エンタングルメント

量子情報班（文責：山本 航輝）

1 エンタングルメント

エンタングルメントとは古典では説明することのできない、量子系の相関のことです。系 A の状態 $|\psi\rangle_A$ と系 B の状態 $|\phi\rangle_B$ があったとき、これら二つの系を一つの系とみなした全体系 AB は次のように表されます（積状態）:

$$|\psi\rangle_A \otimes |\phi\rangle_B \equiv |\psi\rangle_A |\phi\rangle_B \tag{1}$$

一般に状態 $|\cdot\rangle$ は離散的であったり連続的であったりして、またその準位の数もさまざまですが、量子情報では古典コンピュータの 0 と 1 のように 2 準位系を考えることが多いです。古典の 0,1 に対応する状態は $|0\rangle, |1\rangle$ で表され、量子ビット（qubit）と呼ばれます。これら量子ビットを用いて、量子力学の重ね合わせの原理により全体系 AB には次のような状態があり得ます：

$$\begin{aligned} |EPR\rangle &= \frac{1}{\sqrt{2}}|0\rangle_A |0\rangle_B + \frac{1}{\sqrt{2}}|1\rangle_A |1\rangle_B && (2)\\ &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) && (3) \end{aligned}$$

ここで $|0\rangle_A |0\rangle_B$ を簡単に $|00\rangle$ と表す記法を用いました。実はこの $|EPR\rangle$ [1] は積状態では記述することができません。このように積状態で記述不可能な状態をエンタングル状態と呼びます。

$|EPR\rangle$ が積状態で記述することができないことの証明

$|EPR\rangle$ が積状態で記述できると仮定して、$|\psi\rangle_A = a|0\rangle + b|1\rangle, |\phi\rangle_B = c|0\rangle + d|1\rangle$（ただし $a, b, c, d \in \mathbb{C}$）を仮定します。このとき

$$\begin{aligned} |EPR\rangle = |\psi\rangle_A |\phi\rangle_B &= (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle) && (4)\\ &= ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle && (5) \end{aligned}$$

したがって

$$\begin{cases} ac = \frac{1}{\sqrt{2}} \\ ad = 0 \\ bc = 0 \\ bd = \frac{1}{\sqrt{2}} \end{cases} \tag{6}$$

となります。少し考えればわかる通り、これを満たす a, b, c, d は存在しません。したがって $|EPR\rangle$ は積状態で記述することはできません。

□

エンタングル状態における部分系 A,B は相関を持っています。この $|EPR\rangle$ を例に考えてみましょう。部分系 A を測定することを考えます。部分系 A を測定した結果が 0 であったとき、全体系の状態は $|00\rangle$

[1]EPR というのは Einstein-Podolsky-Rosen の三人の頭文字である。彼らは局所実在論の立場を取り、エンタングルメントが局所性を破り、それにより相対論と量子力学は両立しないのではないかと主張した。これは EPR のパラドックスと呼ばれるものであるが、のちに述べる通りベルの不等式の検証などを通して量子力学では局所実在論が成立しないことが明らかになっている。

に収縮し、すなわち部分系 B の状態は $|0\rangle_B$ であることがわかります。また部分系 A を測定した結果が 1 であったとき、全体系の状態は $|11\rangle$ に収縮し、すなわち部分系 B は $|1\rangle_B$ であることがわかります。このように部分系 A,B は相関を持っているのです。

ところでこのような相関は古典的にも考えられるのではないでしょうか。例えば A と B という 2 つの箱を用意し、この 2 つの箱には初めからそれぞれ同じ数字（0 か 1）が書かれた紙が入っているとします。ただし観測者は 0 と 1 のどちらの数が書かれた紙が入っているかは知らないものとします。このとき A の箱を開けて 0 と書かれた紙が入っていれば B にも 0 と書かれた紙が入っているはずです。また A の箱を開けて 1 と書かれた紙が入っていれば B にも 1 と書かれた紙が入っているはずです。これは先ほどのエンタングル状態で見た相関とまったく同じように見えます。

