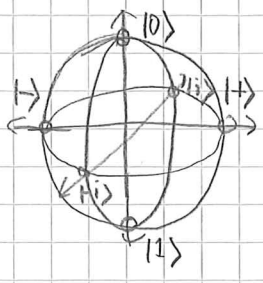
The Bloch sphere (§7.1)

An efficient geometric representation of states in a qubit system.



- pure states $\leftrightarrow$ points on a sphere up to scalar s.t. ONB's are antipodal points
- mixed states $\leftrightarrow$ points in the interior

formally: mixed states $\leftrightarrow$ 2×2 density matrices in qubit sys ρ.

pure states (up to scalar) $\leftrightarrow$ rank 1 density matrices

$D = \{ 2\times 2 \text{ density matrices} \}$ has following structures

- convex: $\rho_1, \rho_2 \in D \Rightarrow t\rho_1 + (1-t)\rho_2 \in D$ $0 \le t \le 1$
- an action of $SO(3)$ from: $Ad_U : D \to D$, $\rho \mapsto U\rho U^\dagger$ $U \in U(2)$
  (trivial if $U = \lambda I_2$ so induces an action of $U(2)/\{\lambda I_2 : |\lambda| = 1\} \cong SO(3)$)
- $\text{rank}(\rho) = 1 \iff \rho$ is extremal in D
  $\hookrightarrow \rho = t\rho_1 + (1-t)\rho_2 \Rightarrow \rho_1 = \rho_2 = \rho$

orbits $D_\lambda = \{ \rho \in D : \rho \text{ has eigenval } \lambda, 1-\lambda \}$ $0 \le \lambda \le \frac{1}{2}$

$D_0 = \{ \rho : \text{rank}(\rho) = 1 \}$

$D_{\frac{1}{2}} = \{ \frac{1}{2} I_2 \}$

$\rightsquigarrow$ D can be identified with $B^3 = \{ x \in \mathbb{R}^3 : \|x\| \le 1 \}$

a (unitary) quantum gate operation corresponds to a rotation of B^3

No-cloning theorem (§ 7.2)

Prop. There is no unitary on $\mathbb{C}^2 \otimes \mathbb{C}^2$ such that

$$U(|\psi\rangle \otimes \underbrace{|0\rangle}_{\text{"ancilla" qubit}}) = |\psi\rangle \otimes |\psi\rangle.$$

such U would be a "cloning machine"

If this was possible, Alice would be able to communicate her choice of basis to Bob

$\varphi = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ max entangled state.

Alice chooses $|0\rangle, |1\rangle$ for measurement

$\rightsquigarrow$ Bob "receives" either $|0\rangle$ or $|1\rangle$

Alice chooses $|+\rangle, |-\rangle$ for measurement

$\rightsquigarrow$ Bob "receives" $(\langle +| \otimes id)\varphi$ or $(\langle -| \otimes id)\varphi$ normalized to unit vec $= |+\rangle, |-\rangle$

If Bob can clone his state many times and do measurement in $|0\rangle, |1\rangle$ basis

→ $|0\rangle$ always or $|1\rangle$ always

→ $|0\rangle$ with prob $\frac{1}{2}$, $|1\rangle$ with prob $\frac{1}{2}$

Proof of Prop.: any unitary matrix preserves inner prod $|\varphi_i'\rangle = U|\varphi_i\rangle \Rightarrow \langle \varphi_0' | \varphi_1' \rangle = \langle \varphi_0 | \varphi_1 \rangle$, $i = 0, 1$

and $(|\psi_0\rangle \otimes |\psi_1\rangle)^\dagger (|\psi_0'\rangle \otimes |\psi_1'\rangle) = \langle \psi_0 | \psi_0' \rangle \langle \psi_1 | \psi_1' \rangle$

$\rightsquigarrow U(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle$ and $U(|\psi'\rangle \otimes |0\rangle) = |\psi'\rangle \otimes |\psi'\rangle$

would give $\langle \psi | \psi' \rangle \langle 0 | 0 \rangle = \langle \psi | \psi' \rangle^2$ for all $|\psi\rangle, |\psi'\rangle$. ∎

Quantum money scheme

"Easy" authentication scheme using qubits.

A "bill" has

- string of 0's and 1's : $i_0 \cdots i_{N-1}$, $i_k = 0, 1$.
  "serial number"
- qubits state $|\psi_0\rangle \otimes \cdots \otimes |\psi_{N-1}\rangle \in \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2$.

The "bank" knows secret information:

for each k, whether one should measure $|\psi_k\rangle$ in the $|0\rangle, |1\rangle$ basis or in the $|+\rangle, |-\rangle$ basis

Pubic knowledge:

if the measurement of $|\psi_k\rangle$ should be measured in $|0\rangle, |1\rangle$ then $|\psi_k\rangle$ should be $|i_k\rangle$

if it should be measured in $|+\rangle, |-\rangle$ then $|\psi_k\rangle$ should be $|+\rangle$ if $i_k = 0$, $|-\rangle$ if $i_k = 1$

Bank's authentication method

measure each $|\psi_k\rangle$ and check consistency of the result with i_k

Outsider: does not know which measurement scheme to use for $|\psi_k\rangle$. Because of no-cloning, it can measure $|\psi_k\rangle$ only once

Suppose $|\psi_k\rangle$ should be measured in $|0\rangle, |1\rangle$ and $i_k = 0$. (so genuine bill has $|\psi_k\rangle = |0\rangle$)

by prob $\frac{1}{2}$, outsider makes wrong guess, measures in $|+\rangle, |-\rangle$. gets $|\psi'_k\rangle = |+\rangle$ or $|-\rangle$ and print that on a counterfeit bill

↝ bank does authentication and (either way for $|\psi'_k\rangle = |+\rangle$ or $|\psi'_k\rangle = |-\rangle$) obs. $|1\rangle$ by prob. $\frac{1}{2}$

(cont.) if the observer makes correct guess, (prob. $\frac{1}{2}$)

he does measurement in $|0\rangle, |1\rangle$, observes $|0\rangle$ and prints it on counterfeit.

$\rightsquigarrow$ this passes banks authentication

$\Rightarrow$ each digit of serial num has prob. $\frac{3}{4}$ of success for outsider

$\Rightarrow$ success prob. of counterfeit bill is $(\frac{3}{4})^N$