Quantum gates II

Quantum computing

G. Chênevert

Jan. 20, 2023

Quantum gates II

Review of last time

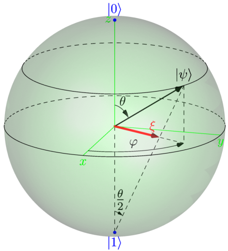
Multiple qubit gates

Last time

- Every qubit state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is equivalent to a state of the form

$$\cos(\tfrac{\theta}{2})|0\rangle + e^{i\varphi}\sin(\tfrac{\theta}{2})|1\rangle$$

corresponding to a (unique) point on the Bloch sphere.



Quantum gates

Certain qubit operations can be represented by 2×2 matrices :

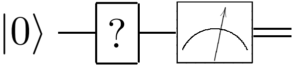
$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \qquad P = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix}$$

$$U = \begin{bmatrix} \cos(\frac{\theta}{2}) & -e^{i\lambda} \sin(\frac{\theta}{2}) \\ e^{i\varphi} \sin(\frac{\theta}{2}) & e^{i(\lambda+\varphi)} \cos(\frac{\theta}{2}) \end{bmatrix}$$

Review quiz: `https://www.wooclap.com/QCOMP`

Exercise: general TRBG

Write a quantum program that outputs $|1\rangle$ with probability 62%.



Solution: it suffices to use a universal gate U with $\theta \approx 1.81316$ (why??)

You may verify on IBM Q that it actually works.

Quantum gates II

Review of last time

Multiple qubit gates

2-qubit system

Consider a system with two qubits A and B. Suppose:

A is in state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

B is in state $|\phi\rangle = \gamma|0\rangle + \delta|1\rangle$

Then the system (A, B) is in state

$$|\psi\rangle \otimes |\phi\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \delta|1\rangle)$$

$$= \alpha\gamma|0\rangle \otimes |0\rangle + \alpha\delta|0\rangle \otimes |1\rangle + \beta\gamma|1\rangle \otimes |0\rangle + \beta\delta|1\rangle \otimes |1\rangle$$

$$= \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle$$

2-qubit system

More generally: the 2-qubit system can be in *any* linear combination state

$$a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle \in \mathcal{V}_2 \otimes \mathcal{V}_2 = \mathcal{V}_4$$

Some of these can*not* be written in the form $|\psi\rangle \otimes |\phi\rangle$: called **entangled**

Example

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} \qquad \textbf{Bell state}$$

Two qubit gates

Do we have the analogues of the classical AND, OR, XOR, NAND, ... gates for quantum bits?

NO! They lose information...

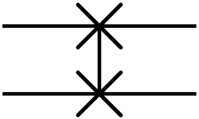
Recall: the space of quantum states for a system of 2 qubits is

$$\mathcal{V}_2 \otimes \mathcal{V}_2 \cong \mathcal{V}_4$$

basis $|0\rangle \otimes |0\rangle$, $|0\rangle \otimes |1\rangle$, $|1\rangle \otimes |0\rangle$, $|1\rangle \otimes |1\rangle$ or $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$ or $|0\rangle$, $|1\rangle$, $|2\rangle$, $|3\rangle$

2-qubit gates are represented by 4×4 *unitary matrices*

SWAP gate



$$|\psi\rangle \otimes |\phi\rangle \;\mapsto\; |\phi\rangle \otimes |\psi\rangle$$

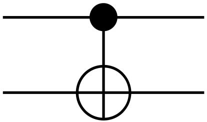
$$\mathrm{SWAP} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \mathrm{diag}(1, X, 1)$$

CNOT = CX gate

$$\mathrm{CX}(|x\rangle \otimes |y\rangle) \text{ "} = \text{" } X^x|y\rangle = \begin{cases} |y\rangle & \text{if } |x\rangle = |0\rangle \\ X|y\rangle & \text{if } |x\rangle = |1\rangle \end{cases} = |x \oplus y\rangle$$

