Huygens’ principle

Each point on a wave front becomes a source of a spherical wave.
Christiaan Huygens predicted in 1678 that light behaves as a wave. Thomas Young showed in 1805 that this is indeed the case.

But if the light is measured at the slits, then it behaves as particles (photons) that travel in a straight line.
An elementary particle can behave as a wave or as a particle.

**Superposition:** A particle can simultaneously be in a range of states, with some probability distribution.

Interaction with an observer causes a particle to assume a single state.

Superposition is represented using *complex* numbers.
Complex numbers

“God made natural numbers; all else is the work of man”
(Leopold Kronecker, 1886)

\[ x + 1 = 0 \quad x = -1 \quad \mathbb{Z} \]
\[ 2x = 1 \quad x = \frac{1}{2} \quad \mathbb{Q} \]
\[ x^2 = 2 \quad x = \sqrt{2} \quad \mathbb{R} \]
\[ x^2 = -1 \quad x = i \quad \mathbb{C} \]

A complex number in \( \mathbb{C} \) is of the form \( a + bi \) with \( a, b \in \mathbb{R} \).

Fundamental theorem of algebra: \( \mathbb{C} \) is algebraically closed!
A qubit (short for quantum bit) is in a superposition

$$\alpha_0 |0\rangle + \alpha_1 |1\rangle$$

with $\alpha_0, \alpha_1 \in \mathbb{C}$, where $|\alpha_0|^2 + |\alpha_1|^2 = 1$.

At interaction with an observer, the qubit takes on the value 0 with probability $|\alpha_0|^2$, and the value 1 with probability $|\alpha_1|^2$.

After such an interaction the qubit is no longer in superposition, but in a single state 0 or 1.

For simplicity we assume that $\alpha_0, \alpha_1 \in \mathbb{R}$. (They can be negative!)
A system of two qubits has four states:

\[ \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{10} |10\rangle + \alpha_{11} |11\rangle \]

where \( \alpha^2_{00} + \alpha^2_{01} + \alpha^2_{10} + \alpha^2_{11} = 1 \).

Two independent qubits \( \alpha_0 |0\rangle + \alpha_1 |1\rangle \) and \( \beta_0 |0\rangle + \beta_1 |1\rangle \) can be described by:

\[ \alpha_0 \cdot \beta_0 |00\rangle + \alpha_0 \cdot \beta_1 |01\rangle + \alpha_1 \cdot \beta_0 |10\rangle + \alpha_1 \cdot \beta_1 |11\rangle \]
Entanglement of qubits

**Example**: Consider the 2-qubit \( \frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle \).

When one of the qubits is observed, *both* qubits assume the same state.

Such a relation between superpositions is called **entanglement**.

Entanglement can occur at the decay of an elementary particle, and is preserved when particles are no longer close to each other.

John Bell confirmed this phenomenon experimentally in 1964.
EPR paradox (1935)

Einstein, Podolsky and Rosen formulated the following paradox.

Let two entangled particles travel to different corners of the universe.

How can the superpositions of these particles be instantly related? According to relativity theory, nothing travels faster than light.
Consider a 2-qubit

$$\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

with $\alpha_{00}^2 + \alpha_{01}^2 + \alpha_{10}^2 + \alpha_{11}^2 = 1$.

If for instance the first of these qubits is measured with outcome 0, then the resulting superposition of the second qubit is

$$\frac{1}{\sqrt{\alpha_{00}^2 + \alpha_{01}^2}}(\alpha_{00}|0\rangle + \alpha_{01}|1\rangle)$$
What does a $2 \times 2$ matrix such as

\[
\begin{pmatrix}
  1 & 3 \\
  -2 & 1
\end{pmatrix}
\]

represent?

**Answer:** A *linear* mapping from $\mathbb{R}^2$ to $\mathbb{R}^2$.

It maps base vector $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ to $\begin{pmatrix} 1 \\ -2 \end{pmatrix}$, and base vector $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ to $\begin{pmatrix} 3 \\ 1 \end{pmatrix}$. 
Matrices

The 2 × 2 matrix

\[
\begin{pmatrix}
\beta_{00} & \beta_{10} \\
\beta_{01} & \beta_{11}
\end{pmatrix}
\]

maps base vector \( \begin{pmatrix} 1 \\ 0 \end{pmatrix} \) to \( \begin{pmatrix} \beta_{00} \\ \beta_{01} \end{pmatrix} \), and base vector \( \begin{pmatrix} 0 \\ 1 \end{pmatrix} \) to \( \begin{pmatrix} \beta_{10} \\ \beta_{11} \end{pmatrix} \).

