Final revision - Quantum Computing

May 14, 2022

0.1 Quantum Computing

[17]:

```
import numpy as np
from qiskit.quantum_info import entropy, Statevector, DensityMatrix
```

The Basic Rules of Quantum Mechanics

Superposition - $\alpha|0\rangle + \beta|1\rangle -$ Combination of 2 basis states

Measurement

$$|\psi\rangle = \frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle$$

Borne Rule -

$$Pr(0) = |\langle 0|\alpha\rangle| = |\alpha|^2 = \left|\frac{\sqrt{3}}{2}\right|^2 = \frac{3}{4}$$

$$Pr(1) = |\langle 1|\beta\rangle| = |\beta|^2 = \left|\frac{1}{2}\right|^2 = \frac{1}{4}$$

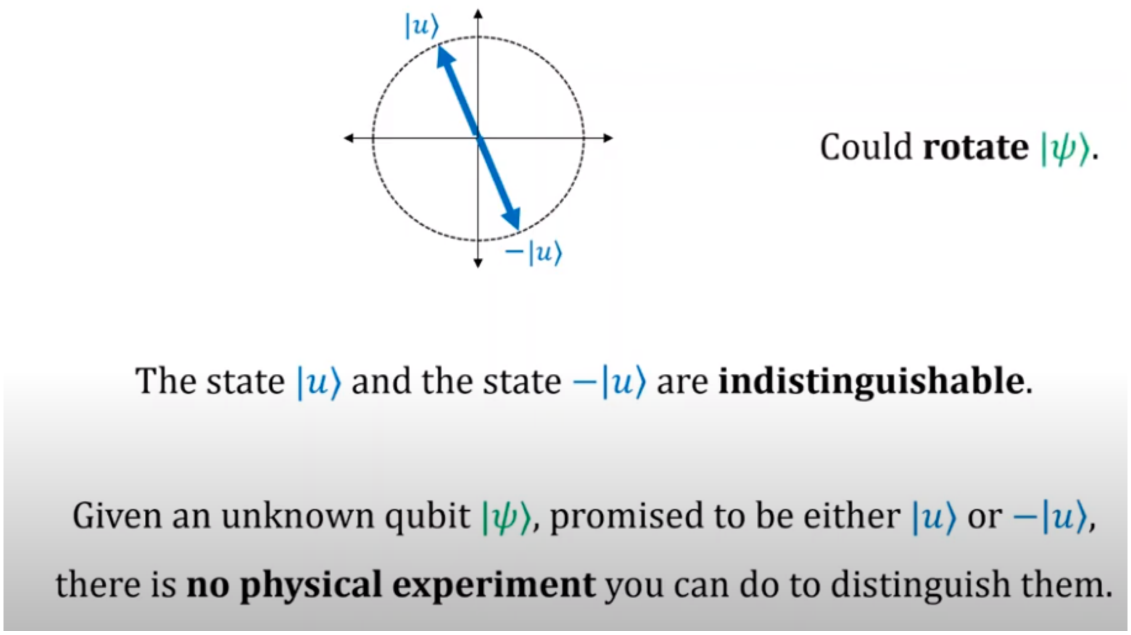
Different Basis for measurement - Introducing Hadamard Gate

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

$$|-\rangle = \frac{(|0\rangle - |1\rangle)}{\sqrt{2}}$$

$$|0\rangle = \frac{(|+\rangle + |-\rangle)}{\sqrt{2}}$$

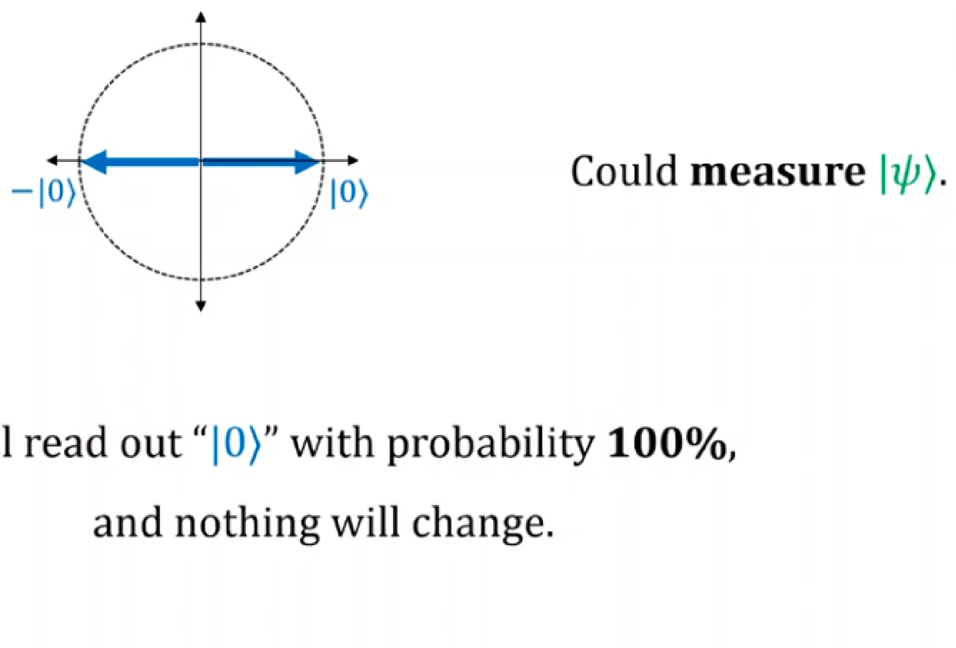
$$|1\rangle = \frac{(|+\rangle - |-\rangle)}{\sqrt{2}}$$



Could **rotate** $|\psi\rangle$.

The state $|u\rangle$ and the state $-|u\rangle$ are **indistinguishable**.

Given an unknown qubit $|\psi\rangle$, promised to be either $|u\rangle$ or $-|u\rangle$, there is **no physical experiment** you can do to distinguish them.



Could **measure** $|\psi\rangle$.

You'll read out "$|0\rangle$" with probability **100%**, and nothing will change.

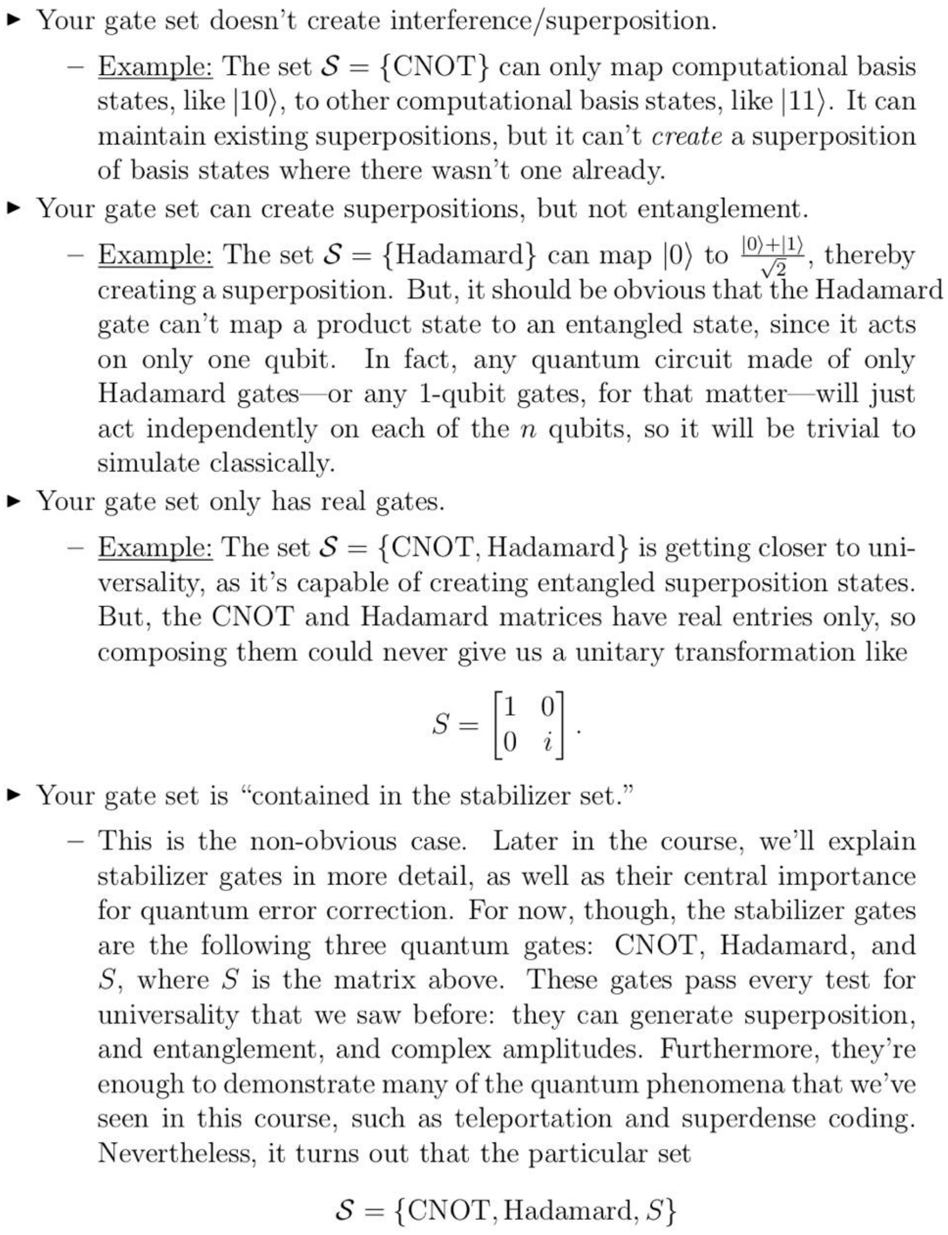
Global vs Relative Phase

So we can only distinguish between relative phase

Quantum Gates(Unitary Matrices) and Circuits Hadamard

Universal Gate Sets Claude Shannon's Theory for Classical Boolean Functions

- Classical universality - NAND gate
- Quantum universality gate set $\mathcal{S}$



