_A 0_B\rangle &= \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} & |0_A 1_B\rangle &= \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \\ |1_A 0_B\rangle &= \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} & |1_A 1_B\rangle &= \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \end{aligned} \quad (37)$$

基底 2 :

$$\begin{aligned} |0_A 0_B\rangle' &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} & |0_A 1_B\rangle' &= \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} \\ |1_A 0_B\rangle' &= \frac{1}{\sqrt{2}} \begin{pmatrix} -1 \\ 0 \\ 1 \\ 0 \end{pmatrix} & |1_A 1_B\rangle' &= \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ -1 \\ 0 \\ 1 \end{pmatrix} \end{aligned} \quad (38)$$

ある純粋状態 $|\psi\rangle$ がエンタングルメント状態で、たとえば、 $|\psi\rangle = \frac{1}{\sqrt{2}}|0_A1_B\rangle + \frac{1}{\sqrt{2}}|1_A0_B\rangle$ であるとき、この状態の密度演算子は

$$\hat{\rho} = |\psi\rangle\langle\psi| \quad (39)$$

となる。密度演算子 $\hat{\rho}$ は基底 1 (37) を使って表すと、

$$\begin{aligned} \hat{\rho} &= |\psi\rangle\langle\psi| \\ &= \left(\frac{1}{\sqrt{2}}(|0_A1_B\rangle + |1_A0_B\rangle) \right) \\ &\quad \left(\frac{1}{\sqrt{2}}(\langle 0_A1_B| + \langle 1_A0_B|) \right) \\ &= \frac{1}{2}|0_A1_B\rangle\langle 0_A1_B| + \frac{1}{2}|0_A1_B\rangle\langle 1_A0_B| \\ &\quad + \frac{1}{2}|1_A0_B\rangle\langle 0_A1_B| + \frac{1}{2}|1_A0_B\rangle\langle 1_A0_B| \quad (40) \end{aligned}$$

となる。密度演算子 $\hat{\rho}$ は基底 2 (38) を使って表すと、

$$\begin{aligned} \hat{\rho} &= |\psi\rangle\langle\psi| \\ &= \left(\frac{1}{\sqrt{2}}(|0_A1_B\rangle' + |1_A0_B\rangle') \right) \\ &\quad \left(\frac{1}{\sqrt{2}}(\langle 0_A1_B|' + \langle 1_A0_B|') \right) \\ &= \frac{1}{2}|0_A1_B\rangle'\langle 0_A1_B|' + \frac{1}{2}|0_A1_B\rangle'\langle 1_A0_B|' \\ &\quad + \frac{1}{2}|1_A0_B\rangle'\langle 0_A1_B|' + \frac{1}{2}|1_A0_B\rangle'\langle 1_A0_B|' \quad (41) \end{aligned}$$

となる。密度演算子 (40) から得た密度行列 ρ_1 は

$$\begin{aligned} \rho_1 &= \frac{1}{2} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} (0100) + \frac{1}{2} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} (0010) \\ &\quad + \frac{1}{2} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} (0100) + \frac{1}{2} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} (0010) \\ &= \frac{1}{2} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad (42) \end{aligned}$$

である。密度演算子 (41) から得た密度行列 ρ_2 は

$$\begin{aligned} \rho_2 &= \frac{1}{4} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} (0101) + \frac{1}{4} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} (-1010) \\ &\quad + \frac{1}{4} \begin{pmatrix} -1 \\ 0 \\ 1 \\ 0 \end{pmatrix} (0101) + \frac{1}{4} \begin{pmatrix} -1 \\ 0 \\ 1 \\ 0 \end{pmatrix} (-1010) \\ &= \frac{1}{4} \begin{pmatrix} 1 & -1 & -1 & -1 \\ -1 & 1 & 1 & 1 \\ -1 & 1 & 1 & 1 \\ -1 & 1 & 1 & 1 \end{pmatrix} \quad (43) \end{aligned}$$

である。

4 エンタングルメントの判定方法と結果

4.1 2 粒子系の量子状態

2 量子ビットの純粋状態はエンタングルメント状態と分離可能な状態に分かれる。2 量子ビットの混合状態は 2 つ以上の純粋状態が割合で組み立てた状態以外に、積状態の混合状態も存在する (図 4.1)。

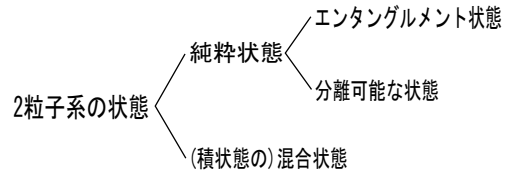


図 4.1 2 量子ビットの状態

量子ビット A と B を含む 2 粒子系の各々の量子状態を説明する。 $|0_A1_B\rangle + |1_A0_B\rangle$ あるいは $|0_A0_B\rangle + |0_A1_B\rangle + |1_A0_B\rangle$ のような状態は分離できない、エンタングルメント状態である。分離可能な状態は量子相関が存在しない、テンソル積で書ける状態である。例えば、 $(|0_A\rangle + |1_A\rangle) \otimes (|0_B\rangle + |1_B\rangle)$ のような状態は分離可能な状態である。積状態は量子ビットが決まった $|0\rangle$ あるいは $|1\rangle$ のような状態、重ね合わせが存在しない状態である。例えば $|0_A1_B\rangle$ が 30% の割合で、 $|1_A0_B\rangle$ が 70% の割合で混ざったような状態は積状態の混合状態である。

4.2 判定方法: TSS と PSS

前の節に説明したように、2 量子ビットの状態は明らかになった。しかし、量子ビットの数が増えると量子状態が複雑になり、エンタングルメント

状態の判定も難しくなる。全体的に準分離可能な k 組のサブシステム (TSS) と部分的に準分離可能な k 組のサブシステム (PSS)[5]、2つの判定方法を使って、 n 粒子系は2粒子系に分解し、個々の粒子と粒子の関係を明らかになった後、元の多粒子系の状態を判定することができる。

まず、よく使う重要な状態、準分離可能な状態 (semi-separability) を定義する。準分離可能な状態とは、粒子系を一個以上の粒子からなるサブシステムに分割し、サブシステムとサブシステムの間量子相関関係が存在しない、テンソル積で表現できる状態である。準分離可能な状態と分離可能な状態は区別がある。分離可能な状態は量子ビットの間に量子相関が存在せず、粒子と粒子のテンソル積が書ける。一方、準分離可能な状態はサブシステム間に量子相関が存在せず、サブシステム間のテンソル積が書ける、サブシステムの中の粒子が分離できるかどうか、はっきりしていない。

準分離可能な状態は全体的に準分離可能な状態と部分的に準分離可能な状態を含んでいる。 n 個粒子を含む多粒子系を一個以上の粒子からなる k 組 ($n > k$) のサブシステムに分割して、 k 組のサブシステムの分離可能性をチェックしたとき、互いに分離可能なら、全体的に準分離可能な k 組のサブシステムと定義する。その状態は全体的に準分離可能な状態 (TSS) である。数式で表すと、

$$|sub_1\rangle \otimes |sub_2\rangle \otimes \dots \otimes |sub_k\rangle \quad (44)$$

になる。 k 組のサブシステムは互いに分離できないなら、必ず何らかのエンタングルメントを含むことになり、その場合は \overline{TSS} と表記する。図 4.2 は全体的に準分離可能な k 組のサブシステムの図である。

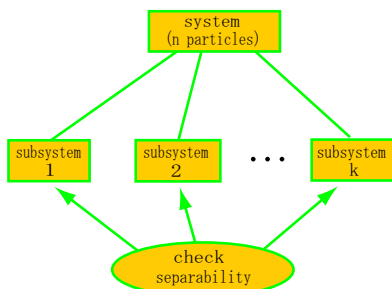


図 4.2 全体的に準分離可能な k 組のサブシステム

一方、その n 粒子系を $k+1$ 組のサブシステムに分割し、まず、任意の一組のサブシステムをのけて、残った k 組のサブシステムの分離可能性をチェックするとき、互いに分離可能なら、部分的に準分離可能な k 組のサブシステムと定義する。その状態は部分的に準分離可能な状態 (PSS) である。

$$|sub_1\rangle \otimes |sub_2\rangle \otimes \dots \otimes |sub_k\rangle, |sub_{k+1}\rangle \quad (45)$$

