An introduction to
Quantum computing

- Quantum computing: A brief historical journey
- States, qubits, superposition, entanglement
- Existing packages: Cirq (main), Quiskit, Forest
- Examples
Resources:


2. J. D. Hidary “Quantum computing: An applied approach.” Springer, 2019


4. Austin Gilliam, Charlene Venci, Sreraman Muralidharan, Vitaliy Dorum, Eric May, Rajesh Narasimhan, and Constantin Gonciulea
   Foundational Patterns for Efficient Quantum Computing

**Motivation:** Moore’s law: harder and harder to gain speed out of traditional computers

- The Church-Turing thesis: *Any algorithmic process can be simulated efficiently using a Turing machine.*

- However some types of computations may be difficult/ impossible to solve *efficiently* on standard computers ... 

- ... but can be solved *efficiently* on non-standard computers – e.g. “Analogue computers”

- Question: How about trying to exploit properties of the quantum world to solve ‘hard problems’?
Question asked by David Deutsch in 1985 - answered the question positively

Breakthrough: Shor’s algorithm [1994]: demonstration of how to find prime factors of large integers – main ingredient of encryption

Currently: Huge regain of interest from governments and private sector

Note: IBM has an experimental quantum computer ('Q' computer, 53 qubits) as does Google ('Sycamore' also 53 qubits),

Caveat emptor: No one knows if QC will succeed in becoming general purpose platforms that will eventually replace current computers..
At the end of the 19th century it was discovered that classical mechanics does not provide an accurate picture of the microscopical world. A few discoveries made in those days set in motion one of the most important and fascinating chapters of physics. See: “30 years that shook physics” - by George Gamov, Dover for an interesting account.

The quantum world is very different from classical one. Can be counter-intuitive.

If one observes a quantum object it looks like a particle, but when it is not being observed it behaves like a wave.

Wave-particle duality → many interesting physical phenomena.

Example: quantum objects can exist in multiple states at once. Superposition of these objects interfere like waves to define a quantum state. The main property that gives quantum computing its power: superposition of states.
"Imagine a pot with water in it. When you have water in a pot with a top on it, you don’t know if it’s boiling or not. Real water is either boiling or not; looking at it doesn't change its state. But if the pot was in the quantum realm, the water (representing a quantum particle) could both be boiling and not boiling at the same time or any linear superposition of these two states. If you took the lid off of that quantum pot, the water would immediately be one state or the other. The measurement forces the quantum particle (or water) into a specific observable state.”

- The state of a quantum-mechanical system is described by a wavefunction $\psi$ - a function of the coordinates of each particle. This function is a solution of the Schrödinger equation.

- The wavefunction $\psi$ lies in a complex Hilbert space [think of this $\mathbb{C}^n$ where $n = \infty$]

- The wavefunction $\psi$ is a linear combination of some orthonormal basis functions (e.g. the eigenstates of the Hamiltonian)
When we observe the state we see only one component. If we repeat the experiment we may observe another state. But the states appear with probabilities given by the amplitudes $= | \text{coefficients} |^2$.

Two or more quantum states in a system can be strongly linked: measurement of one dictates the possible measurement outcomes for another – regardless of the distance between the two objects.

The property underlying this phenomenon is known as entanglement and it at the core of the huge potential power of QC.

**Entanglement**

Two qubits are entangled if they cannot act independently from one another: They are 100% correlated. This situation is physical: the counter-intuitive fact is that the correlation persists even when the particles are physically far apart from each other.
Q: How does QC work?

