PHY682 Special Topics in Solid-State Physics: Quantum Information Science

Lecture time: 2:40-4:00PM Monday & Wednesday

Today 11/4:

1. Quick review
2. Week 10's topics: **No clones in quantum**

Shannon vs. Schumacher noiseless channel coding theorem

Suppose $\{X_i\}$ is an i.i.d. information source with entropy rate $H(X)$.
If $R > H(X)$, then there exists a reliable compression scheme of rate R for the source.
if $R < H(X)$, then any compression scheme will not be reliable.

[See N&C Thm 12.4]

- How to generalize to quantum regime?
  (1) Alphabet is drawn from a set of quantum states $\{|\phi_x\rangle\}$
  (2) $\{X_i\}$ → an ensemble $\rho = \sum_x q_x |\phi_x\rangle\langle\phi_x|$
  (3) Typical sequence → typical subspace; atypical sequence → atypical subspace
  (4) $H(X)$ → $S(\rho)$

Suppose $\{\rho\}$ is an i.i.d. quantum information source with entropy rate $S(\rho)$.
If $R > S(\rho)$, then there exists a reliable compression scheme of rate R for the source.
if $R < S(\rho)$, then any compression scheme will not be reliable.

Noisy channel coding*: classical vs. quantum

$X \to \boxed{\mathcal{N}} \to Y$

[From Nielsen & Chuang]

Theorem 12.7: (**Shannon's noisy channel coding theorem**) For a noisy channel $\mathcal{N}$ the capacity is given by

$$C(\mathcal{N}) = \max_{p(x)} H(X:Y)\,, \tag{12.67}$$

where the maximum is taken over all input distributions $p(x)$ for X, for one use of the channel, and Y is the corresponding induced random variable at the output of the channel.

$$H(X:Y) = H(Y) - H(Y|X)$$
$$= H(Y) - \sum_x p(x) H(Y|X=x)$$

Theorem 12.8: (**Holevo–Schumacher–Westmoreland (HSW) theorem**) Let $\mathcal{E}$ be a trace-preserving quantum operation. Define

$$\chi(\mathcal{E}) \equiv \max_{\{p_j,\rho_j\}} \left[S\left(\mathcal{E}\left(\sum_j p_j \rho_j\right)\right) - \sum_j p_j S(\mathcal{E}(\rho_j)) \right], \tag{12.71}$$

where the maximum is over all ensembles $\{p_j, \rho_j\}$ of possible input states ρ_j to the channel. Then $\chi(\mathcal{E})$ is the product state capacity for the channel $\mathcal{E}$, that is, $\chi(\mathcal{E}) = C^{(1)}(\mathcal{E})$.

Week 11: No clones in quantum: No cloning of quantum states, non-orthogonal state discrimination, quantum tomographic tools, quantum cryptography: quantum key distribution from transmitting qubits and from shared entanglement

Strange quantum features

[Dieks 82'; Wootters & Zurek '82]

- No cloning: cannot xerox in quantum world

$$|\alpha\rangle|\text{blank}\rangle \not\longrightarrow |\alpha\rangle|\alpha\rangle \quad \forall|\alpha\rangle \text{ except certain states}$$

$0 \to 00$

$1 \to 11$

cannot copy

$|+\rangle \to |+\rangle|+\rangle$

Proof: by contradiction, assume possible:

$$|\alpha\rangle|\text{blank}\rangle \longrightarrow |\alpha\rangle|\alpha\rangle$$

$$|\beta\rangle|\text{blank}\rangle \longrightarrow |\beta\rangle|\beta\rangle$$

But overlap preserved by unitary operation:

$$\langle\alpha|\beta\rangle = \langle\alpha|\beta\rangle^2 \to \langle\alpha|\beta\rangle = 0 \text{ or } 1$$

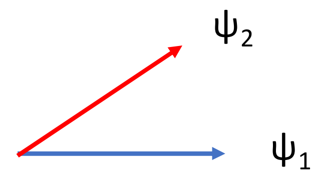
- Cloning would allow to distinguish non-orthogonal states

➔ By making enough copy, they could be made almost orthogonal, and be distinguishable $\quad \langle\alpha|\beta\rangle^n \to 0$

State discrimination

no cloning ⟷ non-orthogonal state discrimination (not deterministic)

- Non-orthogonal states cannot be deterministically distinguished!



