

Quantum Computing With Noisy Qubits

William Schiela, Mehdi Hatefipour
Instructor: Javad Shabani

Fall 2019

Abstract

These are class notes from New York University, PHYS-GA-2023 (Special Topics in Condensed Matter Physics): Quantum Computing with Noisy Qubits.

Contents

1	Basics	2
1.1	Photon polarization	2
1.2	Dirac's bra/ket notation	3
1.3	Single qubit measurement	3
1.4	Example	4
2	BB84 protocol	5
2.1	Example	5
3	Single qubit: Bloch sphere	8
3.1	Arbitrary 2-level quantum system	9
3.2	Spin in a generalized magnetic field	11
3.3	LC oscillator as a superconducting qubit	11
4	Josephson junctions	11
4.1	Josephson junction as qubit	13
4.1.1	Lagrangian for a Cooper pair box	14
5	Multiple qubits	17
5.1	Direct sum of vector spaces	17
5.2	Tensor products of vector spaces	18
5.3	Meaning of entanglement	19
5.3.1	Multi-qubit measurements	19
5.3.2	EPR paradox	20
6	Quantum gates	21
6.1	Single-qubit gates	21
6.2	Two-qubit gates	22

7	Superdense coding	22
8	Density matrices	23
9	Quantifying entanglement	24
9.1	Schmidt decomposition	24
9.2	Entropies	25
9.2.1	Shannon entropy	25
9.2.2	Von Neumann entropy	25
10	Mixed vs. pure states	26
10.1	Reduced density matrix	27
10.2	Quantifying entanglement in mixed states	28
11	Some standard results, protocols, and other bits and bobs	28
11.1	No-cloning theorem	28
11.2	Quantum teleportation	28
11.3	GHZ states	29
11.4	CHSH game	30
11.4.1	Classical version	30
11.4.2	Quantum version	30
11.4.3	Einstein-certified randomness	30
12	Computational complexity	31
12.1	Complexity classes	31
12.2	3-SAT	32
A	Python & Qiskit: Installation & Introduction	33
B	Guest lecture: Quantum algorithms	33
C	Additional Problems	33

1 Basics

Quantum bit

- fundamental units of information in quantum information processing
- we rarely concern ourselves with how the qubits are realized (NOT IN THIS COURSE, here we *do* care)

2-level qubits, 3-level qutrits, n -level qudits.

1.1 Photon polarization

Imagine you have a light source producing a beam of light on a projection screen. Now let's add a polaroid A in between (let's assume polarization of the polaroid is horizontal)

\implies intensity of light is reduced

Let's add a polaroid C which is rotated so that its polarization is orthogonal (vertical) to polaroid A .

\implies no light will reach the screen

Let's add polaroid B in between A and C . Surprisingly at most polarization angles of B (maximal if set at 45°) there will be light.

- For a bright beam of light there is a classical explanation in terms of waves
- We can repeat this for only one photon at a time \implies the results can only be described with quantum mechanics:
 1. A model of a photon's polarization
 2. A model of the interaction between a polaroid and a photon.

The description of this experiment (or qubit) uses linear algebra as vector, basis,

...

QM models a photon polarization state by a unit vector $|\uparrow\rangle, |\leftrightarrow\rangle$.

\implies Arbitrary vector: $|v\rangle = a|\uparrow\rangle + b|\leftrightarrow\rangle$.

e.g. $|45^\circ\rangle = \frac{1}{\sqrt{2}}[|\uparrow\rangle + |\leftrightarrow\rangle]$

When a and b are, $|v\rangle = a|\uparrow\rangle + b|\leftrightarrow\rangle$ with $a^2 + b^2 = 1$ is said to be a *superposition* of $|\uparrow\rangle$ and $|\leftrightarrow\rangle$.

In general, $|v\rangle = a|\uparrow\rangle + b|\leftrightarrow\rangle$ a qubit has a continuum of possible values. (3 unknowns = 2 amplitudes + 2 phases - 1 normalization constraint)

Amplitudes a and b can be complex numbers.

Qubit is any quantum mechanical system that can be modeled by a 2D complex vector space. E.g. photon polarization, electron spin, etc.

The two state label does *not* mean these systems have only two states in their state space (in fact it is infinite).

1.2 Dirac's bra/ket notation

Used to represent the quantum state and its evolution. (A ket $|x\rangle$ refers to a vector representing the quantum state.)

A vector $|v\rangle = a_1|s_1\rangle + a_2|s_2\rangle + \dots + a_n|s_n\rangle \in V$ is a linear combination of vectors in set $S = \{|s_1\rangle, \dots, |s_n\rangle\}$.

The set S generates a complex vector space V .

A set of vectors B for which every element of V can be written uniquely as a linear combination of vectors in B is called a *basis* for V . (QM bases are usually assumed orthonormal).

Inner product $\langle v_1|v_2\rangle = \langle v_2|v_1\rangle$ is *non-negative*. Orthonormal $\langle\beta_1|\beta_2\rangle = 0$. Length $\langle v_1|v_1\rangle$.

Basis $\{|\beta_1\rangle, |\beta_2\rangle\}$. Ket $|v\rangle = a|\beta_1\rangle + b|\beta_2\rangle \doteq \begin{pmatrix} a \\ b \end{pmatrix}$. Kets (bras) are represented by column (row) matrices. Inner product, projection, superposition, etc. etc. etc.

1.3 Single qubit measurement

Interaction of polaroid with a photon \implies probabilistic outcomes *and* effect of the measurement on the state of the system.

Measurement of a quantum state changes the state.

Whenever anyone says “measure a qubit” they must specify with respect to which basis the measurement takes place. Any measurement is worthless without identifying the basis of the measurement.

¹Any device that measures a two-state quantum system must have two preferred states $\{|u\rangle, |u^\perp\rangle\}$. Must transform state to measurement basis.

If a state $|v\rangle = a'|u\rangle + b'|u^\perp\rangle$ is measured as $|u\rangle$ then the state $|v\rangle$ changes to $|u\rangle$. A 2nd measurement with respect to the same basis will return $|u\rangle$ with probability 1.

A single measurement will change the state, making it impossible to determine the original state from any sequence of measurements.

Superposition and measurement are basis dependent. Example:

$$\left. \begin{array}{l} \text{Cat: } 0 \quad \text{or} \quad 1 \\ \text{Qubit: } a|0\rangle + b|1\rangle \end{array} \right\} \xrightarrow{\text{Measurement}} \begin{cases} p^2 \\ |a|^2 \end{cases}$$

Single measurement can mask classical vs. quantum nature/origin of probability.

$|v\rangle$ is a definite state. When measured in certain bases, \rightarrow deterministic results 1. In others, probabilistic result 1/2.

The qubit can take on any of infinitely many states. One might hope that a single qubit could store lots of classical information. However, the properties of quantum measurement *SEVERELY* restrict the amount of information that can be extracted. A single quantum measurement yields at most one classical bit of information. Since measurement changes the state, one cannot make two measurements on the original state of the qubit.

1.4 Example

Question:

Suppose that you have a system of N qubits. How many classical bits does it take to describe the state of the system? First, consider a quantum register containing three qubits, each of which is prepared in state

$$\frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

You perform a measurement that projects each qubit onto either $|0\rangle$ or $|1\rangle$ and record the result in a 3-bit classical register. List all possible outcomes.

Answer:

First we consider a system of 3 qubits, all of them in the state $(|0\rangle + |1\rangle)/\sqrt{2}$, so the combined wave function is:

$$|\psi\rangle = \frac{1}{2\sqrt{2}} (|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle).$$

¹9/11/19

If we measure each qubit in the $\{|0\rangle, |1\rangle\}$ basis, we can have 8 possible outcomes: $|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle$ all with probability $1/8$.

In general, the Hilbert space of N qubits can be expanded as the tensor product of the Hilbert spaces of each of its qubits. This allows us to define a basis in the space of all qubits as the tensor product of all the possible combinations of the basis elements of the single qubit states: $\{|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle\}$ in the case of three qubits. In a system of N qubits the number of basis elements is therefore 2^N . Therefore, to fully characterize the state of an N qubit system we need to specify 2^N complex numbers (or, more precisely, $2^N - 1$ due to the normalization constraint and the ability to ignore an overall global phase, which removes two real parameters, or equivalently one complex parameter). Because the parameters specifying the state are continuous, they cannot be represented precisely/exactly with a finite number of bits, in general.

This exponential scaling of the size of the Hilbert space with the number of qubits is the reason why it is not possible to efficiently simulate quantum computers with classical ones.

A final note about representing a many-body quantum state with a finite number of bits: we are making a rounding error on each component of the wave function, therefore the wave function that we are representing is an approximation ($|\psi_{\text{Approx}}\rangle$) to the exact one ($|\psi\rangle$). We want to have a good approximation so: $\langle\psi_{\text{Approx}}|\psi\rangle \sim 1$. However, this approximation gets intrinsically worse as the number of qubits increases if the precision in the bits is not increased. This a consequence of something known as the **orthogonality catastrophe**. Imagine we can represent our single qubit states with an error ε :

$$\langle\psi_{\text{Approx}}^{(i)}|\psi^{(i)}\rangle = 1 - \varepsilon,$$

where (i) labels qubit (i) . If we form a many-qubit state as the product of the approximate states, its overlap will decay exponentially with the number of qubits:

$$\langle\psi_{\text{Approx}}|\psi\rangle = (1 - \varepsilon)^N \sim e^{-\varepsilon N}.$$

Therefore to accurately describe our quantum many-body states we need a lot of classical bits for each of the exponentially many wave function components.

2 BB84 protocol

²App. A.

2.1 Example

Question :

Alice and Bob have two methods of communication: they can communicate classically (by text messages) and they can communicate quantumly (Alice can send Bob single photons over an optical fiber). It is possible for other people to hack into both of these methods of communication. They agree that Alice will encode a string of ‘0’s and ‘1’s in the polarization state of photons. If they can verify no one intercepted this

string, they will use it as their secret key. They agree to use the following mapping:

$$|\leftrightarrow\rangle \rightarrow 1$$

$$|\updownarrow\rangle \rightarrow 0$$

Alice will send a photon with its polarization oriented either horizontally or vertically. She will choose the polarization randomly, with equal probability for either. She will also text Bob telling him that she sent a photon, without telling which polarization she sent. Bob will measure the photon and text her back to confirm that he received it, without telling her anything about how he measured the photon or the measurement outcome.

- a. How can Bob measure the polarization of the photon that Alice sends? List two ways and explain why one would be better than the other.
- b. If Bob measures a vertically polarized photon, with what percent certainty does he know which polarization Alice sent?
- c. Now suppose there's an eavesdropper named Eve. She is able to intercept the photon Alice sends to Bob, detect it, and send Bob a replacement photon. If she overhears all of the discussions Bob and Alice have about their plan to share the secret key, is it possible for her to know the polarization state of every photon Alice sends with 100% certainty?
- d. Assuming that Eve is able to send the replacement photon instantaneously, would Alice and Bob know that she has eavesdropped? Why or why not?
- e. Explain why it is not secure for Alice to tell Bob in which basis she is sending photons.
- f. In the BB84 protocol, Alice and Bob still have the same two ways of communicating (text messages and single photons), but Alice now has an additional choice of sending light polarized horizontally, vertically, or with one of the two diagonal polarizations. They agree to use the same mapping as in Equation 1 for horizontally or vertically polarized photons, and the following mapping for the diagonally polarized photons:

$$|\nearrow\rangle \rightarrow 0$$

$$|\nwarrow\rangle \rightarrow 1$$

Alice now randomly sends any of the four polarization states with equal probability. Bob doesn't know which basis Alice used, so he randomly chooses a basis (horizontal/vertical or diagonal) in which to measure the photon.

- g. Fill in the empty spaces in the following table. What is the secret key that Alice and Bob generate?

Answer:

- a. 1) Bob can use a filter like an absorptive polarizer which lets light polarized in a particular direction pass while blocking light polarized in the orthogonal direction. If his filter is oriented to accept either horizontally or vertically polarized light, his single-photon detector will either detect a photon (which

Alice's bit	1	1	0	1	0	0	0	1	0
Alice's basis	+	×	×	+	×	+	+	×	×
Alice's polarization	\leftrightarrow	\nearrow	\nwarrow						
Bob's basis	×	×	+	+	+	×	+	×	+
Bob's measurement	\nwarrow	\nwarrow	\updownarrow		\nearrow	\nwarrow			\leftrightarrow
Same basis?	No	Yes							
Shared secret key									

means the polarization of the photon was the same as the direction of the filter) or nothing (which means the polarization of the photon sent was perpendicular to the filter). Using this method, he will only detect photons of one particular polarization.

- 2) Alternatively, Bob can use a polarizing beam splitter, with a single-photon detector positioned at each arm. If the beam splitter is oriented to transmit vertically polarized light and reflect horizontally polarized light, Bob will be able to detect the arrival of all photons and determine each's polarization.

The second option is better because Bob is able to detect all photons using single-photon detectors and thereby determine each's polarization. In the first option, photons polarized perpendicular to the filter will be absorbed (i.e. annihilated), and it will be very difficult (though not physically impossible) to know that a photon was received at all.

- b. The horizontal and vertical polarization states are orthogonal, i.e. $\langle \leftrightarrow | \updownarrow \rangle = \langle \updownarrow | \leftrightarrow \rangle = 0$. Therefore, if Alice prepares only $|\leftrightarrow\rangle$ or $|\updownarrow\rangle$ photons, and Bob measures a $|\updownarrow\rangle$ photon, he knows with 100% certainty that Alice prepared a $|\updownarrow\rangle$ photon.
- c. Yes. It is assumed that Alice and Bob use the classical communication channel to agree upon which measurement basis to use. Since Eve has access to this channel, she will also know the measurement basis. Therefore, in the same way Bob can determine with 100% certainty the polarization state that Alice sends, Eve can also use a polarizing beam splitter to transmit $|\updownarrow\rangle$ and reflect $|\leftrightarrow\rangle$ and thereby determine the polarization state with 100% certainty.
- d. No. Once Eve knows the polarization state, she can prepare an identical copy (in the same way that Alice does) and relay it to Bob. Bob will then measure the same state that Alice prepared, which Eve reproduced. Since it is assumed that Eve can do this instantaneously, there is no delay in the transmission between Alice and Bob, and they cannot use timing records to detect any meddling by Eve. When Alice and Bob later compare notes over the classical communication channel, Bob's measurement outcomes will be 100% correlated with the states Alice prepared.
- e. As already explained in the previous parts, it is not secure for Alice to tell Bob which measurement basis she is using (assuming *only one* basis is being used) because Eve has access to both the classical communication channel and the quantum communication channel, and therefore knows everything that Bob knows. If

Alice's bit	1	1	0	1	0	0	0	1	0
Alice's basis	+	×	×	+	×	+	+	×	×
Alice's polarization	↔	↖	↗	↔	↗	↕	↕	↖	↗
Bob's basis	×	×	+	+	+	×	+	×	+
Bob's measurement	↖	↖	↕	↔	↗ ¹	↖	↕	↖	↔
Same basis?	No	Yes	No	Yes	No	No	Yes	Yes	No
Shared secret key		1		1			0	1	

¹ This is incorrect in the given table.

Table 1: Table for problem 2 part g.

Alice tells Bob the basis she is using, Eve will also know the basis. She can then intercept the photon, measure the polarization, and relay an identical copy to Bob. In this way she can determine the states of all the photons Alice sends and not be detected.

Yet Bob *needs* to know the basis Alice is using so that he can appropriately orient his beam splitter. Clearly, this scheme involving one basis will not work. *We need to employ a second basis.*

- f. This is just a description of the BB84 setup. The key is that Bob knows the two bases being used, but he doesn't *which* basis Alice will use for each photon.
- g. See table 1

3 Single qubit: Bloch sphere

³Spin:

$$H_0 = \frac{e}{m} B_0 \hat{S}_z \quad (1)$$

Energy level splitting due to B -field: $\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$. Rotation matrices:

$$R_x(\theta) = \begin{pmatrix} \cos \theta & -i \sin \theta \\ i \sin \theta & \cos \theta \end{pmatrix}, \quad R_z(\theta) = \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix}$$

Bloch sphere, $|0\rangle$ and $|1\rangle$ at north and south poles, θ polar and φ azimuthal angles (i.e. spherical coordinates). Arbitrary state:

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right) |0\rangle + e^{i\varphi} \sin\left(\frac{\theta}{2}\right) |1\rangle$$

E.g. π -pulse, pulse length Δt defined by

$$\omega \Delta t = \Delta \varphi = \pi \implies \Delta t = \frac{\pi}{\omega}.$$

Need to be able to do Bloch-sphere rotations about multiple axes. Introduce perturbation to spin Hamiltonian:

$$\begin{aligned} \hat{H} &= \frac{e}{m} B_0 \hat{S}_z + \frac{e}{m} B_1 \cos \omega_0 t \hat{S}_x \quad \text{where } B_1 \ll B_0 \\ &= \frac{e\hbar}{2m} \begin{pmatrix} B_0 & B_1 \cos \omega_0 t \\ B_1 \cos \omega_0 t & -B_0 \end{pmatrix} \end{aligned}$$

Since the second term is treated as a perturbation, x -rotations are much slower than z -rotations. Time-dependent state:

$$|\psi(t)\rangle = \cos \frac{\omega_1 t}{2} |0\rangle + e^{i(\omega_0 + \pi)t} \sin \frac{\omega_1 t}{2} |1\rangle$$

$$\text{where } \begin{cases} \theta = \omega_1 t \\ \omega_1 = \frac{eB_1}{2m} \end{cases}$$

3.1 Arbitrary 2-level quantum system

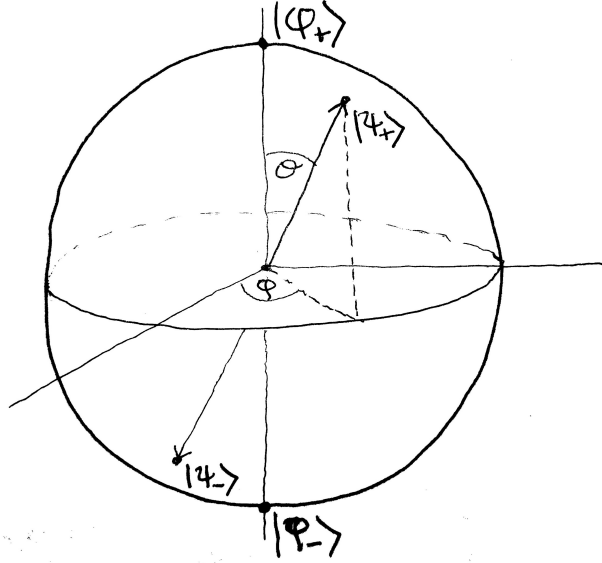


Figure 1: Eigensystem of a general 2-level quantum system on the Bloch sphere. $|\varphi_{\pm}\rangle$ are the eigenstates of the pure-diagonal Hamiltonian (e.g. the spin Hamiltonian (1)), while $|\psi_{\pm}\rangle$ are the eigenstates of the general Hamiltonian with off-diagonal elements.

