

Introduction to Quantum Computing

How I Learned to Stop Worrying and Love the Bomb

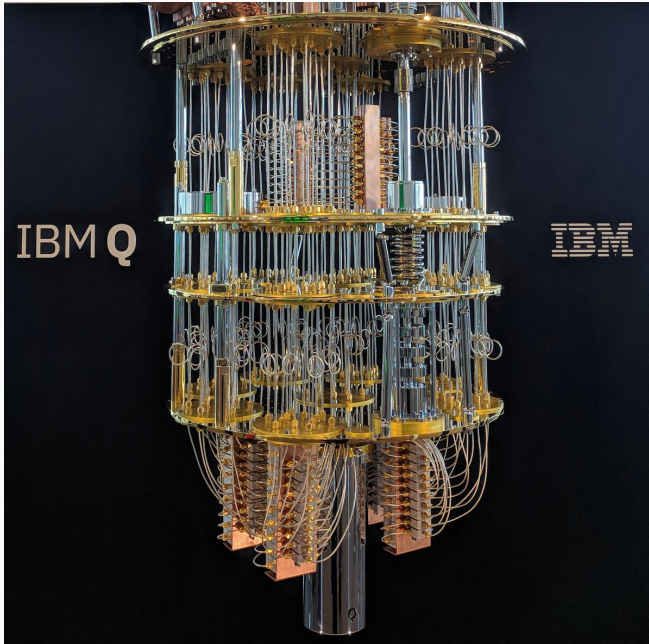
Dr. Omri Har-Shemesh

13. February 2019

Schmiede.ONE GmbH & Co. KG

Introduction

Ce n'est pas un lustre (This is not a Chandelier)



- New computing paradigm

- New computing paradigm
- Uses the rules of quantum mechanics

- New computing paradigm
- Uses the rules of quantum mechanics
- Might be able to solve some problems exponentially faster

- New computing paradigm
- Uses the rules of quantum mechanics
- **Might** be able to solve **some** problems exponentially faster
- **Definitely** could simulate quantum systems better

- New computing paradigm
- Uses the rules of quantum mechanics
- **Might** be able to solve **some** problems exponentially faster
- **Definitely** could simulate quantum systems better
- Realizable in large scale?

- New computing paradigm
- Uses the rules of quantum mechanics
- Might be able to solve some problems exponentially faster
- Definitely could simulate quantum systems better
- Realizable in large scale?
- $\neg_(\text{ツ})_/\neg$

The Technical Part

“Shut up and calculate”

David Mermin

- Representing computation with linear algebra
- Qubits, superposition and quantum logic gates
- Simplest problem where a quantum computer outperforms a classical one
- Bonus: Quantum entanglement and quantum teleportation

Representing classical bits as vectors

One bit with value 0, also written as $|0\rangle$ (Dirac vector notation)

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

One bit with value 1, also written as $|1\rangle$

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Review: matrix multiplication

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}$$

$$\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} ax + by + cz \\ dx + ey + fz \\ gx + hy + iz \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} w & x \\ y & z \end{pmatrix} = \begin{pmatrix} aw + by & ax + bz \\ cw + dy & cx + dz \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}$$

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

Operations on one classical bit (cbit)

Identity	$f(x) = x$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$
Negation	$f(x) = \neg x$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$
Constant-0	$f(x) = 0$	$\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$
Constant-1	$f(x) = 1$	$\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

- Given the operation and the input, you can always infer the output.
 - For $Ax = b$, given b and A , you can uniquely find x .

- Given the operation and the input, you can always infer the output.
 - For $Ax = b$, given b and A , you can uniquely find x .
- Permutations are reversible; erasing and overwriting are not
 - Identity and negation are reversible.
 - Constant-0 and Constant-1 are not reversible.

- Given the operation and the input, you can always infer the output.
 - For $Ax = b$, given b and A , you can uniquely find x .
- Permutations are reversible; erasing and overwriting are not
 - Identity and negation are reversible.
 - Constant-0 and Constant-1 are not reversible.
- Quantum computers use **only reversible operations**.
 - In fact, all quantum operations are their own inverse.

Review: tensor product of vectors

$$\begin{pmatrix} x_0 \\ x_1 \end{pmatrix} \otimes \begin{pmatrix} y_0 \\ y_1 \end{pmatrix} = \begin{pmatrix} x_0 \begin{pmatrix} y_0 \\ y_1 \end{pmatrix} \\ x_1 \begin{pmatrix} y_0 \\ y_1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} x_0 y_0 \\ x_0 y_1 \\ x_1 y_0 \\ x_1 y_1 \end{pmatrix}$$

$$\begin{pmatrix} 1 \\ 2 \end{pmatrix} \otimes \begin{pmatrix} 3 \\ 4 \end{pmatrix} = \begin{pmatrix} 3 \\ 4 \\ 6 \\ 8 \end{pmatrix}$$

$$\begin{pmatrix} x_0 \\ x_1 \end{pmatrix} \otimes \begin{pmatrix} y_0 \\ y_1 \end{pmatrix} \otimes \begin{pmatrix} z_0 \\ z_1 \end{pmatrix} = \begin{pmatrix} x_0 y_0 z_0 \\ x_0 y_0 z_1 \\ x_0 y_1 z_0 \\ x_0 y_1 z_1 \\ x_1 y_0 z_0 \\ x_1 y_0 z_1 \\ x_1 y_1 z_0 \\ x_1 y_1 z_1 \end{pmatrix}$$

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

Representing multiple cbits

$$\begin{aligned} |00\rangle &= \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} & |01\rangle &= \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} & |100\rangle &= \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \\ |10\rangle &= \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} & |11\rangle &= \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \end{aligned}$$

- The tensor representation is called the **product state**.
- It can be **factored** back into the **individual state** representation.
- The product state of n bits is a vector of size 2^n .