もし、分割した k 組のサブシステムは分離不可能なら、必ず何らかのエンタングルメントが含まれ、それを \overline{PSS} と表記する。以下の図 4.3 は部分的に準分離可能な k 組のサブシステムの図である。

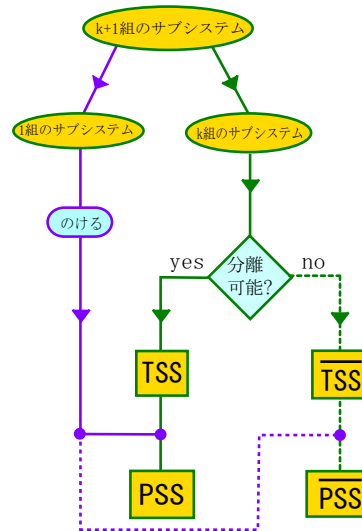


図 4.3 部分的に準分離可能な k 組のサブシステム

4.3 判定結果と証明

前の節で説明した2つの判定方法から判定結果を得た。その判定結果を使えば、量子レジスタの状態が判定しやすくなると考えられる。

まず、判定結果を証明するとき、よく使う「シュミット分解」を説明する。

$|\psi\rangle$ は量子ビット A のヒルベルト空間 H_A と量子ビット B のヒルベルト空間 H_B のテンソル積になった空間 H_{AB} の任意の状態である。ヒルベルト空間 H_A の基底が $\{|0_A\rangle, |1_A\rangle\}$ 、ヒルベルト空間 H_B の基底が $\{|0_B\rangle, |1_B\rangle\}$ 、従って、空間 H_{AB} の基底は $\{|0_A0_B\rangle, |0_A1_B\rangle, |1_A0_B\rangle, |1_A1_B\rangle\}$ と

なる。

$$\begin{aligned} |0_A 0_B\rangle &= |0_A\rangle \otimes |0_B\rangle, |0_A 1_B\rangle = |0_A\rangle \otimes |1_B\rangle \\ |1_A 0_B\rangle &= |1_A\rangle \otimes |0_B\rangle, |1_A 1_B\rangle = |1_A\rangle \otimes |1_B\rangle \end{aligned} \quad (46)$$

$|\psi\rangle$ 状態は空間 H_{AB} の基底状態で表すと

$$|\psi\rangle = C_0|0_A 0_B\rangle + C_1|0_A 1_B\rangle + C_2|1_A 0_B\rangle + C_3|1_A 1_B\rangle \quad (47)$$

となる。ただし、 $\sum_{j=0}^3 |C_j|^2 = 1$ 、 C_j は複素数である。この状態はシュミット分解で表すと、

$$|\psi\rangle = \alpha_0|0_A\rangle \otimes |0_B\rangle + \alpha_1|1_A\rangle \otimes |1_B\rangle \quad (48)$$

あるいは

$$|\psi\rangle = \beta_0|0_A\rangle \otimes |1_B\rangle + \beta_1|1_A\rangle \otimes |0_B\rangle \quad (49)$$

となる [6]。 α_0, α_1 は実数で、 $\alpha_0 \geq 0, \alpha_1 \geq 0, \alpha_0^2 + \alpha_1^2 = 1$ 。 β_0, β_1 は実数で、 $\beta_0 \geq 0, \beta_1 \geq 0, \beta_0^2 + \beta_1^2 = 1$ 。下の図 4.4 は、状態 $|\psi\rangle$ をシュミット分解した状態を表している。

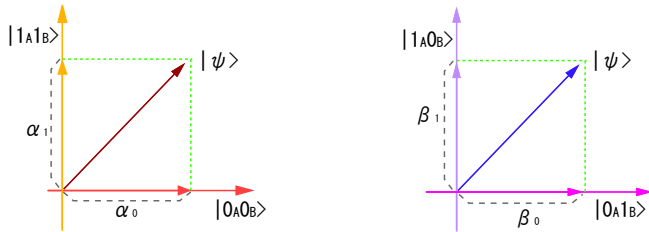


図 4.4 シュミット分解

下の図 4.5 で表しているように、 $C_0|0_A 0_B\rangle$ と $C_1|0_A 1_B\rangle$ の重ね合わせベクトルは $C_0|0_A 0_B\rangle + C_1|0_A 1_B\rangle$ であり、ベクトルの長さは $\sqrt{|C_0|^2 + |C_1|^2}$ である。この重ね合わせベクトルを回転させて、 $|0_A 0_B\rangle$ 基底で表すと、 $\sqrt{|C_0|^2 + |C_1|^2}|0_A 0_B\rangle$ となる。 $|0_A 1_B\rangle$ 基底で表現すると、このベクトルを逆方向に回転させて、 $\sqrt{|C_0|^2 + |C_1|^2}|0_A 1_B\rangle$ になる。

一方、 $C_2|1_A 0_B\rangle$ と $C_3|1_A 1_B\rangle$ の重ね合わせベクトルは $C_2|1_A 0_B\rangle + C_3|1_A 1_B\rangle$ であり、ベクトルの長さは $\sqrt{|C_2|^2 + |C_3|^2}$ である。この重ね合わせベクトルを回転させて、 $|1_A 0_B\rangle$ 基底で表すと、 $\sqrt{|C_2|^2 + |C_3|^2}|1_A 0_B\rangle$ となる。 $|1_A 1_B\rangle$ 基底で表

現すると、このベクトルを逆方向に回転させて、 $\sqrt{|C_2|^2 + |C_3|^2}|1_A 1_B\rangle$ になる。

(47) の状態 $|\psi\rangle$ をシュミット分解するとき、基底 $|0_A 0_B\rangle$ を使うなら、もう一つの基底は $|1_A 1_B\rangle$ にする。ただし、 $\alpha_0 = \sqrt{|C_0|^2 + |C_1|^2}$ 、 $\alpha_1 = \sqrt{|C_2|^2 + |C_3|^2}$ となる。一方、(47) の状態 $|\psi\rangle$ をシュミット分解するとき、片方の基底を $|0_A 1_B\rangle$ とするなら、もう一つの基底は $|1_A 0_B\rangle$ になる。ただし、 $\beta_0 = \sqrt{|C_0|^2 + |C_1|^2}$ 、 $\beta_1 = \sqrt{|C_2|^2 + |C_3|^2}$ となる。シュミット分解を行うときに用いる基底は $|0_A 0_B\rangle, |1_A 1_B\rangle$ の組か、あるいは $|1_A 0_B\rangle, |0_A 1_B\rangle$ の組である。基底 $|0_A 0_B\rangle, |0_A 1_B\rangle$ の組や、あるいは $|1_A 0_B\rangle, |1_A 1_B\rangle$ の組は使うことができない。例えば ($|0_A 0_B\rangle, |0_A 1_B\rangle$) 基底を使って、シュミット分解すると、量子ビット A のヒルベルト空間 H_A 中の $|1_A\rangle$ 基底が含まれない。この場合は、シュミット分解式は空間 H_{AB} を完全に表すことができない。

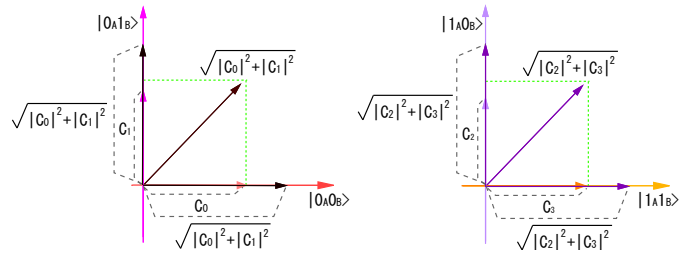


図 4.5 量子ビット A, B のヒルベルト空間

判定結果

- あらゆる TSS が成立する純粋状態は分離可能な状態であるための必要十分条件

まず、十分条件が成立することを証明する。

A, B, C, D 粒子を含む 4 粒子系に、あらゆる TSS が成立する純粋状態は分離可能な状態である。

証明：あらゆる TSS が成立するから、 $TSS(A, B, CD)$ が成立する。 $TSS(A, B, CD)$ が数式で表すと、

$$|\psi_{ABCD}\rangle = |\psi_A\rangle \otimes |\psi_B\rangle \otimes |\psi_{CD}\rangle \quad (50)$$