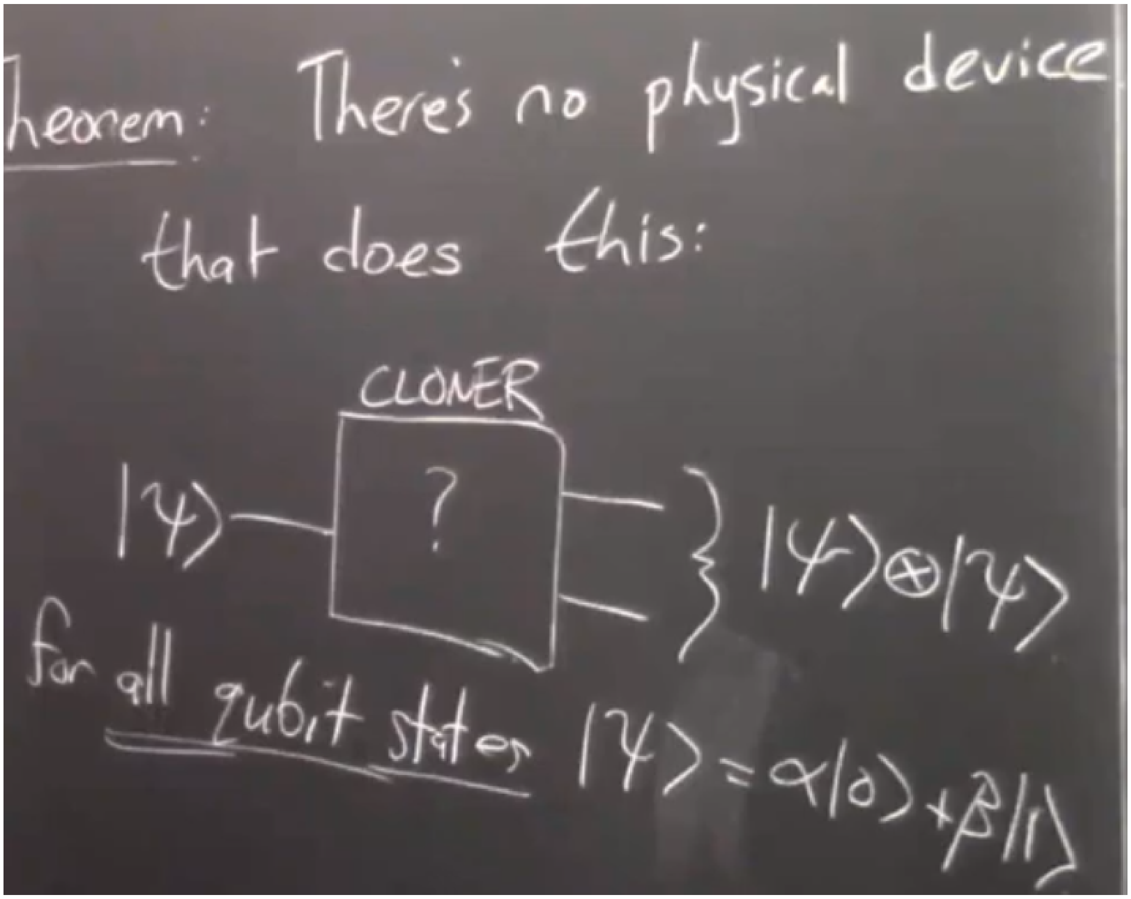
- Your gate set doesn't create interference/superposition.
  - Example: The set $\mathcal{S} = \{\text{CNOT}\}$ can only map computational basis states, like $|10\rangle$, to other computational basis states, like $|11\rangle$. It can maintain existing superpositions, but it can't *create* a superposition of basis states where there wasn't one already.
- Your gate set can create superpositions, but not entanglement.
  - Example: The set $\mathcal{S} = \{\text{Hadamard}\}$ can map $|0\rangle$ to $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$, thereby creating a superposition. But, it should be obvious that the Hadamard gate can't map a product state to an entangled state, since it acts on only one qubit. In fact, any quantum circuit made of only Hadamard gates—or any 1-qubit gates, for that matter—will just act independently on each of the n qubits, so it will be trivial to simulate classically.
- Your gate set only has real gates.
  - Example: The set $\mathcal{S} = \{\text{CNOT}, \text{Hadamard}\}$ is getting closer to universality, as it's capable of creating entangled superposition states. But, the CNOT and Hadamard matrices have real entries only, so composing them could never give us a unitary transformation like

$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}.$$

- Your gate set is "contained in the stabilizer set."
  - This is the non-obvious case. Later in the course, we'll explain stabilizer gates in more detail, as well as their central importance for quantum error correction. For now, though, the stabilizer gates are the following three quantum gates: CNOT, Hadamard, and S, where S is the matrix above. These gates pass every test for universality that we saw before: they can generate superposition, and entanglement, and complex amplitudes. Furthermore, they're enough to demonstrate many of the quantum phenomena that we've seen in this course, such as teleportation and superdense coding. Nevertheless, it turns out that the particular set

$$\mathcal{S} = \{\text{CNOT}, \text{Hadamard}, S\}$$

- **Gottesman-Knill Theorem**
- **Solovay-Kitaev Theorem**



heorem: There's no physical device that does this:

for all qubit states $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

NO-CLONING Theorem Multi-qubit states and Partial measurement

Consider the state - $|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \delta|10\rangle + \gamma|11\rangle$

If you measure Pr[Qubit 1 is 0] , using partial measurement –> We get a joint state

The Church-Turing Thesis

Classical Probability Theory

The Zeno Effect

The Elitzur-Vaidman Bomb

0.1.1 Pure State - superposition of basis states

So far, we've just talked about one way of looking at a state. But in reality, states are more complex.

0.1.2 Mixed State - A classical *probability* distribution over *pure* quantum states

This is the true representation of "true" qubit states. An alternate way of actually representing the whole picture probabilistically

Mixed State of a qudit i.e. a d-dimensional quantum state $\{ p_1$ probability of $|\psi_1\rangle$,

p_2 probability of $|\psi_2\rangle$,

. . .

p_m probability of $|\psi_m\rangle \}$

$$\sum_{i=1}^{m} p_i = 1$$

and $\{|\psi_1\rangle, |\psi_2\rangle .....|\psi_m\rangle\} \in \mathbb{C}^d$ are unit vectors in d-dimensional space

Now, say we measure in an orthonormal basis from set $\{u_1, u_2, u_3....u_d\}$

What is the probability of the measurement being u_i ???

$$\sum_{j=1}^{m} p_j |\langle u_i|\psi_j\rangle|^2$$

, Where p_j is the probability of the mixed state being $|\psi_j\rangle$

Let's tweak the above expression a bit more –>

Let's break the squared part in the expresssion to $\langle u_i|\psi_j\rangle^\dagger = \langle\psi_j|u_i\rangle$. We can substitute this because $|z|^2 = z.z^*$

Thus, the above expression becomes —>

$$\sum_{j=1}^{m} p_j |\langle u_i|\psi_j \times \psi_j|ui\rangle|$$

We can also push the $\sum_{j=1}^{m} p_j$ term inside with some "math jugglery"

Pr[measuring "i"] = $\langle u_i|(\sum_{j=1}^{m} p_j|\psi_j \times \psi_j|)|u_i\rangle$

All the outcome probabilities of any measurement only depend on $\rho = \sum_{j=1}^{m} p_j|\psi_j \times \psi_j|$

Here, ρ is the density matrix and it's the new mathematical way of defining any particle

Examples

1. Particle has a 50% probability of being $|0\rangle$ and 50% of being $|1\rangle$

Let's construct a density matrix $\rho = \frac{1}{2}\begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}1 & 0\end{pmatrix} + \frac{1}{2}\begin{pmatrix}0\\1\end{pmatrix}\begin{pmatrix}0 & 1\end{pmatrix}$

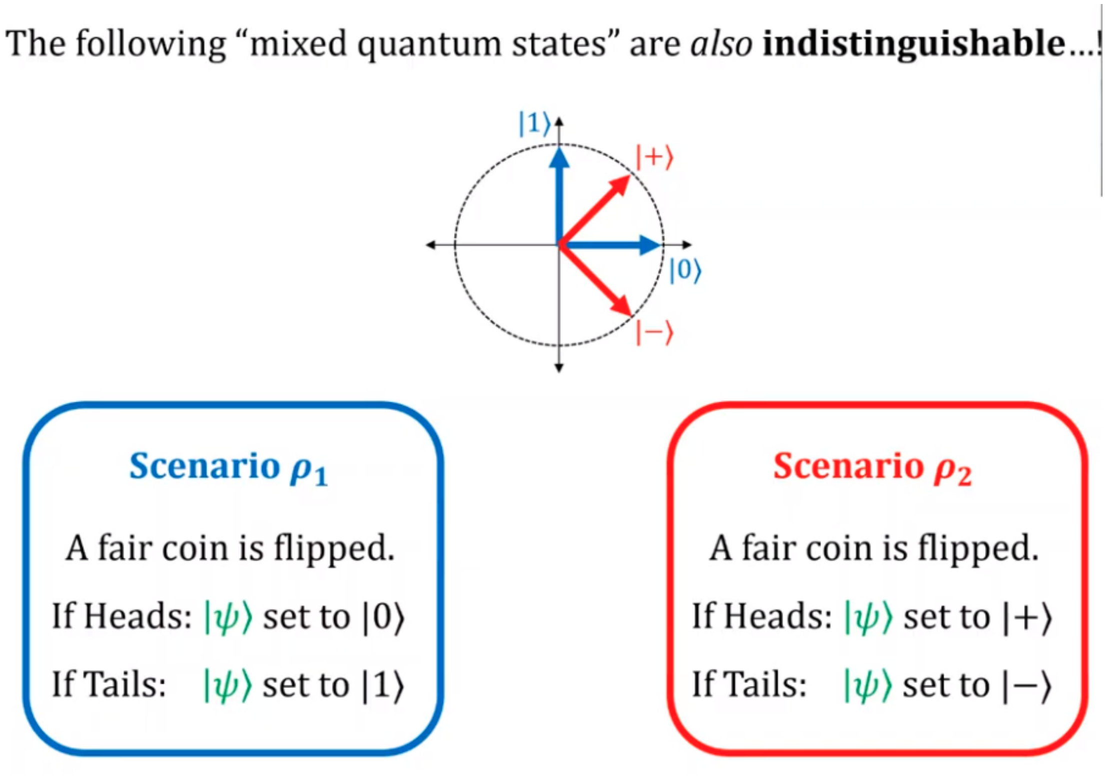
Thus $\rho = \begin{pmatrix}\frac{1}{2} & 0\\0 & \frac{1}{2}\end{pmatrix}$

2. Particle has a 50% probability of being $|+\rangle$ and 50% of being $|-\rangle$

Let’s construct a density matrix $\rho = \frac{1}{2}\begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{pmatrix}\begin{pmatrix}\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}\end{pmatrix} + \frac{1}{2}\begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{-1}{\sqrt{2}}\end{pmatrix}\begin{pmatrix}\frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}}\end{pmatrix}$

Thus $\rho = \begin{pmatrix}\frac{1}{2} & 0\\ 0 & \frac{1}{2}\end{pmatrix}$

Thus, one cannot distinguish between the {0,1} or the {+,-} mixed states



The following “mixed quantum states” are *also* **indistinguishable**...!

Scenario ρ_1

A fair coin is flipped.

If Heads: $|\psi\rangle$ set to $|0\rangle$

If Tails: $|\psi\rangle$ set to $|1\rangle$

Scenario ρ_2

A fair coin is flipped.

