VERIFICATION OF QUANTUM CIRCUITS

Lecture 2: Qubits, Quantum Gates & Quantum Circuits

Reference: Chapter 5 of the text book:

"Quantum computing for Computer Scientists"

– by Yanofsky & Mannucci

Plan for the lecture:

– 1. Bits and Qubits

– 2. Qubytes

– 3. Classical gates: an alternate perspective using matrices

– 4. Reversible (classical) gate

– 5. Quantum gates and Quantum circuits

Part 1: Bits and Qubits

Bit: a unit of information describing a 2-dimensional classical system.

A bit can be in two states: 0 or 1.

→ We will view them as matrices:

State 0 will be represented as $|0\rangle$ ↳ ket notation

State 1 will be represented as $|1\rangle$

$$|0\rangle = \begin{matrix} 0 \\ 1 \end{matrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix}$$ → row corresponding to '0' has 1

$$|1\rangle = \begin{matrix} 0 \\ 1 \end{matrix}\begin{bmatrix} 0 \\ 1 \end{bmatrix}$$ → row corresponding to '1' has 1

- $|0\rangle$ and $|1\rangle$ are the 'basic states'

- A quantum system can be in state $|0\rangle$ AND in state $|1\rangle$ simultaneously.

QUBIT: A quantum bit or a qubit is a unit of information representing a 2-dimensional quantum system.

A qubit is given as follows:

$$\begin{matrix} 0 \\ 1 \end{matrix}\begin{bmatrix} c_0 \\ c_1 \end{bmatrix} \quad \text{s.t.} \quad c_0, c_1 \in \mathbb{C}$$

$$|c_0|^2 + |c_1|^2 = 1$$

Interpretation: When qubit $\begin{bmatrix} c_0 \\ c_1 \end{bmatrix}$ is measured,

it collapses to state $|0\rangle$ with probability $|c_0|^2$

and to state $|1\rangle$ with probability $|c_1|^2$.

Ways of writing a qubit:

$$\begin{bmatrix} c_0 \\ c_1 \end{bmatrix} = c_0|0\rangle + c_1|1\rangle$$

for eg;

$$\begin{bmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{bmatrix} = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

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

$$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix} = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

$$= \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Notice that: $$\frac{|0\rangle - |1\rangle}{\sqrt{2}} = (-1)\cdot\frac{|1\rangle - |0\rangle}{\sqrt{2}}$$

Implementation of qubits: → Chapter 11 of the book gives some details

Some examples:

→ an electron might be in one of two different orbits around the nucleus of an atom

→ a photon might be in one of two polarized states

→ a subatomic particle might have one of two spin directions

Example:

Let $V = \begin{bmatrix} 5+3i \\ 6i \end{bmatrix}$

This is not a qubit since $|5+3i|^2 + |6i|^2 \neq 1$

To make it represent a qubit, divide V by its norm $\sqrt{\langle v, v \rangle}$

$$|V| = \sqrt{\langle v, v \rangle} = \sqrt{\begin{bmatrix} 5-3i, & -6i \end{bmatrix} \begin{bmatrix} 5+3i \\ 6i \end{bmatrix}} = \sqrt{34+36} = \sqrt{70}$$

$$\frac{V}{\sqrt{70}} = \begin{bmatrix} \frac{5+3i}{\sqrt{70}} \\ \frac{6i}{\sqrt{70}} \end{bmatrix} = \underbrace{\frac{5+3i}{\sqrt{70}} \cdot |0\rangle + \frac{6i}{\sqrt{70}} |1\rangle}_{\text{a qubit.}}$$

$\downarrow$

after measuring the qubit $\frac{V}{\sqrt{70}}$,

the probability of it being found in $|0\rangle$ is $\frac{34}{70}$

and the probability of it being found in $|1\rangle$ is $\frac{36}{70}$

Part 2: Qubytes

Consider a system consisting of 2 bits:

0 1

value of first bit — value of second bit

In the quantum setting, we use tensor product to represent combination of states.

Let us see what $|0\rangle \otimes |1\rangle$ corresponds to:

$$|0\rangle \otimes |1\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

$$\begin{matrix} 00 \\ 01 \\ 10 \\ 11 \end{matrix} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \rightarrow$$ There is a 1 corresponding to the entry 01.