A matrix is a \textit{linear} mapping:

vector \( \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} \) is by the matrix mapped to \( \alpha_0 \begin{pmatrix} \beta_{00} \\ \beta_{01} \end{pmatrix} + \alpha_1 \begin{pmatrix} \beta_{10} \\ \beta_{11} \end{pmatrix} \).

In other words,

\[
\begin{pmatrix}
\beta_{00} & \beta_{10} \\
\beta_{01} & \beta_{11}
\end{pmatrix}
\begin{pmatrix}
\alpha_0 \\
\alpha_1
\end{pmatrix}
=
\begin{pmatrix}
\alpha_0 \beta_{00} + \alpha_1 \beta_{10} \\
\alpha_0 \beta_{01} + \alpha_1 \beta_{11}
\end{pmatrix}
\]
A qubit can be interpreted as a vector of length 1:
The quantum operation

\[
\begin{pmatrix}
\beta_{00} & \beta_{10} \\
\beta_{01} & \beta_{11}
\end{pmatrix}
\]

maps \( |0\rangle \) to \( \beta_{00}|0\rangle + \beta_{01}|1\rangle \), and \( |1\rangle \) to \( \beta_{10}|0\rangle + \beta_{11}|1\rangle \).

This operation maps a qubit \( \alpha_0 |0\rangle + \alpha_1 |1\rangle \) to

\[
(\alpha_0 \cdot \beta_{00} + \alpha_1 \cdot \beta_{10}) |0\rangle + (\alpha_0 \cdot \beta_{01} + \alpha_1 \cdot \beta_{11}) |1\rangle
\]
A matrix is **unitary** if its columns are **orthonormal**: they have *length 1* and are **orthogonal** to each other.

\[
\begin{pmatrix}
\beta_{00} & \beta_{10} \\
\beta_{01} & \beta_{11}
\end{pmatrix}
\]

is unitary if:

\[
\begin{align*}
\beta_{00} \cdot \beta_{10} + \beta_{01} \cdot \beta_{11} &= 0 \\
\beta_{00}^2 + \beta_{01}^2 &= 1 \\
\beta_{10}^2 + \beta_{11}^2 &= 1
\end{align*}
\]
Unitary matrices

Unitary matrices leave *lengths* and *angles* unchanged.

Typical examples are *rotations* and *reflections*.

The composition of unitary operations is again a unitary operation.
Quantum operations: example

A quantum operation can be applied to a single qubit of an entangled pair of qubits.

**Example**: Consider the entangled 2-qubit $\frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$.

Apply to the first qubit a rotation of $\frac{\pi}{8}$ ($22.5^\circ$):

$$
\begin{pmatrix}
\cos \frac{\pi}{8} & -\sin \frac{\pi}{8} \\
\sin \frac{\pi}{8} & \cos \frac{\pi}{8}
\end{pmatrix}
$$

The superposition of the 2-qubit then becomes

$$
\frac{1}{\sqrt{2}} (\cos \frac{\pi}{8} |00\rangle - \sin \frac{\pi}{8} |01\rangle + \sin \frac{\pi}{8} |10\rangle + \cos \frac{\pi}{8} |11\rangle)
$$
Quantum operations: example

\[ \frac{1}{\sqrt{2}} (\cos \frac{\pi}{8} |00\rangle - \sin \frac{\pi}{8} |01\rangle + \sin \frac{\pi}{8} |10\rangle + \cos \frac{\pi}{8} |11\rangle) \]

Apply to the second qubit a rotation of \(-\frac{\pi}{8}\):

\[
\begin{pmatrix}
\cos \frac{\pi}{8} & \sin \frac{\pi}{8} \\
-\sin \frac{\pi}{8} & \cos \frac{\pi}{8}
\end{pmatrix}
\]