[Cohen-Tannoudji, Diu, Laloe; Quantum Mechanics Vol. 1] Most general 2×2 Hermitian matrix:

$$\hat{H} = \frac{1}{2} \begin{pmatrix} H_{11} & H_{12} \\ H_{21} & H_{22} \end{pmatrix} \quad \text{where } H_{12}^* = H_{21}, \quad \text{and } H_{11}, H_{22} \in \mathbb{R}$$

Take $H_{11} > H_{22}$ without loss of generality.

Move zero of energy to midway between the levels:

$$\begin{aligned}
H \rightarrow \hat{H} - \frac{H_{11} + H_{22}}{4} \otimes \mathbb{1} &= \frac{1}{2} \begin{pmatrix} \frac{H_{11}-H_{22}}{2} & H_{12} \\ H_{21} & -\frac{H_{11}+H_{22}}{2} \end{pmatrix} \\
&\equiv \frac{1}{2} \begin{pmatrix} \epsilon & \Delta - i\tilde{\Delta} \\ \Delta + i\tilde{\Delta} & -\epsilon \end{pmatrix} \\
&= \frac{\epsilon}{2} \hat{\sigma}_z + \frac{\tilde{\Delta}}{2} \hat{\sigma}_y + \frac{\Delta}{2} \hat{\sigma}_x
\end{aligned}$$

Take $H_0 = \frac{1}{2} \begin{pmatrix} \epsilon & 0 \\ 0 & -\epsilon \end{pmatrix} = \frac{\epsilon}{2} \hat{\sigma}_z$ with eigenvectors $|\varphi_{\pm}\rangle$,

$$H_0 |\varphi_{\pm}\rangle = \pm \frac{\epsilon}{2} |\varphi_{\pm}\rangle,$$

as the north and south pole of the Bloch sphere (see Fig. 1). Then introduce the off-diagonals

$$H = H_0 + H_1, \quad \text{where} \quad H_1 = \frac{1}{2} \begin{pmatrix} 0 & \Delta - i\tilde{\Delta} \\ \Delta + i\tilde{\Delta} & 0 \end{pmatrix}.$$

Solve for the eigensystem:

$$\begin{aligned}
H |\psi_{\pm}\rangle &= E_{\pm} |\psi_{\pm}\rangle \\
\det \begin{pmatrix} \epsilon - 2E_{\pm} & \Delta - i\tilde{\Delta} \\ \Delta + i\tilde{\Delta} & -\epsilon - 2E_{\pm} \end{pmatrix} &= 0 \\
E_{\pm} &= \pm \frac{1}{2} \sqrt{\epsilon^2 + \Delta^2 + \tilde{\Delta}^2} \\
&\equiv \pm \frac{1}{2} \hbar \omega_q
\end{aligned}$$

$$|\psi_{+}\rangle = e^{-i\varphi/2} \cos \frac{\theta}{2} |\varphi_{+}\rangle + e^{i\varphi/2} \sin \frac{\theta}{2} |\varphi_{-}\rangle$$

$$|\psi_{-}\rangle = e^{-i\varphi/2} \sin \frac{\theta}{2} |\varphi_{+}\rangle + e^{i\varphi/2} \cos \frac{\theta}{2} |\varphi_{-}\rangle$$

This orients the $|\psi_{\pm}\rangle$ axis at polar angle θ and azimuthal angle φ relative to the $|\varphi\rangle$ axis (see Fig. 1), where

$$\begin{aligned}
\tan \theta &= \frac{\sqrt{\Delta^2 + \tilde{\Delta}^2}}{\epsilon} \\
\tan \varphi &= \frac{\tilde{\Delta}}{\Delta}
\end{aligned}$$

3.2 Spin in a generalized magnetic field

We can map the results of Sec. 3.1 to the spin problem as follows:

$$\begin{aligned}
|\uparrow\rangle &\longrightarrow |\varphi_+\rangle \\
|\downarrow\rangle &\longrightarrow |\varphi_-\rangle \\
|\uparrow\rangle_y &\longrightarrow |\psi_+\rangle \\
|\downarrow\rangle_y &\longrightarrow |\psi_-\rangle \\
\hbar\gamma B &\longrightarrow \hbar\omega_q \\
B_z &\longrightarrow \epsilon \\
B_x &\longrightarrow \Delta \\
B_y &\longrightarrow \tilde{\Delta}
\end{aligned}$$

$$H = -\frac{\gamma\hbar}{2} \begin{pmatrix} B_z & B_x - iB_y \\ B_x + iB_y & -B_z \end{pmatrix}$$

With a static field $\vec{B} = B_x\hat{x} + B_y\hat{y} + B_z\hat{z}$, a general state just precesses about the new eigenaxis (the $|\psi_{\pm}\rangle$ axis in Fig. 1). With a time-dependent perturbation in the field, $\vec{B} = B_z\hat{z} + B_1\cos(\omega_0 t)\hat{x}$ where $B_1 \ll B_0$, we can get fast precession about the z -axis and slow precession about the x -axis.

3.3 LC oscillator as a superconducting qubit

Frequency: $f = 1/\sqrt{LC} \sim \hbar\omega$.

$$\hat{H} = \frac{1}{2}\hbar\omega_a\hat{\sigma}_z + \hbar\Omega_R\cos(\omega_0 t + \Phi_R)\hat{\sigma}_x$$

LC oscillator has same spectrum as simple harmonic oscillator; evenly-spaced energy levels. Need to introduce anharmonicity via a nonlinear component to break this even spacing so that a single transition between 2 specific levels (qubit) can be addressed. This nonlinear component is the Josephson junction, characterized by a current-phase relationship (CPR).

4 Josephson junctions

⁴E.g. Al–AlO_x–Al, capacitor at room temperature.

Quantum resistance:

$$R_Q = h/e^2 \approx 25.8 \text{ k}\Omega$$

Two coupled Schrödinger equations (one on each side of the junction):

$$i\hbar\frac{\partial\Psi_1}{\partial t} = \mu_1\Psi_1 + K\Psi_2$$

⁴10/7/19

$$i\hbar \frac{\partial \Psi_2}{\partial t} = \mu_2 \Psi_2 + K \Psi_1$$

where K is the coupling across the barrier.

$$\Psi_1 = \sqrt{n_1} e^{i\theta_1}$$

$$\Psi_2 = \sqrt{n_2} e^{i\theta_2}$$

where $n_{1,2}$ are the density of Cooper pairs and $\theta_{1,2}$ are the phases.

$$\hbar \frac{\partial n_1}{\partial t} = -\hbar \frac{\partial n_2}{\partial t} = 2K \sqrt{n_1 n_2} \sin(\theta_2 - \theta_1)$$

$$-\hbar \frac{\partial}{\partial t} (\theta_2 - \theta_1) = \mu_2 - \mu_1$$

Then note current $\sim \frac{\partial n}{\partial t}$. Define $\phi = \theta_2 - \theta_1$, and $I_0 = 2K \sqrt{n_1 n_2} / \hbar$, yielding

$$I = \frac{\partial n_1}{\partial t} = I_0 \sin \phi$$

$$\frac{\partial \phi}{\partial t} = \frac{2e}{\hbar} V$$

where I is known as the supercurrent, first equation known as “current-phase relationship.”

Harmonic oscillator, Schrödinger equation:

$$\left[\frac{-\hbar^2}{2m} \nabla^2 + \frac{1}{2} m \omega^2 x^2 \right] \psi = E \psi$$

$H = T + V$. Solution:

$$E_n = \hbar \omega \left(n + \frac{1}{2} \right)$$

$$\psi_n = A_n (\hat{a}_+)^n \psi_0(x)$$

$$a_{\pm} = \frac{1}{\sqrt{2\hbar\omega m}} (m\omega \hat{x} \mp i\hat{p})$$

Introducing nonlinearity:

$$H = H_0 + \lambda x^4$$

where $H_0 \psi_n = E_n \psi_n$. Then,

$$E_0 = E_0^0 + \lambda E_n^1.$$

Expand x^4 in terms of raising and lowering operators, $x \sim a_- + a_+$ to calculate

$$E_n^{(1)} = \langle \Psi_n | x^4 | \Psi_n \rangle = (6n^2 + 6n + 3) \left(\frac{\hbar}{2m\omega} \right)^2 \lambda$$

Each energy level shifts by a different amount, no longer even spacing between levels.

4.1 Josephson junction as qubit

Classical first:

$$H = T + V \quad \mathcal{L} = T - V$$

Euler-Lagrange equations:

$$\begin{aligned} \frac{d}{dt} \frac{\partial \mathcal{L}}{\partial v_i} - \frac{\partial \mathcal{L}}{\partial x_i} &= 0 \\ \mathcal{L} &= \frac{1}{2}mv^2 - v(x) \\ \dot{x} &= \frac{\partial H}{\partial p} \quad \dot{p} = -\frac{\partial H}{\partial x} \end{aligned}$$

Oscillators:

$$\begin{aligned} \mathcal{L} = T - V &= \frac{1}{2}C\dot{\Phi}^2 - \frac{1}{2L}\Phi^2 \\ Q &= \frac{\partial \mathcal{L}}{\partial \dot{\Phi}} = C\dot{\Phi} = CV \\ H &= \frac{Q^2}{2C} + \frac{\Phi^2}{2L} \equiv \frac{p^2}{2m} + \frac{1}{2}kx^2 \end{aligned}$$

i.e. a harmonic oscillator with “mass” C and “spring constant” $1/L$, natural frequency $\omega_c = 1/\sqrt{LC}$.

Now quantize Hamiltonian: $Q \rightarrow \hat{Q}$ and $\Phi \rightarrow \hat{\Phi}$, note $[Q, \Phi] = -i\hbar$. Operators Q , Φ can be written as raising and lowering operators:

$$\Phi = \Phi_{\text{z.p.}} (a_- + a_+) \quad (2)$$

$$Q = -iQ_{\text{z.p.}} (a_- - a_+) \quad (3)$$

where “z.p.” = zero-point,

$$\Phi_{\text{z.p.}} = \sqrt{\frac{\hbar Z}{2}} \quad Q_{\text{z.p.}} = \sqrt{\frac{\hbar}{2Z}}$$

where $Z = \sqrt{L/C}$ is characteristic impedance. If the characteristic impedance is on the order of quantum resistance h/e^2 , then $Q_{\text{z.p.}}$ is on the order of the electron charge, and $\Phi_{\text{z.p.}}$ is on the order of the flux quantum.

Consider the input admittance of a parallel LC resonator:

$$Y(\omega) = i\omega C + \frac{1}{i\omega L} = \frac{1}{2Z} \left(\frac{\omega_c}{\omega} \right) \left(1 - \left(\frac{\omega}{\omega_c} \right)^2 \right)$$

The Hamiltonian is given by $H = \hbar\omega_c a_+ a_-$ and physical observables flux $\hat{\Phi}$ and charge \hat{Q} that are given by Eqs. (2), (3).

⁵Superconducting qubit: In order to go beyond the simple LC harmonic oscillator to create a qubit, we need a nonlinear element to produce anharmonicity in the spectrum. A number of qubit designs have been developed around Josephson junctions including:

- Cooper pair box based on charge
- flux qubit

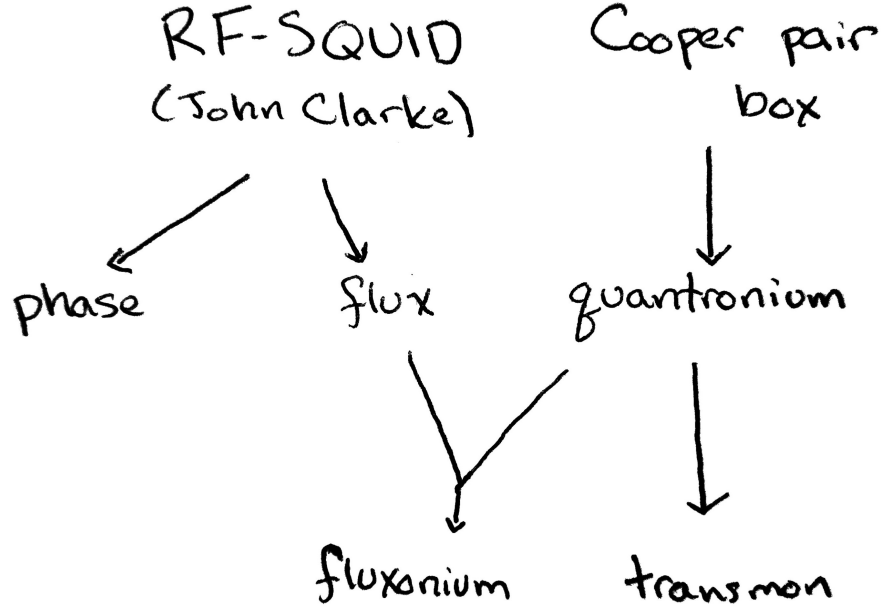


Figure 2: Family tree of superconducting qubits.

- phase qubit
- fluxonium qubit.

Cooper pair box is topologically distinct from the other designs in that it has no wire closing the loop around the junction. It consists very simply of a small antenna whose two halves are connected by a Josephson junction.

⇒ Two sides of the junction are not shunted by an inductor.

⇒ # Cooper pairs transferred through the junction is a well-defined integer.

$[Q, \Phi] = -i\hbar \Rightarrow$ periodicity of spectrum in charge.

⇒ charge-based qubits are sensitive to stray electric field noise.

4.1.1 Lagrangian for a Cooper pair box

Similar to the LC oscillator except unlike the inductor the energy stored in the Josephson junctions is not quadratic but periodic.

$$\mathcal{L} = \frac{1}{2}C_{\Sigma}\dot{\Phi}^2 + E_J \cos \phi$$

where ϕ is phase difference of superconducting order parameter across the JJ,

$$\phi = 2\pi \frac{\Phi}{\Phi_0} = \frac{2e}{\hbar}\Phi$$

with $\Phi_0 = h/2e$, and $C_{\Sigma} = C_{\text{geometry}} + C_J$, thus,

$$\mathcal{L} = \frac{1}{2}C_{\Sigma} \left(\frac{\hbar}{2e} \right)^2 \dot{\phi}^2 + E_J \cos \phi.$$

From Euler-Lagrange,

$$n = \frac{\partial \mathcal{L}}{\partial \dot{\phi}} = \frac{\hbar^2}{4e^2} C_{\Sigma} \dot{\phi}$$

yielding the Hamiltonian,

$$\mathcal{H} = 4E_C(\hat{n} - n_g)^2 - E_J \cos \phi$$

where $E_C = e^2/2C_{\Sigma}$ is charging energy, $n = -i \partial/\partial \phi$ operator, and n_g is the so-called offset charge representing external bias voltage and also containing random fluctuations due to stray charges jumping around.

In the limit $E_J \gg E_C$, the low-frequency noise in the offset charge can be neglected, resulting in very long coherence times \Rightarrow “transmon qubit.” With $E_J \gg E_C$ the “gravitational force” is very strong, and the “moment of inertia” is very large, so the phase angle undergoes very small quantum fluctuations.

$$H_0 = 4E_C \hat{n}^2 + \frac{E_J}{2} \hat{\phi}^2$$

$$V = E_J \left[-\hat{\phi}^4/4! + \dots \right].$$

We see H_0 is the Hamiltonian of a simple LC harmonic oscillator with frequency $\hbar\Omega = \sqrt{8E_J E_C}$ and with leading order effect of the JJ being to play the role of a relatively large linear inductor. In the limit $E_J \gg E_C$, we are effectively ignoring the fact that $\hat{\phi}$ is an angular variable. It is this assumption which makes conjugate momenta \hat{n} have continuous rather than integer values.

Example

Q:

Using the current-phase and voltage-phase relationship of a single Josephson junction:

- (a) derive the inductance of a Josephson junction?
- (b) can it be zero? How about negative?
- (c) calculate the Josephson energy.
- (d) Now consider our junction is made out of aluminum leads separated by $d = 1.2nm$ (at this thickness the resistivity is $5k\Omega/square$) with area A. An ideal junction satisfies: $I_c R_n = \Delta$ where I_c is the supercurrent, R_n is the normal resistance and Δ is the superconducting gap. What is the resonant frequency of this junction?
- (e) Imagine we take the junction and bias it with 10 micro volt of DC voltage. We then monitor the current with an ideal oscilloscope. What frequency do we detect?

