An Introduction to Quantum Computing

Lecture 15:

Implementing Quantum Circuits

Paolo Zuliani

Dipartimento di Informatica
Università di Roma "La Sapienza", Rome, Italy

SAPIENZA
UNIVERSITÀ DI ROMA

Agenda

- Single qubits gates via rotation
- Controlled operation gates
- Universal set of gates

Implementing Quantum Circuits

- Given a quantum circuit (*i.e.*, a unitary operator acting on n qubits), how do we implement it on a quantum computer?
- The set of quantum circuits is *uncountable* (there as many quantum circuits as real/complex numbers).

Implementing Quantum Circuits

- Given a quantum circuit (*i.e.*, a unitary operator acting on n qubits), how do we implement it on a quantum computer?
- The set of quantum circuits is *uncountable* (there as many quantum circuits as real/complex numbers).
- **Question**: is there a *universal* set of gates? (Like for classical Boolean circuits.)
- Answer: kind of!
  - *Exact* implementation
  - *Approximate* implementation

Single Qubits Gates

The Pauli matrices (Wolfgang Pauli 1900-1958, Physics Nobel Prize):

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

Single Qubits Gates

The Pauli matrices (Wolfgang Pauli 1900-1958, Physics Nobel Prize):

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

Hadamard

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

Phase gate

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

$\pi/8$ gate

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

Note: $H = (X + Z)/\sqrt{2}$ and $T^2 = S$ (*i.e.*, T is the square root of S).

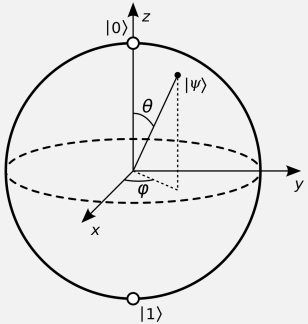
Bloch Sphere (recap)

After Felix Bloch (1905-1983), Physics Nobel Prize.

A qubit can be written as:

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$$

where $0 < \theta < \pi$ and $0 < \varphi 2\pi$.



https://en.wikipedia.org/wiki/File:Bloch_sphere.svg

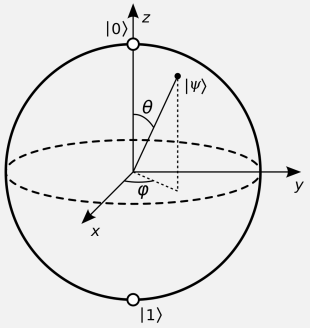
Rotations

Can be defined for an arbitrary angle θ:

$$R_x(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix} = \cos\frac{\theta}{2} I - i\sin\frac{\theta}{2} X$$

$$R_y(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix} = \cos\frac{\theta}{2} I - i\sin\frac{\theta}{2} Y$$

$$R_z(\theta) = \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix} = \cos\frac{\theta}{2} I - i\sin\frac{\theta}{2} Z$$



https://en.wikipedia.org/wiki/File:Bloch_sphere.svg

Rotations I

Theorem

Suppose U is a unitary operation of a single qubit. Then there exist real numbers α, β, γ and δ such that

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta).$$

Rotations I

Theorem

Suppose U is a unitary operation of a single qubit. Then there exist real numbers α, β, γ and δ such that

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta).$$

Proof. First, note that the rows and the columns of a unitary matrix (of any size) must be orthonormal. To show this, let U be an $n \times n$ unitary operator and $\{e_i\}_{i=1}^n$ be the diagonal basis of size n.

Rotations I

Theorem

Suppose U is a unitary operation of a single qubit. Then there exist real numbers α, β, γ and δ such that

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta).$$

Proof. First, note that the rows and the columns of a unitary matrix (of any size) must be orthonormal. To show this, let U be an $n \times n$ unitary operator and $\{e_i\}_{i=1}^n$ be the diagonal basis of size n.
Observe that $Ue_i = (u_{1i}, \ldots, u_{ni})$, *i.e.*, the i-th column of U. Since $\|Ue_i\| = \|e_i\| = 1$, it follows that the i-th column of U has norm 1.