になる。もし、 $|\psi_{CD}\rangle = |\psi_C\rangle \otimes |\psi_D\rangle$ が成立するならば、この状態は分離可能な状態を証明できる。

$|\psi_{CD}\rangle = |\psi_C\rangle \otimes |\psi_D\rangle$ が成立しないと仮定すると、 $|\psi_{CD}\rangle$ はエンタングルメント状態である。シュミット分解 [6] より、

$$|\psi_{CD}\rangle = \alpha|\psi_C\rangle \otimes |\psi_D\rangle + \beta|\psi_C'\rangle \otimes |\psi_D'\rangle \quad (51)$$

になる。しかし、 $\alpha \geq 0$, $\beta \geq 0$, $\alpha^2 + \beta^2 = 1$, $\{|\psi_C\rangle, |\psi_C'\rangle\}$ は量子ビット C の直交基底、 $\{|\psi_D\rangle, |\psi_D'\rangle\}$ は量子ビット D の直交基底。そして、

$$\begin{aligned} |\psi_{ABCD}\rangle &= \alpha|\psi_A\rangle \otimes |\psi_B\rangle \otimes |\psi_C\rangle \otimes |\psi_D\rangle \\ &\quad + \beta|\psi_A\rangle \otimes |\psi_B\rangle \otimes |\psi_C'\rangle \otimes |\psi_D'\rangle \\ &= \alpha|\psi_A\rangle \otimes (|\psi_B\rangle \otimes |\psi_C\rangle) \otimes |\psi_D\rangle \\ &\quad + \beta|\psi_A\rangle \otimes (|\psi_B\rangle \otimes |\psi_C'\rangle) \otimes |\psi_D'\rangle \end{aligned} \quad (52)$$

が成立する。その結果、 $|\psi_D\rangle$ と $|\psi_{BC}\rangle$ は分離できない、つまりエンタングルしている。

しかし、あらゆる TSS が成立するから、 $TSS(A, BC, D)$ が成立する。従って、

$$|\psi_{ABCD}\rangle = |\psi_A\rangle \otimes |\psi_{BC}\rangle \otimes |\psi_D\rangle \quad (53)$$

が成り立つ。仮定から得た (52) と矛盾した。従って、 $|\psi_{CD}\rangle = |\psi_C\rangle \otimes |\psi_D\rangle$ が成立する。そして、 $|\psi_{ABCD}\rangle = |\psi_A\rangle \otimes |\psi_B\rangle \otimes |\psi_C\rangle \otimes |\psi_D\rangle$ が成立する。つまり、その状態は分離可能な状態である。

つぎに、必要条件が成立することを証明する。

ある 3 粒子系の純粋状態 $|\psi_{ABC}\rangle$ が分離可能な状態、その状態のすべての TSS が成立する。

証明： $|\psi_{ABC}\rangle$ は分離可能状態であるから、 $|\psi_{ABC}\rangle = |\psi_A\rangle \otimes |\psi_B\rangle \otimes |\psi_C\rangle$ が成り立つ。その結果、

$$\begin{aligned} TSS(A, BC) : |\psi_{ABC}\rangle &= |\psi_A\rangle \otimes |\psi_{BC}\rangle \\ TSS(B, AC) : |\psi_{ABC}\rangle &= |\psi_B\rangle \otimes |\psi_{AC}\rangle \\ TSS(C, AB) : |\psi_{ABC}\rangle &= |\psi_C\rangle \otimes |\psi_{AB}\rangle \end{aligned} \quad (54)$$

が成り立つ。 $TSS(A, BC)$ 、 $TSS(B, AC)$ 、 $TSS(C, AB)$ は 3 粒子系のすべての TSS の分類である。つまり、必要条件が成り立つ。

2. あらゆる TSS が成立する混合状態は分離可能な状態であるための必要条件

量子ビット A, B, C が含まれる 3 粒子系の基底を用意する。

$$\begin{aligned} |0_A 0_B 0_C\rangle &= \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} & |0_A 0_B 1_C\rangle &= \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} & \dots \\ |1_A 1_B 0_C\rangle &= \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} & |1_A 1_B 1_C\rangle &= \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \end{aligned} \quad (55)$$

まず、必要条件が成り立つことを証明する。

ある混合状態は分離可能なら、あらゆる TSS が成立する。

証明：「分離可能な混合状態」の意味は、その混合状態が含まれる各々の純粋状態が分離可能な状態であること。各々の純粋状態が分離可能であるから、各量子ビットが分離できる。従って、必要条件が成立する。

次に、十分条件が成立しないことを証明する。

あらゆる TSS が成立する混合状態には、エンタングルメント状態が含まれる可能性がある。

証明：3 粒子系のある混合状態は、 $|\psi_0\rangle$ 状態が $1/2$ の割合で、 $|\psi_1\rangle$ 状態が $1/2$ の割合で混ざった状態である。

$$\begin{aligned} |\psi_0\rangle &= \frac{1}{\sqrt{2}}(|0_A 0_B 0_C\rangle + |1_A 1_B 1_C\rangle) \\ |\psi_1\rangle &= \frac{1}{\sqrt{2}}(|0_A 0_B 0_C\rangle - |1_A 1_B 1_C\rangle) \end{aligned} \quad (56)$$

この混合状態の密度演算子 $\hat{\rho}$ は

$$\begin{aligned}\hat{\rho} &= \sum_{i=0}^1 \omega_i |\psi_i\rangle\langle\psi_i| \\ &= \frac{1}{2} |\psi_0\rangle\langle\psi_0| + \frac{1}{2} |\psi_1\rangle\langle\psi_1| \\ &= \frac{1}{2} (|0_A 0_B 0_C\rangle\langle 0_A 0_B 0_C| + |1_A 1_B 1_C\rangle\langle 1_A 1_B 1_C|)\end{aligned}\quad (57)$$

である。

この混合状態を 2 組に分割する。

BC が 1 組、 A が 1 組のときの密度演算子は

$$\begin{aligned}\hat{\rho}_1 &= \frac{1}{2} |\psi_0\rangle\langle\psi_0| + \frac{1}{2} |\psi_1\rangle\langle\psi_1| \\ &= \frac{1}{2} |0_A\rangle\langle 0_A| \otimes |0_B 0_C\rangle\langle 0_B 0_C| \\ &\quad + \frac{1}{2} |1_A\rangle\langle 1_A| \otimes |1_B 1_C\rangle\langle 1_B 1_C| \\ &= \frac{1}{2} (|0_A 0_B 0_C\rangle\langle 0_A 0_B 0_C| + |1_A 1_B 1_C\rangle\langle 1_A 1_B 1_C|)\end{aligned}\quad (58)$$

である。

AC が 1 組、 B が 1 組のときの密度演算子は

$$\begin{aligned}\hat{\rho}_2 &= \frac{1}{2} |\psi_0\rangle\langle\psi_0| + \frac{1}{2} |\psi_1\rangle\langle\psi_1| \\ &= \frac{1}{2} |0_B\rangle\langle 0_B| \otimes |0_A 0_C\rangle\langle 0_A 0_C| \\ &\quad + \frac{1}{2} |1_B\rangle\langle 1_B| \otimes |1_A 1_C\rangle\langle 1_A 1_C| \\ &= \frac{1}{2} (|0_A 0_B 0_C\rangle\langle 0_A 0_B 0_C| + |1_A 1_B 1_C\rangle\langle 1_A 1_B 1_C|)\end{aligned}\quad (59)$$

である。

AB は 1 組、 C は 1 組のときの密度演算子は

$$\begin{aligned}\hat{\rho}_3 &= \frac{1}{2} |\psi_0\rangle\langle\psi_0| + \frac{1}{2} |\psi_1\rangle\langle\psi_1| \\ &= \frac{1}{2} |0_C\rangle\langle 0_C| \otimes |0_A 0_B\rangle\langle 0_A 0_B| \\ &\quad + \frac{1}{2} |1_C\rangle\langle 1_C| \otimes |1_A 1_B\rangle\langle 1_A 1_B| \\ &= \frac{1}{2} (|0_A 0_B 0_C\rangle\langle 0_A 0_B 0_C| + |1_A 1_B 1_C\rangle\langle 1_A 1_B 1_C|)\end{aligned}\quad (60)$$