A:

- a) The Josephson effect describes the supercurrent I_J that flows through the junction according to the classical equations

$$I_J = I_c \sin \delta, \tag{4}$$

$$V = \frac{\Phi_0}{2\pi} \frac{d\delta}{dt} \quad (5)$$

where $\Phi_0 = \frac{h}{2e}$ is the superconducting flux quantum, I_c is the critical-current parameter of the junction, and δ and V are respectively the superconducting phase difference and voltage across the junction. The dynamical behavior of these two equations can be understood by first differentiating Eq. (4) and replacing $\frac{d\delta}{dt}$ with V according to Eq.(5)

$$\frac{dI_J}{dt} = I_c \cos \delta \frac{2\pi}{\Phi_0} V.$$

With $\frac{dI_J}{dt}$ proportional to V , this equation describes an inductor. By defining a Josephson inductance L_J according to the conventional definition $V = L_J \frac{dI_J}{dt}$, one finds

$$L_J = \frac{\Phi_0}{2\pi I_c \cos \delta}. \quad (6)$$

- b) The magnitude of the inductance becomes large as $\delta \rightarrow \frac{\pi}{2}$ or $\frac{3\pi}{2}$, and is negative for $\frac{\pi}{2} < \delta < \frac{3\pi}{2}$. But it cannot be zero because $\cos \delta$ is bounded on $[-1, 1]$.
- c) The energy stored in the junction is given by

$$\begin{aligned} U_J &= \int I_J V dt \\ &= \int I_c \sin \delta \frac{\Phi_0}{2\pi} \frac{d\delta}{dt} dt \\ &= \frac{I_c \Phi_0}{2\pi} \int_0^\delta \sin \delta' d\delta' \\ &= \frac{I_c \Phi_0}{2\pi} (1 - \cos \delta) \end{aligned}$$

- d) The resonant frequency of an LC circuit is

$$\omega_0 = \frac{1}{\sqrt{LC}}$$

where the capacitance $C = \epsilon A/d$ with $d = 1.2 \text{ nm}$ contact separation, A is the area of the interface between the superconducting aluminum contacts and the insulating medium between them, and ϵ is the dielectric constant of the insulator. The inductance $L = L_J$, as given in Eq. (6), depends on the critical current I_c , which can be obtained from the product

$$I_c R_n = \Delta \implies I_c = \Delta / R_n$$

where Δ is the superconducting gap, and the normal resistance of the junction $R_n = \rho d/A$, with ρ the resistivity. Then

$$\omega_o = \frac{1}{\sqrt{\frac{\Phi_0}{2\pi \cos \delta} \frac{\rho \epsilon}{\Delta}}}$$

Note there is some ambiguity in the resistivity provided in the problem. Normally, resistivity has units of [resistance-length], whereas the resistivity given in the problem

has units of [resistance-length⁻²]. If we assume $\rho = 5 \text{ k}\Omega/\text{length}^2$ as given in the problem, and take $R_n = \rho A$, then we obtain

$$\omega_o = \frac{1}{\sqrt{\frac{\Phi_0}{2\pi \cos \delta} \frac{\rho A}{\Delta} \frac{\epsilon A}{d}}}$$

e) The bias voltage introduces a time-dependent phase,

$$V_{dc} = \frac{\Phi_0}{2\pi} \frac{d\delta}{dt} \rightarrow \delta = \frac{2\pi V_{dc}}{\Phi_0} t$$

Then, by the current-phase relationship of the junction,

$$I_J = I_c \sin \delta = I_c \sin \left(2\pi \frac{V_{dc}}{\Phi_0} t \right) \equiv I_c \sin(2\pi f_0 t)$$

which implies a frequency

$$f_0 = \frac{V_{dc}}{\Phi_0} = \frac{V_{dc}}{\frac{h}{2e}} = \frac{10 \mu V}{\frac{4.135 \times 10^{-15} \text{ eVs}}{2e}} = 4.8368 \text{ GHz}$$

5 Multiple qubits

⁶Enormous difference in dimension between classical and quantum state space is due to a difference in the way the spaces combine.

The state of a classical system can be completely characterized by describing the state of each of its component pieces separately.

An unintuitive aspect of quantum systems is that often the state of the system cannot be described in terms of the state of its component pieces \implies *entangled states*.

Feynman/Manin said classical systems cannot simulate entangled states in polynomial time (due to the scaling of the Hilbert space dimension with system size). n qubits $\implies 2^n$ states, $2^n \times 2^n$ dimensional Hilbert space.

Classical system of n objects whose individual state can be described in 2D vector space $\implies 2n$. *Direct sum*, \oplus .

Quantum system of n objects $\implies 2^n$. *Tensor product*, \otimes .

5.1 Direct sum of vector spaces

$$\mathbb{V} : A = \{|\alpha_1\rangle, |\alpha_2\rangle, \dots, |\alpha_n\rangle\}$$

$$\mathbb{W} : B = \{|\beta_1\rangle, |\beta_2\rangle, \dots, |\beta_n\rangle\}$$

Every element $|x\rangle \in \mathbb{V} \oplus \mathbb{W}$ can be written as $|x\rangle = |v\rangle \oplus |w\rangle$ for some $|v\rangle \in \mathbb{V}$ and $|w\rangle \in \mathbb{W}$.

Suppose the state of three objects O_1, O_1, O_3 is fully described by two parameters, the positions x_i and the momenta p_i . Then the state of the system can be described

⁶10/16/19

by direct sum of the states of the individual objects,

$$\begin{pmatrix} x_1 \\ p_1 \end{pmatrix} \oplus \begin{pmatrix} x_2 \\ p_2 \end{pmatrix} \oplus \begin{pmatrix} x_3 \\ p_3 \end{pmatrix} = \begin{pmatrix} x_1 \\ p_1 \\ x_2 \\ p_2 \\ x_3 \\ p_3 \end{pmatrix}$$

\Rightarrow state of n classical objects (each with 1 degree of freedom) has dimension $2n$.

5.2 Tensor products of vector spaces

The tensor product $\mathbb{V} \otimes \mathbb{W}$ of two vector spaces \mathbb{V} and \mathbb{W} with bases $A = \{|\alpha_1\rangle, \dots, |\alpha_n\rangle\}$ and $B = \{|\beta_1\rangle, \dots, |\beta_m\rangle\}$ respectively is an nm -dimensional vector space with a basis consisting of nm elements of the form $|\alpha_i\rangle \otimes |\beta_j\rangle$ where \otimes is the tensor product. All elements of $\mathbb{V} \otimes \mathbb{W}$ can be represented:

$$a_{11} |\alpha_1\rangle \otimes |\beta_1\rangle + a_{12} |\alpha_1\rangle \otimes |\beta_2\rangle + \dots + a_{nm} |\alpha_n\rangle \otimes |\beta_m\rangle$$

The standard basis for the vector space $\mathbb{V}_{n-1} \otimes \mathbb{V}_{n-2} \otimes \dots \otimes \mathbb{V}_0$ for an n -qubit (i.e. 2-level, size 2 basis) system consists of 2^n vectors:

$$\begin{aligned} &|0\rangle_{n-1} \otimes \dots \otimes |0\rangle_1 \otimes |0\rangle_0 \\ &|0\rangle_{n-1} \otimes \dots \otimes |0\rangle_1 \otimes |1\rangle_0 \\ &|0\rangle_{n-1} \otimes \dots \otimes |1\rangle_1 \otimes |0\rangle_0 \\ &\vdots \\ &|1\rangle_{n-1} \otimes \dots \otimes |1\rangle_1 \otimes |1\rangle_0 \end{aligned}$$

Every n -qubit quantum state can be represented:

$$e^{i\theta} (a_0 |000\dots 0\rangle + \dots + a_{2^n-1} |111\dots 1\rangle)$$

$\Rightarrow 2^n - 1$ complex numbers (global phase + normalization condition removes 2 real numbers).

If Alice controls 2 qubits and Bob the last three we may write a state as

$$\frac{1}{\sqrt{2}} (|00\rangle_A |101\rangle_B + |10\rangle_A |011\rangle_B)$$

where the subscripts indicate which qubits Alice controls and which Bob controls.

5.3 Meaning of entanglement

Bell basis for a two-qubit system:

$$\begin{aligned}
 |\Phi^+\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
 |\Phi^-\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\
 |\Psi^+\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\
 |\Psi^-\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)
 \end{aligned} \tag{7}$$

The elements of the Bell basis are entangled. For instance $|\Phi^+\rangle$ cannot be described in terms of the state of its component qubits separately (i.e. in terms of a product state).

⁷Example 4-qubit state:

$$\begin{aligned}
 |\psi\rangle &= \frac{1}{2}(|0000\rangle + |0101\rangle + |1010\rangle + |1111\rangle) \\
 &= \frac{1}{\sqrt{2}}(|0\rangle_1 |0\rangle_3 + |1\rangle_1 |1\rangle_3) \otimes \frac{1}{\sqrt{2}}(|0\rangle_2 |0\rangle_4 + |1\rangle_2 |1\rangle_4)
 \end{aligned}$$

$\Rightarrow |\psi\rangle$ is not entangled with respect to the system composition of a subsystem of the 1st & 3rd qubit and a subsystem of the 2nd & 4th qubit.

5.3.1 Multi-qubit measurements

Two qubits:

$$\begin{aligned}
 |\psi\rangle &= a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle \\
 |a|^2 + |b|^2 + |c|^2 + |d|^2 &= 1
 \end{aligned}$$

We wish to measure the 1st qubit with respect to the standard basis $\{|0\rangle, |1\rangle\}$. Let $\mathbb{V}_1, \mathbb{V}_2$ be the vector spaces of the 1st and 2nd qubits, respectively. Then $\mathbb{V} = \mathbb{V}_1 \otimes \mathbb{V}_2$ is the vector space of the composite system.

$$S_1 = |0\rangle \otimes \mathbb{V}_2, \quad S_2 = |1\rangle \otimes \mathbb{V}_2$$

$$|\psi_1\rangle = \frac{a}{c_1}|00\rangle + \frac{b}{c_1}|01\rangle \in S_1$$

$$|\psi_2\rangle = \frac{c}{c_2}|10\rangle + \frac{d}{c_2}|11\rangle \in S_2$$

$$|\psi\rangle = c_1|\psi_1\rangle + c_2|\psi_2\rangle$$

$$c_1 + \sqrt{|a|^2 + |b|^2}, \quad c_2 + \sqrt{|c|^2 + |d|^2}$$

$$\Rightarrow |\psi\rangle = |0\rangle \otimes (a|0\rangle + b|1\rangle) + |1\rangle \otimes (c|0\rangle + d|1\rangle)$$

Multi-bit measurement can be treated as a series of single-bit measurements in standard basis.

⁷10/21/19

- Measure if two qubits have the same value without learning the actual value of the two qubits.
- Equivalent to unitary transformations followed by a standard measurement of individual qubits.

Measurement gives another way of thinking about entangled particles. Particles are not entangled if the measurement of one has no effect on the other. For example, the state $(|00\rangle + |11\rangle)/\sqrt{2}$ is entangled since the probability that the first bit is measured to be $|0\rangle$ is $1/2$ if the second bit has not been measured. However, if the second bit had been measured, the probability would be 0 or 1. On the other hand, the state $(|00\rangle + |01\rangle)/\sqrt{2} = |0\rangle \otimes (|0\rangle + |1\rangle)/\sqrt{2}$ is not entangled, since any measurement of the first qubit will yield $|0\rangle$ regardless of whether the second qubit was measured.

5.3.2 EPR paradox

Einstein, Podolsky, and Rosen proposed a thought experiment that uses entangled particles which seem to violate principles of relativity.

$$A \longleftarrow \text{EPR source} \longrightarrow B$$

The EPR source generates two maximally entangled particles,

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

A and B can be arbitrarily far apart.

Suppose A measures her particle and observes state $|0\rangle$. \implies means the combined state will now be $|00\rangle$. Now if B measures his particle, he will observe $|0\rangle$.

The change of the combined quantum state occurs instantaneously even though the particles may be arbitrarily far apart. It appears that this would enable A and B to communicate faster than the speed of light. (Actually, they can't.)

EPR proposed local hidden variable theory. Each particle has some internal state that completely determines what the result of the measurement will be, but these variables are hidden from us. For the moment, the best we can do is to make probabilistic predictions.

J. S. Bell showed that the EPR picture must satisfy an inequality (now known as Bell's inequality). This inequality has been experimentally violated \implies EPR cannot explain the results of measurements with respect to a different basis.

Description of *cause and effect*. A measurement by Alice affects a measurement performed by Bob. It is possible to set up the EPR scenario so that one observer *sees* Alice measure first, while another observer *sees* Bob measure first. According to relativity, physics must explain equally well the observation of the first observer as the second. The experimental results should be explained equally. The symmetry shows that Alice and Bob cannot use their EPR pair to communicate faster than the speed of light. All that can be said is that Alice and Bob are observing the same random (though perfectly correlated) behavior.

6 Quantum gates

Quantum systems obey Schrödinger's equation. The dynamics must take states to other states in a way that preserves orthogonality (unitary dynamics). For a complex vector space, linear transformation, unitary.

Suppose matrix M is unitary. $\implies MM^\dagger = \mathbb{1}$. \implies quantum transformations (e.g. gates) are unitary and therefore reversible. \implies *Energy of computation*. Classical computation is *not* reversible.

6.1 Single-qubit gates

Computational basis $\{|0\rangle, |1\rangle\}$.

$$\begin{array}{ll} \mathbb{1} & \begin{array}{l} |0\rangle \rightarrow |0\rangle \\ |1\rangle \rightarrow |1\rangle \end{array} \quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{identity} \\ \\ X & \begin{array}{l} |0\rangle \rightarrow |1\rangle \\ |1\rangle \rightarrow |0\rangle \end{array} \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{negation} \\ \\ Y & \begin{array}{l} |0\rangle \rightarrow -|1\rangle \\ |1\rangle \rightarrow |0\rangle \end{array} \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{note: not Pauli} \\ \\ Z & \begin{array}{l} |0\rangle \rightarrow |0\rangle \\ |1\rangle \rightarrow -|1\rangle \end{array} \quad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{phase flip} \end{array}$$

⁸Hadamard gate:

$$H \quad \begin{array}{l} |0\rangle \rightarrow |+\rangle \\ |1\rangle \rightarrow |-\rangle \end{array} \quad \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad \text{Hadamard gate}$$

Quantum transformations are unitary transformations:

- Invertible/reversible: $U^\dagger U = \mathbb{1} \implies U^\dagger = U^{-1}$.
- Deterministic.
- Continuous: you can apply them in a time-continuous way.

Measurements break all three rules of unitary transformations:

- Irreversible: whatever information we didn't capture is lost.
- Probabilistic: QM is deterministic only until measurement.
- Discontinuous: measurement is assumed to project instantaneously.

Norms:

- p -norm: $|x|_p = (\sum_i |x_i|^p)^{1/p}$

⁸10/23/19

- 1-norm: $|x| = \sum_i |x_i|$ (classical probability)
- 2-norm: $|x|_2 = \sqrt{\sum_i |x_i|^2}$ (QM)

Quantum circuit notion: (quantum circuit diagram).

6.2 Two-qubit gates

Controlled NOT (CNOT) gate. First qubit is control bit:

$$\begin{aligned} |00\rangle &\rightarrow |00\rangle \\ |01\rangle &\rightarrow |01\rangle \\ |10\rangle &\rightarrow |11\rangle \\ |11\rangle &\rightarrow |10\rangle \end{aligned}$$

$$C_{\text{NOT}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} \mathbb{1} & 0 \\ 0 & X \end{pmatrix}$$

$$C_{\text{NOT}} C_{\text{NOT}} = \mathbb{1}$$

The CNOT gate cannot be decomposed into a tensor product of two single qubit transformations.

(Matrix representations of 2-qubit gates constructed as tensor products of single-qubit gates. Connection between operator/Dirac notation and matrix/array representations.)

7 Superdense coding

Information theory (Shannon): by sending n bits, you cannot communicate more than n bits of information.

Superdense coding: Alice can send Bob 2 *classical* bits by sending him *only one qubit*. (Catch: A&B must share some entangled qubit ahead of time. With no prior entanglement, Alice can't send more than one bit per qubit.)

- Alice: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.
- Alice and Bob share a Bell pair in advance: $|\Psi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$.
- Alice is going to *manipulate* her half, then send her qubit to Bob, and Bob can measure both qubits and get 2 bits of information from Alice.

2 qubits \rightarrow 4 states in basis. Will apply a NOT gate and phase flip. Alice can find 3 orthogonal states to the original Bell pair; these will be the other states of the Bell basis (7). Label the two qubits x and y .

- If $x = 1$, she applies a NOT gate.
- If $y = 1$, she applies a phase gate.

For Bob to decode the information, he has to use the inverse transformation.

8 Density matrices

⁹(This is from Scott Aaronson's Quantum Computation course [1, Lec. 6].) So far Basis states are defined: $\{|0\rangle, |1\rangle\} \rightarrow |i\rangle$. Pure states are superpositions of basis states: $|\psi\rangle = \sum \alpha_i |i\rangle$. Pure states exist in isolated quantum systems but you can also have quantum superposition layered together with regular, old probabilistic uncertainty. In some sense, mixed states are a distribution over quantum states, so

$$\{P_i, \Psi_i\} = P_1 |\Psi_1\rangle, \dots, P_n |\Psi_n\rangle,$$

meaning that with probability P_i the superposition is $|\Psi_i\rangle$. Mixed states (that is, the components $|\psi_i\rangle\langle\psi_i|$ of the mixed state) don't have to be orthogonal. Pure state is a degenerate case of a mixed state where all the probabilities are 0, except for one P_i which is 1.

We write a mixed state as a *density matrix*:

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|.$$

(Examples of outer product in matrix representation.)