しかしエンタングル状態は古典よりも遥かに強い相関を持ちます。ここで $|0\rangle, |1\rangle$ を θ だけ回転させた直交基底 $|\alpha\rangle, |\beta\rangle$ を考えます：

$$\begin{cases} |\alpha\rangle = \cos\theta\,|0\rangle + \sin\theta\,|1\rangle \\ |\beta\rangle = -\sin\theta\,|0\rangle + \cos\theta\,|1\rangle \end{cases} \tag{7}$$

すると $|EPR\rangle$ は次のように書き換えることができます：

$$|EPR\rangle = \frac{1}{\sqrt{2}}\left(|\alpha\rangle_A |\alpha\rangle_B + |\beta\rangle_A |\beta\rangle_B\right) \tag{8}$$

したがってエンタングル状態に対する測定結果は基底の取り方に依らず一致するという強い相関があります。これは量子相関と呼ばれます。

エンタングル状態で実現される相関は、局所実在論（遠方で起こった現象の影響が直ちに伝わることはなく、また、全ての物理量は観測に依らずどの瞬間でも定まっていること）を仮定していた古典物理学における相関の上限を超えることができます。これをベルの不等式[2]の破れと言います。実際にこのような強い相関は実験的にも検証されており、量子力学の正当性がここにあります。

2 量子テレポーテーション

量子テレポーテーションを考える際によく Alice と Bob という二者を考えます。ここでもこの二人を考えましょう。二人は (2) 式で定義した $|EPR\rangle$ を持って遠く離れ離れになります。この状況の下で Alice はある 1 量子状態 $|\psi\rangle = a\,|0\rangle + b\,|1\rangle\,(a, b \in \mathbb{C})$ を古典通信のみを用いて Bob に伝えることができるでしょうか。結論を先に言ってしまうと、これは可能です。そしてこれが量子テレポーテーションです。

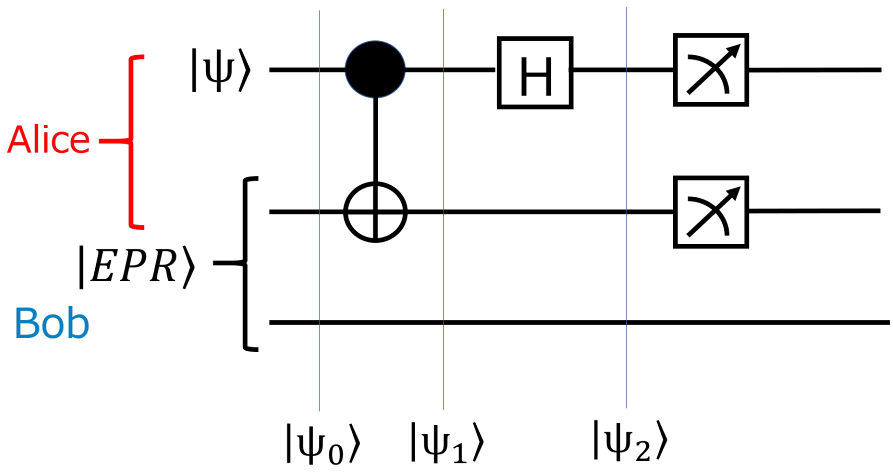

図 1: 量子テレポーテーションをする量子回路

[2]詳しくは Appendix A を参照。

ここで図 1 のような量子回路を考えましょう。●と $\bigoplus$ が線で結ばれた形をしたゲートは CNOT[3]ゲート[4]と呼ばれ、●の状態が 1 のとき $\bigoplus$ の状態を反転させます（$|0\rangle$ を $|1\rangle$ に、$|1\rangle$ を $|0\rangle$ にします）。例えば $|10\rangle$ に CNOT ゲートを作用させれば $|11\rangle$ となります。また H が四角で囲まれたゲートは Hadmard（アダマール）ゲートと呼ばれ、$|0\rangle$ を $\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$ に、$|1\rangle$ を $\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$ にします。矢印が見える最後の四角のものは測定を表します。これらを踏まえると $|\psi_0\rangle, |\psi_1\rangle, |\psi_2\rangle$ は次のようになります：