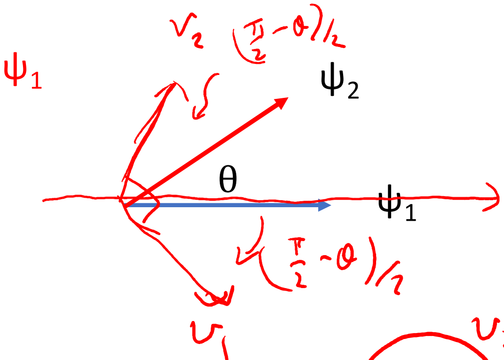
- Deterministic discrimination of non-orthogonal states could be used to perform cloning of non-orthogonal states!

➔ Suppose classical description of two states is known, but don't which one is given. If one could uniquely determine which, one could then produce as many copies (given its description is known)

State discrimination: case (i)

- Imagine there are two one-qubit states which may not be orthogonal: ψ_1 & ψ_2 (equally probable). For simplicity, one can take

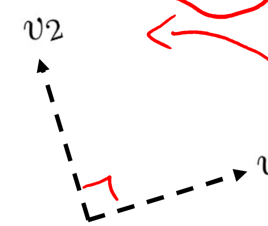
$$|\psi_1\rangle = |0\rangle,\ |\psi_2\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle,\ \text{with}\ 0 \le \theta \le \pi/2$$



> **Question: what is the best strategy to distinguish the two states?**

This question needs to be clarified. We will consider (i) to maximum overall success probability [minimum-error] (ii) to maximize the unambiguous discrimination

Case (i): we will design an orthogonal basis for such a measurement



$$|v_1\rangle = \cos\phi|0\rangle + \sin\phi|1\rangle,\ |v_2\rangle = -\sin\phi|0\rangle + \cos\phi|1\rangle$$

and if the outcome is v_1 then we declare it's ψ_1 ; we declare it's ψ_2 if outcome is v_2

(But this is *not* un-ambiguous.) So we want to maximize:

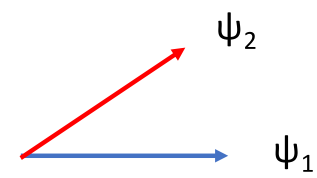
$$P(\phi) = \frac{1}{2}|\langle v_1|\psi_1\rangle|^2 + \frac{1}{2}|\langle v_2|\psi_2\rangle|^2 = \frac{1}{2}\cos^2\phi + \frac{1}{2}\sin^2(\theta-\phi)$$

$$\max\ \text{at}\ \phi = -(\pi/2-\theta)/2:\ \max P = (1+\sin\theta)/2$$

want max $P(\phi)$ over ϕ

e.g. $\theta = \pi/2$ $\psi_1 \perp \psi_2$ $\Rightarrow P_{max} = (1+1)/2 = 1$

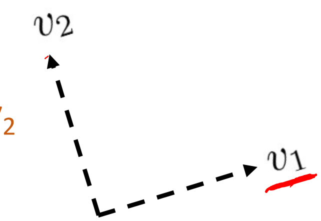
case (i): physical picture



$$|\psi_1\rangle = |0\rangle,\ |\psi_2\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle,\ \text{with}\, 0 \le \theta \le \pi/2$$

Case (i): an orthogonal measurement basis

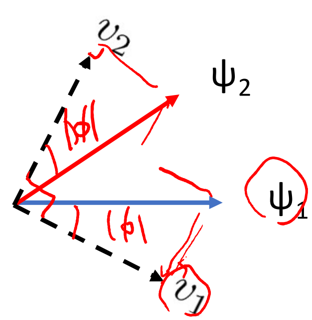
$$|v_1\rangle = \cos\phi|0\rangle + \sin\phi|1\rangle,\ |v_2\rangle = -\sin\phi|0\rangle + \cos\phi|1\rangle$$



and if the outcome is v_1 then we declare it's ψ_1 ; we declare it's ψ_2 if outcome is v_2

So maximize: $$P(\phi) = \frac{1}{2}|\langle v_1|\psi_1\rangle|^2 + \frac{1}{2}|\langle v_2|\psi_2\rangle|^2 = \frac{1}{2}\cos^2\phi + \frac{1}{2}\sin^2(\theta - \phi)$$

$$\max\ \text{at}\ \phi = -(\pi/2 - \theta)/2 :\ \max P_{\text{succ}} = (1 + \sin\theta)/2,\ \min P_{\text{err}} = (1 - \sin\theta)/2$$



when $p_1 = p_2 = \frac{1}{2}$ $4p_1p_2 = 1$

max $P_{err} = \frac{1}{2}\left(1 - \sqrt{1 - |\langle\psi_1|\psi_2\rangle|^2}\right.$