For any two orthogonal states $|v\rangle$ and $|w\rangle$,

$$\frac{|v\rangle\langle v| + |w\rangle\langle w|}{2} = \frac{\mathbf{1}}{2}$$

Measuring ρ in the basis $|1\rangle, \dots, |N\rangle$ gives outcome $|i\rangle$ with probability $\Pr(|i\rangle) = \rho_{ii} = \langle i|\rho|i\rangle$. A diagonal density matrix is another way of writing a classical probability distribution, e.g. $\begin{pmatrix} P_1 & 0 \\ 0 & P_2 \end{pmatrix}$.

Rank of a matrix: $\text{rank}(\rho) =$ the number of non-zero eigenvalues. The rank of an $n \times n$ matrix is at most n .

The matrix $\mathbf{1}/2$ is the even mixture of $|0\rangle$ and $|1\rangle$. It is also an even mixture of $|+\rangle$ and $|-\rangle$. This is a *maximally mixed state*. If we do a unitary transformation U on the states $|\psi_i\rangle$ comprising ρ ,

$$\rho' = \sum_i P_i (U |\psi_i\rangle) (U |\psi_i\rangle)^\dagger = \sum_i P_i U |\psi_i\rangle\langle\psi_i| U^\dagger = U \rho U^\dagger$$

i.e. the new density matrix is unitarily transformed. E.g. $|+\rangle\langle+| = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$ in the $\{|0\rangle, |1\rangle\}$ basis, and the off-diagonals represent the interference between $|0\rangle$ and $|1\rangle$.

What are the constraints on ρ ?

- Square $n \times n$.
- Hermitian $\rho^\dagger = \rho$.
- Probability $\sum_i \rho_{ii} = 1 = \text{Tr}\{\rho\}$.

⁹10/28/19

- Positive semidefinite: all eigenvalues are nonnegative (since they represent probabilities).

(Examples of pure vs. mixed states.)

Alice and Bob may share a bipartite state described by a density matrix. The state of each's qubit is described by the reduced density matrix obtained by taking a partial trace over the other's qubit space. The key points:

- A density matrix encodes all and only what is physically observable.
- Two quantum states will lead to different probabilities iff they have different density matrices.
- No communication theorem: If Alice and Bob share an entangled state, nothing A chooses to do will have any effect on Bob's density matrix \implies there is no observable effect on Bob's end.

Basis state $|i\rangle$. Pure state $|\psi\rangle = \sum_i \alpha_i |i\rangle$. Mixed state $\{P_i, |\psi_i\rangle\} \rightarrow \rho = \sum_i P_i |\psi_i\rangle\langle\psi_i|$, classical probability distributions over pure states.

What represents better the actual physical reality? Pure vs. mixed? When we look at part of an entangled state, a mixed state is the most complete representation possible that only describes the part that we are looking at.

9 Quantifying entanglement

¹⁰How do you quantify how much entanglement there is between two quantum systems?
 \leftrightarrow measuring entanglement.

Entanglement is our resource \leftrightarrow EPR $(|00\rangle + |11\rangle)/\sqrt{2}$. Entanglement of pure states; entanglement of mixed states.

9.1 Schmidt decomposition

Given $\sum_{ij} \alpha_{ij} |i\rangle_A |j\rangle_B$, how do we calculate how many EPR pairs it's worth?

Let $A = (\alpha_{ij})$. In bipartite states, we can always find a change of basis on Alice's side and another on Bob's side that puts the state into the simpler form (Schmidt decomposition) $\sum_i \lambda_i |v_i\rangle |w_i\rangle$ where $\{|v_i\rangle\}$ is an orthonormal set, and $\{|w_i\rangle\}$ is an orthonormal set. This follows from the singular value decomposition of the matrix A : we can multiply A by two unitary matrices, one on each side, to get a diagonal matrix $\Lambda = UAV$. Measuring in the $\{|v_i\rangle, |w_i\rangle\}$ basis would then yield the probability distribution

$$\left(|\lambda_1|^2, \dots, |\lambda_2|^2\right)^T. \quad (8)$$

¹⁰10/30/19

9.2 Entropies

9.2.1 Shannon entropy

For classical probability distribution $D = (P_1, \dots, P_n)$, the Shannon entropy is

$$H(D) = \sum_{i=1}^n P_i \log_2 \frac{1}{P_i} = - \sum_{i=1}^n P_i \log_2 P_i$$

E.g.

- $D = (0, 1) \implies H(D) = -0 \log_2 0 - 1 \log_2 1 = 0.$
- $D = (\frac{1}{2}, \frac{1}{2}) \implies H(D) = 2(\frac{1}{2} \log_2 \frac{1}{2}) = 1$

For the distribution (8), we can calculate the ordinary Shannon entropy of our system as

$$\sum_i |\lambda_i|^2 \log \frac{1}{|\lambda_i|^2}$$

in order to figure out how many Bell pairs our state is equivalent to.

9.2.2 Von Neumann entropy

Generalizes Shannon entropy from classical probability distributions to quantum mixed states. We say that the von Neumann entropy of a mixed state ρ is

$$S(\rho) = \sum_{i=1}^N \lambda_i \log_2 \frac{1}{\lambda_i} = - \sum_i \lambda_i \log_2 \lambda_i.$$

The von Neumann entropy is the Shannon entropy of the vector of eigenvalues of the density matrix of ρ (i.e. λ_i 's here are probabilities).

The von Neumann entropy of any pure state $|\psi\rangle\langle\psi|$ is zero because there is always some measurement basis that returns a definite outcome (i.e. the basis containing $|\psi\rangle$). Example: you could measure $|+\rangle$ in the $\{|0\rangle, |1\rangle\}$ basis where you have complete uncertainty and Shannon entropy of 1, but if you measure in the $\{|+\rangle, |-\rangle\}$ basis you have complete certainty with Shannon entropy of 0. In either case, the von Neumann entropy is 0.

Von Neumann entropy of a maximally mixed qubit state $\mathbb{1}/2$ is 1. The von Neumann entropy of a maximally mixed n -qubit state $\mathbb{1}/2^n$ is n .

Suppose Alice and Bob share a bipartite pure state $|\psi\rangle = \sum_{ij} \alpha_{ij} |i\rangle_A |j\rangle_B$. To quantify the entanglement entropy, we trace out either Alice or Bob's part of the system and calculate the von Neumann entropy of the reduced density matrix representing just Bob's or Alice's part, respectively (which we choose should not matter, $S(\rho_A) = S(\rho_B) = H(\lambda_i)$, Shannon entropy of λ_i which you get by diagonalizing the Alice's or Bob's reduced density matrix).

10 Mixed vs. pure states

¹¹Diagonal elements ρ_{ii} of a density matrix represent the populations in the chosen basis:

$$\rho = \sum_i p_i |i\rangle\langle i|, \quad |i\rangle = \sum_p c_p^{(i)} |p\rangle$$

$$\rho_{ii} = \sum_p \left| c_p^{(i)} \right|^2 p_i \rightarrow \text{population in state } |i\rangle$$

The off-diagonal elements ρ_{ij} of a density matrix provide information on interference of $|i\rangle$ and $|j\rangle \rightarrow$ they represent coherence in mixed states. When a qubit is coupled to an environment, this coupling can cause time-dependence of elements of density matrix \rightarrow Decay of the off-diagonal elements is referred to as “dephasing” (T_2) while the decay of the diagonal elements is referred to as “relaxation” or “dissipation” (T_1).

What is the difference between the pure state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle$ and mixed state $\frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) = \mathbb{1}/2$? Let’s apply a Hadamard gate to both:

pure state	$H +\rangle = 0\rangle$
mixed state	$H \mathbb{1} H / 2 = \mathbb{1} / 2$

In the first case the amplitudes can interfere and produce $|0\rangle$ while in the second case the states cannot interfere because they are in an “incoherent” mixture of the two states.

Open quantum systems can produce evolution which starts out in a pure state and evolves into a mixed state \rightarrow such evolution can destroy our quantum computation \rightarrow quantum error correction.

Recall,

$$\rho = \begin{pmatrix} \rho_{11} & & & \\ & \rho_{22} & & \\ & & \ddots & \\ & & & \rho_{nn} \end{pmatrix}, \quad \text{Tr } \rho = \sum_i \rho_{ii} = 1$$

A nice property of the trace operation is that a basis change leaves it invariant. Trace has a cyclical property,

$$\text{Tr}(ABC) = \text{Tr}(BCA) = \text{Tr}(CAB).$$

Expectation value of any operator \hat{O} in terms of projectors \hat{P}_ψ can be given by:

$$\langle \hat{O} \rangle_\psi = \langle \psi | \hat{O} | \psi \rangle = \text{Tr}(\hat{O} \hat{P}_\psi) = \text{Tr}(\hat{P}_\psi \hat{O}).$$

Suppose we take pure states $|\pm\rangle$. The density matrices are

$$\rho_\pm = \frac{1}{2} \begin{pmatrix} 1 & \pm 1 \\ \pm 1 & 1 \end{pmatrix},$$

¹¹11/4/19

while the classical mixture is

$$\rho = \sum_{i=\pm} p_i |i\rangle\langle i| = \sum_{i=\pm} p_i \rho_i,$$

Statistical physics: statistical mixture of energy eigenstates in thermal equilibrium:

$$\rho = \sum_n p_n |n\rangle\langle n|, \quad \text{where} \quad p_n = \frac{e^{-E_n/kT}}{\mathcal{Z}}, \quad \text{and} \quad \mathcal{Z} = \sum_n e^{-E_n/kT}.$$

\mathcal{Z} is the partition function. When the Hamiltonian does not depend on time, the mixture is time-independent.

Example: mixture where we prepare $|0\rangle$ with probability $\frac{1}{2}$ and $|+\rangle$ with probability $\frac{1}{2}$.

$$\rho = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \frac{1}{2} \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} = \frac{1}{4} \begin{pmatrix} 3 & 1 \\ 1 & 1 \end{pmatrix}$$

The eigenvalues are $\lambda_{\pm} = \frac{1}{2} \pm \frac{\sqrt{2}}{4}$, with eigenvectors $|\phi_{\pm}\rangle = \sqrt{\lambda_{\pm}}|0\rangle + \sqrt{1-\lambda_{\pm}}|1\rangle$. We can now view the mixed state as a mixture of two eigenstates $|\phi_{\pm}\rangle$ with weights equal to λ_{\pm} .

There are two simple ways to determine whether ρ describes a pure state or not:

1. Pure state $\Leftrightarrow \rho^2 = \rho$. Mixed state $\Leftrightarrow \rho^2 \neq \rho$.
2. Pure state $\Leftrightarrow \text{Tr} \rho^2 = 1$. Mixed state $\Leftrightarrow \text{Tr} \rho^2 < 1$.

In fact, we can define the “purity of a state” $P \equiv \text{Tr} \rho^2$. A state is pure if $P = 1$ and mixed otherwise. Example: n qubits, dimension $d = 2^n \rightarrow \rho = \mathbf{1}/d$,

$$\Rightarrow P = \text{Tr}((\mathbf{1}/d)^2) = \sum_1^d \frac{1}{d^2} = \frac{1}{d}.$$

Entropy $S(\rho) = -\sum_k \lambda_k \log_2 \lambda_k$ (note $\lim_{x \rightarrow 0} x \log x = 0$). We use log base 2 so that the unit of the entropy is the “bit.” We can interpret the entropy as the missing information (in bits) about the state. Pure state: $S(\rho) = 0$. Mixed state: $S(\rho) > 0$.

10.1 Reduced density matrix

Consider a measurement just on system A, say of an observable O_A . The expectation value of that observable in terms of ρ_{AB} is

$$\begin{aligned} \langle O_A \rangle &= \text{Tr}(\rho_{AB} O_A) = \sum_{nm} \langle n_A m_B | \rho_{AB} O_A | n_A m_B \rangle \\ &= \sum_{nm} \langle n_A | \langle m_B | \rho_{AB} | m_B \rangle O_A | n_A \rangle. \end{aligned}$$

We then define the reduced density matrix for A as a partial trace over B,

$$\rho_A = \sum_m \langle m | \rho_{AB} | m \rangle \equiv \text{Tr}_B \rho_{AB},$$

and then any observable in A can be expressed,

$$\langle O_A \rangle = \text{Tr}(\rho_A O_A).$$

That is, ρ_A describes the state of system A alone.

10.2 Quantifying entanglement in mixed states

¹²(See [1, Lec. 11].) For bipartite mixed state there are two entanglement measures to consider:

- *Entanglement of formation:* $E_F(\rho_{AB})$ is the number of entangled qubits that A and B need to create one copy of the state ρ_{AB} (in the limit where they are creating many copies of it, and assuming they are allowed unlimited local operations and classical communication (LOCC) for free).
- *Distillable entanglement:* $E_D(\rho_{AB})$ is the number of entangled qubits that A and B can extract per copy of ρ_{AB} again in LOCC for free.

Clearly $E_F \geq E_D$ since if you could ever get out more entanglement than you put in, it would give you a way to increase entanglement (entropy) arbitrarily using LOCC, which is impossible.

What about $E_F \gg E_D$? There exist bipartite states that take a lot of entanglement to make but you can only extract a small fraction of the entanglement.

A bipartite state ρ_{AB} is separable if there is a way to write it as a mixture of product states:

$$\rho_{AB} = \sum_i p_i |v_i\rangle\langle v_i| \otimes |w_i\rangle\langle w_i|$$

A mixed state is called entangled iff it is *not* separable. It could happen that a density matrix looks entangled *but* there's some decomposition that shows it is separable.

Proven by Leonid Gurvits, 2003: If you are given a density matrix ρ_{AB} for a bipartite state then deciding whether ρ_{AB} represents a separable or entangled state is an NP-hard problem.

11 Some standard results, protocols, and other bits and bobs

11.1 No-cloning theorem

Assume that U is a unitary transformation that clones in that $U|a0\rangle = |aa\rangle$ for all quantum states $|a\rangle$. Let $|a\rangle$ and $|b\rangle$ be orthogonal quantum states. Clearly $U|a0\rangle = |aa\rangle$ and $U|b0\rangle = |bb\rangle$. But consider a superposition state, $|c\rangle = (|a\rangle + |b\rangle)/\sqrt{2}$:

$$U|c\rangle = \frac{1}{\sqrt{2}}(|aa\rangle + |bb\rangle) \neq |cc\rangle,$$

therefore U is not a cloning operation.

It is possible to clone a known quantum state. The no-cloning theorem says we cannot reliably clone an *unknown* state. Nor is cloning possible by using measurements.

11.2 Quantum teleportation

It is possible for Alice and Bob to use pre-shared entanglement plus classical communication to perfectly transmit a qubit.

¹²11/6/19

Alice has a single qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. She also shares the EPR pair $(|00\rangle + |11\rangle)/\sqrt{2}$. Alice applies some transformation to $|\psi\rangle$ that entangles it with her half of the Bell pair. She then measures her qubit. Alice tells Bob the measurement outcomes over the phone. Bob then applies some transformation to his qubit of the entangled pair and “magically” will have $|\psi\rangle$.

(Example.) Alice applies CNOT with $|\psi\rangle$ as control and her half of the Bell state as target. Alice then applies Hadamard on $|\psi\rangle$. Alice measures both of her qubits. She tells Bob the result. Depending on the result, Bob applies a corresponding retrieval transformation on his qubit (which was part of the Bell pair), which deterministically reproduces $|\psi\rangle$ on Bob’s end. \implies they have transmitted a qubit without a quantum channel.

¹³Are we sending infinitely more information than two classical bits if we can send over enough information to perfectly describe an arbitrary qubit? In some sense we are sending a perfect qubit but Bob only obtains the information that he can measure which is significantly less.

We didn’t make any assumption that $|\psi\rangle$ has to be unentangled from the rest of the world. You can have a protocol that has $|\psi\rangle$ to be half of another Bell pair. This protocol would entangle the 4th qubit to Bob’s qubit. This suggests that it should be possible to teleport an arbitrary n -qubit entangled state by simply teleporting the qubits one at a time.

A consequence of this is that two qubits don’t need to interact directly to become entangled. Consider a quantum circuit where H acts on qubit 1, followed by a CNOT acting on qubit 2 conditioned on 1, followed by a SWAP gate between 2 and 3. Qubits 1 and 3 end up entangled even though there’s never any “direct” contact between them \rightarrow SWAP gate. *Entanglement swapping*: If Alice has two entangled qubits and also two EPR/Bell states shared with Bob, she can teleport both of her qubits to Bob whereupon they will be entangled on Bob’s end, even though the two qubits on Bob’s end were never in causal contact with each other.

11.3 GHZ states

There is a 3-qubit analogue of the Bell pair called a *GHZ state*:

$$\frac{|000\rangle + |111\rangle}{\sqrt{2}}$$

Suppose three players share a GHZ state, where all three can see the state is entangled. What if Charlie is gone? Can Alice and Bob still see they are entangled? No. Charlie could have measured his qubit without Alice and Bob knowing. But if he did then Alice and Bob would have classical correlation only: either both 0s if Charlie measured zero or 1s if he measured one. Regardless of whether Charlie measured or not, A and B cannot know if they are entangled. (Like Borromean rings.)

¹³11/11/19

11.4 CHSH game

11.4.1 Classical version

We put Alice and Bob in separate rooms and each are given a challenge bit (x and y respectively) by a referee. The challenge bits are chosen uniformly at random and independently of each other. Then Alice sends an answer bit a back to the referee and Bob sends back bit b . Alice and Bob win the game if

$$a + b = xy \pmod{2} \iff \begin{cases} a = b & \text{if } x = 0 \text{ or } y = 0 \\ a \neq b & \text{if } x = y = 1 \end{cases}$$

Alice and Bob know the rules and are allowed to strategize together beforehand.

Optimal strategy: Alice and Bob always return $a = 0$ and $b = 0$. They win with probability $3/4$. (They win on $(x, y) \in \{(0, 0), (0, 1), (1, 0)\}$ and lose on $(x, y) = (1, 1)$.)