である。

3 種類の分類方法から得た密度演算子が元の混合状態の密度演算子と同じであることが分かった。

この密度演算子に対して、基底 (55) を使って得た密度行列は

$$\begin{aligned}\rho &= \sum_{i=0}^1 \omega_i \langle\psi_i|\hat{\rho}|\psi_i\rangle \\ &= \frac{1}{2} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}\end{aligned}\quad (61)$$

になる。

状態 $|\psi_0\rangle' = |0_A 0_B 0_C\rangle$ が 1/2 の割合で、状態 $|\psi_1\rangle' = |1_A 1_B 1_C\rangle$ が 1/2 の割合で混ざった混合状態の密度演算子は

$$\begin{aligned}\hat{\rho}' &= \sum_{i=0}^1 \omega_i |\psi_i\rangle'\langle\psi_i'| \\ &= \frac{1}{2} |0_A 0_B 0_C\rangle\langle 0_A 0_B 0_C| + \frac{1}{2} |1_A 1_B 1_C\rangle\langle 1_A 1_B 1_C|\end{aligned}\quad (62)$$

である。

基底 (55) を使って得た密度行列は

$$\begin{aligned}\rho' &= \sum_{i=0}^1 \omega_i \langle\psi_i'|\hat{\rho}'|\psi_i'\rangle \\ &= \frac{1}{2} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}\end{aligned}\quad (63)$$

である。(57)、(61)、(62)、(63) から見ると、エンタングルメントを含む $|\psi_0\rangle$ 状態と $|\psi_1\rangle$ 状態が 50% の割合で混ざった混合状態は、50% の $|\psi_0\rangle'$ 積状態と 50% の $|\psi_1\rangle'$ 積状態の混合状態の密度演算子と密度行列が同じである。その結果、 $TSS(A, BC)$ 、 $TSS(B, AC)$ 、 $TSS(C, AB)$ が成立する。つまり、あらゆる TSS が成立することである。よって、「あらゆる TSS が成立する混合状態にはエンタングルメント状態が含まれる可能性がある」ことを証明した。

3. \overline{TSS} が成立する純粋状態はエンタングルメント状態であるための必要十分条件

まず、十分条件が成り立つことを証明する。

\overline{TSS} が存在する純粋状態はエンタングルメント状態である。

証明： \overline{TSS} の定義から、分割した k 組のサブシステムが互いに分離できない場合、それは何らかのエンタングルメントが存在することである。従って、その純粋状態はエンタングルメント状態である。十分条件が成り立つ。

つぎに、必要条件が成立することを証明する。

エンタングルメント状態なら、少なくとも 1 種類の \overline{TSS} が成立する。

証明： \overline{TSS} が成立しないと仮定すると、あらゆる TSS が成立する。(判定結果 1) から、あらゆる TSS が成立する純粋状態は分離可能な状態である。従って、仮定は成立しない、 \overline{TSS} が成立し、必要条件が成り立つ。

4. \overline{TSS} が成立する混合状態は、エンタングルメント状態を含むための十分条件

まず、十分条件が成り立つことを証明する。

\overline{TSS} が存在する混合状態にはエンタングルメント状態が含まれる。

証明：多粒子系を分割した k 組サブシステムが分離不可能な場合、それはなんらかのエンタングルメントが存在することになり、 \overline{TSS} と表記する。この \overline{TSS} の定義から、 \overline{TSS} が成立する混合状態にはエンタングルメント状態が含まれる。十分条件を証明した。

必要条件が成立しないことを証明する。

エンタングルメント状態からなる混合状態には、すべての TSS が成り立つこともある。

この証明は 13 ページの「(判定結果 2) の十分条件が成立しない」の証明と同じであり、ここでは省略する。

5. あらゆる PSS が成立する純粋状態は分離可能な状態であるための必要十分条件

まず、十分条件が成り立つことを証明する。

量子ビット A, B, C, D を含む 4 粒子系の純粋状態 $|\psi_{ABCD}\rangle$ には、すべての PSS が成立し、その状態は分離可能な状態である。

証明：すべての PSS が成立するから、 $PSS_D(A, B, C)$ が成り立つ。従って、

$$PSS_D(A, B, C) : |\psi_A\rangle \otimes |\psi_B\rangle \otimes |\psi_C\rangle \quad (64)$$

が成り立つ。量子ビット A と D が分離できないと仮定すると、 A と D がエンタングルする。従って、 $\overline{PSS}_B(A, C, D)$, $\overline{PSS}_C(A, B, D)$ が成り立つ。

しかし、あらゆる PSS が成立するから、 $PSS_B(A, C, D)$, $PSS_C(A, B, D)$ が成立する。従って、仮定が成立しない、量子ビット A と D は分離可能である。その結果、量子ビット A, B, C, D が分離可能である。 $|\psi_{ABCD}\rangle = |\psi_A\rangle \otimes |\psi_B\rangle \otimes |\psi_C\rangle \otimes |\psi_D\rangle$ が成り立つ。つまり、その純粋状態は分離可能な状態である、十分条件が成り立つことを証明できた。

つぎに、必要条件が成立することを証明する。

ある 3 粒子系の純粋状態 $|\psi_{ABC}\rangle$ は分離可能な状態、その状態のすべての PSS が成立する。

証明： $|\psi_{ABC}\rangle$ は分離可能な状態であるから、 $|\psi\rangle = |\psi_A\rangle \otimes |\psi_B\rangle \otimes |\psi_C\rangle$ が成立する。従って、 $|\psi_A\rangle \otimes |\psi_B\rangle$ 、 $|\psi_B\rangle \otimes |\psi_C\rangle$ 、 $|\psi_A\rangle \otimes |\psi_C\rangle$ が成り立つ。その結果 $PSS_C(A, B)$, $PSS_A(B, C)$, $PSS_B(A, C)$ が成り立つ。 $PSS_C(A, B)$, $PSS_A(B, C)$, $PSS_B(A, C)$ は 3 粒子系のすべての PSS の分類である。つまり、必要条件が成り立つ。

6. あらゆる PSS が成立する混合状態は分離可能な状態であるための必要条件

まず、必要条件が成り立つことを証明する。

分離可能な混合状態なら、あらゆる PSS が成り立つ。

証明：すべての PSS が成立しないと仮定すると、少なくとも 1 種類の \overline{PSS} が成立する。 \overline{PSS} の定義からそれは何らかのエンタングルメントを含むことになる。その意味は、その混合状態はエンタングルメント状態が含まれる。しかし、その混合

状態は分離できる状態。その結果、仮定は成立しない。つまり、あらゆる PSS が成立し、必要条件が成り立つ。

つぎに、十分条件が成立しないことを証明する。

あらゆる PSS が成立する混合状態にはエンタングルメントが含まれる可能性がある。

$|\psi_0\rangle$ 状態が $1/2$ の割合で、 $|\psi_1\rangle$ 状態が $1/2$ の割合で混ざった状態は

$$\begin{aligned} |\psi_0\rangle &= |0_A\rangle \otimes |\psi_{BC}^+\rangle \\ |\psi_{BC}^+\rangle &= \frac{1}{\sqrt{2}}(|0_B1_C\rangle + |1_B0_C\rangle) \\ |\psi_1\rangle &= |1_A\rangle \otimes |\psi_{BC}^-\rangle \\ |\psi_{BC}^-\rangle &= \frac{1}{\sqrt{2}}(|0_B1_C\rangle - |1_B0_C\rangle) \end{aligned} \quad (65)$$

