Introduction to Quantum Computing from Math perspective

Pavel Belevich

New York Quantum Computing Meetup

March 28, 2018

What is qubit?

Definition

A qubit is a unit vector in two dimensional space of complex numbers

Examples

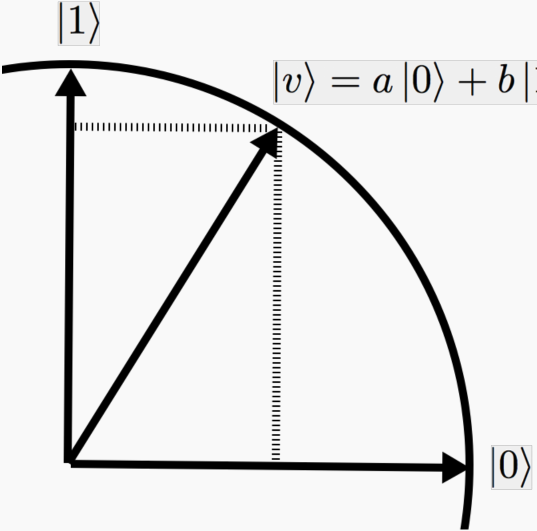
$$\begin{pmatrix} \frac{3}{5} \\ \frac{4}{5} \end{pmatrix}, \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{-i}{\sqrt{2}} \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ i \end{pmatrix}, \begin{pmatrix} \frac{2-3i}{\sqrt{54}} \\ \frac{4+5i}{\sqrt{54}} \end{pmatrix}$$

or any $|v\rangle = a\,|0\rangle + b\,|1\rangle = \begin{pmatrix} a \\ b \end{pmatrix}, s.t. |a|^2 + |b|^2 = 1$

Note

$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ are pure states, corresponded to classical bit values "0" and "1".

What is qubit?



Tossing a coin analogy

Tossing coin("0" is head, "1" is tail) is a perfect analogy of superposition state

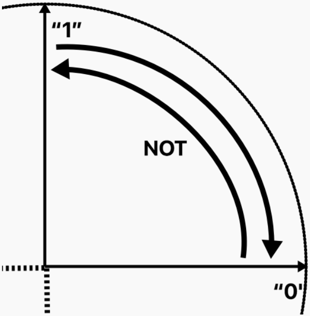
Until it's stopped by observer it is in 50% of "0" and 50% of "1" state

We need something that is between "0" and "1" or rather something that is partially "0" and partially "1"

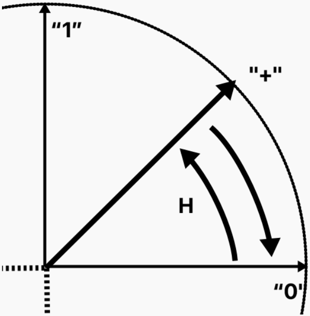
Gates

Q: If we have only unit vectors what can we do with them?
A: Rotate! If we can't change vector length then any transformation is just a rotation

NOT gate rotates $|0\rangle$ to $|1\rangle$ and vise versa



Hadamard gate rotates $|0\rangle$ to $|+\rangle$ and vise versa



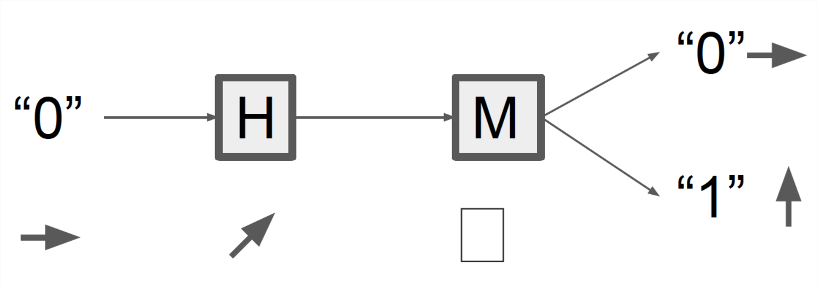
Quantum computing “Hello world”?