Answer: one can design quantum circuits that can be manipulated with, e.g., energy fields – You design the circuit [this is like coding in classical computing] - then the hardware will run the circuit and you observe some output.. need to repeat and average. [one observation by itself is useless]
Quantum computing: Notation

- Linear algebra notation: \[ \psi = a_0 \psi_0 + a_1 \psi_1 + \cdots + a_j \psi_j + \cdots \]
- Quantum mechanics notation: \[ |\psi\rangle = a_0 |0\rangle + a_1 |1\rangle + \cdots + a_j |j\rangle + \cdots \]

- Think of \(|\psi\rangle\) as the column vector \[
\begin{pmatrix}
a_0 \\
a_1 \\
\vdots \\
a_j
\end{pmatrix}
\]
- Then \(\langle \psi |\) will be the transpose conjugate of this vector

- \(\langle u | v \rangle\) is the (complex) inner product of \(u\) and \(v\) - (a scalar).
- ... \(|u\rangle\langle v|\) is the 'outer product' of \(u\) and \(v\) – a matrix \((uv^H)\) in standard LA notation)
\[ |\psi(x_1, x_2, \ldots, x)|^2 \] represents a probability. Its integral over space is 1, i.e.,

\[ \langle \psi | \psi \rangle = 1 \]

The energy of a system is governed by a Hamiltonian

\[ E(\psi) = \langle \psi | H | \psi \rangle \]

Ground state: Minimum energy (i.e., \( \psi \) minimizes \( E(\psi) \))

Feynman suggested to use a quantum-mechanical system to actually compute the wavefunction

L. K. Glover  

Perhaps the most surprising thing about quantum computing is that it was so slow to get started. Physicists have known since the 1920s that the world of subatomic particles is a realm apart, but it took computer scientists another half-century to begin wondering whether quantum effects might be harnessed for computation. The answer was far from obvious.
Early work:

- Charles Bennett [physicist, IBM Watson]
- Paul Benioff [Physicist, Argonne Nat. lab]
- Richard Feynman [Physicist, Caltech]
bits and qubits

- Standard computers use bits. A bit can take the value 0 or 1.
- A quantum bit or ‘qubit’ stores a combination of zero and one. Its state is represented by

\[ |\psi\rangle = a_0|0\rangle + a_1|1\rangle \]

where \( a_0, a_1 \) are complex and

\[ |a_0|^2 + |a_1|^2 = 1 \]

- Difference with classical computing: if we ‘observe’ state \( |\psi\rangle \) we will see either \( |0\rangle \) (probability \( |a_0|^2 \)) or \( |1\rangle \) (probability \( |a_1|^2 \))
The Bloch sphere

* State of a single qubit: \( |\psi\rangle = a_0|0\rangle + a_1|1\rangle \)

* \( a_1, a_2 \) are complex. So in principle we would need 4 real variables

* Also recall that we must have \( |a_0|^2 + |a_1|^2 = 1 \)

* First consider *real* combinations of the two base states. Write in the form:

\[
|\psi\rangle = \cos\left(\frac{\theta}{2}\right) |0\rangle + \sin\left(\frac{\theta}{2}\right) |1\rangle
\]

* Note: for \( \theta = 0 \) we get \( |0\rangle \) and for \( \theta = \pi \) we get \( |1\rangle \)

* Add complex phase to the 2nd term (only) [keeping \( a_0 \) real]:

\[
|\psi\rangle = \cos\left(\frac{\theta}{2}\right) |0\rangle + e^{i\varphi} \sin\left(\frac{\theta}{2}\right) |1\rangle
\]
A qubit state can be represented on a so-called Bloch Sphere.

**Case** \( \varphi = 0 \)

**General case**

Note: \( 0 \leq \theta \leq \pi \quad 0 \leq \varphi < 2\pi \)
How did we manage to use a sphere (3 parameters) in 3 dimensions while we started off with 4 (real) parameters?

What are all 6 states that correspond to the 6 points where the sphere touches the 3 axes ($x, y, z$ axes). [Hint: 2 of these are obvious. For the others determine $\theta$ and $\varphi$....]

Take a state represented in the form $\left( \begin{array}{c} \cos(\theta/2) \\ \sin(\theta/2)e^{i\varphi} \end{array} \right)$. What are the values of $x$, $y$, and $z$ on the sphere?
Operators that act on one qubit in a certain state (to produce one qubit in a certain state)

Each operator is a mapping from $\text{span}\{|0\rangle, |1\rangle\}$ to itself.