11.4.2 Quantum version

If Alice and Bob can share a Bell pair, they can win with probability $\cos^2 \frac{\pi}{8} \approx 85\%$

¹⁴[App. B.](#)

¹⁵[Mid-project presentations.](#)

¹⁶The strategy involves A and B measuring their respective qubits in *different bases* depending on whether their input bits x and y are 0 or 1, and then outputting bits a and b respectively based on the outcomes of those measurements. Let's consider the case where A gets $x = 0$ and she measures $|0\rangle$, she will output $a = 0$ and A and B will win iff Bob outputs $b = 0$. Given that A measured her qubit already Bob's qubit has collapsed to the state $|0\rangle$. First suppose $y = 0$. Bob measures $|0\rangle$ in a basis rotated by $\pi/8$. He outputs 0 and they win. Probability of Bob outputting zero is $\cos^2(\frac{\pi}{8}) \approx 85\%$.

11.4.3 Einstein-certified randomness

In crypto, one of the most important tasks is to create random numbers.

$$|\psi\rangle = a|0\rangle + b|1\rangle \iff n \text{ assumptions}$$

Once we have quantum mechanics, you might think that the solution is trivial. After all, you get a random number by measuring the $|+\rangle$ state in the computational basis. For cryptography, though, this is insufficient. The Bell inequality lets us certify numbers as being truly random under very weak assumptions, namely, that information cannot travel faster than the speed of light.

Given a black box device that generates random numbers, we use one to generate a bit x and another to generate a bit y , and then just play the CHSH game. If the win probability is $\cos^2(\frac{\pi}{8})$, it's perfectly random. Anything above $3/4$ is certifiably random to some degree. Now suppose you have two boxes, designed by your enemies,

¹⁴11/13/19

¹⁵11/18/19–11/20/19

¹⁶11/25/19

that share quantum entanglement. Referee sends random x, y , boxes return a, b . Play CHSH game: if $\Pr(\text{success}) = \cos^2(\frac{\pi}{8})$, we declare the string truly random.

Shannon entropy: $\sum p_x \log_2 \frac{1}{p_x}$ where p_x is the probability that string x will be in general less than n . Problem: we need the input bits to be uniformly random in order to play CHSH game. I.e. x, y truly random, a, b not truly random.

Pironio et al.: You don't have to give Alice and Bob perfectly random bits every time. Instead, you can input $x = y = 0$ most of the time, and occasionally input some random x 's and y 's to prevent Alice and Bob from figuring out the pattern. This is because Alice and Bob have no way of knowing whether each round is for testing or randomness generation.

How much entropy can we get out per bit of entropy put in?

- Colbeck et al.: You can get cn bits out per n bits in ($c > 1$).
- Pironio et al.: n^2 .
- Vazirani et al.: $\exp(\sqrt{n})$.

How many random numbers do I need to jump start this? One naive way is to feed Alice and Bob the same true random bits that they themselves create \rightarrow it is not random to them. Doesn't work.

- Courdon & Yuan: Suppose we only have a fixed number of A and B players. (e.g. suppose $A, B \rightarrow$ referee $\rightarrow C, D$).
- Aaronson & Gross: Few tens of thousands (upper bound).

Reichardt et al. (2012): As long as we have two quantum computers, and as long as they are entangled with each other but unable to exchange messages, we can use CHSH game to *verify* that the computers are behaving as expected.

12 Computational complexity

¹⁷The study of how many resources are required to solve various problems. Divide problems into “easy” and “hard.” Easy problems are those for which the resources needed to solve them grow only like some polynomial in input size. E.g. multiplication of n -bit integer \rightarrow add & shift $\rightarrow n \times 2n$ bitwise addition, which we say is $\mathcal{O}(n^2)$.

Now consider factoring n -bit number, x . The simplest algorithm is to check all the numbers up to \sqrt{x} . This requires $2^{n/2}$ checks \rightarrow exponentially difficult in $n \implies$ hard.

$$n \rightarrow \begin{cases} \text{factoring} & 2^{n/2} \rightarrow \text{hard} \\ \text{multiplication} & n^2 \rightarrow \text{easy} \end{cases}$$

12.1 Complexity classes

See Fig. 3.

- P (polynomial time): Class of decision problems which we can solve in polynomial time (\implies polynomial memory).

¹⁷12/2/19

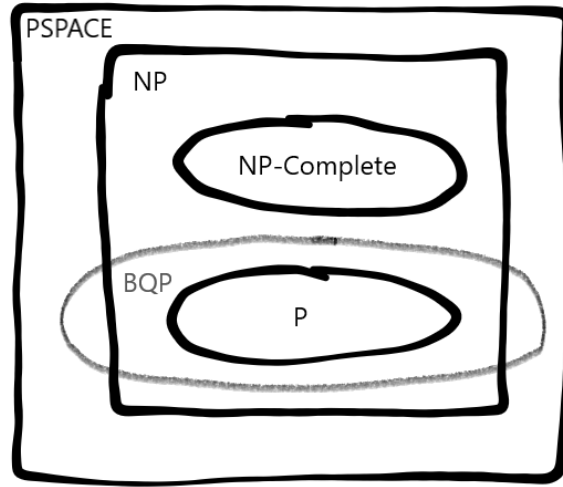


Figure 3: Potential relationship between the complexity classes.

- NP (nondeterministic polynomial): Class of problems which we *may* not be able to solve but we can *verify* a solution in polynomial time (and \therefore polynomial memory) if it is given to us. $P \subseteq NP$.
- NP-hard: Problems which are at least as hard as *anything* in NP. That is, if someone were to give you a box that efficiently solved an NP-hard problem, you could use it to solve any problem in NP in polynomial time.
- NP-complete: Problems which are both NP-hard and are themselves in NP.
- NP-intermediate: Problems which are in NP but are not in P or in NP-complete.
- BQP (bounded-error quantum polynomial): Class of decision problems solvable in polynomial time on a quantum computer with a probability of error less than $1/3$. It seems BQP overlaps with NP-intermediate (e.g. Shor's algorithm).
- PSPACE (polynomial space): Class of problems solvable using polynomial memory but perhaps requiring exponential time.

12.2 3-SAT

See Ref. 5.

3-SAT is a very simple NP-complete problem. We are given a boolean expression which is a big AND (\wedge) of clauses,

$$E = C_0 \wedge C_1 \wedge \cdots \wedge C_{m-1},$$

where each clause C_i is an OR (\vee) of three literals,

$$E = \underbrace{(a \vee b \vee c)}_{C_0} \wedge \underbrace{(\bar{a} \vee \bar{b} \vee \bar{c})}_{C_1} \wedge \underbrace{(a \vee \bar{b} \vee \bar{c})}_{C_2} \cdots$$

Is there an assignment of the variables so that E is true?

Independent set decision problem (ISDP): Given a graph G and a number k , can we find a set of k vertices in G such that there are no edges between any two of the vertices? We want to use 3-SAT to prove that ISDP is NP-complete. First note if you are given a set of k vertices you can easily check to verify that there are no edges between two nodes in the set. Second, map 3-SAT to ISDP:

1. Turn each clause into 3 nodes and label the nodes with their literals.
2. For every pair of nodes with the same, but negated literals (e.g. b and \bar{b}), add an edge between that pair of nodes.
3. Any independent set of size k (corresponding to the number of clauses in the 3-SAT expression) will correspond to an assignment of the literals for which the 3-SAT expression is true.

A Python & Qiskit: Installation & Introduction

To get started with Python and Qiskit, have a look at Ref. 8.

B Guest lecture: Quantum algorithms

Guest lecture by Ali Javadi, IBM.

The hidden shift problem, also known as Simon's problem, is a member of a broader class of so-called "hidden subgroup" problems. Given a function f defined over all binary strings of length n such that

$$f(x) = f(x \oplus s) \quad \forall x,$$

where \oplus denotes bitwise addition, the challenge is to find the value of the bitstring s , known as the "hidden shift." While the function f is unknown, you are provided with an oracle that can evaluate f . In other words, you can ask the oracle the value of $f(x)$ for any x .

Classically, this problem requires $\mathcal{O}(2^{n/2})$ queries to the oracle in order to deduce s with high probability. Using a quantum algorithm (such as Simon's algorithm), this problem may be solved in $\mathcal{O}(n)$ queries, an exponential speedup.

Ref. 4 demonstrates how to solve for the hidden shift of a "bent" function in Qiskit.

C Additional Problems

Q1

Any measurement performed in qiskit is always done along the z-axis of the Bloch sphere, it is however not always the relevant axis in practice. Using adequate operation on the qubit before the measurement, can you figure out how deduce the projection of the qubit state on all three axis of the Bloch Sphere (x, y, z) ?

The answer should rely on the use of the qasm simulator which reflects the actual behavior of the quantum hardware. However feel free to use the state vector simulator to figure out the impact of operations on the qubit.

Solution

It is possible to measure the qubit in any of the three axes of the Bloch sphere by performing a rotation or change of basis right before the measurement. First, the matrix for the change of basis from the σ_z basis to the σ_x basis is the Hadamard gate:

$$U(\sigma_z \rightarrow \sigma_x) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

The matrix of change of basis from the σ_z basis to the σ_y one is:

$$U(\sigma_z \rightarrow \sigma_y) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -i \\ 1 & i \end{pmatrix}.$$

We want to prove that is the case using Qiskit. To do so we need a quantum circuit that firstly takes the initial quantum state $|0\rangle$ and puts it in any desired state $|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\phi} \sin(\theta/2)|1\rangle$, then performs either rotation $U(\sigma_z \rightarrow \sigma_x)$ or $U(\sigma_z \rightarrow \sigma_y)$ and then performs a measurement. To perform both the state preparation and then the rotation we will use the physical gate:

$$U_3(\alpha, \beta, \lambda) = \begin{pmatrix} \cos(\alpha/2) & e^{-i\lambda} \sin(\alpha/2) \\ e^{i\beta} \sin(\alpha/2) & e^{i(\lambda+\beta)} \cos(\alpha/2) \end{pmatrix}.$$

In this language the state preparation is done by applying $U_3(\alpha = \theta, \beta = \phi, \lambda = 0)$ and the rotations as: $U(\sigma_z \rightarrow \sigma_x) = U_3(\alpha = -\pi/2, \beta = \pi, \lambda = 0)$ and $U(\sigma_z \rightarrow \sigma_y) = U_3(\alpha = \pi/2, \beta = 0, \lambda = \pi/2)$:

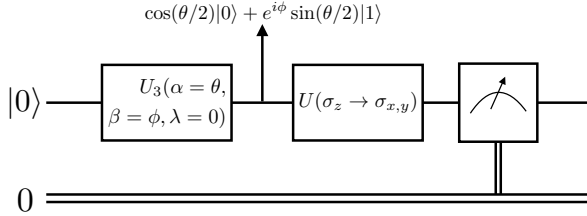


Figure 4: Quantum circuit used.

In order to test our circuit, we will run it with the qasm simulator of Qiskit (collecting $2 \cdot 10^3$ measurements for the statistics) and then compare the output probabilities with the analytical ones. Consider we start with state $|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\phi} \sin(\theta/2)|1\rangle$, the probabilities of measuring it in the states of the basis of σ_x and σ_y are:

$$\begin{aligned}
P\left(|+\rangle_x = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right) &= \frac{1}{2}(1 + \sin(\theta)\cos(\phi)); \\
P\left(|-\rangle_x = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right) &= \frac{1}{2}(1 - \sin(\theta)\cos(\phi)); \\
P\left(|+\rangle_y = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)\right) &= \frac{1}{2}(1 - \sin(\theta)\sin(\phi)); \\
P\left(|-\rangle_y = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)\right) &= \frac{1}{2}(1 + \sin(\theta)\sin(\phi)).
\end{aligned}$$

In order to compare the analytical probabilities versus the simulated ones, with the circuit in Figure 4 we generated 200 random initial states (random uniformly distributed values of $\theta \in [0, \pi]$ and $\phi \in [0, 2\pi]$) and then measured them either in the σ_x or σ_y basis. Figure 5 shows simulated versus analytical probabilities when measuring the random states in σ_x and σ_y basis. It shows that, up to small statistical deviations from the simulated probabilities, the circuit and analytical values exactly agree in all cases. This proves that indeed we can measure the states in any basis we want by rotating the state before the measurement.

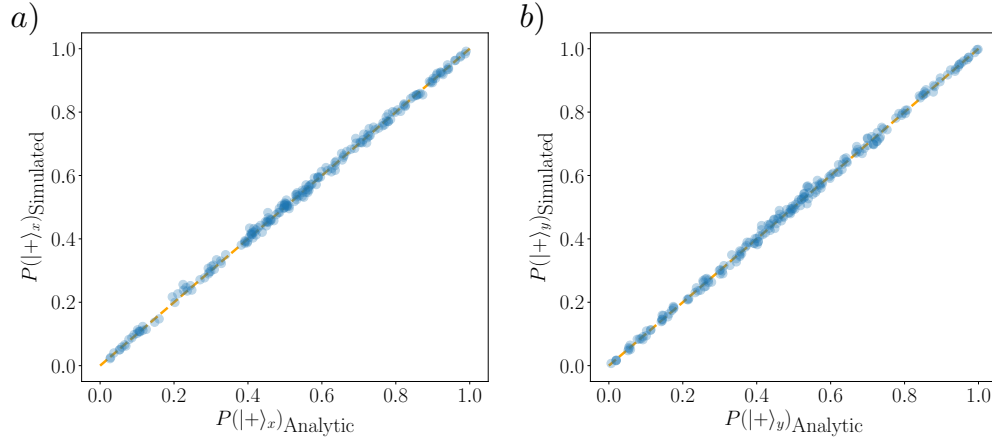


Figure 5: Probabilities simulated from circuit in Figure 4 versus the analytical expected values. Blue dots indicate the probabilities and the dashed orange line is for visual guidance. **a)** Measuring the initial random states in the σ_x basis. **b)** Measuring the initial random states in the σ_y basis.

Q2

Coherent state is nothing more than a displaced vacuum state:

$$|\alpha\rangle = U(\alpha) |0\rangle$$

Find the transformed operators in terms of original ones (a and a dagger):

$$\tilde{a} = U_{\alpha}^{\dagger} a U_{\alpha}$$

$$\tilde{a}^\dagger = U_\alpha^\dagger a^\dagger U_\alpha$$

Remember:

$$a |\alpha\rangle = \alpha |\alpha\rangle$$

Solution

A coherent state $|\alpha\rangle$ may be defined as the unique eigenstate of the annihilation operator a with corresponding eigenvalue $\alpha \in \mathbb{C}$,

$$a |\alpha\rangle = \alpha |\alpha\rangle.$$

The formal solution to this eigenvalue problem is the vacuum state $|0\rangle$ displaced in phase space by α :

$$|\alpha\rangle = D(\alpha) |0\rangle, \quad \text{with} \quad D(\alpha) = e^{\alpha a^\dagger - \alpha^* a}, \quad (9)$$

where $D(\alpha)$ is the displacement operator.¹⁸ It is easy to derive the former relations by writing $|\alpha\rangle = \sum_n \psi_n |n\rangle$ and plugging into the eigenvalue problem:

$$a |\alpha\rangle = \alpha |\alpha\rangle \implies \sum_n \psi_n a |n\rangle = \sum_n \alpha \psi_n |n\rangle \implies \sum_{n=1}^{\infty} \psi_n \sqrt{n} |n-1\rangle = \sum_{n=0}^{\infty} \alpha \psi_n |n\rangle$$

which implies the recursion relation

$$\psi_{n+1} \sqrt{n+1} = \alpha \psi_n \implies \psi_n = \frac{\alpha^n}{\sqrt{n!}} \psi_0.$$

Therefore, the state $|\alpha\rangle$ can be written as:

$$|\alpha\rangle = \psi_0 \sum_n \frac{\alpha^n}{\sqrt{n!}} |n\rangle = \psi_0 \sum_n \left(\frac{(\alpha a^\dagger)^n}{n!} \right) |0\rangle = \psi_0 e^{\alpha a^\dagger} |0\rangle.$$

In principle, we could think of writing $D(\alpha) = e^{\alpha a^\dagger}$, however this operator is not unitary and therefore it does not preserve the norms of states. In the previous derivation, the normalization of the wave function is encoded in ψ_0 , but we can just take $D(\alpha)$ to be unitary and therefore we will not have to worry about ψ_0 . The easiest way to make that operator unitary is to multiply by the inverse of its complex conjugate, $e^{-\alpha^* a}$. The inverse of the complex conjugate will not change its action over $|0\rangle$ as $e^{-\alpha^* a} |0\rangle = |0\rangle$. Therefore:

$$|\alpha\rangle = e^{\alpha a^\dagger - \alpha^* a} |0\rangle \implies D(\alpha) = e^{\alpha a^\dagger - \alpha^* a}$$

Finally, we wish to compute $\tilde{a} = D^\dagger(\alpha) a D(\alpha)$ and $\tilde{a}^\dagger = D^\dagger(\alpha) a^\dagger D(\alpha)$. Using the expression for the displacement operator (9), we have

$$\begin{aligned} \tilde{a} &= e^{\alpha^* a - \alpha a^\dagger} a e^{\alpha a^\dagger - \alpha^* a} \\ \tilde{a}^\dagger &= e^{\alpha^* a - \alpha a^\dagger} a^\dagger e^{\alpha a^\dagger - \alpha^* a}. \end{aligned} \quad (10)$$

¹⁸ $D(\alpha) \equiv U_\alpha$, the notation given in the problem statement.