Tossing coin

1. Take a coin
2. Toss it
3. Catch it
4. Obtain random value "head" or "tail"

Tossing coin program

1. Take a qubit in pure $|0\rangle$ state
2. Apply Hadamard gate to get superposition $|+\rangle$ state
3. Measure it
4. Obtain random value "0" or "1"



NOT Gate

How should NOT Gate X look like if we know that:

$$X\left|0\right\rangle = \left|1\right\rangle \tag{1}$$

$$X\left|1\right\rangle = \left|0\right\rangle \tag{2}$$

In other words what can rotate vector $\begin{pmatrix}1\\0\end{pmatrix}$ into vector $\begin{pmatrix}0\\1\end{pmatrix}$ and vise versa?

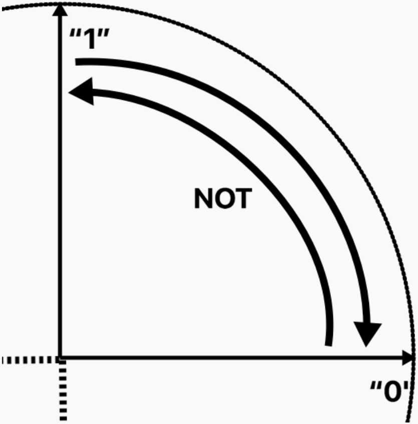
$$X\left|0\right\rangle = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix} = \left|1\right\rangle \tag{3}$$

$$X\left|1\right\rangle = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix} = \left|0\right\rangle \tag{4}$$

So Gate NOT is a matrix

$$X = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix} \tag{5}$$

NOT Gate



Hadamard Gate

Consider matrix $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and let's apply it to $|0\rangle$ and $|1\rangle$:

$$H|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = |+\rangle \tag{6}$$

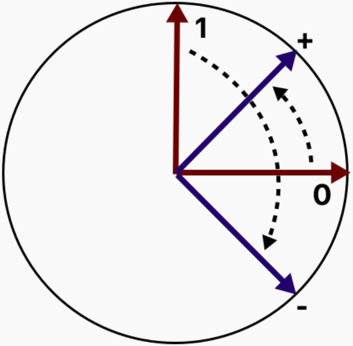
$$H|1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix} = |-\rangle \tag{7}$$

Now let's apply H to to $|+\rangle$ and $|-\rangle$:

$$H|+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 2 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle \tag{8}$$

$$H|-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 0 \\ 2 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle \tag{9}$$

Hadamard Gate



What do we know so far?

- A qubit is a vector, its projections to “0” and “1” axes represent how likely this qubit is “0” and “1”
- We can pass a qubit through some gates that “rotate” it and changes projections to “0” and “1” axes
- A gate is a matrix, applying the gate matrix to a qubit vector "rotates" the qubit
- We can measure a qubit and it becomes either 0 or 1 depending on it’s projections to "0" and "1" axes
- Measurement gives us a natural random mechanism
- Hadamard Gate H rotates $|0\rangle$ to superposition state $|+\rangle$, which has equal projections to "0" and "1" axis
- NOT Gate X rotates $|0\rangle$ to $|1\rangle$ and $|1\rangle$ to $|0\rangle$
- We can write two stupid 1-qubit programs: 1) 0/1 random generator 2) negation program

What about two qubits?

Consider two qubits:

$$|p\rangle = a\,|0_p\rangle + b\,|1_p\rangle \tag{10}$$

$$|q\rangle = c\,|0_q\rangle + d\,|1_q\rangle \tag{11}$$

What if we multiply them?

$$|p\rangle \otimes |q\rangle = ac\,|0_p\rangle \otimes |0_q\rangle + ad\,|0_p\rangle \otimes |1_q\rangle + bc\,|1_p\rangle \otimes |0_q\rangle + bd\,|1_p\rangle \otimes |1_q\rangle \tag{12}$$

Let's define the following notation:

$$|v\rangle \otimes |w\rangle = |vw\rangle \tag{13}$$

$$|pq\rangle = ac\,|0_p 0_q\rangle + ad\,|0_p 1_q\rangle + bc\,|1_p 0_q\rangle + bd\,|1_p 1_q\rangle \tag{14}$$

Or

$$|pq\rangle = ac\,|00\rangle + ad\,|01\rangle + bc\,|10\rangle + bd\,|11\rangle \tag{15}$$

What about two qubits?