のような状態である。

密度演算子が

$$\begin{aligned} \rho &= \frac{1}{2}[(|0_A\rangle\langle 0_A|) \otimes (|\psi_{BC}^+\rangle\langle \psi_{BC}^+|) + \\ &(|1_A\rangle\langle 1_A|) \otimes (|\psi_{BC}^-\rangle\langle \psi_{BC}^-|)] \\ &= \frac{1}{4} \{ |0_A\rangle\langle 0_A| \otimes (|0_B1_C\rangle\langle 0_B1_C| + |0_B1_C\rangle\langle 1_B0_C| \\ &+ |1_B0_C\rangle\langle 0_B1_C| + |1_B0_C\rangle\langle 1_B0_C|) \} \\ &+ \frac{1}{4} \{ |1_A\rangle\langle 1_A| \otimes (|0_B1_C\rangle\langle 0_B1_C| - |0_B1_C\rangle\langle 1_B0_C| \\ &- |1_B0_C\rangle\langle 0_B1_C| + |1_B0_C\rangle\langle 1_B0_C|) \} \\ &= \frac{1}{4} \{ |0_A0_B1_C\rangle\langle 0_A0_B1_C| + |0_A0_B1_C\rangle\langle 0_A1_B0_C| \\ &+ |0_A1_B0_C\rangle\langle 0_A0_B1_C| + |0_A1_B0_C\rangle\langle 0_A1_B0_C| \} \\ &+ \frac{1}{4} \{ |1_A0_B1_C\rangle\langle 1_A0_B1_C| - |1_A0_B1_C\rangle\langle 1_A1_B0_C| \\ &- |1_A1_B0_C\rangle\langle 1_A0_B1_C| + |1_A1_B0_C\rangle\langle 1_A1_B0_C| \} \end{aligned} \quad (66)$$

になる。基底 (55)(13 ページ) を用いると、密度行列は

$$\rho = \frac{1}{4} \left(\begin{array}{cccc|cccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array} \right) \quad (67)$$

となる。

粒子 A を除けて、残った粒子 B, C は $\frac{1}{2}|\psi_{BC}^+\rangle$, $\frac{1}{2}|\psi_{BC}^-\rangle$ の混合状態で存在する。 $\frac{1}{2}|\psi_{BC}^+\rangle$, $\frac{1}{2}|\psi_{BC}^-\rangle$ の混合状態の密度演算子が

$$\begin{aligned} \rho_{BC} &= \frac{1}{2}|\psi_{BC}^+\rangle\langle \psi_{BC}^+| + \frac{1}{2}|\psi_{BC}^-\rangle\langle \psi_{BC}^-| \\ &= \frac{1}{2} \left\{ \frac{1}{\sqrt{2}}(|0_B1_C\rangle + |1_B0_C\rangle) \right. \\ &\quad \left. \frac{1}{\sqrt{2}}(\langle 0_B1_C| + \langle 1_B0_C|) \right\} \\ &+ \frac{1}{2} \left\{ \frac{1}{\sqrt{2}}(|0_B1_C\rangle - |1_B0_C\rangle) \right. \\ &\quad \left. \frac{1}{\sqrt{2}}(\langle 0_B1_C| - \langle 1_B0_C|) \right\} \\ &= \frac{1}{2}|0_B1_C\rangle\langle 0_B1_C| + \frac{1}{2}|1_B0_C\rangle\langle 1_B0_C| \end{aligned} \quad (68)$$

になる。 $\frac{1}{2}|0_B1_C\rangle$, $\frac{1}{2}|1_B0_C\rangle$ の積状態の混合状態の密度演算子は

$$\rho'_{BC} = \frac{1}{2}|0_B1_C\rangle\langle 0_B1_C| + \frac{1}{2}|1_B0_C\rangle\langle 1_B0_C| \quad (69)$$

である。密度演算子 $\hat{\rho}_{BC}$, $\hat{\rho}'_{BC}$ は同じである。基底 (55)(13 ページ) を使って得た密度行列も同じである。

$$\rho_{AB} = \rho'_{AB} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & \frac{1}{2} & 0 & 0 \\ 0 & 0 & \frac{1}{2} & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad (70)$$

従って、 $PSS_A(B, C)$ が成立する。粒子 A と C は分離可能である、粒子 B をのけた場合も分離できる、 $PSS_B(A, C)$ が成立する。粒子 A と B は分離可能である、粒子 C をのけた場合も分離できる、 $PSS_C(A, B)$ が成立する。その結果、あらゆる PSS が成立する。

しかし、実際に、この混合状態には、エンタングルメント状態が含まれる。今から $\overline{TSS}(AB, C)$ が成立することを証明する。 $\overline{TSS}(AB, C)$ が成立するなら、この状態にはエンタングル状態が含まれることを証明できる。粒子 A, B が 1 組のサブシステム、粒子 C が 1 組のサブシステムにして、得た密

度演算子 $\hat{\rho}'$ は

$$\begin{aligned}
\hat{\rho}' &= \frac{1}{2}|\psi_0\rangle\langle\psi_0| + \frac{1}{2}|\psi_1\rangle\langle\psi_1| \\
&= \frac{1}{2} \left\{ \frac{1}{\sqrt{2}}(|0_A0_B1_C\rangle + |0_A1_B0_C\rangle) \right. \\
&\quad \left. \frac{1}{\sqrt{2}}(\langle 0_A0_B1_C| + \langle 0_A1_B0_C|) \right\} \\
&\quad \frac{1}{2} \left\{ \frac{1}{\sqrt{2}}(|1_A0_B1_C\rangle - |1_A1_B0_C\rangle) \right. \\
&\quad \left. \frac{1}{\sqrt{2}}(\langle 1_A0_B1_C| - \langle 1_A1_B0_C|) \right\} \\
&= \frac{1}{4} \{ (|0_A0_B\rangle \otimes |1_C\rangle + |0_A1_B\rangle \otimes |0_C\rangle) \\
&\quad (\langle 0_A0_B| \otimes \langle 1_C| + \langle 0_A1_B| \otimes \langle 0_C|) \} \\
&\quad \frac{1}{4} \{ (|1_A0_B\rangle \otimes |1_C\rangle - |1_A1_B\rangle \otimes |0_C\rangle) \\
&\quad (\langle 1_A0_B| \otimes \langle 1_C| - \langle 1_A1_B| \otimes \langle 0_C|) \} \\
&= \frac{1}{4} (|0_A0_B\rangle\langle 0_A0_B| \otimes |1_C\rangle\langle 1_C| \\
&\quad + |0_A0_B\rangle\langle 0_A1_B| \otimes |1_C\rangle\langle 0_C| \\
&\quad + |0_A1_B\rangle\langle 0_A0_B| \otimes |0_C\rangle\langle 0_C| \\
&\quad + |0_A1_B\rangle\langle 0_A1_B| \otimes |0_C\rangle\langle 0_C| \\
&\quad + |1_A0_B\rangle\langle 1_A0_B| \otimes |1_C\rangle\langle 1_C| \\
&\quad + |1_A0_B\rangle\langle 1_A1_B| \otimes |1_C\rangle\langle 0_C| \\
&\quad + |1_A1_B\rangle\langle 1_A0_B| \otimes |0_C\rangle\langle 0_C| \\
&\quad + |1_A1_B\rangle\langle 1_A1_B| \otimes |0_C\rangle\langle 0_C|) \quad (71)
\end{aligned}$$

である。基底 (55)(13 ページ) を使って、得た密度行列は

$$\rho = \frac{1}{4} \left(\begin{array}{cccc|cccc}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & -1 & 0 \\
\hline
0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & -1 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{array} \right) \quad (72)$$

である。従って、粒子 C は粒子 AB とエンタングルする。その結果、 $\overline{TSS}(AB, C)$ が成立する。つまり、十分条件が成立しないことを証明した。

7. \overline{PSS} が成立する純粋状態はエンタングルド状態であるための必要十分条件

まず、必要条件を証明する。

ある純粋状態はエンタングルメント状態なら、必ず \overline{PSS} が成立する。

証明： \overline{PSS} が成立しないと仮定すると、あらゆる PSS が成立する。(判定結果 5) から、「あらゆる PSS が成立する純粋状態は分離可能な状態である」ことを分かった。しかし、この純粋状態はエンタングルメント状態である。従って、仮定は成立しない、 \overline{PSS} が成立する。その結果、必要条件が成立する。