If Heads: $|\psi\rangle$ set to $|+\rangle$

If Tails: $|\psi\rangle$ set to $|-\rangle$

3. Particle has 100% probability of being $|0\rangle$

$\rho = \begin{pmatrix}1\\ 0\end{pmatrix}\begin{pmatrix}1 & 0\end{pmatrix} = \begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}$

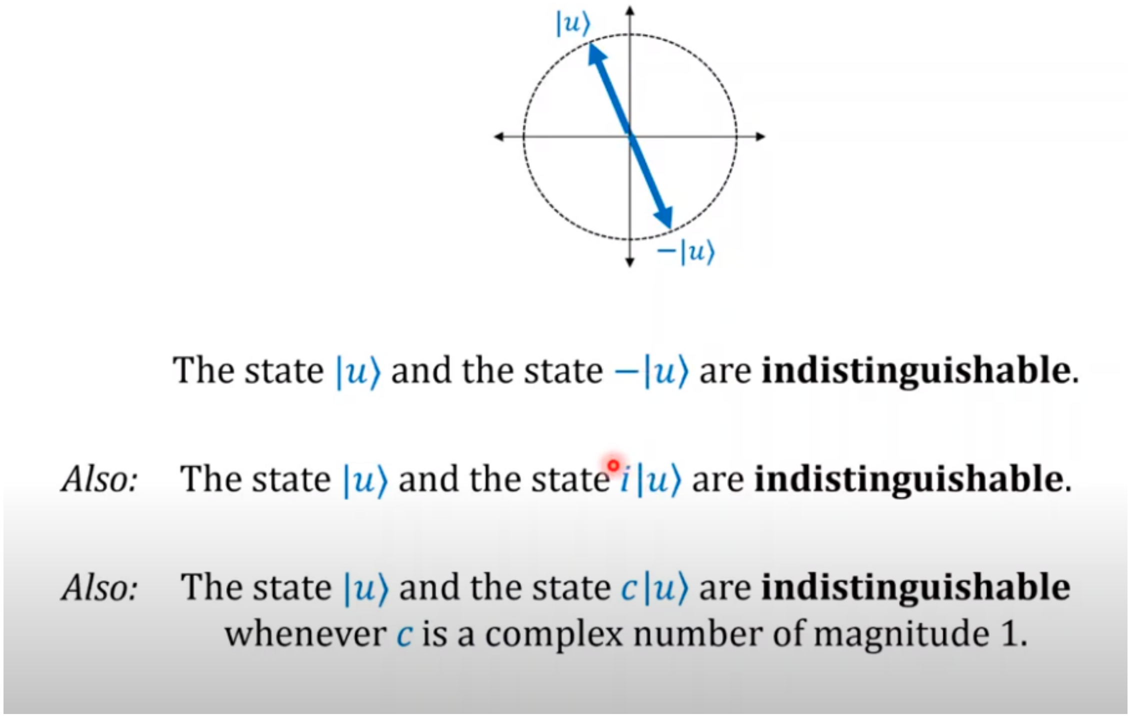
4. Particle has 100% probability of being $-|0\rangle$

$\rho = \begin{pmatrix}-1\\ 0\end{pmatrix}\begin{pmatrix}-1 & 0\end{pmatrix} = \begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}$

5. Particle has 100% probability of being $i|0\rangle$

$\rho = \begin{pmatrix}i\\ 0\end{pmatrix}\begin{pmatrix}-i & 0\end{pmatrix} = \begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}$

3,4,5 Prove the following



The state $|u\rangle$ and the state $-|u\rangle$ are **indistinguishable**.

Also: The state $|u\rangle$ and the state $i|u\rangle$ are **indistinguishable**.

Also: The state $|u\rangle$ and the state $c|u\rangle$ are **indistinguishable** whenever c is a complex number of magnitude 1.

SUCH A c is called a "GLOBAL PHASE"

6. EPR pair $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$

$$\rho = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \end{pmatrix}$$

7. Test

Properties of Density matrix

1. Hermitian (complex number analogue of symmetric) –> $\rho^\dagger = \rho$. $(\sum_{j=1}^{m} p_j|\psi_j \times \psi_j|)$
2. They're "positive" (a.k.a. "positive semi-definite") meaning $\forall |u\rangle, \langle u|\rho|u\rangle \geq 0$
3. $\sum_{i=1}^{d} \rho_{ii} = 1$ –> Trace of ρ or $tr(\rho) = 1$. Sum of diagonal elements is 1

Working with density matrices ρ

- Apply a unitary matrix to the density matrix –> What is the "p_j probability of $U|\psi\rangle$" and $j = (1, 2, ...m)$

NEW Density matrix $\rho' = U\rho U^\dagger$

- Measuring in standard basis

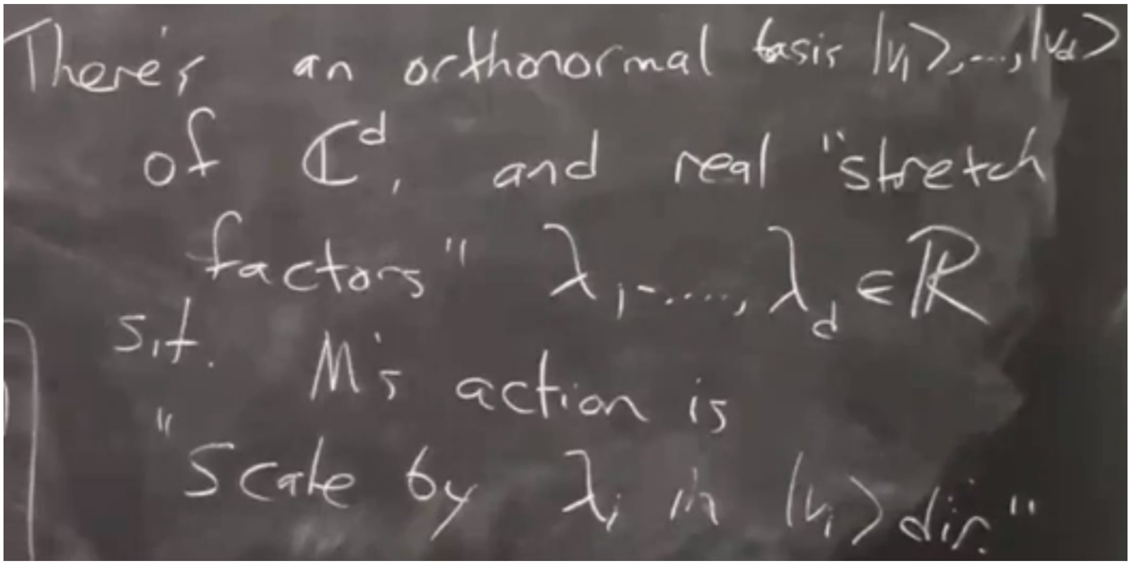
{ ρ_{11} probability of $|\psi_1\rangle$,

ρ_{22} probability of $|\psi_2\rangle$,

⋮

ρ_{dd} probability of $|\psi_d\rangle$ }

- Mixed states having same diagonal entries, will give the same measurement probabilities if measured in the standard basis, but different measurements in other basis.



There's an orthonormal basis $|v_1\rangle, \ldots, |v_d\rangle$
of $\mathbb{C}^d$, and real "stretch
factors" $\lambda_1, \ldots, \lambda_d \in \mathbb{R}$
s.t. M's action is
"Scale by λ_i in $|v_i\rangle$ dir."

-

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$
$$= r_\alpha e^{i\phi_\alpha}|0\rangle + r_\beta e^{i\phi_\beta}|1\rangle$$
$$= r_\alpha|0\rangle + r_\beta e^{i(\phi_\beta - \phi_\alpha)}|1\rangle$$

$z \in \mathbb{C}$, if $x = r\cos\theta$
$y = r\sin\theta$

$$z = r\cos\theta + i r\sin\theta$$
$$= r(\cos\theta + i\sin\theta)$$

Euler's identity :-

$$e^{i\theta} = \cos\theta + i\sin\theta$$
$$\Rightarrow \boxed{z = re^{i\theta}}$$

$$\alpha = r_\alpha e^{i\phi_\alpha}$$
$$\beta = r_\beta e^{i\beta_\alpha}$$

$$\left[r_\alpha,\ r_\beta,\ \underbrace{\phi_\beta - \phi_\alpha}_{\phi}\right] \in \mathbb{R}$$

$r_\beta e^{i\phi} = x + iy$; where $x = r_\beta \cos\phi$, $y = r_\beta \sin\phi$ $\Rightarrow r_\alpha^2 + \underbrace{x^2 + y^2}_{r_\beta^2} = 1$

using trigo:- $\sqrt{r_\alpha^2 + r_\beta^2} = 1$

$r_\alpha = \cos(\theta)$, $r_\beta = \sin(\theta)$

$\underline{\theta, \phi \in \mathbb{R}}$

We only need to consider

$$\frac{\theta}{2}$$

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

Bloch Sphere

Bloch Sphere and Mixed states –>

0.1.3 Entanglement

For a mixture of pure states —> You can't break your state into a tensor product if they're entangled

Quantifying Entanglement and Mixed State Entanglement Schmidt Decomposition

Given a bi-partite state $\sum_{ij} \alpha_{ij}|i\rangle_A|j\rangle_B$. *How do we calculate how many Bell pairs it's worth?*

- Perform an SVD on the density matrix ρ and get the eigenvalues.

Von-Neuman Entropy

Von-Neumann Entropy for a pure state ($|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$) is 0

Von-Neumann Entropy for a mixed state, given ρ is –>

$$S(\rho) = \sum_{i=0}^{n-1} \gamma_i log_2(\frac{1}{\gamma_i})$$

Where $\{\gamma_i\}$ are the eigenvalues of ρ.. We use Schmidt form here.

Entanglement Entropy

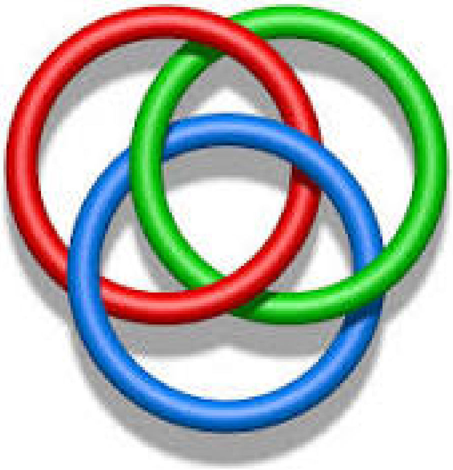
How to quantify entanglement? Say for example, if entropy is .942, then for 1000 copies, 942 qubits can be teleported

Entanglement Entropy for a (pure) bi-partite state

Mixed State entanglement

The GHZ State and Monogamy of Entanglement

- If Alice and Bob share a Maximally Entangled State, q_A and q_B. Then q_A cannot be maximally entangled with q_C , a 3^{rd} party. This is the monogamy of entanglement.
- If you extend this idea to the GHZ state, you can only see the entanglement if you have all 3 qubits together. Imagine it as Borromean rings. Removing any one ring, unentangles the other 2 rings.