We use the basis: $\{|0\rangle, |1\rangle\}$.

In this basis $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

With this: Each operator can be viewed as a mapping from $\mathbb{C}^2$ to itself → Can be expressed as a $2 \times 2$ matrix.

Note: Each of them is unitary [in particular it preserve length]

Why is this property required?

Next we’ll see a few of the most important ones
The NOT operator

['Pauli-X' operator]

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

If we apply \( X \) to the state \( |0\rangle \) we get

\[ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \times \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle \]

Note: for \( j \in \{0, 1\} \) we have:

\[ X|j\rangle = |j \oplus 1\rangle \]

where \( \oplus \) is the exclusive or.

DIAGRAM: \[ \begin{array}{c} \text{X} \\ \end{array} \] or \[ \begin{array}{c} \text{X} \end{array} \]
\[
\begin{pmatrix}
1 \\
0
\end{pmatrix} \rightarrow \begin{pmatrix}
0 \\
1
\end{pmatrix} \quad \text{or} \quad |0\rangle \rightarrow |1\rangle
\]

What does this operation do to a point on the Bloch sphere?

**Sol:** The phase $\varphi$ makes no difference. Assume it is 0.

\[
\begin{pmatrix}
\cos(\theta/2) \\
\sin(\theta/2)
\end{pmatrix} \rightarrow \begin{pmatrix}
\sin(\theta/2) \\
\cos(\theta/2)
\end{pmatrix} = \begin{pmatrix}
\cos(\frac{\pi-\theta}{2}) \\
\sin(\frac{\pi-\theta}{2})
\end{pmatrix}
\]

**Verification:** when applied to $|+\rangle = \frac{1}{\sqrt{2}} [|0\rangle + |1\rangle]$ you get the same result. The point is invariant - as expected.

**θ → π − θ →:** Symmetry about the $x, y$ plane.
The Y operator

\[ Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \]

Example:

\[ Y|j\rangle = (-1)^j i |1 \oplus j\rangle \]

Diagram: \[ \text{Y} \]

The Z operator

\[ Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \]

Example:

\[ Z|j\rangle = (-1)^j |j\rangle \]

Diagram: \[ \text{Z} \]
**The $R_\varphi$ operator**

\[ R_\varphi = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix} \]

Example:

\[ R_\varphi |1\rangle = e^{i\varphi} |1\rangle \]

DIAGRAM: \[ R_\varphi \]

$R_\varphi$ = phase shift op.

- Two particular cases:
  - $\varphi = \pi/2$ → $S$ operator
    - rotates state by $\pi/2$ around z-axis
  - $\varphi = \pi/4$ → $T$ operator
    - rotates state by $\pi/4$ around z-axis

Note that $S = T^2$

**Alternative – and equivalent on the Boch sphere – to $R_\varphi$ is:**

\[ R_z(\varphi) = \begin{pmatrix} e^{-i\varphi} & 0 \\ 0 & e^{i\varphi} \end{pmatrix} \]

**Explain why on Bloch sphere, $R_\varphi$ is equivalent to $R_z(\varphi)$**

**Let us take a look at the Bloch sphere.**
\[
\begin{pmatrix}
1 & 0 \\
0 & e^{i\varphi}
\end{pmatrix}
\begin{pmatrix}
\cos(\theta/2) \\
e^{i\varphi_0} \sin(\theta/2)
\end{pmatrix}
= \begin{pmatrix}
\cos(\theta/2) \\
e^{i(\varphi_0+\varphi)} \sin(\theta/2)
\end{pmatrix}
\]

Rotation of angle \(\varphi\) around \(z\) axis.

