量子力学をもとにした、量子暗号解読体験

筑波大学 University of Tsukuba

丸澤賢司

概要 去年授業の中でpythonというプログラミング言語を学んだので、それと今年の授業内のゼミで学んだ量子力学の知識をいかしてより量子暗号を理解できるようにゲームを作成しました。量子コンピュータがなぜ早いかに興味があります。

量子暗号解読体験ゲームの遊び方

パソコン上で量子測定を表現できるような暗号解読ゲームを作成しました。1人用をプレイして暗号を解読し、それをもとに**以下のクイズ**に正解された方には**記念缶バッジ(限定50個)**をプレゼントさせていただきます。ぜひ挑戦してみてください！右の説明などを読むとより解きやすいと思います。
２人用でも声をかけていただけるとプレゼントできます。

クイズ:暗号が示す、物理に関連がある年号は？
(一般の方にはなじみがないと思うので携帯で検索していただいて大丈夫です。〇〇 year of physics　量子 で検索)
→解けた方は金庫にその4ケタの数字を入れて解錠してください。

①プレイモードを選ぶ

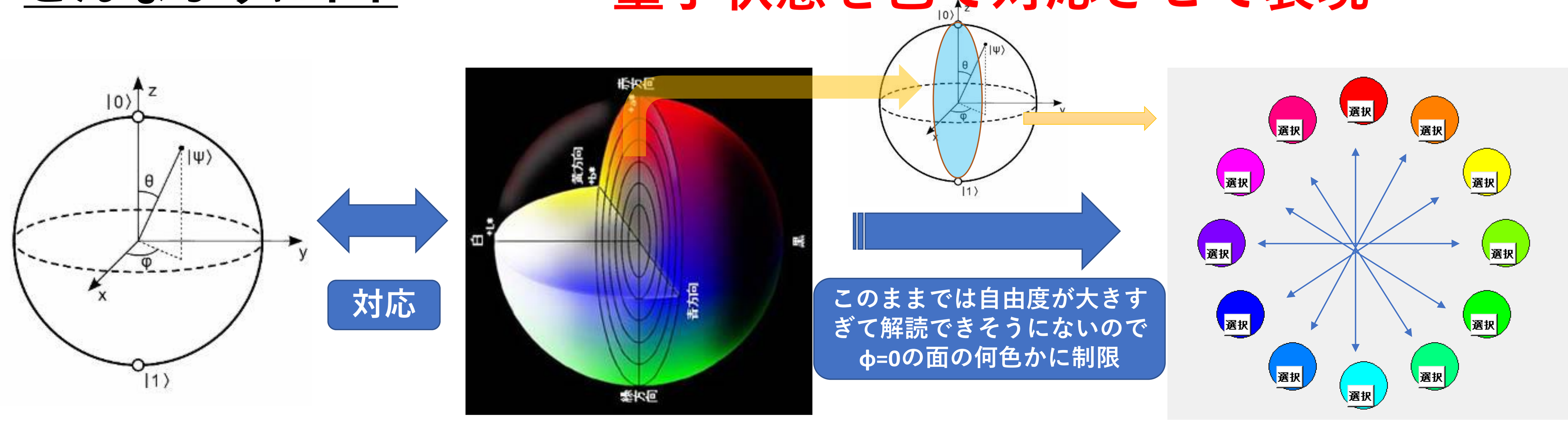
1人用　or　2人用

1人目のプレイヤーが変換表(別紙)にもとに暗号をつくる

②以降は2人目のプレイヤー用

こちら側で自動的にある基底が用意されているので、それにもとづいて情報が量子暗号化されます。

どんなふうに？？ → **量子状態を色で対応させて表現**



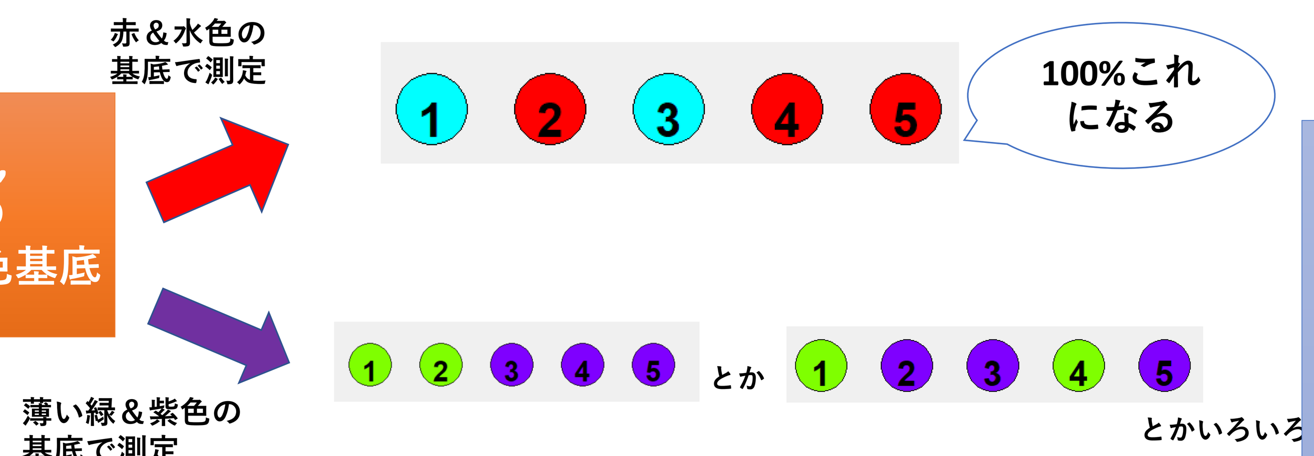
ブロッホ球　　La*b*色空間

②測定に使う色(ブロッホ球上の基底)を選んで測定

→ **実際の量子力学的にそって色(量子状態)が確定し表示される**

例えば…

解読したい暗号:01011,
設定されている基底の
対応方法:1→赤基底,0→水色基底



③測定結果を暗号変換表に照らし合わせ暗号解読