[18]:

```
state_vector = Statevector([np.sqrt(2/3),np.sqrt(1/3)])
state_vector.draw(output='latex')
```

[18]:

$$\frac{\sqrt{6}}{3}|0\rangle + \frac{\sqrt{3}}{3}|1\rangle$$

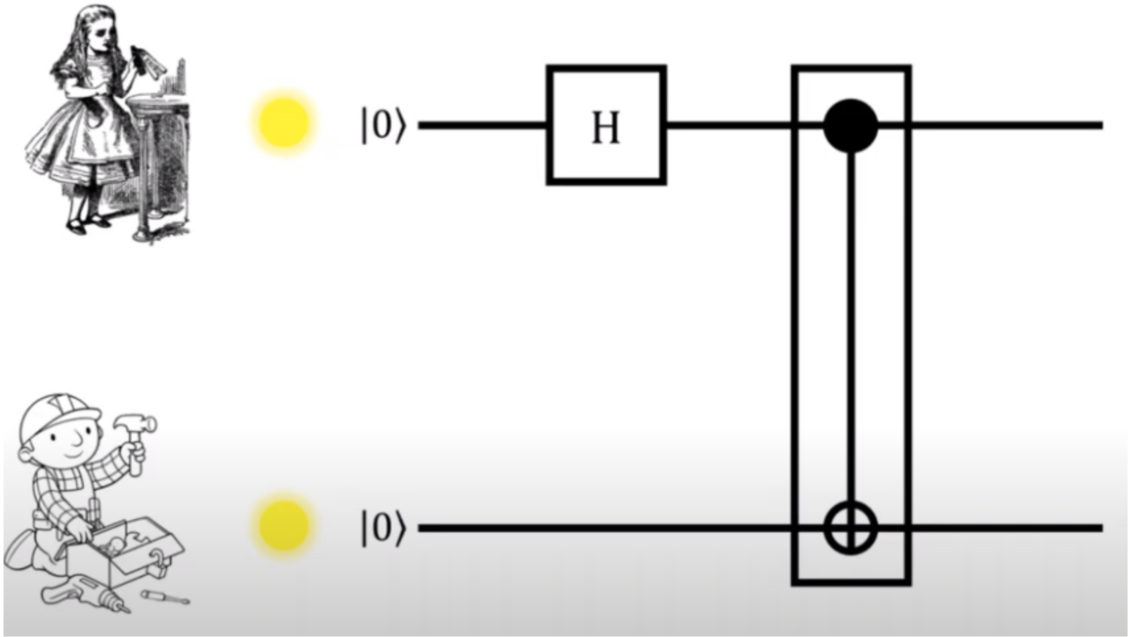
[19]:

```
s1 = entropy(DensityMatrix([[2/3, np.sqrt(2)/3], [np.sqrt(2)/3, 1/3]]))  # Density matrix object
s2 = entropy(state_vector)

print(s1)
print(s2)

print(s1==s2)
```

```
1.6017132519074586e-16
0
False
```



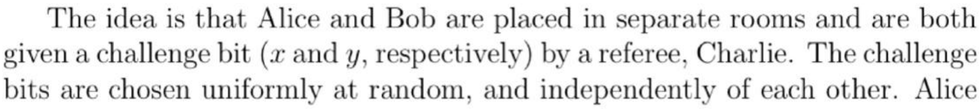
Create a maximally entangled state

Entangled *pair* of qubits - Bell pair/EPR Pair –> $|\frac{00\rangle+|11\rangle}{\sqrt{2}}$ Inter conversion between various states ---> $|\frac{++\rangle+|--\rangle}{\sqrt{2}}$

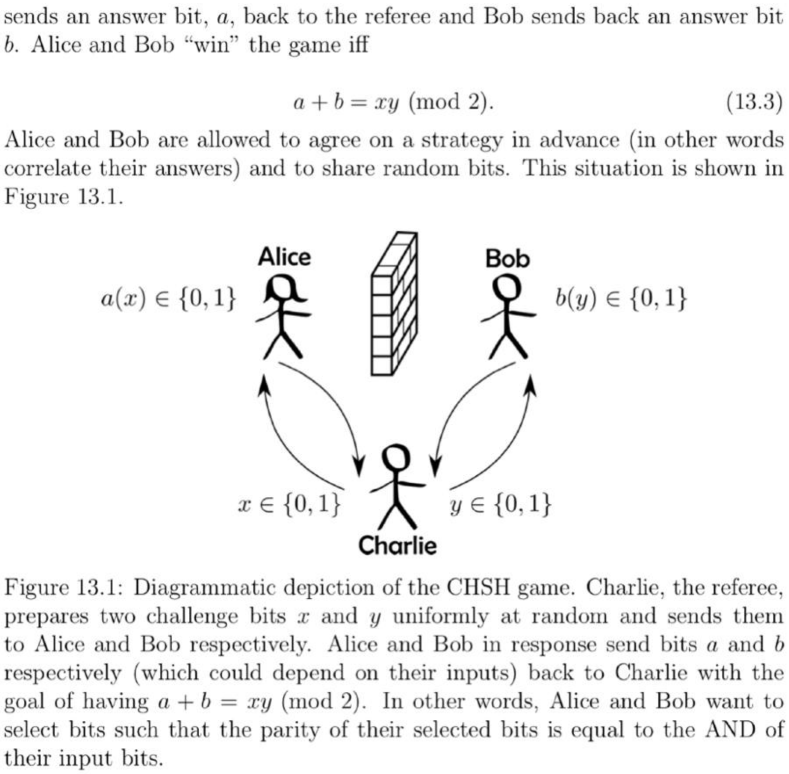
These 2 states are not distinguishable as such

Hidden Variables

Nonlocal Games



The idea is that Alice and Bob are placed in separate rooms and are both given a challenge bit (x and y, respectively) by a referee, Charlie. The challenge bits are chosen uniformly at random, and independently of each other. Alice



sends an answer bit, a, back to the referee and Bob sends back an answer bit b. Alice and Bob "win" the game iff

$$a + b = xy \text{ (mod 2)}. \tag{13.3}$$

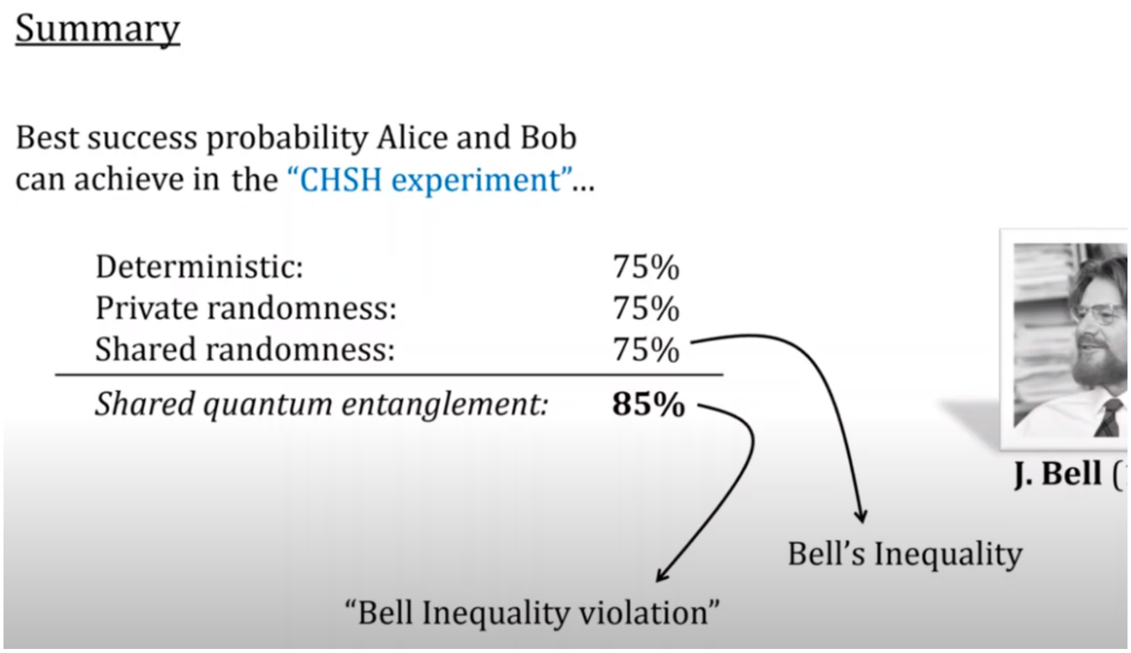
Alice and Bob are allowed to agree on a strategy in advance (in other words correlate their answers) and to share random bits. This situation is shown in Figure 13.1.

Alice
Bob
$a(x) \in \{0,1\}$
$b(y) \in \{0,1\}$
$x \in \{0,1\}$
$y \in \{0,1\}$
Charlie

Figure 13.1: Diagrammatic depiction of the CHSH game. Charlie, the referee, prepares two challenge bits x and y uniformly at random and sends them to Alice and Bob respectively. Alice and Bob in response send bits a and b respectively (which could depend on their inputs) back to Charlie with the goal of having $a + b = xy$ (mod 2). In other words, Alice and Bob want to select bits such that the parity of their selected bits is equal to the AND of their input bits.

CHSH Game

Bell's Inequality



Summary

Best success probability Alice and Bob can achieve in the “CHSH experiment”...

Deterministic:	75%
Private randomness:	75%
Shared randomness:	75%
Shared quantum entanglement:	**85%**

Bell's Inequality

“Bell Inequality violation”

Quantum Teleportation - Faster than light communication ? (Doesn't violate No-Cloning)

- 1 SHARED EPR-Pair + 2bits $\geq$ 1 Qubit --> Read as RHS is required to transport/teleport LHS --> 1 qubit.
- Assume Alice and Bob have a way of doing ``distributed CNOT''. Thus, they start with

$$|\psi\rangle = \alpha|00\rangle + \beta|11\rangle$$

1. Alice does Hadamard on her qubit and measures -

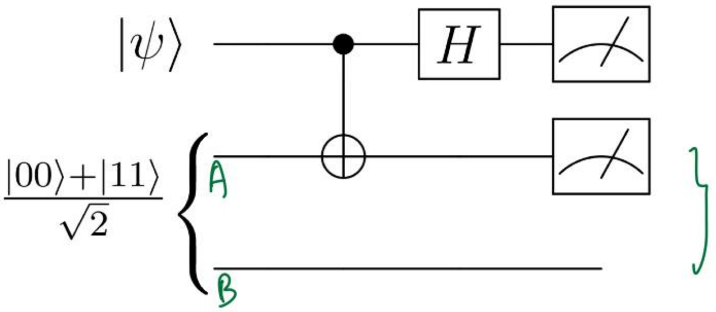
$$H|\psi\rangle = \alpha|+0\rangle + \beta|-1\rangle = \frac{\alpha}{\sqrt{2}}|00\rangle + \frac{\alpha}{\sqrt{2}}|01\rangle + \frac{\beta}{\sqrt{2}}|10\rangle - \frac{\beta}{\sqrt{2}}|11\rangle$$

2. 2 possible outcomes emerge from the above state post measurement.