$$
\begin{aligned}
|\psi_0\rangle &= \frac{1}{\sqrt{2}}(a|0\rangle(|00\rangle+|11\rangle)+b|1\rangle(|00\rangle+|11\rangle)) && (9)\\
|\psi_1\rangle &= \frac{1}{\sqrt{2}}(a|0\rangle(|00\rangle+|11\rangle)+b|1\rangle(|10\rangle+|01\rangle)) && (10)\\
|\psi_2\rangle &= \frac{1}{\sqrt{2}}\left(a\left(\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\right)(|00\rangle+|11\rangle)+b\left(\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\right)(|10\rangle+|01\rangle)\right) && (11)\\
&= \frac{1}{2}(|00\rangle(a|0\rangle+b|1\rangle)+|01\rangle(a|1\rangle+b|0\rangle)+|10\rangle(a|0\rangle-b|1\rangle)+|11\rangle(a|1\rangle-b|0\rangle)) && (12)
\end{aligned}
$$

ここで Alice は $|\psi_2\rangle$ に対して測定を行います。Alice の測定は 1 つ目と 2 つ目の部分系に対して行われますから、この測定で 00 という結果を得たならば Bob の状態は $a|0\rangle+b|1\rangle$ に収縮します。これは Alice が Bob に伝えたかった状態 $|\psi\rangle$ そのものです。またもし Alice が測定の結果 01 を得たならば Bob の状態は $a|1\rangle+b|0\rangle$ となります。これは Alice が伝えたかった状態 $|\psi\rangle$ ではありません。ではこの場合は Alice は Bob に上手く情報を伝達できないということになるのでしょうか。そんなことはありません。この状態に Bob が X ゲートというものを作用させればよいのです。X ゲートは $|0\rangle$ を $|1\rangle$ に、$|1\rangle$ を $|0\rangle$ に変換するゲートです。したがって Alice は自分の結果が 01 だったときは、Bob に対して X ゲートを作用させるように指示すれば最終的に Bob に確実に状態 $|\psi\rangle$ を伝達することができます。次に Alice の結果が 10 のときを考えれば Bob の状態は $a|0\rangle-b|1\rangle$ となります。このときもまた Bob の状態は $|\psi\rangle$ ではありませんが、Z ゲートを作用させればうまくいきます。Z ゲートは $|0\rangle$ はそのまま、$|1\rangle$ を $-|1\rangle$ と変換するゲートです。したがってこのときは Alice は Bob に対して Z ゲートを作用させるように指示すればよいのです。最後に Alice の結果が 11 だった場合を考えましょう。このとき Bob の状態は $a|1\rangle-b|0\rangle$ となります。これに対しては X ゲートを作用させた後に Z ゲートを作用させれば $|\psi\rangle$ と一致することがわかるかと思います。このように Alice は自分が得た結果をもとに適切な指示を Bob に与えることで、Bob に伝えたい状態 $|\psi\rangle$ を確実に伝達することができるのです（以上のことは表 1 にまとめました）。Alice と Bob が遠く離れ離れであっても、Alice の測定によって Bob が（測定することなく）情報を受け取ることができます。これが量子「テレポーテーション」と呼ばれる所以ではないでしょうか。

表 1: Alice の測定結果、Bob の状態、Bob が作用させるべきゲート

Alice の測定結果	Bob の状態	Bob が作用させるべきゲート
00	$a\|0\rangle+b\|1\rangle$	なし
01	$a\|1\rangle+b\|0\rangle$	X ゲート
10	$a\|0\rangle-b\|1\rangle$	Z ゲート
11	$a\|1\rangle-b\|0\rangle$	X ゲートの後に Z ゲート