$\cos^2\theta$

✓ Helstrom bound:

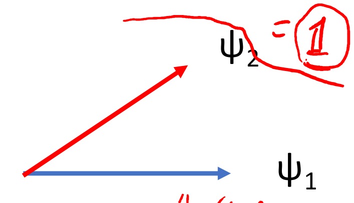
$$P_{\text{err}} \ge \frac{1}{2}\left(1 - \sqrt{1 - 4p_1p_2|\langle\psi_1|\psi_2\rangle|^2}\right)$$

State discrimination: case (ii)

measurement $\{|0\rangle, |1\rangle\} \longleftrightarrow \{|0\rangle\langle 0|, |1\rangle\langle 1|\}$

cf. $|0\rangle\langle 0| + |1\rangle\langle 1| = 1$

$$|\psi_1\rangle = |0\rangle, \ |\psi_2\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle, \ \text{with}\, 0 \le \theta \le \pi/2$$



detector "2" M_2

- Case (ii) to maximize the unambiguous discrimination
  This means that there are three non-negative operators M_1, M_2 and M_3 that correspond to must-be state 1, must-be state 2, and don't know, respectively

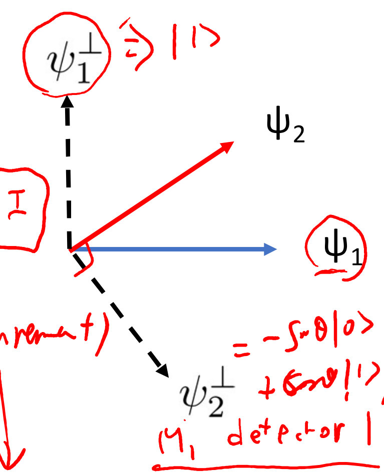
  3

  - Since there are only two states, if we choose an operator proportional to projector orthogonal to ψ_2, then if the corresponding detector clicks, we know it must come from the state ψ_1 , etc. Thus

I don't know

$M_i \geq 0$

$$M_1 = c|\psi_2^\perp\rangle\langle\psi_2^\perp|, \ M_2 = c|\psi_1^\perp\rangle\langle\psi_1^\perp|, \ M_3 = I - \underbrace{M_1 - M_2}_{\geq 0} \qquad \boxed{\sum_i M_i = I}$$



where we allows a constant c (the weight in the unambiguous discrimination), (generalized measurement)
but we want it to be as large as possible, and it is constrained by

$$M_3 = I - c(-\sin\theta|0\rangle + \cos\theta|1\rangle)(-\sin\theta\langle 0| + \cos\theta\langle 1|) - c|1\rangle\langle 1| \geq 0$$

probability

$$P_{\text{success}} = \frac{1}{2}\text{Tr}(|\psi_1\rangle\langle\psi_1| \cdot M_1) + \frac{1}{2}\text{Tr}(|\psi_2\rangle\langle\psi_2| \cdot M_2) \qquad \max_{M_3 \geq 0} c = 1/(1+\cos\theta) \qquad \text{Tr}(\rho M_i)$$

measurement operator; input state

want to max w.r.t. c

detect 1   detect 2

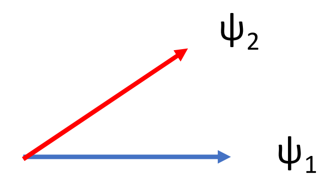
$$= c\frac{1}{2}|\langle 0|(-\sin\theta|0\rangle + \cos\theta|1\rangle)|^2 + c\frac{1}{2}\langle 1|(\cos\theta|0\rangle + \sin\theta|1\rangle)|^2 = c\sin^2\theta \leq 1 - \cos\theta$$

$c\,\frac{1}{2}\sin^2\theta + c\,\frac{1}{2}\sin^2\theta$

e.g. $|\langle 0|\psi\rangle|^2$

case (ii): derivation

$$|\psi_1\rangle = |0\rangle,\ |\psi_2\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle,\ \text{with}\, 0 \le \theta \le \pi/2$$



$$M_1 = c|\psi_2^\perp\rangle\langle\psi_2^\perp|,\ M_2 = c|\psi_1^\perp\rangle\langle\psi_1^\perp|,\ M_3 = I - M_1 - M_2$$

$$M_3 = I - c(-\sin\theta|0\rangle + \cos\theta|1\rangle)(-\sin\theta\langle 0| + \cos\theta\langle 1|) - c|1\rangle\langle 1| \ge 0$$