- If Alice measures 0, Bob's state collapses to --> $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$
- If Alice measures 1, Bob's state collapses to --> $|\psi\rangle = \alpha|0\rangle - \beta|1\rangle$

3. CLASSICAL BIT 2 --> Alice now sends the measured output to Bob

- If the measured bit is 0, Bob does nothing
- If the measured bit is 1, Bob applies Z gate to $|\psi\rangle = \alpha|0\rangle - \beta|1\rangle$ and gets $Z|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$
- HOW to get the ``distributed CNOT''???



$$(\alpha\,|0\rangle + \beta\,|1\rangle) \otimes \frac{|00\rangle + |11\rangle}{\sqrt{2}} = \frac{\alpha\,|000\rangle + \alpha\,|011\rangle + \beta\,|100\rangle + \beta\,|111\rangle}{\sqrt{2}}. \quad (10.2)$$

Following the CNOT the state of the system is

$$\frac{\alpha\,|000\rangle + \alpha\,|011\rangle + \beta\,|110\rangle + \beta\,|101\rangle}{\sqrt{2}}. \quad (10.3)$$

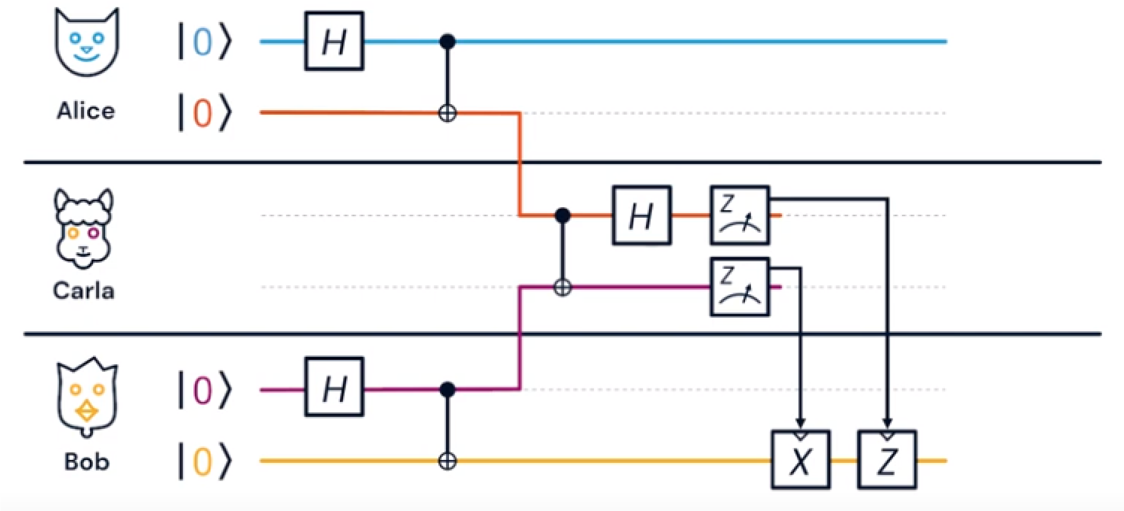
Next, Alice applies a Hadamard to her first qubit which results in the state

$$\begin{aligned} &\frac{1}{\sqrt{2}}\left(\alpha\,|{+}00\rangle + \alpha\,|{+}11\rangle + \beta\,|{-}10\rangle + \beta\,|{-}01\rangle\right) \\ &\quad = \frac{1}{2}\left(\alpha\,|000\rangle + \alpha\,|100\rangle + \alpha\,|011\rangle + \alpha\,|111\rangle + \beta\,|010\rangle - \beta\,|110\rangle + \beta\,|001\rangle - \beta\,|101\rangle\right) \end{aligned} \quad (10.4)$$

Finally, Alice measures both of her qubits in the $\{|0\rangle\,,|1\rangle\}$ basis. This leads to four possible outcomes for the state of Bob's qubit conditioned on her

If Alice Sees:	00	01	10	11
Then Bob's qubit is:	$\alpha\,|0\rangle + \beta\,|1\rangle$	$\alpha\,|1\rangle + \beta\,|0\rangle$	$\alpha\,|0\rangle - \beta\,|1\rangle$	$\alpha\,|1\rangle - \beta\,|0\rangle$

Table 10.1: Summary of Bob's output state conditioned on Alice's measurement results.



Entanglement Swapping

Weisner's money scheme - BBBW '82

Works using the No-Cloning Theorem

- Bank issues a multi-qubit state
- Security parameter - `n'
- Bank picks a random $s \in \{0,1\}^n$
- Bank picks $q \in \{0,1,+,-\}^n$
- Bank creates - $|\psi\rangle = |0\rangle \otimes |+\rangle \otimes |1\rangle \otimes |-\rangle....$
- Bank maintains (s, q)
- You get (s, ψ)
- Bank can verify if the state/coin is valid/forged by using q and measuring in the right basis. If all the measurements pass, it's a valid coin.

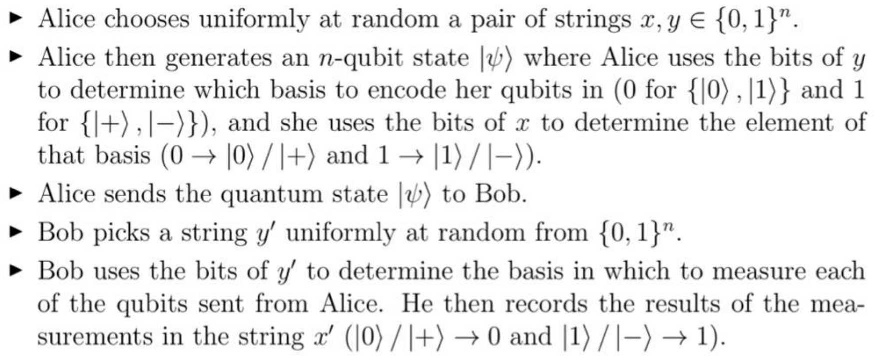
Attacks on Weisner

1. Simple attack - Counterfeiter measures each qubit in the std. basis
2. Interactive attack - Elitzur-Vaidmann Bomb

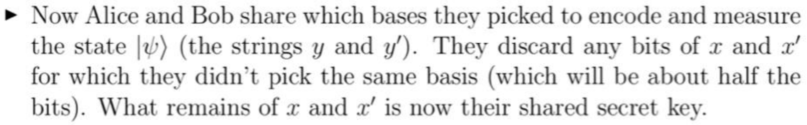
QKD and BB84

Shared key is required.

PROTOCOL



- Alice chooses uniformly at random a pair of strings $x, y \in \{0,1\}^n$.
- Alice then generates an n-qubit state $|\psi\rangle$ where Alice uses the bits of y to determine which basis to encode her qubits in (0 for $\{|0\rangle, |1\rangle\}$ and 1 for $\{|+\rangle, |-\rangle\}$), and she uses the bits of x to determine the element of that basis ($0 \rightarrow |0\rangle / |+\rangle$ and $1 \rightarrow |1\rangle / |-\rangle$).
- Alice sends the quantum state $|\psi\rangle$ to Bob.
- Bob picks a string y' uniformly at random from $\{0,1\}^n$.
- Bob uses the bits of y' to determine the basis in which to measure each of the qubits sent from Alice. He then records the results of the measurements in the string x' ($|0\rangle / |+\rangle \rightarrow 0$ and $|1\rangle / |-\rangle \rightarrow 1$).



- Now Alice and Bob share which bases they picked to encode and measure the state $|\psi\rangle$ (the strings y and y'). They discard any bits of x and x' for which they didn't pick the same basis (which will be about half the bits). What remains of x and x' is now their shared secret key.

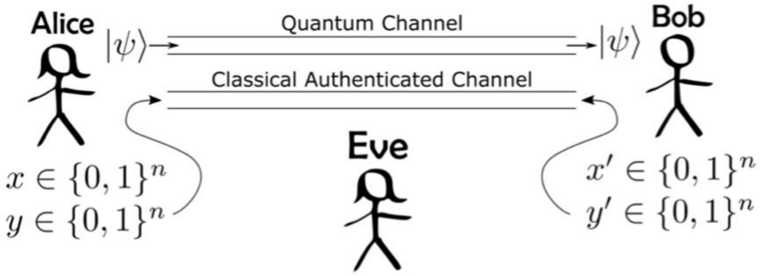
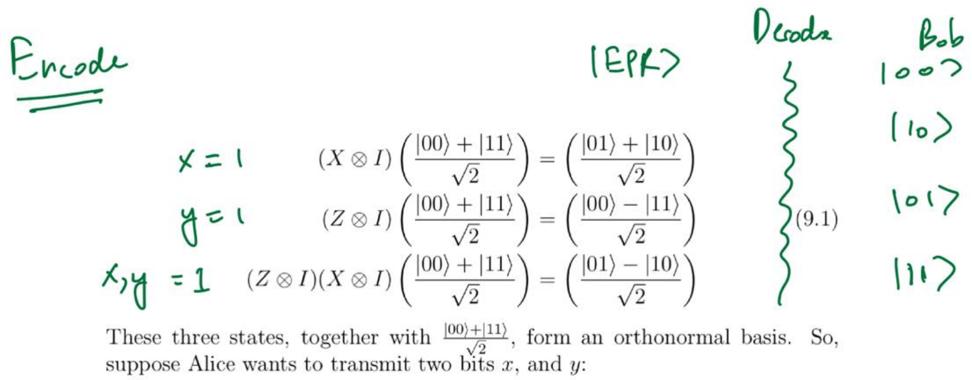


Figure 8.2: Sketch of the BB84 protocol.

Super dense coding **Holevo's Theorem**: Alice can't send more than one bit per qubit to Bob.

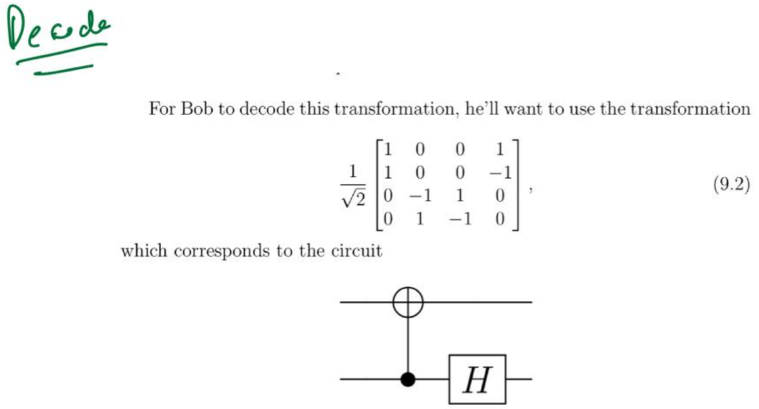
PROTOCOL



Encode
|EPR>
Decode
Bob
|00>
|10>
|01>
|11>
x = 1
y = 1
x, y = 1

$$\begin{aligned}(X\otimes I)\left(\frac{|00\rangle+|11\rangle}{\sqrt{2}}\right)&=\left(\frac{|01\rangle+|10\rangle}{\sqrt{2}}\right)\\(Z\otimes I)\left(\frac{|00\rangle+|11\rangle}{\sqrt{2}}\right)&=\left(\frac{|00\rangle-|11\rangle}{\sqrt{2}}\right)\\(Z\otimes I)(X\otimes I)\left(\frac{|00\rangle+|11\rangle}{\sqrt{2}}\right)&=\left(\frac{|01\rangle-|10\rangle}{\sqrt{2}}\right)\end{aligned}\qquad(9.1)$$

These three states, together with $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$, form an orthonormal basis. So, suppose Alice wants to transmit two bits x, and y:



For Bob to decode this transformation, he'll want to use the transformation

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1&0&0&1\\1&0&0&-1\\0&-1&1&0\\0&1&-1&0\end{bmatrix},\qquad(9.2)$$

which corresponds to the circuit

1-qubit + 1 shared ebit $\geq$ 2 classical bits

Quantum Query Complexity There are 2 major ways to look at complexity of quantum algorithms -->