These are easily computed using the Baker-Hausdorff lemma [7, Eq. 2.3.47],

$$e^{iG\lambda} A e^{-iG\lambda} = A + i\lambda[G, A] + \frac{(i\lambda)^2}{2!}[G, [G, A]] + \cdots + \frac{(i\lambda)^n}{n!}[G, [G, [G, \dots [G, A]]] \dots] + \cdots, \quad (11)$$

for some operator A , where G is Hermitian and λ is a real parameter. Identifying $iG = \alpha^* a - \alpha a^\dagger$ and $\lambda = 1$, we compute the commutators

$$\begin{aligned} [G, a] &= -i[\alpha^* a - \alpha a^\dagger, a] = i\alpha[a^\dagger, a] = -i\alpha \\ [G, a^\dagger] &= -i[\alpha^* a - \alpha a^\dagger, a^\dagger] = -i\alpha^*[a, a^\dagger] = -i\alpha^* \end{aligned}$$

where we have used $[a, a^\dagger] = 1$. As these are each proportional to the identity, all subsequent commutators in (11) vanish, so (10) reduces to

$$\begin{aligned} \tilde{a} &= a + \alpha \\ \tilde{a}^\dagger &= a^\dagger + \alpha^*. \end{aligned}$$

Q3

Consider a phenomenological Hamiltonian:

$$H_T = -\frac{E_J}{2} \sum_N [|N+1\rangle\langle N| + |N\rangle\langle N+1|]$$

as a representation of the microscopic tunneling of Cooper pairs across the JJ, where state $|N\rangle$ represents the integer N number of excess Cooper pairs in the “box”. Let’s also define a set of phase states $|\delta\rangle$ which are the Fourier dual to the number states $|N\rangle$, $|\delta\rangle = \sum_N e^{iN\delta} |N\rangle$. (Note that the phase δ lives on the compact space $[0, 2\pi]$ as the Cooper pair number N on the “island” is a discrete integer).

- Show that the states $|\delta\rangle$ are eigenstates of \hat{H} .
- Find the associated eigenvalues.
- Find the group velocity:

$$v_g \equiv \frac{1}{\hbar} \frac{\partial \lambda_{T,\delta}}{\partial \delta}.$$

Solution

The tunneling of Cooper pairs into or out of a Cooper pair box via a Josephson junction may be represented by the Hamiltonian

$$H_T = -\frac{E_J}{2} \sum_N [|N+1\rangle\langle N| + |N\rangle\langle N+1|] \quad (12)$$

where E_J is the Josephson energy, $|N\rangle$ is the state of the box containing an excess of N Cooper pairs relative to the number of Cooper pairs outside the box,¹⁹ and the sum

¹⁹For $N < 0$, this represents a *deficit* of N Cooper pairs in the box, relative to the number outside the box.

ranges over all integers $N \in \mathbb{Z}$. The phase states $|\delta\rangle$ are Fourier dual to the number states $|N\rangle$,

$$|\delta\rangle = \sum_N e^{iN\delta} |N\rangle. \quad (13)$$

The action of the Hamiltonian (12) on the phase states (13) yields

$$\begin{aligned} H_T |\delta\rangle &= -\frac{E_J}{2} \sum_N \sum_{N'} e^{iN'\delta} \{ |N+1\rangle \langle N|N'\rangle + |N\rangle \langle N+1|N'\rangle \} \\ &= -\frac{E_J}{2} \sum_N \sum_{N'} e^{iN'\delta} \{ |N+1\rangle \delta_{N,N'} + |N\rangle \delta_{N+1,N'} \} \\ &= -\frac{E_J}{2} \sum_N \{ e^{iN\delta} |N+1\rangle + e^{i(N+1)\delta} |N\rangle \} \end{aligned} \quad (14)$$

$$\begin{aligned} &= -\frac{E_J}{2} \sum_N \{ e^{i(N-1)\delta} |N\rangle + e^{i(N+1)\delta} |N\rangle \} \\ &= -\frac{E_J}{2} (e^{-i\delta} + e^{+i\delta}) \sum_N e^{iN\delta} |N\rangle \\ &= -E_J \cos \delta |\delta\rangle \end{aligned} \quad (15)$$

where, in going from (14) to (15), we were able to take $N \rightarrow N-1$ in just the first term because the sum ranges from $-\infty$ to ∞ . Therefore, the phase states $|\delta\rangle$ are eigenstates of the tunneling Hamiltonian H_T with corresponding eigenvalues $-E_J \cos \delta$, for $\delta \in [0, 2\pi]$.

Assuming $\lambda_{T,\delta} = -E_J \cos \delta$, i.e. the energy of state $|\delta\rangle$ associated with tunneling, the group velocity is

$$v_g \equiv \frac{1}{\hbar} \frac{\partial \lambda_{T,\delta}}{\partial \delta} = \frac{E_J}{\hbar} \sin \delta.$$

Q4

Can you always take the square root of a unitary matrix? That is, given a unitary U , does there always exist a \sqrt{U} such that $\sqrt{U}\sqrt{U} = U$?

Solution

Yes, but the square root is not unique. By definition, a complex square matrix U is unitary iff its conjugate transpose is also its inverse:

$$U \text{ is unitary} \iff U^\dagger = U^{-1}, \quad (16)$$

where the inverse of U , denoted U^{-1} , is defined as the matrix that, when left- or right-multiplied by U , produces the identity:

$$U^{-1} \text{ is the inverse of } U \iff UU^{-1} = U^{-1}U = \mathbf{1}. \quad (17)$$

It immediately follows that U is normal. By definition, a complex square matrix N is normal iff it commutes with its conjugate transpose:

$$N \text{ is normal} \iff NN^\dagger = N^\dagger N. \quad (18)$$

Therefore, by definitions (16) and (17),

$$UU^\dagger = \mathbb{1} = U^\dagger U \implies U \text{ is normal.}$$

Furthermore, a matrix is normal iff it is unitarily diagonalizable.²⁰ Consider the forward direction. By the Schur decomposition, any complex square matrix U can be written

$$U = VDV^\dagger,$$

where V is unitary and D is upper-triangular. Then $UU^\dagger = V(DD^\dagger)V^\dagger$ by unitarity of V , and likewise $U^\dagger U = V(D^\dagger D)V^\dagger$. If U is normal, then $DD^\dagger = D^\dagger D$ and D is also normal. Hence D is in fact diagonal, since a normal upper-triangular matrix can only have nonzero elements along the diagonal (this follows trivially from the definition (18) and upper-triangularity). Thus U is unitarily diagonalizable.

Given that U can be unitarily diagonalized and given the fact that $U^\dagger U = 1$, this implies that the eigenvalues of U can be written as:

$$\lambda_j = e^{i\phi_j},$$

where λ_j designates the j^{th} eigenvalue of U . Then,

$$D = \begin{pmatrix} \ddots & & \\ & \lambda_j & \\ & & \ddots \end{pmatrix}$$

In the basis where U is diagonal, its square root is obtained simply by taking the square root of the eigenvalues, i.e.

$$D^{1/2} = \begin{pmatrix} \ddots & & \\ & \sqrt{\lambda_{j\pm}} & \\ & & \ddots \end{pmatrix}.$$

However, for each eigenvalue, there are two possible values of the square root:

$$\sqrt{\lambda_{j+}} = e^{i\phi_j/2} \text{ and } \sqrt{\lambda_{j-}} = e^{i(\phi_j/2+\pi)}.$$

If matrix $U \in \mathbb{C}^{N \times N}$, then there are 2^N possible combinations of $\sqrt{\lambda_{j+}}$ and $\sqrt{\lambda_{j-}}$. Therefore, a unitary matrix has a square root, but there are 2^N different \sqrt{U} . By construction, in the original basis

$$\sqrt{U} = VD^{1/2}V^\dagger.$$

Q5

Prove the following points:

²⁰This is a version of the spectral theorem.

- a) Two quantum states will lead to different probabilities iff they have different density matrices.
- b) No-communication theorem: if Alice and Bob share an entangled state, nothing Alice chooses to do will have any effect on Bob's density matrix \rightarrow There is no observable effect on Bob's end.

Solution

- a) Suppose we measure a mixed state $(p_i, |\psi_i\rangle)$ in an orthonormal basis $|\beta_k\rangle$. Let's calculate the outcome:

We denote the probability of measuring $|\beta_k\rangle$ by $\text{Pr}[k]$. Then

$$\begin{aligned}
 \text{Pr}[k] &= \sum_j p_j |\langle \psi_j | \beta_k \rangle|^2 \\
 &= \sum_j p_j \langle \beta_k | \psi_j \rangle \langle \psi_j | \beta_k \rangle \\
 &= \langle \beta_k | \sum_j p_j |\psi_j\rangle \langle \psi_j| | \beta_k \rangle \\
 &= \langle \beta_k | \rho | \beta_k \rangle
 \end{aligned}$$

Therefore different probabilities (LHS) will lead us different density matrices (RHS) and vice versa.

- b) Consider an arbitrary bipartite state,

$$\rho = \sum_{ijkl} \rho_{ijkl} \underbrace{|i\rangle\langle j|}_A \otimes \underbrace{|k\rangle\langle \ell|}_B,$$

where we take the bases in each subspace to be orthonormal without loss of generality. The reduced density matrix for Bob is²¹

$$\begin{aligned}
 \rho_B &= \text{Tr}_A \rho \\
 &= \sum_m \langle m | \rho | m \rangle && \text{note: } |m\rangle \in \mathcal{H}_A \\
 &= \sum_{ijklm} \rho_{ijkl} \langle m | i \rangle \langle j | m \rangle |k\rangle\langle \ell| && \text{note: } \langle m | i \rangle = \delta_{mi}, \langle j | m \rangle = \delta_{jm} \\
 &= \sum_{k\ell m} \rho_{mmk\ell} |k\rangle\langle \ell|. \tag{19}
 \end{aligned}$$

Suppose Alice performs a local unitary operation, $U : \mathcal{H}_A \rightarrow \mathcal{H}_A$, on her subsystem. The new bipartite state becomes

$$\begin{aligned}
 \rho' &= U \rho U^\dagger \\
 &= \sum_{ijkl} \rho_{ijkl} U |i\rangle\langle j| U^\dagger \otimes |k\rangle\langle \ell|,
 \end{aligned}$$

²¹The trace is basis-independent. For simplicity and without loss of generality, we take the trace with respect to the same orthonormal basis in which Alice's subspace is decomposed.

yet Bob's reduced density matrix remains invariant:

$$\begin{aligned}
\rho_B &= \text{Tr}_A \rho' \\
&= \sum_{ijklm} \rho_{ijkl} \langle m|U|i\rangle \langle j|U^\dagger|m\rangle |k\rangle\langle\ell| && \text{commute scalar matrix elements} \\
&= \sum_{ijklm} \rho_{ijkl} \langle j|U^\dagger|m\rangle \langle m|U|i\rangle |k\rangle\langle\ell| && \text{remove identity } \sum_m |m\rangle\langle m| = \mathbb{1} \\
&= \sum_{ijkl} \rho_{ijkl} \langle j|U^\dagger U|i\rangle |k\rangle\langle\ell| && \text{by unitarity, } U^\dagger U = \mathbb{1} \\
&= \sum_{ijkl} \rho_{ijkl} \langle j|i\rangle |k\rangle\langle\ell| && \text{by orthonormality, } \langle j|i\rangle = \delta_{ji} \\
&= \sum_{jkl} \rho_{jjkl} |k\rangle\langle\ell|. \tag{20}
\end{aligned}$$

In either case, Bob's reduced density matrix (19) or (20) is the same.

In particular, even if ρ is maximally entangled (and therefore pure), there is no operation Alice can perform on her subsystem that will be observable by Bob. Therefore, entanglement does not enable faster-than-light communication.

Q6

Can different probability distributions over pure states give rise to the same mixed state?

Solution

Yes. Consider a uniform distribution over the σ_z eigenstates, $\{(\frac{1}{2}, |0\rangle), (\frac{1}{2}, |1\rangle)\}$. This gives rise to the mixed state

$$\rho = \frac{1}{2} |0\rangle\langle 0| + \frac{1}{2} |1\rangle\langle 1| = \frac{1}{2} \mathbb{1}$$

in the σ_z eigenbasis. However, the identity operator $\mathbb{1}$ has the same representation,

$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, in every orthonormal basis. For instance, consider a uniform distribution over the σ_x eigenstates, $\{(\frac{1}{2}, |+\rangle), (\frac{1}{2}, |-\rangle)\}$. This gives rise to the mixed state

$$\rho = \frac{1}{2} |+\rangle\langle +| + \frac{1}{2} |-\rangle\langle -| = \frac{1}{2} \mathbb{1},$$

now in the σ_x eigenbasis. But, noting $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$,

$$\begin{aligned}
\mathbb{1} &= |+\rangle\langle +| + |-\rangle\langle -| \\
&= \frac{1}{2} (|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + |1\rangle\langle 1|) \\
&\quad + \frac{1}{2} (|0\rangle\langle 0| - |0\rangle\langle 1| - |1\rangle\langle 0| + |1\rangle\langle 1|) \\
&= |0\rangle\langle 0| + |1\rangle\langle 1| = \mathbb{1}.
\end{aligned}$$

This is obvious if we consider the unitary transformation U connecting the two bases, whereby $U\mathbb{1}U^\dagger = UU^\dagger = \mathbb{1}$.

Although one might think that a uniform distribution over $\{|0\rangle, |1\rangle\}$ is physically distinct from a uniform distribution over $\{|+\rangle, |-\rangle\}$ —corresponding to, say, an ensemble of spins with half aligned along $+\hat{z}$ and the other half along $-\hat{z}$, versus an ensemble with half along $+\hat{x}$ and half along $-\hat{x}$ —in fact, there is no measurement which can distinguish between the two.

Q7

Find a maximally mixed state of a 2-qubit system.

Solution

Given the computational basis for a two qubit system, $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, the maximally mixed state is an ensemble mix of all the states with equal probability:

$$\rho = \frac{1}{4}(|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| + |11\rangle\langle 11|)$$

It is trivial to see that the rank of the density matrix is 4, as for a maximally entangled state. In general, for a system of n qubits, with computational basis elements $\{|i\rangle : i = 0, 1, \dots, 2^n - 1\}$, the maximally mixed state is: $\rho = \mathbb{1}/2^n$, which has rank 2^n . The von Neumann entropy of these states is maximal and follows a volume law:

$$S = -\text{Tr}(\rho \log_2 \rho) = -\sum_{i=0}^{2^n-1} \frac{1}{2^n} \log_2 \frac{1}{2^n} = n.$$

Q8

Implement superdense coding in Qiskit. Attach the code and results.

Solution

In this case Alice has two classical bits she wants to send to Bob by just sending one quantum bit. In the following implementation we will map all 4 possible combinations of the two bits to integers from 0 to 3: $00 \rightarrow 0$, $01 \rightarrow 1$, $10 \rightarrow 2$ and $11 \rightarrow 3$.

The algorithm proceeds as follows:

1. Alice decides which combination of two classical bits she wants to send between possibilities 0 to 3. In the qiskit implementation this is stored in variable "bit". In this example Alice wants to send 11 to Bob:

```
#Usual imports
import qiskit
import numpy as np

bit = 3
```

2. Alice and Bob share a maximally entangled qubit pair: $|\psi_0\rangle = \frac{1}{\sqrt{2}}(|0_A 0_B\rangle + |1_A 1_B\rangle)$. In this notation the most significant bit corresponds to Alice. The initial state of the qubits is $|00\rangle$. Therefore, to put the system into state $|\psi_0\rangle$ we apply a Hadamard gate on Alice's qubit and a CNOT(A \rightarrow B) gate where the control qubit is Alice's and the target one is Bob's ($|\psi_0\rangle = \text{CNOT}(A \rightarrow B)H(A)|00\rangle$):

```
#Define the quantum circuit with two classical
#registers and two qubits
qc = QuantumCircuit(2,2)

#Create the entangled pair shared by Alice and Bob
qc.h(0) #Hadamard on 0
qc.cx(0,1) #CNOT where 0 is the control and 1 is target
```

3. Alice performs one operation on her qubit depending on what pair of classical bits she wants to send:

$$\begin{aligned}
00 &\rightarrow \mathbb{1}_A \otimes \mathbb{1}_B |\psi_0\rangle = |\psi_{00}\rangle \frac{1}{\sqrt{2}}(|0_A 0_B\rangle + |1_A 1_B\rangle) \\
01 &\rightarrow X_A \otimes \mathbb{1}_B |\psi_0\rangle = |\psi_{01}\rangle \frac{1}{\sqrt{2}}(|0_A 1_B\rangle + |1_A 0_B\rangle) \\
10 &\rightarrow Z_A \otimes \mathbb{1}_B |\psi_0\rangle = |\psi_{10}\rangle \frac{1}{\sqrt{2}}(|0_A 0_B\rangle - |1_A 1_B\rangle) \\
11 &\rightarrow ZX_A \otimes \mathbb{1}_B |\psi_0\rangle = |\psi_{11}\rangle \frac{1}{\sqrt{2}}(|0_A 1_B\rangle - |1_A 0_B\rangle).
\end{aligned}$$

Which in Qiskit is implemented as follows:

```
if bit == 1: #Sending 01
    qc.x(0)
if bit == 2: #Sending 10
    qc.z(0)
if bit == 3: #Sending 11
    qc.x(0)
    qc.z(0)
```

4. Alice sends her qubit to Bob over a quantum channel. Nothing to do on Qiskit.
5. Bob, who now has the two qubits, applies a CNOT(A \rightarrow B) gate and then applies a Hadamard gate to the qubit that used to belong to Alice. Bob obtains the following set of orthogonal states depending on what qubit Alice sent him:

$$\begin{aligned}
00 &\rightarrow H_A \otimes \mathbb{1}_B \cdot \text{CNOT}(A \rightarrow B) |\psi_{00}\rangle = |00\rangle \\
01 &\rightarrow H_A \otimes \mathbb{1}_B \cdot \text{CNOT}(A \rightarrow B) |\psi_{01}\rangle = |01\rangle \\
10 &\rightarrow H_A \otimes \mathbb{1}_B \cdot \text{CNOT}(A \rightarrow B) |\psi_{10}\rangle = |10\rangle \\
11 &\rightarrow H_A \otimes \mathbb{1}_B \cdot \text{CNOT}(A \rightarrow B) |\psi_{11}\rangle = |11\rangle.
\end{aligned}$$

Bob finally measures the two qubits in the computational basis, obtaining precisely the two classical bits Alice wanted to send. This final step with the simulation of the whole process is implemented in Qiskit:

```

qc.cx(0,1) #Applying the CNOT
qc.h(0) #Applying the Hadamard to Alice's qubit
qc.measure(0,0) #Measuring qubit that used to belong to Alice
qc.measure(1,1) #Measuring qubit that always belonged to Bob

#Simulation using qasm simulator
Measurements = 2000 #Number of measurements
emulator = Aer.get_backend('qasm_simulator')
job = execute(qc, emulator, shots = Measurements)
hist = job.result().get_counts() #results of the measurement
print(hist) #Print results

```

The code will be attached in the email as a “jupyter notebook”. For the results, even using the “qasm” simulator, feeding the program with “bit” = 0 gave output 00 with probability exactly 1. Feeding the program with “bit” = 1 gave output 10 with probability exactly 1. Feeding the program with “bit” = 2 gave output 01 with probability exactly 1, and feeding the program with “bit” = 3 gave output 11 with probability exactly 1. Note that the output for “bit” = 1 and “bit” = 2 are swapped. This is because Qiskit takes the zeroth qubit to be the least significant one. However, the results are correct.