つぎに、十分条件が成り立つことを証明する。

\overline{PSS} が存在する純粋状態はエンタングルメント状態である。

証明： \overline{PSS} の定義から、 \overline{PSS} が成立することは、その状態がエンタングルメント状態である。従って、十分条件が成立する。

8. \overline{PSS} が成立する混合状態はエンタングルド状態が含まれるための十分条件

まず、十分条件が成り立つことを証明する。

\overline{PSS} が成立する混合状態にはエンタングルメント状態が存在する。

証明： \overline{PSS} の定義から、エンタングルメント状態が存在する場合、 \overline{PSS} と表記する。従って、十分条件が成り立つ。

つぎに、必要条件が成立しないことを証明する。

エンタングルメント状態が含まれる混合状態には、すべての PSS が成立する可能性がある。

この命題の証明は 16 ページの結果 6 の十分条件が成立しないことを証明する過程が同じである。

9. ある純粋状態において、1 個の粒子と他のすべての粒子が個別にエンタングルしているような特定の \overline{PSS} が成立するなら、この純粋状態は全粒子がエンタングルしている状態である。

A, B, C 粒子を含む 3 粒子系のある純粋状態はこのような状態である。 $\overline{PSS}_C(A, B)$ が成り立ち、粒子 A と B がエンタングルし、エンタングルメント関係は $|0_A0_B\rangle + |1_A1_B\rangle$ である。 $\overline{PSS}_B(A, C)$ が成り立ち、粒子 A と C がエンタングルし、エンタングルメント関係は $|0_A1_C\rangle + |1_A0_C\rangle$ である。

この純粋状態の全粒子がエンタングルする。

証明：粒子 A, B はエンタングルするから、測定するとき、粒子 A の状態が決めるとき、同時に粒子 B の状態が決めることができる。同様に、粒子 B の状態が決めるとき、同時に粒子 A の状態が決めることができる。同じように、粒子 A, C はエンタングルするから、粒子 A の状態が決めるとき、同時に粒子 C の状態が決めることができる。粒子 C の状態が決めるとき、同時に粒子 A の状態も決めることができる。そして、以下の分析ができる。

$$\begin{aligned} |A\rangle = |0_A\rangle \text{ の場合: } & |B\rangle = |0_B\rangle, |C\rangle = |1_C\rangle \\ |A\rangle = |1_A\rangle \text{ の場合: } & |B\rangle = |1_B\rangle, |C\rangle = |0_C\rangle \\ |B\rangle = |0_B\rangle \text{ の場合: } & |A\rangle = |0_A\rangle, |C\rangle = |1_C\rangle \\ |B\rangle = |1_B\rangle \text{ の場合: } & |A\rangle = |1_A\rangle, |C\rangle = |0_C\rangle \\ |C\rangle = |0_C\rangle \text{ の場合: } & |A\rangle = |1_A\rangle, |B\rangle = |1_B\rangle \\ |C\rangle = |1_C\rangle \text{ の場合: } & |A\rangle = |0_A\rangle, |B\rangle = |0_B\rangle \end{aligned}$$

その結果、粒子 B, C のエンタングルメント関係は $|0_B1_C\rangle + |1_B0_C\rangle$ である。粒子 A, B, C のエンタングルメント関係は $|0_A0_B1_C\rangle + |1_A1_B0_C\rangle$ である。この純粋状態は全粒子がエンタングルする。

10. ある 3 粒子系の純粋状態は、異なる 2 種類 TSS が成立するなら分離可能な状態である；エンタングルした 3 粒子系の純粋状態においては、多くとも 1 種類の TSS しか成立しない。

まず、結果の前半部分を証明する。

例えば A, B, C 粒子を含む 3 粒子系の純粋状態 $|\psi_{ABC}\rangle$ に、 $TSS(AB, C)$ と $TSS(A, BC)$ が成立するならば、 $|\psi_{ABC}\rangle$ は分離可能な状態である。

証明： $TSS(AB, C)$ が成立するから

$$|\psi_{ABC}\rangle = |\psi_{AB}\rangle \otimes |\psi_C\rangle \quad (73)$$

が成立する。 $|\psi_{AB}\rangle = |\psi_A\rangle \otimes |\psi_B\rangle$ が成立しないと仮定すると、 $|\psi_{AB}\rangle$ はエンタングル状態である。シュミット分解により、

$$|\psi_{AB}\rangle = \alpha|\psi_A\rangle \otimes |\psi_B\rangle + \beta|\psi_A'\rangle \otimes |\psi_B'\rangle \quad (74)$$

になる。ただし、 $\alpha \geq 0, \beta \geq 0, \alpha^2 + \beta^2 = 1, \{|\psi_A\rangle, |\psi_A'\rangle\}$ は量子ビット A の直交基底、

$\{|\psi_B\rangle, |\psi_B'\rangle\}$ は量子ビット B の直交基底である。そして、

$$\begin{aligned} |\psi_{ABC}\rangle &= \alpha(|\psi_A\rangle \otimes |\psi_B\rangle) \otimes |\psi_C\rangle \\ &\quad + \beta(|\psi_A'\rangle \otimes |\psi_B'\rangle) \otimes |\psi_C\rangle \\ &= \alpha|\psi_A\rangle \otimes (|\psi_B\rangle \otimes |\psi_C\rangle) \\ &\quad + \beta|\psi_A'\rangle \otimes (|\psi_B'\rangle \otimes |\psi_C\rangle) \end{aligned} \quad (75)$$

が成立する。その結果、 $|\psi_A\rangle$ と $|\psi_{BC}\rangle$ はエンタングルする。

命題から $TSS(A, BC)$ も成立する。従って、

$$|\psi_{ABC}\rangle = |\psi_A\rangle \otimes |\psi_{BC}\rangle \quad (76)$$

が成り立つ。しかし、仮定から $|\psi_A\rangle$ と $|\psi_{BC}\rangle$ はエンタングルするのを得た。その結果、仮定が成立しない、 $|\psi_{AB}\rangle = |\psi_A\rangle \otimes |\psi_B\rangle$ が成り立つ。そして、 $|\psi_{ABC}\rangle = |\psi_A\rangle \otimes |\psi_B\rangle \otimes |\psi_C\rangle$ が成立する。つまり、異なる 2 種類 TSS が成立する 3 粒子系の純粋状態は分離可能な状態である。

結果の後の部分を証明する。

エンタングルした 3 粒子系の純粋状態においては、異なる 2 種類の TSS が成立すると仮定するならば、この判定結果の前の部分により、異なる 2 種類の TSS が成立する 3 粒子系の純粋状態が分離可能な状態と矛盾する。従って、エンタングルした 3 粒子系の純粋状態においては、多くとも 1 種類の TSS しか成立しないと証明できた。

11. ある 4 粒子系の純粋状態において、粒子 1 つと別の粒子が分離可能であり、別の 3 粒子の異なる 2 種類の TSS が成立するなら、その純粋状態は分離可能な状態である。

粒子 A, B, C, D を含む 4 粒子系のある純粋状態 $|\psi_{ABCD}\rangle$ 、粒子 A と粒子 B, C, D が分離可能であり、また、 $TSS(BC, D), TSS(BD, C)$ が成立する、その純粋状態は分離可能な状態である。

証明：粒子 A と粒子 B, C, D が分離可能であるから、 $|\psi_{ABCD}\rangle = |\psi_A\rangle \otimes |\psi_{BCD}\rangle$ が成立する。 $|\psi_{BCD}\rangle$ は分離可能な状態なら、 $|\psi_{ABCD}\rangle$ は分離可能である。(判定結果 10)「ある 3 粒子系の純粋状態は、異なる 2 種類 TSS が成立するなら分離で

きる状態である。」によって、 $|\psi_{BCD}\rangle$ は分離可能である。そして、

$$|\psi_{BCD}\rangle = |\psi_B\rangle \otimes |\psi_C\rangle \otimes |\psi_D\rangle \quad (77)$$

が成り立つ。従って、

$$|\psi_{ABCD}\rangle = |\psi_A\rangle \otimes |\psi_B\rangle \otimes |\psi_C\rangle \otimes |\psi_D\rangle \quad (78)$$