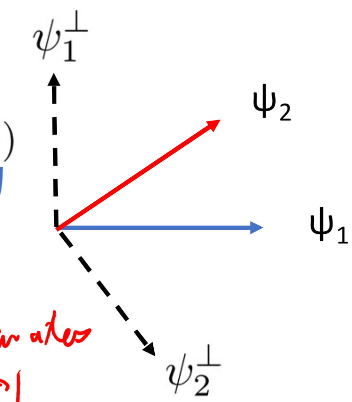
- M_3 in matrix form:

$$M_3 = I - c\begin{pmatrix} \sin^2\theta & -\sin\theta\cos\theta \\ -\sin\theta\cos\theta & \cos^2\theta + 1 \end{pmatrix} = I - c(1 \underbrace{- \cos^2\theta\,\sigma_z - \sin\theta\cos\theta\,\sigma_x}_{\text{eigenvalues } \pm\cos\theta})$$

$= 1 - \cos^2\theta$

$$1 - c(1 \pm \cos\theta) \ge 0$$

$$\max_{M_3 \ge 0} c = 1/(1+\cos\theta) \Leftarrow \text{eigenvalues } \pm\cos\theta$$



$\vec{F}\cdot\vec{\sigma} \Rightarrow$ eigenvalues $\pm|\vec{F}|$

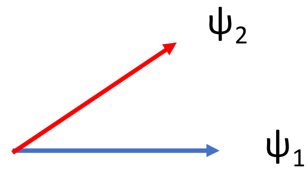
- Success probability:

$$P_{\text{success}} = \frac{1}{2}\mathrm{Tr}(|\psi_1\rangle\langle\psi_1| \cdot M_1) + \frac{1}{2}\mathrm{Tr}(|\psi_2\rangle\langle\psi_2| \cdot M_2)$$

$$= c\frac{1}{2}|\langle 0|(-\sin\theta|0\rangle + \cos\theta|1\rangle|^2 + c\frac{1}{2}\langle 1|(\cos\theta|0\rangle + \sin\theta|1\rangle|^2 = \overset{\frac{1}{1+\cos\theta}}{c}\sin^2\theta \le 1 - \cos\theta = 1 - |\langle\psi_1|\psi_2\rangle|$$

$\sin^2\theta = 1 - \cos^2\theta = (1-\cos\theta)(1+\cos\theta)$

General state discrimination



- ❑ Can consider unequal probability $p_1 \neq p_2$
- ❑ More than 2 pure states
- ❑ Mixed states

Refs:

- Barnett & Croke, Quantum state discrimination, arXiv:0810.1970
- Bae & Kwek, Quantum state discrimination and its applications, arxiv: 1707.02571

No cloning and no perfect discrimination of non-orthogonal states
➔ useful for secure communication

Secure communication?

secret key

- "One-time pad" is secure if length as long as message and used only once

[Vernam 1926]

Alice

Bob

Message:	0 1 0 1 1 0 0 1 0 1 0 1 1 0 0 0
Shared secret key (1-time pad):	1 1 0 0 1 0 1 0 1 1 1 0 0 1 1 0
→ Encrypt by XOR:	1 0 0 1 0 0 1 1 1 0 1 1 1 1 1 0 ➔ send this publicly
→ Receiver decrypt by XOR:	1 1 0 0 1 0 1 0 1 1 1 0 0 1 1 0
With secret key ➔	0 1 0 1 1 0 0 1 0 1 0 1 1 0 0 0

recover message

- Public-key cryptography: e.g. RSA (Rivest, Shamir, and Adleman, 1978)
  [Security relies on difficulty of factoring large integers]

→ a public key and a private key

Bob will publish the public key so that anyone can encrypt a message with the public key and send the encrypted message to Bob, who can decrypt the cipher text with the private key to recover the plain text efficiently.

- ➢ RSA can be broken by Shor's factoring algorithm ☹

RSA public key cryptography

$N=$
e.g. 15

1. Choose two different large prime numbers $\boldsymbol{p}$ and $\boldsymbol{q}$; $\boldsymbol{N} = \boldsymbol{pq}$
2. $\Phi = (\boldsymbol{p}-\mathbf{1})(\boldsymbol{q}-\mathbf{1})$ a number coprime with $\boldsymbol{N}$ and less than $\boldsymbol{N}$.