- Takes two bits, one **control** bit and one **target** bit.
- If the control bit is set, flip the target bit, otherwise leave it.

Operations on multiple cbits: CNOT

- Takes two bits, one **control** bit and one **target** bit.
- If the control bit is set, flip the target bit, otherwise leave it.
- If most significant bit is control, and least-significant is target, then:

$|00\rangle$ $|00\rangle$

$|01\rangle$ $|01\rangle$

$|10\rangle$ $|10\rangle$

$|11\rangle$ $|11\rangle$

Operations on multiple cbits: CNOT

- Takes two bits, one **control** bit and one **target** bit.
- If the control bit is set, flip the target bit, otherwise leave it.
- If most significant bit is control, and least-significant is target, then:

$$|00\rangle \longrightarrow |00\rangle$$

$$|01\rangle \qquad |01\rangle$$

$$|10\rangle \qquad |10\rangle$$

$$|11\rangle \qquad |11\rangle$$

Operations on multiple cbits: CNOT

- Takes two bits, one **control** bit and one **target** bit.
- If the control bit is set, flip the target bit, otherwise leave it.
- If most significant bit is control, and least-significant is target, then:

$$|00\rangle \longrightarrow |00\rangle$$

$$|01\rangle \longrightarrow |01\rangle$$

$$|10\rangle \longrightarrow |11\rangle$$

$$|11\rangle \longrightarrow |10\rangle$$

Operations on multiple cbits: CNOT

- Takes two bits, one **control** bit and one **target** bit.
- If the control bit is set, flip the target bit, otherwise leave it.
- If most significant bit is control, and least-significant is target, then:

$$|00\rangle \longrightarrow |00\rangle$$

$$|01\rangle \longrightarrow |01\rangle$$

$$|10\rangle \longrightarrow |10\rangle$$

$$|11\rangle \longrightarrow |10\rangle$$

Operations on multiple cbits: CNOT

- Takes two bits, one **control** bit and one **target** bit.
- If the control bit is set, flip the target bit, otherwise leave it.
- If most significant bit is control, and least-significant is target, then:

$|00\rangle \longrightarrow |00\rangle$

$|01\rangle \longrightarrow |01\rangle$

$|10\rangle \longrightarrow |11\rangle$

$|11\rangle \longrightarrow |10\rangle$



Operations on multiple cbits: CNOT

- Takes two bits, one **control** bit and one **target** bit.
- If the control bit is set, flip the target bit, otherwise leave it.
- If most significant bit is control, and least-significant is target, then:

$|00\rangle \longrightarrow |00\rangle$

$|01\rangle \longrightarrow |01\rangle$

$|10\rangle \xrightarrow{\text{red}} |11\rangle$

$|11\rangle \xrightarrow{\text{red}} |10\rangle$

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

$$C|10\rangle = C\left(\begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |11\rangle$$

$$C|11\rangle = C\left(\begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |10\rangle$$

$$C|00\rangle = C\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |00\rangle$$

$$C|01\rangle = C\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |01\rangle$$

Qubits and superposition

- Cbits are a special case of Qubits!
- A qbit is represented by $\begin{pmatrix} a \\ b \end{pmatrix}$ where a and b are complex numbers such that $||a||^2 + ||b||^2 = 1$.
 - The cbit vectors $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ fit this definition.
- Example qbit values:

$$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \quad \begin{pmatrix} \frac{1}{2} \\ \frac{\sqrt{3}}{2} \end{pmatrix} \quad \begin{pmatrix} -1 \\ 0 \end{pmatrix} \quad \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \end{pmatrix}$$

What does that mean?

What does that mean?

Superposition

The qbit is in a state of both $|0\rangle$ and $|1\rangle$. We can write this as:

$$\begin{pmatrix} a \\ b \end{pmatrix} = a \begin{pmatrix} 1 \\ 0 \end{pmatrix} + b \begin{pmatrix} 0 \\ 1 \end{pmatrix} = a|0\rangle + b|1\rangle.$$

Qbits and superposition

What does that mean?

Superposition

The qbit is in a state of both $|0\rangle$ and $|1\rangle$. We can write this as:

$$\begin{pmatrix} a \\ b \end{pmatrix} = a \begin{pmatrix} 1 \\ 0 \end{pmatrix} + b \begin{pmatrix} 0 \\ 1 \end{pmatrix} = a|0\rangle + b|1\rangle.$$

Amplitudes

a and b are called amplitudes. $||a||^2$ is the probability of the qbit being 0 when **measured**; $||b||^2$ is the probability of measuring 1.

Qbits and superposition

What does that mean?

Superposition

The qbit is in a state of both $|0\rangle$ and $|1\rangle$. We can write this as:

$$\begin{pmatrix} a \\ b \end{pmatrix} = a \begin{pmatrix} 1 \\ 0 \end{pmatrix} + b \begin{pmatrix} 0 \\ 1 \end{pmatrix} = a|0\rangle + b|1\rangle.$$

Amplitudes

a and b are called amplitudes. $||a||^2$ is the probability of the qbit being 0 when **measured**; $||b||^2$ is the probability of measuring 1.

Measurement

The measurement of the qbit **collapses** its state. It will be in the state $|0\rangle$ if we measured 0 and $|1\rangle$ if we measured 1.

For example

The qbit $\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$ has a $\left\| \frac{1}{\sqrt{2}} \right\|^2 = \frac{1}{2}$ chance of collapsing to $|0\rangle$ or $|1\rangle$.

The qbit $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ has 100% chance of collapsing to $|0\rangle$, and $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ has a 100% chance of collapsing to $|1\rangle$.