To be able to go back we must output $|x\rangle$ as well:

$$\text{"}\,\mathrm{CX}\begin{bmatrix} |x\rangle \\ |y\rangle \end{bmatrix} = \begin{bmatrix} |x\rangle \\ |x \oplus y\rangle \end{bmatrix}\text{"}$$



CNOT = CX gate

Proper way to write this:

$$\mathrm{CX}(|x\rangle \otimes |y\rangle) = |x\rangle \otimes (|x \oplus y\rangle)$$

$$\mathrm{CX}\big(|0\rangle \otimes |\phi\rangle\big) = |0\rangle \otimes |\phi\rangle \qquad \mathrm{CX}\big(|1\rangle \otimes |\phi\rangle\big) = |1\rangle \otimes X|\phi\rangle$$

$$\mathrm{CX} = \mathrm{diag}(I, X) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Reversible operation ! $\mathrm{CX}^2 = I$

Exercise

What is the matrix representation of the 2-qubit gate corresponding to the application of X on the first qubit and H on the second qubit?

Answer:

$$X \otimes H = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \\ 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \end{bmatrix}$$

This can be verified on IBM Q by applying $X \otimes H$ to $|00\rangle, |01\rangle, |10\rangle, |11\rangle$.

!! Watch out for bit-order conventions !!

Other boolean operations

So far we know how to build quantum circuits computing NOT and XOR.

What about other logical gates, *e.g.* AND and OR?

Recall that quantum gates are represented by unitary matrices, *hence always reversible*.

$\implies$ ancillary qubits are needed

The Toffoli gate

Reversibly computes the logical AND of two qubits:

$$\mathrm{Toff}(|x\rangle\,|y\rangle\,|z\rangle) = |x\rangle\,|y\rangle\,|z \oplus \mathrm{AND}(x,y)\rangle$$

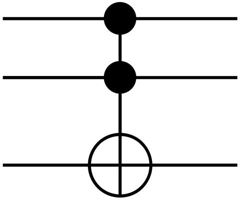
Note:

$$\mathrm{Toff}(|x\rangle\,|y\rangle\,|z\rangle) = \begin{cases} |x\rangle\,|y\rangle\,|z\rangle & \text{if } x = 0 \\ |x\rangle\,|y\rangle\,|y \oplus z\rangle & \text{if } x = 1 \end{cases}$$

so the Toffoli gate may be viewed as a controlled-CNOT gate.

The Toffoli (or CCNOT) gate

$$\mathrm{Toff}(|x\rangle\,|y\rangle\,|z\rangle) = |x\rangle\,|y\rangle\,|z \oplus \mathrm{AND}(x, y)\rangle$$



$$\begin{bmatrix} 1 & & & & & & & \\ & 1 & & & & & & \\ & & 1 & & & & & \\ & & & 1 & & & & \\ & & & & 1 & & & \\ & & & & & 1 & & \\ & & & & & & & 1 \\ & & & & & & 1 & \end{bmatrix}$$

Reversible evaluation

More generally: $f : \{0,1\}^n \to \{0,1\}$ is any boolean function

consider the gate U_f on $n+1$ qubits defined by

$$U_f : |\mathbf{x}\rangle \otimes |y\rangle \mapsto |\mathbf{x}\rangle \otimes |y \oplus f(\mathbf{x})\rangle.$$

You may check that this is a unitary operator on $\mathcal{V}_{2^n} \otimes \mathcal{V}_2 = (\mathcal{V}_2)^{\otimes(n+1)}$

that allows to evaluate f on $\mathbf{x}$ without losing $\mathbf{x}$:

$$U_f(|\mathbf{x}\rangle|0\rangle) = |x\rangle|f(\mathbf{x})\rangle.$$

Quantum gates, general case

General case of a n-qubit system:

$$\underbrace{\mathcal{V}_2 \otimes \cdots \otimes \mathcal{V}_2}_{n} \cong \mathcal{V}_{2^n}$$

Any reversible quantum operation can be viewed as a $2^n \times 2^n$ unitary matrix:

$$G \in \mathrm{U}(2^n).$$

Usually described as a **quantum circuit** made of gates on smaller numbers of qubits.