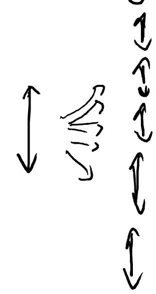
S.KIMMEL

Cloning (or lack of)

Cloning:



$$|\psi\rangle \longrightarrow |\psi\rangle|\psi\rangle$$

Create two copies of a state from 1

Cloning would break quantum Crypto. Why?

- Eve could take intercepted photon, make many copies, then try different measurement settings until she finds correct polarization. She can send one of the copies to Bob, who will have no idea it was intercepted.

Before we get to no cloning, let's talk about more general quantum states.

Qudits

- State $\Rightarrow$ Qudit = d-dimensional quantum state

$$|\psi\rangle \in \mathbb{C}^d, \quad |\psi\rangle = \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{d-1} \end{pmatrix}$$

Normalized

$$1 = \langle\psi|\psi\rangle = \sum_{i=0}^{d-1} |a_i|^2$$

2 quantum systems:

$$|\psi\rangle_A \otimes |\phi\rangle_B$$

(can have different dimensions)

Standard Basis

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ \vdots \end{pmatrix} \quad \cdots \quad |d-1\rangle = \begin{pmatrix} \vdots \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

S.KIMMEL

Q: If you have n qubits, what length vector do you need to represent the full system?

A) n B) $2n$ C) 2^n D) $n!$

$\boxed{\text{Qudit Measurement}}$ $\Rightarrow$ d-dimensional orthonormal basis $M = \{|\phi_i\rangle\}_{i=0}^{d-1}$ $|\phi_i\rangle \in \mathbb{C}^d$

$$\langle \phi_i | \phi_j \rangle = \delta_{ij} = \begin{cases} 1 & i=j \\ 0 & i \neq j \end{cases}$$

If measure $|\psi\rangle \in \mathbb{C}^d$

- Outcome $|\phi_i\rangle$ occurs with probability $|\langle \psi | \phi_i \rangle|^2$
- If outcome $|\phi_i\rangle$ occurs, $|\psi\rangle \xrightarrow[\text{collapses}]{} |\phi_i\rangle$

- Transformation = unitary matrix

$U \in \mathbb{C}^{d \times d}$ is unitary iff $UU^{\dagger} = \mathbb{I} = U^{\dagger}U$

conj. transpose

identity matrix

If apply U to state $|\psi\rangle$, new state is $|\psi'\rangle = U|\psi\rangle$

(Also, $\langle\psi'| = \langle\psi|U$

No Cloning (Wootters)

Suppose for contradiction unitary U is a cloner. Then

$$U(|\psi\rangle_A|0\rangle_B) = |\psi\rangle_A|\psi\rangle_B \quad \forall \text{ states } |\psi\rangle \in \mathbb{C}^d$$

where $U \in \mathbb{C}^{d^2 \times d^2}$, $|0\rangle \in \mathbb{C}^d$.

Finish proof! (Hint: • cloner should work for 2 different states

• Think about inner products

S.KIMMEL

Since U is a universal cloner:

$$U\left(|\phi\rangle_A|0\rangle_B\right) = |\phi\rangle_A|\phi\rangle_B$$

Taking the conjugate transpose of both sides

$$\langle\phi|_A\langle 0|_B U^\dagger = \langle\phi|_A\langle\phi|_B$$

Acting on both sides with $U|\psi\rangle_A|0\rangle_B = |\psi\rangle_A|\psi\rangle_B$, we have

$$\langle\phi|_A\langle 0|_B U^\dagger U|\psi\rangle_A|0\rangle_B = \langle\phi|_A\langle\phi|_B|\psi\rangle_A|\psi\rangle_B$$

Since U is unitary, $U^\dagger U = \mathbb{I}$, so

$$\langle\phi|\psi\rangle\underbrace{\langle 0|0\rangle}_{1} = \langle\phi|\psi\rangle\langle\phi|\psi\rangle$$

$$\langle\phi|\psi\rangle = \langle\phi|\psi\rangle^2$$

$$\Downarrow$$

$$\langle\phi|\psi\rangle = 0 \text{ or } 1$$

U should clone all states, not just orthogonal states, A contradiction