Q9

What choice of $\lambda_1, \dots, \lambda_n$ maximizes the entropy,

$$S(\rho) = - \sum_k \lambda_k \log_2 \lambda_k,$$

where $\sum_k \lambda_k = 1$.

Solution

The von Neumann entropy expressed in units of bits,

$$S(\rho) = - \sum_k \lambda_k \log_2 \lambda_k, \quad (21)$$

may be straightforwardly extremized over all diagonal density operators ρ with eigenvalues λ_k , subject to the probability conservation constraint,

$$\sum_k \lambda_k = 1, \quad (22)$$

by the method of Lagrange multipliers. We form the Lagrange function

$$\mathcal{L}(\{\lambda_k\}, \eta) = S(\rho) - \eta \left(\sum_k \lambda_k - 1 \right),$$

and then vary each parameter $\{\lambda_k\}, \eta$ independently to find the stationary point in the parameter space. Variation with respect to η recovers the probability constraint (22),

while variation with respect to each $\lambda_j \in \{\lambda_k\}$ yields

$$\frac{\partial \mathcal{L}}{\partial \lambda_j} = -(\log_2 \lambda_j + 1) - \eta = 0, \quad \forall j$$

which must vanish at the stationary point. This implies

$$\lambda_j = 2^{-(\eta+1)}, \quad \forall j,$$

i.e. all λ_j 's are equal to the same constant. Enforcing the probability constraint (22) determines η such that

$$\lambda_j = 2^{-n} = \frac{1}{D}, \quad \forall j$$

for n qubits, or Hilbert space dimension $D = 2^n$. Therefore, the von Neumann entropy is maximized²² when $\{\lambda_k\}$ is a uniform distribution, i.e. when ρ is a (\sim classical) maximally mixed state. Moreover, this state is unique.

In the above, we assumed ρ is diagonal, but note that any ρ can be diagonalized and the von Neumann entropy is basis-independent, as

$$\begin{aligned} \rho &= U \rho_d U^\dagger \\ \implies S &= -\text{Tr}(\rho \ln \rho) \\ &= -\text{Tr}\left(U \rho_d U^\dagger \ln[U \rho_d U^\dagger]\right) \\ &= -\text{Tr}\left(U \rho_d U^\dagger [U \ln(\rho_d) U^\dagger]\right) \\ &= -\text{Tr}\left(U \rho_d \ln(\rho_d) U^\dagger\right) \\ &= -\text{Tr}(\rho_d \ln \rho_d) \end{aligned}$$

where the final equality follows the cyclicity of the trace.

For the sake of completeness, note that since $0 \leq \lambda_k \leq 1 \quad \forall k$, the von Neumann entropy $S(\rho) \geq 0$ according to (21). This lower bound is attained for $\lambda_k = 1$ for some particular k and $\lambda_k = 0$ for all others. This occurs for any ρ representing a pure state. So we conclude

$$0 \leq S(\rho) \leq \ln D$$

where the upper bound is attained for the (unique) maximally mixed state $\rho = \mathbf{1}/D$, while the lower bound is attained for every (i.e. not unique) pure state ρ .

Q10

1D harmonic oscillator:

$$\begin{aligned} H |n\rangle &= \hbar\omega\left(n + \frac{1}{2}\right) |n\rangle \\ a |\alpha\rangle &= \alpha |\alpha\rangle \\ |\alpha\rangle, (|\alpha|, n) \end{aligned}$$

a) Time evolution of coherent state.

²²One can verify this extremum is a maximum using a [bordered Hessian](#) test.

b) Calculate:

$$\begin{aligned}\langle x(t) \rangle &= \langle \alpha(t) | x | \alpha(t) \rangle \\ \langle p(t) \rangle &= \langle \alpha(t) | p | \alpha(t) \rangle\end{aligned}$$

c) Consider the mixed state:

$$\rho = \frac{1}{2\pi} \int_0^{2\pi} d\phi \, ||\alpha| \exp(i\phi)\rangle \langle \alpha| \exp(i\phi)|,$$

a mixture of coherent states with random phase and fixed amplitude $|\alpha|$. Show this is equivalent to a mixture of coherent states with a Poisson distribution with $\bar{n} = |\alpha|^2$.

Solution

a) We first expand the coherent state $|\alpha\rangle$ in the Fock basis (derived in our solution to HW2 Problem 2), as

$$|\alpha\rangle = e^{-\frac{1}{2}|\alpha|^2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle. \quad (23)$$

The time evolution of the coherent state is then obtained by time-evolving the individual Fock-state components. These are energy eigenstates of the harmonic oscillator with energy $E_n = \hbar\omega(n + \frac{1}{2})$. Their time evolution follows from the Schrödinger equation as

$$|n\rangle \longrightarrow e^{-in\omega t} e^{-\frac{i\omega t}{2}} |n\rangle,$$

which yields the time-evolved coherent state

$$|\alpha(t)\rangle = e^{-\frac{i\omega t}{2}} e^{-\frac{1}{2}|\alpha|^2} \sum_{n=0}^{\infty} \frac{(\alpha e^{-i\omega t})^n}{\sqrt{n!}} |n\rangle \quad (24)$$

If we define

$$\alpha(t) = \alpha e^{-i\omega t}, \quad (25)$$

then $|\alpha(t)\rangle$ is given by Eq. (23) with $\alpha \rightarrow \alpha(t)$, times a global phase factor $\exp(-i\omega t/2)$.

b) We can write the position and momentum operator in terms of creation and annihilation operators:

$$x = \sqrt{\frac{\hbar}{2m\omega}} (a^\dagger + a), \quad p = i\sqrt{\frac{m\hbar\omega}{2}} (a^\dagger - a).$$

Note that the eigenvalue equation for the coherent state holds at all times,

$$a |\alpha(t)\rangle = \alpha(t) |\alpha(t)\rangle,$$

where the eigenvalue is given by Eq. (25). It is then straightforward to compute

$$\begin{aligned}\langle \alpha(t) | x | \alpha(t) \rangle &= \sqrt{\frac{\hbar}{2m\omega}} (\alpha^* e^{i\omega t} + \alpha e^{-i\omega t}) = x_0 \cos(\omega t - \phi) \\ \langle \alpha(t) | p | \alpha(t) \rangle &= i\sqrt{\frac{m\hbar\omega}{2}} (\alpha^* e^{i\omega t} - \alpha e^{-i\omega t}) = -m\omega x_0 \sin(\omega t - \phi),\end{aligned}$$

where we have defined $\alpha = |\alpha| e^{i\phi}$ and $x_0 = |\alpha| \sqrt{2\hbar/m\omega}$.

- c) In this case we wish to compute the density matrix for the time evolution of state $|\alpha(t)\rangle$ given by Eq. (24). By definition, we wish to compute:

$$\begin{aligned}\rho &= \frac{1}{2\pi} \int_0^{2\pi} d\phi \left| |\alpha|e^{i\phi} \right\rangle \left\langle |\alpha|e^{i\phi} \right| = \frac{e^{-|\alpha|^2}}{2\pi} \int_0^{2\pi} d\phi \sum_{m,n} \frac{(|\alpha|e^{-i\phi}e^{i\omega t})^n (|\alpha|e^{i\phi}e^{-i\omega t})^m}{\sqrt{n!m!}} |m\rangle \langle n| = \\ &= \sum_{n,m} \frac{e^{-|\alpha|^2} |\alpha|^{n+m} e^{-i\omega t(m-n)} \frac{1}{2\pi} \int_0^{2\pi} d\phi e^{i\phi(m-n)}}{\sqrt{n!m!}} |m\rangle \langle n|\end{aligned}$$

Now, taking into account that $\frac{1}{2\pi} \int_0^{2\pi} e^{i\phi(m-n)} = \delta_{m,n}$, we end up obtaining:

$$\rho = \sum_{n=0}^{\infty} \frac{e^{-|\alpha|^2} (|\alpha|^2)^n}{n!} |n\rangle \langle n|$$

Finally recalling that Poisson distribution of average λ is $f(\lambda, n) = \frac{e^{-\lambda} \lambda^n}{n!}$, we see that our density matrix is poisson distributed with average $|\alpha|^2$.

Q11

- Design your own quantum bank that produces quantum money.
- what are the odds for hacking your quantum money?

Solution

- In this scheme, a piece of quantum money comprises an n -qubit “bill” state and a classical serial number. The quantum bank issues money by generating a bill state and assigning it a unique serial number. The description of each issued bill state and its corresponding serial number are stored in a secret ledger maintained by the bank. A vendor, upon receiving a piece of quantum money from a customer, sends the bill state and its serial number to the bank for verification. The bank uses the serial number to look up the bill state description in the ledger and compare it to the bill state received from the vendor. If they match, the transaction is approved.
- The security and performance of this scheme hinges on how the bank produces the n -qubit bill state. One potential method of state generation follows. For each qubit, the bank randomly selects a basis, say σ_x or σ_z , and randomly assigns an eigenstate of that basis to the value of the qubit, i.e. $|0\rangle$ or $|1\rangle$ for σ_z and $|+\rangle$ or $|-\rangle$ for σ_x . The n -qubit bill state can then be prepared by single-qubit rotations, with a typical bill state looking something like,

$$\underbrace{|+ 0 1 - + + - 0 + - 1 - 0 0 1 0 + + 0 0 \dots\rangle}_{n \text{ qubits}}.$$

Note that the space complexity for storing the bill description in the ledger is $\mathcal{O}(n)$, since for each qubit we need to store 1 bit specifying the basis and 1 bit specifying the eigenstate. Furthermore, forging bill states is prohibited by the no-cloning theorem, since the counterfeiter does not know the basis used for

each qubit. Therefore, possession of a bill state does not allow duplicates to be produced.

Given the serial number, the only counterfeiting strategy is to attempt to guess the bill state. Assuming the counterfeiter knows the basis set $\{\sigma_x, \sigma_z\}$, the probability of guessing the correct basis is $1/2$, and the probability of guessing the correct eigenstate within that basis is also $1/2$, so the probability of getting the state of any qubit exactly correct is $1/4$. However, if the counterfeiter guesses the incorrect basis, it is still possible that the bank measures the correct eigenstate during the verification process. Since each wrong-basis eigenstate is a uniform superposition of the right-basis eigenstates, this occurs with probability $1/2$. The probability for the bank to erroneously approve a counterfeit 1-qubit bill state is then

$$\underbrace{\Pr(\text{right eigenstate}|\text{right basis})}_{1} \underbrace{\Pr(\text{right basis})}_{1/2} + \underbrace{\Pr(\text{right eigenstate}|\text{wrong basis})}_{1/2} \underbrace{\Pr(\text{wrong basis})}_{1/2} = 3/4$$

For an n -qubit bill state, every qubit must be approved individually, with a single wrong outcome identifying a counterfeit. The total probability for the bank to erroneously approve a counterfeit n -qubit bill state is then $(3/4)^n$ and is shown in Fig. 6. This scheme is therefore exponentially secure in the number of qubits used for the bill state.²³

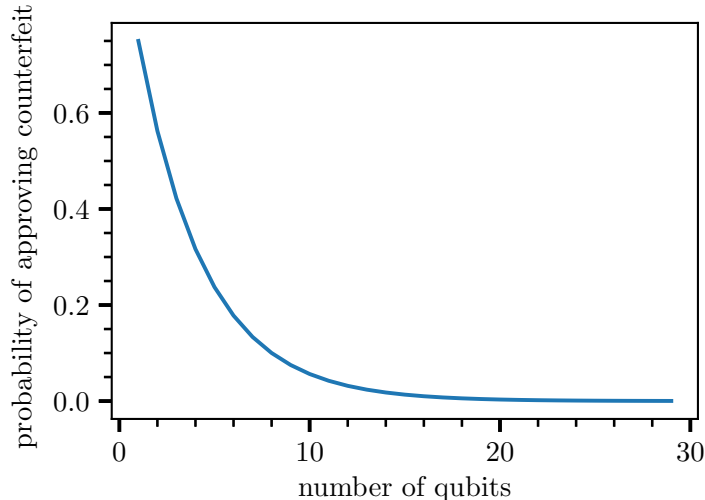


Figure 6: The probability of approving a counterfeit is $(3/4)^n$ where n is the number of qubits.

²³Note that this security analysis is identical to that of the BB84 protocol. Our quantum money scheme is essentially the same as BB84, with the counterfeiter playing the role of the eavesdropper.

Q12

There exist bipartite states that take a lot of entanglement to make but you can only extract a small fraction of the entanglement. Find an example and show $E_f \gg E_D$ can be achieved by extension for larger qubit systems.

Solution

This question is a very active field of research in the moment and it is actually very complicated to answer. Here we will give a simple toy model answer and describe some of the recent works about this matter.

One simple case of such bipartite states that take more entanglement to make than the entanglement you can measure is for example a system with 3 qubits. Suppose that subsystem A is qubit 0 and subsystem B is qubits 1 and 2. Now, imagine that qubits 1 and 2 are in a Bell state:

$$|\psi\rangle_{1,2} = \frac{|11\rangle_{1,2} + |00\rangle_{1,2}}{\sqrt{2}}$$

and qubit number 0 is for example in state $|\psi\rangle_0 = |0\rangle_0$. Then state of the whole system is:

$$|\psi\rangle_{0,1,2} = |0\rangle_0 \otimes \frac{|11\rangle_{1,2} + |00\rangle_{1,2}}{\sqrt{2}}.$$

In this case, the entanglement of formation is 1 as we created a Bell pair in qubits 1 and 2, however, the entanglement between subsystem A and subsystem B is zero and therefore we cannot extract any entanglement out of this partition of the state. Therefore $E_D < E_f$.

In the case of having many qubits, we can choose to split the system in a certain way obtaining subsystems A and B. Now imagine that qubits are laid out in a 1D chain and we form a Bell state of nearest neighbours in subsystem A and do the same in subsystem B, but we don't form a Bell pair between the qubits in the boundaries of A and B. In this case, the total number of Bell pairs we needed to form the state was of the order of the number of qubits, but subsystem A is not entangled with subsystem B and therefore the amount of entanglement I get out of this partition is zero and therefore $E_f \gg E_D$.

Recent studies focus on the entanglement of formation and distillation from a more systematic point of view. Given N copies of a bipartite state ρ_{AB} , we can imagine extracting M copies of a Bell state $|\psi^-\rangle\langle\psi^-|$ using only local operations and classical communication (LOCC),

$$\rho_{AB}^{\otimes N} \xrightarrow{\text{LOCC}} |\psi^-\rangle\langle\psi^-|^{\otimes M}.$$

This process is known as entanglement concentration or distillation. The *distillable entanglement* $E_D(\rho_{AB})$ is the largest value of M/N attainable as $N \rightarrow \infty$. This can be understood as the largest number of Bell states that can be distilled from the given bipartite state.

Conversely, we can imagine starting with M copies of a Bell state and mixing them into N copies of a given bipartite state using LOCC,

$$|\psi^-\rangle\langle\psi^-|^{\otimes M} \xrightarrow{\text{LOCC}} \rho_{AB}^{\otimes N}.$$

This process is known as entanglement dilution. The *entanglement cost* $E_C(\rho_{AB})$ is the *smallest* value of M/N attainable as $N \rightarrow \infty$. It is therefore the asymptotic limit of the entanglement of formation. This can be understood as the smallest number of Bell states required to form the bipartite state.

Since any measure of entanglement cannot increase under LOCC, we must have $E_C(\rho_{AB}) \geq E_D(\rho_{AB})$. Intuitively, one might expect that entanglement distillation and dilution are asymptotically reversible, i.e.

$$|\psi^-\rangle\langle\psi^-|^{\otimes M} \xleftrightarrow{\text{LOCC}} \rho_{AB}^{\otimes N},$$

such that the bound is saturated as $N \rightarrow \infty$. Indeed, for pure states, this is in fact the case, and $E_C = E_D = S(\rho_A)$, the von Neumann entropy of the reduced state of ρ_{AB} .

For mixed states or multipartite entangled states, however, entanglement distillation/dilution is irreversible in the asymptotic limit, and consequently $E_C > E_D$. These processes can therefore be thought of as a type of lossy compression/decompression algorithm. [Horodecki et al.](#) showed the existence of so-called bound entangled states which require entanglement to create, but from which no entanglement can be distilled. [Vidal and Cirac](#) generalized this result to the asymptotic limit. Subsequently, [Vollbrecht et al.](#) showed that mixtures of maximally entangled states can be diluted and distilled reversibly if and only if they realize the lower bound of the Heisenberg uncertainty principle, demonstrating that irreversibility is a generic and common phenomenon. This remains an active area of research. For a more detailed overview of the various entanglement measures and their associated theorems, see Ref. [3].