都合の良い基底を見つけるのは大変なので、ヒントとしてテストモードを用意しました。(メニューより)このゲーム攻略の重要ポイントは問題作成者が設定した基底を正しく予想することです！頑張ってください(^^)/

量子力学の数学的基礎①(とばしても大丈夫です)

量子力学では電子等の状態を表すものを波動関数ψ(r,t)と呼ぶ。
この波動関数を**ヒルベルト空間**というベクトル空間上のベクトルとみなし、記述していく。

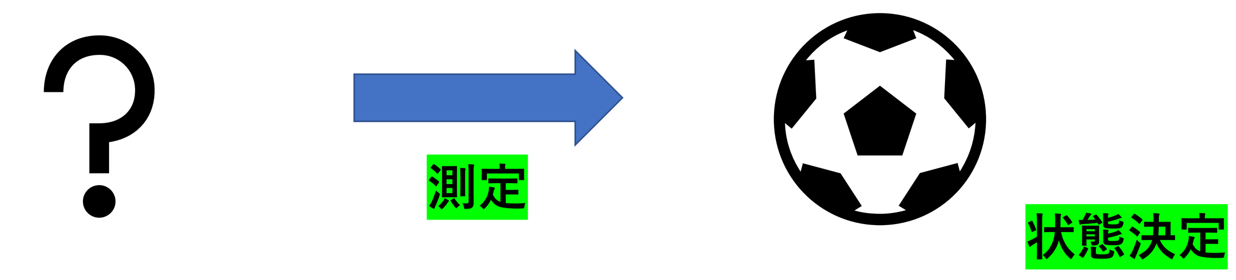
例として、2次元ヒルベルト空間を考える。
基底ベクトルとして|0>と|1>を考える。ヒルベルト空間上のベクトル(つまり元)は|〇>の形で表すことがある。これらはケットベクトルと呼ぶ。
直交しているベクトル同士の内積は0になるはずなので以下の(1)式ように表す。

$$\langle 0|1\rangle = \langle 1|0\rangle = 0 \quad \cdot\cdot\cdot(1) \qquad |\psi\rangle = a|0\rangle + b|1\rangle \quad \cdot\cdot\cdot(2)$$

これがヒルベルト空間の元同士の内積の表現である。<0|や<1|はブラベクトルと言い、それぞれケットベクトルの複素転置をとったものを表している。
この２つの正規直交したケットベクトルの元を使えば、2次元ヒルベルト空間の任意の元は以上の式(2)のように表すことができる。
ここでa,bはそれぞれ複素数である。ただし$|a|^2+|b|^2=1$をみたす。

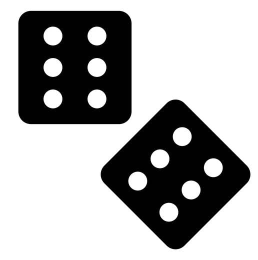
ブロッホ球と測定

当然ですがあらゆる物体は観測を経て初めて状態が分かります。
身近なことで言えば、私たちはそこにボールがあることを見ることによって測定し、認識しています。
物理においての測定とは、もう少し踏み込んで**何かしらの物理量を得ること**です。(物理量とは位置や温度、回転速度等の注目する物理現象を理解するのに必要な数値で表された何かの尺度のこと)