   $2 \cdot 4 = 8$ e.g. $e=3$. $d=3$
3. Choose $\boldsymbol{e}$ coprime with Φ and compute $\boldsymbol{d} = \boldsymbol{e}^{-1}$ (mod Φ) or $\boldsymbol{ed} = \mathbf{1}$ (mod $\boldsymbol{\Phi}$)
4. Broadcast public key $\boldsymbol{e}$ and number $\boldsymbol{N}$ (3, 15)

   e.g. $a = 2$
   $b = 2^3 = 8$
5. Other party encodes message $\boldsymbol{a}$ (assume coprime to $\boldsymbol{N}$) to be $\boldsymbol{b} = \boldsymbol{a}^{\boldsymbol{e}}$ (mod $\boldsymbol{N}$) and we can decode it by $\boldsymbol{b}$^$\boldsymbol{d} = \boldsymbol{a}$^$(\boldsymbol{ed}) = \boldsymbol{a}$^$(\boldsymbol{n}\ \Phi) = \boldsymbol{a}$ (mod $\boldsymbol{N}$), note $\boldsymbol{a}$^$\Phi = \mathbf{1}$ (mod $\boldsymbol{N}$)

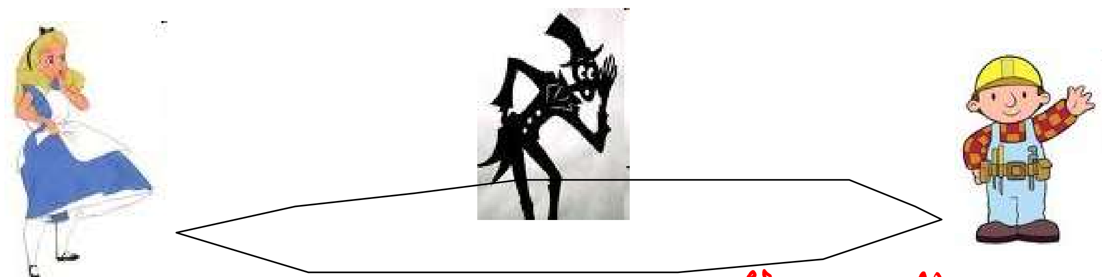
   $b^d = 8^3 = 2$
6. We can identify ourselves by encoding our signature $\boldsymbol{s}$ to be $\boldsymbol{t} = \boldsymbol{s}$^$\boldsymbol{d}$ (mod $\boldsymbol{N}$), everyone can verify by decoding $\boldsymbol{t}$^$\boldsymbol{e} = \boldsymbol{s}$(mod **N**)

   e.g. $s=4$. $t = 4^3 = 4$. $4^3 = 4$.

Factoring breaks RSA ☹

But quantum communication is secure ☺

Eavesdropper



Alice

use quantum states (e.g. non-orthogonal)

→ establish secret keys

Bob

BB84

Bennett Brassard Ekert

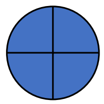
- Quantum states cannot be cloned
- Measurement disturbs quantum states
- Entanglement also helps

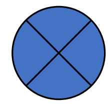
entanglement + Bell inequality

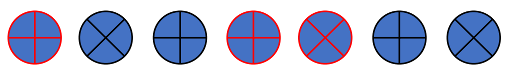
Quantum key distribution (QKD):BB84

classical bits

Goal: to establish a random sequence between Alice and Bob

 0/1 H/V basis: H=0, V=1 |0> and |1>

 +/− D/A basis: D=0, A=1 |+> and |->

1. Alice randomly selects a random sequence, e.g. 0101011…
   For each bit (0 or 1) she randomly selects H/V or D/A basis, e.g.
   HVDVDAV….
2. For each bit Bob randomly selects a basis H/V or D/A to measure, e.g.  ….

   Eve

   Alice $\xrightarrow{H/V/D/A}$ Bob

   Results: H D V V D H D

3. Openly compare bases (not results), keep results when measured in same basis, e.g., H V D … = 0 1 0 ….
4. Can compare a subset of results to make sure the security

Attack QKD?

❑ Intercept-and-resend attack

➢ Eve performs measurement on the intercepted photon (from Alice) in a randomly chosen basis H/V or D/A and resends a new photon to Bob according to her measurement result.

❖ When Alice and Bob happen to use the same basis:
→ If Eve uses correct basis (50%), then both she and Bob will decode Alice's bit value correctly. No error is introduced by Eve.
→ If Eve uses the wrong basis (50%), then both she and Bob will have random measurement results.