If

$$|a|^2 = Prob(p = 0)$$
$$|b|^2 = Prob(p = 1)$$
$$|c|^2 = Prob(q = 0)$$
$$|d|^2 = Prob(q = 1)$$

then

$$|ac|^2 = Prob(p = 0) * Prob(q = 0) = Prob(p = 0; q = 0) = Prob(00)$$

$$|ad|^2 = Prob(p = 0) * Prob(q = 1) = Prob(p = 0; q = 1) = Prob(01)$$
$$|bc|^2 = Prob(p = 1) * Prob(q = 0) = Prob(p = 1; q = 0) = Prob(10)$$
$$|bd|^2 = Prob(p = 1) * Prob(q = 1) = Prob(p = 1; q = 1) = Prob(11)$$

We can describe 2 qubits using 4 dimensional vector in the $(|00\rangle, |01\rangle, |10\rangle, |11\rangle)$ basis.

How do two-qubit vectors look like?

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 * \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ 0 * \begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ \begin{pmatrix} 0 \\ 0 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \tag{16}$$

$$|01\rangle = |0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 * \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ 0 * \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ \begin{pmatrix} 0 \\ 0 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \tag{17}$$

$$|10\rangle = |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 * \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ 1 * \begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} 0 \\ 0 \end{pmatrix} \\ \begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \tag{18}$$

$$|11\rangle = |1\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 * \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ 1 * \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} 0 \\ 0 \end{pmatrix} \\ \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \tag{19}$$

How do two-qubit vectors look like?

$$|p\rangle = a\,|0\rangle + b\,|1\rangle = a\begin{pmatrix}1\\0\end{pmatrix} + b\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}a\\b\end{pmatrix} \tag{20}$$

$$|q\rangle = c\,|0\rangle + d\,|1\rangle = c\begin{pmatrix}1\\0\end{pmatrix} + d\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}c\\d\end{pmatrix} \tag{21}$$

$$|pq\rangle = |p\rangle \otimes |q\rangle = ac\,|00\rangle + ad\,|01\rangle + bc\,|10\rangle + bd\,|11\rangle = \tag{22}$$

$$= ac\begin{pmatrix}1\\0\\0\\0\end{pmatrix} + ad\begin{pmatrix}0\\1\\0\\0\end{pmatrix} + bc\begin{pmatrix}0\\0\\1\\0\end{pmatrix} + bd\begin{pmatrix}0\\0\\0\\1\end{pmatrix} \tag{23}$$

$$= \begin{pmatrix}ac\\ad\\bc\\bd\end{pmatrix} \tag{24}$$

What the ... does it mean???

N qubits can represent 2^N numbers s.t. each number squared is a probability of getting one of 2^N N-bit string.

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

$$|{+}{+}\rangle = H^{\otimes 2}|00\rangle = \frac{1}{\sqrt{2^2}}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

$$|{+}{+}{+}\rangle = H^{\otimes 3}|000\rangle = \frac{1}{\sqrt{2^3}}(|000\rangle + |001\rangle + ... + |110\rangle + |111\rangle)$$

$$\begin{aligned}|{+}{+}{+}{+}{+}{+}{+}{+}\rangle &= H^{\otimes 8}|00000000\rangle \\ &= \frac{1}{\sqrt{2^8}}(|00000000\rangle + |00000001\rangle + ... + |11111110\rangle + |11111111\rangle\end{aligned}$$

Imagine you write a program that has 1 byte input. You need to call it 256 times to get the result for each possible 8 bit number. If you have 8-qubit quantum computer you can construct an initial state that have equal probabilities of each of 256 8-bit string and call it only ONCE.