Circuit Complexity

Query Complexity aka Black-Box Model

Quantum Garbage Collection

0.2 QUANTUM ALGORITHMS

0.2.1 Deutsch-Jozsa Algorithm

Oracle function –> $f(\{0,1\}^n) \rightarrow 0,1$. Check if the function is

- Constant
- Balanced

Classically —> $2^{n-1}+1$ **queries**

Quantum —> Only 1 query/pass through the circuit

0.2.2 Bernstein-Vazirani Algorithm

Oracle function –> $f(x) = s.x(mod2)$. i.e. a bit-wise produce of input with a 'secret' string s. Find s

Classically –> n queries to the Oracle

Quantum –> 1 query/pass through the circuit

0.2.3 Simon's Algorithm

Oracle Function –> $f(x)$ has following properties `Function can be`

- `one-to-one`
- `two-to-one`

Classical Solution –> $2^{n-1} + 1$ queries to the oracle

Quantum Solution –> Repeat n times to solve b

0.2.4 Grover's Algorithm

Problem –> UNORDERED SEARCH. Oracle $f : \{0, 1, ...N - 1\} \to \{0, 1\}$ `Find if there's an x in the input space for which` $f(x) = 1$

Classical Solution `To find the purple box -- the marked item -- using classical computation, one would have to check on average` $\frac{N}{2}$ `of these boxes, and in the worst case, all` N `of them.`

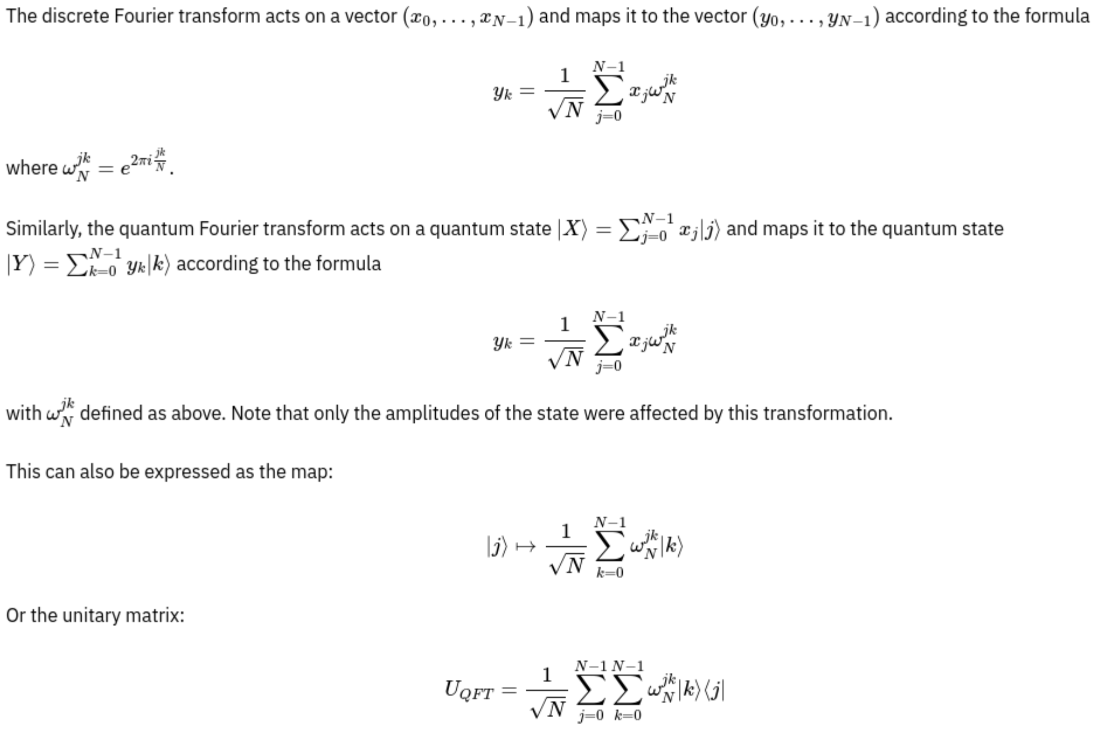
Quantum Solution - $\sqrt{N}$

0.3 #### Applications of Grover's Algorithm

0.3.1 Pre-requisites to Shor

1. **`Fermat's Little Theorem`**
2. **`Euler's Theorem`**
3. **`Euler's Totient Function`**
4. **`Continued Fractions Algorithm`**

0.3.2 QFT - Quantum Fourier Transform



The discrete Fourier transform acts on a vector $(x_0, \ldots, x_{N-1})$ and maps it to the vector $(y_0, \ldots, y_{N-1})$ according to the formula

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \omega_N^{jk}$$

where $\omega_N^{jk} = e^{2\pi i \frac{jk}{N}}$.

Similarly, the quantum Fourier transform acts on a quantum state $|X\rangle = \sum_{j=0}^{N-1} x_j |j\rangle$ and maps it to the quantum state $|Y\rangle = \sum_{k=0}^{N-1} y_k |k\rangle$ according to the formula

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \omega_N^{jk}$$

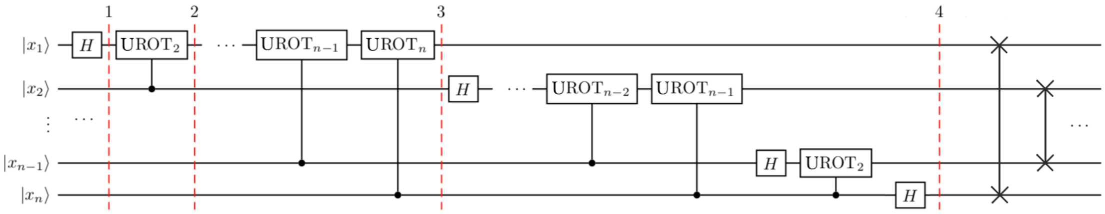
with ω_N^{jk} defined as above. Note that only the amplitudes of the state were affected by this transformation.

This can also be expressed as the map:

$$|j\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \omega_N^{jk} |k\rangle$$

Or the unitary matrix:

$$U_{QFT} = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \sum_{k=0}^{N-1} \omega_N^{jk} |k\rangle\langle j|$$



CIRCUIT

Example - 3bit QFT

6. Example 2: 3-qubit QFT

The steps to creating the circuit for $|y_3y_2y_1\rangle = QFT_8|x_3x_2x_1\rangle$ would be:

1. Apply a Hadamard gate to $|x_1\rangle$

$$|\psi_1\rangle = |x_3\rangle \otimes |x_2\rangle \otimes \frac{1}{\sqrt{2}}\left[|0\rangle + \exp\left(\frac{2\pi i}{2}x_1\right)|1\rangle\right]$$

2. Apply a $UROT_2$ gate to $|x_1\rangle$ depending on $|x_2\rangle$

$$|\psi_2\rangle = |x_3\rangle \otimes |x_2\rangle \otimes \frac{1}{\sqrt{2}}\left[|0\rangle + \exp\left(\frac{2\pi i}{2^2}x_2 + \frac{2\pi i}{2}x_1\right)|1\rangle\right]$$

3. Apply a $UROT_3$ gate to $|x_1\rangle$ depending on $|x_3\rangle$

$$|\psi_3\rangle = |x_3\rangle \otimes |x_2\rangle \otimes \frac{1}{\sqrt{2}}\left[|0\rangle + \exp\left(\frac{2\pi i}{2^3}x_3 + \frac{2\pi i}{2^2}x_2 + \frac{2\pi i}{2}x_1\right)|1\rangle\right]$$

4. Apply a Hadamard gate to $|x_2\rangle$

$$|\psi_4\rangle = |x_3\rangle \otimes \frac{1}{\sqrt{2}}\left[|0\rangle + \exp\left(\frac{2\pi i}{2}x_2\right)|1\rangle\right] \otimes \frac{1}{\sqrt{2}}\left[|0\rangle + \exp\left(\frac{2\pi i}{2^3}x_3 + \frac{2\pi i}{2^2}x_2 + \frac{2\pi i}{2}x_1\right)|1\rangle\right]$$

5. Apply a $UROT_2$ gate to $|x_2\rangle$ depending on $|x_3\rangle$

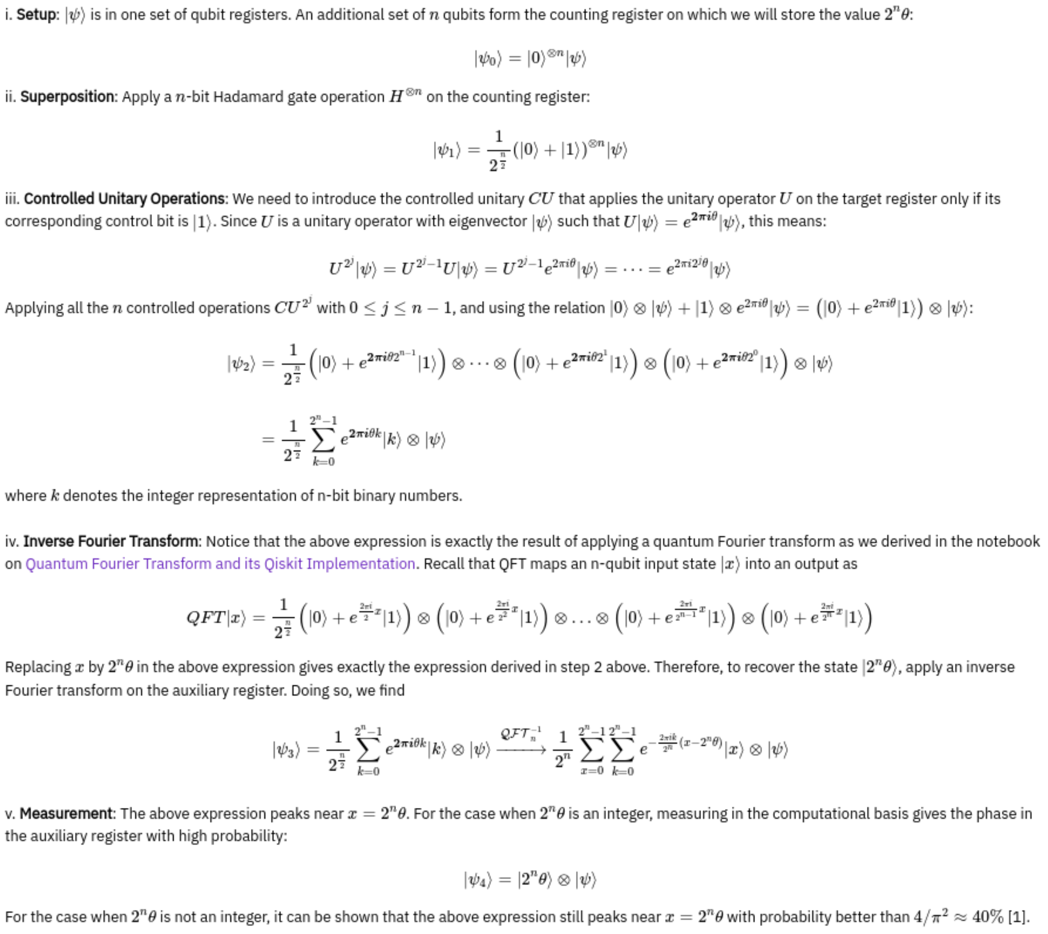
$$|\psi_5\rangle = |x_3\rangle \otimes \frac{1}{\sqrt{2}}\left[|0\rangle + \exp\left(\frac{2\pi i}{2^2}x_3 + \frac{2\pi i}{2}x_2\right)|1\rangle\right] \otimes \frac{1}{\sqrt{2}}\left[|0\rangle + \exp\left(\frac{2\pi i}{2^3}x_3 + \frac{2\pi i}{2^2}x_2 + \frac{2\pi i}{2}x_1\right)|1\rangle\right]$$

6. Apply a Hadamard gate to $|x_3\rangle$

$$|\psi_6\rangle = \frac{1}{\sqrt{2}}\left[|0\rangle + \exp\left(\frac{2\pi i}{2}x_3\right)|1\rangle\right] \otimes \frac{1}{\sqrt{2}}\left[|0\rangle + \exp\left(\frac{2\pi i}{2^2}x_3 + \frac{2\pi i}{2}x_2\right)|1\rangle\right] \otimes \frac{1}{\sqrt{2}}\left[|0\rangle + \exp\left(\frac{2\pi i}{2^3}x_3 + \frac{2\pi i}{2^2}x_2 + \frac{2\pi i}{2}x_1\right)|1\rangle\right]$$

7. Keep in mind the reverse order of the output state relative to the desired QFT. Therefore, we must reverse the order of the qubits (in this case swap y_1 and y_3).