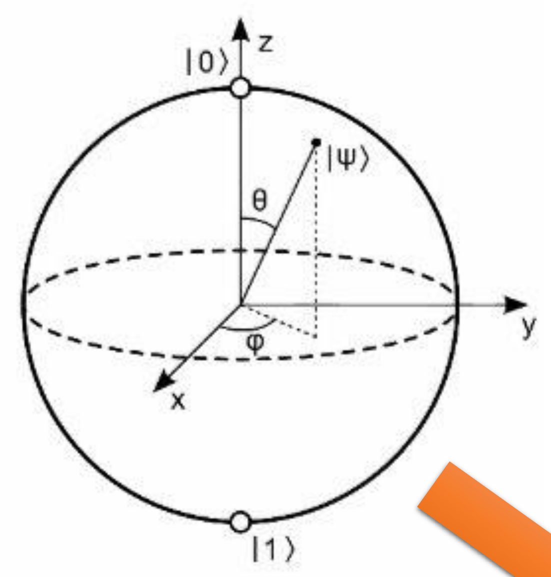


量子力学の主張を大雑把に説明するとすれば、「測定の前まではその測定対象の物理量は確定していなく、ただ〇〇という値が出やすいというように**確率的に出やすい物理量が決まっているだけ**である。測定してはじめて測定対象の物理量が決定される。」というようになります。

まるでサイコロみたいですね。あのアインシュタインも「神はサイコロを振らない」といってこの不思議な理論について慎重に思考をめぐらせました。



ここで、物理量を測定したい対象である、なんらかの量子状態|ψ＞を考えます。(抽象的ですみません。かっこはケットベクトルといいます。あまり気にしなくても大丈夫です。)
この量子状態に、「あなたは|0>ですか|1>ですか」と聞くようなイメージで測定を行うと、どちらかの状態にある確率でいきます。(この測定に使う量子状態は、簡単のために直交しているペアを選ぶとします。直交している状態とは、矢印の上向きと下向き等全く逆の状態というイメージです。)
この**確率を視覚的にわかりやすくしてくれるものとして**ブロッホ球**というものが便利です**。



ブロッホ球

ブロッホ球の球面上の点は任意の量子状態を表せます。実際に指定するときは、地球上で緯度経度を指定すれば、一つの場所が定まるような感じで、θとϕ(角度)で指定します。

端的にいえば、量子状態|ψ＞は測定に使用している**２つの状態のうち、より近いほうになりやすいです**。(確率的に支配されているので、遠いほうが出る時もあります)

この図だと|ψ＞を|0>＆|1>で測定したら|0>になりやすそう！

量子力学の数学的基礎②(とばしても大丈夫です)

実験事実として、「注目している量子状態を観測したとき、どのような確率で状態が変化していくかを計算したいときは、その量子状態と観測する量子状態の**内積の絶対値の2乗を計算すれば良い**」ということが確かめられている。ゲーム内ではこれにもとづいて確率が計算されています。

例　$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ が測定後に|0>になる確率

$$|\langle 0|\psi\rangle|^2 = |\langle 0|\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle|^2 = \left|\frac{1}{\sqrt{2}}\langle 0|0\rangle + \frac{1}{\sqrt{2}}\langle 0|1\rangle\right|^2$$

|0>,|1>は正規直交基底であるから、自分自身との内積は1になるので

$$= \left|\frac{1}{\sqrt{2}} + 0\right|^2 = \frac{1}{2}$$

ブロッホ球の数学的説明

(2)式を書き換える。まずa,bを以下のように極座標表示にする。

$$a = r(cos\theta + isin\theta), b = r'(cos\phi + isin\phi)$$

ただし、 $|a|^2+|b|^2=1$より、$|r|^2+|r'|^2=1$を満たさなければならない。ここで、r=cosγ,　r'=sinγとおけば、自動的に満たすのでこのようにおく。ただしr,r'≧0より、0≦γ≦π/2という条件がつく。以上より、

$$a = cos\gamma(cos\theta + isin\theta) = cos\gamma e^{i\theta}$$
$$b = sin\gamma(cos\phi + isin\phi) = sin\gamma e^{i\phi}$$

量子力学では波動関数を定数倍しても、元の波動関数を表現しているので、$|\psi\rangle$に$e^{-i\theta}$をかけたものを考えて、最終的に以下のように表現できる。

$$|\psi\rangle = cos\gamma|0\rangle + sin\gamma\, e^{i(\phi-\theta)}|1\rangle$$

Φ-θは-4πから4πとりえるが、重複がややこしいので、0,2πに制限し、なおかつ新しい文字βを用いてこれを表すと、

$$|\psi\rangle = cos\gamma|0\rangle + sin\gamma\, e^{i\beta}|1\rangle \quad (0 \le \gamma \le \frac{\pi}{2}, \qquad 0 \le \beta \le 2\pi)$$

と表すことができる。このパラメータを動かすと半球ができるが、それを無理やり拡張して表現させたものがブロッホ球となる。