Rotations I

Theorem

Suppose U is a unitary operation of a single qubit. Then there exist real numbers α, β, γ and δ such that

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta).$$

Proof. First, note that the rows and the columns of a unitary matrix (of any size) must be orthonormal. To show this, let U be an $n \times n$ unitary operator and $\{e_i\}_{i=1}^n$ be the diagonal basis of size n.
Observe that $Ue_i = (u_{1i}, \ldots, u_{ni})$, *i.e.*, the i-th column of U. Since $\|Ue_i\| = \|e_i\| = 1$, it follows that the i-th column of U has norm 1.
To show that the rows have also norm 1, recall that $u_{ij}^\dagger = u_{ji}^*$ and note that since U is unitary then $U^\dagger$ is unitary, as well, so we can apply the same reasoning.

Rotations I

Theorem

Suppose U is a unitary operation of a single qubit. Then there exist real numbers α, β, γ and δ such that

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta).$$

Proof. First, note that the rows and the columns of a unitary matrix (of any size) must be orthonormal. To show this, let U be an $n \times n$ unitary operator and $\{e_i\}_{i=1}^n$ be the diagonal basis of size n.
Observe that $Ue_i = (u_{1i}, \ldots, u_{ni})$, *i.e.*, the i-th column of U. Since $\|Ue_i\| = \|e_i\| = 1$, it follows that the i-th column of U has norm 1.
To show that the rows have also norm 1, recall that $u_{ij}^\dagger = u_{ji}^*$ and note that since U is unitary then $U^\dagger$ is unitary, as well, so we can apply the same reasoning.
Finally, to prove orthogonality note that since U is unitary and the e_i's are orthonormal, it holds that $\forall i, j \ \langle Ue_i | Ue_j \rangle = \langle e_i | e_j \rangle = \delta_{ij}$ and therefore the rows and the columns of U are orthogonal, as well. [Proof continues on the next slide.]

Rotations II

Now, since the rows and columns of U are orthonormal, then there exist real numbers α, β, γ, and δ such that

$$U = \begin{pmatrix} e^{i(\alpha-\beta/2-\delta/2)} \cos\frac{\gamma}{2} & -e^{i(\alpha-\beta/2+\delta/2)} \sin\frac{\gamma}{2} \\ e^{i(\alpha+\beta/2-\delta/2)} \sin\frac{\gamma}{2} & e^{i(\alpha+\beta/2+\delta/2)} \cos\frac{\gamma}{2} \end{pmatrix}.$$

The proof ends by multiplying the rotation matrices as described in the Theorem's thesis to obtain the form of U above.

□

Rotations III

Corollary

Suppose U is a unitary operation of a single qubit. Then there exist operators A, B, C and D on a single qubit such that $ABC = I$ and $U = e^{i\alpha}AXBXC$, where α is some overall phase factor.

Rotations III

Corollary

Suppose U is a unitary operation of a single qubit. Then there exist operators A, B, C and D on a single qubit such that $ABC = I$ and $U = e^{i\alpha}AXBXC$, where α is some overall phase factor.

Proof. Using the previous Theorem, define the operators

- $A = R_z(\beta)R_y(\frac{\gamma}{2})$
- $B = R_y(-\frac{\gamma}{2})R_z(-\frac{\delta+\beta}{2})$
- $C = R_z(\frac{\delta-\beta}{2})$

from which $ABC = I$ follows immediately.

Rotations III

Corollary

Suppose U is a unitary operation of a single qubit. Then there exist operators A, B, C and D on a single qubit such that $ABC = I$ and $U = e^{i\alpha}AXBXC$, where α is some overall phase factor.

Proof. Using the previous Theorem, define the operators

- $A = R_z(\beta)R_y(\frac{\gamma}{2})$
- $B = R_y(-\frac{\gamma}{2})R_z(-\frac{\delta+\beta}{2})$
- $C = R_z(\frac{\delta-\beta}{2})$

from which $ABC = I$ follows immediately.

The other equality follows from the fact that $XR_y(\theta)X = R_y(-\theta)$ and $XX = I$.

□

Controlled Operations (Single Qubit)

if $control\_qubit == 1$ then $target\_qubit = UnitaryOp(target\_qubit)$

Quantum gates do **not** have "hard-wired" controls and targets! They depend on what basis we think the gate is operating on.

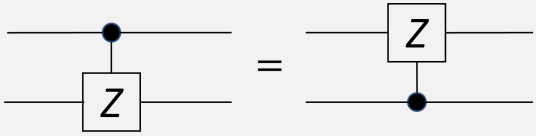
Controlled Operations (Single Qubit)

if $control\_qubit == 1$ then $target\_qubit = UnitaryOp(target\_qubit)$

Quantum gates do **not** have "hard-wired" controls and targets! They depend on what basis we think the gate is operating on.