0.3.3 QPE - Quantum Phase Estimation



i. **Setup**: $|\psi\rangle$ is in one set of qubit registers. An additional set of n qubits form the counting register on which we will store the value $2^n\theta$:

$$|\psi_0\rangle = |0\rangle^{\otimes n}|\psi\rangle$$

ii. **Superposition**: Apply a n-bit Hadamard gate operation $H^{\otimes n}$ on the counting register:

$$|\psi_1\rangle = \frac{1}{2^{\frac{n}{2}}}(|0\rangle + |1\rangle)^{\otimes n}|\psi\rangle$$

iii. **Controlled Unitary Operations**: We need to introduce the controlled unitary CU that applies the unitary operator U on the target register only if its corresponding control bit is $|1\rangle$. Since U is a unitary operator with eigenvector $|\psi\rangle$ such that $U|\psi\rangle = e^{\boldsymbol{2\pi i\theta}}|\psi\rangle$, this means:

$$U^{2^j}|\psi\rangle = U^{2^j-1}U|\psi\rangle = U^{2^j-1}e^{2\pi i\theta}|\psi\rangle = \cdots = e^{2\pi i 2^j\theta}|\psi\rangle$$

Applying all the n controlled operations CU^{2^j} with $0 \leq j \leq n-1$, and using the relation $|0\rangle \otimes |\psi\rangle + |1\rangle \otimes e^{2\pi i\theta}|\psi\rangle = \left(|0\rangle + e^{2\pi i\theta}|1\rangle\right) \otimes |\psi\rangle$:

$$|\psi_2\rangle = \frac{1}{2^{\frac{n}{2}}}\left(|0\rangle + e^{\boldsymbol{2\pi i\theta 2^{n-1}}}|1\rangle\right) \otimes \cdots \otimes \left(|0\rangle + e^{\boldsymbol{2\pi i\theta 2^1}}|1\rangle\right) \otimes \left(|0\rangle + e^{\boldsymbol{2\pi i\theta 2^0}}|1\rangle\right) \otimes |\psi\rangle$$

$$= \frac{1}{2^{\frac{n}{2}}}\sum_{k=0}^{2^n-1} e^{\boldsymbol{2\pi i\theta k}}|k\rangle \otimes |\psi\rangle$$

where k denotes the integer representation of n-bit binary numbers.

iv. **Inverse Fourier Transform**: Notice that the above expression is exactly the result of applying a quantum Fourier transform as we derived in the notebook on Quantum Fourier Transform and its Qiskit Implementation. Recall that QFT maps an n-qubit input state $|x\rangle$ into an output as

$$QFT|x\rangle = \frac{1}{2^{\frac{n}{2}}}\left(|0\rangle + e^{\frac{2\pi i}{2}x}|1\rangle\right) \otimes \left(|0\rangle + e^{\frac{2\pi i}{2^2}x}|1\rangle\right) \otimes \ldots \otimes \left(|0\rangle + e^{\frac{2\pi i}{2^{n-1}}x}|1\rangle\right) \otimes \left(|0\rangle + e^{\frac{2\pi i}{2^n}x}|1\rangle\right)$$

Replacing x by $2^n\theta$ in the above expression gives exactly the expression derived in step 2 above. Therefore, to recover the state $|2^n\theta\rangle$, apply an inverse Fourier transform on the auxiliary register. Doing so, we find

$$|\psi_3\rangle = \frac{1}{2^{\frac{n}{2}}}\sum_{k=0}^{2^n-1} e^{\boldsymbol{2\pi i\theta k}}|k\rangle \otimes |\psi\rangle \xrightarrow{\mathcal{QFT}_n^{-1}} \frac{1}{2^n}\sum_{x=0}^{2^n-1}\sum_{k=0}^{2^n-1} e^{-\frac{2\pi i k}{2^n}(x-2^n\theta)}|x\rangle \otimes |\psi\rangle$$

v. **Measurement**: The above expression peaks near $x = 2^n\theta$. For the case when $2^n\theta$ is an integer, measuring in the computational basis gives the phase in the auxiliary register with high probability:

$$|\psi_4\rangle = |2^n\theta\rangle \otimes |\psi\rangle$$

For the case when $2^n\theta$ is not an integer, it can be shown that the above expression still peaks near $x = 2^n\theta$ with probability better than $4/\pi^2 \approx 40\%$ [1].

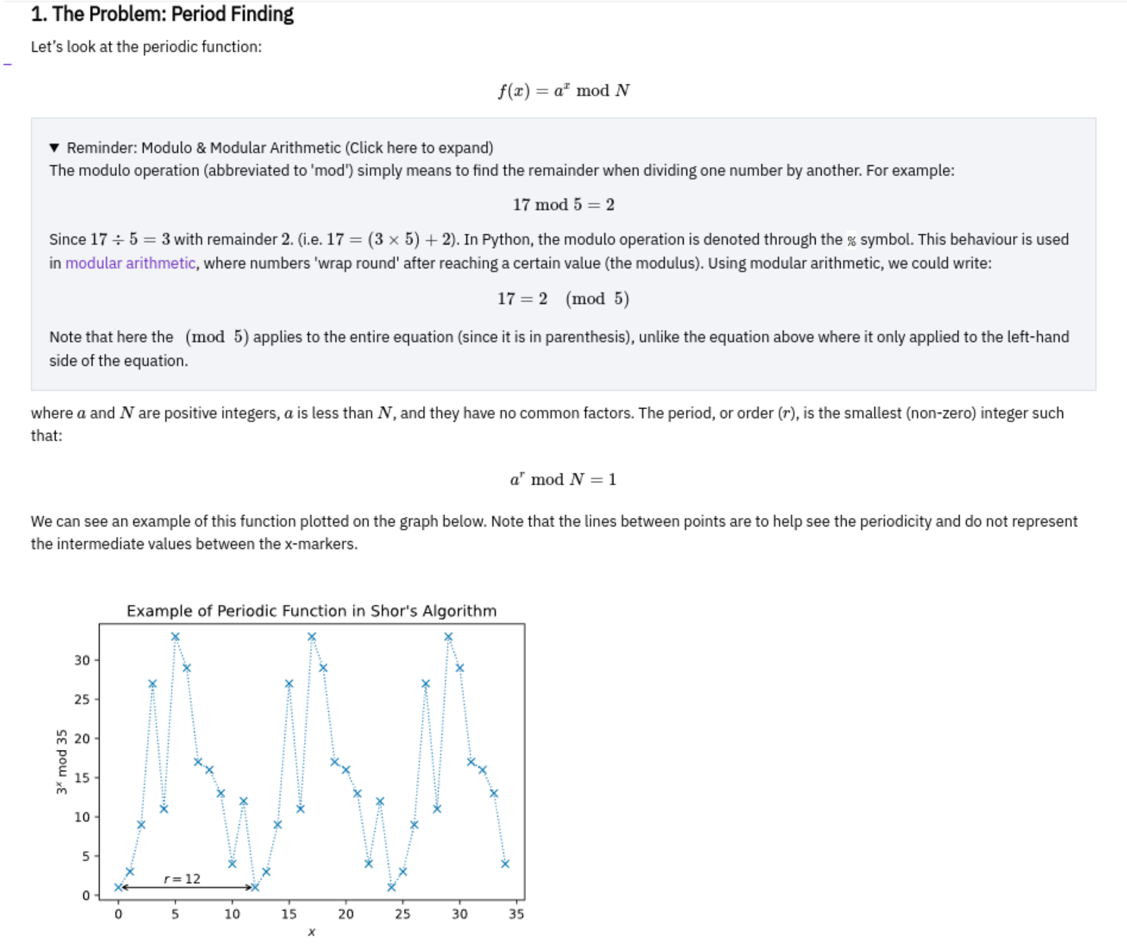
0.4 Cryptography application

0.4.1 RSA Algorithm

0.4.2 Diffie-Hellman

0.4.3 Shor's Algorithm

0.4.4 Problem



1. The Problem: Period Finding

Let's look at the periodic function:

$$f(x) = a^x \bmod N$$

▼ Reminder: Modulo & Modular Arithmetic (Click here to expand)

The modulo operation (abbreviated to 'mod') simply means to find the remainder when dividing one number by another. For example:

$$17 \bmod 5 = 2$$

Since $17 \div 5 = 3$ with remainder 2. (i.e. $17 = (3 \times 5) + 2$). In Python, the modulo operation is denoted through the `%` symbol. This behaviour is used in modular arithmetic, where numbers 'wrap round' after reaching a certain value (the modulus). Using modular arithmetic, we could write:

$$17 = 2 \pmod 5$$

Note that here the $\pmod 5$ applies to the entire equation (since it is in parenthesis), unlike the equation above where it only applied to the left-hand side of the equation.

where a and N are positive integers, a is less than N, and they have no common factors. The period, or order (r), is the smallest (non-zero) integer such that:

$$a^r \bmod N = 1$$

We can see an example of this function plotted on the graph below. Note that the lines between points are to help see the periodicity and do not represent the intermediate values between the x-markers.