The other two rotations \(R_x(\theta)\) and \(R_y(\theta)\) of angle \(\theta\) around the \(x\) and \(y\) axes respectively are:

\[
R_x(\theta) = \begin{pmatrix}
\cos \frac{\theta}{2} & -i \sin \frac{\theta}{2} \\
-i \sin \frac{\theta}{2} & \cos \frac{\theta}{2}
\end{pmatrix}
\]

\[
R_y(\theta) = \begin{pmatrix}
\cos \frac{\theta}{2} & -\sin \frac{\theta}{2} \\
\sin \frac{\theta}{2} & \cos \frac{\theta}{2}
\end{pmatrix}
\]

\[
\text{Bloch sphere: What actions do you get when } \varphi = 0?\]
The Hadamard operator

\[ H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \]

Example:

\[ H |0\rangle = \frac{1}{\sqrt{2}} [ |0\rangle + |1\rangle ] \]

Properties

- \(HXH = ?\)
- \(HZH = X\)
- \(HYH = ?\)
- \(H^{-1} = ?\)
- \(H^2 = ?\)
- \(S^2 = ?\)

Later, we will exploit the relation \(HZH = X\)
Recall: In classical setting, only one gate is needed to implement any function of bits - the NAND gate

<table>
<thead>
<tr>
<th>a</th>
<th>b</th>
<th>a AND b</th>
<th>a NAND b</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

Quantum setting: Any $n$-qubit gate can be made from 2-qubit gates. Specifically: Any multiple qubit logic gate may be composed from CNOT and single qubit gates.

This is because: Any unitary $n \times n$ can be decomposed as a product of 2-level unitary matrices, i.e., unitary matrices that act only on two-or-fewer vector components.

[essentially: rotations, and complex scalings]
Two qubits

- Let $q_0, q_1$ be two qubits.
- A 2-qubit register is a combination of 4 states

$$|\psi\rangle = a_0|00\rangle + a_1|01\rangle + a_2|10\rangle + a_3|11\rangle$$

- The space of these 4 states is $\mathbb{C}^2 \otimes \mathbb{C}^2$
- $|ij\rangle$ means: $q_0$ is in state $|i\rangle$ and $q_1$ is in state $|j\rangle$
- In what follows $e_1, e_2, e_3, e_4$ are the 4 canonical basis vectors of $\mathbb{C}^4$, i.e., the 4 columns of the identity matrix.
By convention the basis of the resulting space is

\[ |\psi_1\rangle = |00\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = e_1 \]

\[ |\psi_2\rangle = |01\rangle, = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = e_2 \]

\[ |\psi_3\rangle = |10\rangle, = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = e_3 \]

\[ |\psi_4\rangle = |11\rangle, = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = e_4 \]

So for example \[ |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \text{ and } |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}. \]
Entanglement: An example

Case 1: $|\psi\rangle = |00\rangle$

Measuring $|\psi\rangle$ we will find with 100% probability that the first qubit $q_0$ is $|0\rangle$ and similarly that $q_1$ is $|0\rangle$.

Case 2: $|\psi\rangle = \frac{1}{\sqrt{2}} [|00\rangle + |11\rangle]$

* 50% chance of observing $|00\rangle$ and 50% chance of observing $|11\rangle$

* However, if we measure $q_0$ and find that $q_0 = |0\rangle$ then we know that the outcome must be $|00\rangle$ therefore $q_1 = |0\rangle$ also

* If we measure $q_0$ and find that $q_0 = |1\rangle$ then we know that the outcome must be $|11\rangle$ therefore $q_1 = |1\rangle$ also

* In case 2, the two qubits are 100% correlated. They are entangled
A important few binary operators

Input: 2 qubits – out 2 qubits

\[
\text{SWAP} = \begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 \\
\end{pmatrix}
\]

DIAGRAM:

\[
\text{CNOT} = \begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 \\
\end{pmatrix}
\]

DIAGRAM:
CNOT stands for controlled not. Very important in quantum logic.

First input qubit $q_0$ plays the role of a control qubit.

Second qubit is the target qubit.

On output top qubit remains the same. Lower one is flipped ('Not' applied to it) when (and only when) control bit is $|1\rangle$.

The following exercise will help you understand this.

