Suppose $n$ qubits, product state

$\mid \psi_n \rangle \rangle \mid \psi_{n-2} \rangle \rangle \cdots \mid \psi_1 \rangle \rangle \mid \psi_0 \rangle \rangle$

has $2^n$ degrees of freedom, no multi-qubit entanglement

\[\begin{array}{cccc}
  n & 1 & 2 & 3 & 4 \\
  2n & 2 & 4 & 6 & 8 \\
  2(2^n-1) & 2 & 6 & 14 & 30
\end{array}\]

growing exponentially compared to product state
Degrees of freedom

\[ \begin{align*}
x, y \\
2x + 3y &= 10 \\
solve for y &= \frac{10 - 2x}{3} \\
\end{align*} \]

\[ x^2 + y^2 = 1 \]

\[ y = \sqrt{1 - x^2} \]

\[ \begin{align*}
x \\
y \\
z \\
2x + 3y + 9z &= 26 \\
x^2 + y^2 + z^2 &= 1 \\
z &= 1/2 \\
\end{align*} \]
Quantum states and entanglement

There are quantum states, i.e., unit vectors in \((\mathbb{C}^2)^\otimes n\), that cannot be written as a tensor product of \(n\) single-qubit states!

**Example: product state**

Consider 2-qubit state: \(\frac{1}{2}\ket{00} + \frac{1}{2}\ket{01} + \frac{1}{2}\ket{10} + \frac{1}{2}\ket{11}\).

This is a product state because it is equal to:

\[
\left(\frac{1}{\sqrt{2}}\ket{0} + \frac{1}{\sqrt{2}}\ket{1}\right) \otimes \left(\frac{1}{\sqrt{2}}\ket{0} + \frac{1}{\sqrt{2}}\ket{1}\right).
\]

**Example: entangled state**

Consider 2-qubit state:

\(\frac{1}{\sqrt{2}}\ket{00} + \frac{1}{\sqrt{2}}\ket{11}\)

This is an entangled state, because it cannot be expressed as a product of two 1-qubit states.

---

**Measurement: example**

\[
|x\rangle = \frac{1}{2\sqrt{3}}\ket{000} + \frac{1}{2\sqrt{3}}\ket{001} + \frac{1}{2}\ket{010} + \frac{1}{2}\ket{011} +
\frac{1}{2\sqrt{3}}\ket{100} + \frac{1}{2\sqrt{3}}\ket{101} + \frac{1}{2\sqrt{3}}\ket{110} + \frac{1}{2\sqrt{3}}\ket{111},
\]

Notice that the modulus squared of the coefficients adds up to 1.

\[
\text{Pr}(000) = \left|\frac{1}{2\sqrt{3}}\right|^2 = \frac{1}{12}, \quad \text{Pr}(001) = \left|\frac{1}{2\sqrt{3}}\right|^2 = \frac{1}{12},
\]

\[
\text{Pr}(010) = \frac{1}{4}, \quad \text{Pr}(011) = \ldots
\]

**Example of single-qubit measurement:**

\[
\text{Pr}(Q1 = 0) = \text{Pr}(000) + \text{Pr}(001) + \text{Pr}(010) + \text{Pr}(011) = \frac{2}{3}
\]

After measurement, the state collapses to what we observed; unmeasured qubits are renormalized.
\[ \frac{1}{3} |10\rangle + \left( \frac{1}{2\sqrt{2}} |100\rangle + \frac{1}{2\sqrt{2}} |101\rangle + \frac{\sqrt{3}}{2\sqrt{2}} |110\rangle + \frac{\sqrt{3}}{2\sqrt{2}} |111\rangle \right) \]

\[ + \frac{1}{\sqrt{3}} |11\rangle \]

Prob of measuring leftmost qubit 0 is 2/3 and the state afterwards is

\[ |10\rangle \left( \frac{1}{2} |10\rangle + \frac{\sqrt{3}}{2} |11\rangle \right) \frac{1}{\sqrt{2}} (|10\rangle + |11\rangle) \]

if measure

\[ |10\rangle \quad 1/2 \]

\[ |11\rangle \quad 1/2 \]
Measurement and entanglement

Consider this **product state**: $\frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle$. We have $\Pr(Q1 = 0) = \Pr(00) + \Pr(01) = \frac{1}{2}$.

If we observe 0 in the first qubit, the state of the register becomes:

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|01\rangle.$$

Consider this **entangled state**: $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$. We have $\Pr(Q1 = 0) = \Pr(00) = \frac{1}{2}$.

If we observe 0 in the first qubit, the state of the register becomes:

$|00\rangle$.

Now a measurement of the second qubit would yield 0 with probability 1!
For an entangled state, measurement outcomes are **dependent variables**.
\[ \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \] "Bell State"

A \rightarrow B

measures 0 \[ p = \frac{1}{2} \]

\rightarrow 100\rangle

No information transmitted

What if A applies an operator, e.g., apply H?