が成立する。その純粋状態は分離可能な状態であることを証明した。

5 エンタングルメントの応用

エンタングルメント状態を判定するのはそれを応用するためである。エンタングルメントは、近年、急速に発達している量子情報処理における重要な資源であり、量子計算や量子通信などに利用されている。

5.1 量子計算

因数分解に対する有名な Shor の量子アルゴリズムは、実際にエンタングルメントが利用されている量子計算の例である。

因数分解すべき数 n とその関数に周期性があることが Shor のアルゴリズムの基礎原理である [3]。まず関数 $f_n(a) = x^a \pmod n$ を計算する。ただし、 x はランダムに選ばれた n と互いに素な整数である。 n を因数分解する問題に関して、 $f_n(a)$ は周期関数であるから、新しい関数 $f_n(a)$ を構成する。 x の異なる値は、異なる関数 $f_n(a)$ を得る。 x の特定の値に対する繰り返し数は、「 n を法とする x の周期」と呼ばれ、通常 r で表される。

$$x^r \equiv 1 \pmod n \quad (79)$$

が成り立つ。もし周期 r が偶数ならば、この方程式を、以下のように 2 つの平方数の差の形に書き直せる。

$$\begin{aligned} (x^{r/2})^2 &\equiv 1 \pmod n \\ (x^{r/2})^2 - 1 &\equiv 0 \pmod n \\ (x^{r/2})^2 - 1^2 &\equiv 0 \pmod n \\ (x^{r/2} - 1)(x^{r/2} + 1) &\equiv 0 \pmod n \end{aligned} \quad (80)$$

最後の式から、積 $(x^{r/2} - 1)(x^{r/2} + 1)$ が n の倍数であることが分かった。即ち、 $(x^{r/2} - 1)(x^{r/2} + 1)$ を

n で割ると、余りは 0 となる。従って、 $\gcd(x^{r/2} - 1, n), \gcd(x^{r/2} + 1, n)$ を計算することにより、 n の因数を高い確率で見つけることができる。

Shor の因数分解アルゴリズムのポイントは、関数 $f_{x,n}(a) = x^a \pmod n$ の周期 r を計算するために重ね合わせ状態を利用することである。重ね合わせ状態を利用すれば、計算速度が古典コンピュータより指数倍速くなる。

一般的には Shor のアルゴリズムは次のようにまとめられる [1,3]。

初めに、 $2^n \leq q \leq 3^n$ を満たす、(小さな素因数を持つ) 数 q を選ぶ。 n と互いに素な整数 x をランダムに選ぶ。レジスタ 1、レジスタ 2 を準備し、 $|\text{reg}_1\rangle|\text{reg}_2\rangle$ とする。毎回、同じランダム数 x を用いて、(1) から (7) のステップを、オーダ $\log(q)$ 回繰り返す。

(1) : レジスタ 1 とレジスタ 2 の状態を $|\psi_i\rangle = |0\rangle|0\rangle$ 用意する。

(2) : レジスタ 1 に q 回アダマード変換を行う。レジスタ 1 の量子状態は重ね合わせ状態になる。

$$\begin{aligned} |\psi_{\text{reg1}}\rangle &= H^{\otimes q}|0\rangle \\ &= H \otimes \cdots \otimes H | \underbrace{00 \dots 0}_q \rangle \\ &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \cdots \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ &= \frac{1}{\sqrt{2^q}}(|00 \dots 0\rangle + \cdots + |11 \dots 1\rangle) \\ &= \frac{1}{\sqrt{2^q}} \sum_{x=0}^{2^q-1} |x\rangle \end{aligned} \quad (81)$$

そして、レジスタ 1 と 2 の全体の状態は

$$|\psi\rangle = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle|0\rangle = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a, 0\rangle \quad (82)$$

である。レジスタ 1 は量子ビットの重ね合わせ状態である。

(3) : レジスタ 1 の重ね合わせ状態に、(量子並列化を用いて) 変換 $x^a \pmod n$ を適用し、その結果をレジスタ 2 に貯える。このとき、レジスタ 1 と 2 がエンタングルメント状態になっている。レジスタ全体の状態は

$$|\psi\rangle = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a, x^a \pmod n\rangle \quad (83)$$

である。

(4) : レジスタ 2 の状態を測定し、状態 $|k\rangle$ を得た。レジスタ 1 と 2 がエンタングルするから、レジスタ 2 の状態 $|k\rangle$ を得たとき、レジスタ 1 の状態は $x^a \bmod n = k$ を満たす値 a のみの重ね合わせ状態になる。従って、レジスタ全体の状態は

$$|\psi\rangle = \frac{1}{\sqrt{|A|}} \sum_{a' \in A} |a', k\rangle \quad (84)$$

になる。ただし、 $|A|$ を集合 A の要素数とすると、 $A = \{a' : x^{a'} \bmod n = k\}$ である。

(5) : 次に、レジスタ 1 の状態の量子フーリエ変換を計算する。量子フーリエ変換は、各状態 $|a'\rangle$ を以下の重ね合わせ状態に写像する。

$$|a'\rangle = \frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} \exp(2\pi i a' c / q) |c\rangle \quad (85)$$

従って、量子フーリエ変換の全体としての効果は

$$|\psi\rangle = \frac{1}{\sqrt{|A|}} \sum_{a' \in A} \frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} \exp(2\pi i a' c / q) |c, k\rangle \quad (86)$$

である。

(6) : レジスタ 1 の状態を測定する。測定の結果、ある数 c' が得られるが、これは q/r の λ 倍の数である。ただし、 r は所望の周期とする。即ち、ある正整数 λ に対して、 $c'/q \approx \lambda/r$ が成り立っている。

(7) : 周期 r を決定するためには、 λ を評価する必要がある。これは、分母が n より小さい間、 c'/q の連分数展開を計算することにより行える。その結果、 λ/r に最も近い分数が得られる。

ステップ (1) から (7) を繰り返して、レジスタ 1 における量子フーリエ変換のサンプルの集合を生成する。この結果、種々の整数 λ_i に対して、 $1/r$ の倍数のサンプル $\lambda_1/r, \lambda_2/r, \lambda_3/r, \dots$ が得られる。アルゴリズムを数回繰り返せば、連分数展開法を用いて λ_i を、つまりは r を計算するのに十分な、レジスタ 1 のサンプルが得られる。 r が分かれば、 n の因数は、 $\gcd(x^{r/2} - 1, n)$ および、 $\gcd(x^{r/2} + 1, n)$ の関係から得られる。

5.2 量子通信

1 量子ビットをテレポートするのはエンタングルメントを利用した簡単な量子通信の 1 つの例であ

る。量子テレポーテーションでは、未知の量子ビットの状態を表される量子情報

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (87)$$

(ただし、 $|\alpha|^2 + |\beta|^2 = 1$ となるように規格化) を A から B へ送信する。未知量子ビットの量子情報を通信するという意味は、図 5.1 のように、入力量子ビット $|\phi\rangle$ の状態を「入力ポート量子ビット」A とは離れた場所 B にある「出力ポート量子ビット」B の状態に再現するという意味である。量子ビットそのものを送るわけではなく、その未知の量子情報のみをエンタングルメントからなる「量子通信経路」を通じて送ることになる。未知の量子状態を未知のまま送信する。

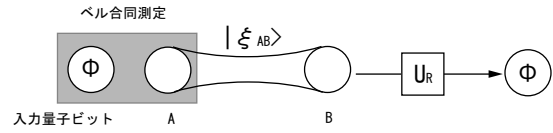


図 5.1 量子テレポーテーションの概念図

量子テレポーテーションで用いるエンタングルメントは 2 量子ビットの最大エンタングルメント状態

$$|\xi_{AB}\rangle = |\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0_A 0_B\rangle + |1_A 1_B\rangle) \quad (88)$$

である。この最大エンタングルメント状態 $|\xi_{AB}\rangle$ が量子情報を A から B へ送るための「量子通信経路」となる。 $|\xi_{AB}\rangle$ を構成する 2 つの量子ビットのうち、一方が量子情報の入力ポートとなる「入力ポート量子ビット」、もう一方が出力ポートとなる「出力ポート量子ビット」となる。