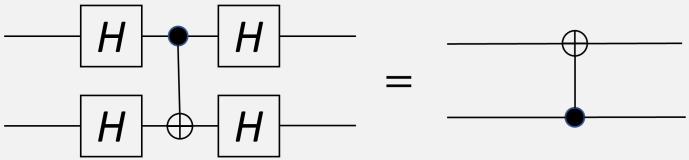
Example: control-Z

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



Controlled Operations (Single Qubit)

Example: control-*NOT*

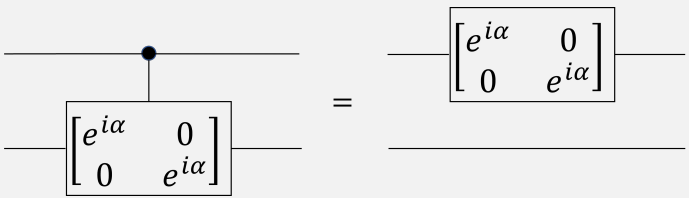


Controlled Operations (Single Qubit)

Corollary

Suppose U is a unitary operation of a single qubit. Then there exist operators A, B, C and D on a single qubit such that $ABC = I$ and $U = e^{i\alpha}AXBXC$, where α is some overall phase factor.

Let us focus on the phase $e^{i\alpha}$. One can show that:

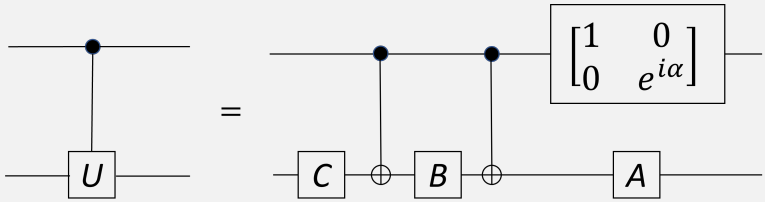


Controlled Operations (Single Qubit)

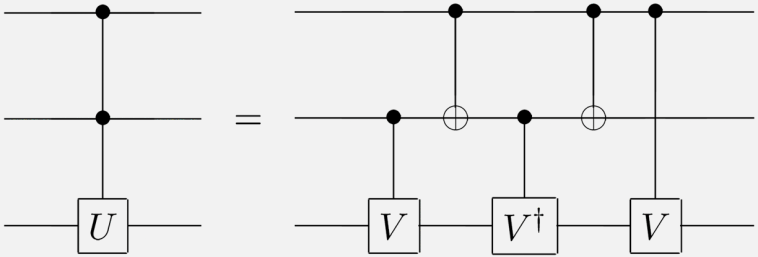
Corollary

Suppose U is a unitary operation of a single qubit. Then there exist operators A, B, C and D on a single qubit such that $ABC = I$ and $U = e^{i\alpha}AXBXC$, where α is some overall phase factor.

We have that:

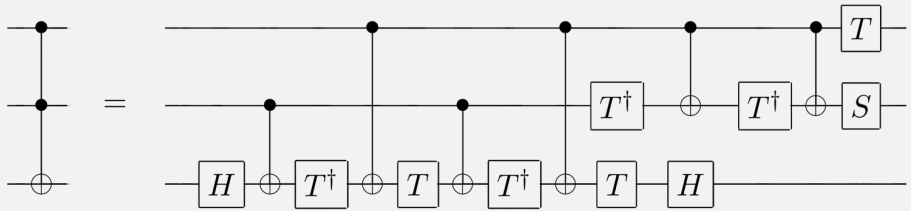


Controlled Operations (Multiple Control Qubits)



- V is the square root of U, *i.e.*, $V^2 = U$. [The square root always exists for positive operators.]
- When $U = NOT$ we get the Toffoli gate.

The Toffoli Gate



With 1-qubit and 2-qubit gates we can implement the Toffoli gate, which is universal for classical (reversible) computation!

- 1-bit and 2-bit reversible gates are **not** universal for reversible computation.

Universal Gates

Classical digital circuits: AND, OR, and NOT can be used to compute any Boolean function $\Rightarrow$ AND, OR, NOT form an *universal set of gates* (for classical circuits)

Quantum circuits: is there an *universal* set of gates?