Then measure 1±\rangle, and B

Can apply some other operator -- still both measure 0, 1 \[ p = 0.5 \]
\[
\frac{1}{\sqrt{2}} \left( |100\rangle + |111\rangle \right) = \frac{1}{\sqrt{2}} \left( |1++\rangle + |1--\rangle \right)
\]

There is a formalism, "density matrix," that describes this situation.

\[
|\Psi\rangle = \alpha |00\rangle + \beta |11\rangle
\]

Suppose you could "clone", but not possible: "no-cloning" theorem.
\[ 14\rangle - \begin{bmatrix} \alpha \beta \\ \alpha^2 \beta^2 \\ \alpha^2 \beta^2 \\ \beta^2 \end{bmatrix} - 14\rangle \]

\[ 10\rangle - \begin{bmatrix} \alpha \beta \\ \alpha \beta \\ \alpha \beta \\ \alpha^2 \beta^2 \end{bmatrix} - 10\rangle \]

\[ (\alpha|0\rangle + \beta|1\rangle)10\rangle \rightarrow (\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle) \]

\[ \text{not linear, can't be unitary} \]

\[ U(v|0\rangle) = v|v\rangle \]

\[ U(v|w\rangle|0\rangle) = w|w\rangle \]

\[ \langle v|w\rangle|010\rangle = \langle v|w\rangle \langle v|w\rangle \]

\[ \langle v|w\rangle = c \]

\[ c = c^2 \quad c = 0, 1 \]

only works if v/w are same or orthogonal
General properties

Unitary transformations:
1) Invertible \( U^* \) inverts \( U \)
2) Deterministic nothing prob.
in unitary evol
3) Continuous

apply \( S \) or \( T \) twice or \( T \) four

\[
\begin{pmatrix}
1 & -i \\
-i & 1
\end{pmatrix}
\begin{pmatrix}
e^{i\theta} & 0 \\
0 & e^{-i\theta}
\end{pmatrix}
\begin{pmatrix}
e^{-i\theta} & 0 \\
0 & e^{i\theta}
\end{pmatrix}
\]

Measurement breaks all!

1) Irrev, lost \( x, \psi \)
2) Probabilistic measurement: random
3) Discontinuous, happens in an instant
Quantum Measurement problem

more is bit by bit XOR

m = 1101100001
r = 1000110001
m\oplus r = 0101010000
Quantum Key Distribution

100% provably secure encryption
One-time pad

\[ m = \text{message}, \quad n \text{ bits} \]

\[ r = n \text{ random bits} \]

\[ c = m \oplus r \quad \text{encoded message} \]

never reuse \( r \)

\[ \text{[Careful } m_0 \oplus r = c_0, \quad m_1 \oplus r = c_1 \]

Then \( c_0 \oplus c_1 = m_0 \oplus m_1 \)

has direct info on \( m_0, m_1 \)

(r cancels if reused) \]
QKD is a secure way of transmitting a onetime pad.

Alice & Bob can agree on a one-time pad and they know if it's intercepted by Eve.

\[ |0\rangle, |1\rangle \quad \begin{array}{c} \text{H} \end{array} |0\rangle \begin{array}{c} \text{H} \end{array} |1\rangle \]
Alice sends photons to Bob and each chooses independently H, I. If they choose same & measure then get same result. But if e.g. Alice \( \text{H/0} \) and Bob measures \( \text{w/o H} \) -- only 50\% agreement

<table>
<thead>
<tr>
<th>Alice prepares</th>
<th>0</th>
<th>1</th>
<th>0</th>
<th>1</th>
<th>0</th>
<th>1</th>
<th>0</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice sends</td>
<td>I</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>I</td>
<td>I</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>Bob Measures</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>I</td>
<td>I</td>
<td>H</td>
<td>I</td>
</tr>
<tr>
<td>Measures</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
By classical channel, communicate sequence of H, I, identify the roughly 50% same choice.

Discard the rest!

How do they know if intercepted by Eve? she has to guess I, H and measure. But if she guesses wrong, e.g., doesn't apply H, measures H/0 \rightarrow 10 \rightarrow then forwards to Bob, he applies H and half the time his measurement will disagree with Alice.
Alice and Bob sacrifice some of their good bits and exchange via public channel. Eve guesses H, I correctly 50% of time. If guesses wrong, then Bob's measurement corrupted half of those times. So \( \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4} \) of the sacrificed bits will disagree if eavesdrop:

\[
P_{\text{detect}} = 1 - \left( \frac{3}{4} \right)^n
\]

For \( n = 72 \) sacrificed,

\[
\approx 0.9999999999 = 1 - 10^{-9}
\]