Similarly $|0\rangle \otimes |0\rangle \otimes |1\rangle$ will correspond to 001.

$$\begin{matrix} 000 \\ 001 \\ 010 \\ 011 \\ 100 \\ 101 \\ 110 \\ 111 \end{matrix} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

Consider a byte (8 bits): 01110101

As a qubit, it is $|0\rangle \otimes |1\rangle \otimes |1\rangle \otimes |1\rangle \otimes |0\rangle \otimes |1\rangle \otimes |0\rangle \otimes |1\rangle$

$$\begin{matrix} 00000000 \\ \vdots \\ 01110101 \\ \vdots \\ 11111111 \end{matrix} \begin{bmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix}$$ a 256×1 matrix

- Eight qubits together is called a qubyte.

A qubyte can be written as:

$$\begin{matrix} 0000\,0000 \\ 0000\,0001 \\ \\ \\ \\ \\ 1111\,1111 \end{matrix} \quad \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ \\ \\ \\ c_{255} \end{bmatrix}$$

→ It requires storing 256 complex numbers.

Ways to write multiple qubits:

$$|0\rangle \otimes |1\rangle \quad \text{or} \quad |0 \otimes 1\rangle \quad \text{or} \quad |01\rangle$$

↑

first qubit is in $|0\rangle$ & second qubit is in $|1\rangle$

Examples:

- $3|01\rangle + 2|11\rangle = \begin{bmatrix} 0 \\ 3 \\ 0 \\ 2 \end{bmatrix}$ → not a qubit since $|3|^2 + |2|^2 \neq 1$

- $\frac{1}{\sqrt{3}} \begin{bmatrix} 1 \\ 0 \\ -1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{3}}|00\rangle - \frac{1}{\sqrt{3}}\cdot|10\rangle + \frac{1}{\sqrt{3}}|11\rangle$

↳ a qubit.

- General form of a two-qubit system:

$$|\psi\rangle = c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle$$

s.t. $|c_{00}|^2 + |c_{01}|^2 + |c_{10}|^2 + |c_{11}|^2 = 1$

Entangled qubits:

Suppose the state of the system is:

$$\frac{|11\rangle + |00\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}|11\rangle + \frac{1}{\sqrt{2}}|00\rangle$$

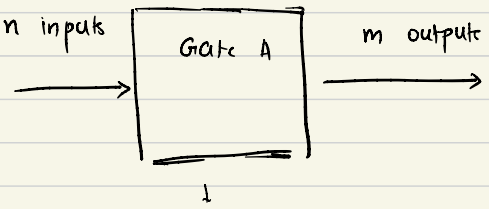
→ If we measure first qubit and find its state to be $|1\rangle$, then the second qubit will be in state $|1\rangle$

Similarly if first qubit is in $|0\rangle$, then second will be in $|0\rangle$.

→ These two qubits are entangled.

Part 3: Classical gates

We will represent classical logic gates / circuit as matrices.

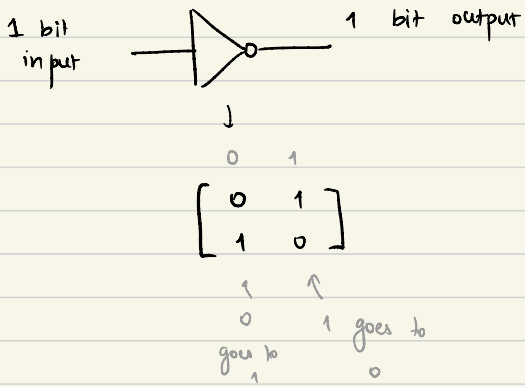


2^m-by-2^n matrix

$$(2^m\text{-by-}2^n) \ * \ (2^n\text{-by-}1) = (2^m\text{-by-}1)$$

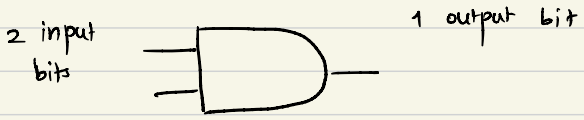
matrix multiplication

Example 1: NOT Gate



$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Example 2: AND Gate



2^1-by-2^2 matrix

$$\begin{array}{c} \\ 0 \\ 1 \end{array}\begin{array}{c} \begin{array}{cccc} 00 & 01 & 10 & 11 \end{array} \\ \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \end{array}$$

$00 \to 0$ $\quad 01 \to 0$ $\quad 10 \to 0$ $\quad 11 \to 1$

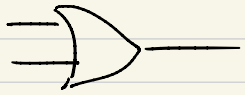
$$\text{AND} = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\text{AND } |11\rangle = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle$$