The resulting superposition of the 2-qubit is (independent from the order in which the rotations are applied):

\[ \frac{1}{\sqrt{2}} ((\cos^2 \frac{\pi}{8} - \sin^2 \frac{\pi}{8}) |00\rangle - 2 \cdot \sin \frac{\pi}{8} \cdot \cos \frac{\pi}{8} |01\rangle \\
+ 2 \cdot \sin \frac{\pi}{8} \cdot \cos \frac{\pi}{8} |10\rangle + (\cos^2 \frac{\pi}{8} - \sin^2 \frac{\pi}{8}) |11\rangle) \]
Alice and Bob each get a randomly chosen bit, $x$ and $y$. They answer, independent of each other, with a bit, $a$ and $b$. Alice and Bob win if

$$a \oplus b = x \land y$$

with $\oplus$ the XOR (i.e., addition modulo 2) and $\land$ conjunction.

$$\begin{align*}
0 \oplus 0 &= 0 \\
0 \oplus 1 &= 1 \\
1 \oplus 0 &= 1 \\
1 \oplus 1 &= 0
\end{align*}$$

On a classical computer, an optimal strategy is that Alice and Bob both always answer 0. They then win with probability 0.75.
Alice and Bob each hold a qubit of the entangled 2-qubit

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

If Alice receives \( x = 1 \), she rotates her qubit with \( \frac{\pi}{8} \).

If Bob receives \( y = 1 \), he rotates his qubit with \( -\frac{\pi}{8} \).

Finally Alice and Bob each measure their own qubit, and return the result as answer \( a \) and \( b \), respectively.

With this strategy, Alice and Bob win with a probability \( > 0.8 \).
Parity game: quantum solution

\[ x = y = 0: \text{ The superposition is } \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle). \]

So \( a \oplus b = 0 \) with probability 1.

\[ x = 1, y = 0: \text{ The superposition is } \frac{1}{\sqrt{2}} (\cos \frac{\pi}{8} |00\rangle - \sin \frac{\pi}{8} |01\rangle + \sin \frac{\pi}{8} |10\rangle + \cos \frac{\pi}{8} |11\rangle). \]

So \( a \oplus b = 0 \) with probability \( \cos^2 \frac{\pi}{8} > 0.85 \).

\[ x = 0, y = 1: \text{ Likewise } a \oplus b = 0 \text{ with probability } \cos^2 \frac{\pi}{8} > 0.85. \]
$x = y = 1$: The superposition is

$$\frac{1}{\sqrt{2}} \left( (\cos^2 \frac{\pi}{8} - \sin^2 \frac{\pi}{8}) |00\rangle - 2 \cdot \sin \frac{\pi}{8} \cdot \cos \frac{\pi}{8} |01\rangle ight)$$

$$+ 2 \cdot \sin \frac{\pi}{8} \cdot \cos \frac{\pi}{8} |10\rangle + (\cos^2 \frac{\pi}{8} - \sin^2 \frac{\pi}{8}) |11\rangle \right)$$

So $a \oplus b = 1$ with probability $(2 \cdot \sin \frac{\pi}{8} \cdot \cos \frac{\pi}{8})^2 = \sin^2 \frac{\pi}{4} = 0.5$. 

**Conclusion**: On average, Alice and Bob win with probability $> 0.8$. 
Quantum operations

Quantum operations can also be applied to $k > 1$ qubits at once.

Then the quantum operation is a *unitary* $2^k \times 2^k$-matrix:
each string in $\{0, 1\}^k$ is a base vector.

**Example:** A unitary matrix

\[
\begin{pmatrix}
\beta_{00} & \beta_{10} & \beta_{20} & \beta_{30} \\
\beta_{01} & \beta_{11} & \beta_{21} & \beta_{31} \\
\beta_{02} & \beta_{12} & \beta_{22} & \beta_{32} \\
\beta_{03} & \beta_{13} & \beta_{23} & \beta_{33}
\end{pmatrix}
\]

results in the following transformations:

\[
|00\rangle \mapsto \beta_{00}|00\rangle + \beta_{01}|01\rangle + \beta_{02}|10\rangle + \beta_{03}|11\rangle
\]
\[
|01\rangle \mapsto \beta_{10}|00\rangle + \beta_{11}|01\rangle + \beta_{12}|10\rangle + \beta_{13}|11\rangle
\]
\[
|10\rangle \mapsto \beta_{20}|00\rangle + \beta_{21}|01\rangle + \beta_{22}|10\rangle + \beta_{23}|11\rangle
\]
\[
|11\rangle \mapsto \beta_{30}|00\rangle + \beta_{31}|01\rangle + \beta_{32}|10\rangle + \beta_{33}|11\rangle
\]
Since quantum operations are unitary (and so invertible), quantum gates always have an equal number of inputs and outputs.