❖ Alice and Bob have 50% of using same basis
➔ Overall quantum bit error rate (QBER) is 25%

refer to Nielsen & Chuang for security proof

❑ An important advantage of QKD:

* once a QKD session is over, no classical "transcript" for Eve to keep since the communication is quantum.
* vs. public key: Eve can copy encrypted messages and wait until private key is broken to decrypt messages

Actual applications of QKD

- Bank transaction and government communication

- QKD was used to encrypt security communications in the 2007 Swiss election and the 2010 World Cup.

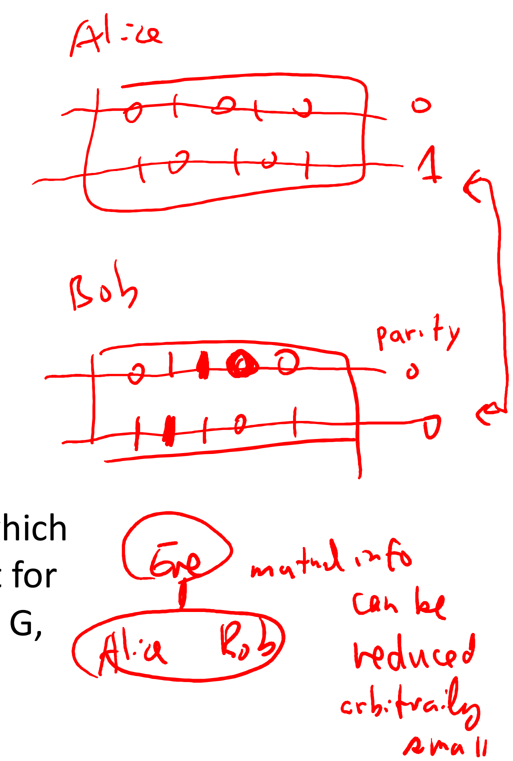
Making keys more secure*

- Alice and Bob can further perform two classical steps to increase correlation between their key strings and reduce mutual information with Eve

  (a) **information reconciliation**: error-correction conducted over a public channel (e.g. using parity check)

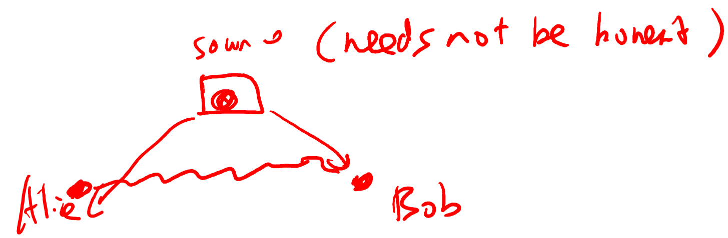
  (b) **privacy amplification**: a procedure for Alice and Bob to distill a common private key from a raw key about which Eve might have partial information.

  → Employ local randomness by using universal hash functions G, which map the set of n-bit strings A to the set of m-bit strings B, such that for any distinct a1 ,a2 ∈ A, when g is chosen uniformly at random from G, then the probability that g(a1) = g(a2) is at most 1/|B|



No cloning and no perfect discrimination of non-orthogonal states
➔ useful for secure communication

❖ Entanglement is also useful!



Violation of Bell inequality and QKD

[Ekert, PRL 67,661 (1991)]

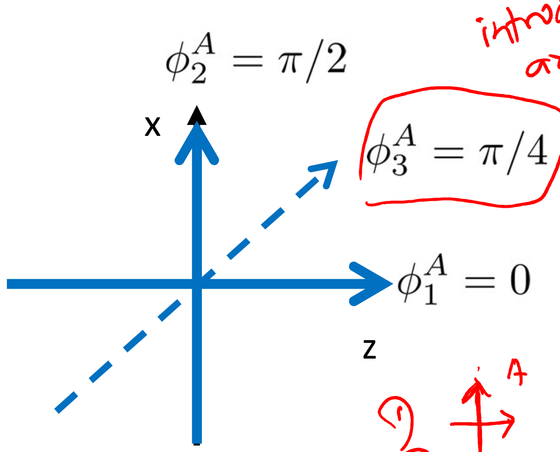
- Use a Bell state: $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$