$\therefore$ AND $|11\rangle = |1\rangle$

Similarly AND $|10\rangle = |0\rangle$

Example 3: OR Gate

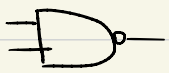


↓

2^1 - by - 2^2 matrix

	00	01	10	11
0	1	0	0	0
1	0	1	1	1

Example 4: NAND gate



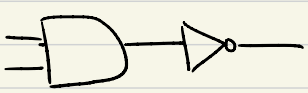
↓

2^1 - by - 2^2 matrix

	00	01	10	11
0	0	0	0	1
1	1	1	1	0

Combining Gates:

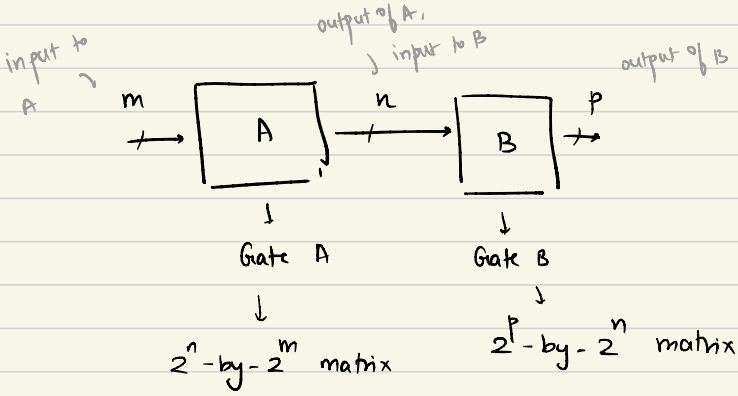
NAND:



NOT $*$ AND = NAND

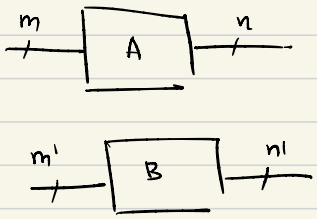
↓

matrix multiplication



Sequential combination

Sequential combination given as: $B * A$



Parallel combination

$A \otimes B$

A: 2^n - by - 2^m

B: $2^{n'}$ - by - $2^{m'}$

$A \otimes B$: $2^n \cdot 2^{n'}$ - by - $2^m \cdot 2^{m'}$

$= 2^{(n+n')}$ - by - $2^{(m+m')}$

- $B \otimes A$ is almost equal to $A \otimes B$ except for rows and columns interchanged.

So we say: $A \otimes B \cong B \otimes A$

(without formally going into details of this equivalence)

→ Try an example to get an idea.

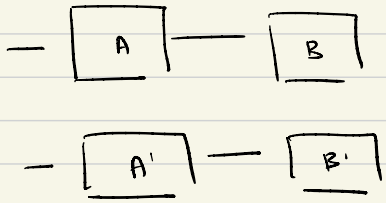
Classical circuits:

- This will be a combination of gates
  - ↳ can be appropriately written as matrices using matrix multiplication $*$ and tensor product $\otimes$

Useful fact:

$$(B \otimes B') * (A \otimes A') = (B * A) \otimes (B' * A')$$

Interpretation for circuits:



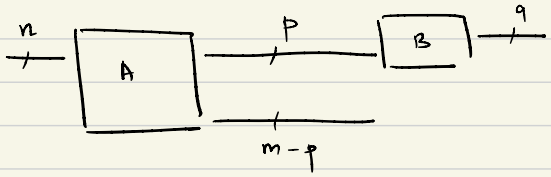
We can do the sequential operations $B * A$ and $B' * A'$ and then take the parallel combination.

or

first do the parallel combinations $B \otimes B'$, $A \otimes A'$ and then combine sequentially.

→ Both result in the same matrix.

Example:



A: n inputs, m outputs

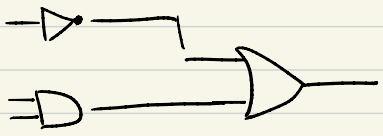
B: takes the first p bits of A's output and produces q outputs.

∴ A: 2^m-by-2^n, B: 2^q-by-2^p

Combination: $(B \otimes I_{m-p}) * A$

↳ Identity matrix with $m-p$ rows.

Example:



OR * (NOT ⊗ AND)

Part 4: Reversible gates

- Consider NOT gate. If output is $|1\rangle$ then we know input is $|0\rangle$
  output is $|0\rangle$ ——— $|1\rangle$

NOT is reversible.

In fact, NOT is reversible by applying itself.

NOT * NOT = I

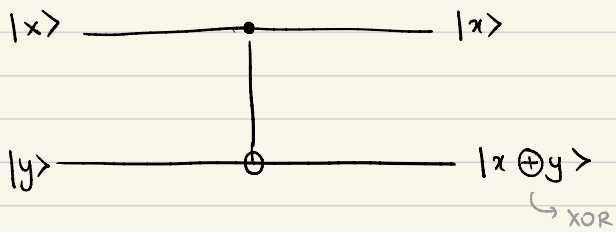
↓

its own inverse.