Q13

Qiskit: Make a circuit to generate a random number between 0 and 2^3-1 . What is the entropy? repeat for 0 and $2^{15}-1$. how much does the entropy change?

Solution

In this case, we will design the simplest random number generator possible, even though in the literature one can find more refined algorithms that take into account that the quantum hardware can be biased (for cryptography applications). These algorithms are all based on the CHSH game with certain variations.

Here we will consider that our quantum hardware is not biased (the NSA has not included a back door) and that therefore we have a perfect quantum device that we have fabricated ourselves. In this case, the task is fairly simple, if we want a random 1-bit generator, we just need to put one qubit in state $|+\rangle$ and measure in the computational basis outputs $|0\rangle$ or $|1\rangle$ with complete randomness and probability $1/2$. Therefore, the protocol is clear if we want to generate a random number between 0 and $2^n - 1$: take n qubits in the computational basis, put all of them in state $|+\rangle$ and measure them in the computational basis. Then, the result of your measurement represents the desired number in binary representation. Note that the random numbers between 0 and $2^n - 1$ will be uniformly sampled with probability $1/2^n$. In this sense, the quantum entropy is 0 as the state of the system is separable, but the classical entropy of the random number probability distribution is maximal: $S = -\sum_x p_x \log_2 p_x = n$, as $p_x = 1/2^n$ for every random number x generated.

This algorithm can also be done with one qubit, where you prepare it to be in the state $|+\rangle$ and then measure it in the computational basis. The process is repeated n times and the output of the measurements is ordered to generate the desired random number in binary representation as depicted in Figure 7 a). This approach might be better in terms of accuracy in NISQ devices where we can have one qubit with better fidelity and decay times than the rest and therefore the errors will be smaller by just using this 1-qubit device. This is the reason why we will implement this approach in Qiskit, just using a circuit with 1 qubit. It also has the advantage that it can be simulated in a classical computer fairly fast. Otherwise it would be pretty hard to simulate the case with 15 qubits.

The Qiskit code we wrote is fairly simple, it is a function that takes as an input the number of random bits to be generated n and outputs the random distribution as a numpy array. In this case, the quantum circuit described above is simulated using the 'qasm' simulator:

```
##### generate random numbers between 0 and  $2^{n-1}$ #####
#need to pass n to the function
def RandomNumberGen(n):
    num = np.zeros(n)
    for i in range(n):
        qc = QuantumCircuit(1,1)
        qc.h(0) #get + state
        qc.measure(0,0) #measure in computational basis

        #Simulate and get results
        emulator = Aer.get_backend('qasm_simulator')
        job = execute(qc, emulator, shots = 1)
        hist = job.result().get_counts()
        if hist.get('0') == None:
            num[i] = 1
        if hist.get('1') == None:
            num[i] = 0
    return num
```

In order to test our random number generator put it under two standard tests: the first one is analyzing if the distribution is uniformly sampled and the second one is making sure that samples are not correlated to each other. By samples, bits corresponding to the same random number are not correlated to each other.

Figure 7 b) and c) show the probability of generating random number x between 0 and 2^n for $n = 3$ (panel b)) and for $n = 15$ (panel c)). Note this probability distributions should be flat and have a probability of $1/2^n$. The error bars correspond to $1/\sqrt{samps}$ according to the central limit theorem, where $samps = 10^3$ is the number of random numbers generated. Note that for $n = 15$ the error bars are much larger than the actual probability. This is due to the fact that the number of possible outputs of the random number generator is exponentially large and in order to do a good sampling of the probability distribution we would need to collect exponentially many samples, which we cannot do with our laptops. However, both for $n = 3$ and $n = 15$, the simulated values of the probabilities agree with the uniform probability distribution within the

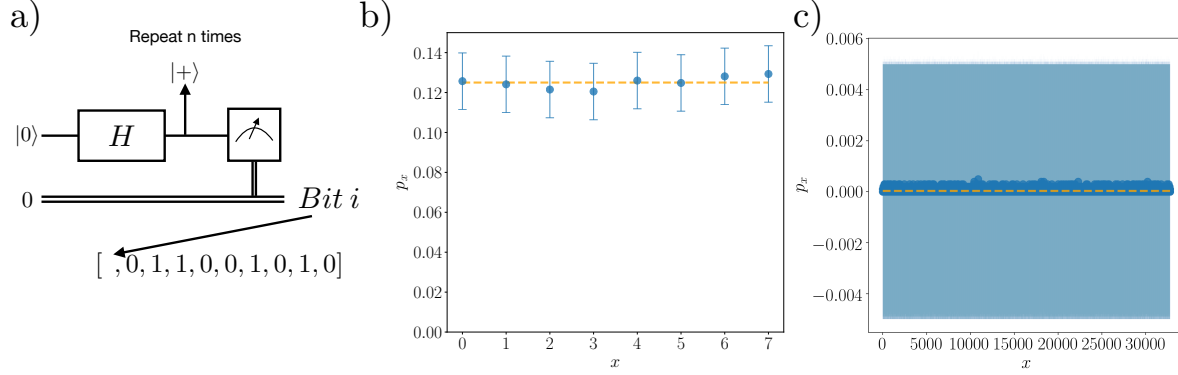


Figure 7: **a)** Schematic representation of the procedure followed to generate random numbers. **b)** Probability distribution of obtaining number x with our random number generator if $n = 3$. Orange dashed line represents the expected value for the probability of obtaining each number: $1/2^n$. **c)** Probability distribution of obtaining number x with our random number generator if $n = 15$. The blue cloud are the error bars. Orange dashed line represents the expected value for the probability of obtaining each number: $1/2^n$

error bars.

The second check our random number generator needs to pass is that the samples are not correlated to each other. Pseudo-random number generators satisfy this condition, so this does not prove pure randomness (because it is impossible to test in a classical computer) but it is a sanity check random numbers should satisfy. To test it, within the same random number, we will compute the correlation between two bits and average over the number of samples taken:

$$C_{i,j} = \langle (x_i - x_j)^2 \rangle - \langle x_i^2 \rangle - \langle x_j^2 \rangle$$

where x_i and x_j are the bits in relevant positions i and j of random number x . Figure 8 shows the average correlations for $n = 3$ and $n = 15$ averaged over $samps = 10^3$ random numbers. It proves that within the error bars, the correlations are zero and therefore our random number generator does not generate correlated bits. **All the code to generate the correlation maps and to collect the statistics is attached as a Jupyter Notebook.**

Q14

Here we prove the optimal quantum strategy to the CHSH game. We assume the following rules:

1. Alice and Bob agree on strategy. Thereafter, they can perform local operations, but they cannot communicate classically.
2. Alice and Bob respectively receive a random bit x and y from the referee.
3. Alice and Bob respectively return bits a and b to the referee.
4. Alice and Bob win iff

$$a + b = xy \pmod{2}. \quad (26)$$

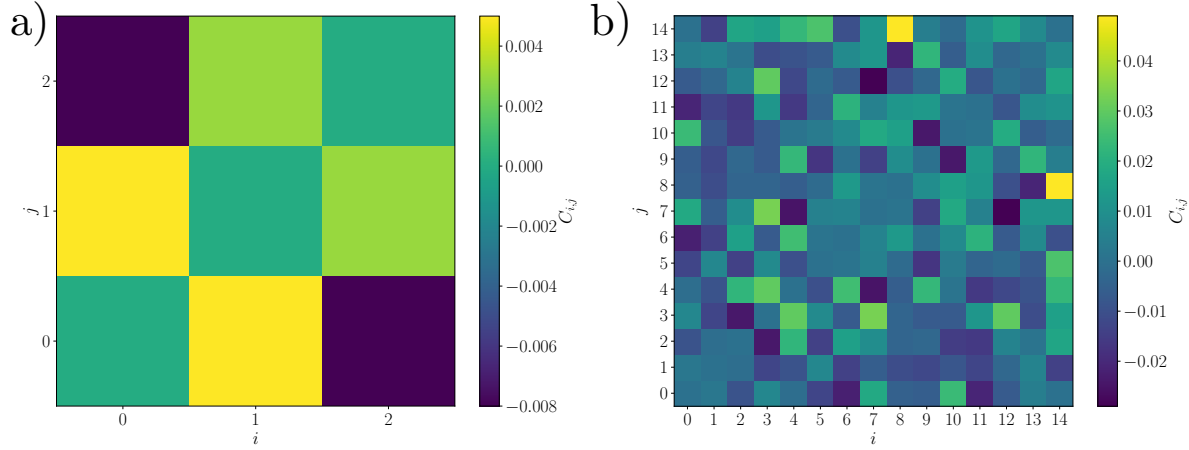


Figure 8: **a)** $n = 3$ **b)** $n = 15$. Correlation between bits i and j of a given random number, averaged over all the random numbers generated $samps = 10^3$

We first consider the classical case. In the win condition, $a + b = 1 \Leftrightarrow a \neq b$. Similarly, $xy = 1 \Leftrightarrow x = y = 1$. If all bits are chosen at random, the former condition occurs with probability $1/2$, while the latter occurs with probability $1/4$. The following truth table then enumerates all possible outcomes and their probabilities:

$a \neq b$	$x = y = 1$	Win	Prob.
T	T	T	1/8
T	F	F	3/8
F	T	F	1/8
F	F	T	3/8

(27)

Therefore, if Alice and Bob choose a and b uniformly at random, they win with probability $1/2$. The optimal classical strategy is for Alice and Bob to agree beforehand to always choose $a = b$ (either both 0 or both 1, always). This eliminates the first two rows of the table (where they are likely to lose), and they win with probability $3/4$. We show that this is optimal by considering Alice's point of view (Bob's is symmetric) in the absence of any strategy. Note that the value of x contains no information as to how she should choose a : if $x = 1$, the probabilities in each row are unaffected (since she doesn't know y), while if $x = 0$, only the second and fourth rows remain, where they still win and lose with equal probability. Therefore, Alice needs knowledge of b so she can choose the fourth row in the case $x = 0$. If she has *perfect* knowledge of b , they will always win in this case (by choosing $a = b$), while they can still only win $1/2$ of the cases where $x = 1$. Since $x = 0$ (always win) and $x = 1$ (win $1/2$) are equally likely, they win with probability $3/4$, and any uncertainty in b will only reduce their win percentage in the $x = 0$ case.

The optimal quantum strategy is obtained as follows. While Alice and Bob are strategizing before the game begins, they share a Bell state

$$|\Psi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}. \quad (28)$$

They also define the orthonormal single-qubit measurement basis

$$\begin{aligned} |\mu_0(\theta)\rangle &= \cos \theta |0\rangle + \sin \theta |1\rangle \\ |\mu_1(\theta)\rangle &= \sin \theta |0\rangle - \cos \theta |1\rangle \end{aligned} \quad (29)$$

and agree to choose their angles based on the respective values of the referee bits x and y :

$$\begin{aligned} \text{Alice: } & \begin{cases} x = 0 \implies \theta = \alpha_0 \\ x = 1 \implies \theta = \alpha_1 \end{cases} \\ \text{Bob: } & \begin{cases} y = 0 \implies \theta = \beta_0 \\ y = 1 \implies \theta = \beta_1. \end{cases} \end{aligned} \quad (30)$$

Finally, they agree to choose their respective answer bits a and b by measuring the Bell state (28) in the measurement basis (29):

$$\begin{aligned} \text{Alice: } & \begin{cases} \mu_0 \implies a = 0 \\ \mu_1 \implies a = 1 \end{cases} \\ \text{Bob: } & \begin{cases} \mu_0 \implies b = 0 \\ \mu_1 \implies b = 1. \end{cases} \end{aligned} \quad (31)$$

We now analyze the above strategy. First consider the particular case $(x, y) = (0, 0)$. According to the angle selection rule (30), Alice uses the measurement basis $\{|\mu_0(\alpha_0)\rangle, |\mu_1(\alpha_0)\rangle\}$ while Bob uses $\{|\mu_0(\beta_0)\rangle, |\mu_1(\beta_0)\rangle\}$. According to the win condition (26), they win if $(a, b) \in \{(0, 0), (1, 1)\}$. According to the answer-bit selection rule (31), these correspond to measurement outcomes $(\mu_a, \mu_b) \in \{(\mu_0, \mu_0), (\mu_1, \mu_1)\}$, which occur with probability,

$$\Pr(\text{win}|x, y = 0, 0) = |\langle \mu_0(\alpha_0) \mu_0(\beta_0) | \Psi^+ \rangle|^2 + |\langle \mu_1(\alpha_0) \mu_1(\beta_0) | \Psi^+ \rangle|^2$$

In more generality, for the cases $(x, y) \in \{(0, 0), (0, 1), (1, 0)\}$ corresponding to rows of the truth table (27) where $x = y = 1$ is False (denote this condition C), they win if $a = b$, which occurs with probability

$$\Pr(\text{win}|C = \text{False}) = \sum_{a=b} |\langle \mu_a(\alpha_x) \mu_b(\beta_y) | \Psi^+ \rangle|^2.$$

In the remaining case, $(x, y) = (1, 1)$ (i.e. C is True), they win if $a \neq b$, which occurs with probability

$$\Pr(\text{win}|C = \text{True}) = \sum_{a \neq b} |\langle \mu_a(\alpha_1) \mu_b(\beta_1) | \Psi^+ \rangle|^2.$$

Using (28) and (29) we compute these probabilities explicitly as

$$\begin{aligned} \Pr(\text{win}|x, y = 0, 0) &= \cos^2(\alpha_0 - \beta_0) \\ \Pr(\text{win}|x, y = 0, 1) &= \cos^2(\alpha_0 - \beta_1) \\ \Pr(\text{win}|x, y = 1, 0) &= \cos^2(\alpha_1 - \beta_0) \\ \Pr(\text{win}|x, y = 1, 1) &= \sin^2(\alpha_1 - \beta_1) \end{aligned}$$

Since x and y are chosen uniformly at random, the total win probability is

$$\Pr(\text{win}) = \frac{1}{4} \left(\cos^2(\alpha_0 - \beta_0) + \cos^2(\alpha_0 - \beta_1) + \cos^2(\alpha_1 - \beta_0) + \sin^2(\alpha_1 - \beta_1) \right).$$

Extremizing with respect to each angle yields the conditions,

$$\begin{aligned} \frac{\partial \Pr}{\partial \alpha_0} = 0 &\implies \sin 2(\alpha_0 - \beta_0) + \sin 2(\alpha_0 - \beta_1) = 0 \\ \frac{\partial \Pr}{\partial \alpha_1} = 0 &\implies \sin 2(\alpha_1 - \beta_0) - \sin 2(\alpha_1 - \beta_1) = 0 \\ \frac{\partial \Pr}{\partial \beta_0} = 0 &\implies \sin 2(\alpha_0 - \beta_0) + \sin 2(\alpha_1 - \beta_0) = 0 \\ \frac{\partial \Pr}{\partial \beta_1} = 0 &\implies \sin 2(\alpha_0 - \beta_1) - \sin 2(\alpha_1 - \beta_1) = 0, \end{aligned}$$

which are satisfied for $\alpha_0 = 0$, $\alpha_1 = \pi/4$, $\beta_0 = \pi/8$, and $\beta_1 = -\pi/8$. These choices for the angles then yield the optimal strategy, and the win probability reduces to

$$\Pr(\text{win}) = \cos^2\left(\frac{\pi}{8}\right) \approx 85\%.$$

References

- [1] Scott Aaronson. Introduction to quantum information science, UT Austin. URL <https://www.scottaaronson.com/qclec/6.pdf>. URL <https://www.scottaaronson.com/qclec/11.pdf>.
- [2] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. Mixed-state entanglement and distillation: Is there a “bound” entanglement in nature? *Phys. Rev. Lett.*, 80:5239–5242, Jun 1998. doi: 10.1103/PhysRevLett.80.5239. URL <https://link.aps.org/doi/10.1103/PhysRevLett.80.5239>.
- [3] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. Quantum entanglement. *Rev. Mod. Phys.*, 81:865–942, Jun 2009. doi: 10.1103/RevModPhys.81.865. URL <https://link.aps.org/doi/10.1103/RevModPhys.81.865>.
- [4] Ali Javadi. Hidden shift iPython notebook and Qiskit code. URL https://github.com/ajavadia/qiskit-terra/blob/Demo/demo/Hidden_Shift_Bent.ipynb. URL https://github.com/ajavadia/qiskit-terra/blob/Demo/demo/python/hidden_shift.py.
- [5] James S. Plank. University of Tennessee CS302 lecture notes. URL <http://web.eecs.utk.edu/~jplank/plank/classes/cs302/Notes/NP/>.
- [6] Eleanor G. Rieffel and Wolfgang H. Polak. *Quantum computing: A gentle introduction*. MIT Press, 2014.
- [7] J. J. Sakurai and Jim Napolitano. *Modern quantum mechanics*. Addison-Wesley, second edition, 1994. ISBN 9780805382914.
- [8] Javad Shabani. Getting started with Python and Qiskit. URL <https://wp.nyu.edu/shabanilab/courses/qiskit/>.
- [9] G. Vidal and J. I. Cirac. Irreversibility in asymptotic manipulations of entanglement. *Phys. Rev. Lett.*, 86:5803–5806, Jun 2001. doi: 10.1103/PhysRevLett.86.5803. URL <https://link.aps.org/doi/10.1103/PhysRevLett.86.5803>.
- [10] Karl Gerd H. Vollbrecht, Reinhard F. Werner, and Michael M. Wolf. Irreversibility of entanglement distillation for a class of symmetric states. *Phys. Rev. A*, 69:062304, Jun 2004. doi: 10.1103/PhysRevA.69.062304. URL <https://link.aps.org/doi/10.1103/PhysRevA.69.062304>.