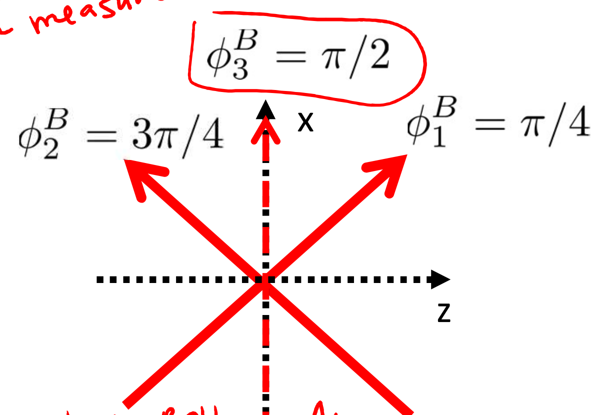
$\rightarrow |B| = \underline{2\sqrt{2}}$ vs 2 (classical)

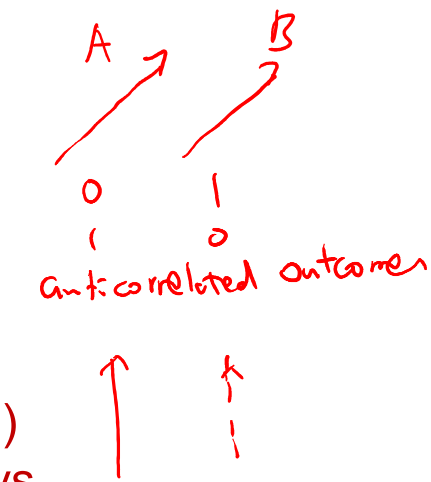
- Measurement along axes 1 and 2 of A & B are used to check violation of Bell inequality

$\langle A_1B_1 + A_1B_2 + A_2B_1 - A_2B_2 \rangle$

introduce a third axis for measurement







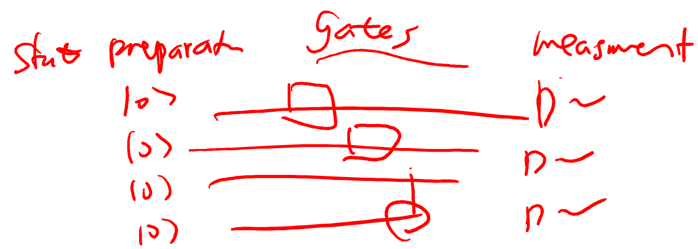
① A B ⇒ check Bell inequality

② ⇒ for key distribution

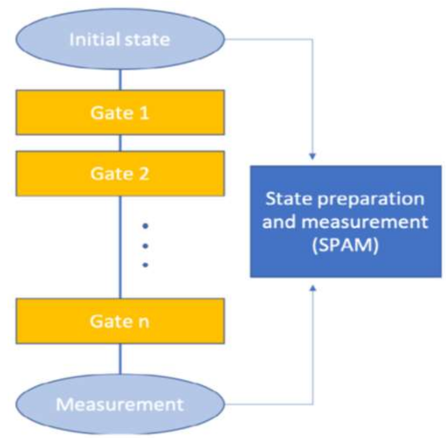
- A third axis is added so that measurement using (A3,B1) and (A2,B3) gives anticorrelation → establish secret keys

Switch topic: tomographic tools for quantum computations

Tomographic tools



- Crucial to ensure proper functioning of QC and correctness of results



- State preparation
  - $\Rightarrow$ State tomography
- Gate operations
  - $\Rightarrow$ Process tomography
- Measurement (i.e. detectors)
  - $\Rightarrow$ Detector tomography

- Note: detector tomography is often ignored, but important to extract correct computational outcomes

Quantum state tomography

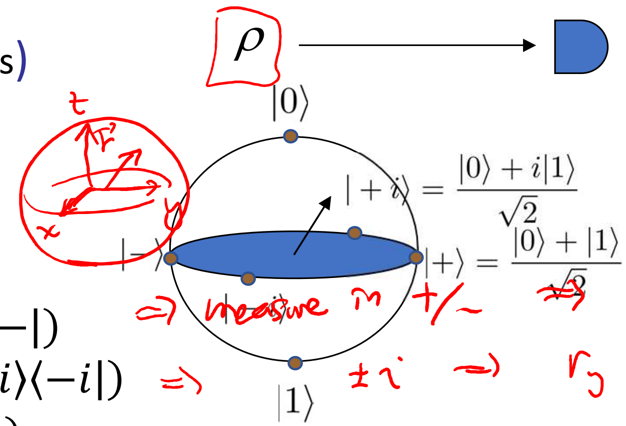
- ❑ Estimate unknown state (given multiple copies)