- AND is not reversible. If output of AND is $|0\rangle$, we do not know what was the input. It could have been $|00\rangle$, $|01\rangle$ or $|10\rangle$.

Reversible gates: from the outputs, one can determine the inputs.

Example: A controlled – NOT gate



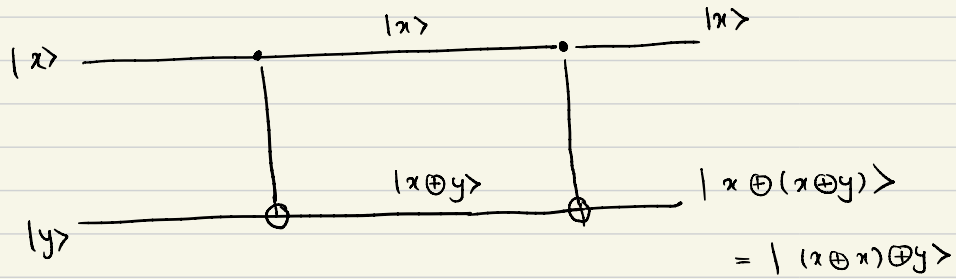
↳ XOR operation

2 inputs, 2 outputs: if $|x\rangle = |0\rangle$, bottom output is same as $|y\rangle$
$|x\rangle = |1\rangle$, bottom output will be opposite of $|y\rangle$

Matrix corresponding to controlled-NOT:

$$\begin{array}{c} \\ 00 \\ 01 \\ 10 \\ 11 \end{array} \begin{array}{c} \begin{array}{cccc} 00 & 01 & 10 & 11 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \end{array} \longrightarrow A$$

Controlled-NOT gate can be reversed by itself:

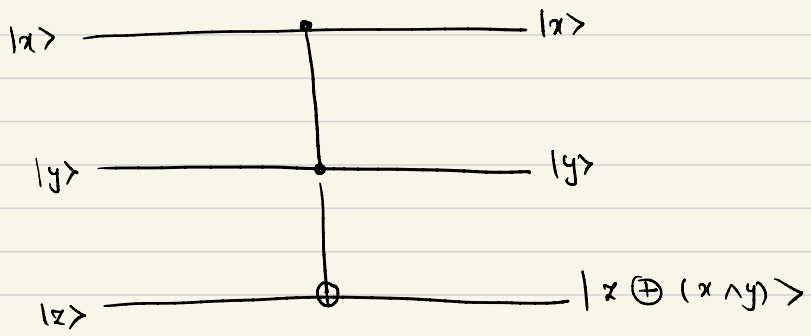


$$= |(x \oplus x) \oplus y\rangle$$
$$= |0 \oplus y\rangle$$
$$= |y\rangle$$

In fact, matrix A above has itself as its inverse.

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} * \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

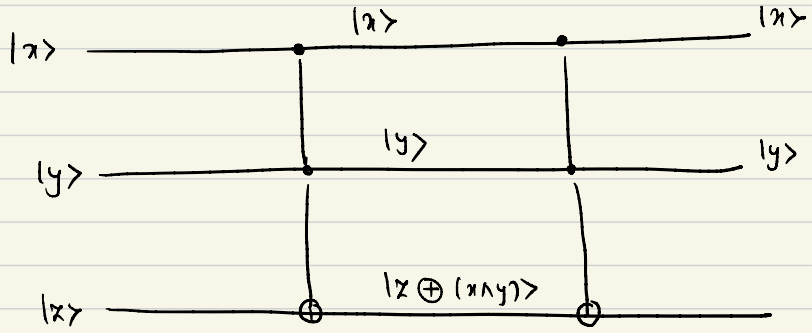
Example: Toffoli gate



→ 2 controlling bits $|x\rangle$ and $|y\rangle$

→ Bottom bit flips if both $|x\rangle$ and $|y\rangle$ are $|1\rangle$

Toffoli gate is reversible by itself.