ところで Alice と Bob は遠く離れ離れであっても、Alice の測定結果によって瞬間的に Bob に状態が伝達されているように思えるかもしれません。もし瞬間的に情報が伝達されているのならばそれは相対論を破っています。しかし量子テレポーテーションは相対論を破る現象ではありません。たしかに Bob の持っている状態は Alice の測定結果によって瞬間的に確定します。しかし測定結果を得るのは Alice であって、Bob は Alice からその結果を受け取るまで自分の状態が何であるかはわかりません。結局のところ、Alice は自分の測定結果を Bob に伝えるためには古典通信を用いる必要があり、量子テレポーテーションによって光の速さを超える情報伝達が実現されるわけでありません。

[3]controlled-not の略。
[4]CNOT ゲートはじめ、いくつかの量子ゲートについては Appendix B を参照。

Appendix A：ベルの不等式

Einstein,Podolsky,Rosen は局所実在論の立場を取り、EPR 論文として知られる有名な論文で量子論は完全ではないと主張しました。しかし局所実在論はそもそも正しいのでしょうか。実はベルの不等式とその実験において局所実在論は否定されました。以下ではこのベルの不等式について見ていきましょう。

まず局所実在論とはどのような考え方でしょうか。局所実在論の考え方は「実在性」と「局所性」に分けることができます。実在性とは、測定対象の状態を定めれば物理量の測定結果が確定している[5]というものです。また局所性とは、離れたところにある系を独立なものとして扱い、両者の間の測定は互いに影響を及ぼしあわないというものです。この二つの考え方と量子論を比較してみましょう。量子論では、物理量の測定結果は測定をすることで初めて確率的に決定すると考えます。またエンタングルメントのように、離れたところにある系の間に一方の測定結果がわかると他方の測定結果もわかるというような相関があります。このように局所実在論と量子論は根本から相容れない考えです。この二つの考え方から導かれる結果を以下で見ていきましょう。

一旦、量子論を離れ「常識」的な（局所実在論的な）思考実験を考えましょう。Alice、Bob、Charlie の三者を考えます。Charlie は、ある決まった状態（EPR 状態）にある 2 粒子を何度も作り出すことができるとし、またこの 2 粒子を Alice と Bob に一つずつ分配するとします。ここで受け取った粒子に対して行う測定、P_Q, P_R, P_S, P_T を考えます。P_Q, P_R, P_S, P_T はその結果が必ず+1 か-1 となる測定であるとします。Alice は受け取った粒子に対して P_Q あるいは P_R のどちらかの測定を完全にランダムに選んで行います。Bob もまったく同様に P_S あるいは P_T のどちらかの測定を完全にランダムに選んで行います。ここで局所性の仮定より Alice と Bob はお互いの測定が互いに影響を及ぼさないとします。次の量について考えましょう：

$$QS + RS + RT - QT = (Q + R)S + (R - Q)T \tag{13}$$

ここで Q, R, S, T は実在ですから測定前からその値は決まっているとしていることに注意しましょう。考えればすぐわかるように $QS + RS + RT - QT = \pm 2$ となります。次に $Q = q, R = r, S = s, T = t$ を取る確率を $p(q, r, s, t)$ と表すことにします。ここで $\boldsymbol{E}(\cdot)$ で期待値を表すことにすると

$$\begin{aligned} \boldsymbol{E}(QS + RS + RT - QT) &= \sum_{q,r,s,t} p(q, r, s, t)(qs + rs + rt - qt) && (14) \\ &\leq \sum_{q,r,s,t} p(q, r, s, t) \times 2 && (15) \\ &= 2 && (16) \end{aligned}$$

となります。また

$$\boldsymbol{E}(QS + RS + RT - QT) = \boldsymbol{E}(QS) + \boldsymbol{E}(RS) + \boldsymbol{E}(RT) - \boldsymbol{E}(QT) \tag{17}$$

です。以上より

$$\boldsymbol{E}(QS) + \boldsymbol{E}(RS) + \boldsymbol{E}(RT) - \boldsymbol{E}(QT) \leq 2 \tag{18}$$