Determine the output states for each of all 4 possible inputs states. Use the CNOT diagram to illustrate this.
Logical operation of CNOT gate: if $a$ is in state $|1\rangle$ flip qubit $b$

<table>
<thead>
<tr>
<th>$ab\rangle$</th>
<th>$ab'\rangle$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$</td>
<td>00\rangle$</td>
</tr>
<tr>
<td>$</td>
<td>01\rangle$</td>
</tr>
<tr>
<td>$</td>
<td>10\rangle$</td>
</tr>
<tr>
<td>$</td>
<td>11\rangle$</td>
</tr>
</tbody>
</table>

0----*----? 0----*----?
| 0---(+)---? 1---(+)---?
| 1----*----? 1----*----?
| 0---(+)---? 1---(+)---?
Controlled $Z$ operator

$q_0 = \text{control qubit}, \quad q_1 = \text{target}$

$Z$ operator applied to $q_1$ iff $q_0 = |1\rangle$

Note: CZ is symmetric, i.e., control-target roles of $q_0, q_1$ can be exchanged
The Bell State

1. Start with \( q_0 := |0\rangle \) and \( q_1 := |0\rangle \)

2. Apply Hadamard to \( q_0 \rightarrow q_0 := H|0\rangle = |+\rangle \)

3. Apply CNOT gate to \( q_0 \) and \( q_1 \): the 2 qubits are now entangled

The resulting entangled state is the state \( |\psi\rangle = \frac{1}{\sqrt{2}} [ |00\rangle + |11\rangle \) of case 2 seen before. It is called a Bell State. In quantum physics this involves two particles that form a so-called EPR pair. [EPR stands for Einstein, Podolsky and Rosen]

• It is known that Einstein was very skeptical about quantum mechanics ("God does not play dice" he once stated). In a 1935 article, Einstein, Podolsky and Rosen, tried to show that quantum mechanics would lead to a contradiction. – it was a contradiction to our logic of thinking. But the nano world is different.
Thus from, say, 500 particles you could, in principle, create a quantum system that is a superposition of as many as $2^{500}$ states. Each state would be a single list of 500 1’s and 0’s. Any quantum operation on that system—a particular pulse of radio waves, for instance, whose action was, say, to execute a controlled-NOT operation on the 175th and 176th qubits—would simultaneously operate on all $2^{500}$ states. Hence with one machine cycle, one tick of the computer clock, a quantum operation could compute not just on one machine state, as serial computers do, but on $2^{500}$ machine states at once! That number, which is approximately equal to a 1 followed by 150 zeros, is far larger than the number of atoms in the known universe. Eventually, of course, observing the system would cause it to collapse into a single quantum state corresponding to a single answer, a single list of 500 1’s and 0’s— but that answer would have been derived from the massive parallelism of quantum computing.
Three qubits

- We now have 3 input qubits and 3 outputs. Operators are $8 \times 8$ matrices.
- State represented by eight vectors $e_1, e_2, \cdots, e_8$.

**Toffoli**

Matrix = $8 \times 8$ Identity with last 2 columns swapped.

- $q_0$ and $q_1$ are both control qubits; $q_2$ = target.
- NOT operator applied to $q_2$ iff $q_0 = |1\rangle$ AND $q_1 = |1\rangle$.
- Determine each of the output states for all 8 possible inputs.
Other symbols used

- Measurement symbol
- $n$ qubit inputs
- Apply operator $n$ qubits
Quantum teleportation (outline of an example)

- Bob and Alice now live far apart. When together they generated an EPR pair and each took one qubit of the pair before separating.
- Alice wants to send a qubit $|\psi\rangle$ to Bob by sending classical information
- Difficulty: measuring $|\psi\rangle$ not possible [will yield one state]
- Solution: Interact the $|\psi\rangle$ with her half of the EPR state. Measure the 2 qubits. Result one of 00, 01, 10, 11.
- Send this (classical info) info to Bob.
- Bob performs one of 4 operations [depending on what he received from Alice]
- Bob recovers $|\psi\rangle$
Notes: double lines carry classical information. Top 2 lines: Alice, Bottom: Bob.

Details to be added