Example of Periodic Function in Shor's Algorithm

Classical Solution Quantum Sieve

Quantum Solution

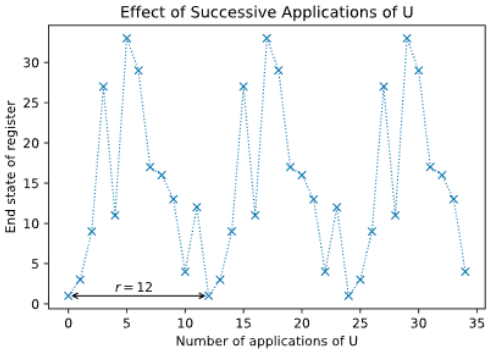
2. The Solution

Shor's solution was to use quantum phase estimation on the unitary operator:

$$U|y\rangle \equiv |ay \bmod N\rangle$$

To see how this is helpful, let's work out what an eigenstate of U might look like. If we started in the state $|1\rangle$, we can see that each successive application of U will multiply the state of our register by $a \pmod N$, and after r applications we will arrive at the state $|1\rangle$ again. For example with $a = 3$ and $N = 35$:

$$\begin{aligned}
U|1\rangle &= |3\rangle \\
U^2|1\rangle &= |9\rangle \\
U^3|1\rangle &= |27\rangle \\
&\vdots \\
U^{(r-1)}|1\rangle &= |12\rangle \\
U^r|1\rangle &= |1\rangle
\end{aligned}$$



So a superposition of the states in this cycle ($|u_0\rangle$) would be an eigenstate of U:

$$|u_0\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |a^k \bmod N\rangle$$

▼ Click to Expand: Example with $a = 3$ and $N = 35$

$$|u_0\rangle = \tfrac{1}{\sqrt{12}}(|1\rangle + |3\rangle + |9\rangle \dots + |4\rangle + |12\rangle)$$

$$U|u_0\rangle = \tfrac{1}{\sqrt{12}}(U|1\rangle + U|3\rangle + U|9\rangle \dots + U|4\rangle + U|12\rangle)$$

$$= \tfrac{1}{\sqrt{12}}(|3\rangle + |9\rangle + |27\rangle \dots + |12\rangle + |1\rangle)$$

$$= |u_0\rangle$$

This eigenstate has an eigenvalue of 1, which isn't very interesting. A more interesting eigenstate could be one in which the phase is different for each of these computational basis states. Specifically, let's look at the case in which the phase of the kth state is proportional to k:

$$|u_1\rangle = \tfrac{1}{\sqrt{r}}\sum_{k=0}^{r-1} e^{-\tfrac{2\pi i k}{r}}|a^k \bmod N\rangle$$

$$U|u_1\rangle = e^{\tfrac{2\pi i}{r}}|u_1\rangle$$

▼ Click to Expand: Example with $a = 3$ and $N = 35$

$$|u_1\rangle = \tfrac{1}{\sqrt{12}}(|1\rangle + e^{-\tfrac{2\pi i}{12}}|3\rangle + e^{-\tfrac{4\pi i}{12}}|9\rangle \dots + e^{-\tfrac{20\pi i}{12}}|4\rangle + e^{-\tfrac{22\pi i}{12}}|12\rangle)$$

$$U|u_1\rangle = \tfrac{1}{\sqrt{12}}(|3\rangle + e^{-\tfrac{2\pi i}{12}}|9\rangle + e^{-\tfrac{4\pi i}{12}}|27\rangle \dots + e^{-\tfrac{20\pi i}{12}}|12\rangle + e^{-\tfrac{22\pi i}{12}}|1\rangle)$$

$$U|u_1\rangle = e^{\tfrac{2\pi i}{12}} \cdot \tfrac{1}{\sqrt{12}}(e^{\tfrac{-2\pi i}{12}}|3\rangle + e^{-\tfrac{4\pi i}{12}}|9\rangle + e^{-\tfrac{6\pi i}{12}}|27\rangle \dots + e^{-\tfrac{22\pi i}{12}}|12\rangle + e^{-\tfrac{24\pi i}{12}}|1\rangle)$$

$$U|u_1\rangle = e^{\tfrac{2\pi i}{12}}|u_1\rangle$$

(We can see $r = 12$ appears in the denominator of the phase.)

This is a particularly interesting eigenvalue as it contains r. In fact, r has to be included to make sure the phase differences between the r computational basis states are equal. This is not the only eigenstate with this behaviour; to generalise this further, we can multiply an integer, s, to this phase difference, which will show up in our eigenvalue:

$$|u_s\rangle = \tfrac{1}{\sqrt{r}}\sum_{k=0}^{r-1} e^{-\tfrac{2\pi i s k}{r}}|a^k \bmod N\rangle$$

$$U|u_s\rangle = e^{\tfrac{2\pi i s}{r}}|u_s\rangle$$

▼ Click to Expand: Example with $a = 3$ and $N = 35$

$$|u_s\rangle = \tfrac{1}{\sqrt{12}}(|1\rangle + e^{-\tfrac{2\pi i s}{12}}|3\rangle + e^{-\tfrac{4\pi i s}{12}}|9\rangle \dots + e^{-\tfrac{20\pi i s}{12}}|4\rangle + e^{-\tfrac{22\pi i s}{12}}|12\rangle)$$

$$U|u_s\rangle = \tfrac{1}{\sqrt{12}}(|3\rangle + e^{-\tfrac{2\pi i s}{12}}|9\rangle + e^{-\tfrac{4\pi i s}{12}}|27\rangle \dots + e^{-\tfrac{20\pi i s}{12}}|12\rangle + e^{-\tfrac{22\pi i s}{12}}|1\rangle)$$

$$U|u_s\rangle = e^{\tfrac{2\pi i s}{12}} \cdot \tfrac{1}{\sqrt{12}}(e^{-\tfrac{2\pi i s}{12}}|3\rangle + e^{-\tfrac{4\pi i s}{12}}|9\rangle + e^{-\tfrac{6\pi i s}{12}}|27\rangle \dots + e^{-\tfrac{22\pi i s}{12}}|12\rangle + e^{-\tfrac{24\pi i s}{12}}|1\rangle)$$

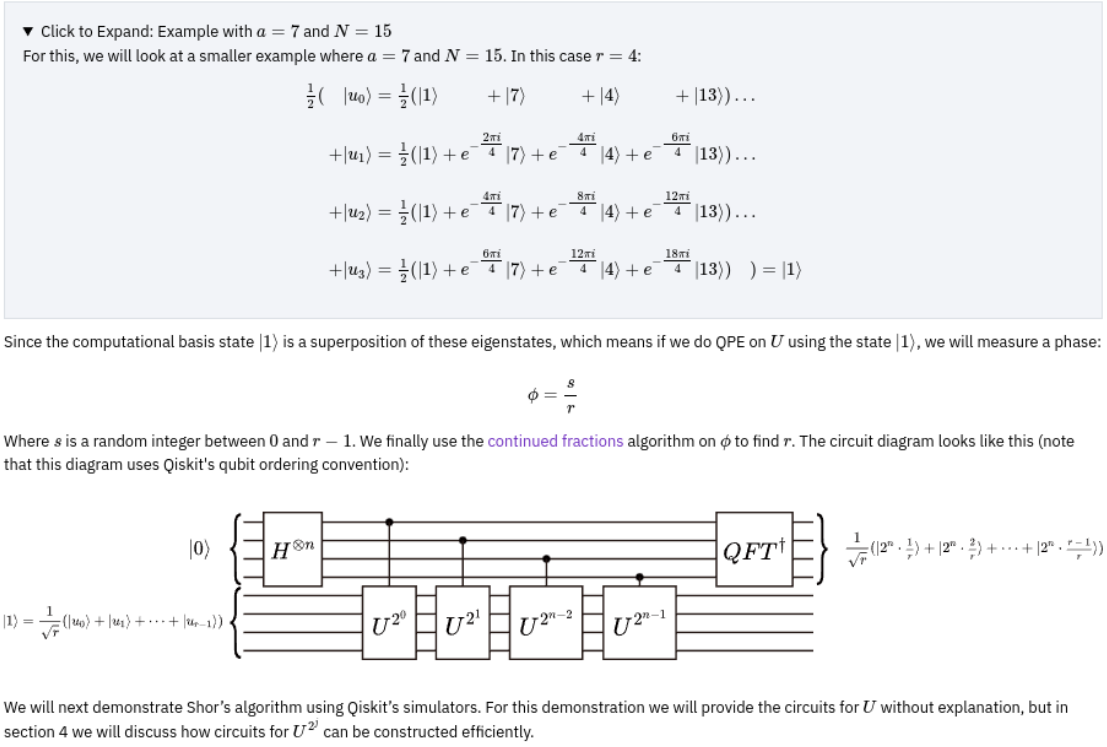
$$U|u_s\rangle = e^{\tfrac{2\pi i s}{12}}|u_s\rangle$$

We now have a unique eigenstate for each integer value of s where

$$0 \leq s \leq r - 1.$$

Very conveniently, if we sum up all these eigenstates, the different phases cancel out all computational basis states except $|1\rangle$:

$$\tfrac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|u_s\rangle = |1\rangle$$



▼ Click to Expand: Example with $a = 7$ and $N = 15$

For this, we will look at a smaller example where $a = 7$ and $N = 15$. In this case $r = 4$:

$$\begin{aligned}
\tfrac{1}{2}(\quad |u_0\rangle &= \tfrac{1}{2}(|1\rangle \qquad + |7\rangle \qquad\quad + |4\rangle \qquad\quad + |13\rangle)\dots \\
+ |u_1\rangle &= \tfrac{1}{2}(|1\rangle + e^{-\frac{2\pi i}{4}}|7\rangle + e^{-\frac{4\pi i}{4}}|4\rangle + e^{-\frac{6\pi i}{4}}|13\rangle)\dots \\
+ |u_2\rangle &= \tfrac{1}{2}(|1\rangle + e^{-\frac{4\pi i}{4}}|7\rangle + e^{-\frac{8\pi i}{4}}|4\rangle + e^{-\frac{12\pi i}{4}}|13\rangle)\dots \\
+ |u_3\rangle &= \tfrac{1}{2}(|1\rangle + e^{-\frac{6\pi i}{4}}|7\rangle + e^{-\frac{12\pi i}{4}}|4\rangle + e^{-\frac{18\pi i}{4}}|13\rangle) \quad) = |1\rangle
\end{aligned}$$

Since the computational basis state $|1\rangle$ is a superposition of these eigenstates, which means if we do QPE on U using the state $|1\rangle$, we will measure a phase:

$$\phi = \frac{s}{r}$$

Where s is a random integer between 0 and $r - 1$. We finally use the continued fractions algorithm on ϕ to find r. The circuit diagram looks like this (note that this diagram uses Qiskit's qubit ordering convention):

$|0\rangle$
$H^{\otimes n}$
$QFT^\dagger$
$\frac{1}{\sqrt{r}}(|2^n \cdot \frac{1}{r}\rangle + |2^n \cdot \frac{2}{r}\rangle + \dots + |2^n \cdot \frac{r-1}{r}\rangle)$
$|1\rangle = \frac{1}{\sqrt{r}}(|u_0\rangle + |u_1\rangle + \dots + |u_{r-1}\rangle)$
U^{2^0}
U^{2^1}
$U^{2^{n-2}}$
$U^{2^{n-1}}$

We will next demonstrate Shor's algorithm using Qiskit's simulators. For this demonstration we will provide the circuits for U without explanation, but in section 4 we will discuss how circuits for U^{2^j} can be constructed efficiently.

####

Applications of Shor's Algorithm

```
[1]: ### Shor Qiskit
```

0.4.5 Classical error correction

0.4.6 Quantum errors

Bit Flip

Phase Flip

Both together

0.4.7 Error Correcting Codes

Shor's 9-bit error correcting code

Interpretations of QM (Copenhagen, Dynamical Collapse, MWI, ...)

Copenhagen Interpretation There exist 2 worlds, 1 quantum and 1 classical ##### Shut up and Calculate ##### Schrodinger's Cat ##### Wigner's Friend ##### Dynamical Collapse ##### GRW Theory ##### Penrose Theory ##### Many-Worlds Interpretation ###### Preferred Basis Problem Decoherence Basis

Experimental Realizations of Quantum Computing