CNOT gate

Consider the following matrix:

$$CNOT = \begin{pmatrix} I & 0 \\ 0 & X \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{25}$$

Where $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $O = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ and $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

Let's apply CNOT to $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$:

$$CNOT\,|00\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = |00\rangle \tag{26}$$

$$CNOT\,|01\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = |01\rangle \tag{27}$$

$$CNOT\,|10\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = |11\rangle \tag{28}$$

$$CNOT\,|11\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = |10\rangle \tag{29}$$

As you can see if the first qubit is 0, CNOT does not change qubits, but if the first qubit is 1 it inverts the second one. This CNOT gate is Conditional NOT gate.

CNOT gate

Consider flipped CNOT gate which inverts the first qubit if the second is equal to 1.
How should $CNOT'$ look like?

$$CNOT' \left|00\right\rangle = \left|00\right\rangle \Leftrightarrow \begin{pmatrix} ? & ? & ? & ? \\ ? & ? & ? & ? \\ ? & ? & ? & ? \\ ? & ? & ? & ? \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \tag{30}$$

$$CNOT' \left|01\right\rangle = \left|11\right\rangle \Leftrightarrow \begin{pmatrix} ? & ? & ? & ? \\ ? & ? & ? & ? \\ ? & ? & ? & ? \\ ? & ? & ? & ? \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \tag{31}$$

$$CNOT' \left|10\right\rangle = \left|10\right\rangle \Leftrightarrow \begin{pmatrix} ? & ? & ? & ? \\ ? & ? & ? & ? \\ ? & ? & ? & ? \\ ? & ? & ? & ? \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \tag{32}$$

$$CNOT' \left|11\right\rangle = \left|01\right\rangle \Leftrightarrow \begin{pmatrix} ? & ? & ? & ? \\ ? & ? & ? & ? \\ ? & ? & ? & ? \\ ? & ? & ? & ? \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \tag{33}$$

Therefore flipped CNOT gate is

$$CNOT' = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \tag{34}$$

SWAP gate

What if we apply *CNOT*, flipped *CNOT* and *CNOT* consequently?

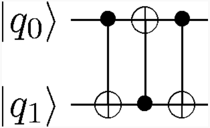


Figure: SWAP circuit [I. Chuang(2004b)]

$$SWAP = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{35}$$

SWAP gate

Let's apply SWAP to $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$:

$$SWAP\,|00\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = |00\rangle \tag{36}$$

$$SWAP\,|01\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = |10\rangle \tag{37}$$

$$SWAP\,|10\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = |01\rangle \tag{38}$$

$$SWAP\,|11\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = |11\rangle \tag{39}$$

Creating Bell state

Consider two qubits and let's apply H to the first and $CNOT$ to both:

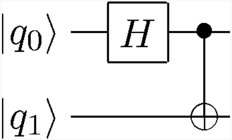


Figure: EPR Creation [I. Chuang(2004a)]

$$CNOT(H \otimes I)\,|00\rangle = \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}\left(\frac{1}{\sqrt{2}}\begin{pmatrix}1&1\\1&-1\end{pmatrix}\otimes\begin{pmatrix}1&0\\0&1\end{pmatrix}\right)\begin{pmatrix}1\\0\\0\\0\end{pmatrix}$$

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

$$= \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix} = \frac{1}{\sqrt{2}}\left(\begin{pmatrix}1\\0\\0\\0\end{pmatrix}+\begin{pmatrix}0\\0\\0\\1\end{pmatrix}\right) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

What is it important?

Applying N Hadamard gates to N qubits constructs a superposition state corresponding to 2^N numbers which is the initial step of most quantum algorithms.

Hadamard-CNOT two-qubits gate creates Bell state, which is crucial for quantum teleportation.

Applying CNOT, flipped CNOT and again CNOT swaps two qubits, which is used in Quantum Fourier transform.

References

I. Chuang.
Epr creation, 2004a.
URL https://www.media.mit.edu/quanta/qasm2circ/test1.png.

I. Chuang.
Swap circuit, 2004b.
URL https://www.media.mit.edu/quanta/qasm2circ/test3.png.

Thank you!