- ❑ One qubit

$\vec{r} = (r_x, r_y, r_z)$

$$\boxed{\rho = \frac{1}{2}(I + r_x\sigma_x + r_y\sigma_y + r_z\sigma_z)}$$

$$\begin{cases} r_x = tr(\rho\sigma_x) = tr(\rho|+\rangle\langle+|) - tr(\rho|-\rangle\langle-|) \\ r_y = tr(\rho\sigma_y) = tr(\rho|+i\rangle\langle+i|) - tr(\rho|-i\rangle\langle-i|) \\ r_z = tr(\rho\sigma_z) = tr(\rho|0\rangle\langle0|) - tr(\rho|1\rangle\langle1|) \end{cases}$$



Bloch sphere

+/−
±i
0/1

⇒ measure in +/− ⇒ r_x
⇒ ±i ⇒ r_y
⇒ 0/1

➔ If one can measure the qubit in all three bases, can extract Bloch vector $\vec{r}$

- ❑ Multi-qubits:

expand in terms of product of pauli

by measuring in corresponding basis

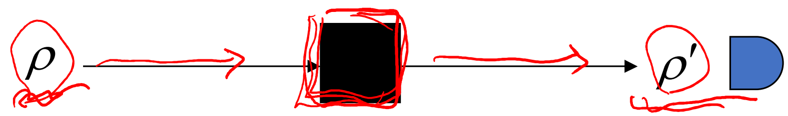
$$\rho_{2-qubit} = \frac{1}{4}\sum_{\mu\nu} r_{\mu\nu}\sigma_\mu \otimes \sigma_\nu\,, \qquad r_{\mu\nu} = tr\left(\rho_{2-qubit}\,\sigma_\mu \otimes \sigma_\nu\right)$$

① — σ_x
② — σ_y

➔ Measure in product of bases (i.e. coincidence)

Quantum process tomography

- ❑ Estimate unknow process (Black box)



state tomography on ρ'

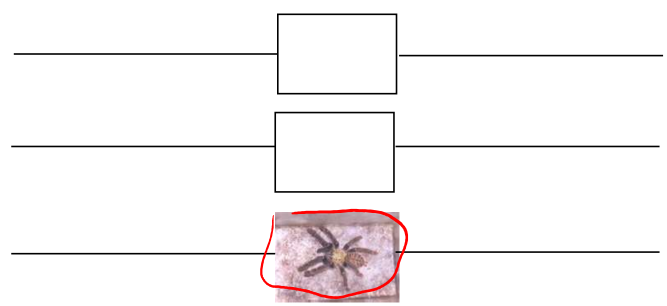
$$E: \rho \rightarrow \sum_i E_i \rho E_i^\dagger$$

(quantum operations) by state tomo.

know input ρ $\longrightarrow$ know out ρ'

- ❑ Possible application: "debugging" quantum gates

quantum circuit:



Q: From measuring a limited number of different input states (but unlimited supply of each), is it possible to predict the result for a general input state?

Three different ways of implementing quantum process tomography (PT)

(I) Standard Quantum PT (SQPT)

- Idea: look at how each element gets transformed

$$E: \underbrace{|j\rangle\langle k|} \rightarrow \sum_i E_i \underbrace{|j\rangle\langle k|} E_i^\dagger$$

$\rho = \begin{pmatrix} \rho_{00} & \rho_{01} \\ \rho_{10} & \rho_{11} \end{pmatrix}$ if I know $\rho_{ij} \longrightarrow \rho'_{ij}$

$|j\rangle\langle k|$ for single qubit are

general state $\sum_{ij} \rho_{jk} |j\rangle\langle k|$

$$|0\rangle\langle 0|$$

$$|0\rangle\langle 1| = |+\rangle\langle +| + i|{+i}\rangle\langle {+i}| - \frac{1+i}{2}|0\rangle\langle 0| - \frac{1+i}{2}|1\rangle\langle 1|$$

$$|1\rangle\langle 0| = |+\rangle\langle +| - i|{+i}\rangle\langle {+i}| - \frac{1-i}{2}|0\rangle\langle 0| - \frac{1-i}{2}|1\rangle\langle 1|$$

$$|1\rangle\langle 1|$$

➔ We only need four different inputs $|0\rangle, |1\rangle, |+\rangle, |+i\rangle$

$\rho \in \{|0\rangle, |1\rangle, |+\rangle, |+i\rangle\}$

ρ'

to figure out the unknown action