\[
\text{NOT: } \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}
\]

This gate transposes \( \alpha_0 |0\rangle + \alpha_1 |1\rangle \) into \( \alpha_1 |0\rangle + \alpha_0 |1\rangle \).
Quantum gates: Controlled NOT

Quantum operations can *not* copy a qubit, because this isn’t invertible, and so not unitary.

\[
\begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0
\end{pmatrix}
\]

| 00⟩  ↔  | 00⟩
| 01⟩  ↔  | 01⟩
| 10⟩  ↔  | 11⟩
| 11⟩  ↔  | 10⟩

The **CNOT** gate can be represented as |xy⟩ ↔ |x(x ⊕ y)⟩
(with ⊕ the XOR, i.e., addition modulo 2).

With CNOT, x can be copied, if we take care that initially y is |0⟩. y is some kind of working memory.
Hadamard: \[
\frac{1}{\sqrt{2}} \begin{pmatrix}
1 & 1 \\
1 & -1
\end{pmatrix}
\]

This transformation carries both \( |0\rangle \) and \( |1\rangle \) over to a superposition in which the outcomes 0 and 1 are equally likely.
Quantum circuits

CNOT

\[ |x\rangle \quad \text{CNOT} \quad |x\rangle \]
\[ |y\rangle \quad |x \oplus y\rangle \]

Hadamard

| H |
Superdense coding

Instead of two classical bits $b_1, b_2$, Alice can send one qubit to Bob. Alice holds the first and Bob the second qubit of an entangled 2-qubit $\frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$.

If $b_1 = 1$, then Alice performs $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ on her qubit.

If $b_2 = 1$, then Alice performs $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ on her qubit.

Alice sends her qubit to Bob, who performs:
- CNOT on the 2-qubit; and next
- Hadamard on the qubit of Alice.

Finally Bob measures both qubits, which have values $b_1$ and $b_2$. 
Superdense coding

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

<table>
<thead>
<tr>
<th>Pauli-Z</th>
<th>NOT</th>
<th>CNOT</th>
<th>Hadamard</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\begin{pmatrix} 1 &amp; 0 \ 0 &amp; -1 \end{pmatrix}$, $b_1 = 1$</td>
<td>$\begin{pmatrix} 0 &amp; 1 \ 1 &amp; 0 \end{pmatrix}$, $b_2 = 1$</td>
<td>$\begin{pmatrix} 1 &amp; 0 &amp; 0 &amp; 0 \ 0 &amp; 1 &amp; 0 &amp; 0 \ 0 &amp; 0 &amp; 0 &amp; 1 \ 0 &amp; 0 &amp; 1 &amp; 0 \end{pmatrix}$</td>
<td>$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 &amp; 1 \ 1 &amp; -1 \end{pmatrix}$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Alice on 1\textsuperscript{st} qubit</th>
<th>Alice on 1\textsuperscript{st} qubit</th>
<th>Bob on 2-qubit</th>
<th>Bob on 1\textsuperscript{st} qubit</th>
</tr>
</thead>
<tbody>
<tr>
<td>$00$</td>
<td>$\frac{1}{\sqrt{2}} (</td>
<td>00\rangle +</td>
<td>11\rangle)$</td>
</tr>
<tr>
<td>$01$</td>
<td>$\frac{1}{\sqrt{2}} (</td>
<td>00\rangle +</td>
<td>11\rangle)$</td>
</tr>
<tr>
<td>$10$</td>
<td>$\frac{1}{\sqrt{2}} (</td>
<td>00\rangle -</td>
<td>11\rangle)$</td>
</tr>
<tr>
<td>$11$</td>
<td>$\frac{1}{\sqrt{2}} (</td>
<td>00\rangle -</td>
<td>11\rangle)$</td>
</tr>
</tbody>
</table>