後で使う 2 量子ビット間の最大エンタングルメント状態であり、ベル状態 (bell states) とも呼ばれ、次のように定義される。

$$\begin{aligned} |\Phi^+\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ |\Phi^-\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\ |\Psi^+\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\ |\Psi^-\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \end{aligned} \quad (89)$$

量子テレポーテーションの手順は次の通りである [3,4]。

(1) 場所 A において送信者は、送りたい未知状態の量子ビット (入力量子ビット) と量子通信経路の入力ポート量子ビットをベル合同測定する。ベル合同測定とは、2つの量子ビットをベル状態からなる基底 $|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle$ で測定することである。入力ビット、入力ポートビットと出力ポートビットを合わせた 3 量子ビットの状態は

$$\begin{aligned} |\phi\rangle \otimes |\xi_{AB}\rangle &= (\alpha|0\rangle + \beta|1\rangle) \\ &\otimes \frac{1}{\sqrt{2}}(|0_A0_B\rangle + |1_A1_B\rangle) \\ &= \frac{\alpha}{\sqrt{2}}(|0\rangle|0_A\rangle|0_B\rangle + |0\rangle|1_A\rangle|1_B\rangle) \\ &\quad + \frac{\beta}{\sqrt{2}}(|1\rangle|0_A\rangle|0_B\rangle + |1\rangle|1_A\rangle|1_B\rangle) \end{aligned} \quad (90)$$

入力量子ビットと入力ポート量子ビットはエンタングルメントのない積状態にある。ベル合同測定を行うと

$$\begin{aligned} |\phi\rangle \otimes |\xi_{AB}\rangle &= \frac{1}{2\sqrt{2}}(|00_A\rangle + |11_A\rangle)(\alpha|0_B\rangle + \beta|1_B\rangle) \\ &\quad + \frac{1}{2\sqrt{2}}(|00_A\rangle - |11_A\rangle)(\alpha|0_B\rangle - \beta|1_B\rangle) \\ &\quad + \frac{1}{2\sqrt{2}}(|01_A\rangle + |10_A\rangle)(\alpha|1_B\rangle + \beta|0_B\rangle) \\ &\quad + \frac{1}{2\sqrt{2}}(|01_A\rangle - |10_A\rangle)(\alpha|1_B\rangle - \beta|0_B\rangle) \\ &= \frac{1}{2}|\Phi^+\rangle(\alpha|0_B\rangle + \beta|1_B\rangle) \\ &\quad + \frac{1}{2}|\Phi^-\rangle(\alpha|0_B\rangle - \beta|1_B\rangle) \\ &\quad + \frac{1}{2}|\Psi^+\rangle(\alpha|1_B\rangle + \beta|0_B\rangle) \\ &\quad + \frac{1}{2}|\Psi^-\rangle(\alpha|1_B\rangle - \beta|0_B\rangle) \end{aligned} \quad (91)$$

入力ビットと入力ポートビットは 4 つのベル状態の中の任意の一つ状態になり、出力ポートビットの状態は対応する状態の 1 つに変化する。

$$\begin{aligned} |\Phi^+\rangle &\leftrightarrow \alpha|0\rangle + \beta|1\rangle, \quad |\Phi^-\rangle \leftrightarrow \alpha|0\rangle - \beta|1\rangle \\ |\Psi^+\rangle &\leftrightarrow \alpha|1\rangle + \beta|0\rangle, \quad |\Psi^-\rangle \leftrightarrow \alpha|1\rangle - \beta|0\rangle \end{aligned} \quad (92)$$

ただし、この段階で受信者は出力ポートビットが 4 つの状態のうちどの状態へ変化したかを知るこ

とはできず、未知量子ビットの情報は伝わっていない。

(2) 送信者は入力ビットと入力ポートビットの状態を測定する。測定の結果は 4 つのベル状態の中の任意の一つになる。それぞれに対して、同時に、出力ポート B の状態も決まる。送信者が測定の結果を、古典的な通信手段、例えば電話で、受信者に通告する。

(3) 受信者は送られた古典の情報によって、出力ポート量子ビットがどの状態へ変化したかを知るため、状態 $|\phi\rangle$ へ戻すために出力ポートビットに「復元操作」を加える。この復元操作とは、送信者の測定結果に対応して出力ポートビットにパウリ演算 $\{\hat{I}, \hat{\sigma}_z, \hat{\sigma}_x, \hat{\sigma}_z \cdot \hat{\sigma}_x\}$ を施すことである。パウリ演算を行列表示で表すと次のようになる。

$$\hat{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \hat{\sigma}_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \hat{\sigma}_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad (93)$$

例えば、受信者は送信者から入力ビットと入力ポートビットの状態が $|\Psi^+\rangle$ と分かたら、パウリ演算子 $\hat{\sigma}_x$ を使って出力ポート B に演算する。

$$\begin{aligned} \hat{\sigma}_x(\alpha|1_B\rangle + \beta|0_B\rangle) &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \beta \\ \alpha \end{pmatrix} \\ &= \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha|0_B\rangle + \beta|1_B\rangle \end{aligned} \quad (94)$$

復元演算の結果、受信者の出力ポートビット B の状態は、 $|\phi_B\rangle = \alpha|0\rangle + \beta|1\rangle$ に変化する。これは、場所 A にいる送信者が送ろうとした入力量子ビットの状態 $|\phi\rangle$ と同じ状態である。量子テレポーテーションの手順によって、送信者の場所 A からはこの量子状態で表される量子情報は消えて、場所 B に同じ状態が再現され、量子テレポーテーションが達成されたことになる。

まとめ

多粒子系において、エンタングルメント状態を判定することはとても困難である。本論文では「完全に準分離可能なサブシステム」と「部分的に準分離可能なサブシステム」という 2 つの判定基準を使い、多粒子系の状態が分離可能かどうかで、分離可能な状態かエンタングルメント

状態に分類した。しかし、エンタングルメント状態には、いろいろな種類がある。例えば、量子ビット A と B を含む 2 粒子系において、 $|\psi_1\rangle = (|0_A\rangle + |1_A\rangle) \otimes (|0_B\rangle + |1_B\rangle)$ のような状態にはエンタングルメントが存在せず、分離可能な状態である。これに対し、 $|\psi_2\rangle = \frac{1}{\sqrt{2}}(|0_A0_B\rangle + |1_A1_B\rangle)$ のような状態は完全なエンタングルメント状態である。 $|\psi_3\rangle = \alpha|0_A0_B\rangle + \beta|1_A1_B\rangle$ ただし、 $|\alpha|^2 + |\beta|^2 = 1$ かつ $\alpha \neq \beta$ のような状態は、エンタングルメント状態であるが、完全なエンタングルメント状態ではない。 $|\psi_4\rangle = \frac{1}{\sqrt{3}}(|0_A0_B\rangle + |1_A0_B\rangle + |1_A1_B\rangle)$ のような状態もエンタングルメント状態であるが、完全なエンタングルメントではない。

これまでの研究において、 $|\psi_1\rangle$ や $|\psi_2\rangle$ のような状態はすでに分類されている。しかし、 $|\psi_3\rangle$ や $|\psi_4\rangle$ のようなエンタングルメント状態は定量的な分類が十分されていない。また、 n 粒子系 ($n > 2$) エンタングルメントの分類はもっと複雑になる。 n 粒子系に対するエンタングルメントの分類が必要だと考えられる。

参考文献

- [1] 佐川弘幸・吉田宣章 「量子情報理論」 シュプリンガー・フェアラーク東京
- [2] 清水明 「新版 量子論の基礎」 サイエンス社
- [3] C.P. ウィリアムズ・S.H. クリアウォーター 「量子コンピューティング」 シュプリンガー・フェアラーク東京
- [4] 細谷暁夫 「量子コンピュータの基礎」 サイエンス社
- [5] Gilles Brassard and Tal Mor, “Multi-particle Entanglement via Two-Particle Entanglement”, C.P. Williams (Ed.): QCQC'98, LNCS (Lecture Notes in Computer Science) **1509**, pp.1-9 (1999)
- [6] Ayman F. Abouraddy, Bahaa E. A. Saleh, “Degree of entanglement for two qubits”, Physical review A, volume 64, 050101(R)