Universal Gates

Classical digital circuits: AND, OR, and NOT can be used to compute any Boolean function $\Rightarrow$ AND, OR, NOT form an *universal set of gates* (for classical circuits)

Quantum circuits: is there an *universal* set of gates? Kind of!

- *Exact* implementation
- *Approximate* implementation

Universal Gates

- **Exact** implementation
  - Single-qubit gates + CNOT are universal, *i.e.*, can implement *exactly* any unitary operator on any number of qubits.

Universal Gates

- **Exact** implementation
  - Single-qubit gates + CNOT are universal, *i.e.*, can implement *exactly* any unitary operator on any number of qubits.

- **Approximate** implementation
  - The *Solovay-Kitaev Theorem* shows that single-qubit gates can be *approximated* using only H, phase (S), and $\pi/8$ (T) gates.
  - Therefore, H, phase, and $\pi/8$, and CNOT are universal for approximate implementation.

Universal Gates

Definition

A *two-level unitary matrix* acts nontrivially only on two (or fewer) components.

Example:

$$\begin{pmatrix} e^{i\alpha} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} ae^{i\alpha} \\ b \\ c \end{pmatrix}$$

Universal Gates

Definition

A *two-level unitary matrix* acts nontrivially only on two (or fewer) components.

Example:

$$\begin{pmatrix} e^{i\alpha} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} ae^{i\alpha} \\ b \\ c \end{pmatrix}$$

Proposition

Any unitary matrix acting on n qubits can be written exactly *as a product of* at most $2^{n-1}(2^n - 1)$ *two-level unitary matrices.*

Single-qubit Gates + CNOT Are Universal

Theorem

Any unitary transformation on n qubits can be implemented exactly by a circuit with $O(n^2 4^n)$ single-qubit gates and CNOTs.

Single-qubit Gates + CNOT Are Universal

Theorem

Any unitary transformation on n qubits can be implemented exactly by a circuit with $O(n^2 4^n)$ single-qubit gates and CNOTs.

- Two-level unitary using only single-qubit gates and CNOTs
- The proof essentially entails lots of swaps ...
- There exists unitary transformations that *necessarily* require an exponential number of gates

Universal Gates: Approximation

How can we measure the "precision" of a unitary transformation approximating another?

Universal Gates: Approximation

How can we measure the "precision" of a unitary transformation approximating another?

Definition

Let $\hat{U}$ be a unitary operator approximating the "correct" unitary U. The precision (or error) is:

$$E(\hat{U}, U) = max_{|\psi\rangle} \|(\hat{U} - U)\,|\psi\rangle\|$$

Proposition

For any $\epsilon > 0$ it is possible to approximate any single-qubit gate within precision ϵ with only Hadamard and $\pi/8$ gates.

Universal Gates: Approximation

Theorem (Solovay-Kitaev Theorem)

Any single-qubit unitary gate can be approximated *to any precision by a finite sequence of Hadamard, phase, and $\pi/8$ gates (and their inverses).*

Universal Gates: Approximation

Theorem (Solovay-Kitaev Theorem)

Any single-qubit unitary gate can be approximated *to any precision by a finite sequence of Hadamard, phase, and $\pi/8$ gates (and their inverses).*

Sequence length $\approx (\log \frac{2}{\epsilon})^c$ where ϵ is the precision of the approximation and $c \approx 2$!

- Extremely efficient!
- Only need to implement a few gates in hardware!

Universal Gates: Approximation

- Therefore, to approximate a circuit with m single-qubit gates and CNOTs, it suffices to use $O(m(\log \frac{m}{\epsilon})^c)$ gates from Hadamard, phase, $\pi/8$, and CNOT.

Universal Gates: Approximation

- Therefore, to approximate a circuit with m single-qubit gates and CNOTs, it suffices to use $O(m(\log \frac{m}{\epsilon})^c)$ gates from Hadamard, phase, $\pi/8$, and CNOT.
- Be careful! The statement does not say how large m is ...
- Approximating an arbitrary unitary over n qubits is in general hard (circuit grows exponentially large in n)

Quantum Circuit Simulation

- Some quantum circuits can be *efficiently* simulated on a classical computer.
- The Clifford gates are Hadamard, phase, and CNOT.

Theorem (Gottesman-Knill Theorem)

Any circuit consisting of Clifford gates, state preparations and measurements in the computational basis can be simulated in polynomial time on a probabilistic classical computer.