となります。これがベルの不等式[6]です。

ここで量子論に戻ってこのベルの不等式を考えましょう。Charlie は次の 2 量子状態を用意するとします：

$$|\psi\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}} \tag{19}$$

[5] このような実在論はとくに素朴実在論と呼ばれる。
[6] これは CHSH 不等式とも呼ばれる。

彼は最初の量子ビットを Alice へ、二つ目の量子ビットを Bob へ渡します。ここで彼らは次の測定を行うとします：

$$Q = Z_1 \tag{20}$$
$$R = X_1 \tag{21}$$
$$S = \frac{-Z_2 - X_2}{\sqrt{2}} \tag{22}$$
$$T = \frac{Z_2 - X_2}{\sqrt{2}} \tag{23}$$

量子論における期待値を $\langle\cdot\rangle$ で書くことにすれば

$$\langle QS\rangle = \frac{1}{\sqrt{2}} \tag{24}$$
$$\langle RS\rangle = \frac{1}{\sqrt{2}} \tag{25}$$
$$\langle RT\rangle = \frac{1}{\sqrt{2}} \tag{26}$$
$$\langle QT\rangle = -\frac{1}{\sqrt{2}} \tag{27}$$

となります。したがって

$$\langle QS\rangle + \langle RS\rangle + \langle RT\rangle - \langle QT\rangle = 2\sqrt{2} \tag{28}$$

となります。ここでベルの不等式 (16) 式を思い出してみましょう。(16) 式と (26) 式は明らかに矛盾しています。ベルの不等式と量子論に基づいた式のどちらが正しいのでしょうか。これは実験的に結論が出ています。実験は量子論による式が正しいと主張します。これは何を意味するでしょうか。この結果はベルの不等式を導いた仮定が誤っていたということを意味します。すなわち
(1)Q, R, S, T という量が測定と独立に存在している、すなわち実在性の考え方。
(2)Alice と Bob の測定はお互いに影響を及ぼさないという局所性の考え方。
のどちらかが間違っているということになります。ここで注意したいのはベルの不等式の破れは (1),(2) のどちらかが間違っているという主張に留まるということです。ベルの不等式の破れが実験的に確かめられたことにより、局所実在論は否定され、量子論の正当性はより強固なものとなりました。

Appendix B：量子ゲート

まず量子ビットを次のようにベクトルで表すことにします：

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{29}$$
$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{30}$$

次の X,Y,Z はパウリ行列[7]と呼ばれ、特に X ゲートは NOT ゲートとも呼ばれます：

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{31}$$
$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \tag{32}$$
$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{33}$$

[7] これらに恒等演算子 I を加えてパウリ行列と呼ぶこともある。

また Hadmard ゲートは

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{34}$$

と表されます。これらのゲートが量子ビットどのように変化させるかは簡単な行列計算によりすぐにわかります。確かめてみましょう。

ここで Kronecker 積を導入します。$m \times n$ 行列 A、$p \times q$ 行列 B について

$$A \otimes B \equiv \begin{pmatrix} a_{11}B & \dots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \dots & a_{mn}B \end{pmatrix} \tag{35}$$

と定義し、得られる行列は $mp \times nq$ となります。例えば $|10\rangle$ は

$$|1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{36}$$

$$= \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \tag{37}$$

となります。すると CNOT ゲートは次のようになります。

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{38}$$

簡単な計算により $C\,|10\rangle = |11\rangle$ などは確かめることができます。スワップゲート S やトフォリゲート[8]T などがあります。これらの行列形式を以下に与えるので、どのような変換をするゲートなのかを実際に計算して考えてみましょう：

$$S = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{39}$$

$$T = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \tag{40}$$

参考文献

[1] Michael A. Nielsen and Issac L. Chuang (2010), *Quantum Computation and Quantum Information: 10th Anniversary Edition”*, Cambridge: Cambridge University Press

[2] 石坂智・小川朋宏・河内亮周・木村元・林正人 (2012), 「量子情報科学入門」, 東京: 共立出版

[8] CCNOT(controlled-controlled-not) ゲートとも呼ばれる。