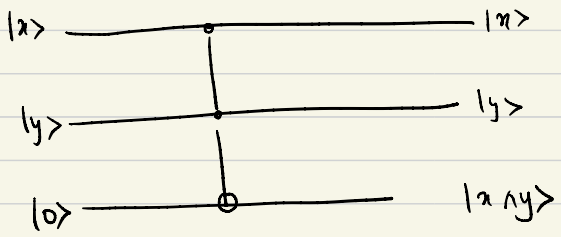
$= |z \oplus ((x \wedge y) \oplus (x \wedge y))\rangle$

$= |z\rangle$

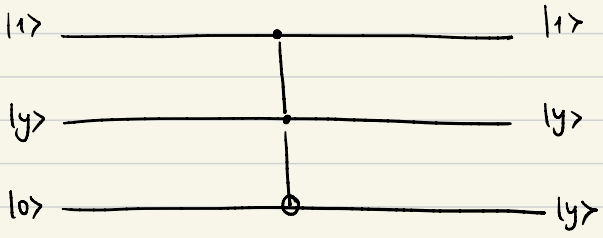
Matrix corresponding to Toffoli gate is its own inverse.

Fact: Toffoli gate is universal. Every logical gate can be made using Toffoli gates.

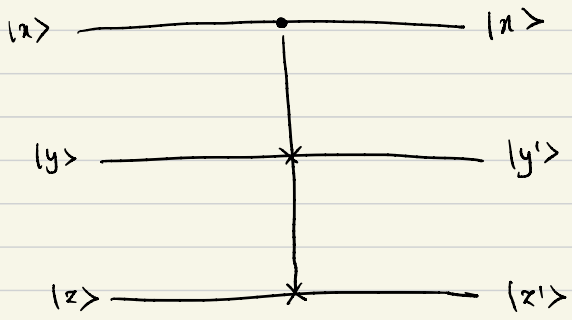
For eg. AND gate :



Copying input to multiple outputs:



Example: Fredkin gate



if $|x\rangle = 0$ then $|y'\rangle = |y\rangle$ and $|z'\rangle = |z\rangle$

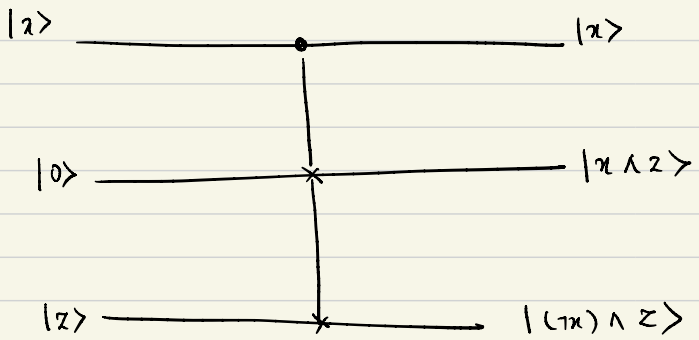
$|x\rangle = 1$ then $|y'\rangle = |z\rangle$ and $|z'\rangle = |y\rangle$

$$|0, y, z\rangle \longrightarrow |0, y, z\rangle \quad \text{and} \quad |1, y, z\rangle \longrightarrow |1, z, y\rangle$$

→ Fredkin gate can also be reversed by applying it twice.
(Fredkin gate is its own inverse).

→ fredkin gate is also universal.

Example: Implement AND gate using fredkin gate.



Part 5: Quantum gates

> A quantum gate is an operator that acts on qubits.
> Such operators will be represented by unitary matrices

- Not gate, controlled-NOT, Toffoli, Fredkin gate are all quantum gates.

Some more examples of quantum gates:

- **Hadamard gate:** $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{bmatrix}$

$H^{-1} = H$

$$\begin{bmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \end{bmatrix} = \begin{bmatrix} 1/\sqrt{2}\, c_0 + 1/\sqrt{2}\, c_1 \\ 1/\sqrt{2}\, c_0 - 1/\sqrt{2}\, c_1 \end{bmatrix}$$

↑ a qubit, $|c_0|^2 + |c_1|^2 = 1$

↘ also a qubit

- **Pauli matrices**

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \qquad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

↳ all unitary

- $S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \qquad T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$

- **$\sqrt{NOT}$:** $\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}$ The gate is not its own inverse.

Moreover $\sqrt{NOT} * \sqrt{NOT} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ (similar to NOT gate)

see next page.

Putting qubits $|0\rangle$ and $|1\rangle$ through $\sqrt{NOT}$ twice:

$$|0\rangle = [1,0]^T \longmapsto \left[\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right]^T \longrightarrow [0,1]^T = |1\rangle$$

$$|1\rangle = [0,1]^T \longmapsto \left[\frac{-1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right]^T \longrightarrow [-1,0]^T = (-1)|0\rangle$$

same state as $|0\rangle$ in the quantum setting (all scalar multiple represent same state).

Summary:

→ Quantum gates are unitary matrices. There are some gates which seem to be not unitary. But we will ignore them for now.

→ Quantum circuits can be formed by $*$ and $\otimes$